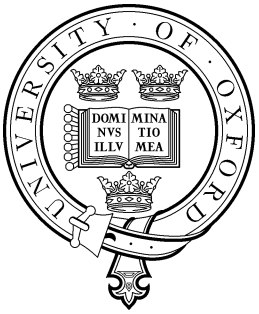
# Reachability Problems for Linear Dynamical Systems




Ventsislav Chonev

Oriel College

University of Oxford

A thesis submitted for the degree of

*Doctor of Philosophy*

Michaelmas 2015

## Acknowledgements

At the risk of treading on the reader's patience, I feel I must nonetheless mention several people whose influence has been formative and whose support indispensable. My mum Veneta Choneva and my dad Krasimir Chonev for teaching me to value learning above all else and for providing unconditionally that unwaveringly solid foundation which all young people need for any undertaking but few have. My brother Radostin Chonev, from whose diligence I draw example and inspiration daily. My wonderful girlfriend Trayana Ilkova, whose love has been a comfort during an arduous time of choices and uncertainty, and whose patience and stoicism have been nothing short of extraordinary in the face of that terrible expanse of the North Sea. My teachers Ben Worrell, Joël Ouaknine and Mike Spivey, for every single minute of their lives that they have spent to broaden my horizons and guide my steps. Finally, let this thesis bear silent witness to the memory of Kalinka Taseva, the most talented and dedicated teacher of Mathematics I have ever known, who was felled by cancer long before her time and without whose instruction, I would never have been able to start on my present path.

# Contents

# Chapter 1

# Introduction

The object of principal interest in this thesis is *linear dynamical systems:* determininstic systems which evolve under a linear operator. They are specified by an *initial state set* $I \subseteq \mathbb{R}^m$ and an *evolution matrix* $\boldsymbol{A} \in \mathbb{R}^{m \times m}$. We distinguish two varieties of linear dynamical systems: *discrete-time* and *continuous-time*. In the discrete-time setting, the state $\boldsymbol{x}(n)$ of the system at time $n \in \mathbb{N}$ is governed by the difference equation $\boldsymbol{x}(n) = \boldsymbol{A}\boldsymbol{x}(n-1)$. Similarly, in the continuous case, the state $\boldsymbol{x}(t)$ at time $t \in \mathbb{R}_{\geq 0}$ is determined by a system of first-order linear differential equations: $\boldsymbol{x}'(t) = \boldsymbol{A}\boldsymbol{x}(t)$. In both cases, $\boldsymbol{x}(0) \in I$.

Throughout the following chapters, we will be interested in the *Reachability Problem* for linear dynamical systems, which may be formulated in a general way as follows:

> Given a *target set* $\mathcal{T} \subseteq \mathbb{R}^m$ and a (discrete- or continuous-time) linear dynamical system specified by the evolution matrix $\boldsymbol{A}$ and the set of initial states $I$, determine whether for all $\boldsymbol{x}(0) \in I$, starting from $\boldsymbol{x}(0)$, the system will eventually be in a state which lies in $\mathcal{T}$.

In order to make the decision problem well-defined, one must first fix an admissible class of initial sets and, similarly, a class of target sets of interest. For the purposes of expressing the problem instance, it is also necessary to restrict the domain of the input data to a subset of $\mathbb{R}$ which may be represented effectively, such as the rational numbers $\mathbb{Q}$ or the algebraic numbers $\mathbb{A}$. As we vary the choice of domain, the types of initial and target sets under consideration and the discreteness of time, a rich landscape of decision problems emerges.

The goal of the present thesis is to explore *pointwise* reachability problems, that is, reachability from a *single initial state*. Under the assumption that $I$ consists of a single point in $\mathbb{R}^m$ provided as part of the input data, we will study reachability to polyhedral targets, in the context of both discrete- and continuous-time linear dynamical systems. We prove both upper complexity bounds and hardness results, employing in the process a wide-ranging arsenal of techniques and mathematical tools. We rely on powerful number-theoretic results, such as Baker's Theorem on inhomogeneous linear forms of logarithms of algebraic numbers, Schanuel's Conjecture on the transcendence degree of certain field extensions of the rationals, and Kronecker's Theorem on simultaneous inhomogeneous Diophantine approximation. We draw interesting connections with the study of linear recurrence sequences and exponential polynomials, and relate pointwise reachability to open problems concerning the approximability by rationals of algebraic numbers and logarithms of algebraic numbers.

Albeit a simple model, linear dynamical systems are of profound interest, both from a theoretical and a practical standpoint. Reachability problems for linear dynamical systems have recently elicited considerable attention, due to their frequent occurrence in practice and their deep and wide-ranging connections with other fascinating areas of study, such as problems on Markov chains [Akshay et al., 2015], quantum automata [Derksen et al., 2005], Lindenmayer systems [Salomaa and Soittola, 1978], linear loops (Section 1.1.1), linear recurrence sequences (Section 1.1.2) and exponential polynomials (Section 1.2.2). In this chapter, we will motivate the topic of the present thesis by outlining some of these connections. Then we will state our results and provide a high-level overview of the structure of this manuscript.

## 1.1 Discrete time

### 1.1.1 Linear loops

One of the the most compelling motivations for the study of linear dynamical systems arises from the context of program verification. Whilst verification of arbitrary programs is impossible, as evidenced by one of the early results of computability theory, Rice's Theorem [Rice, 1953], many properties nonetheless become decidable if one restricts the class of admissible programs.

One such restricted class of programs comprises unnested loops with a vector of variables $\boldsymbol{x}$ which undergo simultaneous deterministic assignments:

$$\textbf{while } \mathit{cond}(\boldsymbol{x}) \textbf{ do } \boldsymbol{x} := f(\boldsymbol{x}). \tag{1.1}$$

After specifying the domain of the variables $\boldsymbol{x}$, the permitted loop guards *cond* and the admissible update functions $f$, a natural decision problem to investigate on such programs is the *Universal Termination Problem*: does the loop (1.1) terminate for all possible initial values of $\boldsymbol{x}$?

Much effort has been focused recently on the Universal Termination Problem for *linear loops:* programs of the form (1.1) where the update function $f$ is linear or affine. The work of [Tiwari, 2004] considered loops of the form

$$\textbf{while } (\boldsymbol{B}\boldsymbol{x} > \boldsymbol{b}) \textbf{ do } \boldsymbol{x} := \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c}, \tag{1.2}$$

for matrices $\boldsymbol{A}, \boldsymbol{B}$ and vectors $\boldsymbol{b}, \boldsymbol{c}$ provided as input data, with entries belonging to some effectively expressible subset of $\mathbb{R}$. Here the guard is interpreted as a conjunction of strict inequalities. Tiwari proved that it is decidable whether (1.2) terminates on all initial valuations of the variables in $\mathbb{R}^m$. The decision procedure relies on the strictness of the inequalities in the loop guard, and, crucially, on the universal quantification over $\mathbb{R}^m$.

A more natural question from a practical standpoint is Universal Termination over $\mathbb{Q}$ or $\mathbb{Z}$. The change of domain is non-trivial: decision problems are commonly altered significantly in the transition from the real case to the integer case[1]. Two years later, the Universal Termination Problem was studied in [Braverman, 2006] for linear loops over the rationals, with both strict and non-strict loop guards:

$$\textbf{while } (\boldsymbol{B_1}\boldsymbol{x} \geq \boldsymbol{b_1} \textbf{ and } \boldsymbol{B_2}\boldsymbol{x} > \boldsymbol{b_2}) \textbf{ do } \boldsymbol{x} := \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c}, \tag{1.3}$$

where $\boldsymbol{A}, \boldsymbol{B_1}, \boldsymbol{B_2}, \boldsymbol{b_1}, \boldsymbol{b_2}, \boldsymbol{c}$ have rational entries, and the domain of $\boldsymbol{x}$ is $\mathbb{Q}^m$. For such loops, Braverman established decidability of the Universal Termination Problem over $\mathbb{Q}^m$ in the general case, and also over $\mathbb{Z}^m$ in the homogeneous case $\boldsymbol{c}, \boldsymbol{b_1}, \boldsymbol{b_2} = \boldsymbol{0}$. Though Braverman and Tiwari claim no upper complexity bound, it is remarked in reference [Ouaknine and Worrell, 2015] that if the input data is rational, then both decision procedures can be carried out in polynomial time, using standard results from linear algebra and the method of [Cai, 1994] for computing the Jordan normal form of a rational matrix.

Finally, the inhomogeneous integer case of the Universal Termination Problem for loops of the form (1.3) was shown decidable in the case of a diagonalisable update matrix $\boldsymbol{A}$ in [Ouaknine et al., 2015]. The proof relies crucially on the result of [Khachiyan and Porkolab, 1997] concerning integral points in convex semi-algebraic sets and on the powerful $S$-Units Theorem of references [Evertse, 1984] and [Van der Poorten and Schlickewei, 1982]. The problem remains open for non-diagonalisable matrices.

Complementary to this work has been the approach of synthesising *ranking functions* as proof of termination. A function from the state space of the program to some well-founded set is a ranking function for the program if and only if any transition of the program strictly reduces the value of the ranking function. Since infinite descent is impossible in well-founded sets, the existence of such a function constitutes proof of termination for the loop on all initial values. For example, consider the following linear loop:

$$\textbf{while } \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix} \boldsymbol{x} \leq \begin{bmatrix} 0 \\ -1 \end{bmatrix} \textbf{ do } \boldsymbol{x} := \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{1.4}$$

If the variables are interpreted as integers, then the function $g(\boldsymbol{x}) = x_1 + x_2 - 1$ is non-negative for all $\boldsymbol{x}$ which satisfy the guard and moreover decreases strictly with each iteration, so it is a ranking function

[1] A famous example of this is the problem of determining the validity of first-order sentences over the structure $(\mathbb{R}, <, +, \times, 0, 1)$, which is decidable by [Tarski, 1951], but becomes undecidable if variables are interpreted over $\mathbb{Z}$, even when only the existential fragment of the theory is considered, by the undecidability of Hilbert's tenth problem [Matiyasevich, 1993].

for the loop. Notice the importance of the choice of domain: if the variables are interpreted as rational numbers, then the loop is non-terminating, as evidenced by the fixed point $x_1 = x_2 = 1/2$, so no ranking function on $\mathbb{Q}^2$ exists for this loop.

Due to the inherent breadth of the definition of ranking functions, the search for them has necessarily been limited to restricted classes, particularly *linear* ranking functions. Effective synthesis methods have been considered for many different variations on the basic model of linear loops. For example, the work of [Podelski and Rybalchenko, 2004] constructs linear ranking functions for loops which admit non-deterministic updates, provided each iteration respects a given set of linear inequalities between the entry and exit values of the variables. This work is also at the core of the termination analysis tool *Terminator* [Cook et al., 2006], which was developed at Microsoft Research and is being used successfully to verify the liveness of Windows device drivers. Other examples of synthesis of linear ranking functions are [Sohn and Van Gelder, 1991, Feautrier, 1992, Colón and Sipma, 2001, Mesnard and Serebrenik, 2008, Alias et al., 2010]. Broadly, the approach is based on constraint solving and yields polynomial-time methods via a reduction to linear programming. Some of these methods are complete over $\mathbb{Q}^m$, in the sense that if a linear ranking function exists on $\mathbb{Q}^m$, then one is guaranteed to be found. It is also reported in [Ben-Amram and Genaim, 2013] that some of these references erroneously claim completeness over $\mathbb{Z}^m$, when their procedures actually yield false negatives on examples such as (1.4). The same paper shows that in the integer case the problem of determining the existence of a linear ranking function is indeed more difficult (**coNP**-complete). This case is also the focus of reference [Bradley et al., 2005], which studies linear ranking functions for loops with integral division and modulus as primitive operations. Broader classes of ranking functions have also been studied, such as the disjunctive ranking relations of [Chen et al., 2012] and the lexicographic-linear ranking functions of [Ben-Amram and Genaim, 2014].

Whilst the Universal Termination Problem for linear loops has received ample attention in the last three decades, work on the *Pointwise Termination Problem*, sometimes called the *Halting Problem*, has been more scarce. This is the problem of determining whether the given loop halts, starting from a specific initial value provided as input. Reference [Kannan and Lipton, 1980] gives a polynomial-time algorithm for the Halting Problem for loops of the form

$$\textbf{while } \boldsymbol{x} \neq \boldsymbol{y} \textbf{ do } \boldsymbol{x} := \boldsymbol{A}\boldsymbol{x},$$

where $\boldsymbol{A}, \boldsymbol{x}$ and $\boldsymbol{y}$ have rational entries. This was later strengthened to place the decision method in the logspace counting hierarchy **GapLH** [Arvind and Vijayaraghavan, 2011]. Some further decidability results follow directly from work on linear recurrence sequences, which we recount in Section 1.1.2, for linear loops over the rational numbers with a single guard of the form $\boldsymbol{y}^{\boldsymbol{T}}\boldsymbol{x} \neq 0$ or $\boldsymbol{y}^{\boldsymbol{T}}\boldsymbol{x} \geq 0$ and with the size of the update matrix $\boldsymbol{A}$ bounded by a constant.

The Halting Problem for homogeneous linear loops is equivalent to pointwise reachability in discrete-time linear dynamical systems: the update matrix and the initial state are the same, whilst the target set for the linear dynamical system comprises all points which violate the guard of the loop. Moreover, one can easily accommodate loops with affine updates at the cost of increasing the dimension of the update matrix by 1. Indeed, the inhomogeneous loop

$$\textbf{while } \mathit{cond}(\boldsymbol{x}) \textbf{ do } \boldsymbol{x} := \boldsymbol{A}\boldsymbol{x} + \boldsymbol{c}$$

halts on $\boldsymbol{x_0}$ if and only the homogeneous loop

$$\textbf{while } \mathit{cond}(\boldsymbol{x}) \textbf{ do } \begin{bmatrix} \boldsymbol{x} \\ z \end{bmatrix} := \begin{bmatrix} \boldsymbol{A} & \boldsymbol{c} \\ \boldsymbol{0} & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{x} \\ z \end{bmatrix}$$

halts on $(\boldsymbol{x_0}, 1)^T$, where $z$ is a fresh variable.

### 1.1.2 Linear recurrence sequences

Another connection is the study of linear recurrence sequences and exponential polynomials. A *linear recurrence sequence (LRS)* over a field $\mathbb{F}$ is an infinite sequence $\langle u_n \rangle_{n=0}^{\infty}$ of terms in $\mathbb{F}$ such that there exists a natural number $k$ and numbers $a_1, \ldots, a_k \in \mathbb{F}$ such that $a_k \neq 0$ and $\langle u_n \rangle_{n=0}^{\infty}$ satisfies the linear recurrence equation

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n. \tag{1.5}$$

The recurrence is said to have order $k$. Note that the same sequence can satisfy different recurrence relations, but it satisfies a unique recurrence of minimum order.

As we show in Section 2.3.1, each LRS $\langle u_n \rangle_{n=0}^{\infty}$ of order $k$ may be written in the form $u_n = \boldsymbol{y}^{\boldsymbol{T}} \boldsymbol{A}^n \boldsymbol{x}$, for vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^k$ and a matrix $\boldsymbol{A} \in \mathbb{F}^{k \times k}$, and conversely, for any such $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{A}$, the sequence $\boldsymbol{y}^{\boldsymbol{T}} \boldsymbol{A}^n \boldsymbol{x}$ satisfies a linear recurrence equation of order at most $k$. Since the state of a discrete-time linear dynamical system at time $n$ is given by $\boldsymbol{x}(n) = \boldsymbol{A}^n \boldsymbol{x}(0)$, it is clear that as a function of $n$, each component of $\boldsymbol{x}(n)$ is a linear recurrence sequence. Four decision problems on LRS are prominent in the literature, each of which may be formulated readily as a reachability problem for discrete-time linear dynamical systems:

1. Given an LRS $\langle u_n \rangle_{n=0}^{\infty}$, does $u_n = 0$ for some $n \in \mathbb{N}$?
2. Given an LRS $\langle u_n \rangle_{n=0}^{\infty}$, does $u_n = 0$ for infinitely many $n \in \mathbb{N}$?
3. Given a real-valued LRS $\langle u_n \rangle_{n=0}^{\infty}$, is $u_n \geq 0$ for all $n \in \mathbb{N}$?
4. Given a real-valued LRS $\langle u_n \rangle_{n=0}^{\infty}$, is $u_n \geq 0$ for all but finitely many $n \in \mathbb{N}$?

Problem 1 is equivalent to pointwise reachability for a discrete-time linear dynamical system to an $(m-1)$-dimensional subspace of $m$-dimensional Euclidean space. It is known as the *(Discrete) Skolem Problem* and has a rich history. The celebrated Skolem-Mahler-Lech Theorem [Skolem, 1934, Mahler, 1935, Lech, 1953] characterises the set of zeros $\{n \in \mathbb{N} : u_n = 0\}$ of the linear recurrence sequence as semilinear, that is, as the union of a finite set with finitely many arithmetic progressions, provided $\mathbb{F}$ has characteristic 0. Although the zeros of LRS have been studied for decades, the decidability of the Discrete Skolem Problem is open. The independent work of [Mignotte et al., 1984, Vereshchagin, 1985] established decidability for LRS of order at most 3 over the algebraic numbers $\mathbb{A}$ and for LRS of order at most 4 over the real algebraic numbers. These are powerful results and rely on deep number-theoretic machinery, specifically, on Baker's Theorem on linear forms of logarithms of algebraic numbers (for which Baker received the Fields Medal in 1970) and on van der Poorten's analogous results for $p$-adic valuations. More recently, decidability for LRS of order 5 was announced in [Halava et al., 2005], and decidability for all orders was claimed in [Litow, 1997], but as pointed out in [Ouaknine and Worrell, 2012], both are erroneous. With regards to lower bounds, the Discrete Skolem Problem was proven **NP**-hard in [Blondel and Portier, 2002].

We call Problem 2 the *Discrete Infinite Zeros Problem*. It is equivalent to the decision problem of whether a discrete-time linear dynamical system reaches an $(m-1)$-dimensional subspace of $m$-dimensional Euclidean space infinitely often. In the case of rational LRS, decidability was established in [Berstel and Mignotte, 1976], whose method computes an effective representation of the arithmetic progressions which comprise the infinite component of the zero set of the LRS. It was later observed in [Vereshchagin, 1985] that the same proof readily generalises to LRS over the algebraic numbers.

Problems 3 and 4 are known as the *Positivity Problem* and the *Ultimate Positivity Problem*, respectively. Their complements are equivalent to the decision problem of whether a discrete-time linear dynamical system reaches an $m$-dimensional open halfspace of $\mathbb{R}^m$, respectively at least once and infinitely often. For both problems, the literature has focused exclusively on LRS over $\mathbb{Z}$, or equivalently, over $\mathbb{Q}$. Whilst the zero set of a linear recurrence sequence is well-understood, relatively little is known about the set of indices $\{n \in \mathbb{N} : u_n \geq 0\}$ where the LRS is non-negative. It is known from reference [Bell and Gerhold, 2007] that its natural density always exists, but there is no analogue of the Skolem-Mahler-Lech Theorem to describe this set more precisely.

Before outlining the known results on Positivity and Ultimate Positivity, let us mention some easily shown reductions amongst the four problems we have stated. First, given a rational LRS, a simple scaling argument allows us to construct another LRS over the integers with the same order and zero set, rendering the rational and the integer cases of the Discrete Skolem Problem equivalent. Second, an integer LRS $\langle u_n \rangle_{n=0}^{\infty}$ has a zero if and only if the sequence $\langle v_n \rangle_{n=0}^{\infty}$ defined by $v_n = u_n^2 - 1$ has a negative term. Since LRS are closed under addition and multiplication [Everest et al., 2003], the sequence $\langle v_n \rangle_{n=0}^{\infty}$ is also a linear recurrence sequence, albeit of greater order, so we have shown a reduction from the Skolem Problem to the complement of the Positivity Problem. Finally, notice that the Positivity Problem becomes trivial given a procedure for Ultimate Positivity which not only decides the problem but also computes a threshold $N$ beyond which the given sequence is never negative, if such a threshold exists.

For the Positivity Problem, references [Halava et al., 2006, Laohakosol and Tangsupphathawat, 2009] give decision procedures for LRS of order 2 and 3, relying only on elementary techniques and, in one instance, Kronecker's Approximation Theorem. An erroneous proof for order 4 was also announced in [Tangsupphathawat et al., 2012]. Finally, [Ouaknine and Worrell, 2014a, Ouaknine and Worrell, 2014b] established decidability, with complexity in the fourth level of the counting hierarchy, for LRS of order at most 5, or of order up to 9 under the simplifying assumption that the given LRS is *simple*, that is, it may be written in matrix form as $\boldsymbol{y}^{\boldsymbol{T}}\boldsymbol{A}^n\boldsymbol{x}$ with a diagonalisable matrix $\boldsymbol{A}$.

For the Ultimate Positivity Problem, elementary approaches have yielded decidability for LRS of order 2 [Burke and Webb, 1981] and 3 [Nagasaka and Shiue, 1990, Laohakosol and Tangsupphathawat, 2009]. More recently, decidability was established for LRS of order up to 5 with polynomial-time complexity and for simple LRS of arbitrary order in [Ouaknine and Worrell, 2014a, Ouaknine and Worrell, 2014b] with complexity in the counting hierarchy. Due to the non-constructive nature of the Diophantine approximation tools underlying the decision procedure, beyond order 9 the method for the Ultimate Positivity Problem does not yield a threshold $N$ such that $u_n \geq 0$ for all $n \geq N$.

In terms of lower bounds, the Positivity Problem immediately inherits **coNP**-hardness from the reduction from the Discrete Skolem Problem and the work of [Blondel and Portier, 2002]. More interestingly, reference [Ouaknine and Worrell, 2014b] proved a strong hardness result for the Positivity Problem and the Ultimate Positivity Problem at order 6 or greater, namely that decidability would entail a method to approximate to within arbitrary precision respectively the Lagrange constant $L_\infty(x)$ and the homogeneous Diophantine approximation type $L(x)$ of all real numbers $x$ of the form $\arg(\lambda)/2\pi$ with $\lambda$ a Gaussian rational. As we explain in Section 2.2, this would be a significant advancement in number theory, as currently almost nothing is known about $L_\infty(x)$ and $L(x)$ for any specific $x$. Finally, the same paper showed that for simple LRS, Ultimate Positivity is hard for the class **co**$\exists\mathbb{R}$. This is the complement of the class $\exists\mathbb{R}$, introduced in [Schaefer and Štefankovic, 2011], which lies between **NP** and **PSPACE**, and comprises all problems reducible in polynomial time to the problem of deciding the validity of existentially quantified sentences in the first-order theory of the reals.

## 1.2 Continuous time

### 1.2.1 Cyber-physical systems

Continuous-time linear dynamical systems have connections with important models developed over the last two decades, jointly known as *cyber-physical systems* [Alur, 2015]. These were motivated by the need to model and analyse devices which interact with real-world processes via sensors and actuators. The interaction with the physical world necessitates that formal models for cyber-physical systems combine a discrete state space with continuous dynamics.

The problems examined in this thesis have particular relevance to two formal models for cyber-physical systems: *hybrid automata* [Alur et al., 1995] and the subclass of *timed automata* [Alur and Dill, 1994]. A hybrid automaton is a finite state machine with a finite set of continuously-changing real-valued variables. Each state is equipped with differential equations governing the dynamics of the variables. State transitions take place instantaneously and are only enabled if transition guards comprising boolean combinations of equalities and inequalities on the variables are satisfied. In some variations, entering a new state also triggers a (possibly non-deterministic) reset on the variables. In timed automata, an additional constraint is added that each variable $x$ be a *clock*, in the sense that in all states, its dynamics are given by $x' = 1$.

Thus, reachability problems for continuous-time linear dynamical systems are essentially problems on hybrid automata with a single state, governed by linear dynamics. For example, asking whether a particular transition of a hybrid automaton is ever enabled is a reachability question to the region defined by the guard of the transition. Similarly, for hybrid automata with resets and more than one state, state-to-state reachability may be recast as a sequence of reachability queries in continuous dynamical systems, each governed by the dynamics of some state of the automaton, with initial set given by the reset conditions of the state, and target set given by the guard of some outgoing transition.

As we remark in Section 1.3, this thesis focuses on *linear* dynamics because even slightly more complex behaviour is known to lead to undecidability. Nonetheless, even with such simple dynamics,

few reachability problems have been shown decidable thus far. Reference [Hainry, 2008] proves that reachability from point to point in a continuous-time linear dynamical system is decidable, whilst the later work [Chen et al., 2015] gives a sharper upper complexity bound of **PTIME**, thereby establishing a parallel to the result of [Kannan and Lipton, 1980] in the discrete case. As we recount in Section 1.2.2, reference [Bell et al., 2010] studies a continuous analogue of the Discrete Skolem Problem and establishes decidability in some restricted cases.

### 1.2.2 Exponential polynomials

The continuous analogue of linear recurrence sequences are the unique solutions of initial-value problems comprising an ordinary linear differential equation

$$f^{(k)} = a_1 f^{(k-1)} + \ldots + a_k f, \tag{1.6}$$

with real coefficients $a_1, \ldots, a_k$ and initial conditions $f(0), f'(0), \ldots, f^{(k-1)}(0)$. As we show in Section 2.3.2, such functions $f$ may always be written in the form $\boldsymbol{y}^{\boldsymbol{T}} e^{\boldsymbol{A}t}\boldsymbol{x}$ for vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^k$ and a matrix $\boldsymbol{A} \in \mathbb{R}^{k\times k}$. Conversely, given such $\boldsymbol{x}, \boldsymbol{y}$ and $\boldsymbol{A}$ of size $k$, the expression $\boldsymbol{y}^{\boldsymbol{T}} e^{\boldsymbol{A}t}\boldsymbol{x}$ as a function of $t$ satisfies an order-$k$ linear differential equation as above. Carrying out the multiplication in the matrix form $\boldsymbol{y}^{\boldsymbol{T}} e^{\boldsymbol{A}t}\boldsymbol{x}$ shows that $f$ may also be written as $\sum_{j=1}^{l} P_j(t) e^{\lambda_j t}$, where $\lambda_j$ are the eigenvalues of $\boldsymbol{A}$ and $P_j$ are univariate polynomials with complex coefficients. The function $f$ is said to be an *exponential polynomial* of order $k$.

It is easy to show that the state $\boldsymbol{x}(t)$ of a continuous-time linear dynamical system is given by $\boldsymbol{x}(t) = e^{\boldsymbol{A}t}\boldsymbol{x}(0)$, so clearly, as the state of a discrete-time linear dynamical system is a vector of linear recurrence sequences, so is the state of a continuous-time linear dynamical system a vector of exponential polynomials. Consequently, there is significant overlap between continuous-time reachability problems and the study of exponential polynomials.

In [Bell et al., 2010], a continuous extension of the Skolem Problem is studied: given an exponential polynomial $f$ and an interval $I \subseteq \mathbb{R}_{\geq 0}$, determine whether $f$ has a zero on $I$. In that paper, $I$ is taken to be $\mathbb{R}_{\geq 0}$ throughout. This is precisely the problem of reachability to an $(m-1)$-dimensional subspace of $\mathbb{R}^m$ in a continuous linear dynamical system. The authors establish several important results. First, they prove decidability when $\boldsymbol{A}$ has size 2, or is a Metzler matrix (that is, has only non-negative off-diagonal entries), or has only complex eigenvalues of maximum real part. Second, on the assumption that the eigenvalues of $\boldsymbol{A}$ of maximum real part include at least two pairs of complex numbers, with algebraic multiplicity equal to 1, whose imaginary parts are linearly independent over $\mathbb{Q}$, the authors show it is decidable whether $f$ has infinitely many zeros (the *Continuous Infinite Zeros Problem*), and if not, they obtain a bound $T$ such that all zeros of $f$ must lie in $[0, T]$, thereby reducing to a *bounded* version of the Continuous Skolem Problem. Note that, whilst in the discrete case such a bound immediately renders the Skolem Problem decidable, this is not so for the continuous case, mostly due to the additional challenge posed by the possibility of tangential zeros. Finally, the third main result of [Bell et al., 2010] is that the problem of determining whether $f$ is non-negative everywhere (the *Continuous Positivity Problem*) is **NP**-hard and decidable in exponential time.

## 1.3 Stronger models

It is interesting to observe that in some sense, linear loops are the 'correct' context in which to study pointwise reachability with a reasonable expectation of decidability. Indeed, many examples are known of simple discrete-time systems which admit only a small amount of non-linearity, typically some form of piecewise-linear or piecewise-affine updates, yet are sufficiently powerful to simulate a universal Turing Machine. Examples include the generalised shifts of [Moore, 1990, Moore, 1991], the neural nets with inputs of [Siegelmann and Sontag, 1991, Siegelmann and Sontag, 1995, Sontag, 1995] and the piecewise-affine maps of [Koiran et al., 1994]. Most recently, reference [Ben-Amram et al., 2012] established the undecidability of both the Termination Problem and the Halting Problem for discrete-time systems whose

updates are piecewise linear with only two pieces, that is, linear loops of the form

$$\begin{aligned}&\textbf{while } \boldsymbol{Bx} \geq \boldsymbol{b} \textbf{ do}\\ &\qquad \textbf{if } x_1 > 0 \textbf{ then } \boldsymbol{x} := \boldsymbol{A_1 x}\\ &\qquad \textbf{else } \boldsymbol{x} := \boldsymbol{A_2 x}.\end{aligned}$$

Similarly, admitting piecewise linear behaviour leads to undecidability in the continuous case as well, as exemplified by the piecewise-constant derivative systems of [Asarin et al., 1995]. These comprise a finite partition of the Euclidean space $\mathbb{R}^m$ into polyhedral regions, with the state of the system in each region governed by the simple continuous dynamic of a constant first derivative. The authors prove that if $m \geq 3$, this model is sufficiently powerful to simulate a Turing Machine. The same happens if one allows higher-degree polynomial dynamics in the continuous case, as shown in reference [Graça et al., 2008]. In fact, [Hainry, 2009, Lemma 28] shows that even quadratic dynamics are sufficiently powerful to simulate Turing Machines, by explicitly rewriting systems of higher-degree polynomial ODEs as systems of quadratic ODEs at the cost of increasing the dimension of the ambient space.

## 1.4 Results

In this thesis, we study several pointwise reachability problems for linear dynamical systems, both in the discrete and the continuous case. Our results are the following.

First, we study the Discrete Skolem Problem, that is, pointwise reachability to an $(m-1)$-dimensional subspace of $\mathbb{R}^m$ in a discrete linear dynamical system. We prove upper complexity bounds which sharpen the known decidability results of [Mignotte et al., 1984, Vereshchagin, 1985] for the subproblem in which $m \leq 4$. Specifically, over the rationals, we show membership in **PTIME** when $m = 2$, and in $\mathbf{NP^{RP}}$ when $m \in \{3, 4\}$. This is the focus of Chapter 3, which in turn is based on our publication [Chonev et al., 2016] (to appear).

Second, we study the more general problem of pointwise reachability to a vector subspace $\mathcal{V}$ of $\mathbb{R}^m$, under the appellation *Discrete Orbit Problem*. We prove that, if the input data is rational and $\dim(\mathcal{V}) \leq 3$, then the problem is in $\mathbf{NP^{RP}}$, and moreover, if $\dim(\mathcal{V}) = 1$, then the problem is in **PTIME**. Note that these complexity bounds are independent of the dimension $m$ of the ambient space. In proving this result, we confirm an old conjecture made by [Kannan and Lipton, 1986]. We also remark that a simple homogenisation technique immediately yields membership in $\mathbf{NP^{RP}}$ for the problem of reachability to an *affine* subspace of dimension 1 or 2. We establish these results in Chapter 4, which is also based on [Chonev et al., 2016].

Third, we study the problem of pointwise reachability to an affine polyhedron in a discrete linear dynamical system, under the name of *Polyhedron-Hitting Problem*. Assuming rational input data, for each pair $(m, d) \in \mathbb{N}_+^2$ with $m \geq d$, we focus on reachability to a $d$-dimensional polyhedron in $\mathbb{R}^m$, defined as the intersection of closed affine halfspaces. For each such pair, we establish either a decidability result or a hardness result. Specifically, our main decidability result is that if $d \in \{1, 2\}$ or $m = d = 3$, then the problem lies in **PSPACE**. Our main hardness result is that a decision procedure for the Polyhedron-Hitting Problem with $m \geq d \geq 4$ would entail the approximability to within arbitrary precision of the homogeneous Diophantine approximation type $L(x)$ for all real $x$ of the form $\arg(\lambda)/2\pi$ with $\lambda$ a Gaussian rational. As we explain in Section 2.2, this would be a major breakthrough in number theory and constitutes a strong barrier, as currently almost nothing is known about $L(x)$ for any specific $x$. Finally, for $m > d \geq 3$, we show a reduction from the Discrete Skolem Problem of order $\max(d + 1, 5)$, thereby establishing another difficult barrier to decidability. These results are the focus of Chapter 5, which is based on our paper [Chonev et al., 2015c].

Fourth, we consider the Continuous Skolem Problem, that is, pointwise reachability to an $(m - 1)$-dimensional subspace of $\mathbb{R}^m$ in a continuous linear dynamical system. We show that the time-bounded case is decidable for all orders, provided Schanuel's Conjecture is true, and also unconditionally for $m \leq 3$. This resolves an outstanding question in [Bell et al., 2010, Open Problem 17]. On the other hand, for the time-unbounded case, we prove a hardness result, namely that decidability for $m \geq 9$ would entail the approximability to within arbitrary precision of $L(x)$ for all real algebraic $x$. These results are the focus of Chapter 6, which is based on our work [Chonev et al., 2015a].

Fifth, we examine the Continuous Infinite Zeros Problem, which, like the Continuous Skolem Problem, concerns pointwise reachability to an $(m-1)$-dimensional subspace of $\mathbb{R}^m$ in a continuous linear dynamical system, but instead asks about reaching the target space *infinitely often*. For $m \leq 7$, we show the problem decidable. Furthermore, if an instance of order at most 7 is negative, then we show an effective bound $T$ such that any time $t$ at which the system intersects the target space must satisfy $t \leq T$. This gives a reduction from the unbounded case of the Continuous Skolem Problem to the bounded case, thereby establishing decidability, conditional on Schanuel's Conjecture, for the unbounded version with $m \leq 7$. Finally, for $m \geq 9$, we establish a Diophantine hardness result for the Continuous Infinite Zeros Problem, namely that a decision procedure would yield the approximability to within arbitrary precision of the Lagrange constant $L_\infty(x)$ of all real algebraic numbers $x$. These results are the focus of Chapter 7, which is based on our unpublished work [Chonev et al., 2015b].

Finally, we consider a generalisation of the Continuous Skolem Problem, namely the *Continuous Orbit Problem*: pointwise reachability to a vector subspace in a continuous linear dynamical system. In Chapter 8, we prove this problem decidable in the case of a one-dimensional target vector space, regardless of the dimension of the ambient space.

## 1.5 Thesis structure

Chapter 2 contains results from various mathematical fields which arise throughout the present thesis. Each subsequent chapter is equipped with a list of prerequisites indicating the pertinent sections of Chapter 2 which should be read in advance. In terms of proof techniques, each chapter is essentially self-contained, with one major exception: Section 5.5 assumes knowledge of the techniques of Chapter 4 for the Discrete Orbit Problem and refines them to establish our upper complexity bounds for the Polyhedron-Hitting Problem. Thus, although a linear reading starting from Chapter 3 and accessing the relevant sections of Chapter 2 on demand appears most natural to the author, it is generally safe to skip ahead at one's leisure.

# Chapter 2

# Mathematical Techniques

## 2.1 Number-theoretic tools

### 2.1.1 Algebraic numbers: representation and manipulation

A complex number $\alpha$ is *algebraic* if there exists a polynomial $P \in \mathbb{Q}[x]$ such that $P(\alpha) = 0$. The set of algebraic numbers, denoted by $\mathbb{A}$, is a subfield of $\mathbb{C}$. The *minimal polynomial* of $\alpha$ is the unique monic polynomial of least degree which vanishes at $\alpha$. The *degree* of $\alpha \in \mathbb{A}$ is defined as the degree of its minimal polynomial and is denoted by $\deg(\alpha)$. The *height* of $\alpha$, denoted by $H_\alpha$, is defined as the maximum absolute value of the coefficients of the integer polynomial obtained by scaling the minimal polynomial of $\alpha$ by the least common multiple of the denominators of its coefficients. The roots of the minimal polynomial of $\alpha$ (including $\alpha$) are called the *Galois conjugates* of $\alpha$. The *absolute norm* of $\alpha$, denoted $\mathcal{N}_{abs}(\alpha)$, is the product of the Galois conjugates of $\alpha$. By Viete's laws, we have

$$\mathcal{N}_{abs}(\alpha) = (-1)^{\deg(\alpha)} \frac{a}{b}$$

where $a, b$ are respectively the constant term and the leading coefficient of the minimal polynomial of $\alpha$. It follows that $\mathcal{N}_{abs}(\alpha) \in \mathbb{Q}$. An *algebraic integer* is an algebraic number whose minimal polynomial has integer coefficients. The set of algebraic integers, denoted $\mathcal{O}_\mathbb{A}$, is a ring under the usual addition and multiplication. The algebraic integers are *integrally closed*, that is, the roots of any monic polynomial with coefficients in $\mathcal{O}_\mathbb{A}$ are all algebraic integers. For any $\alpha \in \mathbb{A}$, it is possible to find $\beta \in \mathcal{O}_\mathbb{A}$ and $m \in \mathbb{Z}$ such that $\alpha = \beta/m$.

The *canonical representation* of an algebraic number $\alpha$ is its minimal polynomial, along with a numerical approximation of $\Re(\alpha)$ and $\Im(\alpha)$ of sufficient precision to distinguish $\alpha$ from its Galois conjugates [Cohen, 1993, Section 4.2.1]. More precisely, we represent $\alpha$ by the tuple

$$(P, x, y, R) \in (\mathbb{Q}[x] \times \mathbb{Q}^3)$$

meaning that $\alpha$ is the unique root of the irreducible (over $\mathbb{Q}$) polynomial $P$ which lies inside the circle centred at $(x, y)$ in the complex plane with radius $R$. A bound due to Mignotte [Mignotte, 1982] states that for roots $\alpha_j \neq \alpha_k$ of a polynomial $P(x)$,

$$|\alpha_j - \alpha_k| > \frac{\sqrt{6}}{d^{(d+1)/2} H^{d-1}}, \tag{2.1}$$

where $d$ and $H$ are the degree and height of $P$, respectively. Thus, if $R$ is restricted to be less than a quarter of the root separation bound, the representation is well-defined and allows for equality checking. Observe that given its minimal polynomial, the remaining data necessary to describe $\alpha$ is polynomial in the length of the input. It is known how to obtain polynomially many bits of the roots of any $P \in \mathbb{Q}[x]$ in polynomial time [Pan, 1996].

When we say an algebraic number $\alpha$ is given, we assume we have a canonical description of $\alpha$. We will denote by $\|\alpha\|$ the length of this description, assuming that integers are expressed in binary and

rationals are expressed as pairs of integers. Observe that $|\alpha|$ is an exponentially large quantity in $\|\alpha\|$ whereas $\log|\alpha|$ is polynomially large. Notice also that $1/\log|\alpha|$ is at most exponentially large in $\|\alpha\|$. For a rational $a$, $\|a\|$ is just the sum of the lengths of its numerator and denominator written in binary. For a polynomial $P \in \mathbb{Q}[x]$, $\|P\|$ will denote $\sum_{j=0}^{\deg(P)} \|p_j\|$ $p_j$ are the coefficients of $P$.

**Lemma 1.** *Given canonical representations of $\alpha, \beta \in \mathbb{A}$ and a polynomial $P \in \mathbb{Q}[x]$, it is possible to compute canonical descriptions of $\alpha \pm \beta$, $\alpha\beta^{\pm 1}$ and $P(\alpha)$ in time polynomial in the length of the input (that is, in $\|\alpha\| + \|\beta\| + \|P\|$).*

*Proof.* Let $R, Q$ be the minimal polynomials of $\alpha$ and $\beta$, respectively. Then the resultant of $R(x-y)$ and $Q(y)$, interpreted as polynomials in $y$ with coefficients in $\mathbb{Q}[x]$, is a polynomial in $x$ which vanishes at $\alpha+\beta$. We compute it in polynomial time using the Sub-Resultant algorithm (see Algorithm 3.3.7 in [Cohen, 1993]) and factor it into irreducibles using the LLL algorithm [Lenstra et al., 1982]. Finally, we approximate the roots of each irreducible factor to identify the minimal polynomial of $\alpha+\beta$. The degree of $\alpha+\beta$ is at most $\deg(\alpha)\deg(\beta)$, while its height is bounded by $H_{\alpha+\beta} \le H_\alpha^{\deg(\alpha)} H_\beta^{\deg(\beta)}$ [Zippel, 1997]. Therefore, by (2.1), a polynomial number of bits suffices to describe $\alpha+\beta$ unambiguously. Similarly, we can compute canonical representations of $\alpha-\beta$, $\alpha\beta$ and $\alpha/\beta$ in polynomial time using resultants, see [Cohen, 1993].

To calculate $P(\alpha)$ we repeatedly use addition and multiplication. It suffices to prove that all intermediate results may be represented in polynomial space. It is clear that their degrees are at most $\deg(\alpha)$, but it is not obvious how quickly the coefficients of their minimal polynomials grow. However, there is a simple reason why their representation is polynomially bounded. Let $\boldsymbol{A}$ be the companion matrix of the minimal polynomial of $\alpha$. Then $P(\alpha)$ is an eigenvalue of $P(\boldsymbol{A})$. We can calculate $P(\boldsymbol{A})$ using only polynomial space. Then from the Leibniz formula

$$\det(\lambda \boldsymbol{I} - P(\boldsymbol{A})) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} (\lambda \boldsymbol{I} - P(\boldsymbol{A}))_{i,\sigma(i)},$$

it is evident that the coefficients of the characteristic polynomial of $P(\boldsymbol{A})$ are exponentially large in the length of the input, so their representation requires only polynomial space. This characteristic polynomial may be factored into irreducibles in polynomial time, so the description of $P(\alpha)$ and of all intermediate results is polynomially bounded. □

It is trivial to check whether $\alpha = \beta$ and whether $\alpha$ belongs to one of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$. It takes only polynomial time to determine whether $\alpha$ is a root of unity, and if so, to calculate its order and phase.

### 2.1.2 Number fields and ideals

In this section, we recall some terminology and results from algebraic number theory. For more details, see [Cohen, 1993, Stewart and Tall, 2002]. We also define the ideal-counting function $v_P$, which is a notion of magnitude of algebraic numbers distinct from the usual absolute value. We follow the presentation of [Halava et al., 2005].

An *algebraic number field* is a field extension $\mathbb{K}$ of $\mathbb{Q}$ which, considered as a $\mathbb{Q}$-vector space, has finite dimension. This dimension is called the *degree* of the number field and is denoted by $[\mathbb{K} : \mathbb{Q}]$. Given two algebraic numbers $\alpha$ and $\beta$, the *Field Membership Problem* is to determine whether $\beta \in \mathbb{Q}(\alpha)$ and, if so, to return a polynomial $P$ with rational coefficients such that $\beta = P(\alpha)$. This problem can be decided using the LLL algorithm, see [Cohen, 1993, Section 4.5.4].

For any number field $\mathbb{K}$, there exists an element $\theta \in \mathbb{K}$ such that $\mathbb{K} = \mathbb{Q}(\theta)$. Such a $\theta$ is called a *primitive element* of $\mathbb{K}$ and satisfies $\deg(\theta) = [\mathbb{K} : \mathbb{Q}]$. The proof is constructive: there is always a primitive element for $\mathbb{Q}(\alpha_1, \alpha_2)$ of the form $\alpha_1 + l\alpha_2$ for some small integer $l$. Thus, repeatedly using an algorithm for the Field Membership Problem for different $l$ is guaranteed to yield a primitive element for $\mathbb{Q}(\alpha_1, \alpha_2)$, and therefore by induction, for any number field $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ specified by algebraic numbers $\alpha_1, \ldots, \alpha_k$. Also using an algorithm for the Field Membership Problem, one can represent each $\alpha_j$ as a polynomial in $\theta$ and thereby determine a maximal $\mathbb{Q}$-linearly independent subset of $\{\alpha_1, \ldots, \alpha_k\}$.

There exist exactly $\deg(\theta)$ monomorphisms from $\mathbb{K}$ into $\mathbb{C}$, given by $\theta \to \theta_j$, where $\theta_j$ are the Galois conjugates of the primitive element $\theta$. If $\alpha \in \mathbb{K}$, then $\deg(\alpha) | \deg(\theta)$. Moreover, if $\sigma_1, \ldots, \sigma_{\deg(\theta)}$ are the

monomorphisms from $\mathbb{K}$ into $\mathbb{C}$ then $\sigma_1(\alpha), \ldots, \sigma_{\deg(\theta)}(\alpha)$ are exactly the Galois conjugates of $\alpha$, each repeated $\deg(\theta)/\deg(\alpha)$ times. The *norm of $\alpha$ relative to $\mathbb{K}$* is defined as

$$\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \prod_{j=1}^{\deg(\theta)} \sigma_j(\alpha) = (\mathcal{N}_{abs}(\alpha))^{\deg(\theta)/\deg(\alpha)}$$

For a number field $\mathbb{K}$, the set $\mathcal{O}_\mathbb{K} = \mathcal{O}_\mathbb{A} \cap \mathbb{K}$ of algebraic integers in $\mathbb{K}$ forms a ring under the usual addition and multiplication. The ideals of $\mathcal{O}_\mathbb{K}$ are finitely generated, and form a commutative ring under the operations

$$IJ = [\{xy \mid x \in I, y \in J\}]$$
$$I + J = \{x + y \mid x \in I, y \in J\},$$

with unit $\mathcal{O}_\mathbb{K}$ and zero $\{0\}$, where $[S]$ denotes the ideal generated by $S$. An ideal $P$ is *prime* if $P = AB$ implies $A = P$ or $A = [1]$. The fundamental theorem of ideal theory states that each non-zero ideal may be represented uniquely (up to reordering) as a product of prime ideals.

This theorem gives rise to the following *ideal-counting function* $v_P : \mathcal{O}_\mathbb{K} \backslash \{0\} \to \mathbb{N}$. For a fixed prime ideal $P$, we define $v_P(\alpha)$ to be the number of times $P$ appears in the factorisation into prime ideals of $[\alpha]$. That is,

$$v_P(\alpha) = k \text{ if and only if } P^k \mid [\alpha] \text{ and } P^{k+1} \nmid [\alpha]$$

We also define $v_P(0) = \infty$. The function satisfies the following properties:

- $v_P(\alpha\beta) = v_P(\alpha) + v_P(\beta)$
- $v_P(\alpha + \beta) \geq \min\{v_P(\alpha), v_P(\beta)\}$
- If $v_P(\alpha) \neq v_P(\beta)$, then $v_P(\alpha + \beta) = \min\{v_P(\alpha), v_P(\beta)\}$.

For any $\alpha \in \mathbb{K}$ we can find an algebraic integer $\beta \in \mathcal{O}_\mathbb{K}$ and a rational integer $n \in \mathbb{Z} \subseteq \mathcal{O}_\mathbb{K}$ such that $\alpha = \beta/n$. We extend $v_P$ to $\mathbb{K}$ by defining $v_P(\alpha) = v_P(\beta) - v_P(n)$. The first of the three properties of $v_P$ above guarantees that this value is independent of the choice of $\beta, n$, making the extension of $v_P$ to $\mathbb{K}$ well-defined. Note that the extension preserves the above three properties.

For an ideal $I \neq \{0\}$, the quotient ring $\mathcal{O}_\mathbb{K}/I$ is finite. The *norm* of $I$, denoted $\mathcal{N}(I)$, is defined as $|\mathcal{O}_\mathbb{K}/I|$. We define also $\mathcal{N}([0]) = \infty$. Notice that $\mathcal{N}(I) = 1$ if and only if $I = \mathcal{O}_\mathbb{K}$, otherwise $\mathcal{N}(I) \geq 2$. Each prime ideal $P$ contains a unique prime number $p$, and $\mathcal{N}(P) = p^f$ for some natural number $f \geq 1$. In general,

$$|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)| = \mathcal{N}([\alpha]) \geq 2^{v_P(\alpha)}$$

since $\mathcal{N}(P) \geq 2$ for any prime ideal $P$. Hence,

$$v_P(\alpha) \leq \log_2 |\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)| \leq \log_2 |\mathcal{N}_{abs}(\alpha)|^d$$

where $d = [\mathbb{K} : \mathbb{Q}]$. Thus, if we are given $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ for canonically represented algebraic numbers $\alpha_j$ and a canonically represented $\alpha \in \mathbb{K}$, we can observe that $d$ is at most polynomially large in the length of the input and $|\mathcal{N}_{abs}(\alpha)|$ is at most exponentially large in the length of the input. Therefore, $v_P(\alpha)$ is only polynomially large.

The following lemma is simple, but useful:

**Lemma 2.** *Let $\mathbb{K}$ be a number field and $\alpha \in \mathbb{K}$ with $\alpha \notin \mathcal{O}_\mathbb{K}$. Then there exists a prime ideal $P$ of $\mathcal{O}_\mathbb{K}$ such that $v_P(\alpha) \neq 0$.*

*Proof.* There exist $\beta \in \mathcal{O}_\mathbb{K}$ and $m \in \mathbb{Z}$ such that $\alpha = \beta/m$. If $[\beta] = [m]$, then $\beta$ and $m$ are associates, so $\alpha$ must be a unit of $\mathcal{O}_\mathbb{K}$. Since $\alpha \notin \mathcal{O}_\mathbb{K}$, it follows that $[\beta] \neq [m]$, so the factorisations of $[\beta]$ and $[m]$ into prime ideals must differ. Therefore, $v_P(\beta) \neq v_P(m)$ for some prime ideal $P$, so $v_P(\alpha) \neq 0$. □

### 2.1.3 Transcendental number theory

We now move to some techniques from Transcendental Number Theory on which our results depend in a critical way. The following theorem was originally proven in [Gelfond, 1934, Gelfond and Vinogradov, 1934] and independently in [Schneider, 1935a, Schneider, 1935b], settling Hilbert's seventh problem in the affirmative.

**Theorem 3.** *(Gelfond-Schneider) If $\alpha$ and $\beta$ are algebraic numbers with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, then $\alpha^\beta$ is transcendental.*

A *transcendence basis* of a field extension $\mathbb{L} : \mathbb{K}$ is a subset $S \subseteq \mathbb{L}$ such that $S$ is algebraically independent over $\mathbb{K}$ and $\mathbb{L}$ is algebraic over $\mathbb{K}(S)$. All transcendence bases of $\mathbb{L} : \mathbb{K}$ have the same cardinality, which is called the *transcendence degree* of the extension.

**Theorem 4.** *(Lindemann–Weierstrass) If $\alpha_1, \ldots, \alpha_m$ are algebraic numbers linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_m}$ are algebraically independent over $\mathbb{Q}$. Equivalently, the transcendence degree of $\mathbb{Q}(e^{\alpha_1}, \ldots, e^{\alpha_m})$ over $\mathbb{Q}$ is $m$.*

An immediate consequence is the following:

**Lemma 5.** *Let $\alpha$ be algebraic. If $\alpha \neq 1$, then $\log(\alpha)$ is transcendental, and if $\alpha \neq 0$, then $e^\alpha$ is transcendental.*

Next we state a powerful result due to Baker on linear forms of logarithms of algebraic numbers.

**Theorem 6.** *[Baker, 1975, Theorem 3.1] Let $\alpha_1, \ldots, \alpha_m$ be non-zero algebraic numbers with degrees at most $d$ and heights at most $A$. Further, let $\beta_0, \ldots, \beta_m$ be algebraic numbers with degrees at most $d$ and heights at most $B \geq 2$. Write*

$$\Lambda = \beta_0 + \beta_1 \log(\alpha_1) + \ldots + \beta_m \log(\alpha_m)\,.$$

*Then either $\Lambda = 0$ or $|\Lambda| > B^{-C}$, where $C$ is an effectively computable number depending only on $m, d, A$ and the chosen branch of the complex logarithm.*

Various quantitative versions of this theorem are known with explicit constants, as well as sharper lower bounds for restricted cases. Of these, in the present thesis we make use of the following result, due to Baker and Wüstholz, concerning the homogeneous case with (rational) integer coefficients:

**Theorem 7.** *[Baker and Wüstholz, 1993] With the notation as in Theorem 6, suppose $\beta_0 = 0$, $\alpha_1, \ldots, \alpha_m \neq 1$, $\beta_1, \ldots, \beta_m \in \mathbb{Z}$ and $A, B \geq e$. Let also* log *be the principal branch of the natural logarithm, defined by $\log(z) = \log|z| + i\arg(z)$, where $-\pi < \arg(z) \leq \pi$. Let also $D$ be the degree of the extension field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ over $\mathbb{Q}$. Then if $\Lambda \neq 0$, then*

$$\log|\Lambda| > -(16mD)^{2(m+2)}(\log(A))^m \log(B).$$

The next theorem, due to van der Poorten [van der Poorten, 1977] is analogous to Baker's bound, but with respect to $P$-adic valuations instead of the usual Archimedean absolute value.

**Theorem 8.** *[van der Poorten, 1977] Let $\alpha_1, \ldots, \alpha_m$ be algebraic numbers of degree at most $d$ belonging to a number field $\mathbb{K}$ and with heights at most $A$. Let $P$ be a prime ideal of $\mathbb{K}$ containing the rational prime $p$. Let also $\beta_1, \ldots, \beta_m$ be rational integers with absolute values at most $B \geq e^2$. If $\alpha_1^{\beta_1}\alpha_2^{\beta_2}\ldots\alpha_m^{\beta_m} \neq 1$, then*

$$v_P(\alpha_1^{\beta_1}\ldots\alpha_m^{\beta_m} - 1) \leq (16(m+1)d)^{12(m+1)}(p^d/\log(p))(\log(A))^m(\log(B))^2.$$

Finally, some of the results in this thesis depend on Schanuel's conjecture, a unifying conjecture in transcendental number theory [Lang, 1966], which, if true, greatly generalises several of the central results in the field, including the Gelfond-Schneider Theorem, the Lindemann-Weierstrass Theorem and Baker's Theorem.

**Conjecture 9** (Schanuel's Conjecture [Lang, 1966])**.** *Let $\alpha_1, \ldots, \alpha_m$ be complex numbers that are linearly independent over $\mathbb{Q}$. Then the extension*

$$\mathbb{Q}(\alpha_1, \ldots, \alpha_m, e^{\alpha_1}, \ldots, e^{\alpha_m}) : \mathbb{Q}$$

*has transcendence degree at least $m$.*

### 2.1.4 Algebraic integers near the unit circle

Suppose $\alpha \neq 0$ is an algebraic integer. It is easy to see that it is impossible for all the Galois conjugates of $\alpha$ to be strictly within the unit circle: just notice that the product of all Galois conjugates of $\alpha$ must be a non-zero integer by Viete's laws. Further, an old result due to Kronecker [Kronecker, 1875] establishes that unless $\alpha$ is a root of unity, then at least one of its Galois conjugates must be strictly outside the unit circle. In this thesis, we make use of the following theorem, due to Blanksby and Montgomery [Blanksby and Montgomery, 1971], which strengthens Kronecker's result by providing an effective separation between this Galois conjugate and the unit circle.

**Theorem 10.** *Let $\alpha$ be an algebraic integer of degree $d \geq 2$. Then there is a Galois conjugate $\sigma(\alpha)$ of $\alpha$ such that $|\sigma(\alpha)| > 1 + 1/(30d^2 \log(6d))$.*

## 2.2 Diophantine approximation

### 2.2.1 Irrationality measure, Lagrange constant and Lagrange type

Diophantine approximation is a branch of number theory concerned with approximating real numbers by rationals. Clearly, one can approximate any real number with rationals to within any constant additive error simply by resorting to approximations with ever greater denominators. The question becomes more interesting, however, if the desired precision is a function of the denominator used. In particular, one question of great interest in Diophantine approximation is the following: given a real number $x$, for what choices of the exponent $k \geq 1$ does the inequality

$$0 < \left| x - \frac{n}{m} \right| < \frac{1}{m^k} \tag{2.2}$$

have infinitely many solutions $n, m \in \mathbb{Z}$? The infimum of all such values $k$ is known as the *irrationality measure* of $x$, denoted $\mu(x)$.

It is easy to see that $\mu(x) = 1$ for any $x \in \mathbb{Q}$. An old observation made by Dirichlet circa 1840 based on the pigeonhole principle showed that for all $x \notin \mathbb{Q}$, the inequality (2.2) has infinitely many solutions for $k = 2$. The Thue-Siegel-Roth Theorem [Roth, 1955], a powerful result for which Roth received the Fields medal in 1958, states that for all $x \in \mathbb{A} \setminus \mathbb{Q}$, (2.2) has only finitely many solutions for each $k > 2$. Thus, $\mu(x) = 2$ for all irrational algebraic $x$. Almost all (in the measure-theoretic sense) $x \in \mathbb{R}$ have $\mu(x) = 2$, although transcendental numbers with greater irrationality measure are known, e.g, the *Liouville numbers* are precisely those with infinite irrationality measure and form an uncountable subset of $\mathbb{R}$.

Thus, in some sense, 'quadratically good' rational approximations are the best that can be hoped for. It is of interest, then, to what extent the numerator in (2.2) can be improved in the case $k = 2$. That is, for what choices of $c \in \mathbb{R}$ does the inequality

$$0 < \left| x - \frac{n}{m} \right| < \frac{c}{m^2} \tag{2.3}$$

have infinitely many solutions for $n, m \in \mathbb{Z}$? Dirichlet's result guarantees that each $x \in \mathbb{R}$ has infinitely many solutions to (2.3) with $c = 1$. This was later sharpened to $c = 1/\sqrt{5}$, a result known as Hurwitz's Theorem [Hurwitz, 1891], even though it appeared in Markoff's work earlier [Markoff, 1879]. Hurwitz's Theorem is 'tight': any further improvement in the constant would require that exceptions be made for some real numbers $x$. Specifically, for all $x$ whose continued fraction expansion from some stage onwards consists only of 1's, matching that of the golden ratio $(1 + \sqrt{5})/2 = [1, 1, \dots]$, the constant $c = 1/\sqrt{5}$ in Hurwitz's Theorem cannot be improved upon. If these exceptions are excluded, then (2.3) holds for infinitely many $n, m$ with $c = 1/\sqrt{8}$. This constant is optimal for all $x$ whose continued fraction eventually consists only of 2's, such as $1 + \sqrt{2} = [2, 2, \dots]$. Continuing this process yields a sequence of constants $c \in (1/3, 1/\sqrt{5}]$, known as the *Markoff spectrum*, which accumulates at $1/3$.

The idea arises naturally of measuring the approximability of $x$ by the best possible constant $c$ which admits infinitely many such 'good' approximations. More precisely, for $x \in \mathbb{R}$, define the *Lagrange constant* (or *homogeneous Diophantine approximation constant*) of $x$ by

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

Following the terminology of Lagarias and Shallit [Lagarias and Shallit, 1997], the *(homogeneous Diophantine approximation) type* of $x$ is similarly defined by

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

The set $\{L_\infty(x) : x \in \mathbb{R}\} \subset [0, 1/\sqrt{5}]$ is known as the *Lagrange spectrum* and coincides with the Markoff spectrum on $(1/3, 1/\sqrt{5}]$. The two spectra have been the focus of sustained research over the years, which has yielded many deep results, see [Cusick and Flahive, 1989]. One important connection is that the behaviour of the continued fraction expansion of $x$ is closely related to $L_\infty(x)$ and $L(x)$. Indeed, numbers whose continued fraction expansions have bounded partial quotients are known as *badly approximable*, and are precisely the real numbers $x$ such that $L_\infty(x) > 0$ or equialently $L(x) > 0$ [Schmidt, 1980, pp. 22-23].

Khinchin showed in 1926 [Khinchin, 1926], [Khinchin, 1961, Theorem 32] that almost all real numbers (in the measure-theoretic sense) have Lagrange constant and type equal to zero. On the other hand, the Lagrange spectrum is known to be continuous on the interval $[0, f)$ where $f$ is *Freiman's constant*, so for all $c < f$, there exists some $x \in \mathbb{R}$ such that $L_\infty(x) = c$. Unfortunately, more concrete information on the Lagrange constants and types of specific numbers or classes of numbers has proven to be elusive.

In the context of algebraic numbers, it is well known that a real algebraic number of degree two over the rationals has a simple continued fraction expansion that is ultimately periodic, so such numbers have bounded partial quotients, but nothing is known about real algebraic numbers of degree three or more: indeed, no example is known with bounded partial quotients, nor with unbounded quotients. Guy [Guy, 2004] asks:

> *Is there an algebraic number of degree greater than two whose simple continued fraction expansion has unbounded partial quotients? Does every such number have unbounded partial quotients?*

In other words, the question is whether there is a real algebraic number $x$ of degree at least three such that $L_\infty(x), L(x) > 0$, or whether $L_\infty(x) = L(x) = 0$ for all such $x$.

Thus, despite great strides in the field of Diophantine approximation, with the exception of isolated examples, very little is known at present about the values of these approximation measures for specific real numbers. This motivates some of the hardness results exhibited in this thesis for certain problems on linear dynamical systems, which, if shown decidable, would entail the computability (in the sense of approximation to within arbitrarily small additive error) of $L_\infty(x)$ or $L(x)$ for large classes of real $x$.

### 2.2.2 Kronecker's Theorem

The discussion in Section 2.2.1 referred exclusively to *homogeneous* approximation. That is, for given $x \in \mathbb{R}$, we were interested in finding integers $m$ which minimise the fractional part of $|mx|$. More broadly, however, one may consider minimising the fractional part of the inhomogeneous form $|mx - y|$ for given $x, y \in \mathbb{R}$. A significant number of technical results throughout this thesis rely crucially on Kronecker's Approximation Theorem, a celebrated result concerning the simultaneous Diophantine approximation of inhomogeneous forms.

**Theorem 11.** *(Kronecker, appears in [Hardy and Wright, 1999]) Let $\lambda_1, \ldots, \lambda_m$ and $x_1, \ldots, x_m$ be real numbers. The following two statements are equivalent:*

1. *For all integers $u_1, \ldots, u_m$ such that $u_1\lambda_1 + \cdots + u_m\lambda_m \in \mathbb{Z}$, we also have $u_1x_1 + \cdots + u_m\lambda_m \in \mathbb{Z}$. That is, all integer relations (modulo $\mathbb{Z}$) among the $\lambda_j$ also hold among the $x_j$.*
2. *For all $\epsilon > 0$, there exist $p_1, \ldots, p_m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that $|n\lambda_j - x_j - p_j| < \epsilon$ for all $1 \leq j \leq m$.*

A particular special case is when $1, \lambda_1, \ldots, \lambda_m$ are linearly independent over $\mathbb{Q}$: then for *all* real vectors $(x_1, \ldots, x_m)$ and $\epsilon > 0$, it is possible to find $n \in \mathbb{N}$ and $(p_1, \ldots, p_m)$ with $|n\lambda_j - x_j - p_j| < \epsilon$ for all $1 \leq j \leq m$. The following is straightforward corollary.

**Lemma 12.** *Let $a_1, \ldots, a_m \in \mathbb{R}$ be linearly independent over $\mathbb{Q}$ and let $\varphi_1, \ldots, \varphi_m \in \mathbb{R}$. Write $x \bmod 2\pi$ to denote $\min_{k\in\mathbb{Z}} |x + 2k\pi|$ for any $x \in \mathbb{R}$. Let the mapping $h(t)$ be given by*

$$h(t) : \mathbb{R}_{\geq 0} \to [0, 2\pi)^m$$
$$h(t) = ((a_1 t + \varphi_1) \bmod 2\pi, \ldots, (a_m t + \varphi_m) \bmod 2\pi).$$

*Then $\{h(t) : t \in \mathbb{N}\}$ is dense in $[0, 2\pi)^m$, and $\{h(t) : (a_1 t + \varphi_1) \bmod 2\pi = 0\}$ is dense in $\{0\} \times [0, 2\pi)^{m-1}$.*

*Proof.* Note that the linear independence of $1, a_1/2\pi, \ldots, a_m/2\pi$ follows from the linear independence of $a_1, \ldots, a_m$ and the transcendence of $\pi$. Then the first part of the claim follows directly from Kronecker's Theorem. For the second part, $h(t)$ has zero first coordinate precisely when $t = -\varphi_1/a_1 + 2n\pi$ for some $n \in \mathbb{Z}$, at which times we have is

$$h\left(\frac{-\varphi_1}{a_1} + 2n\pi\right) = \{0\} \times \left(n\frac{2\pi a_j}{a_1} + \frac{a_1\varphi_j - \varphi_1 a_j}{a_1} \bmod 2\pi\right)_{2\leq j\leq m}$$

As before, we have that $\{1, 2\pi a_2/a_1, \ldots, 2\pi a_m/a_1\}$ are linearly independent over $\mathbb{Q}$ from the linear independence of $a_1, \ldots, a_m$ and the transcendence of $\pi$, so applying Kronecker's Theorem to the last $m - 1$ components yields the second part of the claim. □

## 2.3 Recurrence and ordinary differential equations

### 2.3.1 Linear recurrence sequences

We now recall some basic properties of linear recurrence sequences. For more details, we refer the reader to [Everest et al., 2003, Halava et al., 2005]. Let $\mathbb{F}$ be $\mathbb{R}$ or $\mathbb{C}$ throughout this section. A *linear recurrence sequence (LRS)* over $\mathbb{F}$ is an infinite sequence $\langle u_n\rangle_{n=0}^{\infty}$ of terms in $\mathbb{F}$ such that there exists a natural number $k$ and numbers $a_1, \ldots, a_k \in \mathbb{F}$ such that $a_k \neq 0$ and $\langle u_n\rangle_{n=0}^{\infty}$ satisfies the linear recurrence equation

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n. \tag{2.4}$$

The recurrence (2.4) is said to have order $k$. Note that the same sequence can satisfy different recurrence relations, but it satisfies a unique recurrence of minimum order. The *characteristic polynomial* of the sequence $\langle u_n\rangle_{n=0}^{\infty}$ is

$$P(x) = x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k$$

and its roots are called the *characteristic roots* of the sequence.

If $\boldsymbol{A} \in \mathbb{F}^{k\times k}$ is a square matrix and $\boldsymbol{v}, \boldsymbol{w} \in \mathbb{F}^k$ are column vectors, then it can be shown that the sequence $u_n = \boldsymbol{v}^{\boldsymbol{T}}\boldsymbol{A}^n\boldsymbol{w}$ satisfies a linear recurrence of order $k$. Indeed, by the Cayley-Hamilton Theorem, $\boldsymbol{A}$ satisfies its own characteristic equation $\det(\boldsymbol{A} - x\boldsymbol{I}) = 0$, which gives a recurrence relation on $\langle u_n\rangle_{n=0}^{\infty}$ with coefficients matching those of the characteristic polynomial $\det(\boldsymbol{A} - x\boldsymbol{I})$ of $\boldsymbol{A}$. Conversely, any LRS may be expressed in this way. Given a linear recurrence relation (2.4), it is sufficient to take $\boldsymbol{A}$ to be:

$$\boldsymbol{A} = \begin{bmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix}.$$

Then if $\boldsymbol{v}$ is the vector $(u_{k-1}, \ldots, u_0)^T$ of initial terms of $\langle u_n\rangle_{n=0}^{\infty}$ in reverse order and $\boldsymbol{w}$ is the unit vector $(0, \ldots, 0, 1)^T$, we have $u_n = \boldsymbol{v}^{\boldsymbol{T}}\boldsymbol{A}^n\boldsymbol{w}$. The characteristic polynomial of the LRS is the characteristic polynomial of $\boldsymbol{A}$, and the characteristic roots of the LRS are precisely the eigenvalues of $\boldsymbol{A}$.

By converting to the Jordan form, from the matrix expression $u_n = \boldsymbol{v}^{\boldsymbol{T}}\boldsymbol{A}^n\boldsymbol{w}$ we can obtain a closed-form solution for the $n$-th term of the linear recurrence sequence in terms of the eigenvalues $\lambda_1, \ldots, \lambda_l$ of $\boldsymbol{A}$:

$$u_n = \sum_{j=0}^{l} P_j(n)\lambda_j^n \tag{2.5}$$

for all $n \geq 0$, where $P_j \in \mathbb{F}[x]$ are univariate polynomials of degree strictly less than the multiplicity of $\lambda_j$ as a root of the characteristic polynomial of $\boldsymbol{A}$. In the case $\mathbb{F} = \mathbb{R}$, the set of characteristic roots is closed under complex conjugation. Thus, if $\rho_1, \ldots, \rho_l \in \mathbb{R}$ are the real roots of $P(x)$ and $\gamma_1, \overline{\gamma}_1, \ldots, \gamma_m, \overline{\gamma}_m \in \mathbb{C}$ are the complex ones, the sequence is given by

$$u_n = \sum_{j=1}^{l} A_j(n)\rho_j^n + \sum_{j=1}^{m} \left(C_j(n)\gamma_j^n + \overline{C_j}(n)\overline{\gamma_j}^n\right) \tag{2.6}$$

for all $n \geq 0$, where $A_j \in \mathbb{R}[x]$ and $C_j \in \mathbb{C}[x]$. The coefficients of $P_j$ in (2.5) and of $A_j, C_j$ in (2.6) are algebraic numbers, effectively computable in polynomial time from the description of the LRS.

A linear recurrence sequence is called *degenerate* if for some pair of distinct characteristic roots $\lambda_1, \lambda_2$ of its minimum-order recurrence, the ratio $\lambda_1/\lambda_2$ is a root of unity, otherwise the sequence is *non-degenerate*. As pointed out in [Everest et al., 2003], the study of arbitrary LRS can effectively be reduced to that of non-degenerate LRS by partitioning the original LRS into finitely many non-degenerate subsequences. Specifically, for a given degenerate linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ with characteristic roots $\lambda_j$ and matrix form $u_n = \boldsymbol{v}^{\boldsymbol{T}}\boldsymbol{A}^n\boldsymbol{w}$, let $L$ be the least common multiple of the orders of all ratios $\lambda_i/\lambda_j$ which are roots of unity. Then for each $j \in \{0, \ldots, L-1\}$, consider the sequence

$$u_n^{(j)} = \boldsymbol{v}^{\boldsymbol{T}}\boldsymbol{A}^{nL+j}\boldsymbol{w} = \boldsymbol{v}^{\boldsymbol{T}}(\boldsymbol{A}^L)^n(\boldsymbol{A}^j\boldsymbol{w}).$$

Each of these sequences has characteristic roots $\lambda_i^L$ and is therefore non-degenerate, because $(\lambda_1/\lambda_2)^{Lk} = 1$ implies $\lambda_1^L = \lambda_2^L$. From the crude lower bound $\varphi(r) \geq \sqrt{r/2}$ on Euler's totient function, it follows that if $\alpha \in \mathbb{A}$ has degree $d$ and is a primitive $r$-th root of unity, then $r \leq 2d^2$. There are $||\boldsymbol{A}||^{\mathcal{O}(1)}$ ratios $\lambda_i/\lambda_j$ to consider, and if a ratio is a root of unity then its order is $||\boldsymbol{A}||^{\mathcal{O}(1)}$, so it follows that $L = 2^{\mathcal{O}(||\boldsymbol{A}||)}$. Thus, non-degeneracy can be ensured by considering at most exponentially many subsequences of the original LRS.

### 2.3.2 Exponential polynomials

In this section, we recall some facts about the general form of solutions of ordinary linear differential equations.

Consider a homogeneous linear differential equation of order $k$ with real coefficients $a_0, \ldots, a_{k-1}$ and real initial conditions $f(0), f'(0), \ldots, f^{(k-1)}(0)$:

$$f^{(k)} = a_1 f^{(k-1)} + \ldots + a_k f. \tag{2.7}$$

Consider also a system of linear first-order differential equations

$$\boldsymbol{x}'(t) = \boldsymbol{A}\boldsymbol{x}(t) \tag{2.8}$$

with $\boldsymbol{A} \in \mathbb{R}^{k \times k}$ and initial conditions $\boldsymbol{x}(0) \in \mathbb{R}^k$. We recall here that the solutions $f$ of order-$k$ differential equations of the form (2.7) are precisely the functions of the form $\boldsymbol{y}^{\boldsymbol{T}}\boldsymbol{x}(t)$ for $\boldsymbol{y} \in \mathbb{R}^k$ and $\boldsymbol{x}(t)$ solutions of systems of first-order differential equations of the form (2.8).

Indeed, suppose we are given an order-$k$ ODE of the form (2.7). Writing

$$\boldsymbol{A} = \begin{bmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix}.$$

and $\boldsymbol{x}(t) = (f^{(k-1)}(t), f^{(k-2)}(t), \ldots, f(t))^T$, we have $\boldsymbol{x}'(t) = \boldsymbol{A}\boldsymbol{x}(t)$, with $\boldsymbol{x}(0)$ given by the initial conditions of the original order-$k$ differential equation. From here, we recover $f(t) = \boldsymbol{y}^{\boldsymbol{T}}\boldsymbol{x}(t)$, where $\boldsymbol{y} = (0, 0, \ldots, 1)^T$.

Conversely, suppose a system (2.8) of linear first-order ODEs is given. Linearity of differentiation yields $\boldsymbol{x}^{(j)}(t) = \boldsymbol{A}^j\boldsymbol{x}(t)$ for all $j \in \mathbb{N}$. Then by the Cayley-Hamilton Theorem, $\boldsymbol{A}$ satisfies its own

characteristic equation: $P(\boldsymbol{A}) = \mathbf{0}$, where $P \in \mathbb{R}[x]$ has degree at most $k$. Therefore, we have $P(\boldsymbol{A})\boldsymbol{x}(t) = \mathbf{0}$, whence it is clear that $\boldsymbol{x}(t)$ satisfies an order-$k$ differential equation of the form (2.7) component-wise. Then clearly for any given $\boldsymbol{y} \in \mathbb{R}^k$, $\boldsymbol{y^T x(t)}$ is the unique solution of an order $k$ linear differential equation (2.7) with initial conditions directly obtainable from $\boldsymbol{A}$ and $\boldsymbol{x}(0)$.

Thus, we can assume that we can convert freely between these two representations. In the conversion, the size of the square matrix $\boldsymbol{A}$ in the system matches the order of the higher-order differential equation. Moreover, the coefficients $a_1, \ldots, a_k$ and initial values $f(0), f'(0), \ldots, f^{(k-1)}(0)$ are algebraic if and only if the entries of $\boldsymbol{A}$ and $\boldsymbol{x}(0)$ are algebraic.

Now we give explicit expressions for the solutions of such initial-value problems. We assume the real numbers in the description of the problem to be algebraic. The *characteristic polynomial* of the differential equation (2.7) is

$$P(x) = x^k - c_{k-1}x^{k-1} - \cdots - c_0 = 0,$$

and the roots of $P(x)$ are the *characteristic roots* of the differential equation. If $\lambda$ is a root of $P(x)$ of multiplicity $m$, then the function $f(t) = t^j e^{\lambda t}$ satisfies (2.7) for $j = 0, 1, \ldots, m-1$. There are $k$ distinct linearly independent solutions of (2.7) having this form, and these span the space of all solutions. The unique solution of the system (2.8) is $\boldsymbol{x}(t) = e^{\boldsymbol{A}t}\boldsymbol{x}(0)$.

Let the distinct roots of $P(x)$ be $\lambda_1, \ldots, \lambda_l$, with respective multiplicities $m_1, \ldots, m_l$. Write $\lambda_j = r_j + ia_j$ for real algebraic numbers $r_j, a_j$, $j = 1, \ldots, l$. Given real algebraic initial values of $f(0), f'(0), \ldots, f^{(n-1)}(0)$, the uniquely defined solution $f$ of (2.7) can be written in one of the following equivalent forms.

1. As a function of the form
$$f(t) = \boldsymbol{y^T} e^{\boldsymbol{A}t}\boldsymbol{x}(0),$$
where $e^{\boldsymbol{A}t}$ is the matrix exponential, obtained from the Taylor expansion of the exponential function applied to $\boldsymbol{A}t$.

2. As an *exponential polynomial*
$$f(t) = \sum_{j=1}^{l} P_j(t)e^{\lambda_j t}$$
where each $P_j$ is a polynomial with (complex) algebraic coefficients and degree at most $m_j - 1$.

3. As a function of the form
$$f(t) = \sum_{j=1}^{l} e^{r_j t}(P_j(t)\cos(a_j t) + Q_j(t)\sin(a_j t))$$
where the polynomials $P_j, Q_j$ have real algebraic coefficients and degrees at most $m_j - 1$.

4. As a function of the form
$$f(t) = \sum_{j=1}^{l} e^{r_j t} \sum_{s=0}^{m_s-1} b_{j,s} t^s \cos(a_j t + \varphi_{j,s})$$
where $b_{j,s}$ is real algebraic and $e^{i\varphi_{j,s}}$ algebraic for each $j, s$.

The conversion of the matrix formulation 1 to forms 2, 3 is easily seen from the Jordan form of $\boldsymbol{A}$. Indeed, if $\boldsymbol{A} = \boldsymbol{P^{-1}}\, diag(\boldsymbol{J_1}, \ldots, \boldsymbol{J_m})\boldsymbol{P}$, the matrix exponential is then given by

$$e^{\boldsymbol{A}t} = \boldsymbol{P^{-1}}\, diag\left(e^{\boldsymbol{J_1}t}, \ldots, e^{\boldsymbol{J_m}t}\right)\boldsymbol{P}$$

together with the well-known closed form for the exponential of a Jordan block $\boldsymbol{J}$ with eigenvalue $\lambda$:

$$\left(e^{\boldsymbol{J}t}\right)_{j,s} = e^{t\lambda}\frac{t^{j-s}}{(j-s)!} \text{ for } j \geq s$$

Carrying out the multiplication immediately yields form 2. To obtain form 3, it suffices to observe that $f$ is real-valued and then to systematically take real parts everywhere. Finally, to obtain form 4, for each $j$ in form 3, group terms of $P'_j$ and $P''_j$ of matching degree:

$$f(t) = \sum_{j=1}^{l} e^{r_j t} \sum_{k=0}^{m_j - 1} t^k (c_{j,k} \cos(a_j t) + d_{j,k} \sin(a_j t)).$$

Then take $b_{j,k} = \sqrt{c_{j,k}^2 + d_{j,k}^2}$ and let $\varphi_{j,k}$ be the angle in $[0, 2\pi)$ with $\cos(\varphi_{j,k}) = c_{j,k}/b_{j,k}$ and $\sin(\varphi_{j,k}) = -d_{j,k}/b_{j,k}$.

## 2.4 First-order theory of the reals

In this thesis we occasionally resort to the first-order theory of the real closed field, with and without exponentiation. We give a brief outline here, whilst a more complete overview may be found in [Marker, 2002].

### 2.4.1 Without exponentiation

We denote by $\mathcal{L}$ the first-order language $\mathbb{R}\langle +, \times, 0, 1, <, = \rangle$. Atomic formulas in this language are of the form $P(x_1, \ldots, x_n) = 0$ and $P(x_1, \ldots, x_n) > 0$ for $P \in \mathbb{Z}[x_1, \ldots, x_n]$ a polynomial with integer coefficients. A set $X \subseteq \mathbb{R}^n$ is *definable* in $\mathcal{L}$ if there exists some $\mathcal{L}$-formula $\phi(\bar{x})$ with free variables $\bar{x}$ which holds precisely for valuations in $X$. Analogously, a function is definable if its graph is a definable set. A set is *semi-algebraic* if it is definable by a quantifier-free formula of $\mathcal{L}$. It is worth remarking that any real algebraic number is readily definable within $\mathcal{L}$ using its minimal polynomial and a rational approximation to distinguish it from the other roots. Thus, we can treat real algebraic constants as built into the language and use them freely in the construction of formulas.

We denote by $Th(\mathbb{R})$ *the first-order theory of the reals*, that is, the set of all valid sentences in the language $\mathcal{L}$. Let $Th^{\exists}(\mathbb{R}_{exp})$ be the *existential first-order theory of the reals*, that is, the set of all valid sentences in the existential fragment of $\mathcal{L}$. A celebrated result due to Tarski [Tarski, 1951] is that $\mathcal{L}$ admits quantifier elimination: each formula $\phi_1(\bar{x})$ in $\mathcal{L}$ is equivalent to some effectively computable formula $\phi_2(\bar{x})$ which uses no quantifiers. This immediately entails the decidability of $Th(\mathbb{R})$. It also follows that sets definable in $\mathcal{L}$ are precisely the semialgebraic sets. Tarski's original result had non-elementary complexity, but improvements followed, culminating in the detailed analysis of Renegar [Renegar, 1992]:

**Theorem 13.** *1. $Th(\mathbb{R})$ is complete for* **2-EXPTIME**.

*2. $Th^{\exists}(\mathbb{R}_{exp})$ is decidable in* **PSPACE**.

*3. If $m \in \mathbb{N}$ is a fixed constant and we consider only existential sentences where the number of variables is bounded above by $m$, then validity is decidable in* **PTIME**.

### 2.4.2 With exponentiation

Decidability and geometrical properties of definable sets in the first-order theory of the structure $\mathcal{L}_{exp} = \mathbb{R}\langle +, \times, 0, 1, <, =, \exp \rangle$, the reals with exponentiation, have been explored by a number of authors. The work of Wilkie [Wilkie, 1996], combined with the earlier results of Khovanskii [Khovanskii, 1980], showed that the theory is *o-minimal*: that is, any set $X \subseteq \mathbb{R}^n$ definable in $\mathcal{L}_{exp}$ is a finite union of *cells*. The definition of a cell in $\mathbb{R}^n$ is inductive:

- If $X \subseteq \mathbb{R}$, then $X$ is a cell if and only if $X$ is a point or an interval.
- If $X \subseteq \mathbb{R}^n$ is a cell, and $f, g : X \to \mathbb{R}$ are continuous $\mathcal{L}_{exp}$-definable functions with $f(x) < g(x)$ for all $x \in X$, then $\{(x, y) \mid x \in X \text{ and } f(x) \sim_1 y \sim_2 g(x)\} \subseteq \mathbb{R}^{n+1}$ is also a cell, where $\sim_1, \sim_2 \in \{<, \leq\}$.

The decidability of $Th(\mathbb{R}_{exp})$ is still open. However, a celebrated result due to Macintyre and Wilkie is that if Schanuel's Conjecture is true then the theory is decidable [Macintyre and Wilkie, 1996].

We will not need the above two results in this thesis, however we use the following very special case, which we establish directly.

**Lemma 14.** *There is a procedure that, given a semi-algebraic set $S \subseteq \mathbb{R}^k$ and real algebraic numbers $a_1, \ldots, a_k$, returns an integer $T$ such that $\{t \geq 0 : (e^{a_1 t}, \ldots, e^{a_k t}) \in S\}$ either contains the interval $(T, \infty)$ or is disjoint from $(T, \infty)$. The procedure also decides which of these two eventualities is the case.*

*Proof.* Consider a polynomial $P \in \mathbb{Z}[u_1, \ldots, u_k]$. For suitably large $t$ the sign of $P(e^{a_1 t}, \ldots, a^{a_k t})$ is identical to the sign of the coefficient of the dominant term in the expansion of $P(e^{a_1 t}, \ldots, a^{a_k t})$ as an exponential polynomial. It follows that the sign of $P(e^{a_1 t}, \ldots, a^{a_k t})$ is eventually constant. It is moreover clear that one can effectively compute a threshold beyond which the sign $P(e^{a_1 t}, \ldots, a^{a_k t})$ remains the same. Since the set $S$ is a defined by a Boolean combination of inequalities $P(u_1, \ldots, u_k) \sim 0$, for $\sim \in \{<, =\}$, the claim immediately follows. □

## 2.5 Polyhedra

Here we state some basic properties of polyhedra. For more details we refer the reader to, for example [Grünbaum et al., 1967, McMullen and Shephard, 1971, Ziegler, 1995]. A *halfspace* in $\mathbb{R}^d$ is the set of points $\boldsymbol{x} \in \mathbb{R}^d$ satisfying $\boldsymbol{v^T x} \geq c$ for some fixed vector $\boldsymbol{v} \in \mathbb{R}^d$ and real number $c$. A *polyhedron* in $\mathbb{R}^d$ is the intersection of finitely many halfspaces:

$$\mathcal{P} = \left\{ \boldsymbol{x} \in \mathbb{R}^d : \begin{array}{rcl} \boldsymbol{v_1^T x} & \geq & c_1 \\ & & \vdots \\ \boldsymbol{v_m^T x} & \geq & c_m \end{array} \right\} \tag{2.9}$$

We call the set $\{(\boldsymbol{v_1}, c_1), \ldots, (\boldsymbol{v_m}, c_m)\}$ a *halfspace description* of a polyhedron, or simply an *H-polyhedron*. The problem of determining a minimal subset of the inequalities (2.9) that define the same polyhedron is called the *H-redundancy removal problem* and is solvable in polynomial time by reduction to linear programming. Thus, we may freely assume that there are no redundant constraints in the descriptions of H-polyhedra.

The *dimension* of a polyhedron $\mathcal{P}$, denoted $\dim(\mathcal{P})$, is the dimension of the subspace of $\mathbb{R}^d$ spanned by $\mathcal{P}$. The task of calculating the dimension of an H-polyhedron, called the *H-dimension problem*, can be done in polynomial time by solving polynomially many linear programs. If $\dim(\mathcal{P}) = d$, we call $\mathcal{P}$ *full-dimensional*. The minimal halfspace representation of a full-dimensional polyhedron is unique, up to scaling of the inequalities in (2.9).

The *convex cone* of a finite set of vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}$ is defined as

$$\text{cone}(\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}\}) = \{\lambda_1 \boldsymbol{v_1} + \cdots + \lambda_m \boldsymbol{v_m} : \lambda_j \geq 0 \text{ for all } j = 1, \ldots, m\}$$

If the vectors $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}$ are linearly independent, the cone is called *simplicial*. A classical result, due to Carathéodory, states that each finitely generated cone can be written as a finite union of simplicial cones:

**Theorem 15.** *(Carathéodory) Let $\boldsymbol{v_1}, \ldots, \boldsymbol{v_m} \in \mathbb{R}^d$. If $\boldsymbol{v} \in cone(\boldsymbol{v_1}, \ldots, \boldsymbol{v_m})$, then $\boldsymbol{v}$ belongs to the cone generated by a linearly independent subset of $\{\boldsymbol{v_1}, \ldots, \boldsymbol{v_m}\}$.*

We use this to prove that any two-dimensional polyhedron decomposes into a finite union of simple two-dimensional shapes:

**Lemma 16.** *Suppose $\mathcal{P} \subseteq \mathbb{R}^d$ is a two-dimensional polyhedron. Then $\mathcal{P} = \bigcup_{j=1}^{m} \mathcal{P}_j$, where $m$ is finite and each of $\mathcal{P}_j$ is of the form*

$$\mathcal{P}_j = \{\boldsymbol{u_j} + \alpha \boldsymbol{v_j} + \beta \boldsymbol{w_j} : p_j(\alpha, \beta)\}$$

*for vectors $\boldsymbol{u_j}, \boldsymbol{v_j}, \boldsymbol{w_j} \in \mathbb{R}^d$ and predicates $p_j(\alpha, \beta)$ chosen from the following:*

- *$\alpha \geq 0$ and $\beta \geq 0$ ($\mathcal{P}_j$ is an infinite cone)*

- $\alpha \geq 0$ *and* $\beta \geq 0$ *and* $\alpha + \beta \leq 1$ *($\mathcal{P}_j$ is a triangle)*
- $\alpha \geq 0$ *and* $\beta \geq 0$ *and* $\beta \leq 1$ *($\mathcal{P}_j$ is an infinite strip)*

*Furthermore, if we are given a halfspace description of $\mathcal{P}$ with length $\|\mathcal{P}\|$, the size of the representation of each vector $\boldsymbol{u_j}, \boldsymbol{v_j}, \boldsymbol{w_j}$ is at most $||\mathcal{P}||^{\mathcal{O}(1)}$.*

*Proof.* Let

$$\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : \boldsymbol{A}\boldsymbol{x} \geq \boldsymbol{b}\}$$

for some $\boldsymbol{A} \in \mathbb{R}^{m \times d}$, $\boldsymbol{b} \in \mathbb{R}^d$ and define the polygon

$$\mathcal{P}' = \{\boldsymbol{y} \in \mathbb{R}^{d+1} : [\ \boldsymbol{A} \quad -\boldsymbol{b}\ ]\, \boldsymbol{y} \geq 0\}$$

so that $\dim(\mathcal{P}') = 3$ and

$$\mathcal{P} = \{\boldsymbol{x} \in \mathbb{R}^d : (\ \boldsymbol{x} \quad 1\ )^T \in \mathcal{P}'\}$$

Notice that $\mathcal{P}'$ is specified using only homogeneous inequalities, so there exist vectors $V = \{\boldsymbol{v_1}, \ldots, \boldsymbol{v_s}\}$ such that $\mathcal{P}' = \text{cone}(V)$. By scaling if necessary, we can assume the $(d+1)$-th component of each $\boldsymbol{v_j}$ is either 0 or 1. Let $\mathcal{H}$ denote the hyperplane in $\mathbb{R}^{d+1}$ where the $(d+1)$-th coordinate is 1. By Carathéodory's Theorem, $\mathcal{P}'$ may be written as the union of finitely many cones generated from linearly independent subsets of $V$. Let $\boldsymbol{u_j}$ be the projection of $\boldsymbol{v_j}$ to the first $d$ coordinates. Since $\dim(\mathcal{P}') = 3$, no more than three elements of $V$ can be linearly independent, so

$$\mathcal{P}' = \bigcup_{(j_1,j_2,j_3) \in I} \text{cone}(\boldsymbol{v_{j_1}}, \boldsymbol{v_{j_2}}, \boldsymbol{v_{j_3}})$$

The intersection $\mathcal{H} \cap \text{cone}(\boldsymbol{v_{j_1}}, \boldsymbol{v_{j_2}}, \boldsymbol{v_{j_3}})$ is non-empty if and only if at least one of $\boldsymbol{v_{j_1}}, \boldsymbol{v_{j_2}}, \boldsymbol{v_{j_3}}$ has 1 in the $(d+1)$-th coordinate. Therefore, $\mathcal{P}$ is the finite union of shapes $\mathcal{P}_j$ with only two degrees of freedom:

$$\mathcal{P}_j = \{\alpha \boldsymbol{u_{j_1}} + \beta \boldsymbol{u_{j_2}} + \gamma \boldsymbol{u_{j_3}} : \alpha, \beta, \gamma \geq 0 \text{ and } p_j(\alpha, \beta, \gamma)\}$$

where each predicate $p_j$ is $\alpha = 1$, or $\alpha + \beta = 1$, or $\alpha + \beta + \gamma = 1$. These are precisely the desired three types of parametric shapes. The descriptions of the vectors involved is polynomially large because each vector $\boldsymbol{v_j}$ is the intersection of $d$ of the halfspaces in $\mathbb{R}^{d+1}$ which define $\mathcal{P}'$. □

A simpler version of the above result gives a similar parametric form in the case $\dim(\mathcal{P}) = 1$:

**Lemma 17.** *Suppose $\mathcal{P} \subseteq \mathbb{R}^d$ is a one-dimensional polyhedron. Then*

$$\mathcal{P} = \{\boldsymbol{v_1} + \alpha \boldsymbol{v_2} : p(\alpha)\}$$

*where the predicate $p(\alpha)$ is one of $\alpha \in \mathbb{R}$, $\alpha \geq 0$ and $\alpha \in [0, 1]$. Furthermore, if we are given a halfspace description of $\mathcal{P}$ with length $\|\mathcal{P}\|$, the size of the representation of $\boldsymbol{v_1}, \boldsymbol{v_2}$ is at most $||\mathcal{P}||^{\mathcal{O}(1)}$.*

# Chapter 3

# Discrete Skolem Problem

*Prerequisites:* Sections 2.1.1, 2.1.2, 2.1.4 and 2.3.1. Theorems 7 and 8 from Section 2.1.3.

## 3.1 Introduction

In this chapter, we study the *Discrete Skolem Problem*: given a linear recurrence sequence (LRS) $\langle u_n \rangle_{n=0}^{\infty}$, determine whether there exists a natural number $n$ such that $u_n = 0$. The sequence may be real- or complex-valued, but to make the problem well-defined, we shall require that the sequence be given in some effective form. For this reason, we take all the linear recurrence sequences in this chapter to be over the algebraic numbers, at times restricting further to real-valued or rational sequences.

Though it is not immediately obvious how a problem on linear recurrence sequences pertains to reachability in linear dynamical systems, the Discrete Skolem Problem nonetheless occupies a central place in this thesis. The connection becomes evident if we recall the matrix representation of linear recurrence sequences. If $\langle u_n \rangle_{n=0}^{\infty}$ is given by $u_n = \boldsymbol{y}^{\boldsymbol{T}} \boldsymbol{A}^n \boldsymbol{x}$ for a $d \times d$ matrix $\boldsymbol{A}$ and vectors $\boldsymbol{x}$ and $\boldsymbol{y}$, then $u_n = 0$ if and only if $\boldsymbol{A}^n \boldsymbol{x} \in \{\boldsymbol{y}\}^{\perp}$. That is, the orbit of $\boldsymbol{x}$ under $\boldsymbol{A}$ intersects the $(d-1)$-dimensional hyperplane $\{\boldsymbol{y}\}^{\perp}$ if and only if the linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order $d$ contains zero as an element.

The Discrete Skolem Problem has a history dating back to the 1930s, as evidenced by the celebrated Skolem-Mahler-Lech Theorem, a powerful result which characterises the zero sets of linear recurrence sequences:

**Theorem 18.** *(Skolem-Mahler-Lech) Let $\langle u_n \rangle_{n=0}^{\infty}$ be a linear recurrence sequence over a field with characteristic 0. Then the zero set of $\langle u_n \rangle_{n=0}^{\infty}$, $Z(u) = \{n \in \mathbb{N} : u_n = 0\}$, is semilinear, that is, the union of a finite set and finitely many arithmetic progressions.*

This result was originally established in the case of rational LRS in [Skolem, 1934], then strengthened to include LRS over the algebraic numbers in [Mahler, 1935], and finally extended to any field of characteristic 0 [Lech, 1953, Mahler and Cassels, 1956]. These proofs rely heavily on $p$-adic analysis and unfortunately do not yield constructive methods to compute the zero set of a given linear recurrence, nor to determine its emptiness. Nonetheless, later work [Berstel and Mignotte, 1976] established an effective procedure to explicitly calculate the arithmetic progressions mentioned in the theorem for LRS over the rationals. This immediately renders decidable the problem of deciding finiteness of the zero set of a rational LRS. In a similar vein, it is also decidable whether the zero set of a rational LRS is equal to $\mathbb{N}$, and whether it has a finite complement [Salomaa and Soittola, 1978, Section II.12].

Whilst the computation of the infinite component of the zero set is a significant advancement, no effective method is known to compute the finite component or to decide its emptiness. Thus, the decidability of the Discrete Skolem Problem remains open and is an outstanding question in number theory and theoretical computer science; see, for example, the exposition of [Tao, 2008, Section 3.9]. Efforts towards an upper complexity bound have yielded only partial results: decidability for LRS over $\mathbb{A}$ of order at most 3 and for LRS over $\mathbb{R} \cap \mathbb{A}$ of order 4 in references [Vereshchagin, 1985, Mignotte et al., 1984]. The decision method relies crucially on sophisticated results in transcendental number theory, specifically, Baker's

lower bounds on the magnitudes of linear forms in logarithms of algebraic numbers and van der Poorten's analogous results in the context of $p$-adic valuations. Recently, a proof of decidability for LRS of order 5 was announced in [Halava et al., 2005]. However, as pointed out in [Ouaknine and Worrell, 2012], the proof incorrectly addresses the case of LRS of the form:

$$u_n = A\lambda_1^n + \overline{A\lambda_1^n} + B\lambda_2^n + \overline{B\lambda_2^n} + Cr^n,$$

with one real and four complex characteristic roots with magnitudes satisfying $|\lambda_1| = |\lambda_2| > |r|$. Another paper [Litow, 1997] claims decidability for all orders, but is also flawed [Ouaknine and Worrell, 2012].

In terms of lower bounds, the strongest known result for the Discrete Skolem Problem is **NP**-hardness [Blondel and Portier, 2002]. Reference [Litow, 1997] claims **PSPACE**-hardness, but this has also been shown incorrect [Ouaknine and Worrell, 2012].

## 3.2 Main result and chapter outline

All the results contained in this chapter are based on our conference paper [Chonev et al., 2013] and its journal version [Chonev et al., 2016] (to appear). The main technical result of this chapter is the following:

**Theorem 19.** *Let $\langle u_n \rangle_{n=0}^{\infty}$ be a non-degenerate LRS of order $d$ over $\mathbb{A}$ whose description has size $\|u\|$.*

1. *If $d = 2$, then there exists a bound $N = ||u||^{\mathcal{O}(1)}$ such that if $u_n = 0$, then $n < N$.*
2. *If $d = 3$, then there exists a bound $N = 2^{\mathcal{O}(||u||)}$ such that if $u_n = 0$, then $n < N$.*
3. *If $d = 4$ and $\langle u_n \rangle_{n=0}^{\infty}$ is over $\mathbb{R} \cap \mathbb{A}$, then there exists a bound $N = 2^{\mathcal{O}(||u||)}$ such that if $u_n = 0$, then $n < N$.*

References [Mignotte et al., 1984, Vereshchagin, 1985] show the existence of similar bounds, but make no attempt to quantify the bounds in terms of the description of the input, thereby showing the problems decidable, but yielding no more specific complexity upper bound. The contribution of this chapter is to show the bounds are at most exponential in the size of the input, and in fact, polynomial for LRS of order 2. This permits us to obtain the following complexity bounds for the Discrete Skolem Problem for rational LRS:

**Theorem 20.** *For LRS over $\mathbb{Q}$ of order at most 4, the Discrete Skolem Problem is in the complexity class $\mathbf{NP}^{\mathbf{RP}}$. Further, for LRS over $\mathbb{Q}$ of order 2, the problem is in* **PTIME**.

Two points need to be addressed: how to reduce from arbitrary LRS to non-degenerate LRS, and how to obtain the complexity results of Theorem 20 from the bounds of Theorem 19.

On the first point, as we showed in Section 2.3.1, the study of arbitrary LRS can be reduced effectively to the non-degenerate case. This uses the technique of partitioning a given LRS into $L$ non-degenerate subsequences, where

$$L = \operatorname{lcm}\{\operatorname{order}(\lambda_i/\lambda_j) \,:\, \lambda_i, \lambda_j \text{ characteristic roots and } \lambda_i/\lambda_j \text{ root of unity }\}. \tag{3.1}$$

Specifically, if $\langle u_n \rangle_{n=0}^{\infty}$ is given, then we consider the sequences $\langle v_n^{(j)} \rangle_{n=0}^{\infty}$ defined by $v_n^{(j)} = u_{Ln+j}$ for $j = 0, \ldots, L-1$. These subsequences are non-degenerate, so for the purposes of showing decidability, non-degeneracy may be assumed without loss of generality. However, when attempting to establish a more precise complexity upper bound, the size of $L$ needs to be taken into account.

Recall that if $\alpha$ is an algebraic number of degree $d$ and a root of unity of order $r$, then $r \leq 2d^2$. In particular, if $\langle u_n \rangle_{n=0}^{\infty}$ is an LRS defined by $u_n = \boldsymbol{x}^{\boldsymbol{T}} \boldsymbol{A}^n \boldsymbol{y}$ described using $\|u\| = \|\boldsymbol{x}\| + \|\boldsymbol{A}\| + \|\boldsymbol{y}\|$ bits, and $\lambda_i, \lambda_j$ are characteristic roots such that $\lambda_i/\lambda_j$ is a root of unity, then $\operatorname{order}(\lambda_i/\lambda_j) = ||u||^{\mathcal{O}(1)}$. Since (3.1) takes the least common multiple of the orders of $\mathcal{O}(\|u\|^2)$ ratios $\lambda_i/\lambda_j$ and each order is polynomially large in the size of the input, it follows that $L = 2^{\mathcal{O}(||u||)}$. Moreover, this is not an over-approximation: it is easy to construct LRS where the ratios $\lambda_i/\lambda_j$ are roots of unity of mutually coprime orders, thereby making $L$ at least exponential in the size of the input. Thus, for arbitrary LRS, applying this technique to eliminate non-degeneracy carries an exponential overhead.

However, in this thesis, we restrict our attention to LRS of order at most 4. Therefore, in (3.1), the number of ratios considered is bounded by an absolute constant, so $L$ is the least common multiple of a fixed number of polynomially large orders, hence $L = ||u||^{\mathcal{O}(1)}$.

Furthermore, if the LRS is over $\mathbb{Q}$, then the degree of each characteristic root $\lambda_i$ is at most 4, since we know *a priori* that the characteristic polynomial of the sequence has rational coefficients. Then the degrees of all ratios $\lambda_i/\lambda_j$ are also absolutely bounded, so $L = \mathcal{O}(1)$. Therefore, in our context of rational LRS of bounded order, non-degeneracy may be obtained by considering a constant number of subsequences, whose matrix representation may be computed from that of $\langle u_n \rangle_{n=0}^{\infty}$ in polynomial time.

The second point is how to obtain the complexity upper bounds. For non-degenerate rational LRS $\langle u_n \rangle_{n=0}^{\infty}$ defined by $u_n = \boldsymbol{x}^{\boldsymbol{T}} \boldsymbol{A}^n \boldsymbol{y}$, let $N$ denote the bound provided by Theorem 19. If the sequence is of order 2, then $N$ is only polynomial in the size of the input. Thus, we simply calculate $u_n$ for all $n < N$. All intermediate results are rational numbers, and we only ever raise $\boldsymbol{A}$ to a polynomially large power, so the representation of all intermediate results stays polynomially bounded. Thus, the **PTIME** upper bound for LRS of order 2 follows directly.

For rational LRS of order 3 or 4, the bound $N$ is at most exponential in the size of the input. We argue the problem is in $\mathbf{NP}^{\mathbf{EqSLP}}$, where **EqSLP** is the complete class for the following problem: given a division-free straight-line program (or equivalently, an arithmetic circuit) producing an integer $M$, determine whether $M = 0$. Since the bound $N$ is at most exponentially large in the size of the input, an **NP** algorithm can guess the index of a purported zero: $n \in \mathbb{N}$ with $n < N$. Thus, we only need to verify that $u_n = 0$. Direct calculation is not an option, since $n$ is exponential in the size of the input, whilst the entries of $\boldsymbol{A}^n$ are doubly-exponential in magnitude, requiring an exponential number of bits to write down. However, we can easily represent the entries of $\boldsymbol{A}^n$ as polynomially-sized arithmetic circuits, using the technique of repeated squaring. Then verifying $u_n = 0$ reduces to checking whether a polynomially-large arithmetic circuit evaluates to 0, which can be solved by an **EqSLP** oracle. The bound $\mathbf{NP}^{\mathbf{EqSLP}}$ follows directly. Finally, it is known that **EqSLP** $\subseteq$ **coRP** [Schönhage, 1979], so we also have membership in $\mathbf{NP}^{\mathbf{RP}}$, as Theorem 20 claims.

Therefore, all that remains is to prove Theorem 19. We devote the rest of this chapter to the technical details of the proof. Sections 3.3, 3.5 and 3.6 address LRS of order 2, 3 and 4, respectively. Section 3.4 shows two applications of Baker's Theorem which are crucially important for orders 3 and 4. On a first reading, the rest of this chapter may be skipped safely if the reader is prepared to accept Theorem 19 on faith.

## 3.3 LRS of order two

In this section, we consider the problem of whether a linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order 2 over $\mathbb{A}$ contains zero as a term. The characteristic equation of the recurrence may have one repeated root $\theta$, or two distinct roots $\theta_1, \theta_2$. Thus, the $n$-th term of the sequence is given by one of the following:

$$u_n = (A + Bn)\theta^n \qquad \text{(where } A, B, \theta \in \mathbb{A} \text{ and } B, \theta \neq 0\text{)} \tag{3.2}$$

$$u_n = A\theta_1^n + B\theta_2^n \qquad \text{(where } A, B, \theta_1, \theta_2 \in \mathbb{A} \text{ and } A, B, \theta_1, \theta_2 \neq 0\text{)} \tag{3.3}$$

Solving the Skolem Problem for LRS of the form (3.2) is trivial: simply determine whether the unique root of $A + Bx$ is a natural number. We therefore concentrate on LRS of the form (3.3). In this case, $u_n = 0$ if and only if $(\theta_1/\theta_2)^n = -B/A$.

Thus, the problem reduces to the *algebraic number power problem:* decide whether there exists $n \in \mathbb{N}$ such that

$$\alpha^n = \beta \tag{3.4}$$

for given $\alpha, \beta \in \mathbb{A}$. The assumption of non-degeneracy of $\langle u_n \rangle_{n=0}^{\infty}$ allows us to assume $\alpha$ is not a root of unity[1]. The algebraic number power problem is decidable [Halava et al., 2005]. Reference [Kannan and Lipton, 1986] proved a polynomial bound on $n$ when $\beta$ has the form $P(\alpha)$ for a given $P \in \mathbb{Q}[x]$. We give a brief recapitulation of the decidability proof of [Halava et al., 2005] and sharpen it to extract a polynomial bound on $n$.

[1]Notice in passing that if $\alpha$ is a root of unity, then the algebraic number power problem is easy to decide: simply determine whether $\beta$ is an $r$-th root of unity, where $r$ is the order of $\alpha$. If this is indeed the case, however, then there exists no bound of the kind promised by Theorem 19, since $\alpha^n = \beta$ holds periodically.

**Lemma 21.** *Suppose $\alpha, \beta \in \mathbb{A}$. If $\alpha$ is not a root of unity, then there exists a bound $N$ such that if (3.4) holds, then $n < N$. Moreover, $N = ||I||^{\mathcal{O}(1)}$, where $\|I\| = \|\alpha\| + \|\beta\|$ is the length of the input.*

*Proof.* Let $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$. If $\alpha$ is not an algebraic integer, then by Lemma 2 there exists a prime ideal $P$ in the ring $\mathcal{O}_{\mathbb{K}}$ such that $v_P(\alpha) \neq 0$. Then if $\alpha^n = \beta$, we have

$$v_P(\alpha^n) = nv_P(\alpha) = v_P(\beta).$$

If $v_P(\alpha)$ and $v_P(\beta)$ have different signs, then we are done. Otherwise,

$$n = \frac{v_P(\beta)}{v_P(\alpha)} \leq |v_P(\beta)| \leq \log_2 |\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\beta)| \leq \log_2 |\mathcal{N}_{abs}(\beta)|^d,$$

where $d = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is at most polynomially large in $\|\alpha\| + \|\beta\|$. It follows that the bound on $n$ is polynomially large in the length of the input.

Suppose therefore that $\alpha$ is an algebraic integer. It is not a root of unity by the premise of the Lemma, so by Theorem 10 (Blanksby and Montgomery), $\alpha$ has a Galois conjugate $\sigma(\alpha)$ such that

$$|\sigma(\alpha)| > 1 + \frac{1}{30d^2 \log(6d)},$$

where $d$ is the degree of $\alpha$. This implies

$$\frac{1}{\log |\sigma(\alpha)|} < 60d^2 \log(6d).$$

Then if $\alpha^n = \beta$, we have

$$n = \frac{\log |\sigma(\beta)|}{\log |\sigma(\alpha)|} < \log |\sigma(\beta)| 60d^2 \log(6d).$$

Observe that if we are given canonical descriptions of $\alpha$ and $\beta$, then $60d^2 \log(6d)$ is at most polynomially large in $\|\alpha\|$, and $\log |\sigma(\beta)|$ is at most polynomially large in $\|\beta\|$. It follows that the bound on $n$ is polynomial in the length of the input. □

## 3.4 Application of Baker's Theorem

Before we proceed to LRS of order 3 and 4, we make a brief diversion to show two pertinent applications of Baker's Theorem. They essentially capture the technically difficult core of the Discrete Skolem Problem for LRS of order 3 or 4, so for clarity, they are exhibited here first, prior to their use in the context of LRS.

The first application concerns powers $\lambda^n$ ($n \in \mathbb{N}$) of an algebraic number $\lambda$ on the unit circle. We show that for large $n$ and any fixed $b \in \mathbb{A}$, the distance $|\lambda^n - b|$ cannot be 'too small', unless $\lambda$ is a root of unity.

**Lemma 22.** *Let $\lambda, b \in \mathbb{A}$, where $|\lambda| = 1$ and $\lambda$ is not a root of unity. Suppose $\phi(n)$ is a function from $\mathbb{N}$ to $\mathbb{C}$ for which there exist $a, \chi \in \mathbb{Q}$ such that $\chi \in (0, 1)$ and $|\phi(n)| \leq a\chi^n$. There exists a bound $N$ such that if*

$$\lambda^n = \phi(n) + b, \tag{3.5}$$

*then $n < N$. Moreover, $N$ is at most exponential in the length of the input $\|I\| = \|\lambda\| + \|b\| + \|a\| + \|\chi\|$.*

*Proof.* The left-hand side of (3.5) describes points on the unit circle, whereas the right-hand side tends to $b$. If $|b| \neq 1$, then for $n$ large enough, the right-hand side of (3.5) will always be off the unit circle. This happens when

$$n > \frac{\log(||b| - 1|/a)}{\log(\chi)}.$$

The difficult case is when $b$ is on the unit circle. Here we will use Baker's Theorem to derive a bound on $n$. Consider the angle $\Lambda$ between $\lambda^n$ and $b$. Since $\lambda$ is not a root of unity, by Lemma 21, this angle can be zero for at most one value of $n$, which is polynomially large in $\|I\|$. Otherwise, write

$$\Lambda = \log \frac{\lambda^n}{b} = n \log(\lambda) - \log(b) + 2k_n \log(-1) \neq 0,$$

where $k_n$ is an integer chosen so that $\Lambda = i\tau$ for some $\tau \in [0, 2\pi)$. Then $2n$ is an upper bound on the height of the coefficients in front of the logarithms (because $k_n \leq n$), $H = \max\{H_\lambda, H_b, 3\}$ is a height bound for the arguments to the logarithms and $d = \max\{\deg(\lambda), \deg(b)\}$ is a bound on the degrees. Then by Theorem 7 (Baker-Wüstholz), we have

$$\log|\Lambda| > -(48d)^{10}\log^2 H \log(2n),$$

which is equivalent to

$$|\Lambda| > (2n)^{-(48d)^{10}\log^2 H}.$$

This is a lower bound on the length of the arc between $\lambda^n$ and $b$. The length of the chord is at least half of the bound: $|\lambda^n - b| \geq |\Lambda|/2$. So in the equation $\lambda^n - b = \phi(n)$, the left-hand side is bounded below by an inverse polynomial in $n$. However, the right-hand side shrinks exponentially quickly in $n$. For all $n$ large enough, the right-hand side will be smaller in magnitude than the left-hand side.

We will now quantify the bound on $n$. Let $p_1 = (48d)^{10}\log^2 H$ and $p_2 = 2$. Observe that $p_1, p_2 = ||I||^{\mathcal{O}(1)}$. Then (3.5) cannot hold if

$$\frac{1}{2}(p_2 n)^{-p_1} \geq a\chi^n,$$

which is equivalent to

$$-\log(2) - \log(a) - p_1\log(p_2) - p_1\log(n) \geq n\log(\chi).$$

Define $p_3 = \log(2) + \log(a) + p_1\log(p_2)$ and $p_4 = \max\{p_3, p_1\} = ||I||^{\mathcal{O}(1)}$. Then it suffices to have

$$\frac{p_4}{-\log(\chi)} \leq \frac{n}{1+\log(n)},$$

which is guaranteed by

$$\sqrt{n} \geq \frac{p_4}{-\log(\chi)}.$$

Observe that $-1/\log(\chi)$ is at most exponentially large in $\|\chi\|$. Therefore, the bound on $n$ is exponential in the size of the input. □

Continuing in the same line, we next consider two algebraic numbers, $\lambda_1$ and $\lambda_2$, whose powers define discrete trajectories embedded in two circles in the complex plane: $a\lambda_1^n$ and $b\lambda_2^n + c$ as $n$ varies over $\mathbb{N}$. The following lemma shows that unless $\lambda_1, \lambda_2$ are roots of unity, then for large $n$, the $n$-th points of the two trajectories are never 'too close' to each other.

**Lemma 23.** *Suppose $\lambda_1, \lambda_2, a, b, c \in \mathbb{A}$ are non-zero, where $|\lambda_1| = |\lambda_2| = 1$ and $\lambda_1, \lambda_2$ are not roots of unity. Let $\phi(n)$ be a function from $\mathbb{N}$ to $\mathbb{C}$ such that $0 < |\phi(n)| \leq w\chi^n$ for some $w, \chi \in \mathbb{Q}$, $\chi \in (0,1)$. Then there exists a bound $N$ such that if*

$$a\lambda_1^n = b\lambda_2^n + c + \phi(n), \tag{3.6}$$

*then $n < N$. Moreover, $N = 2^{\mathcal{O}(||I||)}$, where $\|I\| = \|\lambda_1\| + \|\lambda_2\| + \|a\| + \|b\| + \|c\| + \|w\| + \|\chi\|$.*

*Proof.* Multiplying the equation by $\overline{c}/|c||a|$ allows us to assume that $|a| = 1$ and $c \in \mathbb{R}^+$.

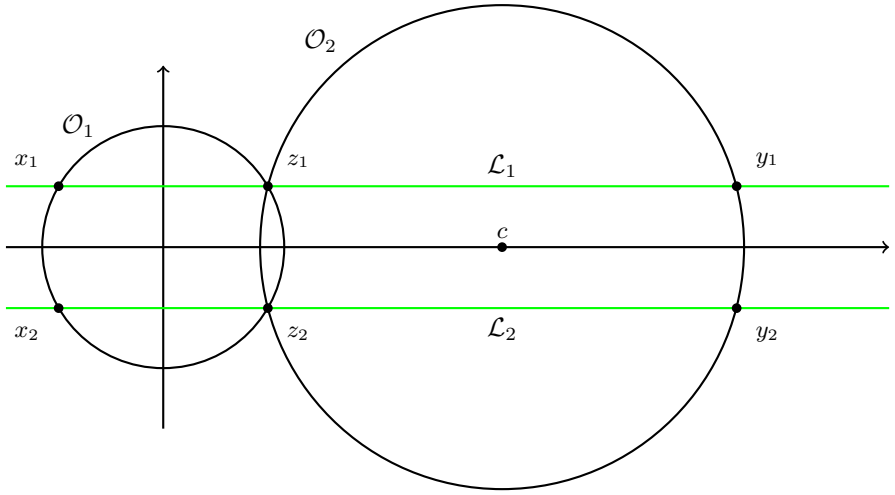
Let $f(n) = a\lambda_1^n$, $g(n) = b\lambda_2^n + c$. It is clear that $f(n)$ describes points on the unit circle $\mathcal{O}_1$, whilst $g(n)$ describes points on the circle $\mathcal{O}_2$ with centre $c$ on the real line and radius $|b|$.

If these circles do not intersect, then for $n$ large enough, $|\phi(n)|$ will be forever smaller than the smallest distance between the circles. This happens when

$$n > \frac{\log(c - |b| - 1) - \log(w)}{\log(\chi)},$$

which is an exponential lower bound on $n$ in the size of the input.

Suppose now the circles intersect in two points, $z_1$ and $z_2$. Let $\mathcal{L}_1$ be the horizontal line through $z_1$ and $\mathcal{L}_2$ the horizontal line through $z_2$. Let $\mathcal{L}_1 \cap \mathcal{O}_1 = \{x_1, z_1\}$, $\mathcal{L}_1 \cap \mathcal{O}_2 = \{y_1, z_1\}$, $\mathcal{L}_2 \cap \mathcal{O}_1 = \{x_2, z_2\}$ and $\mathcal{L}_2 \cap \mathcal{O}_2 = \{y_2, z_2\}$. It is trivial that $z_2 = \overline{z_1}$, $x_2 = \overline{x_1}$, $y_2 = \overline{y_1}$.




We first argue that for $n$ large enough, (3.6) can hold only if for some intersection point $z_i$, $\Re(z_i)$ lies between $\Re(f(n))$ and $\Re(g(n))$, or $\Im(z_i)$ lies between $\Im(f(n))$ and $\Im(g(n))$. This can only be violated in two symmetric situations: either

1. $f(n)$ is on the arc $z_1z_2$ of $\mathcal{O}_1$ which lies inside $\mathcal{O}_2$ and $g(n)$ is on the arc $y_1y_2$ of $\mathcal{O}_2$ which lies outside $\mathcal{O}_1$, or
2. $f(n)$ is on the arc $x_1x_2$ of $\mathcal{O}_1$ which lies outside $\mathcal{O}_2$ and $g(n)$ is on the arc $z_1z_2$ of $\mathcal{O}_2$ which lies inside $\mathcal{O}_1$.

In the first situation, when $g(n)$ is on the arc $y_1y_2$ of $\mathcal{O}_2$ outside $\mathcal{O}_1$, we have

$$|f(n) - g(n)| \geq |g(n)| - 1 \geq |y_1| - 1.$$

Since the point $y_1$ is strictly to the right of 1 on the complex plane, this lower bound is positive, and moreover it is independent of $n$, so (3.6) cannot hold for $n$ large enough because $\phi(n)$ tends to zero exponentially quickly. In particular, (3.6) does not hold if

$$n > \frac{\log(|y_1| - 1) - \log(w)}{\log(\chi)},$$

which is exponentially large in the size of the input. The second situation is analogous.

Therefore, we can assume that one of the intersection points $z_i$ separates $f(n)$ and $g(n)$ horizontally or vertically in the figure. That is, $z_i$ satisfies $\Re(f(n)) \leq \Re(z_i) \leq \Re(g(n))$ or $\Im(f(n)) \leq \Im(z_i) \leq \Im(g(n))$. We will show a lower bound on $|f(n)-g(n)|$ which shrinks slower than exponentially. The real (horizontal) and imaginary (vertical) cases are completely analogous. We show the working for the real case. Assume that $\Re(z_i)$ lies between $\Re(f(n))$ and $\Re(g(n))$. Clearly,

$$|f(n) - g(n)| \geq |\Re(g(n) - f(n))| = |\Re(z_i - f(n))| + |\Re(g(n) - z_i)|.$$

Let $\alpha = \arg(\lambda_1)$, $\gamma = \arg(a)$ and $\beta = \arg(z_i)$. Then

$$|\Re(z_i - f(n))| = |\cos(n\alpha + \gamma) - \cos(\beta)| = 2\left|\sin\frac{\beta - n\alpha - \gamma}{2}\sin\frac{\beta + n\alpha + \gamma}{2}\right|.$$

Let $u_n, v_n$ be appropriately chosen integers so that

$$\frac{\beta - n\alpha - \gamma}{2} + u_n\pi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right],$$

$$\frac{\beta + n\alpha + \gamma}{2} + v_n\pi \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right].$$

Then using the inequality

$$|\sin(x)| \geq \frac{|x|}{\pi} \text{ for } x \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right],$$

we have

$$\left|\sin\frac{\beta-n\alpha-\gamma}{2}\right| \geq \frac{1}{\pi}\left|\frac{\beta-n\alpha-\gamma}{2}+\pi u_n\right|,$$
$$\left|\sin\frac{\beta+n\alpha+\gamma}{2}\right| \geq \frac{1}{\pi}\left|\frac{\beta+n\alpha+\gamma}{2}+\pi v_n\right|.$$

Both of these expressions are sums of logarithms of algebraic numbers, non-zero for $n$ exceeding a polynomially large bound in $\|I\|$ by Lemma 21, so we can give lower bounds for them using Theorem 7 (Baker-Wüstholz) as in Lemma 22:

$$|\Re(z_i - f(n))| \geq (p_1 n)^{-p_2}$$

for some $p_1, p_2 > 0$ which are independent of $n$ and at most polynomially large in the input. A similar lower bound holds for $|\Re(g(n) - z_i)|$. If $\delta = \arg(\lambda_2)$, $\eta = \arg(b)$ and $\theta = \arg(z_i - c)$, we have

$$|\Re(g(n) - z_i)| = |b|(\cos(n\delta + \eta) - \cos(\theta)) \geq (p_3 n)^{-p_4},$$

where $p_3, p_4 > 0$ are independent of $n$ and have at most polynomial size in the input. Hence we have

$$|f(n) - g(n)| \geq 2(p_5 n)^{-p_6},$$

where $p_5 = \max\{p_1, p_3\}$ and $p_6 = \max\{p_2, p_4\}$. Since $\phi(n)$ shrinks exponentially quickly, a bound on $n$ follows past which (3.6) cannot hold. In the manner of Lemma 22, we can show that this bound is exponentially large in the size of the input. The vertical case is analogous, except that considering imaginary parts gives sines instead of cosines, so we shift all angles by $\pi/2$ and proceed as above. If the circles are tangent and neither lies inside the other, then the intersection point separates $f(n)$ and $g(n)$ horizontally, so we are done by the above analysis.

Finally, suppose that the circles are tangent and one lies inside the other: $|b| + c = 1$. The argument of $f(n)$ is $\gamma + n\alpha$. By the law of cosines applied to the triangle with vertices $f(n)$ and the centres of the circles, we have

$$|f(n) - c|^2 = c^2 + 1 - 2c\cos(\gamma + n\alpha).$$

Therefore, the shortest distance from $f(n)$ to a point on $\mathcal{O}_2$ is

$$h(n) = \sqrt{c^2 + 1 - 2c\cos(\gamma + n\alpha)} - (1 - c).$$

Let $A(n) = \sqrt{c^2 + 1 - 2c\cos(\gamma + n\alpha)}$ and $B = 1 - c$. Since $A \leq 1 + c$, we have $A + B \leq 2$, so

$$h(n) = A - B = \frac{A^2 - B^2}{A + B} \geq c(1 - \cos(\gamma + n\alpha))$$

Let $k_n$ be an integer, so that

$$\gamma + n\alpha + k_n 2\pi \in [-\pi, \pi).$$

By Lemma 21, this is zero for at most one, polynomially large in $\|I\|$, value of $n$. For larger $n$, a lower bound on this angle follows from Theorem 7 (Baker-Wüstholz):

$$|\gamma + n\alpha + k_n 2\pi| \geq (p_7 n)^{-p_8}$$

for some constants $p_7, p_8 > 0$ which are polynomially large in the input. Then

$$\cos(\gamma + n\alpha) \leq \cos((p_7 n)^{-p_8}),$$

so

$$h(n) \geq c(1 - \cos((p_7 n)^{-p_8})).$$

From the Taylor expansion of $\cos(x)$, it follows easily that

$$1 - \cos(x) \geq \frac{11}{24}x^2 \text{ for } x \leq 1.$$

Since $p_7, p_8 \geq 1$, we have $(p_7 n)^{-p_8} \leq 1$. Therefore,

$$h(n) \geq c\frac{11}{24}(p_7 n)^{-2p_8}.$$

This lower bound on $h(n)$ shrinks inverse-polynomially as $n$ grows. Recall that $h(n)$ is the smallest distance from $f(n)$ to $\mathcal{O}_2$. It follows that for $n$ large enough, $|\phi(n)| < h(n)$ forever, so $f(n) = g(n) + \phi(n)$ cannot hold. In the manner of Lemma 22, we can show that the bound on $n$ is exponentially large in the input. □

## 3.5 LRS of order three

We now move to the problem of determining whether a linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order 3 over $\mathbb{A}$ contains zero as an element. The characteristic equation of such a sequence may have either three distinct (real or complex) roots, or one repeated real root and one simple real root, or one real root of multiplicity 3. Thus, the $n$-th element of the sequence is given by one of the following:

$$u_n = A\alpha^n + B\beta^n + C\gamma^n \qquad \text{(where } A, B, C, \alpha, \beta, \gamma \in \mathbb{A} \text{ are all non-zero)} \tag{3.7}$$

$$u_n = (A + Bn)\alpha^n + C\beta^n \qquad \text{(where } A, B, C, \alpha, \beta \in \mathbb{A} \text{ with } B, C, \alpha, \beta \neq 0) \tag{3.8}$$

$$u_n = (Cn^2 + Bn + A)\alpha^n \qquad \text{(where } A, B, C, \alpha \in \mathbb{A} \text{ with } C, \alpha \neq 0) \tag{3.9}$$

Finding the zeros of LRS of the form (3.9) is trivial: simply check whether the quadratic $Cn^2 + Bn + A$ has roots which are natural numbers. Thus, we focus on the remaining two possibilities. We will consider only non-degenerate sequences: the ratios of the roots $\alpha, \beta, \gamma$ are not roots of unity.

First we consider $\langle u_n \rangle_{n=0}^{\infty}$ given by (3.7). Notice that $A, B, C, \alpha, \beta, \gamma$ are all non-zero, otherwise the sequence satisfies a recurrence relation of lower order. Thus, we can rearrange $u_n = 0$ to obtain:

$$\left(\frac{\beta}{\alpha}\right)^n = -\frac{C}{B}\left(\frac{\gamma}{\alpha}\right)^n - \frac{A}{B}. \tag{3.10}$$

Assume without loss of generality $|\alpha| \geq |\beta| \geq |\gamma|$. In Lemmas 24, 25, 26 below, we consider separately the cases $|\alpha| > |\beta|$, $|\alpha| = |\beta| > |\gamma|$ and $|\alpha| = |\beta| = |\gamma|$, and obtain a bound on $n$ which is exponential in the length of the description of the sequence and beyond which $u_n = 0$ cannot hold.

**Lemma 24.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is given by (3.7). If $|\alpha| > |\beta|$, then there exists a bound $N$ such that if $u_n = 0$, then $n < N$. Moreover, $N = 2^{\mathcal{O}(||I||)}$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|\alpha\| + \|\beta\| + \|\gamma\|$.*

*Proof.* This follows straightforwardly from the dominance of $\alpha$. If

$$n > \max\left\{\frac{\log|A/2B|}{\log|\beta/\alpha|}, \frac{\log|A/2C|}{\log|\gamma/\alpha|}\right\},$$

then

$$\left|-\frac{B}{A}\left(\frac{\beta}{\alpha}\right)^n - \frac{C}{A}\left(\frac{\gamma}{\alpha}\right)^n\right| \leq \left|\frac{B}{A}\left(\frac{\beta}{\alpha}\right)^n\right| + \left|\frac{C}{A}\left(\frac{\gamma}{\alpha}\right)^n\right| < \frac{1}{2} + \frac{1}{2} = 1.$$

□

**Lemma 25.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is given by (3.7). If $|\alpha| = |\beta| > |\gamma|$, then there exists a bound $N$ such that if $u_n = 0$, then $n < N$. Moreover, $N = 2^{\mathcal{O}(||I||)}$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|\alpha\| + \|\beta\| + \|\gamma\|$.*

*Proof.* This is a direct application of Lemma 22 to equation (3.10). □

**Lemma 26.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is given by (3.7). If $|\alpha| = |\beta| = |\gamma|$, there exist at most two values of $n$ such that $u_n = 0$. Moreover, they are at most exponential in the length of the input $\|A\| + \|B\| + \|C\| + \|\alpha\| + \|\beta\| + \|\gamma\|$ and are computable in polynomial time.*

*Proof.* The left-hand side of (3.10) as a function of $n$ describes points on the unit circle in the complex plane, whereas the right-hand side describes points on a circle centred at $-A/B$ with radius $|C/B|$. Note these circles do not coincide, because $A \neq 0$. We can obtain their equations and compute their intersection point(s). If they do not intersect, then equation (3.10) can never hold. Otherwise, the equation can only hold if the two sides are simultaneously equal to the same intersection point. For each of the (at most two) intersection points $\theta$, let

$$S_1 = \left\{n \;\middle|\; \left(\frac{\beta}{\alpha}\right)^n = \theta\right\},$$

$$S_2 = \left\{n \;\middle|\; -\frac{C}{B}\left(\frac{\gamma}{\alpha}\right)^n - \frac{A}{B} = \theta\right\}.$$

Observe that $|S_i| \leq 1$, because $\beta/\alpha$ and $\gamma/\alpha$ are not roots of unity. We compute $S_1$ and $S_2$ from the bound in Lemma 21 and check whether $S_1 \cap S_2$ is non-empty. □

Next, we consider LRS of the form (3.8). We will assume that $B, C, \alpha, \beta$ are all non-zero, otherwise the sequence satisfies a linear recurrence of lower order.

**Lemma 27.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is given by (3.8). There exists a bound $N$ such that if $u_n = 0$, then $n < N$. Moreover, $N = 2^{\mathcal{O}(||I||)}$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|\alpha\| + \|\beta\|$.*

*Proof.* We wish to solve for $n \in \mathbb{N}$ the equation:

$$(A + Bn)\alpha^n + C\beta^n = 0. \tag{3.11}$$

If $|\alpha| \geq |\beta|$, then for

$$n > \frac{|A| + |C|}{|B|},$$

we have

$$|C| < |B|n - |A| \leq |A + Bn|,$$

so

$$|C\beta^n| < |(A + Bn)\alpha^n|,$$

therefore (3.11) cannot hold. Now suppose $|\alpha| > |\beta|$ and rewrite (3.11) as

$$\frac{A + Bn}{C} = -\left(\frac{\beta}{\alpha}\right)^n.$$

Equation (3.11) implies

$$\left|\frac{\beta}{\alpha}\right|^n = \left|\frac{A + Bn}{C}\right| \leq \left|\frac{A}{C}\right| + \left|\frac{B}{C}\right| n.$$

However, we will show that for all $n$ large enough, this fails to hold. Indeed, the inequality

$$\left|\frac{\beta}{\alpha}\right|^n > \left|\frac{A}{C}\right| + \left|\frac{B}{C}\right| n$$

is implied by

$$d\,(n+1) < \left|\frac{\beta}{\alpha}\right|^n,$$

where $d = \max\{|A/C|, |B/C|\}$. Taking logarithms, we see that it suffices to have

$$\frac{n}{1 + \log(n+1)} > \frac{f}{\log|\beta/\alpha|},$$

where $f = \max\{\log(d), 1\}$. Noting that $1 + \log(n+1) < 2\sqrt{n}$ for all $n \geq 1$, we see that it suffices to have

$$n > 4f^2 / \log^2|\beta/\alpha|$$

to guarantee that (3.11) cannot hold. This is an exponential bound on $n$ in the length of the input. □

## 3.6 LRS of order four

We now proceed to the problem of determining whether a linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of order 4 over $\mathbb{A}$ contains zero as an element. As before, we assume non-degeneracy of the sequence. Depending on the roots of the characteristic polynomial, the $n$-th term of the sequence is given by one of the following (where $A, B, C, D, \alpha, \beta, \gamma, \delta$ are algebraic):

$$u_n = A\alpha^n + B\beta^n + C\gamma^n + D\delta^n \qquad \text{(where } A, B, C, D \neq 0\text{)} \tag{3.12}$$

$$u_n = (A + Bn)\alpha^n + C\beta^n + D\gamma^n \qquad \text{(where } B, C, D \neq 0\text{)} \tag{3.13}$$

$$u_n = (A + Bn)\alpha^n + (C + Dn)\beta^n \qquad \text{(where } B, D \neq 0\text{)} \tag{3.14}$$

$$u_n = (A + Bn + Cn^2)\alpha^n + D\beta^n \qquad \text{(where } C, D \neq 0\text{)} \tag{3.15}$$

$$u_n = (A + Bn + Cn^2 + Dn^3)\alpha^n \qquad \text{(where } D \neq 0\text{)} \tag{3.16}$$

Solving $u_n = 0$ in the case of $\langle u_n \rangle_{n=0}^{\infty}$ given by (3.16) is trivial: just calculate canonical descriptions of the roots of $A + Bx + Cx^2 + Dx^3$ and check whether any are natural numbers.

In the case of $\langle u_n \rangle_{n=0}^{\infty}$ given by (3.15), rearrange $u_n = 0$ as

$$(A + Bn + Cn^2)\left(\frac{\alpha}{\beta}\right)^n = -D.$$

The left-hand side tends to 0 or $\infty$ in magnitude, depending on whether $|\alpha| < |\beta|$. In both cases, since $C, D \neq 0$, a bound on $n$ follows which is at most exponential in the size of the input.

The remaining three cases, where $\langle u_n \rangle_{n=0}^{\infty}$ is of the form (3.12), (3.13) or (3.14) are more involved. They are the subject of Lemmas 28, 29, 30 and 31, which show the existence of a bound $N$ which is at most exponentially large in the size of the input and beyond which $u_n = 0$ cannot hold.

Note that for complex algebraic LRS given by (3.12) with characteristic roots all of the same magnitude, the Discrete Skolem Problem is not known to be decidable. Thus, our final technical result, Lemma 31 will require the simplifying assumption that $u_n \in \mathbb{R} \cap \mathbb{A}$ for all $n$. This is the only reason why Theorem 19 insists that LRS of order 4 be real algebraic. In all other cases, as shown by Lemmas 28, 29 and 30, an exponential bound on $n$ exists even for complex algebraic LRS.

**Lemma 28.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is non-degenerate and is given by (3.14). There exists a bound $N = 2^{\mathcal{O}(||I||)}$ such that if $u_n = 0$, then $n < N$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|D\| + \|\alpha\| + \|\beta\|$.*

*Proof.* We wish to solve for $n \in \mathbb{N}$ the equation:

$$(A + Bn)\alpha^n + (C + Dn)\beta^n = 0 \text{ (where } B, D \neq 0). \tag{3.17}$$

Rearrange (3.17) as

$$\lambda^n = -\frac{(C + Dn)}{(A + Bn)}, \tag{3.18}$$

where $\lambda = \alpha/\beta$ is not a root of unity. The right-hand side of (3.18) tends to $-D/B$ as $n$ tends to infinity.

If $\lambda$ is an algebraic integer, then by Theorem 10 (Blanksby and Montgomery), it has a Galois conjugate $\sigma(\lambda)$ such that

$$|\sigma(\lambda)| > 1 + \frac{1}{30d^2 \log(6d)},$$

where $d$ is the degree of $\lambda$. Assume the monomorphism $\sigma$ has been applied to both sides of (3.18), so $|\lambda|$ is bounded away from 1 by an inverse polynomial in the size of the input. By the triangle inequality, if

$$n \geq \frac{|BC| + |AD| + |AB|}{|B|^2} \stackrel{\text{def}}{=} N_1 = 2^{\mathcal{O}(||I||)},$$

then

$$\left|\frac{C + Dn}{A + Bn}\right| \leq \frac{|D|n + |C|}{|B|n - |A|} \leq \left|\frac{D}{B}\right| + 1.$$

Following the reasoning of Lemma 21 and relying on the Blansky and Montgomery bound, we see there exists a bound $N_2 \in ||I||^{\mathcal{O}(1)}$ such that if $n > N_2$, then $|\lambda^n| > |D/B| + 1$. Therefore, for $n > \max\{N_1, N_2\} = 2^{\mathcal{O}(||I||)}$, equation (3.18) cannot hold.

Second, suppose $\lambda$ is not an algebraic integer. Then by Lemma 2 there exists a prime ideal $P$ in the ring of integers of $\mathbb{K} = \mathbb{Q}(\alpha, \beta, A, B, C, D)$ such that $v_P(\lambda) \neq 0$. Without loss of generality, we can

assume $v_P(\lambda) > 0$ (if $v_P(\lambda) < 0$, swap $\alpha$ with $\beta$, $A$ with $C$, and $B$ with $D$). Applying $v_P$ to (3.18) gives

$$\begin{aligned} v_P(\lambda^n) &= nv_P(\lambda) \\ &= v_P\left(-\frac{C+Dn}{A+Bn}\right) \\ &\leq \log\left|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}\left(-\frac{C+Dn}{A+Bn}\right)\right| \\ &\leq [\mathbb{K}:\mathbb{Q}]\log\left|\mathcal{N}_{abs}\left(-\frac{C+Dn}{A+Bn}\right)\right| \\ &= [\mathbb{K}:\mathbb{Q}]\log\prod_{i=1}^{[\mathbb{K}:\mathbb{Q}]}\left|\frac{\sigma_i(C)+\sigma_i(D)n}{\sigma_i(A)+\sigma_i(B)n}\right|, \end{aligned}$$

where $\sigma_1, \ldots, \sigma_{[\mathbb{K}:\mathbb{Q}]}$ are the monomorphisms from $\mathbb{K}$ into $\mathbb{C}$. As in the previous case, if

$$n > \frac{|\sigma_i(BC)| + |\sigma_i(AD)| + |\sigma_i(AB)|}{|\sigma_i(B)|^2} \stackrel{\text{def}}{=} N_i = 2^{\mathcal{O}(||I||)},$$

then we have

$$\left|\frac{\sigma_i(C)+\sigma_i(D)n}{\sigma_i(A)+\sigma_i(B)n}\right| \leq \left|\frac{\sigma_i(D)}{\sigma_i(B)}\right| + 1 \stackrel{\text{def}}{=} e_i = 2^{\mathcal{O}(||I||)}.$$

It follows therefore that if $n > \max_i\{N_i\}$, we have

$$v_P\left(-\frac{C+Dn}{A+Bn}\right) \leq [\mathbb{K}:\mathbb{Q}]\sum_{i=1}^{[\mathbb{K}:\mathbb{Q}]}\log e_i \stackrel{\text{def}}{=} M = ||I||^{\mathcal{O}(1)}.$$

Then for $n > \max_i\{N_i\}$ and $n > M$, we have

$$v_P(\lambda^n) = nv_P(\lambda) \geq n > M,$$

whereas

$$v_P\left(-\frac{C+Dn}{A+Bn}\right) \leq M,$$

so equation (3.18) cannot hold. □

**Lemma 29.** *Suppose $\langle u_n\rangle_{n=0}^{\infty}$ is non-degenerate and is given by (3.13). There exists a bound $N = 2^{\mathcal{O}(||I||)}$ such that if $u_n = 0$, then $n < N$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|D\| + \|\alpha\| + \|\beta\| + \|\gamma\|$.*

*Proof.* We wish to solve for $n \in \mathbb{N}$ the equation:

$$(A+Bn)\alpha^n + C\beta^n + D\gamma^n = 0 \text{ (where } B, C, D \neq 0). \tag{3.19}$$

First suppose $|\alpha| \geq |\beta|, |\gamma|$. Then the term $(A+Bn)\alpha^n$ is dominant. More precisely, rewrite (3.19) as

$$A + Bn = -C\left(\frac{\beta}{\alpha}\right)^n - D\left(\frac{\gamma}{\alpha}\right)^n$$

and observe that if

$$n > \frac{|A| + |C| + |D|}{|B|},$$

then

$$|A+Bn| \geq |B|n - |A| > |C| + |D| \geq \left|-C\left(\frac{\beta}{\alpha}\right)^n - D\left(\frac{\gamma}{\alpha}\right)^n\right|,$$

so (3.19) cannot hold due to the strictness of the above inequality.

Second, suppose that $|\beta| > |\alpha|, |\gamma|$. Then the term $C\beta^n$ is dominant. More precisely, rewrite (3.19) as

$$(A+Bn)\left(\frac{\alpha}{\beta}\right)^n + D\left(\frac{\gamma}{\beta}\right)^n = -C. \tag{3.20}$$

We show that for $n$ sufficiently large, the inequalities

$$\left|D\left(\frac{\gamma}{\beta}\right)^n\right| < \frac{|C|}{2}$$

and

$$\left|(A+Bn)\left(\frac{\alpha}{\beta}\right)^n\right| < \frac{|C|}{2}$$

both hold, rendering (3.20) impossible. The former inequality holds for $n > \log|C/2D|/\log|\gamma/\beta|$, which is at most exponentially large in the input. The latter inequality is implied by

$$\left|(n+1)\left(\frac{\alpha}{\beta}\right)^n\right| < \frac{|C|}{2M},$$

where $M = \max\{|A|, |B|\}$. Now let $r = \lceil -\log(2)/\log(\alpha/\beta)\rceil$, so that

$$\left(\frac{\alpha}{\beta}\right)^r \leq \frac{1}{2},$$

and consider only $n$ of the form $n = kr$ for $k \in \mathbb{Z}^+$. If

$$k > \frac{\log|C/4Mr|}{\log(7/8)}$$

and $k \geq 5$, we have

$$\left(\frac{\alpha}{\beta}\right)^{kr} k < \left(\frac{1}{2}\right)^k (k+1) < \left(\frac{7}{8}\right)^k < \frac{|C|}{4Mr},$$

so

$$\left(\frac{\alpha}{\beta}\right)^n (n+1) \leq \left(\frac{\alpha}{\beta}\right)^n 2n < \frac{|C|}{2M}.$$

It is clear that $r$ is at most exponentially large in the size of the input, whereas the bound on $k$ is polynomial. Therefore, the bound on $n$ is exponential.

Finally, suppose $|\beta| = |\gamma| > |\alpha|$. Rewrite (3.19) as

$$\left(\frac{\beta}{\gamma}\right)^n = -\frac{D}{C} - \frac{A+Bn}{C}\left(\frac{\alpha}{\gamma}\right)^n.$$

Then an exponential bound on $n$ follows from Lemma 22, because the right-hand side is a constant plus an exponentially decaying term, whereas the left-hand side is on unit circle. □

**Lemma 30.** *Suppose $\langle u_n\rangle_{n=0}^{\infty}$ is non-degenerate and is given by (3.12). Suppose that $\alpha, \beta, \gamma, \delta$ do not all have the same magnitude. There exists a bound $N = 2^{\mathcal{O}(||I||)}$ such that if $u_n = 0$, then $n < N$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|D\| + \|\alpha\| + \|\beta\| + \|\gamma\| + \|\delta\|$.*

*Proof.* We wish to solve for $n \in \mathbb{N}$ the equation:

$$A\alpha^n + B\beta^n + C\gamma^n + D\delta^n = 0 \text{ (where } A, B, C, D \neq 0). \tag{3.21}$$

Let $|\alpha| \geq |\beta| \geq |\gamma| \geq |\delta|$. First, if $|\alpha| > |\beta|$, then $A\alpha^n$ is the dominant term in (3.21). Rewrite the equation as

$$\frac{B}{A}\left(\frac{\beta}{\alpha}\right)^n + \frac{C}{A}\left(\frac{\gamma}{\alpha}\right)^n + \frac{D}{A}\left(\frac{\delta}{\alpha}\right)^n = -1$$

and observe that if

$$n > \max\left\{\frac{\log|3B/A|}{\log|\alpha/\beta|}, \frac{\log|3C/A|}{\log|\alpha/\gamma|}, \frac{\log|3D/A|}{\log|\alpha/\delta|}\right\},$$

then

$$\left|\frac{B}{A}\left(\frac{\beta}{\alpha}\right)^n + \frac{C}{A}\left(\frac{\gamma}{\alpha}\right)^n + \frac{D}{A}\left(\frac{\delta}{\alpha}\right)^n\right| < \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1.$$

Second, if $|\alpha| = |\beta| > |\gamma|$, then rewrite (3.21) as

$$\left(\frac{\beta}{\alpha}\right)^n = -\frac{A}{B} - \frac{C}{B}\left(\frac{\gamma}{\alpha}\right)^n - \frac{D}{B}\left(\frac{\delta}{\alpha}\right)^n. \tag{3.22}$$

The left-hand side of (3.22) is on the unit circle, whereas the right is a constant plus exponentially decaying terms. An exponential bound on $n$ follows from Lemma 22.

Finally, if $|\alpha| = |\beta| = |\gamma| > |\delta|$, then an exponential bound on $n$ follows from Lemma 23 applied to equation (3.22). □

Thus, the only outstanding problem is to solve $u_n = 0$ in the case of $\langle u_n \rangle_{n=0}^{\infty}$ given by (3.12) when $|\alpha| = |\beta| = |\gamma| = |\delta|$. This case is difficult for general algebraic $\alpha, \beta, \gamma, \delta$: it is in fact the reason why the Discrete Skolem Problem is open for LRS of order 4 over $\mathbb{A}$. However, for real LRS, the set of characteristic roots is closed under complex conjugation, so complex roots come in conjugate pairs.

Another simplifying observation necessary for this last outstanding case is that for any LRS $\langle u_n \rangle_{n=0}^{\infty}$ over $\mathbb{A}$, one can find another LRS $\langle v_n \rangle_{n=0}^{\infty}$ over $\mathcal{O}_{\mathbb{A}}$ such that $u_n = 0$ if and only if $v_n = 0$. Indeed, recall that for any algebraic number $\alpha$, it is possible to find an algebraic integer $\beta$ and a rational integer $M$ such that $\alpha = \beta/M$: it is sufficient to choose $M$ to be the least common multiple of all denominators of the coefficients of the minimal polynomial of $\alpha$. Then suppose the sequence $\langle u_n \rangle_{n=0}^{\infty}$ has initial terms $u_0, \ldots, u_{d-1} \in \mathbb{A}$ and satisfies a recurrence equation $u_n = \sum_{j=0}^{d-1} a_j u_{n-j-1}$ with $a_0, \ldots, a_{d-1} \in \mathbb{A}$. Let $M \in \mathbb{Z}$ be chosen so that $Ma_j \in \mathcal{O}_{\mathbb{A}}$ and $Mu_j \in \mathcal{O}_{\mathbb{A}}$ for $j = 0, \ldots, d-1$. Then it is easy to see that the sequence $\langle v_n \rangle_{n=0}^{\infty}$ defined by $v_n = M^{n+1} u_n$ has the same zero set as $\langle u_n \rangle_{n=0}^{\infty}$, has algebraic integer initial terms and satisfies a linear recurrence relation of order $d$ with algebraic integer coefficients. Since $M$ can be written down using only polynomial space, this reduction to the integer case can be carried out in polynomial time. Therefore, by the integral closure of $\mathcal{O}_{\mathbb{A}}$, we can assume the characteristic roots $\alpha, \beta, \gamma, \delta$ are algebraic integers.

With these two observations in place, we proceed to the final technical result concerning the Discrete Skolem Problem for LRS of order 4 over $\mathbb{R} \cap \mathbb{A}$:

**Lemma 31.** *Suppose $\langle u_n \rangle_{n=0}^{\infty}$ is non-degenerate and is given by (3.12). Suppose that $\alpha, \beta, \gamma, \delta$ are algebraic integers with $|\alpha| = |\beta| = |\gamma| = |\delta|$. Suppose also $\{\alpha, \beta, \gamma, \delta\}$ is closed under complex conjugation. There exists a bound $N = 2^{\mathcal{O}(||I||)}$ such that if $u_n = 0$, then $n < N$, where $\|I\|$ is the length of the input $\|A\| + \|B\| + \|C\| + \|D\| + \|\alpha\| + \|\beta\| + \|\gamma\| + \|\delta\|$.*

*Proof.* Let $\mathbb{K} = \mathbb{Q}(\alpha, \beta, \gamma, \delta, A, B, C, D)$. We have to solve for $n \in \mathbb{N}$ the equation:

$$A\alpha^n + B\beta^n + C\gamma^n + D\delta^n = 0 \text{ (where } A, B, C, D \neq 0). \tag{3.23}$$

The closure of $\{\alpha, \beta, \gamma, \delta\}$ under complex conjugation, the equality $|\alpha| = |\beta| = |\gamma| = |\delta|$ and the non-degeneracy of the LRS imply that the characteristic roots are two pairs of complex conjugates, so assume without loss of generality that $\beta = \overline{\alpha}$ and $\gamma = \overline{\delta}$. If $\alpha/\beta$ is an algebraic integer, then since it is not a root of unity, there exists a monomorphism $\sigma$ from $\mathbb{K}$ to $\mathbb{C}$ such that $|\sigma(\alpha)| \neq |\sigma(\beta)|$. Applying $\sigma$ to (3.23) leads to a Skolem instance of order 4 with roots whose magnitudes are not all the same. A bound on $n$ follows from Lemma 30.

Suppose then that $\alpha/\beta$ is not an algebraic integer. By the reasoning of Lemma 2, there exists a prime ideal $P$ in $\mathcal{O}_{\mathbb{K}}$ such that $v_P(\alpha) \neq v_P(\beta)$ and at least one of $v_P(\alpha)$ and $v_P(\beta)$ is strictly positive. Assume without loss of generality that

$$v_P(\alpha) > v_P(\beta) \geq 0.$$

Since $\alpha\beta = \gamma\delta = |\alpha|^2$, we have

$$v_P(\alpha) + v_P(\beta) = v_P(\gamma) + v_P(\delta).$$

Therefore, at most two of the roots are smallest under the valuation $v_P$.

If one root, say $\beta$, is strictly smaller under $v_P$ than the rest, then rewrite (3.23) as

$$A\alpha^n + B\beta^n = -C\gamma^n - D\delta^n \tag{3.24}$$

Since $v_P(\beta) < v_P(\alpha)$, for $n > v_P(A/B)/v_P(\beta/\alpha)$ we have

$$v_P(A\alpha^n + B\beta^n) = v_P(B) + nv_P(\beta),$$

whereas

$$v_P(-C\gamma^n - D\delta^n) \geq v_P(C) + nv_P(\gamma).$$

Therefore, for $n > v_P(B/C)/v_P(\gamma/\beta)$, we have that the left-hand side of (3.24) is strictly smaller under $v_P$ than the right-hand side, so (3.23) cannot hold. This bound on $n$ is polynomial in the input size.

Now suppose that there are two roots with strictly smallest valuation with respect to $v_P$:

$$0 \leq v_P(\beta) = v_P(\gamma) < v_P(\alpha) = v_P(\delta).$$

Then rewrite (3.23) as

$$B\beta^n \left( \left( -\frac{C}{B} \right) \left( \frac{\gamma}{\beta} \right)^n - 1 \right) = A\alpha^n + D\delta^n. \tag{3.25}$$

Since $\gamma/\beta$ is not a root of unity, the term $(-C/B)(\gamma/\beta)^n - 1$ can be zero for at most one value of $n$. This value is at most polynomially large in the input size (by Lemma 21). For all other $n$, we use Theorem 8 to this term. Let $p$ be the unique prime rational integer in the ideal $P$, and let $d = [\mathbb{K} : \mathbb{Q}]$. Let $H$ be an upper bound for the heights of $-C/B$ and $\gamma/\beta$. Then by Theorem 8 (van der Poorten), we have

$$v_P \left( \left( -\frac{C}{B} \right) \left( \frac{\gamma}{\beta} \right)^n - 1 \right) \leq (48d)^{36} \frac{p^d}{\log p} (\log H)^2 (\log n)^2. \tag{3.26}$$

It is classical that $\mathcal{N}(P) = p^f$ for some positive integer $f$, so $\mathcal{N}(P) \geq p$. Moreover, since $\alpha$ is an algebraic integer, all prime ideals $P_1, \ldots, P_s$ in the factorisation of $[\alpha]$ appear with positive exponents $k_1, \ldots, k_s$:

$$[\alpha] = P_1^{k_1} \ldots P_s^{k_s}.$$

Since $\mathcal{N}(P_i) \geq 2$ for all $P_i$, we have

$$|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)| = \mathcal{N}([\alpha]) \geq \mathcal{N}(P) \geq p.$$

Therefore, $p$ is at most exponentially large in the input size. Then we can write (3.26) as

$$v_P \left( \left( -\frac{C}{B} \right) \left( \frac{\gamma}{\beta} \right)^n - 1 \right) \leq E_1 (\log n)^2,$$

where $E_1$ is exponentially large in the input size and independent of $n$. Now we apply $v_P$ to both sides of equation (3.25):

$$v_P(LHS) \leq v_P(B) + nv_P(\beta) + E_1(\log n)^2$$

and

$$v_P(RHS) \geq v_P(A) + nv_P(\alpha).$$

Equation (3.23) cannot hold if

$$v_P(B) + nv_P(\beta) + E_1(\log n)^2 < v_P(A) + nv_P(\alpha),$$

which is implied by

$$v_P(B/A) + E_1(\log n)^2 < n,$$

since $v_P(\alpha) > v_P(\beta)$. Let $E_2 = \max\{v_P(B/A), E_1\}$, then this is implied by

$$E_2((\log n)^2 + 1) < n.$$

Since

$$(\log n)^2 + 1 < \frac{5\sqrt{n}}{2}$$

for all $n \geq 1$, it suffices to have

$$n > \left( \frac{5}{2} E_2 \right)^2.$$

This bound on $n$ is exponential in the size of the input. □

# Chapter 4

# Discrete Orbit Problem

*Prerequisites:*
Sections 2.1.1, 2.3.1 and 3.2.
Theorem 19 and its constituent Lemmas 21, 24-31. (Statements sufficient, proofs not requisite.)

## 4.1 Introduction

The *Discrete Orbit Problem* was introduced by Harrison in [Harrison, 1969] as a formulation of the reachability problem for linear sequential machines. The problem is stated as follows:

> Given a square matrix $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$ and vectors $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Q}^m$, decide whether there exists a non-negative integer $n$ such that $\boldsymbol{A}^n\boldsymbol{x} = \boldsymbol{y}$.

The decidability of this problem remained open for over ten years, until it was shown to be decidable in polynomial time by Kannan and Lipton [Kannan and Lipton, 1980]. In the conclusion of the journal version of their work [Kannan and Lipton, 1986], the authors discuss a higher-dimensional extension of the Orbit Problem, as follows:

> Given a square matrix $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, a vector $\boldsymbol{x} \in \mathbb{Q}^m$, and a subspace $\mathcal{V}$ of $\mathbb{Q}^m$, decide whether there exists a non-negative integer $n$ such that $\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V}$.

As Kannan and Lipton point out, the higher-dimensional Orbit Problem is closely related to the Discrete Skolem Problem. Indeed, the Skolem Problem is the special case in which the target space $\mathcal{V}$ has dimension $m-1$.

Kannan and Lipton speculated in [Kannan and Lipton, 1986] that for target spaces of dimension one the higher-dimensional Orbit Problem might be solvable, "hopefully with a polynomial-time bound". They moreover observed that the cases in which the target space $\mathcal{V}$ has dimension two or three seem "harder", and proposed this line of research as an approach towards the Skolem Problem. In spite of this, to the best of our knowledge, no progress has been recorded on the higher-order Orbit Problem in the intervening two-and-a-half decades.

In this chapter, we show that the higher-order Orbit Problem is in **PTIME** if the target space has dimension one and in $\mathbf{NP}^{\mathbf{RP}}$ if the target space has dimension two or three, thereby confirming Kannan and Lipton's hypothesis. While we make extensive use of the techniques of Chapter 3 and of [Mignotte et al., 1984, Vereshchagin, 1985] on the Discrete Skolem Problem, the results in this chapter, in contrast, are independent of the dimension $m$ of the ambient space.

The following example illustrates some of the phenomena that emerge in the Orbit Problem for two-dimensional target spaces. Consider the following matrix and initial vector:

$$\boldsymbol{A} = \begin{bmatrix} 4 & 6 & 14 & 21 \\ -8 & -2 & -28 & -7 \\ -2 & -3 & -6 & -9 \\ 4 & 1 & 12 & 3 \end{bmatrix} \quad \boldsymbol{x} = \begin{bmatrix} 28 \\ -14 \\ -10 \\ 5 \end{bmatrix}$$

Then with target space

$$\mathcal{V} = \{(u_1, u_2, u_3, u_4) \in \mathbb{Q}^4 : 4u_1 + 7u_3 = 0, 4u_2 + 7u_4 = 0\}$$

it can be shown that $\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V}$ if and only if $n$ has residue 2 modulo 6. Such periodic behaviour can be analysed in terms of the eigenvalues of the matrix $\boldsymbol{A}$. These are $\lambda\omega$, $\overline{\lambda}\omega$, $\lambda\overline{\omega}$ and $\overline{\lambda\omega}$, where $\omega = e^{\pi i/3}$ is a primitive 6-th root of unity and $\lambda = (-1 + i\sqrt{39})/2$. The key observation is that the eigenvalues of $\boldsymbol{A}$ fall into only two classes under the equivalence relation $\sim$, defined by $\alpha \sim \beta$ if and only if $\alpha/\beta$ is a root of unity. We handle such instances by analysing the equivalence classes this relation. We show that, provided $\sim$ has sufficiently many equivalence classes, there is at most one exponent $n$ such that $\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V}$. On the other hand, for instances where $\sim$ has too few equivalence classes, allowing the exponents $n$ to exhibit periodic behaviour as above, we show that if there exists a witness $n$ to $\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V}$, then a 'small' witness may be found.

## 4.2 Main result and outline

This chapter is based on our publications [Chonev et al., 2013] and [Chonev et al., 2016]. The main technical results are the following theorems:

**Theorem 32.** *Suppose we are given an instance of the Orbit Problem, comprising a square matrix $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, a vector $\boldsymbol{x} \in \mathbb{Q}^m$ and a subspace $\mathcal{V} \subseteq \mathbb{Q}^m$ with $\dim(\mathcal{V}) \leq 3$. Let $\|I\|$ be the length of the description of the input data. There exists a bound $N = 2^{\mathcal{O}(\|I\|)}$ such that if the instance is positive, then there exists a witness (that is, $n \in \mathbb{N}$ with $\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V}$) such that $n < N$.*

**Theorem 33.** *The Orbit Problem with $\dim(\mathcal{V}) \leq 3$ is in $\mathbf{NP}^{\mathbf{RP}}$. Further, if $\dim(\mathcal{V}) = 1$, then the problem is in* **PTIME**.

In this section we give a high-level overview of the argument. Afterwards, Sections 4.3, 4.4, 4.5 and 4.6 provide the details of the proof.

The first step of the argument is a reduction to a similar problem, a polynomial version of the *matrix power problem:* given a rational square matrix $\boldsymbol{A}$ and polynomials $P_1, \ldots, P_d \in \mathbb{Q}[x]$ such that $P_1(\boldsymbol{A}), \ldots, P_d(\boldsymbol{A})$ are linearly independent over $\mathbb{Q}$, determine whether there exists $n$ such that $\boldsymbol{A}^n$ lies in the $\mathbb{Q}$-vector space $span\{P_1(\boldsymbol{A}), \ldots, P_d(\boldsymbol{A})\}$. The reduction does not increase the dimension of the target space, so we will always have $d \leq 3$. The reduction can be carried out in polynomial time and rests entirely on standard techniques from linear algebra.

For the second step, we construct a *Master System.* This is a system of equations, based on the eigenvalues of $\boldsymbol{A}$ and the polynomials $P_1, \ldots, P_d$. It has $d + 1$ unknowns: the exponent $n$ and the coefficients $\kappa_1, \ldots, \kappa_d$ which witness the membership of $\boldsymbol{A}^n$ in $span\{P_1(\boldsymbol{A}), \ldots, P_d(\boldsymbol{A})\}$. The solutions $(n, \kappa_1, \ldots, \kappa_d)$ of the Master System will be exactly the solutions of the matrix equation $\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A}) + \cdots + \kappa_d P_d(\boldsymbol{A})$. The domain of $n$ is $\mathbb{N}$ throughout. Since the input data is rational, any solution $(n, \kappa_1, \ldots, \kappa_d)$ of the Master System will necessarily have $\kappa_1, \ldots, \kappa_d \in \mathbb{Q}$.

Next, in Section 4.4, we give a polynomial-time decision procedure to determine whether the Master System for an instance with a one-dimensional target space has a solution. The algorithm explicitly manipulates the equations in the system, preserving the set of solutions at every step, to determine the existence of a solution in polynomial time, settling the one-dimensional case of Theorem 33. The section rests critically on Theorem 19 for non-degenerate linear recurrence sequences of order 2, which allows us to bound the exponent in all cases when $\boldsymbol{A}$ has two eigenvalues whose ratio is not a root of unity. In all other situations, the given Orbit instance essentially reduces to a system of linear congruences, easily solved using the Chinese Remainder Theorem. The solution method yields the full set of witness exponents $n$ when this set is finite, or a description of the witness set as an arithmetic progression when it is infinite. Thus, if the problem instance is positive, a witness exponent which is at most exponentially large is automatically guaranteed to exist, as promised by Theorem 32, by virtue of our ability to write it down using polynomially many bits.

As in Chapter 3, the notion of degeneracy arises here as well. An instance $(\boldsymbol{A}, \boldsymbol{x}, \mathcal{V})$ of the Orbit Problem is defined as *degenerate* if there exist two distinct eigenvalues of $\boldsymbol{A}$ whose quotient is a root of unity, otherwise the instance is *non-degenerate.* In general, it is possible to reduce an arbitrary Orbit

Problem instance to a set of non-degenerate instances, using a technique similar to that of Sections 2.3.1 and 3.2 for partitioning a linear recurrence sequence into non-degenerate subsequences. Let $L$ be the least common multiple of the orders of all quotients of eigenvalues of $\boldsymbol{A}$ which are roots of unity. For each $j \in \{0, \ldots, L-1\}$, consider separately the problem of deciding whether there exists $n \in \mathbb{N}$ such that $(\boldsymbol{A}^L)^n \left(\boldsymbol{A}^j \boldsymbol{x}\right) \in \mathcal{V}$. These instances are all non-degenerate,[1] and the original problem instance is positive if and only if at least one of these $L$ non-degenerate instances is positive.

However, it is important to recognise that in the present chapter, non-degeneracy may not be assumed freely, as it was in Chapter 3 for the Discrete Skolem Problem. Indeed, the Skolem Problem is the special case in which the dimension of the ambient space exceeds the dimension of the target space by exactly 1. Bounding one bounds the other, resulting in $L$ being absolutely bounded by a constant. In this chapter, however, whilst the target space is at most three-dimensional, the dimension of the ambient space remains unconstrained, and $L$ remains exponentially large in the size of the input.

We adopt the following strategy for solving the Orbit Problem for possibly degenerate instances. Assume that as part of the input, we are given the residue $r = n \bmod L$. Thus, we are interested in determining whether the Master System has a solution $(n, \kappa_1, \ldots, \kappa_d)$ with exponent $n$ such that $r = n \bmod L$. We will prove that for any $r$, there exists a bound $N_r$ such that if there exists such an exponent with residue $r$, then one exists which does not exceed the bound $N_r$. Furthermore, $N_r = 2^{\mathcal{O}(||I'||)}$, where $\|I'\| = \|I\| + \|r\|$ is the length of the input augmented with the binary representation of $r$. This is clearly sufficient to prove Theorem 32: simply take $N = \max\{N_r : r \in \{0, \ldots, L-1\}\}$. The case analysis on $r$ simplifies the Master System considerably, effectively eliminating degeneracy as a concern, and allowing us to derive the existence of $N_r$ using our results on the Discrete Skolem Problem for LRS of order 3 and 4. For each fixed $r$, algebraic manipulation yields either a 'small' witness $n$ of the correct residue, or a non-degenerate linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ of low order such that if the Master System has a solution with exponent $n$ with the desired residue $r$, then $u_n = 0$. The description of this linear recurrence sequence is computable in polynomial time from the input instance and $r$. Since $\|r\| = ||I||^{\mathcal{O}(1)}$, it follows that $\|u\| = ||I'||^{\mathcal{O}(1)} = ||I||^{\mathcal{O}(1)}$, so by Theorem 19, the desired bound $N_r$ exists and $N_r = 2^{\mathcal{O}(||I||)}$.

We must emphasise that this algebraic manipulation of the Master System and the calculation of the description of $\langle u_n \rangle_{n=0}^{\infty}$ is not part of the decision procedure for the Orbit Problem. Rather, it is a technical device whose sole purpose is to prove the existence of the desired bounds $N_r$, and hence of $N$. We make use of the observation that this manipulation can, in principle, be carried out in polynomial time, so that we can conclude $N_r = 2^{\mathcal{O}(||I'||)}$ and $N = 2^{\mathcal{O}(||I||)}$, and hence establish Theorem 32, but we do not actually carry it out.

Given the bound $N$ of Theorem 32, we employ a *guess-and-check* procedure to obtain the complexity upper bounds of Theorem 33. Since $N$ is at most exponentially large in the size of the input, an **NP** procedure can guess an exponent $n$ such that $n < N$. Then we compute $\boldsymbol{A}^n \boldsymbol{x}$ by iterated squaring, thereby using polynomially many arithmetic operations. Moreover, all integers that occur in this algorithm have a polynomial-sized representation via arithmetic circuits. Now, to verify $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{V}$, we compute the determinant of $\boldsymbol{B}^{\boldsymbol{T}} \boldsymbol{B}$, where $\boldsymbol{B}$ is the matrix whose columns are $\boldsymbol{A}^n \boldsymbol{x}$ and the basis vectors specifying $\mathcal{V}$, also as an arithmetic circuit. Clearly, $n$ is a witness to the problem instance if and only if this determinant is zero. This is easy to determine with an **EqSLP** oracle, so we have membership in $\mathbf{NP}^{\mathbf{EqSLP}}$. It is known that $\mathbf{EqSLP} \subseteq \mathbf{coRP}$ [Schönhage, 1979], so we have membership in $\mathbf{NP}^{\mathbf{RP}}$, thereby establishing Theorem 33.

Finally, we remark that one can accommodate an affine target space at the cost of increasing the dimensions of the target space and the ambient space by 1. Indeed, the existence of an exponent $n \in \mathbb{N}$ and coefficients $\kappa_1, \ldots, \kappa_d \in \mathbb{Q}$ such that

$$\boldsymbol{A}^n \boldsymbol{x} = \boldsymbol{y_0} + \sum_{j=1}^{d} \kappa_j \boldsymbol{y}_j$$

[1] Indeed, the eigenvalues of $\boldsymbol{A}^L$ are exactly $\lambda_i^L$ where $\lambda_i$ are the eigenvalues of $\boldsymbol{A}$. If for any two distinct such eigenvalues, say $\lambda_i^L \neq \lambda_j^L$, we have $\left(\lambda_i^L / \lambda_j^L\right)^t = 1$, then $\lambda_i / \lambda_j$ must also be a root of unity. Then by the definition of $L$, $\lambda_i^L / \lambda_j^L = 1$, which gives the contradiction $\lambda_i^L = \lambda_j^L$.

is equivalent to the existence of $n \in \mathbb{N}$ and $\kappa_0, \ldots, \kappa_d \in \mathbb{Q}$ such that

$$\begin{bmatrix} \boldsymbol{A} & 0 \\ \boldsymbol{0} & 1 \end{bmatrix}^n \begin{bmatrix} \boldsymbol{x} \\ 1 \end{bmatrix} = \kappa_0 \begin{bmatrix} \boldsymbol{y}_0 \\ 1 \end{bmatrix} + \sum_{j=1}^{d} \kappa_j \begin{bmatrix} \boldsymbol{y}_j \\ 0 \end{bmatrix}.$$

Thus, by Theorem 33, we immediately have membership in $\mathbf{NP}^{\mathbf{RP}}$ for the pointwise reachability problem to an affine subspace of dimension 1 or 2.

## 4.3 Reduction

### 4.3.1 Matrix power problem

Suppose we are given a matrix $\boldsymbol{A} \in \mathbb{Q}^{m \times m}$, a vector $\boldsymbol{x} \in \mathbb{Q}^m$ and a target vector space $\mathcal{V} \subseteq \mathbb{Q}^m$ specified by a basis of rational vectors $\boldsymbol{y_1}, \ldots, \boldsymbol{y_k}$. We wish to decide whether there exists $n \in \mathbb{N}$ such that $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{V}$.

Observe that we can rescale $\boldsymbol{A}$ in polynomial time by the least common multiple of all denominators appearing in $\boldsymbol{A}$. This reduces the general problem to the sub-problem in which $\boldsymbol{A}$ is an integer matrix.

Let $\nu = \max\{m \mid \boldsymbol{x}, \boldsymbol{Ax}, \ldots, \boldsymbol{A}^m\boldsymbol{x} \text{ are linearly independent}\}$, $B = \{\boldsymbol{x}, \boldsymbol{Ax}, \ldots, \boldsymbol{A}^\nu\boldsymbol{x}\}$, $\mathcal{U} = \mathit{span}(B)$ and $\boldsymbol{D} = \begin{bmatrix} \boldsymbol{x} & \boldsymbol{Ax} & \ldots & \boldsymbol{A}^\nu\boldsymbol{x} \end{bmatrix}$. It is clear that $\mathcal{U}$ is invariant under the linear transformation $\boldsymbol{A}$, so consider the restriction of $\boldsymbol{A}$ to $\mathcal{U}$. Suppose $\boldsymbol{b} = (b_0, \ldots, b_\nu)^T$ are the coordinates of $\boldsymbol{A}^{\nu+1}\boldsymbol{x}$ with respect to $B$, that is, $\boldsymbol{A}^{\nu+1}\boldsymbol{x} = \boldsymbol{Db}$. The restriction of $\boldsymbol{A}$ to $\mathcal{U}$ with respect to the basis $B$ is described by the matrix

$$\boldsymbol{M} = \begin{bmatrix} 0 & 0 & \ldots & 0 & b_0 \\ 1 & 0 & \ldots & 0 & b_1 \\ 0 & 1 & \ldots & 0 & b_2 \\ 0 & 0 & \ddots & 0 & \vdots \\ 0 & 0 & \ldots & 1 & b_\nu \end{bmatrix}.$$

It is easy to check that $\boldsymbol{DM} = \boldsymbol{AD}$. Thus, if some vector $\boldsymbol{z}$ has coordinates $\boldsymbol{z'}$ with respect to $B$, so that $\boldsymbol{z} = \boldsymbol{Dz'}$, then $\boldsymbol{Az}$ has coordinates $\boldsymbol{Mz'}$ with respect to $B$, so that $\boldsymbol{Az} = \boldsymbol{DMz'}$. By induction, for all $n \in \mathbb{N}$, $\boldsymbol{A}^n\boldsymbol{x} = \boldsymbol{DM}^n\boldsymbol{x'}$, where $\boldsymbol{x'} = (1, 0, \ldots, 0)^T$. Next we calculate a basis for $\mathcal{W} \stackrel{\text{def}}{=} \mathcal{U} \cap \mathcal{V}$, let this basis be $\{\boldsymbol{w_1}, \ldots, \boldsymbol{w_t}\}$ and let $\boldsymbol{w_i} = \boldsymbol{Dw_i'}$ for all $i$. Now,

$$\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{V} \iff \boldsymbol{A}^n\boldsymbol{x} \in \mathcal{W} \iff \boldsymbol{M}^n\boldsymbol{x'} \in \mathit{span}\{\boldsymbol{w_1'}, \ldots, \boldsymbol{w_t'}\}.$$

Notice that the matrix $\boldsymbol{M}$ describes a restriction of the linear transformation denoted by $\boldsymbol{A}$, so its eigenvalues are a subset of the eigenvalues of $\boldsymbol{A}$. In particular, since $\boldsymbol{A}$ was rescaled to an integer matrix, the eigenvalues of $\boldsymbol{M}$ are algebraic integers as well.

Define the matrices $\boldsymbol{T_1}, \ldots, \boldsymbol{T_t}$ by

$$\boldsymbol{T_i} = \begin{bmatrix} \boldsymbol{w_i'} & \boldsymbol{Mw_i'} & \ldots & \boldsymbol{M}^\nu\boldsymbol{w_i'} \end{bmatrix}.$$

We will show that $\boldsymbol{M}^n\boldsymbol{x'} \in \mathit{span}\{\boldsymbol{w_1'}, \ldots, \boldsymbol{w_t'}\}$ if and only if $\boldsymbol{M}^n \in \mathit{span}\{\boldsymbol{T_1}, \ldots, \boldsymbol{T_t}\}$. If for some coefficients $\kappa_i$ we have

$$\boldsymbol{M}^n = \sum_{i=0}^{t} \kappa_i \boldsymbol{T_i},$$

then considering the first column of both sides, we have

$$\boldsymbol{M}^n\boldsymbol{x'} = \sum_{i=0}^{t} \kappa_i \boldsymbol{w_i'}.$$

Conversely, suppose $\boldsymbol{M}^n\boldsymbol{x'} = \sum_{i=0}^{t} \kappa_i \boldsymbol{w_i'}$. Then note that $\boldsymbol{x'}, \boldsymbol{Mx'}, \ldots, \boldsymbol{M}^\nu\boldsymbol{x'}$ are just the unit vectors of size $\nu + 1$. Multiplying by $\boldsymbol{M}^j$ for $j = 0, \ldots, \nu$ gives $\boldsymbol{M}^{n+j}\boldsymbol{x'} = \sum_{i=0}^{t} \kappa_i \boldsymbol{M}^j \boldsymbol{w_i'}$. The left-hand side is exactly the $(j+1)$-th column of $\boldsymbol{M}^n$, whereas $\boldsymbol{M}^j\boldsymbol{w_i'}$ on the right-hand side is exactly the $(j+1)$-th column of $\boldsymbol{T_i}$. So we have $\boldsymbol{M}^n = \sum_{i=0}^{t} \kappa_i \boldsymbol{T_i}$.

Thus, we have reduced the Orbit Problem to the *matrix power problem:* determining whether some power of a given matrix lies inside a given vector space of matrices. Now we will perform a further reduction step. It is clear that within the space $\mathcal{T} \stackrel{\text{def}}{=} span\{\boldsymbol{T_1}, \ldots, \boldsymbol{T_t}\}$ it suffices to consider only matrices of the shape $P(\boldsymbol{M})$ where $P \in \mathbb{Q}[x]$. We find a basis for the space $\mathcal{P} \stackrel{\text{def}}{=} \{P(\boldsymbol{M}) \mid P \in \mathbb{Q}[x]\}$ and then a basis $\{P_1(\boldsymbol{M}), \ldots, P_s(\boldsymbol{M})\}$ for $\mathcal{P} \cap \mathcal{T}$. Then $\boldsymbol{M}^n \in \mathcal{T} \iff \boldsymbol{M}^n \in \mathcal{P} \cap \mathcal{T}$. We call the problem of determining, given $\boldsymbol{M}$ and $P_1, \ldots, P_s$, whether there exists $n \in \mathbb{N}$ such that $\boldsymbol{M}^n \in span\{P_1(\boldsymbol{M}), \ldots, P_s(\boldsymbol{M})\}$, the *polynomial version* of the matrix power problem. Observe that $\dim(\mathcal{V}) \geq \dim(\mathcal{T}) \geq \dim(\mathcal{T} \cap \mathcal{P})$, so the dimension of the target vector space does not grow during the described reductions. All described operations may be performed in polynomial time using standard techniques from linear algebra.

### 4.3.2 Master System of equations

Suppose now we have an instance $(\boldsymbol{A}, P_1, \ldots, P_s)$ of the polynomial version of the matrix power problem. Calculate the minimal polynomial of $\boldsymbol{A}$ and obtain canonical representations of its roots $\alpha_1, \ldots, \alpha_k$, that is, the eigenvalues of $\boldsymbol{A}$. This may be done in polynomial time, see Section 2.1.1. Throughout this chapter, for an eigenvalue $\alpha_i$ we will denote by $mul(\alpha_i)$ the multiplicity of $\alpha_i$ as a root of the minimal polynomial of the matrix.

Fix an exponent $n \in \mathbb{N}$ and coefficients $\kappa_1, \ldots, \kappa_s \in \mathbb{C}$ and define the polynomials $P(x) = \sum_{i=1}^{s} \kappa_i P_i(x)$ and $Q(x) = x^n$. It is easy to see that

$$Q(\boldsymbol{A}) = P(\boldsymbol{A})$$

if and only if

$$\forall i \in \{1, \ldots, k\}. \forall j \in \{0, \ldots, mul(\alpha_i) - 1\}. P^{(j)}(\alpha_i) = Q^{(j)}(\alpha_i). \tag{4.1}$$

Indeed, $P - Q$ is zero at $\boldsymbol{A}$ if and only if the minimal polynomial of $\boldsymbol{A}$ divides $P - Q$, that is, each $\alpha_i$ is a root of $P - Q$ with multiplicity at least $mul(\alpha_i)$, or equivalently, each $\alpha_i$ is a root of $P - Q$ and its first $mul(\alpha_i) - 1$ derivatives.

Thus, in order to decide whether there exists an exponent $n$ and coefficients $\kappa_i$ such that $\boldsymbol{A}^n = \sum_{i=1}^{s} \kappa_i P_i(\boldsymbol{A})$, it is sufficient to solve the system of equations (4.1) where the unknowns are $n \in \mathbb{N}$ and $\kappa_1, \ldots, \kappa_s \in \mathbb{C}$. Each eigenvalue $\alpha_i$ contributes $mul(\alpha_i)$ equations which specify that $P(x)$ and its first $mul(\alpha_i) - 1$ derivatives all vanish at $\alpha_i$.

For brevity in what follows, we will denote by $eq(\alpha_i, j)$ the $j$-th derivative equation contributed to the system by $\alpha_i$, that is, $P^{(j)}(\alpha_i) = Q^{(j)}(\alpha_i)$. This notation is defined only for $0 \leq j < mul(\alpha_i)$. We will also denote by $Eq(\alpha_i)$ the set of equations contributed by $\alpha_i$ to the system:

$$Eq(\alpha_i) = \{eq(\alpha_i, 0), \ldots, eq(\alpha_i, mul(\alpha_i) - 1)\}.$$

For example, if the minimal polynomial of $\boldsymbol{A}$ has roots $\alpha_1$, $\alpha_2$, $\alpha_3$ with multiplicities $mul(\alpha_i) = i$ and the target space is $span\{P_1(\boldsymbol{A}), P_2(\boldsymbol{A})\}$ then the system contains six equations:

$$\begin{aligned}
\alpha_1^n &= \kappa_1 P_1(\alpha_1) + \kappa_2 P_2(\alpha_1) \\
\alpha_2^n &= \kappa_1 P_1(\alpha_2) + \kappa_2 P_2(\alpha_2) \\
n\alpha_2^{n-1} &= \kappa_1 P_1'(\alpha_2) + \kappa_2 P_2'(\alpha_2) \\
\alpha_3^n &= \kappa_1 P_1(\alpha_3) + \kappa_2 P_2(\alpha_3) \\
n\alpha_3^{n-1} &= \kappa_1 P_1'(\alpha_3) + \kappa_2 P_2'(\alpha_3) \\
n(n-1)\alpha_3^{n-2} &= \kappa_1 P_1''(\alpha_3) + \kappa_2 P_2''(\alpha_3)
\end{aligned}$$

Then $eq(\alpha_3, 0)$ is the equation

$$\alpha_3^n = \kappa_1 P_1(\alpha_3) + \kappa_2 P_2(\alpha_3)$$

and $Eq(\alpha_2)$ is the two equations

$$\begin{aligned}
\alpha_2^n &= \kappa_1 P_1(\alpha_2) + \kappa_2 P_2(\alpha_2) \\
n\alpha_2^{n-1} &= \kappa_1 P_1'(\alpha_2) + \kappa_2 P_2'(\alpha_2)
\end{aligned}$$

## 4.4 One-dimensional target space

Suppose we are given a one-dimensional matrix power problem instance $(\boldsymbol{A}, P)$ and wish to decide whether $\boldsymbol{A}^n \in \mathit{span}\{P(\boldsymbol{A})\}$ for some $n$. We have constructed a system of equations in the exponent $n$ and the coefficient $\kappa$ as in (4.1). For example, if the roots of the minimal polynomial of $\boldsymbol{A}$ are $\alpha_1, \alpha_2, \alpha_3$ with multiplicities $\mathit{mul}(\alpha_j) = j$, the system is:

$$\begin{aligned}
\alpha_1^n &= \kappa P(\alpha_1) \\
\alpha_2^n &= \kappa P(\alpha_2) \\
n\alpha_2^{n-1} &= \kappa P'(\alpha_2) \\
\alpha_3^n &= \kappa P(\alpha_3) \\
n\alpha_3^{n-1} &= \kappa P'(\alpha_3) \\
n(n-1)\alpha_3^{n-2} &= \kappa P''(\alpha_3)
\end{aligned}$$

In this section we will describe how such systems may be solved in polynomial time. First, we perform some preliminary calculations.

1. We check whether $\kappa = 0$ has a corresponding $n$ which solves the matrix equation $\boldsymbol{A}^n = \kappa P(\boldsymbol{A})$, that is, whether $\boldsymbol{A}$ is nilpotent. Otherwise, assume $\kappa \neq 0$.
2. Let $k = \max_j\{\mathit{mul}(\alpha_j)\}$. We check for all $n < k$ whether $\boldsymbol{A}^n$ is a multiple of $P(\boldsymbol{A})$. If so, we are done. Otherwise, assume $n \geq k$.
3. We check whether $\alpha_j = 0$ for some $j$. If so, then all of the equations $Eq(\alpha_i)$ are of the form $0 = \kappa P^{(t)}(0)$, which is equivalent to $0 = P^{(t)}(0)$. We can easily check whether these equations are satisfied. If so, we dismiss them from the system without changing the set of solutions. If not, then there is no solution and we are done. Now we assume $\alpha_j \neq 0$ for all $j$.
4. Finally, we check whether the right-hand side $\kappa P^{(t)}(\alpha_j)$ of some equation is equal to 0, by dividing $P^{(t)}(x)$ by the minimal polynomial of $\alpha_j$. If this is the case, then the problem instance is negative, because the left-hand sides are all non-zero.

Let $\mathit{eq}(\alpha_i, k)/\mathit{eq}(\alpha_j, t)$ denote the equation obtained from $\mathit{eq}(\alpha_i, k)$ and $\mathit{eq}(\alpha_j, t)$ by asserting that the ratio of the left-hand sides equals the ratio of the right-hand sides, that is,

$$\frac{n(n-1)\dots(n-k+1)\alpha_i^{n-k}}{n(n-1)\dots(n-t+1)\alpha_j^{n-t}} = \frac{P^{(k)}(\alpha_i)}{P^{(t)}(\alpha_j)}.$$

We compute representations of all quotients $\alpha_i/\alpha_j$, and consider three cases.

*Case I.* Some quotient $\alpha_i/\alpha_j$ is not a root of unity. Then $\mathit{eq}(\alpha_i, 0)$ and $\mathit{eq}(\alpha_j, 0)$ together imply $\mathit{eq}(\alpha_i, 0)/\mathit{eq}(\alpha_j, 0)$, that is,

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{P(\alpha_i)}{P(\alpha_j)}.$$

In Section 2.1.1, we discuss the efficient representation and manipulation of algebraic numbers. By Lemma 1, we can compute representations of $P(\alpha_i)/P(\alpha_j)$ and $\alpha_i/\alpha_j$ in polynomial time. Then by Lemma 21 in Section 3.3, $n$ is bounded by a polynomial in the input. We check $\boldsymbol{A}^n \in \mathit{span}\{P(\boldsymbol{A})\}$ for all $n$ up to the bound and we are done.

*Case II.* All quotients $\alpha_i/\alpha_j$ are roots of unity, and all roots of the minimal polynomial of $\boldsymbol{A}$ are simple. Then the system is equivalent to

$$\kappa = \frac{\alpha_1^n}{P(\alpha_1)} \wedge \bigwedge_{i<j} \frac{\mathit{eq}(\alpha_i, 0)}{\mathit{eq}(\alpha_j, 0)}.$$

It is sufficient to determine whether there exists some $n$ which satisfies

$$\bigwedge_{i<j} \frac{\mathit{eq}(\alpha_i, 0)}{\mathit{eq}(\alpha_j, 0)}. \tag{4.2}$$

Consider each equation $eq(\alpha_i, 0)/eq(\alpha_j, 0)$:

$$\left(\frac{\alpha_i}{\alpha_j}\right)^n = \frac{P(\alpha_i)}{P(\alpha_j)}. \tag{4.3}$$

Suppose $\alpha_i/\alpha_j$ is an $r$-th root of unity. If the right-hand side of (4.3) is also an $r$-th root of unity, then the solutions of (4.3) are $n \equiv t \bmod r$ for some $t$. If not, then (4.3) has no solution, so the entire system (4.1) has no solution, and the problem instance is negative. By Lemma 1, we can determine in polynomial time whether the right-hand side of (4.3) is a root of unity, and if so, calculate $t$. We transform each equation in (4.2) into an equivalent congruence in $n$. This gives a system of congruences in $n$ which is equivalent to (4.2). We solve it using the Chinese Remainder Theorem. The problem instance is positive if and only if the system of congruences has a solution.

*Case III.* All quotients $\alpha_i/\alpha_j$ are roots of unity, and $f_A(x)$ has repeated roots. We transform the system into an equivalent one in the following way. First, we include in the new system all the quotients of equations $eq(\alpha_i, 0)$ as in Case 2. Second, for each repeated root $\alpha_i$ of $f_A(x)$, we take the quotients $\bigwedge_{j=0}^{mul(\alpha_i)-2} eq(\alpha_i, j)/eq(\alpha_i, j+1)$. Third, we include the equation $\kappa = \alpha_1/P(\alpha_1)$.

$$\bigwedge_{i<j} \frac{eq(\alpha_i, 0)}{eq(\alpha_j, 0)} \wedge \bigwedge_i \bigwedge_{j=0}^{mul(\alpha_i)-2} \frac{eq(\alpha_i, j)}{eq(\alpha_i, j+1)} \wedge \kappa = \frac{\alpha_1}{P(\alpha_1)}.$$

We solve the first conjunct as in Case 2. If there is no solution, then we are done. Otherwise, the solution is some congruence $n \equiv t_1 \bmod t_2$. For the remainder of the system, each ratio $eq(\alpha_i, j)/eq(\alpha_i, j+1)$ contributed by a repeated root $\alpha_i$ has the shape

$$\frac{\alpha_i}{n-j} = \frac{P^{(j)}(\alpha_i)}{P^{(j+1)}(\alpha_i)},$$

which is equivalent to

$$n = j + \frac{P^{(j+1)}(\alpha_i)}{P^{(j)}(\alpha_i)}\alpha_i. \tag{4.4}$$

For each such equation (4.4), we calculate the right-hand side in polynomial time, using the methods outlined in Section 2.1.1, and check whether it is in $\mathbb{N}$. If not, then the system has no solution. Otherwise, (4.4) points to a single candidate $n_0$. We do this for all equations where $n$ appears outside the exponent. If they point to the same value of $n$, then the system is equivalent to

$$\begin{aligned} n &\equiv t_1 \bmod t_2 \\ n &= n_0 \\ \kappa &= \alpha_1^n/P(\alpha_1) \end{aligned}$$

We check whether $n_0$ satisfies the congruence and we are done.

## 4.5 Two-dimensional target space

Suppose we are given a rational square matrix $\boldsymbol{A}$ and polynomials $P_1, P_2$ with rational coefficients such that $P_1(\boldsymbol{A})$ and $P_2(\boldsymbol{A})$ are linearly independent over $\mathbb{Q}$. We want to decide whether there exists $n \in \mathbb{N}$ such that $\boldsymbol{A}^n$ lies in the $\mathbb{Q}$-vector space $span\{P_1(\boldsymbol{A}), P_2(\boldsymbol{A})\}$. We have derived a Master System of equations (4.1) in the unknowns $(n, \kappa_1, \kappa_2)$ whose solutions are precisely the solutions of the matrix equation $\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A}) + \kappa_2 P_2(\boldsymbol{A})$.

In this section, we will show that there exists a bound $N$, exponentially large in the size of the input, such that if the problem instance is positive, then there exists a witness exponent $n$ with $n < N$. This will be sufficient to show that the problem is in the complexity class $\mathbf{NP^{RP}}$, as outlined earlier.

Notice that we may freely assume that the eigenvalues of $\boldsymbol{A}$ are non-zero. Indeed, if 0 is an eigenvalue, then consider $eq(0, 0)$:

$$0 = \kappa_1 P_1(0) + \kappa_2 P_2(0).$$

If at least one of $P_1(0)$, $P_2(0)$ is non-zero, then we have a linear dependence between $\kappa_1, \kappa_2$. Then we express one of the coefficients $\kappa_1, \kappa_2$ in terms of the other, obtaining a Master System of dimension 1, and then the claim follows inductively. Otherwise, if $P_1(0) = P_2(0) = 0$, then $eq(0,0)$ is trivially satisfied for all $n, \kappa_1, \kappa_2$, so we remove $eq(0,0)$ from the Master System without altering the set of solutions. We examine in this way all equations contributed by 0, either removing them from the system, or obtaining a lower-dimensional system which then yields the required bound $N$ inductively.

As outlined in Section 4.2, we show the existence of the bound $N$ by performing a case analysis on $n \bmod L$, where

$$L = \text{lcm}\{\text{order}(\lambda_i/\lambda_j) : \lambda_i, \lambda_j \text{ eigenvalues of } \boldsymbol{A} \text{ and } \lambda_i/\lambda_j \text{ root of unity}\}.$$

We will show that for any fixed value $r \in \{0, \ldots, L-1\}$, there exists a bound $N_r$, exponentially large in the size of the input, such that if the Master System has a solution with exponent of residue $r$ modulo $L$, then it has a solution with exponent $n$ such that $n < N_r$. To obtain the bounds $N_r$, we show how the Master System can be manipulated algebraically in polynomial time to yield a non-degenerate linear recurrence sequence of order 3 whose zeros are a superset of the exponents $n$ which solve the Master System. This manipulation is a proof technique to show the existence of the bound $N_r$, not a feature of the algorithm. The decision method is instead the guess-and-check procedure explained in Section 4.2.

Thus, from here onwards, we assume we are given a fixed $r$, which increases the input size only polynomially, and are interested solely in exponents $n$ with $n \bmod L = r$. Since we admit degenerate problem instances, we need to consider the relation $\sim$ on the eigenvalues of $\boldsymbol{A}$, defined by

$$\alpha \sim \beta \text{ if and only if } \alpha/\beta \text{ is a root of unity.}$$

It is clear that $\sim$ is an equivalence relation. The equivalence classes $C_1, \ldots, C_k$ of $\sim$ are of two kinds. First, a class can be its own image under complex conjugation:

$$C_i = \{\overline{\alpha} \mid \alpha \in C_i\}$$

Each such self-conjugate class $\{\alpha_1, \ldots, \alpha_s\}$ has the form $\{\alpha\omega_1, \ldots, \alpha\omega_s\}$ where $\omega_i$ are roots of unity, and $|\alpha_j| = \alpha \in \mathbb{R} \cap \mathbb{A}$. Call this $\alpha$ the *representative* of the equivalence class $C_i$. Second, if an equivalence class is not self-conjugate, then its image under complex conjugation must be another equivalence class of $\sim$. Thus, the remaining equivalence classes of $\sim$ are grouped into pairs $(C_i, C_j)$ such that $C_i = \{\overline{x} \mid x \in C_j\} = \overline{C_j}$. In this case, we can write $C_i$ and $C_j$ as

$$C_i = \{\lambda\omega_1, \ldots, \lambda\omega_s\}$$

$$C_j = \{\overline{\lambda\omega_1}, \ldots, \overline{\lambda\omega_s}\}$$

where $\omega_i$ are roots of unity, $\lambda \in \mathbb{A}$ and $\arg(\lambda)$ is an irrational multiple of $2\pi$. Call $\lambda$ the representative of $C_i$ and $\overline{\lambda}$ the representative of $C_j$.

Observe that the representatives of self-conjugate classes are distinct positive real numbers, and that no ratio of representatives can be a root of unity. Recall also that we can assume the eigenvalues of $\boldsymbol{A}$ are algebraic integers, as a by-product of the reduction from the Orbit Problem. Since roots of unity and their multiplicative inverses are algebraic integers, it follows that the representatives of equivalence classes must also be algebraic integers.

Let

$$Eq(C) = \bigcup_{\alpha \in C} Eq(\alpha)$$

denote the set of equations contributed to the system by the eigenvalues in $C$, and let

$$Eq(C, i) = \bigcup_{\substack{\alpha \in C \\ mul(\alpha) > i}} \{eq(\alpha, i)\}$$

denote the set of $i$-th derivative equations contributed by the roots in $C$.

To show the existence of the required bound $N_r$, we will perform a case analysis on the number of equivalence classes of $\sim$.

*Case I.* Suppose $\sim$ has exactly one equivalence class $C = \{\alpha\omega_1, \ldots, \alpha\omega_s\}$, necessarily self-conjugate, with representative $\alpha$. Consider the set of equations $Eq(C, 0)$:

$$\begin{aligned}(\alpha\omega_1)^n &= \kappa_1 P_1(\alpha\omega_1) + \kappa_2 P_2(\alpha\omega_1)\\ &\vdots\\ (\alpha\omega_s)^n &= \kappa_1 P_1(\alpha\omega_s) + \kappa_2 P_2(\alpha\omega_s)\end{aligned}$$

For our fixed $r$, the values of $\omega_1^n, \ldots, \omega_s^n$ are easy to calculate in polynomial time, since $\omega_i$ are roots of unity whose order divides $L$. Then the equations $Eq(C, 0)$ are equivalent to

$$\begin{bmatrix} \alpha^n \\ \vdots \\ \alpha^n \end{bmatrix} = \boldsymbol{B} \begin{bmatrix} \kappa_1 \\ \kappa_2 \end{bmatrix}, \tag{4.5}$$

where $\boldsymbol{B}$ is an $s \times 2$ matrix over $\mathbb{A}$ which, given $r$, is computable in polynomial time. Next we subtract the first row of (4.5) from rows $2, \ldots, s$, obtaining

$$\alpha^n = c_1\kappa_1 + c_2\kappa_2 \wedge \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = \boldsymbol{B'} \begin{bmatrix} \kappa_1 \\ \kappa_2 \end{bmatrix}.$$

Here $(c_1, c_2)$ is the first row of the matrix $\boldsymbol{B}$, and $\boldsymbol{B'}$ is the result of subtracting $(c_1, c_2)$ from each of the bottom $s-1$ rows of $\boldsymbol{B}$. Thus, $Eq(C, 0)$ is equivalent to $\alpha^n = c_1\kappa_1 + c_2\kappa_2$ together with the constraint that $(\kappa_1, \kappa_2)^T$ must lie in the nullspace of $\boldsymbol{B'}$. We now consier the nullspace of $\boldsymbol{B'}$. If its dimension is less than 2, then we have a linear constraint on $\kappa_1, \kappa_2$. This constraint is of the form $\kappa_1 = \chi\kappa_2$ when the nullspace of $\boldsymbol{B'}$ has dimension 1, and is $\kappa_1 = \kappa_2 = 0$ when the nullspace is of dimension 0. In both cases, the Master System is equivalent to a lower-dimensional one which may be computed in polynomial time, so the existence of the bound $N_r$ follows inductively. In the case when the nullspace of $\boldsymbol{B'}$ has dimension 2, then the linear constraint is vacuous, and $Eq(C, 0)$ is equivalent to $\alpha^n = c_1\kappa_1 + c_2\kappa_2$.

In the same way, for this fixed $r$, $Eq(C, 1)$ reduces to a single first-derivative equation:

$$n\alpha^{n-1} = c_3\kappa_1 + c_4\kappa_2.$$

We do this for all $Eq(C, i)$, obtaining a system of equations equivalent to (4.1) based on the representative of $C$, rather than the actual eigenvalues in $C$. Denote the resulting set of equations by $\mathcal{F}(Eq(C))$.

If some eigenvalue $x \in C$ has $mul(x) \geq 3$, then $\mathcal{F}(Eq(C))$ contains the following triple of equations:

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \\ n(n-1)\alpha^{n-2} \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \\ c_5 \end{bmatrix} + \kappa_2 \begin{bmatrix} c_2 \\ c_4 \\ c_6 \end{bmatrix}. \tag{4.6}$$

If the vectors on the right-hand side of (4.6) are linearly independent over $\mathbb{A}$, then they specify a plane in $\mathbb{A}^3$, and the triple states that the point on the left-hand side must lie on this plane. Letting $(A_1, A_2, A_3)^T$ be the normal of the plane, we obtain

$$\begin{aligned}&A_1\alpha^n + A_2 n\alpha^{n-1} + A_3 n(n-1)\alpha^{n-2} = 0\\ \iff &A_1\alpha^2 + A_2 n\alpha + A_3 n(n-1) = 0.\end{aligned}$$

This is a quadratic equation in $n$. It has at most two roots, both at most exponentially large in the size of the input, so we just take $N_r$ to be the greater root. If the vectors on the right-hand side of (4.6) are linearly dependent over $\mathbb{A}$, then the exponents $n$ which solve (4.6) are precisely those which solve:

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \\ n(n-1)\alpha^{n-2} \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \\ c_5 \end{bmatrix}.$$

We divide the first equation by the second to obtain

$$\frac{\alpha}{n} = \frac{c_1}{c_3},$$

which limits $n$ at most one, exponentially large, candidate value $\alpha c_3/c_1$.

If all eigenvalues $x$ in $C$ have $mul(x) \leq 2$ and at least one has $mul(x) = 2$, then $\mathcal{F}(Eq(C))$ consists of exactly two equations:

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \end{bmatrix} + \kappa_2 \begin{bmatrix} c_2 \\ c_4 \end{bmatrix}. \tag{4.7}$$

If $(c_1, c_3)^T$ and $(c_2, c_4)^T$ are linearly independent over $\mathbb{A}$, then the right-hand side of (4.7) spans all of $\mathbb{A}^2$ as $\kappa_1, \kappa_2$ range over $\mathbb{A}$. Then (4.7) is solved by all $n \in \mathbb{N}$, so we can take $N_r = L$. Otherwise, the exponents $n$ which solve (4.7) are exactly those which solve

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \end{bmatrix}.$$

This limits $n$ to at most one candidate value $\alpha c_3/c_1$, which is exponentially large in the input size.

Finally, if all eigenvalues $x$ in $C$ have $mul(x) = 1$, then $\mathcal{F}(Eq(C))$ contains only the equation

$$\alpha^n = \kappa_1 c_1 + \kappa_2 c_2,$$

which is solved by all $n \in \mathbb{N}$ if at least one of $c_1, c_2$ is non-zero, and has no solutions if $c_1 = c_2 = 0$. Either way, we take $N_r = L$ and are done.

*Case II.* Suppose $\sim$ has exactly two equivalence classes, $C_1$ and $C_2$, with respective representatives $\alpha$ and $\beta$, so that

$$C_1 = \{\alpha\omega_1, \ldots, \alpha\omega_s\},$$
$$C_2 = \{\beta\omega'_1, \ldots, \beta\omega'_l\}.$$

The classes could be self-conjugate, in which case $\alpha, \beta \in \mathbb{A} \cap \mathbb{R}$, or they could be each other's image under complex conjugation, in which case $\alpha = \overline{\beta}$. In both cases, $\alpha/\beta$ is not a root of unity.

As in *Case I,* we transform the system $Eq(C_1) \wedge Eq(C_2)$ into the equivalent system $\mathcal{F}(Eq(C_1)) \wedge \mathcal{F}(Eq(C_2))$. If all eigenvalues $x$ of $\boldsymbol{A}$ have $mul(x) = 1$, then the resulting system consists of two equations, one for each equivalence class of $\sim$:

$$\alpha^n = \kappa_1 c_1 + \kappa_2 c_2$$
$$\beta^n = \kappa_1 c_3 + \kappa_2 c_4$$

If $(c_1, c_3)^T$ and $(c_2, c_4)^T$ are linearly independent over $\mathbb{A}$, then there is a solution for each $n$, so just take $N_r = L$. Otherwise, it suffices to look for $n$ which satisfies

$$\alpha^n = \kappa_1 c_1$$
$$\beta^n = \kappa_1 c_3$$

and hence

$$\left(\frac{\alpha}{\beta}\right)^n = \frac{c_1}{c_3}.$$

A bound on $n$ follows from Lemma 21. This argument relies crucially on the fact that $\alpha/\beta$ is not a root of unity.

If some eigenvalue $x$ of $\boldsymbol{A}$ has $mul(x) \geq 2$, say $x \in C_1$, then the system contains the following triple of equations:

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \\ \beta^n \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \\ c_5 \end{bmatrix} + \kappa_2 \begin{bmatrix} c_2 \\ c_4 \\ c_6 \end{bmatrix}. \tag{4.8}$$

If the vectors on the right-hand side of (4.8) are linearly dependent over $\mathbb{A}$, so that the right-hand side describes a space of dimension 1, it suffices to look for solutions to

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \\ \beta^n \end{bmatrix} = \kappa_1 \begin{bmatrix} c_1 \\ c_3 \\ c_5 \end{bmatrix}.$$

Then dividing we obtain

$$\frac{\alpha}{n} = \frac{c_1}{c_3},$$

which limits $n$ to at most one, exponentially large candidate value $\alpha c_3/c_1$. Otherwise, if the vectors on the right-hand side of (4.8) are linearly independent over $\mathbb{A}$, we calculate the normal $(A_1, A_2, A_3)^T$ to the plane described by them and obtain

$$A_1\alpha^n + A_2 n\alpha^{n-1} + A_3\beta^n = 0.$$

A bound on $n$ which is exponential in the size of the input follows from Lemma 27. This again relies on the fact that $\alpha/\beta$ cannot be a root of unity.

*Case III.* Suppose $\sim$ has at least three equivalence classes. Then we can choose eigenvalues $\alpha, \beta, \gamma$, each from a distinct equivalence class, and consider $eq(\alpha, 0)$, $eq(\beta, 0)$ and $eq(\gamma, 0)$:

$$\begin{bmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{bmatrix} = \kappa_1 \begin{bmatrix} P_1(\alpha) \\ P_1(\beta) \\ P_1(\gamma) \end{bmatrix} + \kappa_2 \begin{bmatrix} P_2(\alpha) \\ P_2(\beta) \\ P_2(\gamma) \end{bmatrix}.$$

If the vectors on the right-hand side are linearly independent over $\mathbb{A}$, we eliminate $\kappa_1, \kappa_2$ to obtain

$$A_1\alpha^n + A_2\beta^n + A_3\gamma^n = 0.$$

The left-hand side is a non-degenerate linear recurrence sequence of order 3, so a bound on $n$ follows from Lemmas 24, 25, 26. If the vectors on the right-hand side are not linearly independent over $\mathbb{A}$, then we may equivalently consider

$$\begin{bmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{bmatrix} = \kappa_1 \begin{bmatrix} P_1(\alpha) \\ P_1(\beta) \\ P_1(\gamma) \end{bmatrix},$$

which gives

$$\left(\frac{\alpha}{\beta}\right)^n = \frac{P_1(\alpha)}{P_1(\beta)}.$$

An exponential bound on $n$ follows from Lemma 21, because $\alpha/\beta$ is not a root of unity.

Thus, we have now shown that for any $r \in \{0, \ldots, L-1\}$, the required bound $N_r$ exists and is at most exponential in the size of the input. Then $N = \max\{N_r : r \in \{0, \ldots, L-1\}\}$ exists and is exponentially large, so the Discrete Orbit Problem with two-dimensional target space is in $\mathbf{NP^{RP}}$, by the complexity argument of Section 4.2.

## 4.6 Three-dimensional target space

Suppose we are given a rational square matrix $\boldsymbol{A}$ and polynomials $P_1, P_2, P_3$ with rational coefficients such that $P_1(\boldsymbol{A}), P_2(\boldsymbol{A}), P_3(\boldsymbol{A})$ are linearly independent over $\mathbb{Q}$. We want to decide whether there exists $n \in \mathbb{N}$ such that $\boldsymbol{A}^n$ lies in the $\mathbb{Q}$-vector space $span\{P_1(\boldsymbol{A}), P_2(\boldsymbol{A}), P_3(\boldsymbol{A})\}$. We have derived a Master System of equations (4.1) in the unknowns $(n, \kappa_1, \kappa_2, \kappa_3)$ whose solutions are precisely the solutions of the matrix equation $\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A}) + \kappa_2 P_2(\boldsymbol{A}) + \kappa_3 P_3(\boldsymbol{A})$.

In this section, we will show that there exists a bound $N$, exponentially large in the size of the input, such that if the problem instance is positive, then there exists a witness exponent $n$ with $n < N$. This will be sufficient to show that the problem is in the complexity class $\mathbf{NP^{RP}}$, as outlined earlier.

The eigenvalues of $\boldsymbol{A}$ may be assumed to be non-zero algebraic numbers: if 0 is an eigenvalue, then $eq(0, 0)$ gives a linear dependence between the coefficients $\kappa_1, \kappa_2, \kappa_3$, yielding a lower-dimensional Master System, so the existence of the bound $N$ follows inductively.

Following the strategy of the two-dimensional case, we will perform a case analysis on the residue of $n$ modulo $L$: let $n \bmod L = r$ be fixed throughout this section. To obtain the required bound $N$, it is sufficient to derive a bound $N_r$, also exponentially large in the size of the input, such that if there exists a witness exponent of residue $r$ modulo $L$, then such a witness may be found which does not exceed $N_r$. As in the two-dimensional case, we will select tuples of equations and obtain a bound on $n$ using the

results for the Discrete Skolem Problem for recurrences of order 4 in Section 3.6. We will again perform a case analysis on the equivalence classes of the relation $\sim$.

*Case I.* Suppose there are at least two pairs of classes $(C_i, \overline{C_i})$, $(C_j, \overline{C_j})$ which are not self-conjugate. Then let $\alpha \in C_i$, $\beta = \overline{\alpha} \in \overline{C_i}$, $\gamma \in C_j$, $\delta = \overline{\gamma} \in \overline{C_j}$. Then we consider the tuple of equations

$$\begin{bmatrix} \alpha^n \\ \beta^n \\ \gamma^n \\ \delta^n \end{bmatrix} = \kappa_1 \begin{bmatrix} P_1(\alpha) \\ P_1(\beta) \\ P_1(\gamma) \\ P_1(\delta) \end{bmatrix} + \kappa_2 \begin{bmatrix} P_2(\alpha) \\ P_2(\beta) \\ P_2(\gamma) \\ P_2(\delta) \end{bmatrix} + \kappa_3 \begin{bmatrix} P_3(\alpha) \\ P_3(\beta) \\ P_3(\gamma) \\ P_3(\delta) \end{bmatrix}. \tag{4.9}$$

If the vectors on the right-hand side are linearly dependent over $\mathbb{A}$, then we rewrite the right-hand side as a linear combination of at most two vectors and obtain the required bound on $n$ by considering a linear recurrence sequence of order 2 or 3. If the vectors on the right-hand side of (4.9) are linearly independent over $\mathbb{A}$, then we calculate the normal of the three-dimensional subspace of $\mathbb{A}^4$ that they span, obtaining an equation

$$A_1\alpha^n + A_2\beta^n + A_3\gamma^n + A_4\delta^n = 0 \tag{4.10}$$

and hence an exponential bound on $n$ from Lemmas 30 and 31. We are relying on the fact that the ratios of $\alpha, \beta, \gamma, \delta$ are not roots of unity. Notice that we need $(\alpha, \beta)$ and $(\gamma, \delta)$ to be pairwise complex conjugates in order to apply Lemma 31. Notice also that we may assume without loss of generality that $\alpha, \beta, \gamma, \delta$ are algebraic integers, as Lemma 31 requires. Indeed, as remarked at the beginning of Section 4.3, the input data may be assumed to be over $\mathbb{Z}$, instead of $\mathbb{Q}$, with the simple technique of scaling the input by an integer chosen so as to 'clear the denominators'. Then $\boldsymbol{A}$ is an integer matrix, so its eigenvalues are algebraic integers.

*Case II.* Suppose now that there is exactly one pair of classes $(C_i, \overline{C_i})$ which are not self-conjugate. In general, for any eigenvalue $x$ of $\boldsymbol{A}$ we must have $mul(x) = mul(\overline{x})$. Therefore, if any eigenvalue $\alpha \in C_i$ has $mul(\alpha) > 1$, we can select the tuple of equations $eq(\alpha, 0)$, $eq(\alpha, 1)$, $eq(\overline{\alpha}, 0)$, $eq(\overline{\alpha}, 1)$:

$$\begin{bmatrix} \alpha^n \\ \overline{\alpha}^n \\ n\alpha^{n-1} \\ n\overline{\alpha}^{n-1} \end{bmatrix} = \kappa_1 \begin{bmatrix} P_1(\alpha) \\ P_1(\overline{\alpha}) \\ P_1'(\alpha) \\ P_1'(\overline{\alpha}) \end{bmatrix} + \kappa_2 \begin{bmatrix} P_2(\alpha) \\ P_2(\overline{\alpha}) \\ P_2'(\alpha) \\ P_2'(\overline{\alpha}) \end{bmatrix} + \kappa_3 \begin{bmatrix} P_3(\alpha) \\ P_3(\overline{\alpha}) \\ P_3'(\alpha) \\ P_3'(\overline{\alpha}) \end{bmatrix}.$$

This gives a non-degenerate linear recurrence sequence of order 4 over $\mathbb{A}$ for a recurrence sequence with two repeated characteristic roots:

$$A_1\alpha^n + A_2\overline{\alpha}^n + A_3 n\alpha^{n-1} + A_4 n\overline{\alpha}^{n-1} = 0.$$

An exponential bound $N$ on $n$ follows from Lemma 28, since $\alpha/\overline{\alpha}$ is not a root of unity.

We can now assume that eigenvalues in $C_i$ and $\overline{C_i}$ contribute exactly one equation to the system. Now we use the fixed value of $r$ to transform $Eq(C_i) \wedge Eq(\overline{C_i})$ into $\mathcal{F}(Eq(C_i)) \wedge \mathcal{F}(Eq(\overline{C_i}))$. Since all eigenvalues in $C_i$ and $\overline{C_i}$ contribute one equation each, $\mathcal{F}(Eq(C_i)) \wedge \mathcal{F}(Eq(\overline{C_i}))$ is just

$$\begin{aligned} \lambda^n &= \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3 \\ \overline{\lambda}^n &= \kappa_1 c_4 + \kappa_2 c_5 + \kappa_3 c_6 \end{aligned}$$

where $\lambda, \overline{\lambda}$ are the representatives of $C_i$ and $\overline{C_i}$. We do the same to all self-conjugate classes as well, reducing the system of equations to an equivalent system based on the representatives of the equivalence classes, not the actual eigenvalues of $\boldsymbol{A}$. This is beneficial, because the representatives cannot divide to give roots of unity, so we can use 4-tuples of equations to construct non-degenerate linear recurrence sequences of order 4.

If there are at least two self-conjugate equivalence classes, with respective representatives $\alpha, \beta$, we take the tuple

$$\begin{aligned} \lambda^n &= \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3 \\ \overline{\lambda}^n &= \kappa_1 c_4 + \kappa_2 c_5 + \kappa_3 c_6 \\ \alpha^n &= \kappa_1 c_7 + \kappa_2 c_8 + \kappa_3 c_9 \\ \beta^n &= \kappa_1 c_{10} + \kappa_2 c_{11} + \kappa_3 c_{12} \end{aligned}$$

and obtain the following equation, where the left-hand side is a non-degenerate linear recurrence sequence:

$$A_1\lambda^n + A_2\overline{\lambda}^n + A_3\alpha^n + A_4\beta^n = 0.$$

Then we have an exponentially large bound $N_r$ from Lemmas 30 and 31. Similarly, if there is only one self-conjugate equivalence class, with representative $\alpha$, but some of its eigenvalues are repeated, we use the tuple

$$\begin{aligned}\lambda^n &= \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3\\ \overline{\lambda}^n &= \kappa_1 c_4 + \kappa_2 c_5 + \kappa_3 c_6\\ \alpha^n &= \kappa_1 c_7 + \kappa_2 c_8 + \kappa_3 c_9\\ n\alpha^{n-1} &= \kappa_1 c_{10} + \kappa_2 c_{11} + \kappa_3 c_{12}\end{aligned}$$

to obtain the non-degenerate instance

$$A_1\lambda^n + A_2\overline{\lambda}^n + A_3\alpha^n + A_4 n\alpha^{n-1} = 0,$$

which gives an exponential bound $N_r$ according to Lemma 29. If there is exactly one self-conjugate class, with representative $\alpha$, containing no repeated roots, then the system consists of three equations:

$$\begin{aligned}\lambda^n &= \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3\\ \overline{\lambda}^n &= \kappa_1 c_4 + \kappa_2 c_5 + \kappa_3 c_6\\ \alpha^n &= \kappa_1 c_7 + \kappa_2 c_8 + \kappa_3 c_9\end{aligned}$$

Depending on whether the vectors $(c_1, c_4, c_7)^T$, $(c_2, c_5, c_8)^T$, $(c_3, c_6, c_9)^T$ are linearly independent over $\mathbb{A}$, either this triple is solved by all $n \in \mathbb{N}$ (in which case set $N_r = L$), or it reduces to a lower-dimensional Master System, yielding the claim inductively. Finally, if there are no self-conjugate classes, the system consists of only two equations:

$$\begin{aligned}\lambda^n &= \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3\\ \overline{\lambda}^n &= \kappa_1 c_4 + \kappa_2 c_5 + \kappa_3 c_6\end{aligned}$$

Again, depending on the dimension of

$$span\left\{\begin{bmatrix} c_1 \\ c_4 \end{bmatrix}, \begin{bmatrix} c_2 \\ c_5 \end{bmatrix}, \begin{bmatrix} c_3 \\ c_6 \end{bmatrix}\right\},$$

we can either set the bound $N_r$ to $L$ (because the transformed Master System is solved by all $n \in \mathbb{N}$), or obtain $N_r$ inductively from a lower-dimensional Master System.

*Case III.* All equivalence classes of $\sim$ are self-conjugate. The techniques used for this case are identical to the ones already presented. We use the fixed value of $r$ to reduce to a non-degenerate system based on the representatives of the classes, with the number of equations contributed by each class determined by the maximum multiplicity of an eigenvalue in that class.

If there are less than four equations, then we study the dimension of the vector space spanned by the vectors on the right-hand side: if it has full dimension, then we see the Master System is satisfied by all $n$ of the correct residue $r$, so we can just set $N_r = L$. Otherwise, we obtain the bound inductively from a lower-dimensional non-degenerate Master System.

On the other hand, if there are at least four equations, then we can choose four equations which have a solution for $n$ if and only if an effectively computable non-degenerate LRS of order 4 vanishes at $n$. We then employ the bounds of Chapter 3 concerning LRS of order 4 to obtain the desired $N_r$.

As we remarked in Section 4.5, it is only for this final case that we need the representatives of self-conjugate classes to be real, necessitating the choice of the magnitude of the eigenvalues in the class for representative, regardless of whether this magnitude is itself an eigenvalue. The reason for this technical point is that Lemma 31, which gives a bound on the index of zeros of an LRS of order 4 with four distinct characteristic roots, requires that the characteristic roots be closed under complex conjugation. No strengthening of Lemma 31 is known which avoids this precondition – as we remark in Section 3.6, this is the reason why the Discrete Skolem Problem is open for LRS of order 4 over $\mathbb{A}$. If we had chosen the representative of a self-conjugate class to be an arbitrary (possibly complex) eigenvalue, we would obtain LRS of order 4 whose characteristic roots do not satisfy the precondition on Lemma 31, and we would not be able to obtain our bound $N_r$ here.

# Chapter 5

# Polyhedron-Hitting Problem

*Prerequisites:*
Sections 2.1.1, 2.2, 2.4.1 and 2.5.
Chapter 4 and Theorem 19 from Chapter 3.
Theorem 7 from Section 2.1.3.

## 5.1 Introduction

In this chapter, we study a natural generalisation of the Discrete Orbit Problem, which we call the *Discrete Polyhedron-Hitting Problem*: given a discrete-time linear dynamical system specified by a starting point $\boldsymbol{x} \in \mathbb{Q}^m$ and a linear transformation $\boldsymbol{A} \in \mathbb{Q}^{m \times m}$, and a target (bounded or unbounded) polyhedron $\mathcal{P} \subseteq \mathbb{Q}^m$, determine whether the system will eventually reach $\mathcal{P}$, that is, whether there exists $n \in \mathbb{N}$ such that $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{P}$. This problem was also considered in [Tarasov and Vyalyi, 2011] under the appellation of *Chamber-Hitting Problem*. However, that paper focused on connections with formal language theory rather than on establishing decidability. In this chapter, we present what amounts to a complete characterisation of the decidability landscape for this problem, expressed as a function of the dimension $m$ of the ambient space $\mathbb{Q}^m$, together with the dimension $d$ of the polyhedral target $\mathcal{P}$; more precisely, for each pair of dimensions, we either establish decidability, or show hardness for longstanding number-theoretic open problems.

This work significantly extends our results on the Discrete Orbit Problem from Chapters 3 and 4, where only vector-space targets were permitted. Polyhedra, defined as intersections of affine halfspaces, pose substantial new challenges. Indeed, whilst reachability to a vector space broadly corresponds to determining whether linear recurrence sequences vanish, permitting halfspace targets leads to questions about LRS being simultaneously non-negative, which in turn entails new obstacles to decidability and necessitates further tools not invoked in the previous chapters, such as techniques from Diophantine approximation, convex geometry and decision procedures for the existential fragment of the first-order theory of the real closed field.

## 5.2 Main result and outline

This chapter is based on our publication [Chonev et al., 2015c]. The focus of this chapter is the *Polyhedron-Hitting Problem*: given a square matrix $\boldsymbol{A} \in \mathbb{Q}^{m \times m}$, a vector $\boldsymbol{x} \in \mathbb{Q}^m$ and polyhedron $\mathcal{P}$ (represented as the intersection of affine halfspaces), determine whether there exists a natural number $n$ such that $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{P}$. We will denote by $PHP(m, d)$ the version of the problem in which the ambient space is $\mathbb{Q}^m$ and the target polyhedron has dimension $d \leq m$.

Our results are summarised in Fig. 5.2. For each pair $(m, d)$, we have either an upper complexity bound or a hardness result for $PHP(m, d)$. Upper complexity bounds are denoted by **PTIME** and **PSPACE**, indicating membership in these classes. We include for completeness the row $d = 0$, referring to Kannan and Lipton's original result on point-to-point reachability [Kannan and Lipton, 1980,

| | $m=1$ | $m=2$ | $m=3$ | $m=4$ | $m=d$ | $m \geq d+1$ |
|---|---|---|---|---|---|---|
| $d=0$ | **P** | **P** | **P** | **P** | **P** | **P** |
| $d=1$ | **PSPACE** | **PSPACE** | **PSPACE** | **PSPACE** | **PSPACE** | **PSPACE** |
| $d=2$ | | **PSPACE** | **PSPACE** | **PSPACE** | **PSPACE** | **PSPACE** |
| $d=3$ | | | **PSPACE** | $S_5$ | **PSPACE** | $S_5$ |
| $d=4$ | | | | $D$ | $D$ | $D$ & $S_5$ |
| $d \geq 5$ | | | | | $D$ | $D$ & $S_{d+1}$ |

Figure 5.1: Upper and lower complexity bounds for instances of the Polyhedron-Hitting Problem in ambient dimension $m$ with a $d$-dimensional target.

Kannan and Lipton, 1986]. Lower bounds are of two kinds, denoted by $D$ and $S_d$ in the table. Entries $S_d$ indicate a reduction from the Discrete Skolem Problem for rational LRS of order $d$, whereas entries $D$ indicate a reduction from the following problem in Diophantine approximation: given an algebraic number $\lambda \in \mathbb{Q}(i)$ and $\varepsilon \in \mathbb{Q}$, calculate $L(\arg(\lambda)/2\pi)$ to within absolute additive error $\varepsilon$, where $L$ denotes the Lagrange approximation type defined in Section 2.2.1.

The structure of this chapter is as follows. First, in Section 5.3, we study the Polyhedron-Hitting Problem in the case when the target polyhedron has *full dimension*, that is, the dimension of the ambient space matches the dimension of the target polyhedron. In this case, the Polyhedron-Hitting Problem is equivalent to the *Simultaneous Non-negativity Problem*: given a family of linear recurrence sequences over $\mathbb{Q}$ which all satisfy a common characteristic equation, determine whether there exists $n \in \mathbb{N}$ such that the $n$-th term of each given LRS is non-negative. In Section 5.3.1, we show this problem is in **PSPACE** for LRS whose common characteristic equation is of order at most 3, or of order 4 but with a simple real characteristic root. This establishes membership in **PSPACE** for $PHP(d, d)$ for $d \leq 3$. Then in Section 5.3.2, we show that a decision procedure for $PHP(4, 4)$ may be used to compute the Lagrange type of all real numbers of the form $\arg(\lambda)/2\pi$ for $\lambda \in \mathbb{Q}(i)$. Thus, solving $PHP(4, 4)$ is highly unlikely without major breakthroughs in analytic number theory, as very little is known about the approximation type of the vast majority of transcendental numbers.

Afterwards, in Section 5.4, we show several simple reductions aimed at establishing the remaining bounds on the Polyhedron-Hitting Problem, that is, the off-diagonal entries in the table. Specifically, Section 5.4.1 reduces $PHP(m, 1)$ and $PHP(m, 2)$ to the *Extended Orbit Problem,* a generalisation of the Discrete Orbit Problem studied in Chapter 4 which admits linear inequalities on the coefficients $\boldsymbol{\kappa}$ which witness membership of $\boldsymbol{A}^n\boldsymbol{x}$ in the target space. This problem essentially specialises the target of the Polyhedron-Hitting Problem to a cone and assumes a particular parametric representation. Then in Section 5.4.2 we give reductions from the Discrete Skolem Problem and moreover establish all hardness results appearing in the table by embedding lower-dimensional versions of the Polyhedron-Hitting Problem into higher-dimensional ones.

Finally, in Section 5.5, we treat in full technical detail the Extended Orbit Problem for cones of dimension at most three to establish our **PSPACE** upper bounds for $PHP(m, 1)$ and $PHP(m, 2)$. Whilst the method employs many of the same techniques showcased in Chapter 4, complications arise in the cases of a Master System which is 'too small' to directly bound the exponent $n$. We perform a case analysis on the residue of $n$ and show that after algebraic manipulation of the Master System, these problematic cases reduce to the Simultaneous Non-negativity Problem of Section 5.3.

## 5.3 Polyhedra of full dimension

We begin with the case of the Polyhedron-Hitting Problem when the target polyhedron $\mathcal{P}$ has dimension $m$, matching the dimension of the ambient space $\mathbb{Q}^m$. Denote this problem by $PHP(m, m)$. We are given $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, $\boldsymbol{x} \in \mathbb{Q}^m$ and a halfspace description of a polyhedron $\mathcal{P}$, consisting of vectors $\boldsymbol{y_1}, \ldots, \boldsymbol{y_k} \in \mathbb{Q}^m$ and scalars $c_1, \ldots, c_k \in \mathbb{Q}$, where each pair $(\boldsymbol{y_j}, c_j)$ defines a halfspace in $\mathbb{Q}^m$ and the intersection of the halfspaces gives the polyhedron $\mathcal{P}$:

$$\mathcal{P} = \bigcap_{j=1}^{k} \{\boldsymbol{x} \in \mathbb{Q}^m : \boldsymbol{y_j^T}\boldsymbol{x} \geq c_j\}.$$

We show both a decidability result and a hardness result concerning $PHP(m, m)$. First, in Section 5.3.1, we show the problem is in **PSPACE** for $m \leq 3$. Then in Section 5.3.2, we prove that a decision procedure for $PHP(4, 4)$ would yield the computability of the Lagrange type $L(x)$ of all real numbers $x$ of the form $x = \arg(\lambda)/2\pi$ with $\lambda$ a Gaussian rational.

### 5.3.1 Low dimension: decidability

Suppose $m \leq 3$ and we are given an instance of $PHP(m, m)$ as above. For $j = 1, \ldots, k$, define the linear recurrence sequences $\langle v_n^{(j)} \rangle_{n=0}^{\infty} = \boldsymbol{y_j^T A}^n \boldsymbol{x}$. By the Cayley-Hamilton Theorem, the sequences $\langle v_n^{(j)} \rangle_{n=0}^{\infty}$ satisfy a common recurrence equation whose characteristic polynomial is the minimal polynomial $P \in \mathbb{Q}[x]$ of $\boldsymbol{A}$. Define also the sequences $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ by $u_n^{(j)} = v_n^{(j)} - c_j$. The LRS $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ also satisfy a common recurrence equation, with characteristic polynomial $(x-1)P(x)$ (if $P(1) \neq 0$) or $P(x)$ (if $P(1) = 0$). Since $P(x)$ has degree at most $m \leq 3$, the recurrence equation shared by the sequences $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ has order at most three, or order four but with 1 as a simple characteristic root. The problem instance is positive if and only if there exists $n$ such that $u_n^{(j)} \geq 0$ for all $j = 1, \ldots, k$.

We call this the *Simultaneous Non-negativity Problem for linear recurrence sequences.* For the purposes of proving that $PHP(m, m)$ is in **PSPACE**, it is sufficient to take our LRS to be over $\mathbb{Q}$. However, for technical convenience for our later results in Section 5.5, we instead consider the problem in slightly greater generality, allowing the given LRS to be over $\mathbb{R} \cap \mathbb{A}$. Therefore, in the rest of this section we prove the following:

**Theorem 34.** *The Simultaneous Non-negativity Problem for LRS over $\mathbb{R} \cap \mathbb{A}$ which all satisfy a common recurrence equation of order up to three, or of order four with the simple characteristic root 1, is in* **PSPACE**.

We will restrict our attention to non-degenerate LRS. As outlined in Section 2.3.1, a degenerate sequence $\langle u_n \rangle_{n=0}^{\infty}$ can be partitioned into at most $2^{\mathcal{O}(||u||)}$ non-degenerate subsequences, where $\|u\|$ denotes the length of the description of $\langle u_n \rangle_{n=0}^{\infty}$. Then the problem instance is equivalent to the disjunction of all instances where each degenerate sequence has been replaced by one of its exponentially many non-degenerate subsequences. We can guess nondeterministically a non-degenerate subsequence of each given degenerate LRS without degrading our desired **PSPACE** complexity upper bound. The assumption of non-degeneracy guarantees that there can be at most one real root among the dominant roots of the sequences. We can assume without loss of generality that any real root of the sequence is positive (otherwise we separately consider the cases of even and odd $n$).

The asymptotic behaviour of a linear recurrence sequence $\langle u_n \rangle_{n=0}^{\infty}$ is closely linked to its dominant characteristic roots, that is, the characteristic roots of greatest magnitude. If $\lambda_1, \ldots, \lambda_s$ are the dominant roots, we can write

$$\frac{u_n}{|\lambda_1|^n} = P_1(n) \left( \frac{\lambda_1}{|\lambda_1|} \right)^n + \cdots + P_s(n) \left( \frac{\lambda_s}{|\lambda_1|} \right)^n + r(n),$$

where $r(n)$ tends to 0 exponentially quickly. We can use the polynomial root-separation bound (2.1) in Section 2.1.1 to bound the absolute value of the quotient $\lambda/\lambda_1$, where $\lambda$ is a non-dominant characteristic root. Thus we can show:

**Lemma 35.** *Suppose we are given an LRS $\langle u_n \rangle_{n=0}^{\infty}$ as above. Then there exist constants $\varepsilon \in \mathbb{Q}$ and $N \in \mathbb{N}$ such that $\varepsilon \in (0, 1)$, $N \in 2^{\mathcal{O}(||u||)}$, $\varepsilon^{-1} \in 2^{\mathcal{O}(||u||)}$, and $|r(n)| < (1-\varepsilon)^n$ for all $n > N$.*

At various points throughout the decision procedure, we resort to a guess-and-check technique. If we have some computable bound $N \in 2^{\mathcal{O}(||I||)}$, we can seach for witnesses up to $N$ by choosing a witness $n$ nondeterministically and then verifying $u_n^{(j)} \geq 0$. The verification procedure is via the first-order theory of the real closed field, see Section 2.4.1. Writing the $j$-th sequence in matrix form, $u_n^{(j)} = \boldsymbol{v_j^T M_j}^n \boldsymbol{w_j}$ with all entries real algebraic, we can construct a sentence $\tau_j$ in the existential fragment $Th^{\exists}(\mathbb{R}_{exp})$ of the first-order theory of the reals which is true if and only if $u_n^{(j)} \geq 0$. We use iterated squaring to keep the formula polynomially large: $\|\tau_j\| = ||I||^{\mathcal{O}(1)}$. Then immediately we have a polynomially large formula $\tau = \bigwedge_j \tau_j$ which is true if and only if the problem instance is positive. The validity of $\tau$ can be decided in **PSPACE** by Theorem 13.

We now proceed with the decision method. We consider two cases, according to the number of dominant complex roots of the shared recurrence equation.

*Case I.* Suppose first the dominant characteristic roots are all real. By non-degeneracy, there is only one dominant root $\rho$, and we may take it without loss of generality to be positive. Then the $j$-th sequence is given by

$$\frac{u_n^{(j)}}{\rho^n} = P_j(n) + r_j(n),$$

where $r_j$ is itself a linear recurrence of lower order which converges to 0 exponentially quickly, and $P_j \in (\mathbb{R} \cap \mathbb{A})[x]$. Each polynomial $P_j(n)$ is either identically zero, ultimately positive or ultimately negative as $n$ tends to infinity. In the latter two cases, there is an effective threshold $N_j \in 2^{\mathcal{O}(||u^{(j)}||)}$ beyond which the sign of $u_n^{(j)}$ does not change. If some $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ is ultimately negative, then any witness to the problem instance must be bounded above by $N_j$. Since $N_j$ is at most exponentially large in the size of the input, we use a guess-and-check procedure and are done. Similarly, for each sequence $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ for which $P_j$ is ultimately positive we can search for witnesses up to the threshold $N_j$ and if none are found, we discard $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ as if it were uniformly positive. Finally, we are left only with sequences $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ for which $P_j$ is identically zero. Then the problem instance reduces to an instance of the Simultaneous Non-negativity Problem comprising the sequences $r_j$. These sequences satisfy a common recurrence equation of lower order, so we proceed inductively.

*Case II.* Suppose now that the dominant roots of the shared recurrence equation are a pair of complex roots $\lambda, \overline{\lambda}$ and possibly a real dominant root $\rho_1 > 0$, with all characteristic roots simple. The $j$-th sequence is given by

$$\begin{aligned} u_n^{(j)} &= a_j \lambda^n + \overline{a_j}\,\overline{\lambda}^n + b_j \rho_1^n + c_j \rho_2^n \\ &= |\lambda|^n \left(2|a_j| \cos(\alpha_j + n\varphi) + b_j + r_j(n)\right), \end{aligned}$$

where $a_j, \lambda \in \mathbb{A}$, $b_j, \rho_1, \rho_2 \in \mathbb{R} \cap \mathbb{A}$, $\alpha_j = \arg(a_j)$, $\varphi = \arg(\lambda)$ and $r_j(n)$ is a linear recurrence sequence of order at most 2 with real characteristic roots. By non-degeneracy, we have $\varphi/2\pi \notin \mathbb{Q}$. Observe that for all $j$, $b_j + r_j(n)$ is either ultimately positive or ultimately negative as $n$ tends to infinity. Furthermore, a threshold beyond which the sign does not change is effectively computable and at most exponential in $\|u^{(j)}\|$. Following the reasoning of the previous case, we see that we can dismiss sequences $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ which have $a_j = 0$.

Assume therefore that $a_j \neq 0$ for all $j$. Dividing through by $2|\lambda|^n|a_j| > 0$ and replacing $b_j$ by $b_j/2|a_j|$ and $r_j(n)$ by $r_j(n)/2|a_j|$, we can assume the $j$-th sequence is given by:

$$u_n^{(j)} = \cos(\alpha_j + n\varphi) + b_j + r_j(n).$$

By Lemma 36 below, for each sequence $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ there exists an effective threshold $N_j$, exponentially large in $\|u^{(j)}\|$, such that for $n > N_j$, $r_j(n)$ is too small to influence the sign of $u_n^{(j)}$. That is, for all $n > N_j$, we have

$$u_n^{(j)} \geq 0 \iff b_j + \cos(\alpha_j + n\varphi) \geq 0.$$

Therefore, for $n \geq N = \max_j\{N_j\}$, the problem instance is equivalent to a conjunction of inequalities in $n$:

$$\forall j.\, \cos(\alpha_j + n\varphi) \geq -b_j.$$

We use guess-and-check to look for witnesses $n < N$. If none are found, the problem instance is then decidable in **PSPACE** by Lemma 37 below.

**Lemma 36.** *Let $a, \lambda \in \mathbb{A}$ and $C, \chi \in \mathbb{A} \cap \mathbb{R}$ be given where $\lambda$ is not a root of unity and $|\chi| < |\lambda| = 1$. Let $\alpha = \arg(a)$ and $\varphi = \arg(\lambda)$. Then there exists an effectively computable bound $N \in \mathbb{N}$ such that for all $n > N$, $|C + \cos(\alpha + n\varphi)| > |\chi|^n$. Moreover, $N = 2^{\mathcal{O}(||I||)}$ where $\|I\| = \|\lambda\| + \|\chi\| + \|a\| + \|C\|$.*

*Proof.* Suppose that $|C| \leq 1$ and let $b = C + i\sqrt{1 - C^2} = e^{i\beta}$, so that $C = \cos(\beta)$. Then $b$ is algebraic with $\deg(b) = ||I||^{\mathcal{O}(1)}$ and height $H_b = 2^{\mathcal{O}(||I||)}$. From elementary trigonometry, we have

$$C + \cos(\alpha + n\varphi) = 2\cos\frac{\alpha + \beta + n\varphi}{2}\cos\frac{\alpha - \beta + n\varphi}{2}.$$

Since $\lambda$ is not a root of unity, by Lemma 21, there exists an effective bound $N_1 = ||I||^{\mathcal{O}(1)}$ such that if $ab^{\pm 1}\lambda^n = -1$ then $n \leq N_1$. Therefore, we have

$$n > N_1 \Rightarrow \cos\left(\frac{\alpha \pm \beta + n\varphi}{2}\right) \neq 0.$$

Let $k_n$ be the unique integer such that $k_n\pi + (\alpha + \beta + n\varphi + \pi)/2 \in [-\pi/2, \pi/2)$. Notice that $|k_n| < 2n$. Then

$$\begin{aligned}\left|\cos\frac{\alpha+\beta+n\varphi}{2}\right| &= \left|\sin\frac{\alpha+\beta+n\varphi+(2k_n+1)\pi}{2}\right| \\ &\geq \frac{|\alpha+\beta+n\varphi+(2k_n+1)\pi|}{2\pi}\end{aligned}$$

by the inequality $|\sin(x)| \geq |x|/\pi$ for $x \in [-\pi/2, \pi/2]$. Note that $\alpha$, $\beta$, $\varphi$ and $\pi$ are logarithms of algebraic numbers with degree polynomial in $\|I\|$ and height exponential in $\|I\|$. Then by Theorem 7 (Baker-Wüstholz), there exist effective positive $p_1, p_2 = ||I||^{\mathcal{O}(1)}$ such that

$$n > N_1 \Rightarrow \left|\cos\frac{\alpha+\beta+n\varphi}{2}\right| > (p_1 n)^{-p_2}.$$

Similarly, there exist effective positive $N_2, p_3, p_4$, all polynomially large in $\|I\|$, such that

$$n > N_2 \Rightarrow \left|\cos\frac{\alpha-\beta+n\varphi}{2}\right| > (p_3 n)^{-p_4}.$$

However, since $\chi^n$ shrinks exponentially with $n$, it follows that there exists an effective bound $N_3 = 2^{\mathcal{O}(||I||)}$ such that for all $n > N_3$,

$$(p_1 n)^{-p_2}(p_3 n)^{-p_4} > |\chi^n|.$$

Then for all $n > \max\{N_1, N_2, N_3\}$, we have

$$|C + \cos(\alpha + n\varphi)| > p_1 p_3 n^{-(p_2+p_4)} > |\chi^n|,$$

as desired.

The remaining case $|C| > 1$ is easy. If $C > 1$, we have

$$C + \cos(\alpha + n\varphi) > 1 + \cos(\alpha + n\varphi) = \cos(0) + \cos(\alpha + n\varphi)$$

and the lemma follows by the above argument with $\beta = 0$. Similarly when $C < -1$. □

**Lemma 37.** *Suppose $a_1, \ldots, a_m$ and $\lambda$ are all algebraic numbers on the unit circle and $\lambda$ is not a root of unity. Suppose also $c_1, \ldots, c_m \in \mathbb{R} \cap \mathbb{A}$. Let $\alpha_j = \arg(a_j)$ and $\varphi = \arg(\lambda)$. Write*

$$\|I\| = \sum_{j=1}^{m} (\|a_j\| + \|c_j\|) + \|\lambda\|$$

*for the length of the input. Then it is decidable whether there exists a natural number $n$ such that $\cos(\alpha_j + n\varphi) \geq c_j$ for all $j = 1, \ldots, m$. Further, the procedure also determines whether there are finitely many such $n$. The decision procedure's running time is $||I||^{\mathcal{O}(1)}$.*

*Proof.* Inequalities where $c_j \leq -1$ may be discarded, as they are satisfied for all $n$, whereas the presence of inequalities with $c_j > 1$ immediately makes the problem instance negative. Now assuming $c_j \in (-1, 1]$, each inequality

$$\cos(\alpha_j + n\varphi_1) \geq c_j \tag{5.1}$$

defines an arc on the unit circle which $\lambda^n$ must lie within. Specifically, (5.1) holds if and only if $\lambda^n$ lies on the arc $\mathcal{A}_j$ defined by

$$\mathcal{A}_j = \{z \in \mathbb{C} : |z| = 1 \text{ and } h(w_1, w_2, z) \leq 0\}$$

where $w_1 = \overline{a_j}\left(c_j - i\sqrt{1-c_j^2}\right)$ and $w_2 = \overline{a_j}\left(c_j + i\sqrt{1-c_j^2}\right)$ are the endpoints of the arc, and

$$h(x,y,z) = \det \begin{bmatrix} \Re(x) & \Im(x) & 1 \\ \Re(y) & \Im(y) & 1 \\ \Re(z) & \Im(z) & 1 \end{bmatrix}$$

is the orientation function. (Recall that $h(x,y,z) > 0$ if the points $x, y, z$ (in that order) are arranged counter-clockwise on the complex plane, $h(x,y,z) < 0$ if they are arranged clockwise, and $h(x,y,z) = 0$ if they are collinear.)

The endpoints of $\mathcal{A}_j$ are clearly algebraic and may be computed explicitly in polynomial time in $\|I\|$. Then the intersection $\mathcal{A} = \bigcap_j \mathcal{A}_j$ is also computable in polynomial time. Since $\lambda$ is not a root of unity, the set $\{\lambda^n : n \in \mathbb{N}\}$ is dense on the unit circle by Theorem 11 (Kronecker). If $\mathcal{A}$ is empty, then the problem instance is negative. If $\mathcal{A}$ is a nontrivial arc on the unit circle, then by density, the problem instance is positive. Finally, if $\mathcal{A}$ is a set of at most two points $z_1, z_2$ on the unit circle, then the problem instance is positive if and only if there exists an exponent $n \in \mathbb{N}$ such that $\lambda^n = z_j$ for some $j \in \{1,2\}$. A polynomial bound on $n$ then follows from Lemma 21. □

### 5.3.2 High dimension: Diophantine hardness

Recall the homogeneous Diophantine approximation type $L(x)$ of a real number $x$, defined in Section 2.2.1:

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

This is a measure of how well $x$ can be approximated by rationals. Very little progress has been made on calculating the approximation type for the vast majority of transcendental numbers. Our main hardness result for the Polyhedron-Hitting Problem is the following:

**Theorem 38.** *Suppose that PHP$(4,4)$ is decidable. Then for any $\lambda \in \mathbb{Q}(i)$ on the unit circle, $L(\arg(\lambda)/2\pi)$ is a computable number, in the sense that $L(\arg(\lambda)/2\pi)$ may be approximated to within arbitrary precision.*

Suppose we wish to calculate $L(\varphi/2\pi)$, where $\varphi = \arg(\lambda)$ for some $\lambda \in \mathbb{Q}(i)$ of magnitude 1. Consider the two sequences $\langle u_n\rangle_{n=0}^{\infty}$ and $\langle v_n\rangle_{n=0}^{\infty}$ defined by

$$u_n = \frac{1}{2}\left((q-in)\lambda^n + (q+in)\overline{\lambda}^n\right)$$
$$v_n = \frac{1}{2}\left((q+in)\lambda^n + (q-in)\overline{\lambda}^n\right)$$

for some fixed rational number $q$. It is straightforward to verify that $\langle u_n\rangle_{n=0}^{\infty}$ and $\langle v_n\rangle_{n=0}^{\infty}$ are both LRS over $\mathbb{Q}$ satisfying a recurrence equation of order 4 with characteristic polynomial $(x-\lambda)^2(x-\overline{\lambda})^2$. Moreover we have

$$\begin{aligned} u_n &= n\cos(n\varphi - \pi/2) + q\cos(n\varphi) \\ &= q\cos(n\varphi) + n\sin(n\varphi), \\ v_n &= n\cos(n\varphi + \pi/2) + q\cos(n\varphi) \\ &= q\cos(n\varphi) - n\sin(n\varphi). \end{aligned}$$

Let $\langle w_n\rangle_{n=0}^{\infty}$ be the sequence over $\mathbb{Q}$ given by

$$\begin{aligned} w_n &= n|\sin(n\varphi)| - q\cos(n\varphi) \\ &= -\min\{u_n, v_n\}. \end{aligned}$$

Clearly, $u_n \geq 0$ and $v_n \geq 0$ if and only if $w_n \leq 0$.

Notice also that determining the existence of $n \in \mathbb{N}$ such that $u_n \geq 0$ and $v_n \geq 0$ is an instance of *PHP*$(4,4)$. Indeed, write $\langle u_n\rangle_{n=0}^{\infty}$ and $\langle v_n\rangle_{n=0}^{\infty}$ in matrix form:

$$u_n = \boldsymbol{y_1^T M^n x}$$
$$v_n = \boldsymbol{y_2^T M^n x}$$

where $\boldsymbol{M} \in \mathbb{Q}^{4\times 4}$ is the transpose of the companion matrix of the polynomial $(x-\lambda)^2(x-\overline{\lambda})^2$, the vectors $\boldsymbol{y_1}, \boldsymbol{y_2} \in \mathbb{Q}^4$ are the initial values of $\langle u_n \rangle_{n=0}^{\infty}$ and $\langle v_n \rangle_{n=0}^{\infty}$, respectively, and $\boldsymbol{x}$ is the unit vector $[0,0,0,1]^T$. Then $u_n, v_n \geq 0$ if and only if the orbit of $\boldsymbol{x}$ under $\boldsymbol{M}$ intersects the polyhedron

$$\mathcal{P} = \left\{ \boldsymbol{z} \in \mathbb{Q}^4 : \begin{array}{rcl} \boldsymbol{y_1^T z} & \geq & 0 \\ \boldsymbol{y_2^T z} & \geq & 0 \end{array} \right\}.$$

It is easy to check that $\boldsymbol{y_1}, \boldsymbol{y_2}$ are not collinear, so $\dim(\mathcal{P}) = 4$. Thus, an oracle for $PHP(4,4)$ may be used to determine whether there exists $n \in \mathbb{N}$ such that $u_n \geq 0$ and $v_n \geq 0$. We will show that such an oracle may be used on these sequences with different choices of $q$ in order to compute arbitrarily good approximations of $L(\varphi/2\pi)$. We begin by proving two technical results, which establish a connection between large non-positive elements of $\langle w_n \rangle_{n=0}^{\infty}$ and $L(\varphi/2\pi)$.

Fix some rational $\varepsilon \in (0,1)$, and recall that there exists a computable rational $\delta > 0$ such that:

$$\text{if } x \in [-\delta, \delta], \text{ then } (1-\varepsilon)|x| \leq |\sin(x)| \leq |x|, \tag{5.2}$$

$$\text{if } x \in [-\delta, \delta], \text{ then } 1-\varepsilon \leq \cos(x). \tag{5.3}$$

Moreover, there exists $N \in \mathbb{N}$ such that

$$q/N \leq \delta, \text{ and if } |\sin(x)| \leq q/N, \text{ then } |x| \leq \delta. \tag{5.4}$$

**Lemma 39.** *Suppose that $n \geq N$ is such that $w_n \leq 0$. Then $L(\varphi/2\pi) \leq q/(1-\varepsilon)2\pi$.*

*Proof.* Since $w_n \leq 0$ and $n \geq N$, we have

$$|\sin(n\varphi)| \leq \frac{q}{n}\cos(n\varphi) \leq \frac{q}{n} \leq \frac{q}{N}.$$

Let $m \in \mathbb{Z}$ be chosen so that $|n\varphi - 2\pi m|$ is minimised. Then by (5.4), it follows that $|n\varphi - 2\pi m| \leq \delta$. Then by (5.2), we have

$$\frac{q}{n} \geq |\sin(n\varphi)| \geq (1-\varepsilon)|n\varphi - 2\pi m|.$$

Rearranging, we obtain

$$\left|\frac{\varphi}{2\pi} - \frac{m}{n}\right| \leq \frac{q}{2\pi(1-\varepsilon)n^2},$$

so we conclude $L(\varphi/2\pi) \leq q/2\pi(1-\varepsilon)$. □

**Lemma 40.** *Let $L(\varphi/2\pi) \leq q(1-\varepsilon)/2\pi$ and suppose this is witnessed by the rational approximation $m/n$ with $n \geq N$. Then $w_n \leq 0$.*

*Proof.* By the premise of the Lemma, we have

$$\left|\frac{\varphi}{2\pi} - \frac{m}{n}\right| \leq \frac{q(1-\varepsilon)}{2\pi n^2},$$

so rearranging and noting that $q/N \leq \delta$ by (5.4), we obtain

$$|n\varphi - 2\pi m| \leq \frac{q(1-\varepsilon)}{n} \leq \frac{q}{N} \leq \delta.$$

Then by (5.2), we have

$$|\sin(n\varphi)| \leq |n\varphi - 2\pi m|.$$

Combining the upper and lower bound on $|n\varphi - 2\pi m|$, we have

$$|\sin(n\varphi)| \leq \frac{q(1-\varepsilon)}{n}.$$

Finally, from the definition of $\langle w_n \rangle_{n=0}^{\infty}$ and (5.3), we obtain

$$w_n = n|\sin(n\varphi)| - q\cos(n\varphi) \leq n|\sin(n\varphi)| - q(1-\varepsilon) \leq 0,$$

as required. □

We immediately have the following corollary:

**Lemma 41.** *If $w_n > 0$ for all $n \geq N$, then either $L(\varphi/2\pi) > q(1-\varepsilon)/2\pi$, or $L(\varphi/2\pi) \leq q(1-\varepsilon)/2\pi$ and this is witnessed by a rational approximation with denominator $n < N$.*

We now explain how to compute $L(\varphi/2\pi)$ to within arbitrary precision. Clearly it suffices to compute $2\pi L(\varphi/2\pi)$ to within arbitrary precision. Write $x = 2\pi L(\varphi/2\pi)$ and suppose we maintain a confidence interval $[a, b]$, that is, a pair of rational numbers $a, b$ such that $a \leq x \leq b$. Compute rational $\varepsilon \in (0, 1)$ and $q$ such that

$$a < q(1-\varepsilon) < \frac{q}{1-\varepsilon} < b. \tag{5.5}$$

Calculate also the threshold $N \in \mathbb{N}$ from $q, \varepsilon$. Write $A = q(1-\varepsilon)$ and $B = q/(1-\varepsilon)$.

First, we look for good approximations of $\varphi/2\pi$ with denominators smaller than $N$. Specifically, want to find witnesses $m/n$ to $x = 2\pi L(\varphi/2\pi) \leq A$ such that $n < N$. We consider separately every denominator $n < N$ and every numerator $m \leq n$. If we find a witness $m/n$ to $x \leq A$, then we continue the approximation procedure of $x$ with confidence interval $[a, A]$.

Notice that to check whether a rational $m/n$ witnesses $x \leq A$, we need to determine whether the inequality

$$|n\varphi - 2\pi m| \leq \frac{A}{n} \tag{5.6}$$

holds. Note that we can approximate $|n\varphi - 2\pi m|$ to within arbitrarily small additive error, obtaining as many bits of $|n\varphi - 2\pi m|$ as we need. Provided that (5.6) does not hold with equality, the approximation will eventually obtain sufficiently many bits of $|n\varphi - 2\pi m|$ to determine whether (5.6) is true, but if (5.6) happens to hold with equality, then no amount of precision will be sufficient. However, there is a simple workaround: choose a rational number $\varepsilon'$ such that $\varepsilon' < \varepsilon$ and inequality (5.5) is satisfied by $(q, \varepsilon')$ in place of $(q, \varepsilon)$. Write $A' = q(1-\varepsilon')$, clearly $A' > A$. For every pair of integers $m, n$ for which we wish to verify (5.6), we run two instances of the above approximation procedure in parallel, one with $(q, \varepsilon)$ and another with $(q, \varepsilon')$, until one terminates. Since $\varepsilon \neq \varepsilon'$, this is guaranteed to happen. Now, if the procedure with $(q, \varepsilon)$ terminates first, then we have successfully determined whether (5.6) is true, as desired. On the other hand, if the procedure with $(q, \varepsilon')$ terminates first, then there are two possibilities: either we have $|n\varphi - 2\pi m| > A'/n > A/n$, in which case (5.6) is false and we proceed to the next pair $(n, m)$, or we have $|n\varphi - 2\pi m| < A'/n$, in which case we conclude $x \leq A'$ and continue approximating $x$ with confidence interval $[a, A']$.

If we exhaust all denominators $n < N$ without finding a better upper bound for $x$ than $b$, then clearly there is no witness $n < N$ to $x \leq A$. We run a $PHP(4, 4)$ oracle on the $N$-th tails of the two sequences $\langle u_n \rangle_{n=0}^{\infty}$ and $\langle v_n \rangle_{n=0}^{\infty}$ to determine whether $w_n \leq 0$ for some $n \geq N$. If so, then by Lemma 39, we have $x \leq B$. Otherwise, Lemma 41 yields $x > A$. Then we continue to approximate $x$ recursively with confidence interval $[a, B]$ or $[A, b]$, depending on the outcome of the oracle query.

Notice that one can always choose $q, \varepsilon$ at each stage in such a way that the confidence interval shrinks by at least a fixed factor, whatever the outcome of the oracle invocations and the search for witnesses with small denominators. It follows therefore that $L(\varphi/2\pi)$ can be approximated to within arbitrary precision, completing the proof of Theorem 38.

## 5.4 Polyhedra of smaller dimension

### 5.4.1 Low dimension: reduction to Extended Orbit Problem

Our **PSPACE** results for $PHP(m, 1)$ and $PHP(m, 2)$ are based on a reduction to a generalisation of the Discrete Orbit Problem studied in Chapter 4. We call this generalisation the *Extended Discrete Orbit Problem*, and define it as follows: given a linear transformation $\boldsymbol{A} \in \mathbb{Q}^{m \times m}$, a vector $\boldsymbol{x} \in \mathbb{Q}^m$, a target $\mathbb{Q}$-vector space $\mathcal{V}$ defined by a basis $\{\boldsymbol{y_1}, \ldots, \boldsymbol{y_d}\} \subseteq \mathbb{Q}^m$ and a constraint matrix $\boldsymbol{B} \in \mathbb{Q}^{k \times d}$, determine whether there exists some exponent $n \in \mathbb{N}$ such that $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{V}$ and the witness coordinates $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_d)^T$ of $\boldsymbol{A}^n \boldsymbol{x}$ with respect to the basis $\{\boldsymbol{y_1}, \ldots, \boldsymbol{y_d}\}$ satisfy the conjunction of linear inequalities $\boldsymbol{B\kappa} \geq 0$.

In this section, we will show how to reduce $PHP(m, d)$ to the Extended Orbit Problem with ambient space $\mathbb{Q}^{m+1}$ and target vector space $\mathcal{V}$ of dimension $d+1$ in the cases $d = 1$ and $d = 2$. The reduction is polynomial-time when $d = 1$, and polynomial-space when $d = 2$. This, combined with the technical results of Section 5.5 is sufficient to establish membership in **PSPACE** for $PHP(m, d)$ for all $m$ and $d \in \{1, 2\}$.

**Lemma 42.** *$PHP(m, 1)$ reduces in polynomial time to the Extended Orbit Problem with ambient space $\mathbb{Q}^{m+1}$ and target vector space of dimension two.*

*Proof.* By Lemma 17, a one-dimensional polyhedron is of the form

$$\mathcal{P} = \{\boldsymbol{v_1} + \alpha \boldsymbol{v_2} : \alpha \in I\}, \text{ where } I = \mathbb{R},\ I = [0, 1] \text{ or } I = [0, \infty).$$

Moreover, this parametric representation is computable in polynomial time from the halfspace description of $\mathcal{P}$. Now consider the problem of determining whether $n \in \mathbb{N}$ and $\kappa_1, \kappa_2 \in \mathbb{Q}$ exist such that

$$\begin{bmatrix} \boldsymbol{A} & 0 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \boldsymbol{x} \\ 1 \end{bmatrix} = \kappa_1 \begin{bmatrix} \boldsymbol{v_1} \\ 1 \end{bmatrix} + \kappa_2 \begin{bmatrix} \boldsymbol{v_2} \\ 0 \end{bmatrix}.$$

Notice that the $(m+1)$-th component forces any witness to this problem instance to have $\kappa_1 = 1$. Therefore, further requiring $\kappa_2 \geq 0$ and $\kappa_1 - \kappa_2 \geq 0$, that is,

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \boldsymbol{\kappa} \geq 0,$$

renders this an instance of the Extended Orbit Problem which is positive if and only if the segment $\{\boldsymbol{v_1} + \kappa_2 \boldsymbol{v_2} : \kappa_2 \in [0, 1]\}$ intersects the orbit $\{\boldsymbol{A}^n \boldsymbol{x} : n \in \mathbb{N}\}$. Requiring instead only $\kappa_2 \geq 0$ gives the half-line $\{\boldsymbol{v_1} + \kappa_2 \boldsymbol{v_2} : \kappa_2 \in [0, \infty)\}$, whereas setting no restriction gives the whole line $\{\boldsymbol{v_1} + \kappa_2 \boldsymbol{v_2} : \kappa_2 \in \mathbb{R}\}$. In all cases, the resulting Extended Orbit instance has ambient space of dimension $m + 1$ and target vector space of dimension two, as required. □

**Lemma 43.** *$PHP(m, 2)$ reduces in polynomial space to the Extended Orbit Problem with ambient space $\mathbb{Q}^{m+1}$ and target vector space of dimension three.*

*Proof.* By Lemma 16, any two-dimensional polyhedron can be decomposed into a finite union of simple shapes: $P = \bigcup_{i=1}^{s} \mathcal{S}_i$ where

$$\mathcal{S}_i = \{\boldsymbol{v_{i_1}} + \alpha \boldsymbol{v_{i_2}} + \beta \boldsymbol{v_{i_3}} : \alpha \geq 0 \text{ and } \beta \geq 0 \text{ and } T(\alpha, \beta)\}$$

where the predicate $T$ is either $\alpha + \beta \leq 1$, or $\beta \leq 1$ or true. It is easy to see from the proof of Lemma 16 that $s \in 2^{\mathcal{O}(||\mathcal{P}||)}$, where $\|\mathcal{P}\|$ is the length of the description of $\mathcal{P}$. For each $i$, the problem of whether there exists $n$ such that $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{S}_i$ reduces to the Extended Orbit Problem with a three-dimensional target, analogously to the reduction shown by Lemma 42. For example, if the predicate $T_i$ is $\alpha + \beta \leq 1$, so that $\mathcal{S}_i$ is a triangle, then $\boldsymbol{A}^n \boldsymbol{x} \in \mathcal{S}_i$ if and only if there exist $\kappa_1, \kappa_2, \kappa_3 \in \mathbb{Q}$ such that $\kappa_2 \geq 0$, $\kappa_3 \geq 0$, $\kappa_1 - \kappa_2 - \kappa_3 \geq 0$ and

$$\begin{bmatrix} \boldsymbol{A} & 0 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \boldsymbol{x} \\ 1 \end{bmatrix} = \kappa_1 \begin{bmatrix} \boldsymbol{v_{i_1}} \\ 1 \end{bmatrix} + \kappa_2 \begin{bmatrix} \boldsymbol{v_{i_2}} \\ 0 \end{bmatrix} + \kappa_3 \begin{bmatrix} \boldsymbol{v_{i_3}} \\ 0 \end{bmatrix}.$$

The $(m+1)$-th component forces $\kappa_1 = 1$ and allows us to express the constraint $\kappa_2 + \kappa_3 \leq 1$ with the homogeneous inequality $\kappa_1 - \kappa_2 - \kappa_3 \geq 0$. The remaining possible choices of predicate $T$ reduce similarly. Thus, for the required polynomial-space reduction, it suffices to note that $\mathcal{P}$ is the union of at most exponentially many $\mathcal{S}_i$, so one may be chosen non-deterministically by Savitch's Theorem. □

### 5.4.2 High dimension: hardness for Skolem Problem

Now we proceed to give hardness results for the Polyhedron-Hitting Problem. First, observe that lower-dimensional versions of the Polyhedron-Hitting Problem reduce to higher-dimensional ones:

**Lemma 44.** *For all $m, d$ such that $m \geq d$, $PHP(m, d)$ reduces to $PHP(m+1, d)$ and to $PHP(m+1, d+1)$.*

*Proof.* Given $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, $\boldsymbol{x} \in \mathbb{Q}^m$ and a polyhedron $\mathcal{P} \subseteq \mathbb{Q}^m$ with $\dim(\mathcal{P}) = d$, we define the polyhedra $\mathcal{P}' = \{(\boldsymbol{t}, 0) \in \mathbb{Q}^{m+1} : \boldsymbol{t} \in \mathcal{P}\}$ and $\mathcal{P}'' = \{(\boldsymbol{t}, q) \in \mathbb{Q}^{m+1} : \boldsymbol{t} \in \mathcal{P}, q \in [0, 1]\}$. Note that $\dim(\mathcal{P}') = d$ and $\dim(\mathcal{P}'') = d + 1$. Then

$$\boldsymbol{A}^n\boldsymbol{x} \in \mathcal{P} \iff \begin{bmatrix} \boldsymbol{A} & 0 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \boldsymbol{x} \\ 0 \end{bmatrix} \in \mathcal{P}' \iff \begin{bmatrix} \boldsymbol{A} & 0 \\ 0 & 1 \end{bmatrix}^n \begin{bmatrix} \boldsymbol{x} \\ 1 \end{bmatrix} \in \mathcal{P}'',$$

which shows both reductions. □

Next, recall that the Discrete Skolem Problem is the problem of deciding reachability from a point to an $m-1$ dimensional vector subspace in $\mathbb{Q}^m$. This is a special case of $PHP(m, m-1)$: just take the target to be the polyhedron

$$\left\{ \boldsymbol{t} \in \mathbb{Q}^m : \begin{array}{rcl} \boldsymbol{n^T t} & \geq & 0 \\ \boldsymbol{-n^T t} & \geq & 0 \end{array} \right\},$$

where $\boldsymbol{n}$ is the normal of the target space. Therefore, the Discrete Skolem Problem for rational LRS of order $m$ reduces to $PHP(m, m-1)$. This observation, together with Lemma 44 yields the following:

**Lemma 45.** *For all $m, d$ with $m > d$, decidability of $PHP(m, d)$ would entail decidability of the Discrete Skolem Problem for LRS of order $d + 1$.*

Moreover, we can show that even the decidability of $PHP(4, 3)$ would entail decidability for the Discrete Skolem Problem for LRS of order five.

**Lemma 46.** *The Discrete Skolem Problem for LRS of order five reduces to $PHP(4, 3)$.*

*Proof.* As discussed in reference [Ouaknine and Worrell, 2012], the only outstanding case of the Skolem Problem for rational LRS of order five is when the LRS has five characteristic roots: two pairs of complex conjugates $\lambda_1, \overline{\lambda_1}$, $\lambda_2, \overline{\lambda_2}$ and a real root $\rho$, such that $|\lambda_1| = |\lambda_2| > |\rho| > 0$. Therefore, let $\langle u_n \rangle_{n=0}^{\infty}$ be such a sequence, given by

$$u_n = a\lambda_1^n + \overline{a\lambda_1^n} + b\lambda_2^n + \overline{b\lambda_2^n} + c\rho^n.$$

Define LRS of order four $\langle v_n \rangle_{n=0}^{\infty}$ by

$$v_n = \frac{a\lambda_1^n + \overline{a\lambda_1^n} + b\lambda_2^n + \overline{b\lambda_2^n}}{\rho^n}.$$

Let $\langle v_n \rangle_{n=0}^{\infty}$ be expressed in matrix form as $v_n = [0, 0, 0, 1]\boldsymbol{A}^n\boldsymbol{x}$, where $\boldsymbol{x}$ contains the initial values of $\langle v_n \rangle_{n=0}^{\infty}$. Now $u_n = 0$ if and only if $v_n = -c$, or equivalently, if there exist $\kappa_1, \kappa_2, \kappa_3$ such that

$$\boldsymbol{A}^n\boldsymbol{x} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ -c \end{bmatrix} + \kappa_1 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \kappa_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \kappa_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

The right-hand side describes a three-dimensional affine space, so the problem is clearly a special case of $PHP(4, 3)$. □

Then by Lemma 44, we have the required hardness result for $PHP(m, 3)$ for all $m \geq 4$.

## 5.5 Extended Orbit Problem

In this section, we study the *Extended Discrete Orbit Problem*. We are given a matrix $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, an initial point $\boldsymbol{x} \in \mathbb{Q}^m$, and a *target cone* specified by basis $\{\boldsymbol{y_1}, \ldots, \boldsymbol{y_d}\} \subseteq \mathbb{Q}^m$ and a constraint matrix $\boldsymbol{B} \in (\mathbb{R} \cap \mathbb{A})^{k\times d}$. The goal is to determine whether there exists an exponent $n \in \mathbb{N}$ and coordinates $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_d)^T \in \mathbb{Q}^d$ such that $\boldsymbol{A}^n\boldsymbol{x} = \sum_{i=1}^{d} \kappa_i \boldsymbol{y_i}$ and $\boldsymbol{B}\kappa \geq 0$. The reduction we showed in Section 5.4 yielded an integer constraint matrix $\boldsymbol{B}$, but for technical reasons, we study the problem in slightly greater generality and take $\boldsymbol{B}$ to be real algebraic. Our main decidability result concerning the Extended Orbit Problem is the following theorem, to which we devote the rest of this section.

**Theorem 47.** *The Extended Orbit Problem is in* **PTIME** *in the case* $d = 1$*, and in* **PSPACE** *in the cases* $d = 2$ *and* $d = 3$*.*

The first step is to adapt straightforwardly, mutatis mutandis, the reduction in Section 4.3, thereby reducing the Extended Orbit Problem to a generalisation of the matrix power problem with linear inequalities on the coefficients $\boldsymbol{\kappa}$: given $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$, $P_1, \ldots, P_d \in \mathbb{Q}[x]$ and $\boldsymbol{B}^{k\times d} \in \mathbb{R} \cap \mathbb{A}$, determine whether there exist $n \in \mathbb{N}$ and $\boldsymbol{\kappa} = (\kappa_1, \ldots, \kappa_d)^T \in \mathbb{Q}^d$ such that $\boldsymbol{A}^n = \sum_{i=1}^{d} \kappa_i P_i(\boldsymbol{A})$ and $\boldsymbol{B\kappa} \geq 0$.

Next, recall that $\boldsymbol{A}^n = \sum_i P_i(\boldsymbol{A})$ is equivalent to the system of equations (4.1). Putting this is conjunction with $\boldsymbol{B\kappa} \geq 0$ yields a *Master System* of equations and inequalities, whose unknowns are $n \in \mathbb{N}$ and $\kappa_1, \ldots, \kappa_d \in \mathbb{Q}$ and whose solutions are precisely the witnesses to our problem instance.

Recall the relation $\sim$ on the eigenvalues of $\boldsymbol{A}$, defined by $\alpha \sim \beta$ if and only if $\alpha/\beta$ is a root of unity. In Sections 4.5 and 4.6, we studied the equivalence classes of $\sim$. In particular, our analysis yielded Theorem 32, according to which for every instance of the Orbit Problem, there exists a bound $N$ which is exponential in the length of the description of the instance and such that if the instance is positive, then there exists a witness exponent $n$ with $n < N$.

In fact a stronger claim holds in the cases when the Master System is 'sufficiently large', though in the interest of clarity, we did not make this explicit in Chapter 4. For an equivalence class $C$ of $\sim$, let $mul(C)$ denote the maximum multiplicity of an eigenvalue of $\boldsymbol{A}$ in $C$, or equivalently, the maximum number of equations contributed to the Master System by an eigenvalue in $C$. Then the following can be recovered from Sections 4.4, 4.5, 4.6:

**Theorem 48.** *Suppose we are given* $\boldsymbol{A} \in \mathbb{Q}^{m\times m}$ *and* $P_1, \ldots, P_d \in \mathbb{Q}[x]$ *with* $d \leq 3$ *and write* $\|I\|$ *for the length of the description of the instance. If the sum of the multiplicities of the equivalence classes of* $\sim$ *is at least* $d+1$*, then there exists a bound* $N = 2^{\mathcal{O}(||I||)}$ *such that if* $\boldsymbol{A}^n \in span\{P_1(\boldsymbol{A}), \ldots, P_d(\boldsymbol{A})\}$*, then* $n < N$*. Further, if* $d = 1$*, then* $N = ||I||^{\mathcal{O}(1)}$*.*

This is a bound on *all* the witness exponents to a problem instance and derives from the analogous bounds for the zeros of non-degenerate LRS studied in Chapter 3. Indeed, if the premise of Theorem 48 holds, then it is possible to choose $d + 1$ equations from the Master System provided by eigenvalues unrelated by $\sim$, obtain a non-degenerate LRS over $\mathbb{R} \cap \mathbb{A}$ whose zeros are a superset of the witness exponents of the Orbit Problem instance, and hence bound all such exponents by Theorem 19.

It is clear that the witnesses of an Extended Orbit Problem instance are a strict subset of the witness set of the corresponding Orbit Problem instance obtained by omitting the constraint $\boldsymbol{B\kappa} \geq 0$, so Theorem 48 carries over directly to the Extended Orbit Problem. Then given the bound $N$ of Theorem 48, membership in **PSPACE** follows using a guess-and-check procedure identical to the one described in Section 5.3.1 for the Polyhedron-Hitting Problem in full dimension: guess an exponent $n$, express $\boldsymbol{A}^n = \sum_{i=1}^{d} \kappa_i P_i(\boldsymbol{A})$ and $\boldsymbol{B\kappa} \geq 0$ as an existential formula in the first-order theory $Th(\mathbb{R})$ of the real closed field, and check its validity in **PSPACE** by Theorem 13. In the case $d = 1$, the bound $N$ is polynomial in the size of the input, so it suffices to simply try all $n < N$ to obtain a polynomial-time algorithm.

Thus, all that remains is to show Theorem 47 for Extended Orbit instances with 'small' Master Systems, that is, instances where the sum of multiplicities of the equivalence classes of $\sim$ is at most $d$. In Sections 5.5.1, 5.5.3 and 5.5.4 below, we cover these remaining cases for $d = 1$, $d = 2$ and $d = 3$, respectively.

### 5.5.1 One-dimensional case

In the one-dimensional Extended Orbit Problem, we have to decide whether there exist some $n \in \mathbb{N}$ and $\kappa_1 \in \mathbb{Q}$ such that $\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A})$ and $\kappa_1 \geq 0$. We show this problem is in **PTIME**.

We assume the relation $\sim$ has only one equivalence class. Then the eigenvalues $\alpha_1, \ldots, \alpha_k$ of $\boldsymbol{A}$ may be written as $\{\alpha\omega_1, \ldots, \alpha\omega_k\}$ where $\omega_1, \ldots, \omega_k$ are effectively computable roots of unity and $\alpha \in \mathbb{R} \cap \mathbb{A}$ is the magnitude of the eigenvalues.

First, suppose each eigenvalue contributes exactly one equation to the Master System. Following the analysis of *Case II* in Section 4.4, we consider equations in pairs, and deduce that each pair is either

unsatisfiable, rendering the problem instance negative, or that it is equivalent to a linear congruence on $n$. Solving the conjunction of congruences using the Chinese Remainder Theorem, we see that the Master System reduces to:

$$\begin{aligned} n &\equiv t \bmod L \\ \kappa_1 &= \frac{\alpha_1^n}{P_1(\alpha_1)} = \frac{\alpha^n \omega_1^n}{P_1(\alpha_1)} \geq 0, \end{aligned}$$

where $L$ is the least common multiple of the orders of $\omega_1, \ldots, \omega_k$. Noting that the congruence on $n$ determines the value of $\omega_1^n$, we can calculate $\omega_1^n / P_1(\alpha_1) \in \mathbb{R} \cap \mathbb{A}$ directly and accept if it is non-negative, otherwise reject.

Second, suppose some eigenvalues contribute more than one equations to the Master System. Following the analysis of *Case III* in Section 4.4, this is similar to the previous case, with the exception that the exponent $n$ is limited to a single candidate value which must conform to a congruence modulo $L$. If $n$ satisfies the congruence, we proceed to determine the sign of $\kappa_1$ as above, otherwise the problem instance is negative.

### 5.5.2 Algebraic manipulation of the Master System

Before proceeding to showing the Extended Orbit Problem with $d = 2$ to be in **PSPACE**, we first recall a technique from Chapter 4.

Recall that equivalence classes of $\sim$ consist of pairs of conjugate classes, which are each other's image under complex conjugation, and individual self-conjugate classes, which are closed under complex conjugation. Self-conjugate classes may be written as

$$C = \{\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_s\}$$

where $\alpha \in \mathbb{R} \cap \mathbb{A}$ with $\alpha > 0$ is the magnitude of the eigenvalues, and $\omega_1, \ldots, \omega_s$ are roots of unity. We call $\alpha$ the representative of $C$. Pairs of conjugate classes are of the form

$$\begin{aligned} C &= \{\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_s\} \\ \overline{C} &= \{\overline{\alpha\omega_1}, \overline{\alpha\omega_2}, \ldots, \overline{\alpha\omega_s}\}, \end{aligned}$$

where $\alpha$ is complex algebraic and not a root unity. We call $\alpha, \overline{\alpha}$ are the representatives of $C, \overline{C}$, respectively.

Let $L$ be the least common multiple of all the orders of the ratios of eigenvalues of $\boldsymbol{A}$ which are roots of unity. Recall that if we fix the residue $r = n \bmod L$ and only look for witnesses whose exponents have this residue, the set of equations $Eq(C)$ contributed by eigenvalues in $C$ simplifies significantly. For example, consider $Eq(C, 0)$, the set of 0-th derivative equations contributed by $C = \{\alpha\omega_1, \alpha\omega_2, \ldots, \alpha\omega_s\}$:

$$\begin{aligned} (\alpha\omega_1)^n &= \sum_{i=1}^{d} \kappa_i P_i(\alpha\omega_1) \\ &\cdots \\ (\alpha\omega_s)^n &= \sum_{i=1}^{d} \kappa_i P_i(\alpha\omega_s) \end{aligned}$$

For a fixed residue of $n$ modulo $L$, $\omega_1^n, \ldots, \omega_s^n$ are also fixed, so each $P_i(\alpha\omega_j)/\omega_j^n$ is easily computable. Then this is equivalent to the conjunction of an equation with a linear system:

$$\alpha^n = \sum_{i=1}^{d} \kappa_i \frac{P_i(\alpha\omega_s)}{\omega_s^n} \text{ and } \boldsymbol{B'}\boldsymbol{\kappa} = 0, \tag{5.7}$$

where $\boldsymbol{B'}$ is an $(s-1) \times d$ matrix over $\mathbb{A}$ defined by

$$\boldsymbol{B'}_{j,i} = \frac{P_i(\alpha\omega_j)}{\omega_j^n} - \frac{P_i(\alpha\omega_{j+1})}{\omega_{j+1}^n}.$$

Writing $c_i$ for $P_i(\alpha\omega_s)/\omega_s^n$ and considering separately the real and imaginary parts of $\boldsymbol{B'\kappa} = 0$, we see that (5.7) is equivalent to

$$\alpha^n = c_1\kappa_1 + \cdots + c_d\kappa_d \text{ and } \boldsymbol{B''\kappa} = 0,$$

where

$$\boldsymbol{B''} = \begin{bmatrix} \Re(\boldsymbol{B'}) \\ \Im(\boldsymbol{B'}) \end{bmatrix}$$

is a $2(s-1) \times d$ matrix over $\mathbb{R} \cap \mathbb{A}$. If the nullspace of $\boldsymbol{B''}$ is not $(\mathbb{R} \cap \mathbb{A})^d$, then there exists a linear dependence with real algebraic coefficients between the components of $\boldsymbol{\kappa}$: $\psi_1\kappa_1 + \cdots + \psi_d\kappa_d = 0$, where $\psi_1, \ldots, \psi_d \in \mathbb{R} \cap \mathbb{A}$. Therefore, we can eliminate some coefficient $\kappa_i$, replacing all of its occurrences, including in the inequalities including in the linear inequalities $\boldsymbol{B\kappa} \geq 0$. This yields a Master System of dimension $d-1$ which we proceed to solve inductively subject to $n \bmod L = r$.

Therefore, we can assume that the column rank of $\boldsymbol{B''}$ is zero, so the constraint $\boldsymbol{B''\kappa} = 0$ is satisfied by all vectors $\boldsymbol{\kappa}$. Thus, for this particular residue of $n$ modulo $L$, the equations $Eq(C, 0)$ are equivalent to the single equation $\alpha^n = c_1\kappa_1 + \cdots + c_d\kappa_d$. Further, if the equivalence class $C$ is self-conjugate, then $\alpha \in \mathbb{R} \cap \mathbb{A}$, so we may replace each $c_i$ with its real part and assume $c_i \in \mathbb{R} \cap \mathbb{A}$. On the other hand, we if we have a pair of conjugate classes, then $Eq(C, 0)$ and $Eq(\overline{C}, 0)$ together reduce to $\alpha^n = c_1\kappa_1 + \cdots + c_d\kappa_d$ with complex $c_1, \ldots, c_d$. Similarly, for $j > 0$ and a fixed residue of $n$ modulo $L$, the equations $Eq(C, j)$ reduce to the equivalent single equation

$$n(n-1)\ldots(n-j+1)\alpha^{n-j} = \sum_{i=1}^{d} c_i\kappa_i.$$

### 5.5.3 Two-dimensional case

Now suppose we have a problem instance $(\boldsymbol{A}, \boldsymbol{B}, P_1, P_2)$ and we have to determine whether there exist an exponent $n \in \mathbb{N}$ and coefficients $\boldsymbol{\kappa} = (\kappa_1, \kappa_2)^T \in \mathbb{Q}^2$ such that

$$\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A}) + \kappa_2 P_2(\boldsymbol{A}) \text{ and } \boldsymbol{B\kappa} \geq 0.$$

We can restrict our attention to problem instances where the sum of the multiplicities of the equivalence classes of $\sim$ is at most 2. In each case, we will proceed by case analysis on $r = n \bmod L$. For each $r$, we use the technique of Section 5.5.2 to reduce the Master System to a system based on the representatives of the equivalence classes of $\sim$. Unlike in Chapter 4, however, where this case analysis was merely a proof device, here we will explicitly require that the algorithm consider each $r$ in turn, perform the operations described in Section 5.5.2 to simplify the Master System, and then proceed as below. This can all be done in **PSPACE**.

*Case I.* Suppose $\sim$ has only one equivalence class and its multiplicity is 1. For a fixed residue, the Master System reduces to

$$\alpha^n = \kappa_1 c_1 + \kappa_2 c_2 \text{ and } \boldsymbol{B\kappa} \geq 0, \tag{5.8}$$

where $\alpha, c_1, c_2 \in \mathbb{R} \cap \mathbb{A}$ and $\alpha > 0$. Now observe that either all values of $n$ satisfy (5.8), or no value of $n$ does. Indeed, if $n$ is a witness with coefficients $(\kappa_1, \kappa_2)$, then $n+1$ and $n-1$ are also witnesses, with coefficients $(\kappa_1\alpha, \kappa_2\alpha)$ and $(\kappa_1/\alpha, \kappa_2/\alpha)$, respectively. Therefore, it suffices to try $n = 0$. This leads to a conjunction of the equation $1 = \kappa_1 c_1 + \kappa_2 c_2$ with the inequalities $\boldsymbol{B\kappa}$, which is easy to solve.

*Case II.* Suppose that $\sim$ has two equivalence classes, both of multiplicity 1. Proceed by case analysis on the residue of $n$ and reduce the Master System to

$$\begin{bmatrix} \alpha^n \\ \beta^n \end{bmatrix} = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix} \begin{bmatrix} \kappa_1 \\ \kappa_2 \end{bmatrix} \text{ and } \boldsymbol{B\kappa} \geq 0. \tag{5.9}$$

If the equivalence classes are both self-conjugate, then $c_1, \ldots, c_4, \alpha, \beta$ are all real algebraic, otherwise $c_3 = \overline{c_1}$, $c_4 = \overline{c_2}$ and $\alpha = \overline{\beta}$. If the $2 \times 2$ matrix in (5.9) is invertible, then multiplying by its inverse yields

$$\begin{bmatrix} \kappa_1 \\ \kappa_2 \end{bmatrix} = \begin{bmatrix} \psi_1 & \psi_2 \\ \psi_3 & \psi_4 \end{bmatrix} \begin{bmatrix} \alpha^n \\ \beta^n \end{bmatrix} \text{ and } \boldsymbol{B\kappa} \geq 0,$$

where either $\psi_1, \ldots, \psi_4$ are real, or $\psi_2 = \overline{\psi_1}$ and $\psi_4 = \overline{\psi_3}$. Now observe that $\kappa_1, \kappa_2$ satisfy a linear recurrence formula with characteristic equation $(x - \alpha)(x - \beta) = 0$. Then $\boldsymbol{B\kappa}$ is a vector of linear recurrence sequences over $\mathbb{R} \cap \mathbb{A}$. Each sequence $\langle u_n^{(j)} \rangle_{n=0}^{\infty}$ has order at most 2 and is given by

$$u_n^{(j)} = a_j \alpha^n + b_j \beta^n,$$

where $a_j, b_j \in \mathbb{R} \cap \mathbb{A}$. These LRS all satisfy the same shared recurrence formula. Further, observe that they are non-degenerate, since $\alpha/\beta$ is not a root of unity. Therefore, for this particular residue of $n$, the problem instance reduces to the Simultaneous Non-negativity Problem for sequences of order at most 2, which is in **PSPACE** by Theorem 34.

Notice that here we are actually reducing to a slight generalisation of the Simultaneous Non-negativity Problem: not only do we look for $n$ such that the $n$-th terms of the given LRS are non-negative, but we also require that $n$ satisfy a congruence $n \bmod L = r$, for $r, L$ provided as inputs. This problem, however, is decided by the same decision procedure as the one already presented. Indeed, our method in Section 5.3.1 can terminate in two different ways. First, it could obtain a bound $N$ such that any witness $n$ satisfies $n < N$, and then resort to a guess-and-check procedure. This part of the argument remains unaltered by the introduction of the constraint $n \bmod L = r$. Second, it could determine that any 'large' $n$ such that $\lambda^n \in \mathcal{A}$ is a witness, where $\lambda \in \mathbb{A}$ is an algebraic number on the unit circle which is not a root of unity, and $\mathcal{A}$ is a non-trivial arc on the unit circle. Then density of $\{\lambda^n : n \in \mathbb{N}\}$ on the unit circle by Theorem 11 (Kronecker) guarantees there are infinitely many such witnesses, so the problem instance is positive. This reasoning also remains unaltered by the introduction of the extra constraint, since $\{\lambda^{kL+r} : k \in \mathbb{N}\}$ is also dense in the unit circle.

Finally, if the $2 \times 2$ matrix in (5.9) is singular, then there is a non-trivial linear combination of the rows which equates to zero. Then the same linear combination of $\alpha^n, \beta^n$ equals zero. This yields a non-degenerate LRS of order 2 which must vanish at $n$, so a bound on $n$ follows from Theorem 19.

*Case III.* The last remaining case is when there is one equivalence class of $\sim$ and it has multiplicity 2. This reduces to the Simultaneous Non-negativity Problem in the same way as the previous case, but the resulting recurrence sequences have characteristic equation $(x - \alpha)^2 = 0$ and are given by $u_n^{(j)} = (a_j + b_j n)\alpha^n$ for $a_j, b_j \in \mathbb{R} \cap \mathbb{A}$.

### 5.5.4 Three-dimensional case

Now suppose we have a problem instance $(\boldsymbol{A}, \boldsymbol{B}, P_1, P_2, P_3)$ and we have to determine whether there exist an exponent $n \in \mathbb{N}$ and coefficients $\boldsymbol{\kappa} = (\kappa_1, \kappa_2, \kappa_3)^T \in \mathbb{Q}^3$ such that

$$\boldsymbol{A}^n = \kappa_1 P_1(\boldsymbol{A}) + \kappa_2 P_2(\boldsymbol{A}) + \kappa_3 P_3(\boldsymbol{A}) \text{ and } \boldsymbol{B\kappa} \geq 0.$$

We only consider instances where the sum of the multiplicities of the equivalence classes of $\sim$ is at most 3. In each case, we will proceed by case analysis on $r = n \bmod L$. For each $r$, we use the technique of Section 5.5.2 to reduce the Master System to a system based on the representatives of the equivalence classes of $\sim$.

*Case I.* Suppose there are exactly three equivalence classes, each of multiplicity 1. Then one class must necessarily be self-conjugate whereas the other two can be either self-conjugate or each other's conjugates. Either way, this case is analogous to the case of two simple equivalence classes in the two-dimensional version. For each fixed residue $r$ of $n$, we simplify the Master System and obtain:

$$\begin{bmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{bmatrix} = \boldsymbol{T\kappa} \text{ and } \boldsymbol{B\kappa} \geq 0, \tag{5.10}$$

where $\boldsymbol{T}$ is a $3 \times 3$ matrix over $\mathbb{R} \cap \mathbb{A}$. If $\boldsymbol{T}$ is invertible, then we multiply both sides of (5.10) by $\boldsymbol{T^{-1}}$ and see that $\kappa_1, \kappa_2, \kappa_3$ are linear recurrence sequences over $\mathbb{R} \cap \mathbb{A}$ with characteristic roots $\alpha, \beta, \gamma$. Then the left-hand side of each linear inequality $\boldsymbol{B\kappa} \geq 0$ is also an LRS over $\mathbb{R} \cap \mathbb{A}$ and has order 3. Thus the problem instance reduces to the Simultaneous Non-negativity Problem for LRS of order 3 over $\mathbb{R} \cap \mathbb{A}$. On the other hand, if $\boldsymbol{T}$ is singular, then a linear combination of its rows is zero, so the same linear combination of $\alpha^n, \beta^n, \gamma^n$ is also zero. Noting that no two of $\alpha, \beta, \gamma$ are related by $\sim$, we obtain a bound on $n$ from Theorem 19.

*Case II.* Next, suppose $\sim$ has two equivalence classes, one of multiplicity 1 and the other of multiplicity 2. This is analogous to the previous case. For a fixed residue of $n$ modulo $L$, the Master System is equivalent to

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \\ \beta^n \end{bmatrix} = \boldsymbol{T}\boldsymbol{\kappa} \text{ and } \boldsymbol{B}\boldsymbol{\kappa} \geq 0, \tag{5.11}$$

where $\boldsymbol{T}$ is a $3 \times 3$ matrix over $\mathbb{R} \cap \mathbb{A}$. Now if $\boldsymbol{T}$ is invertible, then we multiply both sides of (5.11) by $\boldsymbol{T^{-1}}$ and see that each of $\kappa_1, \kappa_2, \kappa_3$ is a linear recurrence sequence over $\mathbb{R} \cap \mathbb{A}$ with characteristic equation $(x-\alpha)^2(x-\beta) = 0$. Substituting into the homogeneous linear inequalities $\boldsymbol{B}\boldsymbol{\kappa} \geq 0$, we now have an instance of the Simultaneous Non-negativity Problem for LRS of order 3 with a repeated characteristic root. If $\boldsymbol{T}$ is singular, then a linear combination of $\alpha^n$, $n\alpha^{n-1}$ and $\beta^n$ must equal zero, so a bound on $n$ follows from Theorem 19, because the ratio of $\alpha$ and $\beta$ is not a root of unity.

*Case III.* Suppose now that $\sim$ has only one equivalence class and its multiplicity is 1. The situation is analogous to the same case in the two-dimensional version. We have to find $n, \kappa_1, \kappa_2, \kappa_3$ such that

$$\alpha^n = \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3 \text{ and } \boldsymbol{B}\boldsymbol{\kappa} \geq 0.$$

We observe that either all $n$ are witnesses to the problem instance, or none are, so it suffices to consider $n = 0$, reducing the problem to a conjunction of the linear inequalities $\boldsymbol{B}\boldsymbol{\kappa} \geq 0$ with the equation $1 = \kappa_1 c_1 + \kappa_2 c_2 + \kappa_3 c_3$.

*Case IV.* Let $\sim$ have two equivalence classes, both of multiplicity 1. For a fixed residue of $n$ modulo $L$, the Master System simplifies to

$$\begin{bmatrix} \alpha^n \\ \beta^n \end{bmatrix} = \boldsymbol{T}\boldsymbol{\kappa} \text{ and } \boldsymbol{B}\boldsymbol{\kappa} \geq 0, \tag{5.12}$$

where $\boldsymbol{T}$ is a $2 \times 3$ matrix. All the numbers involved are algebraic. There are two possibilities: either $\alpha$, $\beta$ and the entries of $\boldsymbol{T}$ are in $\mathbb{R} \cap \mathbb{A}$, or $\alpha = \overline{\beta}$ and the second row of $\boldsymbol{T}$ is the complex conjugate of the first row.

We consider the real and the complex cases separately. First, suppose $\boldsymbol{T}, \alpha, \beta$ are real. The dimension of the column space of $\boldsymbol{T}$ is 0, 1 or 2. If the dimension of the column space is 0, then the Master System is unsatisfiable, since $\boldsymbol{T}$ maps everything to zero, whereas $\alpha^n$ and $\beta^n$ cannot be zero. If the dimension of the column space of $\boldsymbol{T}$ is 1, then it is spanned by a single vector $(t_1, t_2) \in (\mathbb{R} \cap \mathbb{A})^2$, so for any witness $n$, $(\alpha^n, \beta^n)$ must be collinear with $(t_1, t_2)$. If at least one of $t_1, t_2$ is zero, then (5.12) is unsatisfiable, because $\alpha, \beta \neq 0$. Otherwise, we can conclude that $(\alpha/\beta)^n = t_1/t_2$. Since $\alpha/\beta$ is not a root of unity, a bound on $n$ which is polynomial in the length of the input follows from Theorem 19.

Assume therefore that the dimension of the column space of $\boldsymbol{T}$ is 2. Each of the inequalities $\boldsymbol{B}\boldsymbol{\kappa} \geq 0$ specifies that $(\kappa_1, \kappa_2, \kappa_3)$ lies in a halfspace $\mathcal{H}_j$ of $\mathbb{R}^3$. By Lemma 49 below, the image of each $\mathcal{H}_j$ under $\boldsymbol{T}$ can be the entire plane $\mathbb{R}^2$ or a halfplane with boundary line going through the origin. A description of each image $\boldsymbol{T}(\mathcal{H}_j)$ is easy to calculate in polynomial time. Then $n$ is a witness to (5.12) if and only if $(\alpha^n, \beta^n) \in \cap_j \boldsymbol{T}(\mathcal{H}_j)$. We can clearly discard from the conjunction all $j$ such that $\boldsymbol{T}(\mathcal{H}_j) = \mathbb{R}^2$, leaving a conjunction of halfplanes $\{(x, y) : A_j x + B_j y \geq 0\}$ with effectively computable $A_j, B_j \in \mathbb{R} \cap \mathbb{A}$. Thus, we have to determine whether there exists $n \in \mathbb{N}$ such that $A_j \alpha^n + B_j \beta^n \geq 0$ for all $j$. This is an instance of the Simultaneous Non-negativity Problem for LRS of order 2 over $\mathbb{R} \cap \mathbb{A}$ with common characteristic polynomial $(x-\alpha)(x-\beta)$, so we are done by Theorem 34.

Suppose now that $\alpha = \overline{\beta}$ and $\boldsymbol{T}$ is of the form

$$\boldsymbol{T} = \begin{bmatrix} a & b & c \\ \overline{a} & \overline{b} & \overline{c} \end{bmatrix}.$$

We may freely replace $\alpha, \beta$ by $\alpha/|\alpha|$ and $\beta/|\alpha|$: indeed, $(n, \kappa_1, \kappa_2, \kappa_3)$ is a witness to the original problem instance if and only if $(n, \kappa_1/|\alpha|^n, \kappa_2/|\alpha|^n, \kappa_3/|\alpha|^n)$ is a witness to the modified problem instance. Thus, assume without loss of generality that $|\alpha| = |\beta| = 1$. Let $\boldsymbol{T'} \in \mathbb{R}^{2\times 3}$ be the matrix

$$\boldsymbol{T'} = \begin{bmatrix} \Re(a) & \Re(b) & \Re(c) \\ \Im(a) & \Im(b) & \Im(c) \end{bmatrix}.$$

Then clearly (5.12) is equivalent to:

$$\begin{bmatrix} \Re(\alpha^n) \\ \Im(\alpha^n) \end{bmatrix} = \boldsymbol{T'}\boldsymbol{\kappa} \text{ and } \boldsymbol{B}\boldsymbol{\kappa} \geq 0.$$

We now proceed as in the real case. The rank of $\boldsymbol{T'}$ is 1 or 2. First, if $\text{rank}(\boldsymbol{T'}) = 1$, then the column space of $\boldsymbol{T'}$ is spanned by a single unit vector $(t_1, t_2) \in \mathbb{R}^2$. If $t_1 = 0$ or $t_2 = 0$, then the problem instance is negative, since $\Re(\alpha^n) = 0$ or $\Im(\alpha^n) = 0$ would entail $\alpha$ is a root of unity, which is a contradiction. Otherwise, we must have $\alpha^n = \pm(t_1 + it_2)$, so a bound on $n$ follows from Theorem 19 and we are done.

Now assume $\text{rank}(\boldsymbol{T'}) = 2$. Write $\mathcal{H}_j$ for the halfspaces in $\mathbb{R}^3$ defined by the linear inequalities $\boldsymbol{B\kappa}$. The problem instance is positive if and only if there exists $n$ such that $(\Re(\alpha^n), \Im(\alpha^n)) \in \mathcal{H} = \cap_j \boldsymbol{T'}(\mathcal{H}_j)$. By Lemma 49, the image under $\boldsymbol{T'}$ of each halfspace $\mathcal{H}_j$ is either the entire plane $\mathbb{R}^2$, or a halfplane whose boundary contains the origin. Then the intersection $\mathcal{H}$, if non-empty, is one of the following: the cone of two vectors in $\mathbb{R}^2$, one or two halflines starting at the origin, a halfplane with boundary containing the origin, or all of $\mathbb{R}^2$. Hence, the intersection of $\mathcal{H}$ with the unit circle $\mathcal{O}$ is either empty, or up to two individual points, or an arc. Further, this intersection is easy to compute explicitly in polynomial time. If $\mathcal{H} \cap \mathcal{O} = \emptyset$, then the problem instance is negative, since $\alpha^n \in \mathcal{O}$ for all $n$. If $\mathcal{H} \cap \mathcal{O}$ is an arc, then the problem instance is positive, since $\alpha$ is not a root of unity, so by Theorem 11 (Kronecker), $\{\alpha^n : n \in \mathbb{N}\}$ is dense in $\mathcal{O}$. Finally, if $\mathcal{H} \cap \mathcal{O}$ is of the form $\{z_1\}$ or $\{z_1, z_2\}$ for some $z_1, z_2 \in \mathbb{A}$, then a polynomially large bound on $n$ follows from Theorem 19, so we are done.

**Lemma 49.** *Let $\mathcal{H}$ be a halfspace in $\mathbb{R}^3$ whose defining plane contains the origin and let $\boldsymbol{T} \in \mathbb{R}^{2\times 3}$ with $\boldsymbol{T} \neq \boldsymbol{0}$. If rank$(\boldsymbol{T}) = 1$, then the image of $\mathcal{H}$ under $\boldsymbol{T}$ is a line through the origin or a halfline with the origin as its endpoint. Otherwise, if rank$(\boldsymbol{T}) = 2$, then the image of $\mathcal{H}$ under $\boldsymbol{T}$ is either all of $\mathbb{R}^2$ or a halfplane in $\mathbb{R}^2$ whose defining line contains the origin.*

*Proof.* The halfspace $\mathcal{H}$ may be written as

$$\mathcal{H} = \{x\boldsymbol{v_1} + y\boldsymbol{v_2} + z\boldsymbol{v_3} : x, y, z \in \mathbb{R} \text{ and } z \geq 0\},$$

where $\boldsymbol{v_1}, \boldsymbol{v_2}, \boldsymbol{v_3} \in \mathbb{R}^3$ are linearly independent. Writing $\boldsymbol{V} \in \mathbb{R}^{3\times 3}$ for the matrix with columns $\boldsymbol{v_1}, \boldsymbol{v_2}, \boldsymbol{v_3}$, we have $\dim(\textit{span}\{\boldsymbol{Tv_1}, \boldsymbol{Tv_2}, \boldsymbol{Tv_3}\}) = \text{rank}(\boldsymbol{TV}) = \text{rank}(\boldsymbol{T})$, since $\boldsymbol{V}$ is invertible by the linear independence of $\boldsymbol{v_1}, \boldsymbol{v_2}, \boldsymbol{v_3}$.

Since $\boldsymbol{T}$ is non-zero, we have $\text{rank}(\boldsymbol{T}) \in \{1, 2\}$. If $\text{rank}(\boldsymbol{T}) = 1$, then $\boldsymbol{Tv_1}, \boldsymbol{Tv_2}, \boldsymbol{Tv_3}$ all have the same direction $\boldsymbol{u}$ and there are two possibilities for $\boldsymbol{T}(\mathcal{H})$. If $\boldsymbol{Tv_1} = \boldsymbol{Tv_2} = \boldsymbol{0}$, then $\boldsymbol{T}(\mathcal{H}) = \{z\boldsymbol{u} : z \geq 0\}$ is a halfline starting at the origin, otherwise $\boldsymbol{T}(\mathcal{H}) = \{z\boldsymbol{u} : z \in \mathbb{R}\}$ is a line through the origin.

Now suppose the rank of $\boldsymbol{T}$ is 2. If $\{\boldsymbol{Tv_j}, \boldsymbol{Tv_3}\}$ with $j \in \{1, 2\}$ is a basis for $\textit{span}\{\boldsymbol{Tv_1}, \boldsymbol{Tv_2}, \boldsymbol{Tv_3}\}$, then

$$\mathcal{H} = \{x\boldsymbol{Tv_j} + z\boldsymbol{Tv_3} : x, z \in \mathbb{R} \text{ and } z \geq 0\},$$

which is a halfplane whose bounding line contains the origin. On the other hand, if $\{\boldsymbol{Tv_1}, \boldsymbol{Tv_2}\}$ is a basis for $\textit{span}\{\boldsymbol{Tv_1}, \boldsymbol{Tv_2}, \boldsymbol{Tv_3}\}$, then

$$\mathcal{H} = \{x\boldsymbol{Tv_1} + y\boldsymbol{Tv_2} : x, y \in \mathbb{R}\},$$

which is the whole plane $\mathbb{R}^2$. □

*Case V.* Finally, suppose $\sim$ has a single equivalence class and its multiplicity is 2. Then for a fixed residue of $n$ modulo $L$, the Master System simplifies to

$$\begin{bmatrix} \alpha^n \\ n\alpha^{n-1} \end{bmatrix} = \boldsymbol{T\kappa} \text{ and } \boldsymbol{B\kappa} \geq 0,$$

where $\alpha$ and $T$ are both real algebraic. This case is solved analogously to *Case IV* for a real $\boldsymbol{T}$ and reduces to the Simultaneous Non-negativity Problem for LRS with characteristic equation $(x - \alpha)^2 = 0$.

# Chapter 6

# Continuous Skolem Problem

*Prerequisites:* Sections 2.1.1, 2.1.3, 2.2.1 and 2.3.2.

## 6.1 Introduction

We now move to reachability problems for continuous-time linear dynamical systems, some examples of which amongst many are linear hybrid automata and continuous-time Markov chains [Alur, 2015]. At any given time $t \geq 0$, such systems have state $\boldsymbol{x}(t) \in \mathbb{R}^m$, with continuous dynamics determined by linear differential equations of the form $\boldsymbol{x'}(t) = \boldsymbol{A}\boldsymbol{x}(t)$, where $\boldsymbol{A} \in \mathbb{R}^{m \times m}$. Many natural reachability questions arise in this context. For example, one can ask whether the continuous flow of a hybrid automaton in a given location leads to a particular transition guard being satisfied. Time-bounded versions of such reachability problems are also of considerable interest.

In this chapter, we study a fundamental reachability question on continuous-time linear dynamical systems, the *Continuous Skolem Problem*: given $\boldsymbol{x}(0), \boldsymbol{u} \in \mathbb{R}^m$, $\boldsymbol{A} \in \mathbb{R}^{m \times m}$ and a (bounded or unbounded) interval $I \subseteq \mathbb{R}_{\geq 0}$, determine whether there exists $t \in I$ such that at time $t$, the state $\boldsymbol{x}(t)$ of the linear dynamical system $(\boldsymbol{A}, \boldsymbol{x}(0))$ lies in the $(m-1)$-dimensional subspace $\{\boldsymbol{y} \in \mathbb{R}^m : \boldsymbol{u}^T \boldsymbol{y} = 0\}$. Based on the boundedness of $I$, we distinguish two subproblems, respectively the *Bounded* and the *Unbounded* Continuous Skolem Problem. For the purposes of representing the input data effectively, we will assume that the (one or two) endpoints of $I$ are rational, whilst the vectors $\boldsymbol{x}(0), \boldsymbol{u}$ and the matrix $\boldsymbol{A}$ are real algebraic, with all entries described using the representation given in Section 2.1.1.

Using the well-known closed-form solution for $\boldsymbol{x}(t)$, we see the problem may equivalently be stated as determining whether the function $f(t) = \boldsymbol{u}^{\boldsymbol{T}} e^{\boldsymbol{A}t} \boldsymbol{x}(0)$ has a zero in the interval $I$. As shown in Section 2.3.2, functions of this form are precisely the real-valued exponential polynomials. Thus, an equivalent formulation of the Continuous Skolem Problem is, given an interval $I \subseteq \mathbb{R}_{\geq 0}$ with rational endpoints, a differential equation

$$f^{(m)} + a_{m-1} f^{(m-1)} + \ldots + a_0 f = 0 \tag{6.1}$$

with $a_0, \ldots, a_{m-1} \in \mathbb{R} \cap \mathbb{A}$, and initial conditions $f(0), \ldots, f^{(m-1)}(0) \in \mathbb{R} \cap \mathbb{A}$, determine whether the unique solution $f : \mathbb{R}_{\geq 0} \to \mathbb{R}$ of (6.1) which satisfies the initial conditions has a zero in $I$. The order of the differential equation (6.1) in this formulation matches the dimension of $\boldsymbol{A}$ in the matrix formulation.

Observe that the Continuous Skolem Problem can be viewed as a continuous-time analogue of the Discrete Skolem Problem studied in Chapter 3, hence motivating the nomenclature. Both problems formulate reachability questions for linear dynamical systems from a single initial point to a target vector subspace of dimension $m-1$ in $\mathbb{R}^m$. Equivalently, the two problems pose the question of existence of zeros for functions satisfying two closely-related classes of equations: linear difference equations and ordinary differential equations.

Decidability is currently open for the Continuous Skolem Problem, as well as its bounded and unbounded subproblems, with the bounded case cited as an outstanding problem in [Bell et al., 2010, Open Problem 17]. The same paper gives some partial decidability results which all require strong assumptions

on the matrix $\boldsymbol{A}$ in the equation $\boldsymbol{x}'(t) = \boldsymbol{A}\boldsymbol{x}(t)$, for example that $\boldsymbol{A}$ be a Metzler matrix or that $\boldsymbol{A}$ have dimension 2. Under similarly restrictive spectral assumptions on $\boldsymbol{A}$, Theorem 14 of the same paper shows how to reduce the Continuous Skolem Problem to the bounded subproblem. The reachability problem for linear flows $\boldsymbol{x}'(t) = \boldsymbol{A}\boldsymbol{x}(t)$ has also been considered under the framework of o-minimal hybrid systems [Lafferriere et al., 2001, Corollary 3.10]. Here again one requires strong spectral assumptions on $\boldsymbol{A}$ to obtain decidability, such as that $\boldsymbol{A}$ be nilpotent or that its spectrum be either entirely real or entirely imaginary.

## 6.2 Main result and outline

This chapter is based on our recent work [Chonev et al., 2015a] and presents two main results. First, in Section 6.3 we show a conditional decidability result for the bounded subproblem:

**Theorem 50.** *If Schanuel's Conjecture is true, then the Bounded Continuous Skolem Problem is decidable for exponential polynomials of all orders. Further, for exponential polynomials of order at most* 3*, the problem is decidable unconditionally.*

Schanuel's Conjecture is a unifying conjecture in transcendental number theory, generalising both the Lindemann-Weierstrass Theorem and Baker's Theorem on linear independence of logarithms of algebraic numbers. A celebrated paper of MacIntyre and Wilkie [Macintyre and Wilkie, 1996] obtains decidability of the first-order theory of the real exponential field, assuming Schanuel's Conjecture. While this result is relevant to the present chapter, we emphasize that we are concerned here with complex exponentiation. Schanuel's Conjecture is also invoked in the analysis of exponential polynomials in [D'Aquino et al., 2014, Zilber, 2002], although not in the context of decidability.

Intuitively, decidability of the Bounded Continuous Skolem Problem is non-trivial because an exponential polynomial $f$ can approach 0 tangentially. It is not obvious *a priori* how to confirm the existence of a tangential zero by finite-precision numerical computation. Moreover it is clear that tangential zeros can arise: a very simple example is the exponential polynomial $f(t) = 2 + 2\cos(t)$. Note that in this case $f$ can be written as a product of complex-valued exponential polynomials $f(t) = (1 + e^{it})(1 + e^{-it})$, with the two factors having common zeros. More generally, assuming Schanuel's Conjecture, we show that any exponential polynomial admits a factorisation such that the zeros of each factor can be detected using finite-precision numerical computations. Our method however does not enable us to bound the precision required to find zeros, so, as yet, we have no complexity upper bound for our procedure.

In Section 6.3.1, we give details of a procedure for determining the existence of zeros of a differentiable real-valued function with bounded derivative and no tangential zeros in an interval of interest. The method samples the function over the given interval with increasingly small step-size, seeking to detect a change of sign and using the bound on the derivative to determine when to terminate and conclude there are no zeros to be found. In Sections 6.3.2, we introduce the ring of Laurent polynomials and briefly study elements of the ring which are associates with their complex conjugates. Then in Sections 6.3.3 and 6.3.4, we use Schanuel's Conjecture to show the given exponential polynomial factorises in this ring into exponential polynomials with no tangential zeros. Since the factors may be complex-valued, as in the example above, from each factor we obtain a real-valued function with the same zero set and no tangential zeros, in order to apply the procedure of Section 6.3.1 and to complete the decision method. Finally, in Section 6.3.5, we observe that for exponential polynomials of order at most 3, one may eschew Schanuel's Conjecture in favour of a much simpler argument from the Gelfond-Schneider Theorem to eliminate tangential zeros as a concern and obtain unconditional decidability.

For our second main result, in Section 6.4, we show by way of hardness that decidability of the unbounded subproblem would entail a major new effectiveness result in Diophantine approximation:

**Theorem 51.** *If the Unbounded Continuous Skolem Problem is decidable for exponential polynomials of order* 9*, even with the input interval fixed to be* $[0, \infty)$*, then the homogeneous Diophantine approximation type* $L(x)$ *is computable for all real algebraic numbers* $x$*, in the sense that* $L(x)$ *may be approximated to within arbitrary precision.*

As we have discussed in Section 2.2, currently almost nothing is known about the homogeneous Diophantine approximation type of numbers of degree three or higher, rendering this a significant barrier

to decidability. Now one possibility is that all such numbers $L(a)$ are zero, and hence trivially computable. However the significance of Theorem 51 is that in order to prove the decidability of the Continuous Skolem Problem one would have to establish, *one way or another*, the computability of $L(a)$ for every real algebraic number $a$.

Notice the similarity to our Diophantine hardness result for the Discrete Polyhedron-Hitting Problem (Theorem 38) and to the hardness result of [Ouaknine and Worrell, 2014b, Theorem 5.2]. Both of these results show that computability of $L(\varphi/2\pi)$ for all arguments $\varphi$ of Gaussian rationals would follow from the decidability of problems concerning the non-negativity of LRS, which in turn correspond to reachability to halfspace targets for discrete-time linear dynamical systems. No such connection is known for the Discrete Skolem Problem and thus for reachability to whole spaces. In the present setting, however, continuity renders the two types of problems essentially equivalent and admits Diophantine hardness for the Continuous Skolem Problem.

## 6.3 Bounded case: conditional decidability

### 6.3.1 Zero-finding algorithm

Our procedure for computing zeros of exponential polynomials is based on a straightforward sampling method. Let $f : (a, b) \to \mathbb{R}$ be a differentiable function defined on a bounded open interval of reals with rational endpoints. Assume that given a rational argument $t \in (a, b)$ and positive error bound $\varepsilon \in \mathbb{Q}$ we can compute $f(t)$ to within additive error $\varepsilon$, i.e., we can compute $q \in \mathbb{Q}$ such that $|f(t) - q| < \varepsilon$. Assume also that we are given a bound $M$ such that $|f'(t)| \leq M$ for all $t \in (a, b)$. Finally we suppose that the equations $f(t) = f'(t) = 0$ have no solution $t \in (a, b)$, i.e., $f$ has no tangential zeros. Under the above assumptions we describe a procedure for computing zeros of $f$.

For each integer $N \geq 2$ we consider $N - 1$ evenly spaced sample points $s_j := \frac{(N-j)a+jb}{N}$, $j = 1, \ldots, N-1$, in the interval $(a, b)$. For each sample point $s_j$, we compute a rational number $q_j$ such that $|q_j - f(s_j)| < \frac{1}{N}$ and proceed as follows:

1. If $q_{j_1} \geq \frac{1}{N}$ and $q_{j_2} \leq -\frac{1}{N}$ for some $j_1, j_2 \in \{1, \ldots, N-1\}$ then output that $f$ has a zero in $(a, b)$.
2. If $q_j > \frac{M+1}{N}$ for all $k \in \{1, \ldots, N-1\}$ or $q_j < -\frac{M+1}{N}$ for all $j \in \{1, \ldots, N-1\}$ then output that $f$ has no zero in $(a, b)$.
3. If neither of the above hold then the result is inconclusive and we proceed to the next value of $N$.

It is not hard to see that the above procedure eventually terminates given our assumption that $f$ has no tangential zeros in $(a, b)$.

### 6.3.2 Background: Laurent polynomials

Fix non-negative integers $r$ and $s$, and consider a single variable $x$ and tuples of variables $\boldsymbol{y} = \langle y_1, \ldots, y_r \rangle$ and $\boldsymbol{z} = \langle z_1, \ldots, z_s \rangle$. Consider the ring of Laurent polynomials

$$\mathcal{R} := \mathbb{C}[x, y_1, y_1^{-1}, \ldots, y_r, y_r^{-1}, z_1, z_1^{-1}, \ldots, z_s, z_s^{-1}] \,,$$

which can be seen as a localisation of the polynomial ring $\mathcal{A} := \mathbb{C}[x, y_1, \ldots, y_r, z_1, \ldots, z_s]$ in the multiplicative set generated by the set of variables $\{y_1, \ldots, y_r\} \cup \{z_1, \ldots, z_s\}$. The multiplicative units of $\mathcal{R}$ are the non-zero monomials in variables $y_1, \ldots, y_r$ and $z_1, \ldots, z_s$. As the localisation of a unique factorisation domain, $\mathcal{R}$ is itself a unique factorisation domain [Cohn, 2002, Theorem 10.3.7]. From the proof of this fact it moreover easily follows that $\mathcal{R}$ inherits from $\mathcal{A}$ the properties that a polynomial with algebraic coefficients factors as a product of polynomials that also have algebraic coefficients and that this factorisation can be effectively computed [Kaltofen, 1982].

We extend the operation of complex conjugation to a ring automorphism of $\mathcal{R}$ as follows. Given a polynomial

$$P = \sum_{j=1}^{n} a_j x^{u_j} {y_1}^{v_{j1}} \ldots {y_r}^{v_{jr}} {z_1}^{w_{j1}} \ldots {z_s}^{w_{js}} \,,$$

where $a_1, \ldots, a_n \in \mathbb{C}$, define its conjugate to be

$$\overline{P} := \sum_{j=1}^{n} \overline{a_j} x^{u_j} {y_1}^{v_{j1}} \ldots {y_r}^{v_{jr}} {z_1}^{-w_{j1}} \ldots {z_s}^{-w_{js}} .$$

This definition corresponds to the intuition that variables $x$ and $y_1, \ldots, y_r$ are real-valued, while variables $z_1, \ldots, z_s$ take values in the unit circle in the complex plane.

We will need the following lemma concerning polynomials in $\mathcal{R}$ that are associated with their conjugates. Here we use pointwise notation for exponentiation: given a tuple of integers $\boldsymbol{u} = \langle u_1, \ldots, u_s \rangle$, we write $\boldsymbol{z}^{\boldsymbol{u}}$ for the monomial $z_1^{u_1} \ldots z_s^{u_s}$.

**Lemma 52.** *Let $P \in \mathcal{R}$ be such that $P = \boldsymbol{z}^{\boldsymbol{u}} \overline{P}$ for $\boldsymbol{u} \in \mathbb{Z}^s$. Then either (i) $P$ has an associate $Q \in \mathcal{R}$ such that $Q = \overline{Q}$, or (ii) there exists $Q \in \mathcal{R}$ such that $P = Q + \boldsymbol{z}^{\boldsymbol{u}} \overline{Q}$ and $P$ does not divide $Q$ in $\mathcal{R}$.*

*Proof.* Consider a monomial $M$ such that $\boldsymbol{z}^{\boldsymbol{u}} \overline{M} = M$. Then $M$ has a real coefficient and the exponent $\boldsymbol{w}$ of $\boldsymbol{z}$ in $M$ satisfies $2\boldsymbol{w} = \boldsymbol{u}$. Thus if $\boldsymbol{z}^{\boldsymbol{u}} \overline{M} = M$ for every monomial $M$ appearing in $P$ then $P$ has the form $Q\boldsymbol{z}^{\boldsymbol{w}}$, where $2\boldsymbol{w} = \boldsymbol{u}$ and $Q$ is a polynomial in the variables $x$ and $\boldsymbol{y}$ with real coefficients. In particular $Q = \overline{Q}$, and statement (i) of the claim applies.

Suppose now that $\boldsymbol{z}^{\boldsymbol{u}} \overline{M} \neq M$ for some monomial $M$ appearing in $P$. Then the map sending $M$ to $\boldsymbol{z}^{\boldsymbol{u}} \overline{M}$ induces a permutation of order 2 on the monomials on $P$. Thus we may write $P = \sum_{j=1}^{n} M_j$, where $n = k + 2\ell$ for some $k \geq 0$ and $\ell \geq 1$ such that $\boldsymbol{z}^{\boldsymbol{u}} \overline{M_j} = M_j$ for $1 \leq j \leq k$ and $\boldsymbol{z}^{\boldsymbol{u}} \overline{M_j} = M_{j+\ell}$ for $k+1 \leq j \leq \ell$. Then, writing $Q := \frac{1}{2} \sum_{j=1}^{k} M_j + \sum_{j=k+1}^{k+\ell} M_j$, we have $P = Q + \boldsymbol{z}^{\boldsymbol{u}} \overline{Q}$.

The set of monomials appearing in $Q$ is a proper subset of the set of monomials appearing in $P$ (up to constant coefficients). Thus $Q$ cannot be a constant multiple of $P$. Furthermore for each variable $\sigma \in \{x, y_j, z_k : 1 \leq j \leq r, 1 \leq k \leq s\}$, the maximum degree of $\sigma$ in $P$ is at least its maximum degree in $Q$, and likewise for $\sigma^{-1}$. It follows that $Q$ cannot be a multiple of $P$ by a non-constant polynomial. We conclude that $P$ does not divide $Q$. □

### 6.3.3 Application of Schanuel's Conjecture

The main result of this chapter depends on Schanuel's Conjecture (Conjecture 9), which we apply via the following lemma.

**Lemma 53.** *Let $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ be $\mathbb{Q}$-linearly independent sets of real algebraic numbers. Furthermore, let $P, Q \in \mathcal{R}$ be two polynomials that have algebraic coefficients and are coprime in $\mathcal{R}$. Then the equations*

$$P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{6.2}$$
$$Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) = 0 \tag{6.3}$$

*have no non-zero solution $t \in \mathbb{R}$.*

*Proof.* Consider a solution $t \neq 0$ of Equations (6.2) and (6.3). By passing to suitable associates, we may assume without loss of generality that $P$ and $Q$ lie in $\mathcal{A}$, i.e., that all variables in $P$ and $Q$ appear with non-negative exponent. Moreover, since $P$ and $Q$ are coprime in $\mathcal{R}$, their greatest common divisor $R$ in $\mathcal{A}$ is a monomial. In particular,

$$R(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) \neq 0 .$$

Thus, dividing $P$ and $Q$ by $R$, we may assume that $P$ and $Q$ are coprime in $\mathcal{A}$ and that Equations (6.2) and (6.3) still hold.

By Schanuel's Conjecture, the extension

$$\mathbb{Q}(a_1 t, \ldots, a_r t, ib_1 t, \ldots, ib_s t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) : \mathbb{Q}$$

has transcendence degree at least $r + s$. Since $a_1, \ldots, a_r$ and $b_1, \ldots, b_s$ are algebraic over $\mathbb{Q}$, writing

$$S := \langle t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t} \rangle ,$$

it follows that the extension $\mathbb{Q}(S) : \mathbb{Q}$ also has transcendence degree at least $r + s$.

From Equations (6.2) and (6.3) we can regard $S$ as specifying a common root of $P$ and $Q$. Pick some variable $\sigma \in \{x, y_j, z_j : 1 \leq i \leq r, 1 \leq j \leq s\}$ that has positive degree in $P$. Then the component of $S$ corresponding to $\sigma$ is algebraic over the remaining components of $S$. We claim that the remaining components of $S$ are algebraically dependent and thus $S$ comprises at most $r + s - 1$ algebraically independent elements, contradicting Schanuel's Conjecture. The claim clearly holds if $\sigma$ does not appear in $Q$. On the other hand, if $\sigma$ has positive degree in $Q$ then, since $P$ and $Q$ are coprime polynomials, the multivariate resultant $\mathrm{Res}_\sigma(P, Q)$ is a non-zero polynomial in the set of variables $\{x, y_j, z_j : 1 \leq i \leq r, 1 \leq j \leq s\} \setminus \{\sigma\}$ which has a root at $S$ (see, e.g., [Cox et al., 2007, Page 163]). Thus the claim also holds in this case. In either case we obtain a contradiction to Schanuel's Conjecture and we conclude that Equations (6.2) and (6.3) have no non-zero solution $t \neq 0$. □

### 6.3.4 Eliminating tangential zeros

Let $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ be $\mathbb{Q}$-linearly independent sets of real algebraic numbers and consider the exponential polynomial

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}), \tag{6.4}$$

where $P \in \mathcal{R}$ is irreducible. We say that $f$ is a *Type-1* exponential polynomial if $P$ and $\overline{P}$ are not associates in $\mathcal{R}$, we say that $f$ is *Type-2* if $P = \alpha\overline{P}$ for some $\alpha \in \mathbb{C}$, and we say that $f$ is *Type-3* if $P = U\overline{P}$ for some non-constant unit $U \in \mathcal{R}$. These three cases are mutually exhaustive by construction.

The simplest example of a Type-3 exponential polynomial is $g(t) = 1 + e^{it}$. Here $g(t) = P(e^{it})$, where $P(z) = 1 + z$ is an irreducible polynomial that is associated with its conjugate $\overline{P}(z) = 1 + z^{-1}$. Note that the exponential polynomial $f(t) = 2 + \cos(t)$ from the Introduction factors as the product of two type-3 exponential polynomials $f(t) = g(t)\overline{g(t)}$.

In the case of a Type-2 exponential polynomial $P = \alpha\overline{P}$ it is clear that we must have $|\alpha| = 1$. Moreover, by replacing $P$ by $\beta P$, where $\beta^2 = \overline{\alpha}$, we may assume without loss of generality that $P = \overline{P}$. Similarly, in the case of a Type-3 exponential polynomial, we can assume without loss of generality that $P = \boldsymbol{z}^{\boldsymbol{u}}\overline{P}$ for some non-zero vector $\boldsymbol{u} \in \mathbb{Z}^s$.

Now consider an arbitrary exponential polynomial $f(t) := \sum_{j=1}^{n} P_j(t)e^{\lambda_j t}$. Let $\{a_1, \ldots, a_r\}$ be a basis of the $\mathbb{Q}$-vector space spanned by $\{\Re(\lambda_j) : 1 \leq j \leq n\}$ and let $\{b_1, \ldots, b_s\}$ be a basis of the the $\mathbb{Q}$-vector space spanned by $\{\Im(\lambda_j) : 1 \leq j \leq n\}$. Without loss of generality we may assume that each characteristic root $\lambda$ is an integer linear combination of $a_1, \ldots, a_r$ and $ib_1, \ldots, ib_s$. Then $e^{\lambda t}$ is a product of positive and negative powers of $e^{a_1 t}, \ldots, e^{a_r t}$ and $e^{ib_1 t}, \ldots, e^{ib_s t}$. It follows that there is a Laurent polynomial $P \in \mathcal{R}$ such that

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}). \tag{6.5}$$

Since $P$ can be written as a product of irreducible factors, it follows that $f$ can be written as product of Type-1, Type-2, and Type-3 exponential polynomials, and moreover this factorisation can be computed from $f$. Thus it suffices to show how to decide the existence of zeros of these three special forms of exponential polynomial. We will handle all three cases using Schanuel's Conjecture, or more specifically, Lemma 53.

**Theorem 54.** *The Bounded Continuous Skolem Problem is decidable subject to Schanuel's Conjecture.*

*Proof.* Consider an exponential polynomial

$$f(t) = P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}), \tag{6.6}$$

where $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$ are $\mathbb{Q}$-linearly independent sets of real algebraic numbers, and $P \in \mathcal{R}$ is irreducible. We show how to decide whether $f$ has a zero in a bounded interval $I \subseteq \mathbb{R}_{\geq 0}$, considering separately the case of Type-1, Type-2, and Type-3 exponential polynomials.

If $f(t) = 0$ and $t$ is algebraic then $e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}$ are algebraically dependent over $\mathbb{Q}$. But this is impossible unless $t = 0$ by the Lindemann-Weierstrass Theorem. Thus $f(t) \neq 0$ for any non-zero rational number $t$ and it is no loss of generality to assume that $I = (c, d)$ is an open interval.

*Case I.* Suppose first that $f$ is Type-1. By assumption, $P$ and $\overline{P}$ are both irreducible and are not associates and are therefore coprime. We claim that in this case the equation $f(t) = 0$ has no solution $t \in \mathbb{R}$. Indeed $f(t) = 0$ implies

$$\begin{aligned} P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) &= 0 \\ \overline{P}(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) &= 0\,, \end{aligned}$$

and the non-existence of a zero of $f$ follows immediately from Lemma 53.

*Case II.* Now suppose that $f$ is Type-2. In this case we have $P = \overline{P}$ and so $f$ is real-valued. It will suffice to show that the equations $f(t) = f'(t) = 0$ have no solution $t \in \mathbb{R}$, for then we can use the procedure of Section 6.3.1 to determine whether or not $f$ has a zero in $(c, d)$.

We can write $f'(t)$ in the form

$$f'(t) = Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t})\,,$$

where $Q$ is the polynomial

$$Q = \frac{\partial P}{\partial x} + \sum_{j=1}^{r} a_j y_j \frac{\partial P}{\partial y_j} + \sum_{j=1}^{s} i b_j z_j \frac{\partial P}{\partial z_j}\,.$$

We claim that $P$ and $Q$ are coprime. Indeed, since $P$ is irreducible, $P$ and $Q$ can only fail to be coprime if $P$ divides $Q$.

If $P$ has strictly positive degree $k$ in $x$ then $Q$ has degree $k-1$ in $x$ and thus $P$ cannot divide $Q$. On the other hand, if $P$ has degree 0 in $x$ then $Q$ is obtained from $P$ by multiplying each monomial $\boldsymbol{y}^{\boldsymbol{u}}\boldsymbol{z}^{\boldsymbol{v}}$ appearing in $P$ by the constant $\sum_{j=1}^{r} a_j u_j + i \sum_{j=1}^{s} b_j v_j$. Moreover, by the assumption of linear independence of $\{a_1, \ldots, a_r\}$ and $\{b_1, \ldots, b_s\}$, each monomial in $P$ is multiplied by a different constant. Since $P$ is not a unit it has at least two different monomials and so $P$ is not a constant multiple of $Q$. Furthermore, for each variable $\sigma \in \{y_j, y_j^{-1} : 1 \leq j \leq r\} \cup \{z_j, z_j^{-1} : 1 \leq j \leq s\}$, the degree of $\sigma$ in $P$ is at least the degree of $\sigma$ in $Q$. Thus $P$ cannot be a multiple of $Q$ by a non-constant polynomial.

We conclude that $P$ does not divide $Q$ and hence $P$ and $Q$ are coprime. It now follows from Lemma 53 that the equations $f(t) = f'(t) = 0$ have no solution $t \in \mathbb{R}$.

*Case III.* Finally, suppose that $f$ is a Type-3 exponential polynomial. Then in (6.6) we have that $P = \boldsymbol{z}^{\boldsymbol{u}}\overline{P}$ for some non-zero vector $\boldsymbol{u} \in \mathbb{Z}^s$. By Lemma 52 we can write $P = Q + \boldsymbol{z}^{\boldsymbol{u}}\overline{Q}$ for some polynomial $Q \in \mathcal{R}$ that is coprime with $P$.

Now define

$$g_1(t) := Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t})$$

and $g_2(t) := e^{ib_1 u_1} \ldots e^{ib_s u_s}\overline{g_1(t)}$, so that $f(t) = g_1(t) + g_2(t)$ for all $t$.

We show that $g_2(t) \neq 0$ for all $t \in \mathbb{R}$. Indeed if $g_2(t) = 0$ for some $t$ then we also have $g_1(t) = 0$ and hence $f(t) = 0$. For such a $t$ it follows that

$$\begin{aligned} P(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) &= 0 \\ Q(t, e^{a_1 t}, \ldots, e^{a_r t}, e^{ib_1 t}, \ldots, e^{ib_s t}) &= 0\,. \end{aligned}$$

But $P$ and $Q$ are coprime and so these two equations cannot both hold by Lemma 53. Not only do we have $g_2(t) \neq 0$ for all $t \in \mathbb{R}$, but, applying the sampling procedure in Section 6.3.1 to $|g_2(t)|^2$ (which is a differentiable function) we can compute a strictly positive lower bound on $|g_2(t)|$ over the interval $(c, d)$.

Let log denote the principal branch of the complex logarithm defined by $\log(z) = |z| + i \arg(z)$ where $\arg(z) \in (-\pi, \pi]$. Recall that one can compute $\log(z)$ and $e^z$ to within arbitrarily small additive error given a sufficiently precise approximation of $z$ [Brent, 1976]. Since $g_2(t) \neq 0$ for all $t \in \mathbb{R}$ we may define the function $h : (c, d) \to \mathbb{R}$ by

$$h(t) := i \log\left(1 + i + i\,\frac{g_1(t)}{g_2(t)}\right)\,.$$

Moreover $h$ is differentiable since (from the fact that $|g_1(t)| = |g_2(t)|$) the argument of log is bounded away from the branch cut along the negative real axis.

Note that $h(t) = 0$ if and only if $f(t) = 0$. Our aim is to use the procedure of Section 6.3.1 to decide the existence of a zero of $h$ in the interval $(c, d)$, and thus decide whether $f$ has a zero in $(c, d)$. To this end, we first observe that using the strictly positive lower bound on $|g_2(t)|$ over the interval $(c, d)$, obtained above, we can compute an upper bound on $|h'(t)|$ on $(c, d)$. It remains to show that $h$ has no tangential zeros in this interval.

Now let $t \in (c, d)$ be such that $h(t) = 0$. Then $g_1(t) = -g_2(t)$. Moreover for such $t$, recalling that $g_2(t) \neq 0$, we have

$$\begin{aligned} h'(t) = 0 \quad &\text{iff} \quad \frac{g_2(t)}{ig_1(t) + ig_2(t) + g_2(t)} \frac{g_1'(t)g_2(t) - g_2'(t)g_1(t)}{g_2(t)^2} = 0 \\ &\text{iff} \quad g_1'(t)g_2(t) - g_2'(t)g_1(t) = 0 \\ &\text{iff} \quad g_1'(t)g_2(t) + g_2'(t)g_2(t) = 0 \\ &\text{iff} \quad g_1'(t) + g_2'(t) = 0 \\ &\text{iff} \quad f'(t) = 0\,. \end{aligned}$$

Thus $h(t) = h'(t) = 0$ implies $f(t) = f'(t) = 0$. But the proof in *Case II* shows that $f(t) = f'(t) = 0$ is impossible. (Nothing in that argument hinges on $f$ being real-valued.) Thus $h$ has no tangential zeros and this concludes the proof. □

### 6.3.5 Unconditional argument for order at most three

In this section, we show unconditional decidability for the Bounded Skolem Problem for exponential polynomials of order at most 3. The problem is clearly trivial at order 1, so Suppose we are given an exponential polynomial $f(t)$ of order 2 or 3, together with a bounded interval $I$. We will analyse the characteristic roots of $f$ and for each case will either show how to detect the existence of tangential zeros in $I$, or we will rule them out completely. We eschew Schanuel's Conjecture and insteady rely on the Gelfond-Schneider Theorem (Theorem 3) and the Lindemann-Weierstrass Theorem (Theorem 4). There are four cases to consider, based on the characteristic roots of $f(t)$ and their multiplicities.

*Case I.* First, suppose $f(t)$ is of order 3 with one characteristic root, necessarily real, of multiplicity 3, so that our exponential polynomial is of the form

$$f(t) = (Ct^2 + Bt + A)e^{tr}$$

for some $A, B, C, r \in \mathbb{R} \cap \mathbb{A}$ with $C \neq 0$. The problem instance is positive if and only if the quadratic $Ct^2 + Bt + A$ has a zero in $I$, which is easy to determine.

*Case II.* Second, suppose $f(t)$ is of order 3 with two real characteristic roots, one repeated and one simple, so that the function is of the form:

$$f(t) = (A + Bt)e^{at} + Ce^{bt}$$

for some $A, B, C, a, b \in \mathbb{R} \cap \mathbb{A}$ with $B, C \neq 0$ and $a \neq b$. Notice that $f(t)$ has the same zeros as $f(t)/e^{at}$, so we may assume without loss of generality that $a = 0$. We will prove that $f$ can have no tangential zeros other than $t = 0$. Indeed, suppose $f'(t) = f(t) = 0$. From $f'(t) = 0$, we obtain

$$e^{bt} = -\frac{B}{Cb} \in \mathbb{R} \cap \mathbb{A},$$

and hence from $f(t) = 0$, we have

$$t = -\frac{Ce^{bt} + A}{B} \in \mathbb{R} \cap \mathbb{A}.$$

Thus, both $bt$ and $e^{bt}$ are algebraic. By Lemma 5 (which follows directly from the Lindemann-Weierstrass Theorem), this entails $bt = 0$. Since $a \neq b$ (otherwise the exponential polynomial is of order 2), it follows that $b \neq 0$, so we must have $t = 0$.

*Case III.* Third, suppose $f(t)$ is of order 3 with three simple real characteristic roots, so that

$$f(t) = Ae^{at} + Be^{bt} + Ce^{ct},$$

where $A, B, C, a, b, c \in \mathbb{R} \cap \mathbb{A}$ with $A, B, C \neq 0$ and $\{a, b, c\}$ are all distinct. We can assume without loss of generality that $a > b > c$. Moreover, since the zeros of $f(t)$ are precisely the zeros of $f(t)/e^{ct}$, we may also assume without loss of generality that $c = 0$. We now show how to detect whether $f$ has tangential zeros in $I$. The equation $f(t) = f'(t) = 0$ is equivalent to

$$\begin{bmatrix} A & B \\ Aa & Bb \end{bmatrix} \begin{bmatrix} e^{at} \\ e^{bt} \end{bmatrix} = \begin{bmatrix} -C \\ 0 \end{bmatrix}. \tag{6.7}$$

The matrix in (6.7) has determinant $AB(b-a)$, which is non-zero (otherwise the exponential polynomial is of lower order). Therefore, $f(t) = f'(t) = 0$ is equivalent to $(e^{at}, e^{bt}) = (D, E)$ for some $D, E \in \mathbb{R} \cap \mathbb{A}$. Thus, both $e^{bt}$ and $e^{at} = \left(e^{bt}\right)^{a/b}$ are algebraic. By Theorem 3 (Gelfond-Schneider), at least one of two statements must hold: $t = 0$ or $a/b \in \mathbb{Q}$. We can easily check whether $a/b \in \mathbb{Q}$, and if not, conclude that $f$ has no tangential zeros, except possibly $t = 0$, which is also easy to check by direct calculation. Assume now that $a/b = n/m$ for positive natural numbers $n, m$. Let $t = mu$, then $f(t) = f'(t) = 0$ is equivalent to

$$\begin{aligned} 0 &= A\left(e^{bu}\right)^n + B\left(e^{bu}\right)^m + C, \\ 0 &= Aa\left(e^{bu}\right)^n + Bb\left(e^{bu}\right)^m. \end{aligned}$$

As $u$ varies over $\mathbb{R}_{\geq 0}$, clearly $e^{bu}$ varies over $[1, \infty)$. We find all common real zeros $\{\alpha_1, \ldots, \alpha_k\}$ in $[1, \infty)$ of the polynomials $Ax^n + Bx^m + C$ and $Aax^n + Bbx^m$, these are clearly algebraic and may be represented as usual. Each $\alpha_j$ corresponds to a tangential zero of $f$ on $\mathbb{R}_{\geq 0}$. Thus, all that remains is, for each $\alpha_j$, to determine whether $e^{bu} = e^{bmt} = \alpha_j$ occurs for $t \in I$, or equivalently, whether $\log(\alpha_j)/bm \in I$. Notice that $\alpha_j = 1$ corresponds to $t = 0$, which we have already discounted. Therefore, by Lemma 5, $\log(\alpha_j)$ is transcendental. Since $b, m \in \mathbb{R} \cap \mathbb{A}$, clearly $\log(\alpha_j)/bm$ is transcendental, so in particular, it must be distinct from the endpoints of $I$. Then it suffices to approximate $\log(\alpha_j)/bm$ until sufficiently many bits are obtained to compare with the endpoints of $I$.

*Case IV.* Next, suppose $f(t)$ is of order 3 with one real and two complex characteristic roots, so that

$$f(t) = A_1 e^{t(a+bi)} + A_2 e^{t(a-bi)} + Ce^{rt}.$$

with $a, b, r, C \in \mathbb{R} \cap \mathbb{A}$, $A_1, A_2 \in \mathbb{A}$ and $b > 0$. Since the zeros of $f(t)$ are precisely the zeros of $f(t)/e^{rt}$, we can assume without loss of generality that $r = 0$. Using Euler's identity, we can express $f(t)$ as

$$f(t) = e^{at}(A\cos(bt) + B\sin(bt)) + C,$$

where $A, B \in \mathbb{R} \cap \mathbb{A}$. We will first show that unless $a = 0$, the only possible tangential zero is $t = 0$. The equation $f(t) = f'(t) = 0$ is equivalent to:

$$\begin{bmatrix} A & B \\ B + Aa & Ba - A \end{bmatrix} \begin{bmatrix} e^{at}\cos(bt) \\ e^{at}\sin(bt) \end{bmatrix} = \begin{bmatrix} -C \\ 0 \end{bmatrix}. \tag{6.8}$$

The $2 \times 2$ matrix in (6.8) has determinant $-A^2 - B^2$, which is clearly non-zero (otherwise $f$ is the constant function $C$). Therefore, $f(t) = f'(t) = 0$ is equivalent to

$$\begin{bmatrix} e^{at}\cos(bt) \\ e^{at}\sin(bt) \end{bmatrix} = \begin{bmatrix} E \\ F \end{bmatrix} \tag{6.9}$$

for some $E, F \in \mathbb{R} \cap \mathbb{A}$. Then $e^{2at} = E^2 + F^2$ is algebraic, and therefore $e^{at} \in \mathbb{A}$ also. Hence, $\cos(bt) = E/e^{at} \in \mathbb{A}$ and $\sin(bt) = F/e^{at} \in \mathbb{A}$. Thus, we have that $e^{ibt}$ and $e^{at} = \left(e^{ibt}\right)^{a/bi}$ are both algebraic. Then by Theorem 3 (Gelfond-Schneider), $t = 0$ or $a/bi \in \mathbb{Q}$, that is, $a = 0$, as required.

Thus, all that remains is to investigate the tangential zeros of $f(t)$ in the case $a = 0$. In this case, the function is

$$f(t) = A\cos(bt) + B\sin(bt) + C.$$

By (6.9), it can only have tangential zeros if $E^2 + F^2 = 1$, in which case it has infinitely many tangential zeros, all of the form $t_k = \varphi/b + 2k\pi/b$ where $k \in \mathbb{N}$ and $\varphi$ is the unique real number in $[0, 2\pi)$ such that $\cos(\varphi) = E$ and $\sin(\varphi) = F$.

It only remains to determine whether $t_k \in I$ for some $k$. Assuming $t_k$ is distinct from the endpoints of $I$, this is easy: for each $k$, we obtain sufficiently many bits of $t_k$ to compare it with the endpoints of $I$. We stop when we encounter $t_k$ to the right of $I$.

Finally, notice that it is no loss of generality to assume that $t_k$ is distinct from the endpoints of $I$. Indeed, if $q \in \mathbb{Q}$ is one such endpoint, $t_k = q$ would entail $e^{i\varphi} = e^{ibq} \in \mathbb{A}$. Since $ibq$ is also algebraic, by Lemma 5 we have $ibq = 0$. But $b \neq 0$ by assumption, so $q = 0 = t_k$. Therefore, as we have already discounted the possibility of a tangential zero at $t = 0$, we are done.

*Case V.* Finally, suppose $f(t)$ is of order 2. There are three possibilities for $f(t)$.

$$f(t) = (Bt + A)e^{rt} \qquad (A, B, r \in \mathbb{R} \cap \mathbb{A} \text{ and } B \neq 0) \tag{6.10}$$

$$f(t) = Ae^{at} + Be^{bt} \qquad (A, B, a, b \in \mathbb{R} \cap \mathbb{A},\ A, B \neq 0 \text{ and } a \neq b) \tag{6.11}$$

$$f(t) = e^{at}(A\cos(bt) + B\sin(bt)), \qquad (A, B, a, b \in \mathbb{R} \cap \mathbb{A},\ b > 0 \text{ and } A, B \text{ not both zero}) \tag{6.12}$$

If $f(t)$ is of the form (6.10), then clearly the only possible zero is $-A/B \in \mathbb{R} \cap \mathbb{A}$, and it is easy to check whether it lies in $I$. If $f(t)$ is of the form (6.11), the situation is identical to *Case III* above with $C = 0$. In particular, there can be no tangential zeros, since (6.7) with $C = 0$ is equivalent to $e^{at} = e^{bt} = 0$, which is impossible. Similarly, if $f(t)$ is of the form (6.12), we are in *Case IV* above with $C = 0$. There can be no tangential zeros, since (6.8) with $C = 0$ is equivalent to $e^{at}\cos(bt) = e^{at}\sin(bt) = 0$, which is impossible.

## 6.4 Unbounded case: Diophantine hardness

Recall the homogeneous Diophantine approximation type $L(x)$ of a real number $x$, defined in Section 2.2.1:

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

The central result of this section is Theorem 51. We show that decidability of the Unbounded Continuous Skolem Problem entails significant new effectiveness results in Diophantine approximation, namely the computability of $L(a)$ for all real algebraic numbers $a$, thereby identifying a formidable mathematical obstacle to further progress in the unbounded case.

Fix positive $a, b, c \in \mathbb{R} \cap \mathbb{A}$ and let $j, k$ be two bits, not both zero: $(j, k) \in \{0, 1\}^2 \setminus (0, 0)$. We define the following functions:

$$g_{j,k}(t) = be^t(1 - \cos(t)(-1)^j) + (2t + b)(1 - \cos(at)(-1)^k) - c\sin(at),$$
$$h_{j,k}(t) = be^t(1 - \cos(t)(-1)^j) + (2t + b)(1 - \cos(at)(-1)^k) + c\sin(at),$$
$$f_{j,k}(t) = be^t(1 - \cos(t)(-1)^j) + (2t + b)(1 - \cos(at)(-1)^k) - c|\sin(at)| = \min\{g_{j,k}(t), h_{j,k}(t)\}.$$

Clearly $g_{j,k}(t)$ and $h_{j,k}(t)$ are exponential polynomials of order 9, with six characteristic roots: three simple (1 and $1 \pm i$) and three repeated (0 and $\pm ai$). Moreover it is easy to check that the function $f_{j,k}(t)$ has a zero in an unbounded interval $I$ if and only if at least one of $g_{j,k}(t)$, $h_{j,k}(t)$ has a zero in $I$.

We will first prove two lemmas which show a connection between the existence of zeros of $f_{j,k}(t)$ and the approximation type $L(a)$. Specifically, zeros of $f_{j,k}$ will correspond to 'good' rational approximations of $a$ where the denominator and the numerator have parities $j$ and $k$, respectively. We will then derive an algorithm to compute $L(a)$ using an oracle for the Continuous Skolem Problem, thereby demonstrating our desired hardness result.

**Lemma 55.** *Fix positive $a, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $\varepsilon \in (0, 1)$. Then it is possible to choose a positive $b \in \mathbb{R} \cap \mathbb{A}$ large enough, so that if some $f_{j,k}$ has a zero on $[0, \infty)$, then $L(a) \leq c/\pi^2(1 - \varepsilon)$.*

*Proof.* Suppose $f_{j,k}(t) = 0$ for some $t \geq 0$. Let $\delta_1, \delta_2$ be the unique real numbers in $[-\pi, \pi)$ such that $t = \pi m + \delta_1$, $at = \pi n + \delta_2$ and $m, n \in \mathbb{N}$ have parities $j, k$, respectively. Then we have

$$f_{j,k}(t) = be^t(1 - \cos(\delta_1)) + (2t + b)(1 - \cos(\delta_2)) - c|\sin(\delta_2)| = 0.$$

It is easy to see that

$$\left|a - \frac{n}{m}\right| = \frac{|\delta_2 - a\delta_1|}{\pi m}.$$

Write $f$ for $f_{j,k}$. We will use $f(t) = 0$ to bound $|\delta_2|$ and $|a\delta_1|$ separately from above. Then we will apply the triangle inequality to bound $|\delta_2 - a\delta_1|$, obtaining the desired upper bound on $L(a)$.

Choose $\alpha, \beta \in \mathbb{Q}$ such that $\alpha > 0$, $\beta \in (0,1)$ and $\alpha^{-1} + \beta^{-1} = (1-\varepsilon)^{-1}$. Note that this is always possible, given $\varepsilon \in (0,1)$. We first seek an upper bound on $|\delta_1|$. To this end, let $b$ be large enough so that

$$\text{if } 1 - \cos(x) \leq \frac{c}{b} \text{ and } |x| \leq \pi, \text{then } 1 - \cos(x) \geq \frac{x^2}{4}, \tag{6.13}$$

$$be^x \geq \frac{4\alpha^2(x-y)^2a^2}{c} \quad \text{for all } x \geq 0 \text{ and } |y| \leq \pi. \tag{6.14}$$

Since the term $(2t+b)(1-\cos(\delta_2))$ is non-negative, from $f(t) = 0$, we obtain

$$1 - \cos(\delta_1) = \frac{c|\sin(\delta_2)| - (2t+b)(1-\cos(\delta_2))}{be^t} \leq \frac{c}{be^t} \leq \frac{c}{b}. \tag{6.15}$$

Since $|\delta_1| \leq \pi$, by (6.13) and (6.15), we have

$$\frac{\delta_1^2}{4} \leq 1 - \cos(\delta_1) \leq \frac{c}{be^t}.$$

Combining the upper and lower bound on $1 - \cos(\delta_1)$, we have

$$\begin{aligned}
\delta_1^2 &\leq \frac{4c}{be^t} \\
&\leq \frac{c^2}{\alpha^2 a^2 (t-\delta_1)^2} && \{ \text{ by (6.14) with } x = t \text{ and } y = \delta_1 \ \} \\
&= \frac{c^2}{a^2\alpha^2 m^2 \pi^2}. && \{ \text{ by } \delta_1 = t - \pi m \ \}
\end{aligned}$$

Therefore,

$$|a\delta_1| \leq \frac{c}{\alpha m \pi}.$$

Next, we proceed to bound $|\delta_2|$. Let $b$ be large enough so that

$$\text{if } 1 - \cos(x) \leq \frac{c}{b}, \text{ then } \frac{\beta x^2}{2} \leq 1 - \cos(x). \tag{6.16}$$

Noting that the term $be^t(1-\cos(\delta_1))$ is non-negative, we obtain the following inequalities from $f(t) = 0$:

$$1 - \cos(\delta_2) \leq \frac{c|\sin(\delta_2)|}{2t+b} \leq \frac{c|\sin(\delta_2)|}{b} \leq \frac{c}{b}.$$

Then by (6.16) and the inequality $|\sin(x)| \leq |x|$ for $x \in [-\pi, \pi]$, we have

$$\frac{\beta\delta_2^2}{2} \leq 1 - \cos(\delta_2) \leq \frac{c|\sin(\delta_2)|}{2t+b} \leq \frac{c|\delta_2|}{2t+b}.$$

Combining the upper and lower bound on $1 - \cos(\delta_2)$ then yields:

$$\begin{aligned}
|\delta_2| &\leq \frac{2c}{\beta(2t+b)} \\
&\leq \frac{c}{\beta(t-\delta_1)} && \{ \text{ by taking } b \geq 2\pi \text{ and noting } |\delta_1| \leq \pi \ \} \\
&= \frac{c}{\beta m \pi}. && \{ \text{ by } t = \pi m + \delta_1 \ \}
\end{aligned}$$

Finally, by the triangle inequality and the bounds on $|a\delta_1|$ and $|\delta_2|$, we have

$$\left|a - \frac{n}{m}\right| = \frac{|\delta_2 - a\delta_1|}{\pi m} \leq \frac{|\delta_2| + |a\delta_1|}{\pi m} \leq \frac{1}{\pi m}\left(\frac{c}{\beta m \pi} + \frac{c}{\alpha m \pi}\right) = \frac{c}{(1-\varepsilon)\pi^2 m^2},$$

so the natural numbers $n, m$ witness $L(a) \leq c/\pi^2(1-\varepsilon)$. □

**Lemma 56.** *Fix positive $a, b, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $\varepsilon \in (0,1)$. There exists an effective threshold $M$, dependent on $a, b, c, \varepsilon$, such that if $L(a) \leq c(1-\varepsilon)/\pi^2$ holds and is witnessed by natural numbers $n, m$ with $m \geq M$, then $f_{j,k}(t) = 0$ for some $t \geq \pi M$ and $(j,k) \in \{0,1\}^2 \setminus (0,0)$.*

*Proof.* Write $\gamma = \sqrt{1-\varepsilon} \in (0,1)$. Select $M$ large enough, so that $c/M < \pi$ and

$$\text{if } |x| < \tfrac{c}{M}, \text{ then } \gamma|x| \leq |\sin(x)|, \tag{6.17}$$

$$1 + \frac{b}{2\pi M} \leq \gamma^{-1}. \tag{6.18}$$

Suppose now that $L(a) \leq c(1-\varepsilon)/\pi^2$, let this be witnessed by $n, m \in \mathbb{N}$ with $m \geq M$. Without loss of generality, $n$ and $m$ are not both even. Let $j, k$ be the parities of $m$ and $n$, respectively. Define $t = \pi m$ and write $f = f_{j,k}$. We will show that $f(t) \leq 0$. This suffices, because $f$ is continuous and moreover is positive for arbitrarily large times, so it must have a zero on $[t, \infty)$.

Since $L(a) \leq c(1-\varepsilon)/\pi^2$, we have

$$|am - n| \leq \frac{c(1-\varepsilon)}{\pi^2 m} < \frac{c}{M} < \pi.$$

Therefore, we can write $at = \pi am = \pi n + \delta$ for some $\delta$ satisfying

$$|\delta| \leq \frac{c(1-\varepsilon)}{\pi m} < \frac{c}{M} < \pi. \tag{6.19}$$

It is easy to see from the choice of $j, k$ that

$$f(t) = (2t + b)(1 - \cos(\delta)) - c|\sin(\delta)|.$$

Then we have

$$\begin{aligned}
f(t) &= (2\pi m + b)(1 - \cos(\delta)) - c|\sin(\delta)| && \{ \text{ by choice of } j, k \text{ and } t \ \} \\
&\leq |\delta| \left( (2\pi m + b)\frac{|\delta|}{2} - c\gamma \right) && \{ \text{ by (6.17) and } 1 - \cos(x) \leq x^2/2 \text{ for } |x| \leq \pi \ \} \\
&\leq |\delta| \left( (2\pi m + b)\frac{c(1-\varepsilon)}{2\pi m} - c\gamma \right) && \{ \text{ by (6.19) } \} \\
&\leq |\delta| c\gamma \left( \left( 1 + \frac{b}{2\pi M} \right) \gamma - 1 \right) && \{ \text{ by } m \geq M \text{ and } \gamma^2 = 1 - \varepsilon \ \} \\
&\leq 0. && \{ \text{ by (6.18) } \}
\end{aligned}$$

□

The following corollary is immediate:

**Lemma 57.** *Fix positive $a, b, c \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon \in \mathbb{Q}$ with $\varepsilon \in (0,1)$. There exists an effective threshold $M$, dependent on $a, b, c, \varepsilon$, such that if $f_{j,k}(t) \neq 0$ for all $t \geq 0$ and all $(j,k) \in \{0,1\}^2 \setminus (0,0)$, then either $L(a) < c(1-\varepsilon)/\pi^2$ and this is witnessed by natural numbers $n, m$ with $m < M$, or $L(a) \geq c(1-\varepsilon)/\pi^2$.*

We now use the above lemmas to show prove Theorem 51. Fix a real algebraic number $a$ and suppose we wish to approximate $L(a)$ to within arbitrary precision. Suppose also we know $L(a) \in [p, q]$ for non-negative $p, q \in \mathbb{Q}$. Choose $c \in \mathbb{R} \cap \mathbb{A}$ with $c > 0$ and a rational $\varepsilon \in (0,1)$ such that

$$p < \frac{c(1-\varepsilon)}{\pi^2} < \frac{c}{\pi^2(1-\varepsilon)} < q.$$

Write $A = c(1-\varepsilon)/\pi^2$ and $B = c/\pi^2(1-\varepsilon)$. Calculate the constant $b$ given by Lemma 55 and the threshold $M$ required by Lemma 57. Check for all denominators $m \leq M$ whether there exists a numerator $n$ such that $n, m$ witness $L(a) \leq A$. If so, then continue the approximation procedure recursively with confidence interval $[p, A]$. Otherwise, for each $j, k$, use the oracle for the Unbounded Continuous Skolem Problem to determine whether at least one of the functions $g_{j,k}, h_{j,k}$ has a zero on $[0, \infty)$. If this is the case, then

$f_{j,k}$ also has a zero on $[0, \infty)$, so by Lemma 55, $L(a) \leq B$ and we continue the approximation recursively on the interval $[p, B]$. If none of the functions $f_{0,1}, f_{1,0}, f_{1,1}$ has a zero, then $L(a) \geq A$ by Lemma 57, so we continue on the interval $[A, q]$. Notice that in this procedure, one can choose $c, \varepsilon$ at each stage in such a way that the confidence interval shrinks by at least a fixed factor, whatever the outcome of the oracle invocations. It follows therefore that $L(a)$ can be approximated to within arbitrary precision, completing the proof and establishing Theorem 51.

# Chapter 7

# Continuous Infinite Zeros Problem

*Prerequisites:* Sections 2.1.1, 2.1.3, 2.2, 2.3.2 and 2.4. Theorem 50 from Section 6.2

## 7.1 Introduction

In Chapter 6, we focused on reachability in a continuous-time linear dynamical system from a single starting point to a target $(m-1)$-dimensional subspace of $\mathbb{R}^m$. Though similar to the analogous problem in the discrete-time setting, the Continuous Skolem Problem presented new challenges, relying on powerful number-theoretic tools for decidability even of the bounded subproblem, and presenting us with a strong barrier to decidability at order 9 in the unbounded case.

In this chapter, we continue exploring reachability to a hyperplane in the continuous-time setting, and focus on another natural question: does a given continuous-time linear dynamical system $(\boldsymbol{A}, \boldsymbol{x}(0))$ intersect a given target hyperplane $\{\boldsymbol{y} \in \mathbb{R}^m : \boldsymbol{u}^T\boldsymbol{y} = 0\}$ infinitely often, or equivalently, does a given exponential polynomial $f(t) = \sum_{j=1}^{k} P_j(t)e^{t\lambda_j}$ have infinitely many zeros? This is the *Continuous Infinite Zeros Problem*. Since analyticity prevents exponential polynomials from having infinitely many zeros on any bounded interval, we may dispense with the interval $I$ which was part of the input of the Continuous Skolem Problem and instead fix the interval of interest to be $[0, \infty)$.

Like the Continuous Skolem Problem, this too has a discrete-time counterpart, the *Discrete Infinite Zeros Problem*: determine whether a given linear recurrence sequence has infinitely many zeros. Recall that the Skolem-Mahler-Lech Theorem characterises the zero set of LRS over any field of characteristic 0 as a semilinear set, that is, a finite set together with a finite union of arithmetic progressions. The work of [Berstel and Mignotte, 1976] showed how to effectively compute the infinite component in the case of rational LRS, whilst later it was observed in [Vereshchagin, 1985] that the proof readily generalises to LRS over the algebraic numbers.

Whilst the decidability of the Discrete Infinite Zeros Problem is settled for LRS of all orders, we shall see in this chapter that the continuous version admits a Diophantine hardness result at order 9, thereby necessitating simplifying assumptions on our exponential polynomials for the purposes of decidability. Specifically, we will be interested in exponential polynomials of order at most 7, as well as in exponential polynomials of arbitrary order but whose complex characteristic roots have imaginary parts which are all rational multiples of one another. In parallel, we study a second, equally important issue, namely, the existence of an effective threshold $T$ such that if an exponential polynomial has only finitely many zeros, they are all contained in $[0, T]$. In all cases where we show decidability of the Continuous Infinite Zeros Problem, we also establish the existence and effectiveness of such a threshold $T$, thereby obtaining a reduction from the Unbounded to the Bounded Continuous Skolem Problem.

## 7.2 Main result and outline

This chapter is based on our unpublished work [Chonev et al., 2015b]. Our first main result on the Continuous Infinite Zeros Problem is that decidability for exponential polynomials of high order is impossible without significant advances in Diophantine approximation:

**Theorem 58.** *If the Continuous Infinite Zeros Problem is decidable for exponential polynomials of order 9, then the Lagrange constant $L_\infty(a)$ may be computed to within arbitrary precision for all real algebraic numbers $a$.*

This is analogous to the hardness result in Chapter 6 for the Unbounded Continuous Skolem Problem (Theorem 51), but since here we are interested in the existence of infinitely many zeros, decidability at high orders yields computability of the Lagrange constant $L_\infty(a)$ in place of the homogeneous Diophantine approximation type $L(a)$. We prove Theorem 58 in Section 7.3.

Our second main result is the following:

**Theorem 59.** *Let $f(t)$ be an exponential polynomial with characteristic roots $\lambda_1, \dots, \lambda_k$ and suppose $span\{\Im(\lambda_j) : j = 1, \dots, k\}$ is a one-dimensional $\mathbb{Q}$-vector space. Then it is decidable whether $f$ has infinitely many zeros and, if there are only finitely many zeros, then there exists a computable bound $T$ such that all zeros of $f$ lie in $[0, T]$.*

We prove this in Section 7.4 using techniques from model theory, specifically, the Cell Decomposition Theorem for functions definable in the first-order language of real closed fields.

Finally, in Section 7.5, we focus on exponential polynomials of low order and establish the central result of this chapter:

**Theorem 60.** *For exponential polynomials of order at most 7, the Continuous Infinite Zeros Problem is decidable, and the Unbounded Continuous Skolem Problem reduces to the Bounded Continuous Skolem Problem.*

At the beginning of Section 7.5, we analyse the possible forms of the given exponential polynomial $f$, thereby outlining the high-level case split. Then in Sections 7.5.1, 7.5.2, 7.5.3 and 7.5.4, we give the full technical details of the proof for each possible shape of $f$, depending on the number of its complex dominant characteristic roots. We employ a wide range of techniques from transcendental number theory, model theory and Diophantine approximation: the Gelfond-Schneider Theorem, the Tarski-Seidenberg Theorem, Kronecker's Approxmation Theorem, Baker's Theorem and decidability of $Th^{\exists}(\mathbb{R}_{exp})$, among others. Theorem 60, together with our results from Chapter 6, specifically Theorem 50, yields the following immediate consequence:

**Corollary 61.** *For exponential polynomials of order at most 7, the Unbounded Continuous Skolem Problem is decidable subject to Schanuel's conjecture.*

## 7.3 Order nine: Diophantine hardness

For a real number $a$, recall the Lagrange constant $L_\infty(a)$:

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

In this section, we will show that a decision procedure for the Continuous Infinite Zeros Problem would yield the computability of $L_\infty(a)$ for all $a \in \mathbb{R} \cap \mathbb{A}$.

Fix positive $a \in \mathbb{R} \cap \mathbb{A}$, $c \in \mathbb{Q}$ and define the functions:

$$\begin{aligned} f_1(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) - c\sin(at), \\ f_2(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) + c\sin(at), \\ f(t) &= e^t(1 - \cos(t)) + t(1 - \cos(at)) - c|\sin(at)| \quad = \min\{f_1(t), f_2(t)\}. \end{aligned}$$

It is easy to see that $f_1(t)$ and $f_2(t)$ are exponential polynomials of order 9, with six characteristic roots: three simple (1 and $1 \pm i$) and three repeated (0 and $\pm ai$). Thus, the problem of determining whether $f_j(t)$ has infinitely many zeros is an instance of the Continuous Infinite Zeros Problem. Moreover, it is easy to check that $f(t)$ has infinitely many zeros if and only if at least one of $f_1(t)$ and $f_2(t)$ has infinitely many zeros.

We will first prove two lemmas which show a connection between the existence of infinitely many zeros of $f(t)$ and the Lagrange constant of $a$.

**Lemma 62.** *Fix $a \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon, c \in \mathbb{Q}$ with $a, c > 0$ and $\varepsilon \in (0, 1)$. If $f(t) = 0$ for infinitely many $t \geq 0$, then $L_\infty(a) \leq c/2\pi^2(1-\varepsilon)$.*

*Proof.* Suppose $f(t) = 0$ for infinitely many $t$. Clearly, this also entails $f(t) = 0$ for infinitely many $t \geq T$, for any particular threshold $T \geq 0$. (Indeed, $f(t) = \min\{f_1(t), f_2(t)\}$ for exponential polynomials $f_1$ and $f_2$ given at the beginning of Section 6.4. Thus, on any bounded interval, $f$ has no more zeros than $f_1$ and $f_2$ combined, i.e., only finitely many, by the analiticity of $f_1$ and $f_2$.) We will show that $T$ can be chosen in such a way that every zero of $f(t)$ on $[T, \infty)$ yields a pair $(n, m) \in \mathbb{N}^2$ which satisfies the inequality

$$\left|a - \frac{n}{m}\right| < \frac{c}{2\pi^2 m^2 (1-\varepsilon)}.$$

This is sufficient, since infinitely many zeros of $f$ yield infinitely many solutions, and therefore witness $L_\infty(a) \leq c/2\pi^2(1-\varepsilon)$.

Thus, consider some $t$ such that $f(t) = 0$ and $t \geq T$ for some threshold $T$ to be specified later. Let $t = 2\pi m + \delta_1$ and $at = 2\pi n + \delta_2$, where $m, n \in \mathbb{N}$ and $\delta_1, \delta_2 \in [-\pi, \pi)$. Then we have

$$\left|a - \frac{n}{m}\right| = \frac{|\delta_2 - a\delta_1|}{2\pi m}.$$

We will show that for $T$ large enough, $f(t) = 0$ for $t \geq T$ allows us to bound $|\delta_2|$ and $|a\delta_1|$ separately from above and then apply the triangle inequality to bound $|\delta_2 - a\delta_1|$.

First, choose $\varphi_1, \varphi_2 \in (0, 1)$ such that $1 - \varphi_2 > 1 - \varphi_1 > 1 - \varepsilon$. Let $T$ be large enough for the following property to hold:

$$\frac{t + \pi}{t - 2\pi} \leq \frac{1 - \varphi_2}{1 - \varphi_1} \text{ for all } t \geq T.$$

In particular, since $m = (t - \delta_1)/2\pi$ and $|\delta_1| \leq \pi$, we have

$$\frac{2m}{2m - 1} \leq \frac{t + \pi}{t - 2\pi} \leq \frac{1 - \varphi_2}{1 - \varphi_1}. \tag{7.1}$$

Let also $T$ be large enough to make the following property valid:

$$\text{if } 1 - \cos(x) \leq c|x|/T \text{ and } |x| \leq \pi, \text{ then } (1 - \varphi_2)x^2/2 \leq 1 - \cos(x). \tag{7.2}$$

Now we have the following chain of inequalities:

$$\begin{aligned}
&1 - \cos(\delta_2) \\
&\leq \{\ f(t) = 0, \text{ noting } e^t(1 - \cos(t)) \geq 0\ \} \\
&\frac{c|\sin(\delta_2)|}{t} \\
&\leq \{\ \text{by } |\sin(x)| \leq |x|\ \} \\
&\frac{c|\delta_2|}{t}.
\end{aligned}$$

Then by (7.2), we have

$$1 - \cos(\delta_2) \geq \frac{(1 - \varphi_2)\delta_2^2}{2}.$$

Thus, combining the upper and lower bounds on $1 - \cos(\delta_2)$ and using (7.1) on the last step, we have

$$|\delta_2| \leq \frac{2c}{t(1 - \varphi_2)} \leq \frac{2c}{(2m - 1)\pi(1 - \varphi_2)} \leq \frac{c}{m\pi(1 - \varphi_1)}.$$

Second, let $\alpha = (1-\varepsilon)^{-1} - (1-\varphi_1)^{-1} > 0$. Let the threshold $T$ be large enough so that

$$e^{-t} \leq \frac{c\alpha^2}{4\pi^2 a^2}\left(\frac{2\pi}{t+\pi}\right)^2 \text{ for } t \geq T \tag{7.3}$$

and

$$\text{if } 1-\cos(x) \leq c/e^T \text{ and } |x| \leq \pi, \text{ then } x^2/4 \leq 1-\cos(x). \tag{7.4}$$

The following chain of inequalities holds:

$$\begin{aligned}
&1-\cos(\delta_1)\\
=&\{ \text{ by } f(t)=0 \}\\
&\frac{c|\sin(\delta_2)| - t(1-\cos(\delta_2))}{e^t}\\
\leq&\{ \text{ by } |\sin(\delta_2)|, |\cos(\delta_2)| \leq 1\}\\
&\frac{c}{e^t}\\
\leq&\{ \text{ by (7.3) } \}\\
&\frac{c^2\alpha^2}{4\pi^2 a^2}\left(\frac{2\pi}{t+\pi}\right)^2\\
\leq&\{ \text{ by } |\delta_1| \leq \pi \}\\
&\frac{c^2\alpha^2}{4\pi^2 a^2}\left(\frac{2\pi}{t-\delta_1}\right)^2\\
=&\{ \text{ } t = 2\pi m + \delta_1 \text{ } \}\\
&\frac{c^2\alpha^2}{4\pi^2 a^2 m^2}.
\end{aligned}$$

Moreover, as $1-\cos(\delta_1) \leq ce^{-t} \leq ce^{-T}$, by (7.4), we have

$$1-\cos(\delta_1) \geq \frac{\delta_1^2}{4},$$

so combining the lower and upper bound on $1-\cos(\delta_1)$, we can conclude

$$|a\delta_1| \leq \frac{c\alpha}{\pi m}.$$

Finally, by the triangle inequality and the bounds on $|a\delta_1|$ and $|\delta_2|$, we have

$$\left|a - \frac{n}{m}\right| = \frac{|\delta_2 - a\delta_1|}{2\pi m} \leq \frac{|\delta_2| + |a\delta_1|}{2\pi m} \leq \frac{c}{2\pi^2 m^2}\left(\alpha + \frac{1}{1-\varphi_1}\right) = \frac{c}{2\pi^2 m^2(1-\varepsilon)}.$$

Now, by the premise of the Lemma, there are infinitely many $t \geq T$ such that $f(t) = 0$, each yielding a pair $(n,m) \in \mathbb{N}^2$ which satisfies the above inequality. These infinitely many pairs $(n,m)$ witness $L_\infty(a) \leq c/2\pi^2(1-\varepsilon)$, as required. □

**Lemma 63.** *Fix $a \in \mathbb{R} \cap \mathbb{A}$ and $\varepsilon, c \in \mathbb{Q}$ with $a, c > 0$ and $\varepsilon \in (0,1)$. If $L_\infty(a) \leq c(1-\varepsilon)/2\pi^2$, then $f(t) = 0$ for infinitely many $t \geq 0$.*

*Proof.* We will show that there exists an effective threshold $M$, dependent on $a, c, \varepsilon$, such that if

$$\left|a - \frac{n}{m}\right| \leq \frac{c(1-\varepsilon)}{2\pi^2 m^2} \tag{7.5}$$

for natural numbers $n, m$ with $m \geq M$, then $f(2\pi m) \leq 0$. Note that this is sufficient to prove the Lemma: the premise guarantees infinitely many solutions $(n,m) \in \mathbb{N}^2$ of (7.5), so there must be infinitely many solutions with $m \geq M$, each yielding $f(2\pi m) \leq 0$. Since $f(t)$ is continuous and moreover is positive for arbitrarily large times, it must have infinitely many zeros on $[2\pi M, \infty)$.

Now let $M$ be large enough, so that $c(1-\varepsilon)/\pi M < \pi$ and

$$\text{if } |x| < c(1-\varepsilon)/\pi M, \text{ then } (1-\varepsilon)|x| \leq |\sin(x)|. \tag{7.6}$$

Suppose that (7.5) holds for $n, m \in \mathbb{N}$ with $m \geq M$ and write $t = 2\pi m$. We will show that $f(t) \leq 0$. By (7.5), we have $|am - n| \leq c(1-\varepsilon)/2\pi^2 m$. Therefore, $at = 2\pi am = 2\pi n + \delta$ where $|\delta| \leq c(1-\varepsilon)/\pi m < \pi$. We have

$$\begin{aligned}
& f(t) \\
= & \{ \text{ as } \cos(t) = 1 \ \} \\
& t(1-\cos(\delta)) - c|\sin(\delta)| \\
\leq & \{ \text{ by (7.6) and } 1-\cos(x) \leq x^2/2 \ \} \\
& \pi m \delta^2 - c(1-\varepsilon)|\delta| \\
\leq & \{ \text{ by } |\delta| \leq c(1-\varepsilon)/\pi m \ \} \\
& 0.
\end{aligned}$$

□

We now use the above lemmas to derive an algorithm to compute $L_\infty(a)$ using an oracle for the Continuous Infinite Zeros Problem, establishing Theorem 58, the central hardness result of this chapter.

Suppose we know $L_\infty(a) \in [p, q]$ for non-negative $p, q \in \mathbb{Q}$. Choose $c \in \mathbb{Q}$ with $c > 0$ and $\varepsilon \in \mathbb{Q}$ with $\varepsilon \in (0, 1)$ such that

$$p < \frac{c(1-\varepsilon)}{2\pi^2} < \frac{c}{2\pi^2(1-\varepsilon)} < q.$$

Write $A = c(1-\varepsilon)/2\pi^2$ and $B = c/2\pi^2(1-\varepsilon)$. Use the oracle for the Continuous Infinite Zeros Problem to determine whether at least one of $f_1(t), f_2(t)$ has infinitely many zeros. If this is the case, then $f(t)$ also has infinitely many zeros, so by Lemma 62, $L_\infty(a) \leq B$ and we continue the approximation recursively on the interval $[p, B]$. If not, then $L(a) \geq A$ by Lemma 63, so we continue on the interval $[A, q]$. Notice that in this procedure, one can choose $c, \varepsilon$ at each stage in such a way that the confidence interval shrinks by at least a fixed factor, whatever the outcome of the oracle invocations. It follows therefore that $L_\infty(a)$ can be approximated to within arbitrary precision.

## 7.4 One linearly independent oscillation: decidability

In this section we consider an exponential polynomial $f(t) = \sum_{j=1}^{k} P_j(t) e^{\lambda_j t}$ under the assumption that the span of $\{\Im(\lambda_j) : j = 1, \ldots, k\}$ is a one-dimensional $\mathbb{Q}$-vector space. We will use fundamental geometric properties of semi-algebraic sets to decide whether or not $f$ has finitely many zeros and, if so, to compute an interval $[0, T]$ that contains all zeros of $f$, thereby establishing Theorem 59.

Write $\lambda_j = a_j + ib_j$, where $a_j, b_j$ are real algebraic numbers for $j = 1, \ldots, k$. By assumption there is a single real algebraic number $b$ such that each $b_j$ is an integer multiple of $b$. Recall that for each integer $n$, both $\cos(nbt)$ and $\sin(nbt)$ can be written as polynomials in $\sin(bt)$ and $\cos(bt)$ with integer coefficients. Using this fact we can write $f$ in the form

$$f(t) = Q(t, e^{a_1 t}, \ldots, e^{a_k t}, \cos(bt), \sin(bt)),$$

for some multivariate polynomial $Q$ with algebraic coefficients.

Now consider the semi-algebraic set

$$E := \left\{ (\boldsymbol{u}, s) \in \mathbb{R}^{k+2} : Q\left(u_0, \ldots, u_k, \tfrac{1-s^2}{1+s^2}, \tfrac{2s}{1+s^2}\right) = 0 \right\}.$$

Recall that $\left\{ \left( \frac{1-s^2}{1+s^2}, \frac{2s}{1+s^2} \right) : s \in \mathbb{R} \right\}$ comprises all points in the unit circle in $\mathbb{R}^2$ except $(-1, 0)$. Indeed, given $\theta \in (-\pi, \pi)$, setting $s := \tan(\theta/2)$ we have $\cos(\theta) = \frac{1-s^2}{1+s^2}$ and $\sin(\theta) = \frac{2s}{1+s^2}$. It follows that $f(t) = 0$ and $\cos(bt) \neq -1$ imply that $(t, e^{a_1 t}, \ldots, e^{a_k t}, \tan(bt/2)) \in E$.

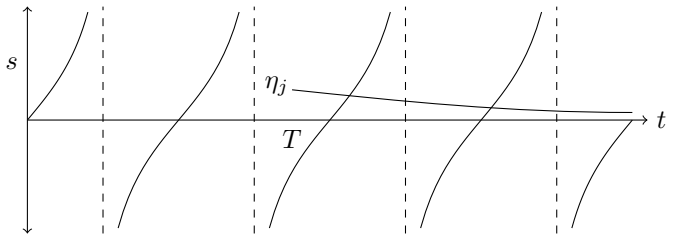



Figure 7.1: Intersection points of $\eta_j(t)$ and $\tan(bt/2)$.

By the Cell Decomposition Theorem for semi-algebraic sets [Marker, 2002], there are semi-algebraic sets $C_1, \ldots, C_m \subseteq \mathbb{R}^{k+2}$, $D_1, \ldots, D_m \subseteq \mathbb{R}^{k+1}$, and continuous semi-algebraic functions $\xi_j, \xi_j^{(1)}, \xi_j^{(2)} : D_j \to \mathbb{R}$ such that $E$ can be written as a disjoint union $E = C_1 \cup \ldots \cup C_m$, where either

$$C_j \quad = \quad \{(\boldsymbol{u}, s) \in \mathbb{R}^{k+2} : \boldsymbol{u} \in D_j \wedge s = \xi_j(\boldsymbol{u})\} \tag{7.7}$$

or

$$C_j \quad = \quad \{(\boldsymbol{u}, s) \in \mathbb{R}^{k+2} : \boldsymbol{u} \in D_j \wedge \xi_j^{(1)}(\boldsymbol{u}) < s < \xi_j^{(2)}(\boldsymbol{u})\} \tag{7.8}$$

Moreover such a decomposition is computable from $E$. Clearly then

$$\{t \in \mathbb{R} : f(t) = 0\} \subseteq \bigcup_{j=1}^{m} \{t \in \mathbb{R} : (t, e^{a_1 t}, \ldots, e^{a_k t}) \in D_j\} \cup Z\,,$$

where $Z := \{t \in \mathbb{R} : \cos(bt) = -1\}$.

The restriction of $f$ to $Z$ is given by $f(t) = Q(t, e^{a_1 t}, \ldots, e^{a_k t}, -1, 0)$. Since this expression is a linear combination of terms of the form $t^j e^{rt}$ for real algebraic $r$, for sufficiently large $t$ the sign of $f(t)$ is determined by the sign of the coefficient of the dominant term. Thus $f$ is either identically zero on $Z$ (in which case $f$ has infinitely many zeros) or we can compute a threshold $T$ such that all zeros of $f$ in $Z$ lie in the interval $[0, T]$.

We now consider zeros of $f$ that do not lie in $Z$. There are two cases. First suppose that each set $\{t \in \mathbb{R} : (t, e^{a_1 t}, \ldots, e^{a_k t}) \in D_j\}$ is bounded for $j = 1, \ldots, m$. In this situation, using Lemma 14, we can compute an upper bound $T$ such that if $f(t) = 0$ then $t < T$. On the other hand, if some set $\{t \in \mathbb{R}_{\geq 0} : (t, e^{a_1 t}, \ldots, e^{a_k t}) \in D_j\}$ is unbounded then, by Lemma 14, it contains an infinite interval $(T, \infty)$. We claim that in this case $f$ must have infinitely many zeros $t \geq 0$. We first give the argument in the case $C_j$ satisfies (7.7).

Define $\eta_j(t) = \xi_j(t, e^{a_1 t}, \ldots, e^{a_k t})$ for $t \in (T, \infty)$. Then for $t \in (T, \infty) \setminus Z$,

$$\begin{aligned} f(t) = 0 \quad &\Longleftarrow \quad (t, e^{a_1 t}, \ldots, e^{a_k t}, \tan(bt/2)) \in C_j \\ &\Longleftrightarrow \quad (t, e^{a_1 t}, \ldots, e^{a_k t}) \in D_j \text{ and } \eta_j(t) = \tan(bt/2)\,. \end{aligned}$$

In other words, $f$ has a zero at each point $t \in (T, \infty) \setminus Z$ at which the graph of $\eta_j$ intersects the graph of $\tan(bt/2)$. Since $\eta_j$ is continuous there are clearly infinitely many such intersection points, see Figure 7.1.

The case when $C_j$ satisifes (7.8) is handled similarly. In fact, this case cannot arise at all, since by the above argument, if $C_j$ satisfies (7.8), then $f$ has a non-trivial interval of zeros. This is impossible, since $f$ is analytic, and hence has only isolated zeros. This completes the proof.

## 7.5 Order at most seven: decidability

We now shift our attention to instances of the Continuous Infinite Zeros Problem of low order. Given an exponential polynomial $f(t)$, we will once again be interested in two questions: does $f$ have infinitely many zeros, and if not, can we derive a bound $T$ such that all zeros of $f$ lie in the interval $[0, T]$? In particular, for exponential polynomials corresponding to differential equations of order at most 7, we settle

both questions, establishing decidability of the Continuous Infinite Zeros Problem and a reduction from the Unbounded Continuous Skolem Problem to the Bounded Continuous Skolem Problem. Both of these results are independent of Schanuel's Conjecture. The latter result, combined with Theorem 50, immediately yields decidability, conditional on Schanuel's Conjecture, for the Unbounded Skolem Problem of order up to 7.

We first restate two useful theorems due to Bell et al. [Bell et al., 2010].

**Theorem 64.** *([Bell et al., 2010, Theorem 12]) Exponential polynomials $f(t)$ with no real dominant characteristic roots have infinitely many zeros.*

**Theorem 65.** *([Bell et al., 2010, Theorem 15]) Suppose we are given an exponential polynomial whose dominant characteristic roots are simple, at least four in number and have imaginary parts linearly independent over $\mathbb{Q}$. Then the existence of infinitely many zeros is decidable. Moreover, if there are finitely many zeros, there exists an effective threshold $T$ such that all zeros are in $[0, T]$.*

We now proceed to prove Theorem 60. Suppose we are given an exponential polynomial $f(t)$ of order at most 7. Sort the characteristic roots according to their real parts, and let $r_j$ denote throughout the $j$-th largest real part of a characteristic root. We will refer to the characteristic roots of maximum real part as the *dominant characteristic roots*. Let also $mul(\lambda)$ denote the multiplicity of $\lambda$ as a root of the characteristic polynomial of $f(t)$.

We will now perform a case analysis on the number of dominant characteristic roots. By Theorem 64, it is sufficient to confine our attention to exponential polynomials with an odd number of dominant characteristic roots. Throughout, we rely on known general forms of solutions to ordinary linear differential equations, outlined in Section 2.3.2.

*Case I.* Suppose first that there is only one dominant, necessarily real, root $r$. Then if we divide $f(t)$ by $e^{rt}$, we have:

$$\frac{f(t)}{e^{rt}} = P_1(t) + \mathcal{O}\left(e^{(r_2-r)t}\right),$$

as the contribution of the non-dominant roots shrinks exponentially, relative to that of the dominant root. Thus, for large $t \geq 0$, the sign of $f(t)$ matches the sign of the leading coefficient of $P_1(t)$, so $f(t)$ cannot have infinitely many zeros. Further, a bound $T$ on the zeros of $f(t)$ can be found easily from the description of $f(t)$.

*Case II.* We now move to the case of three dominant characteristic roots: $r$ and $r \pm ia$, so that

$$\frac{f(t)}{e^{rt}} = P_1(t) + P_2(t)\cos(at) + P_3(t)\sin(at) + \mathcal{O}\left(e^{(r_2-r)t}\right),$$

where $P_1, P_2, P_3 \in (\mathbb{R} \cap \mathbb{A})[x]$ have degrees $d_1 \stackrel{\text{def}}{=} \deg(P_1) \leq mul(r) - 1$ and $d_2 \stackrel{\text{def}}{=} \deg(P_2) = \deg(P_3) \leq mul(r \pm ai)$.

*Case IIa.* Suppose $d_1 > d_2$. Now, it is easy to see that for large $t$ the sign of $f(t)$ matches the sign of the leading coefficient $p_1$ of $P_1(t)$:

$$\frac{f(t)}{e^{rt}t^{d_1}} = p_1 + \mathcal{O}(1/t) + \mathcal{O}\left(e^{(r_2-r)t}\right),$$

so a bound $T$ follows such that $f(t) = 0 \Rightarrow t \leq T$. Similarly, if $d_2 > d_1$, then $f(t)$ clearly has infinitely many zeros. Indeed, if $p_2, p_3$ are the leading coefficients of $P_2, P_3$, respectively, then we have:

$$\begin{aligned}\frac{f(t)}{e^{rt}t^{d_2}} &= p_2\cos(at) + p_3\sin(at) + \mathcal{O}(1/t) + \mathcal{O}\left(e^{(r_2-r)t}\right) \\ &= \frac{\cos(at+\varphi)}{\sqrt{p_2^2+p_3^2}} + \mathcal{O}(1/t) + \mathcal{O}\left(e^{(r_2-r)t}\right)\end{aligned}$$

where $\varphi \in [0, 2\pi)$ with $\tan(\varphi) = -p_3/p_2$, so $f(t)$ is infinitely often positive and infinitely often negative.

Thus, we can now assume $d_1 = d_2$. Notice that since the order of our exponential polynomial is no greater than 7, we must have $d_1 = d_2 \leq 2$.

*Case IIb.* Suppose that $d_1 = d_2 = 2$. Then our function is of the form

$$\frac{f(t)}{e^{rt}} = t(A\cos(at+\varphi_1)+B) + (C\cos(at+\varphi_2)+D) + e^{(r_2-r)t}F,$$

for constants $A, B, C, D, F, a \in \mathbb{R} \cap \mathbb{A}$ with $a > 0$ and $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$. In this case, Theorem 60 follows from Lemma 72 in Section 7.5.4.

*Case IIc.* Suppose that $d_1 = d_2 = 1$, so that

$$\frac{f(t)}{e^{rt}} = A_1\cos(at+\varphi_1) + A_2 + e^{(r_2-r)t}F_1(t),$$

where $A_1, A_2, a \in \mathbb{R} \cap \mathbb{A}$, $a > 0$, $e^{i\varphi_1} \in \mathbb{A}$ and $F_1(t)$ is an exponential polynomial with dominant characteristic root whose real part is 0. Consider first the magnitudes of $A_1$ and $A_2$. If $|A_1| > |A_2|$, then the term $A_1\cos(at+\varphi_1)$ makes $f(t)$ change sign infinitely often, so $f(t)$ must have infinitely many zeros. On the other hand, if $|A_1| < |A_2|$, then $f(t)$ is clearly ultimately positive or ultimately negative, depending on the sign of $A_2$, with an effective threshold beyond which $f(t) \neq 0$. The remaining case is that $|A_1| = |A_2|$. Dividing $f(t)$ by $A_2$, replacing $\varphi_1$ by $\varphi_1 + \pi$ if needed and scaling constants by $A_2$ as necessary, we can assume the function has the form:

$$\frac{f(t)}{e^{rt}} = 1 - \cos(at+\varphi_1) + e^{(r_2-r)t}F_1(t).$$

We now enumerate the possibilities for the dominant characteristic roots of the exponential polynomial $F_1(t)$, that is, the characteristic roots of $f(t)$ with second-largest real part. Since $f(t)$ has order at most 7, there are the following cases to consider:

- $F_1(t)$ has four simple, necessarily complex, dominant roots, so that

  $$\frac{f(t)}{e^{rt}} = 1 - \cos(at+\varphi_1) + e^{(r_2-r)t}(B\cos(bt+\varphi_2) + C\cos(ct+\varphi_3)),$$

  where $B, C, b, c \in \mathbb{R} \cap \mathbb{A}$ with $b, c > 0$ and $e^{i\varphi_2}, e^{i\varphi_3} \in \mathbb{A}$. In this case, Theorem 60 follows from Lemma 68 in Section 7.5.1.

- $F_1(t)$ has some subset of one real and two complex numbers as dominant roots, all simple, so that

  $$\frac{f(t)}{e^{rt}} = 1 - \cos(at+\varphi_1) + e^{(r_2-r)t}(B\cos(bt+\varphi_2) + C) + e^{(r_3-r)t}F_2(t),$$

  where $B, C, b \in \mathbb{R} \cap \mathbb{A}$, $b > 0$, $e^{i\varphi_2} \in \mathbb{A}$ and $F_2(t)$ is an exponential polynomial with dominant characteristic root whose real part is 0. In this case, Theorem 60 follows from Lemma 67 in Section 7.5.1.

- $F_1(t)$ has a repeated real and possibly two simple complex dominant roots, so that

  $$\frac{f(t)}{e^{rt}} = 1 - \cos(at+\varphi_1) + e^{(r_2-r)t}(B\cos(bt+\varphi_2) + P(t)) + e^{(r_3-r)t}F_2(t),$$

  where $B, b \in \mathbb{R} \cap \mathbb{A}$, $b > 0$, $e^{i\varphi_2} \in \mathbb{A}$, and $P(t) \in (\mathbb{R} \cap \mathbb{A})[x]$ is non-constant. Now, if the leading coefficient of $P(t)$ is negative, then $f(t)$ will be infinitely often negative (consider large times $t$ such that $\cos(at+\varphi_1) = 1$) and infinitely often positive (consider large times $t$ such that $\cos(at+\varphi_1) = 0$), so $f(t)$ must have infinitely many zeros. On the other hand, if the leading coefficient of $P(t)$ is positive, then it is easy to see that $f(t)$ is ultimately positive, with an effective threshold.

- $F_1(t)$ has a repeated pair of complex roots, so that

  $$\frac{f(t)}{e^{rt}} = 1 - \cos(at+\varphi_1) + e^{(r_2-r)t}(Bt\cos(bt+\varphi_2) + C\cos(bt+\varphi_3)),$$

  where $B, C, b \in \mathbb{R} \cap \mathbb{A}$, $b > 0$ and $e^{i\varphi_2}, e^{i\varphi_3} \in \mathbb{A}$. In this case, Theorem 60 follows from Lemma 69 in Section 7.5.1.

*Case III.* We now consider the case of five dominant characteristic roots. Let these be $r$, $r \pm ai$ and $r \pm bi$. If $r \pm ai$ are repeated, i.e., $mul(r \pm ai) \geq 2$, then we must have $mul(r) = mul(r \pm bi) = 1$, since otherwise the order of our exponential polynomial exceeds 7. Then by an argument analogous to *Case IIa* above, $f(t)$ must have infinitely many zeros. The situation is symmetric when $mul(r \pm bi) \geq 2$. Similarly, if $mul(r) \geq 2$, then $mul(r \pm ai) = mul(r \pm bi) = 1$, since otherwise the instance exceeds order 7. Then by the same argument as in *Case IIa*, $f(t)$ is ultimately positive or ultimately negative, with an effectively computable threshold $T$. Thus, we may assume that all the dominant roots are simple, so the exponential polynomial is of the form:

$$\frac{f(t)}{e^{rt}} = A\cos(at + \varphi_1) + B\cos(bt + \varphi_2) + C + e^{(r_2 - r)t}F(t),$$

where $A, B, C, a, b \in \mathbb{R} \cap \mathbb{A}$, $a, b > 0$, $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$ and $F(t)$ is an exponential polynomial of order at most 2 whose dominant characteristic roots have real part equal to 0. In this case, Theorem 60 follows from Lemma 70 in Section 7.5.2.

*Case IV.* Finally, suppose there are seven dominant characteristic roots: $r$, $r \pm ai$, $r \pm bi$ and $r \pm ci$. Since we are limiting ourselves to instances of order 7, these roots must all be simple, and there can be no other characteristic roots. Thus, the exponential polynomial has the form

$$\frac{f(t)}{e^{rt}} = A\cos(at + \varphi_1) + B\cos(bt + \varphi_2) + C\cos(ct + \varphi_3) + D,$$

with $A, B, C, D, a, b, c \in \mathbb{R} \cap \mathbb{A}$ with $a, b, c > 0$ and $e^{i\varphi_1}, \ldots, e^{i\varphi_3} \in \mathbb{A}$. In this case, Theorem 60 follows from Lemma 71 in Section 7.5.3.

### 7.5.1 One dominant oscillation

**Lemma 66.** *Let $A, B, a, b, r \in \mathbb{R} \cap \mathbb{A}$ where $a, b, r > 0$. Let $\varphi_1, \varphi_2 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$. Suppose also that $a, b$ are linearly dependent over $\mathbb{Q}$ and that whenever $1 - \cos(at + \varphi_1) = 0$, it holds that $A\cos(bt + \varphi_2) + B > 0$. Define the function*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{-rt}(A\cos(bt + \varphi_2) + B).$$

*Then $f(t) = \Omega(e^{-rt})$, that is, there exist effective constants $T \geq 0$ and $c > 0$ such that for $t \geq T$, we have $f(t) \geq ce^{-rt}$.*

*Proof.* The case of $A = 0$ is easy: by the premise of the Lemma, we have $B > 0$ and then $f(t) \geq Be^{-rt}$ for all $t$. Thus, assume $A \neq 0$ throughout. Let the linear dependence between $a, b$ be given by $an_1 - bn_2 = 0$ for $n_1, n_2 \in \mathbb{N}$ coprime and let $\mathcal{C}$ be the equivalence class of $-\varphi_1/a$ modulo $2\pi/a$, that is,

$$\mathcal{C} = \left\{ \frac{-\varphi_1 + 2k\pi}{a} \,\middle|\, k \in \mathbb{Z} \right\}.$$

We will refer to $\mathcal{C}$ as the set of *critical points* throughout.

It is clear that at critical points, we have $1 - \cos(at + \varphi_1) = 0$. Moreover, the linear dependence of $a, b$ entails that for each fixed value of $(\cos(at), \sin(at))$, there are only finitely many possible values for $(\cos(bt), \sin(bt))$. Indeed, we have

$$e^{ibt} \in \{\omega e^{iatn_1} \,|\, \omega \text{ an } n_2\text{-th root of unity}\},$$

so in particular, for $t \in \mathcal{C}$, we have

$$e^{ibt} \in \{\omega e^{-in_1\varphi_1} \,|\, \omega \text{ an } n_2\text{-th root of unity}\}.$$

Thus, the possible values of $(\cos(bt), \sin(bt))$ for $t$ critical are algebraic and effectively computable. Let $M = \min\{A\cos(bt + \varphi_2) + B \,|\, t \in \mathcal{C}\}$. By the premise of the Lemma, we have $M > 0$.

Let $t_1, t_2, \ldots, t_j, \ldots$ be the non-negative critical points. Note that by construction we have $|t_j - t_{j-1}| = 2\pi/a$. For each $t_j$, define the *critical region* to be the interval $[t_j - \delta, t_j + \delta]$, where we define

$$\delta = \frac{M}{2|A|b}.$$

Let $g(t) = A\cos(bt + \varphi_2) + B$ and notice that $g'(t) \leq |A|b$ everywhere. We first prove the claim for $t$ inside critical regions: suppose $t$ lies in a critical region and let $j$ minimise $|t - t_j| \leq \delta$. Then by the Mean Value Theorem, we have

$$|g(t) - g(t_j)| \leq |t - t_j||A|b \leq \delta|A|b = \frac{M}{2},$$

so

$$g(t) \geq g(t_j) - \frac{M}{2} \geq \frac{M}{2},$$

whence $f(t) \geq e^{-rt}g(t) \geq Me^{-rt}/2 = \Omega(e^{-rt})$.

Now suppose $t$ is outside all critical regions and let $j$ minimise $|t - t_j|$. Since the distance between critical points is $2\pi/a$ by construction, we have $a|t - t_j| \leq \pi$. Therefore,

$$1 - \cos(at + \varphi_1) = 1 - \cos(at - at_j) \geq \frac{|a(t - t_j)|^2}{2} > \frac{(a\delta)^2}{2} = \frac{a^2M^2}{8|A|^2b^2} > 0.$$

Thus, there exists a computable constant $D > 0$ such that $f(t) = 1 - \cos(at + \varphi_1) + e^{-rt}g(t) \geq D$ for all large enough $t$ outside critical regions.

Combining the two results, we have $f(t) = \Omega(e^{-rt})$ everywhere. □

**Lemma 67.** *Let $C, D, a, b, r_1, r_2$ be real algebraic numbers such that $a, b, r_1, r_2 > 0$ and $C, D$ are not both 0. Let also $\varphi_1, \varphi_2 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{-r_1t}(C\cos(bt + \varphi_2) + D) + e^{-(r_1+r_2)t}F(t).$$

*Here $F(t)$ is an exponential polynomial whose dominant characteristic roots are purely imaginary. Suppose also that $f(t)$ has order at most 7. Then it is decidable whether $f(t)$ has infinitely many zeros. Moreover, if $f(t)$ has only finitely many zeros, then there exists an effectively computable threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* Notice that the dominant term of $f(t)$ is always non-negative, so the function is positive for arbitrarily large $t$. Thus, $f(t) = 0$ for some $t$ if and only if $f(t) \leq 0$ for some $t$, and analogously, $f(t)$ has infinitely many zeros if and only if $f(t) \leq 0$ infinitely often. We can eliminate the case $|D| > |C|$, since then $f(t)$ is clearly ultimately positive or oscillating, depending on the sign of $D$. Thus, we can assume $|D| \leq |C|$.

We now consider two cases, depending on whether $a/b \in \mathbb{Q}$.

*Case I.* Suppose first that $a, b$ are linearly independent over $\mathbb{Q}$. By Lemma 12, the trajectory $(at + \varphi_1 \bmod 2\pi, bt + \varphi_2 \bmod 2\pi)$ is dense in $[0, 2\pi)^2$, and moreover the restriction of this trajectory to $at + \varphi_1 \bmod 2\pi = 0$ is dense in $\{0\} \times [0, 2\pi)$.

If $|D| < |C|$, then we argue that $f(t)$ is infinitely often negative, and hence has infinitely many zeros. Indeed, $|D| < |C|$ entails the existence of a non-trivial interval $I \subseteq [0, 2\pi)$ such that

$$t \bmod 2\pi \in I \Rightarrow C\cos(bt + \varphi_2) + D < 0.$$

What is more, we can in fact find $\epsilon > 0$ and a subinterval $I' \subseteq I$ such that

$$t \bmod 2\pi \in I' \Rightarrow C\cos(bt + \varphi_2) + D < -\epsilon.$$

Thus, by density, $1-\cos(at+\varphi_1) = 0$ and $C\cos(bt+\varphi_2)+D < -\epsilon$ will infinitely often hold simultaneously. Then just take $t$ large enough to ensure, say, $|e^{-r_2t}F(t)| < \epsilon/2$ at these infinitely many points, and the claim follows.

Thus, suppose now $|C| = |D|$. Replacing $\varphi_2$ by $\varphi_2 + \pi$ if necessary, we can write the function as:

$$f(t) = 1 - \cos(at + \varphi_1) + De^{-r_1t}(1 - \cos(bt + \varphi_2)) + e^{-(r_1+r_2)t}F(t).$$

As $a, b$ are linearly independent, for all $t$ large enough, $1 - \cos(at + \varphi_1)$ and $1 - \cos(bt + \varphi_2)$ cannot simultaneously be 'too small'. More precisely, Lemma 13 in [Bell et al., 2010] uses Baker's Theorem to

prove that the linear independence of $a, b$ over $\mathbb{Q}$ entails the existence of effective constants $E, T, N > 0$ such that for all $t \geq T$, we have

$$1 - \cos(at + \varphi_1) > E/t^N \text{ or } 1 - \cos(bt + \varphi_2) > E/t^N.$$

Now, if $D < 0$, it is easy to show that $f(t)$ has infinitely many zeros. Indeed, consider the times $t$ where the dominant term $1 - \cos(at + \varphi_1)$ vanishes. For all large enough such $t$, since $t^{-N}$ shrinks more slowly than $e^{-r_2 t}$, we will have

$$\begin{aligned} f(t) &= e^{-r_1 t} D(1 - \cos(bt + \varphi_2)) + e^{-(r_1+r_2)t} F(t) \\ &< e^{-r_1 t}(EDt^{-N} + e^{-r_2 t} F(t)) \\ &\leq e^{-r_1 t} \frac{1}{2} EDt^{-N} \\ &< 0, \end{aligned}$$

so $f(t)$ has infinitely many zeros. Similarly, if $D > 0$, we can show that $f(t)$ is ultimately positive. Indeed, for all $t$ large enough, we have

$$\begin{aligned} f(t) &\geq e^{-r_1 t} D(1 - \cos(bt + \varphi_2)) + e^{-(r_1+r_2)t} F(t) \\ &> e^{-r_1 t} DEt^{-N} + e^{-(r_1+r_2)t} F(t) \\ &> 0, \end{aligned}$$

or

$$\begin{aligned} f(t) &\geq 1 - \cos(at + \varphi_1) + e^{-(r_1+r_2)t} F(t) \\ &> Et^{-N} + e^{-(r_1+r_2)t} F(t) \\ &> 0. \end{aligned}$$

Therefore, $f(t)$ has only finitely many zeros, all occurring up to some effective bound $T$.

*Case II.* Now suppose $a, b$ are linearly dependent. By the premise of the Lemma, the order of $F(t)$ is at most 2 (in fact, at most 1 if $D \neq 0$). However, by Theorem 59, the claim follows immediately for all cases in which the characteristic roots of $F(t)$ are all real or complex but with frequencies linearly dependent on $a$. Thus, the only remaining case to consider is the function

$$f(t) = 1 - \cos(at + \varphi_1) + e^{-r_1 t} C \cos(bt + \varphi_2) + e^{-(r_1+r_2)t} H \cos(ct + \varphi_3),$$

where $H, c \in \mathbb{R} \cap \mathbb{A}$, $c > 0$ and $a/c \notin \mathbb{Q}$.

As explained at the beginning of the proof of Lemma 66, due to the linear dependence of $a, b$ over $\mathbb{Q}$, when $1 - \cos(at + \varphi_1) = 0$, there are only finitely many possibilities for the value of $C \cos(bt + \varphi_2)$, each algebraic, effectively computable and occurring periodically. If at least one of these values is non-positive, then by the linear independence of $a, c$ over $\mathbb{Q}$, we will simultaneously have $1 - \cos(at + \varphi_1) = 0$, $C \cos(bt + \varphi_2) \leq 0$ and $H \cos(ct + \varphi_3) < 0$ infinitely often, which yields $f(t) < 0$ infinitely often and entails the existence of infinitely many zeros. On the other hand, if at the critical points $1 - \cos(at + \varphi_1) = 0$ we always have $C \cos(bt + \varphi_2) > 0$, then by Lemma 66, we have

$$1 - \cos(at + \varphi_1) + e^{-r_1 t} C \cos(bt + \varphi_2) = \Omega(e^{-r_1 t}),$$

whereas obviously

$$\left| e^{-(r_1+r_2)t} H \cos(ct + \varphi_3) \right| = \mathcal{O}(e^{-(r_1+r_2)t}).$$

An effective threshold $T$ follows such that for $t \geq T$, $f(t)$ is ultimately positive. □

**Lemma 68.** *Let $A, B, a, b, c, r$ be real algebraic numbers such that $a, b, c, r > 0$, $A, B \neq 0$. Let also $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = 1 - \cos(ct + \varphi_3) + e^{-rt}(A\cos(at + \varphi_1) + B\cos(bt + \varphi_2)).$$

*Then it is decidable whether $f(t)$ has infinitely many zeros. Moreover, if $f(t)$ has only finitely many zeros, then there exists an effective threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* We argue the function is infinitely often positive and infinitely often negative by looking at the values of $t$ for which the dominant term $1 - \cos(ct + \varphi_3)$ vanishes. This happens precisely at the times $t = -(\varphi_3 + 2k\pi)/c$ for $k \in \mathbb{Z}$, giving rise to a discrete restriction of $f$:

$$g(k) \stackrel{\text{def}}{=} e^{r\varphi_3}\left(e^{2\pi r}\right)^k \left(A\cos\left(k\frac{2\pi a}{c} - \frac{a\varphi_3}{c} + \varphi_1\right) + B\cos\left(k\frac{2\pi b}{c} - \frac{b\varphi_3}{c} + \varphi_2\right)\right)$$

This is a linear recurrence sequence over $\mathbb{R}$ of order 4, with characteristic roots $e^{2\pi(r \pm ia/c)}$ and $e^{2\pi(r \pm ib/c)}$. In particular, it has no real dominant characteristic root. It is well-known that real-valued linear recurrence sequences with no dominant real characteristic root are infinitely often positive and infinitely often negative: see for example [Győri and Ladas, 1991, Theorem 7.1.1]. Therefore, by continuity, $f(t)$ must have infinitely many zeros. □

**Lemma 69.** *Let $A, B, a, b, r$ be real algebraic numbers such that $a, b, r > 0$, $A \neq 0$. Let also $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = 1 - \cos(at + \varphi_1) + e^{-rt}(At\cos(bt + \varphi_2) + B\cos(bt + \varphi_3)).$$

*Then it is decidable whether $f(t)$ has infinitely many zeros. Moreover, if $f(t)$ has only finitely many zeros, then there exists an effective threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* If $a/b \in \mathbb{Q}$, then the claim follows immediately from Theorem 59. If $a/b \notin \mathbb{Q}$, then by Lemma 12, it will happen infinitely often that $1 - \cos(at + \varphi_1) = 0$ and $At\cos(bt + \varphi_2) < -|A|t/2$. Then clearly $f(t) < 0$ infinitely often. Since $f(t) > 0$ infinitely often as well, due to the non-negative dominant term $1 - \cos(at + \varphi_1)$, it follows that $f(t)$ has infinitely many zeros. □

### 7.5.2 Two dominant oscillations

**Lemma 70.** *Let $A, B, C, a, b, r$ be real algebraic numbers such that $a, b, r > 0$, $a \neq b$ and $A, B, C \neq 0$. Let also $\varphi_1, \varphi_2 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = A\cos(at + \varphi_1) + B\cos(bt + \varphi_2) + C + e^{-rt}F(t).$$

*where $F(t)$ is an exponential polynomial whose dominant characteristic roots are purely imaginary. Suppose also $f(t)$ has order at most 8. It is decidable whether $f(t)$ has infinitely many zeros, and moreover, if $f(t)$ has only finitely many zeros, then there exists an effective threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* If the frequencies $a, b$ of the dominant term's oscillations are linearly independent over $\mathbb{Q}$, then the claim follows immediately by Theorem 65. Therefore, assume $na - mb = 0$ for some $n, m \in \mathbb{N}^+$. Notice that $a \neq b$ guarantees $n \neq m$. We perform the change of variable $t \to tm/a$, so that:

$$f(t) = A\cos(mt + \varphi_1) + B\cos(nt + \varphi_2) + C + e^{-rmt/a}F(tm/a).$$

Using the standard trigonometric identities, we express the dominant term as a polynomial in $\sin(t), \cos(t)$:

$$f(t) = P(\sin(t), \cos(t)) + e^{-rmt/a}F(tm/a),$$

where $P \in (\mathbb{R} \cap \mathbb{A})[x, y]$ has effectively computable coefficients. It is clear that the dominant term is periodic. It is immediate from the definition of exponential polynomials and the premise of the Lemma that $F(tm/a) \stackrel{\text{def}}{=} F_2(t)$ is an exponential polynomial in $t$, of the same order as $F(t)$, also with

purely imaginary dominant characteristic roots. Let $\alpha(t) = P(\sin(t), \cos(t))$, $r_2 = rm/a > 0$ and $\beta(t) = e^{-rmt/a}F(tm/a) = e^{-r_2 t}F_2(t)$.

We are now interested in the extrema of $P(\sin(t), \cos(t))$. Let

$$M_1 = \min_{x^2+y^2=1} P(x, y) = \min_{t \geq 0} \alpha(t),$$
$$M_2 = \max_{x^2+y^2=1} P(x, y) = \max_{t \geq 0} \alpha(t).$$

We can construct defining formulas $\phi_1(u), \phi_2(u)$ in the first-order language $\mathcal{L}$ of real closed fields for $M_1, M_2$, so that each $\phi_j(u)$ holds precisely for the valuation $u = M_j$. Then performing quantifier elimination on these formulas using Renegar's algorithm [Renegar, 1992], we convert $\phi_1, \phi_2$ into the form

$$\phi_j(u) \equiv \bigvee_l \bigwedge_k P_{l,k}(u) \sim_{l,k} 0,$$

where $P_{l,k}$ are polynomials with integer coefficients and each $\sim_{l,k}$ is either $<$ or $=$. Now $\phi_j(u)$ must have a satisfiable disjunct. Using the decidability of the theory $Th(\mathbb{R})$, we can readily identify this disjunct. Moreover, since $\phi_j(u)$ has a unique satisfying valuation, namely $u = M_j$, this disjunct must contain at least one equality predicate. It follows immediately that $M_1, M_2$ are algebraic. Moreover, we can effectively compute from $\phi_j(u)$ a representation for $M_j$ consisting of its minimal polynomial and a sufficiently accurate rational approximation to distinguish $M_j$ from its Galois conjugates. By an analogous argument, the pairs $(\sin(t), \cos(t))$ at which $P(\sin(t), \cos(t))$ achieves the extrema $M_1, M_2$ are also algebraic and effectively computable.

We now perform a case analysis on the signs of $M_1$ and $M_2$.

- First, if $0 < M_1 \leq M_2$, then $f(t)$ cannot have infinitely many zeros: if $t$ is large enough to ensure $|\beta(t)| < M_1$, we have $f(t) > 0$.
- Second, if $M_1 \leq M_2 < 0$, then by the same reasoning, the function will ultimately be strictly negative.
- Third, if $M_1 < 0 < M_2$, then $f(t)$ oscillates around 0: for all $t$ such that $\alpha(t) = M_1 < 0$ and large enough to ensure $|\beta(t)| < |M_1|$, we will have $f(t) < 0$, and similarly, for large enough $t$ such that $\alpha(t) = M_2 > 0$, we will have $f(t) > 0$, so the function must have infinitely many zeros.
- Next, we argue that the case $M_1 = M_2 = 0$ is impossible. Indeed, if $M_1 = M_2 = 0$, then $\alpha(t) = P(\sin(t), \cos(t))$ is identically zero, and the same holds for all derivatives of $\alpha(t)$. Thus, from $\alpha'(t) \equiv \alpha'''(t) \equiv 0$, we have

  $$0 \equiv -Am \sin(mt + \varphi_1) - Bn \sin(nt + \varphi_2),$$
  $$0 \equiv Am^3 \sin(mt + \varphi_1) + Bn^3 \sin(nt + \varphi_2).$$

  Multiplying the first identity through by $m^2$ and summing, we have

  $$Bn \sin(nt + \varphi_2)(n^2 - m^2) \equiv 0.$$

  By the premise of the Lemma, $B \neq 0$, so $n(n - m)(n + m) = 0$, which is a contradiction.
- Finally, only the symmetric cases $M_1 < M_2 = 0$ and $0 = M_1 < M_2$ remain. Without loss of generality, by replacing $f(t)$ by $-f(t)$ if necessary, we need only consider the case $0 = M_1 < M_2$.

Thus, assume $0 = M_1 < M_2$. We now move our attention to the possible forms of $F_2(t)$. Since $f(t)$ has order at most 8, it follows that $F_2(t)$ has order at most 3. Thus, there are three possibilities for the set of dominant characteristic roots of $F_2(t)$: $\{0\}$, $\{\pm ic\}$, or $\{0, \pm ic\}$, for some positive $c \in \mathbb{R} \cap \mathbb{A}$. We consider each of these cases in turn.

First, if $F_2(t)$ only has the real dominant eigenvalue 0, then $F_2(t)$ is ultimately positive or ultimately negative, depending on the sign of the most significant term of $F_2(t)$, with an effectively computable

threshold. Ultimate positivity of $F_2(t)$ entails ultimate positivity of $f(t)$ as well, since $P(\sin(t), \cos(t)) \geq 0$ everywhere, whereas an ultimately negative $F_2(t)$ makes $f(t)$ change sign infinitely often.

Second, assume the dominant characteristic roots of $F_2(t)$ are $\{\pm ic\}$, so that

$$f(t) = P(\sin(t), \cos(t)) + e^{-r_2 t}\left(D\cos(ct + \varphi_3) + Ee^{-r_3 t}\right)$$

for some $r_3 > 0$ and $\varphi_3 \in \mathbb{R}$ such that $e^{i\varphi_3} \in \mathbb{A}$. Without loss of generality, we can assume $c \notin \mathbb{Q}$, since otherwise, we are done by Theorem 59. But by Lemma 12, it will happen infinitely often that $P(\sin(t), \cos(t)) = 0$ and $D\cos(ct + \varphi_3) < -|D|/2$, say. For large enough such $t$, $|Ee^{-(r_2+r_3)t}| < |D|/4$, so we conclude that $f(t)$ is infinitely often negative, and hence has infinitely many zeros.

Third, assume the dominant characteristic roots of $F_2(t)$ are $\{0, \pm ic\}$, so that

$$f(t) = P(\sin(t), \cos(t)) + e^{-r_2 t}(D\cos(ct + \varphi_3) + E).$$

We again assume $c \notin \mathbb{Q}$, since otherwise the claim follows from Theorem 59. Let $M_3 = E - |D| = \min_{t\geq 0} F_2(t)$. If $M_3 > 0$, then $f(t)$ clearly has no zeros. If $M_3 < 0$, then there exists a non-trivial interval $I \subseteq [0, 2\pi)$ such that if $ct + \varphi_3 \bmod 2\pi \in I$, then $F_2(t) < 0$. Since $c \notin \mathbb{Q}$, Lemma 12 guarantees that $F_2(t) < 0 = P(\sin(t), \cos(t))$ happens infinitely often, so $f(t)$ must have infinitely many zeros. Finally, if $M_3 = 0$, we argue that $f(t)$ is ultimately positive. Indeed, since $P(\sin(t), \cos(t))$ and $F_2(t)$ are both non-negative everywhere, $f(t) = 0$ can only happen if $P(\sin(t), \cos(t)) = D\cos(ct + \varphi_3) + E = 0$. This, however, would entail $e^{it} \in \mathbb{A}$ and $e^{ict} \in \mathbb{A}$, which contradicts the Gelfond-Schneider Theorem, since $c \notin \mathbb{Q}$. Thus, we conclude $f(t)$ has no zeros.

□

### 7.5.3 Three dominant oscillations

**Lemma 71.** *Let $A, B, C, a, b, c$ be real algebraic numbers such that $a, b, c > 0$ and $A, B, C \neq 0$. Let also $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2}, e^{i\varphi_3} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = A\cos(at + \varphi_1) + B\cos(bt + \varphi_2) + C\cos(ct + \varphi_3) + D.$$

*It is decidable whether $f(t)$ has infinitely many zeros, and moreover, if $f(t)$ has only finitely many zeros, then there exists an effective threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* The argument consists of three cases, depending on the linear dependencies over $\mathbb{Q}$ satisfied by $a, b$ and $c$.

*Case I.* First, if $a, b, c$ are linearly independent over $\mathbb{Q}$, then the claim follows directly from Theorem 65.

*Case II.* Second, suppose that $a, b, c$ are all rational multiples of one another:

$$b = \frac{n}{m}a,\ c = \frac{k}{l}a \text{ where } n, m, k, l \in \mathbb{N}^+.$$

We make the change of variable $t \to tml$ to obtain:

$$f(t) = A\cos((at)ml + \varphi_1) + B\cos((at)nl + \varphi_2) + C\cos((at)km + \varphi_3) + D = P(\sin(at), \cos(at)),$$

where $P \in \mathbb{A}[x, y]$ is a polynomial obtained using the standard trigonometric identities. It is now clear that $f(t)$ is periodic, so it has either no zeros or infinitely many zeros. Let

$$M_1 = \min_{x^2+y^2=1} P(x, y) = \min_{t\geq 0} f(t),$$
$$M_2 = \max_{x^2+y^2=1} P(x, y) = \max_{t\geq 0} f(t).$$

Using the same reasoning as in Lemma 70, we see that $M_1, M_2$ are algebraic and effectively computable: simply construct defining formulas in the first-order language $\mathcal{L}$ of real closed fields, and then perform quantifier elimination using Renegar's algorithm [Renegar, 1992]. Then $f(t)$ clearly has infinitely many zeros if and only if $M_1 \leq 0 \leq M_2$.

*Case III.* Finally, suppose that $a, b, c$ span a $\mathbb{Q}$-vector space of dimension 2, so that $a, b, c$ satisfy a single linear dependence $am + bn + cp = 0$ where $m, n, p \in \mathbb{Z}$ are coprime. At most one of the ratios $a/b$, $a/c$ and $b/c$ is rational (otherwise we have $\dim span\{a, b, c\} = 1$), so assume without loss of generality that $a/c \notin \mathbb{Q}$ and $b/c \notin \mathbb{Q}$.

Define the set

$$\begin{aligned}\mathbb{T} &= \left\{x \in [0, 2\pi)^3 \,\middle|\, \forall u \in \mathbb{Z}^3 \,.\, u \cdot (a, b, c) \in 2\pi\mathbb{Z} \Rightarrow u \cdot x \in 2\pi\mathbb{Z}\right\} \\ &= \left\{(x_1, x_2, x_3) \in [0, 2\pi)^3 \,\middle|\, mx_1 + nx_2 + px_3 = 0 \in 2\pi\mathbb{Z}\right\}\end{aligned}$$

Notice that if $mx_1 + nx_2 + px_3 = 2k\pi$ for $x_1, x_2, x_3$, then $k \leq |m| + |n| + |p|$, so $\mathbb{T}$ partitions naturally into finitely many subsets: $\mathbb{T} = \bigcup_{k=1}^{N} \mathbb{T}_k$, where we define

$$\mathbb{T}_k = \left\{(x_1, x_2, x_3) \in [0, 2\pi)^3 \,\middle|\, mx_1 + nx_2 - px_3 = 2k\pi\right\}.$$

Consider the trajectory $h(t) = \{(at, bt, ct) \bmod 2\pi \,|\, t \geq 0\}$. Define also the sets $R = \{h(2k\pi) \,|\, k \in \mathbb{N}\}$ and $H = \{h(t) \,|\, t \geq 0\}$. Because of the linear dependence satisfied by $a, b, c$, it is easy to see that $R \subseteq H \subseteq \mathbb{T}$. By Kronecker's Theorem, $R$ is a dense subset of $\mathbb{T}$, so clearly $H$ must be a dense subset of $\mathbb{T}$ as well.

Now define the function

$$F(x_1, x_2, x_3) = A\cos(x_1 + \varphi_1) + B\cos(x_2 + \varphi_2) + C\cos(x_3 + \varphi_3) + D,$$

so that the image of $f(t)$ is exactly $\{F(x_1, x_2, x_3) \,|\, (x_1, x_2, x_3) \in H\}$. Let also the extrema of $F$ over $\mathbb{T}$ be:

$$\begin{aligned}M_1 &= \min_{\mathbb{T}} F(x_1, x_2, x_3), \\ M_2 &= \max_{\mathbb{T}} F(x_1, x_2, x_3).\end{aligned}$$

Both of these values are algebraic and can be computed using quantifier elimination in the first-order language $\mathcal{L}$ of the real numbers: just use separate variables for $\cos(x_j), \sin(x_j)$ and apply the standard trigonometric identities to convert the linear dependence on $x_1, x_2, x_3$ into a polynomial dependence between $\cos(x_j), \sin(x_j)$.

Now, by the density of $H$ in $\mathbb{T}$, if $M_1 < 0 < M_2$, then $f(t)$ must clearly be infinitely often positive and infinitely often negative, so it must have infinitely many zeros. The case $M_1 < 0 = M_2$ is symmetric to $0 = M_1 < M_2$ (just replace $f$ and $F$ by $-f$ and $-F$, respectively), so without loss generality, we can assume $0 = M_1 < M_2$. In this case, we argue that $f(t)$ has no zeros, that is, even though $F$ vanishes on some points in $\mathbb{T}$, none of these points appear in the dense subset $H$. Indeed, consider the set

$$Z = \{(\cos(x_1), \sin(x_1), \ldots, \cos(x_3), \sin(x_3)) \,|\, (x_1, x_2, x_3) \in \mathbb{T}, F(x_1, x_2, x_3) = 0\}.$$

Note that $Z$ is clearly semi-algebraic, as one can directly write a defining formula in $\mathcal{L}$ from $F(x_1, x_2, x_3) = 0$ and $mx_1 + nx_2 + px_3 \in 2\pi\mathbb{Z}$. Moreover, by the Zero-Dimensionality Lemma [Ouaknine and Worrell, 2014a, Lemma 10], the function $F(x_1, x_2, x_3)$ achieves its minimum $M_1 = 0$ at only finitely many points in $\mathbb{T}_k$, for each $k$. Since $\mathbb{T}$ is the union of finitely many $\mathbb{T}_k$, we immediately have that $Z$ is finite. By the Tarski-Seidenberg Theorem, projecting $Z$ to any fixed component will also give a finite, semi-algebraic subset of $\mathbb{R}$, that is, a finite subset of $\mathbb{A}$. Thus, we have shown that if $F(x_1, x_2, x_3) = 0$, then $e^{ix_j} \in \mathbb{A}$ for all $j = 1, 2, 3$. Now if $f(t) = 0$ for some $t \geq 0$, then we must have $e^{ati}, e^{cti} \in \mathbb{A}$, which by the Gelfond-Schneider Theorem entails $a/c \in \mathbb{Q}$, a contradiction. □

### 7.5.4 One repeated oscillation

**Lemma 72.** *Let $A, B, C, D, a, r$ be real algebraic numbers such that $a, r > 0$ and $A \neq 0$. Let also $\varphi_1, \varphi_2 \in \mathbb{R}$ be such that $e^{i\varphi_1}, e^{i\varphi_2} \in \mathbb{A}$. Define the exponential polynomial $f(t)$ by*

$$f(t) = t(A\cos(at + \varphi_1) + B) + (C\cos(at + \varphi_2) + D) + e^{-rt}F(t)$$

*where $F(t)$ is an exponential polynomial with purely imaginary dominant characteristic roots. Suppose also that $f(t)$ has order at most 8. It is decidable whether $f(t)$ has infinitely many zeros, and moreover, if $f(t)$ has only finitely many zeros, then there exists an effective threshold $T$ such that all zeros of $f(t)$ are contained in $[0, T]$.*

*Proof.* Since $f(t)$ has order no greater than 8, it follows that $F(t)$ has order at most 2. Therefore, $F(t)$ must be of the form $E\cos(bt+\varphi_3)$ for some $E, b \in \mathbb{R} \cap \mathbb{A}$, $b > 0$, such that $a/b \notin \mathbb{Q}$, and some $\varphi_3$ such that $e^{i\varphi_3} \in \mathbb{A}$, since otherwise the imaginary parts of the characteristic roots of $f(t)$ are pairwise linearly dependent over $\mathbb{Q}$, so our claim is proven immediately by Theorem 59.

Consider first the magnitudes of $A$ and $B$. If $|A| > |B|$, then the term $tA\cos(at+\varphi_1)$ makes $f(t)$ change sign infinitely often, whereas if $|B| > |A|$, then for $t$ large enough, the term $tB$ makes $f(t)$ ultimately positive or ultimately negative, depending on the sign of $B$. Thus, we can assume $|A| = |B|$. Dividing $f(t)$ by $B$, and replacing $\varphi_1$ by $\varphi_1 + \pi$ if necessary, we can assume the function has the form:

$$f(t) = t(1-\cos(at+\varphi_1)) + (C\cos(at+\varphi_2)+D) + e^{-rt}E\cos(bt+\varphi_3).$$

Considering the dominant term, it is clear that $f(t)$ is infinitely often positive. Let $\alpha(t) = t(1-\cos(at+\varphi_1))$, $\beta(t) = C\cos(at+\varphi_2)+D$ and $\gamma(t) = e^{-rt}E\cos(bt+\varphi_3)$.

We now focus on the sign of the term $\beta(t)$ at the positive *critical times* $t_j \stackrel{\text{def}}{=} -\varphi_1/a + 2j\pi/a$ $(j \in \mathbb{Z})$ when $1-\cos(at+\varphi_1)$ vanishes. Notice that $\beta(t_j) = C\cos(\varphi_2-\varphi_1)+D \stackrel{\text{def}}{=} M$ is independent of $j$. First, if $M < 0$, then for all $t_j$ large enough, $f(t_j) < 0$, so the function must have infinitely many zeros. Second, if $M = 0$, then by the linear independence of $a, b$ and Lemma 12, we have $\alpha(t_j) = \beta(t_j) = 0 > \gamma(t_j)$ for infinitely many $t_j$, so we can conclude $f(t)$ has infinitely many zeros.

Finally, suppose $M > 0$. We will prove that $f(t)$ is ultimately positive. For each $t_j$, define the *critical region* $[t_j - \delta_j, t_j + \delta_j]$, given by

$$\delta_j = \frac{2\sqrt{|C|+|D|}}{a\sqrt{t_{j-1}}}.$$

From here onwards, we only consider $t$ large enough for any two adjacent critical regions to be disjoint. The argument consists of two parts: first we show $f(t) > 0$ for all large enough $t$ outside all critical regions, and then we show $f(t) > 0$ for large enough $t$ in a critical region.

Suppose $t$ is outside all critical regions and let $j$ minimise $|t-t_j|$. Since the distance between critical points is $2\pi/a$ by construction, we have $a|t-t_j| \le \pi$. Therefore,

$$\frac{|a(t-t_j)|^2}{2} \le 1-\cos(at-at_j) = 1-\cos(at+\varphi_1).$$

On the other hand, we have the following chain of inequalities:

$$\begin{aligned}
&\frac{|a(t-t_j)|^2}{2} \\
&> \{\ |t-t_j| > \delta_j\ \} \\
&\frac{(a\delta_j)^2}{2} \\
&= \{\ \text{definition of } \delta_j\ \} \\
&\frac{2(|C|+|D|)}{t_{j-1}} \\
&> \{\ \text{by } t > t_{j-1}\ \} \\
&\frac{2(|C|+|D|)}{t} \\
&\ge \{\ \text{triangle inequality and } |\cos(x)| \le 1\ \} \\
&\frac{|C|+|D|}{t} + \frac{|C\cos(at+\varphi_2)+D|}{t}.
\end{aligned}$$

Combining, we have

$$\alpha(t)+\beta(t) \ge \alpha(t) - |\beta(t)| = t(1-\cos(at+\varphi_1)) - |C\cos(at+\varphi_2)+D| \ge |C|+|D|.$$

Thus, if $t$ is large enough to ensure $|\gamma(t)| < |C|+|D|$, we have $f(t) > 0$ outside critical regions.

For the second part of the argument, we consider $t$ in critical regions. Notice that the values of $\beta(t)$ on $[t_j-\delta_j, t_j+\delta_j]$ are independent of the choice of $t_j$. Moreover, we have $\beta(t_j) = M > 0$, so there exists

some $\epsilon > 0$ such that for all $t \in [t_j - \epsilon, t_j + \epsilon]$, we have $\beta(t) \geq M/2$, say. Now for any critical point $t_j$ chosen large enough, we will have $[t_j - \delta_j, t_j + \delta_j] \subseteq [t_j - \epsilon, t_j + \epsilon]$, so $\beta(t) > M/2$ on the entire critical region. Let also $t_j$ be large enough so that for any $t$ in the critical region, we have $|\gamma(t)| < M/2$. Then we have $f(t) = \alpha(t) + \beta(t) + \gamma(t) \geq \beta(t) - |\gamma(t)| > 0$, completing the claim. $\square$

# Chapter 8

# Continuous Orbit Problem

*Prerequisites:* Sections 2.1.1 and 2.1.3.

## 8.1 Introduction

We conclude this thesis with one final result on continuous-time linear dynamical systems. Recall that thus far, we have studied reachability of an $(m-1)$-dimensional hyperplane in $\mathbb{R}^m$. As in the discrete-time setting, one can generalise this problem by decoupling the dimension of the target space from that of the ambient space. This yields the *Continuous Orbit Problem:* given $\boldsymbol{x}(0) \in \mathbb{R}^m$, $\boldsymbol{A} \in \mathbb{R}^{m \times m}$, a vector subspace $\mathcal{V} \subseteq \mathbb{R}^m$ specified by a basis $\boldsymbol{y_1}, \ldots, \boldsymbol{y_d}$ and an interval $I$, determine whether there exists $t \in I$ such that the state $\boldsymbol{x}(t)$ at time $t$ of the continuous-time linear dynamical system $(\boldsymbol{A}, \boldsymbol{x}(0))$ lies in $\mathcal{V}$. As in Chapters 6 and 7, for the purposes of representing the input data effectively, we will assume all entries of $\boldsymbol{A}, \boldsymbol{x}(0), \boldsymbol{y_1}, \ldots, \boldsymbol{y_d}$ and the endpoints of $I$ are real algebraic.

In this chapter, we will study the Continuous Orbit Problem with one-dimensional target subspace $\mathcal{V}$. This builds upon the work of [Hainry, 2008], where reachability to a single point was shown decidable, and [Chen et al., 2015], which further refined the upper bound to **PTIME**.

## 8.2 Main result and outline

The main result of this chapter is the following:

**Theorem 73.** *The Continuous Orbit Problem with one-dimensional target space is decidable.*

Our proof technique is similar to the one employed for the Discrete Orbit Problem with one-dimensional target in Chapter 4. By resorting to a spectral decomposition, in Section 8.3.1, we show that the matrix equation $e^{\boldsymbol{A}t}\boldsymbol{x}(0) = \kappa \boldsymbol{y}$ has the same set of solutions $(t, \kappa) \in \mathbb{R}^2$ as a Master System of equations based on the eigenvalues of $\boldsymbol{A}$. Then in Section 8.3.2, we employ the Gelfond-Schneider Theorem and the Lindemann-Weierstrass Theorem to provide sufficient conditions for the negativity of the problem instance, thereby significantly limiting the possible shapes of the Master System. Finally, in Section 8.3.3, we show how to solve the constrained Master System by explicitly manipulating the equations whilst preserving the set of solutions at each step. Two notable cases arise, depending on whether all eigenvalues of $\boldsymbol{A}$ are dominant, in the sense of having the same real part. In a manner reminiscent of the case analysis of Section 4.4, one case limits the unknown $t$ to at most one candidate value, whilst the other case admits the possibility of infinitely many witnesses $t$ on $\mathbb{R}_{\geq 0}$. In both cases, we rely crucially on Baker's Theorem in order to verify via numerical approximation whether given linear forms of logarithms of algebraic numbers are zero.

## 8.3 One-dimensional target space: decidability

### 8.3.1 Master System of equations

Suppose we are given $\boldsymbol{A} \in (\mathbb{R} \cap \mathbb{A})^{m \times m}$, $\boldsymbol{x}, \boldsymbol{y} \in (\mathbb{R} \cap \mathbb{A})^m$ and an interval $I \subseteq \mathbb{R}_{\geq 0}$ with algebraic endpoint(s), and wish to decide whether there exists $t \in I$ such that $e^{\boldsymbol{A}t}\boldsymbol{x}$ lies in the $\mathbb{R}$-vector space $span\{\boldsymbol{y}\}$.

In the spirit of Chapter 4, we first construct a Master System in the exponent $t \in \mathbb{R}$ and the coefficient $\kappa \in \mathbb{R}$ witnessing $e^{\boldsymbol{A}t}\boldsymbol{x} \in span\{\boldsymbol{y}\}$. Let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues of $\boldsymbol{A}$, and let $mul(\lambda_j)$ denote the algebraic multiplicity of each eigenvalue $\lambda_j$. Let the Jordan form of $\boldsymbol{A}$ be $\boldsymbol{M^{-1}JM}$, where

$$\boldsymbol{J} = diag\{\boldsymbol{J_1}, \ldots, \boldsymbol{J_k}\}$$

is composed of Jordan blocks, one for each eigenvalue $\lambda_j$, with size $mul(\lambda_j)$. Recall that the matrix exponential is given by

$$e^{\boldsymbol{A}t} = \boldsymbol{M^{-1}}\, diag\left(e^{\boldsymbol{J_1}t}, \ldots, e^{\boldsymbol{J_k}t}\right) \boldsymbol{M},$$

together with the well-known closed form for the exponential of a Jordan block $\boldsymbol{J_s}$ with eigenvalue $\lambda_s$:

$$\left(e^{\boldsymbol{J_s}t}\right)_{j,l} = \begin{cases} e^{\lambda_s t}\frac{t^{j-l}}{(j-l)!}, & \text{if } j \geq l \\ 0 & \text{otherwise.} \end{cases}$$

Thus, the equation $e^{\boldsymbol{A}t}\boldsymbol{x} = \kappa\boldsymbol{y}$ is equivalent to

$$\begin{bmatrix} e^{(t\boldsymbol{J_1})} & 0 & \ldots & 0 \\ 0 & e^{(t\boldsymbol{J_2})} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & e^{(t\boldsymbol{J_k})} \end{bmatrix} \boldsymbol{Mx} = \kappa \boldsymbol{My}. \tag{8.1}$$

We refer to (8.1) as the *Master System*. Carrying out the multiplication shows that each eigenvalue $\lambda_j$ contributes exactly $mul(\lambda_j)$ equations to the Master System, each of the form

$$e^{t\lambda_j} P_{j,l}(t) = \kappa y_{j,l}, \tag{8.2}$$

where $l$ assumes all values in $\{0, \ldots, mul(\lambda_j) - 1\}$, $P_{j,l} \in \mathbb{A}[x]$ with $\deg(P_{j,l}) \leq l$ has rational multiples of the entries of $\boldsymbol{Mx}$ as coefficients, and $y_{j,l} \in \mathbb{A}$ are the entries of $\boldsymbol{My}$ in some order. Adapting the notation of Chapter 4, let $eq(\lambda_j, l)$ denote the equation (8.2).

### 8.3.2 Preliminaries

Before proceeding, we make some preliminary calculations. First, check directly whether $t = 0$ is a solution. Second, use the algorithm of [Hainry, 2008] to check whether there exists a witness $t$ with $\kappa = 0$. Henceforth, we will assume $t \neq 0$ and $\kappa \neq 0$.

Next, consider $eq(\lambda_j, 0)$ for some eigenvalue $\lambda_j$. Since $\deg(P_{j,l}) \leq l$ for all $l$, the polynomial $P_{j,0}(t)$ is a constant. If $P_{j,0} = 0$, then since $\kappa \neq 0$ by assumption, we must have $y_{j,0} = 0$, otherwise the Master System is unsatisfiable and the problem instance is negative. Then $eq(\lambda_j, 0)$ trivially holds for all $t, \kappa$, so we can remove it from the Master System without altering the set of solutions. Moreover, it is easy to see from the formula for the exponential of a Jordan block that the leading coefficient of $P_{j,l}$ for all $l \leq mul(\lambda_j) - 1$ is a rational multiple of $P_{j,0}$. Thus, if $P_{j,0} = 0$, then in (8.1), we can remove the corresponding components of $\boldsymbol{Mx}$ and $\boldsymbol{My}$, and replace $e^{\boldsymbol{J_j}t}$ with the exponential of a Jordan block with dimension one less, in order to remove the trivially satisfied equation from the Master System. By repeating this process, we can ensure that the least-order equation contributed by each eigenvalue has a non-zero left-hand side and, since $\kappa \neq 0$, a non-zero right-hand side. Thus, for any $j \neq s$, we can always eliminate the coefficient $\kappa$ from $eq(\lambda_j, 0) \wedge eq(\lambda_s, 0)$ by asserting the ratio of the left-hand sides equals the ratio of the right-hand sides.

However, we will ensure that the eigenvalues used in the Master System remain closed under complex conjugation. Thus, if in the above process we remove all the equations referring to some complex

eigenvalue $\overline{\lambda_j}$, but at least one equation remains which refers to $\lambda_j$, say $e^{t\lambda_j}P_{j,0} = \kappa y_{j,0}$, we introduce into the Master System the (equivalent) equation $e^{t\overline{\lambda_j}}\overline{P_{j,0}} = \kappa\overline{y_{j,0}}$.

We will refer to the resulting Master System as *reduced*. From here onwards, we will use the word eigenvalue to refer exclusively to eigenvalues of $\boldsymbol{A}$ which contribute at least one equation to the reduced Master System. Moreover, for an eigenvalue $\lambda$, we redefine $mul(\lambda)$ to mean the number of equations in the reduced Master System contributed by $\lambda$. Now, we show that the imaginary parts of all complex eigenvalues must be rational multiples of one another, otherwise the problem instance is immediately negative.

**Lemma 74.** *The reduced Master System has no solution if there are two distinct pairs of complex eigenvalues $(\lambda_1, \overline{\lambda_1})$ and $(\lambda_2, \overline{\lambda_2})$ such that $\Im(\lambda_1)/\Im(\lambda_2)$ is irrational.*

*Proof.* Let $\lambda_j = r_j + ib_j$ for $j = 1, 2$, and consider the least-order equation contributed by each of the four complex eigenvalues:

$$e^{t(r_1+ib_1)}x_1 = \kappa y_1 \tag{8.3}$$
$$e^{t(r_2+ib_2)}x_2 = \kappa y_2 \tag{8.4}$$
$$e^{t(r_1-ib_1)}x_3 = \kappa y_3 \tag{8.5}$$
$$e^{t(r_2-ib_2)}x_4 = \kappa y_4, \tag{8.6}$$

for algebraic $x_1, \ldots, x_4, y_1, \ldots, y_4$. Since the Master System is reduced, we have $x_j, y_j \neq 0$ for $j = 1, \ldots, 4$. Eliminating $\kappa$ from (8.3) and (8.5) shows that $e^{2itb_1}$ is algebraic. Similarly, eliminating $\kappa$ from (8.4) and (8.6) shows $e^{2itb_2}$ is algebraic as well. Then by Theorem 3 (Gelfond-Schneider), $t = 0$ or $b_1/b_2 \in \mathbb{Q}$ must hold, which is a contradiction. □

Next, we prove another criterion for unsatisfiability of the reduced Master System.

**Lemma 75.** *The reduced Master System has no solution if there are at least two distinct eigenvalues $\lambda_1, \lambda_2$ and $mul(\lambda_1) > 1$.*

*Proof.* Suppose that $\lambda_1$ and $\lambda_2$ are distinct eigenvalues with $\lambda_1$ contributing at least two equations. Then we have

$$e^{t\lambda_1}x_1 = \kappa y_1 \tag{8.7}$$
$$e^{t\lambda_1}(x_1 t + x_2) = \kappa y_2 \tag{8.8}$$
$$e^{t\lambda_2}x_3 = \kappa y_3 \tag{8.9}$$

with $x_j, y_j \in \mathbb{A}$ for all $j$, and $x_1, x_3, y_1, y_2, y_3 \neq 0$. Eliminating $\kappa$ from (8.7) and (8.8), we see $t = (y_2x_1 - x_2y_1)/x_1y_1 \in \mathbb{A}$. On the other hand, eliminating $\kappa$ from (8.7) and (8.9) gives $e^{t(\lambda_1-\lambda_2)} = y_1x_3/x_1y_3 \in \mathbb{A}$. Thus, both $t(\lambda_1 - \lambda_2)$ and $e^{t(\lambda_1-\lambda_2)}$ are algebraic. Then by Lemma 5, we must have $t(\lambda_1 - \lambda_2) = 0$, which is a contradiction. □

### 8.3.3 Decision method

We now proceed with the main decision method. First, we handle the situation where the Master System refers to only one, necessarily real, eigenvalue $\lambda$. Then the Master System is of the form

$$\bigwedge_{j=0}^{mul(\lambda)-1} e^{t\lambda}P_j(t) = \kappa y_j$$

for $y_j \in \mathbb{A}$ and polynomials $P_j \in \mathbb{A}[x]$. Notice that $(t, \kappa)$ is a solution of the Master System if and only if $(t, \kappa e^{-t\lambda})$ is a solution of the Master System obtained by setting $\lambda$ to zero, so we may assume without loss of generality that $\lambda = 0$. Then eliminating $\kappa$ from each pair of equations, we see that the problem instance is positive if and only if there exists $t \in I$ such that

$$\bigwedge_{0\leq j<s<mul(\lambda)} y_sP_j(t) - y_jP_s(t) = 0,$$

which we can determine by directly obtaining the roots of each polynomial $y_sP_j - y_jP_s \in \mathbb{A}[x]$ (see [Kaltofen, 1982]) and checking whether a common real root in $I$ exists.

Thus, we can now assume there are at least two eigenvalues. By Lemma 75, each eigenvalue contributes exactly one equation to the Master System. By Lemma 74, the imaginary parts of the eigenvalues must be rational multiples of one another. Thus, let $\lambda_1, \ldots, \lambda_k$ be the eigenvalues, with $k \geq 2$, $\lambda_j = r_j + iq_jb$ with $r_j, b \in \mathbb{R} \cap \mathbb{A}$ and $q_j \in \mathbb{Q}$, and let the Master System be

$$\bigwedge_{j=1}^{k} e^{t\lambda_j} x_j = \kappa y_j, \tag{8.10}$$

where $x_j, y_j \in \mathbb{A}$. Eliminating $\kappa$ from (8.10), we see the problem instance is positive if and only there exists some $t \in I$ such that

$$\bigwedge_{1 \leq j < s \leq k} e^{t(\lambda_j - \lambda_s)} = \frac{y_j x_s}{y_s x_j}. \tag{8.11}$$

Writing $z_{j,s} = y_j x_s / y_s x_j \in \mathbb{A}$ and $\varphi_{j,s} = \arg(z_{j,s})$, we can observe that (8.11) is equivalent to

$$\bigwedge_{1 \leq j < s \leq k} e^{t(r_j - r_s)} = |z_{j,s}| \wedge e^{itb(q_j - q_s)} = e^{i\varphi_{j,s}}. \tag{8.12}$$

Now, if $r_j = r_s$, then the condition $e^{t(r_j - r_s)} = |z_{j,s}|$ is either unsatisfiable, rendering the problem instance immediately negative, or satisfied by all $t$, depending on whether $|z_{j,s}| = 1$. On the other hand, if $r_j \neq r_s$, then this condition is equivalent to $t = \log|z_{j,s}|/(r_j - r_s)$, thereby limiting $t$ to at most one value. Thus, we consider the following two cases separately.

*Case I.* Suppose first that not all eigenvalues have the same real part, that is, there exist $j, s$ such that $r_j \neq r_s$. Then (8.12) is equivalent to

$$\left( \bigwedge_{r_j \neq r_s} t = \frac{\log|z_{j,s}|}{r_j - r_s} \right) \wedge \left( \bigwedge_{1 \leq j < s \leq k} tb(q_j - q_s) \equiv \varphi_{j,s} \bmod 2\pi \right). \tag{8.13}$$

To verify the satisfiability of the first conjunct, we need to be able to check the validity of equalities of the form $A\log(B) = C\log(D)$ given $A, B, C, D \in \mathbb{R} \cap \mathbb{A}$. We can do this using Theorem 6 (Baker), which yields a computable lower bound $E$ such that if $A\log(B) - C\log(D) \neq 0$, then $|A\log(B) - C\log(D)| > E$. We approximate $A\log(B) - C\log(D)$ until we can determine its sign, or until our approximation yields $|A\log(B) - C\log(D)| < E$, at which point we conclude $A\log(B) - C\log(D) = 0$.

We apply this procedure to each pair of constraints in the first conjunct of (8.13) to determine whether each constraint is satisfied by the same value of $t$. If not, then the problem instance is negative. Otherwise, (8.13) is equivalent to

$$t = A\log(B) \wedge \left( \bigwedge_{1 \leq j < s \leq k} tb(q_j - q_s) \equiv \varphi_{j,s} \bmod 2\pi \right), \tag{8.14}$$

for some effectively computable $A, B \in \mathbb{R} \cap \mathbb{A}$.

Next, we use the same technique to check each constraint of the second conjunct of (8.14) is satisfied by this $t$. Calculate

$$g(l) = Ab(q_j - q_s)\log(B) - \varphi_{j,s} + 2l\pi$$

for $l = 0, \pm 1, \pm 2, \ldots$ using Theorem 6 (Baker) to determine for which $l$ the sign of $g(l)$ changes. If $g(l) = 0$ for some $l \in \mathbb{Z}$, then the constraint $tb(q_j - q_s) \equiv \varphi_{j,s}$ is satisfied, otherwise (8.14) is unsatisfiable and the problem instance is negative.

If all such constraints are satisfied, then (8.14) is equivalent to $t = A\log(B)$, and all that remains is to check whether $t \in I$. This can also be done using approximation: since $t$ is transcendental by Lemma 5 whilst the endpoints of $I$ are algebraic, a sufficiently precise approximation of $t$ is guaranteed to distinguish $t$ from the endpoints of $I$ and hence determine whether $t \in I$.

*Case II.* Second, suppose that all eigenvalues have the same real part. Then (8.12) is equivalent to

$$\bigwedge_{1 \leq j < s \leq k} e^{itb(q_j - q_s)} = e^{i\varphi_{j,s}}. \tag{8.15}$$

Recall that $e^{i\varphi_{j,s}} = z_{j,s}/|z_{j,s}|$ is algebraic for all $j, s$, and $q_j$ is rational for all $j$. Let $q_j - q_s = n_{j,s}/m_{j,s}$ for coprime integers $n_{j,s}, m_{j,s}$. Then (8.15) is equivalent to

$$\bigwedge_{1 \le j < s \le k} e^{itb} \in \{\omega e^{im_{j,s}\varphi_{j,s}} : \omega \text{ an } n_{j,s}\text{-th root of unity}\}. \tag{8.16}$$

The sets on the right-hand side of (8.16) are finite subsets of $\mathbb{A}$, so we can compute them directly and obtain their intersection. If this intersection is empty, then the problem instance is immediately negative. Otherwise, (8.16) is equivalent to

$$\bigvee_j e^{itb} = A_j,$$

for algebraic numbers $A_j$ on the unit circle.

Without loss of generality, assume there is only one disjunct, so that we have to decide whether there exists $t \in I$ such that $e^{itb} = A$, with $A \in \mathbb{A}$ and $|A| = 1$. Writing $A = e^{i\varphi}$, we need to decide whether $g(l) = (\varphi + 2l\pi)/b$ lies in $I$ for some $l \in \mathbb{Z}$. Since $e^{ibg(l)} = A \in \mathbb{A}$, it follows from Lemma 5 that $g(l)$ is transcendental, whilst the endpoints of $I$ are algebraic. Thus, for any fixed $l$, we can compare $g(l)$ with the endpoints of $I$ using a sufficiently precise approximation. Then it suffices to consider $l = 0, \pm 1, \pm 2, \ldots$ in turn, until we determine for which $l$ the relative position on the real line of $g(l)$ and the interval $I$ changes. The problem instance is positive if and only if some $l \in \mathbb{Z}$ exists such that $g(l) \in I$.

# Bibliography


[Akshay et al., 2015] Akshay, S., Antonopoulos, T., Ouaknine, J., and Worrell, J. (2015). Reachability problems for markov chains. *Information Processing Letters*, 115(2):155–158.

[Alias et al., 2010] Alias, C., Darte, A., Feautrier, P., and Gonnord, L. (2010). Multi-dimensional rankings, program termination, and complexity bounds of flowchart programs. In *Static Analysis*, pages 117–133. Springer.

[Alur, 2015] Alur, R. (2015). *Principles of Cyber-Physical Systems*. MIT Press.

[Alur et al., 1995] Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T. A., Ho, P.-H., Nicollin, X., Olivero, A., Sifakis, J., and Yovine, S. (1995). The algorithmic analysis of hybrid systems. *Theoretical computer science*, 138(1):3–34.

[Alur and Dill, 1994] Alur, R. and Dill, D. L. (1994). A theory of timed automata. *Theoretical computer science*, 126(2):183–235.

[Arvind and Vijayaraghavan, 2011] Arvind, V. and Vijayaraghavan, T. (2011). The orbit problem is in the GapL hierarchy. *J. Comb. Optim.*, 21(1):124–137.

[Asarin et al., 1995] Asarin, E., Maler, O., and Pnueli, A. (1995). Reachability analysis of dynamical systems having piecewise-constant derivatives. *Theoretical computer science*, 138(1):35–65.

[Baker, 1975] Baker, A. (1975). *Transcendental number theory.* Cambridge University Press, Cambridge.

[Baker and Wüstholz, 1993] Baker, A. and Wüstholz, G. (1993). Logarithmic forms and group varieties. *Jour. Reine Angew. Math.*, 442:19–62.

[Bell and Gerhold, 2007] Bell, J. P. and Gerhold, S. (2007). On the positivity set of a linear recurrence sequence. *Israel Journal of Mathematics*, 157(1):333–345.

[Bell et al., 2010] Bell, P. C., Delvenne, J.-C., Jungers, R. M., and Blondel, V. D. (2010). The Continuous Skolem-Pisot Problem. *Theoretical Computer Science*, 411(40-42):3625–3634.

[Ben-Amram and Genaim, 2013] Ben-Amram, A. M. and Genaim, S. (2013). On the linear ranking problem for integer linear-constraint loops. In *Proceedings of the 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '13, pages 51–62, New York, NY, USA. ACM.

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

[Ben-Amram et al., 2012] Ben-Amram, A. M., Genaim, S., and Masud, A. N. (2012). On the termination of integer loops. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 34(4):16.

[Berstel and Mignotte, 1976] Berstel, J. and Mignotte, M. (1976). Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Société Mathématique de France*, 104:175–184.

[Blanksby and Montgomery, 1971] Blanksby, P. and Montgomery, H. (1971). Algebraic integers near the unit circle. *Acta Arith.*, pages 355–369.

[Blondel and Portier, 2002] Blondel, V. and Portier, N. (2002). The presence of a zero in an integer linear recurrent sequence is NP-hard to decide.

[Bradley et al., 2005] Bradley, A. R., Manna, Z., and Sipma, H. B. (2005). Termination analysis of integer linear loops. In *CONCUR 2005–Concurrency Theory*, pages 488–502. Springer.

[Braverman, 2006] Braverman, M. (2006). Termination of integer linear programs. In *Proceedings of the 18th International Conference on Computer Aided Verification*, CAV, LNCS 4144, pages 372–385. Springer.

[Brent, 1976] Brent, R. P. (1976). Fast multiple-precision evaluation of elementary functions. *J. ACM*, 23(2):242–251.

[Burke and Webb, 1981] Burke, J. R. and Webb, W. A. (1981). Asymptotic behavior of linear recurrences.

[Cai, 1994] Cai, J.-y. (1994). Computing Jordan normal forms exactly for commuting matrices in polynomial time. *International Journal of Foundations of Computer Science*, 5(03n04):293–302.

[Chen et al., 2012] Chen, H. Y., Flur, S., and Mukhopadhyay, S. (2012). Termination proofs for linear simple loops. *International Journal on Software Tools for Technology Transfer*, 17(1):47–57.

[Chen et al., 2015] Chen, T., Yu, N., and Han, T. (2015). Continuous-time orbit problems are decidable in polynomial-time. *Inf. Process. Lett.*, 115(1):11–14.

[Chonev et al., 2013] Chonev, V., Ouaknine, J., and Worrell, J. (2013). The orbit problem in higher dimensions. In *STOC*, pages 941–950. ACM.

[Chonev et al., 2015a] Chonev, V., Ouaknine, J., and Worrell, J. (2015a). On the decidability of the Bounded Continuous Skolem Problem. *CoRR*, abs/1506.00695.

[Chonev et al., 2015b] Chonev, V., Ouaknine, J., and Worrell, J. (2015b). On the decidability of the continuous infinite zeros problem. *CoRR*, abs/1507.03632.

[Chonev et al., 2015c] Chonev, V., Ouaknine, J., and Worrell, J. (2015c). The polyhedron-hitting problem. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 940–956. SIAM.

[Chonev et al., 2016] Chonev, V., Ouaknine, J., and Worrell, J. (2016). On the complexity of the orbit problem. *Journal of the ACM*.

[Cohen, 1993] Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*. Springer.

[Cohn, 2002] Cohn, P. M. (2002). *Basic Algebra: Groups, Rings and Fields*. Springer.

[Colón and Sipma, 2001] Colón, M. A. and Sipma, H. B. (2001). Synthesis of linear ranking functions. In *Tools and Algorithms for the Construction and Analysis of Systems*, pages 67–81. Springer.

[Cook et al., 2006] Cook, B., Podelski, A., and Rybalchenko, A. (2006). Termination proofs for systems code. In *ACM SIGPLAN Notices*, volume 41, pages 415–426. ACM.

[Cox et al., 2007] Cox, D. A., Little, J., and O'Shea, D. (2007). *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer.

[Cusick and Flahive, 1989] Cusick, T. W. and Flahive, M. E. (1989). *The Markoff and Lagrange Spectra*. American Mathematical Society.

[D'Aquino et al., 2014] D'Aquino, P., Macintyre, A., and Terzo, G. (2014). From Schanuel's conjecture to Shapiro's conjecture. *Comment. Math. Helv.*, 89(3):597–616.

[Derksen et al., 2005] Derksen, H., Jeandel, E., and Koiran, P. (2005). Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39(3):357–371.

[Everest et al., 2003] Everest, G., van der Poorten, A., Ward, T., and Shparlinski, I. (2003). *Recurrence Sequences*. American Mathematical Society.

[Evertse, 1984] Evertse, J.-H. (1984). On sums of $S$-units and linear recurrences. *Compositio Mathematica*, 53(2):225–244.

[Feautrier, 1992] Feautrier, P. (1992). Some efficient solutions to the affine scheduling problem. I. one-dimensional time. *International journal of parallel programming*, 21(5):313–347.

[Gelfond, 1934] Gelfond, A. O. (1934). On Hilbert's seventh problem. In *Dokl. Akad. Nauk. SSSR*, volume 2, pages 1–6.

[Gelfond and Vinogradov, 1934] Gelfond, A. O. and Vinogradov, I. (1934). Sur le septieme probleme de Hilbert. *Bull. Acad. Sci. URSS*, pages 623–634.

[Graça et al., 2008] Graça, D. S., Campagnolo, M. L., and Buescu, J. (2008). Computability with polynomial differential equations. *Advances in Applied Mathematics*, 40(3):330–349.

[Grünbaum et al., 1967] Grünbaum, B., Klee, V., Perles, M. A., and Shephard, G. C. (1967). *Convex polytopes*. Springer.

[Guy, 2004] Guy, R. (2004). *Unsolved Problems in Number Theory*. Springer, third edition.

[Győri and Ladas, 1991] Győri, I. and Ladas, G. (1991). *Oscillation Theory of Delay Differential Equations: with Applications*. Oxford mathematical monographs. Oxford University Press.

[Hainry, 2008] Hainry, E. (2008). Reachability in linear dynamical systems. In *Logic and Theory of Algorithms*, pages 241–250. Springer.

[Hainry, 2009] Hainry, E. (2009). Decidability and undecidability in dynamical systems.

[Halava et al., 2006] Halava, V., Harju, T., and Hirvensalo, M. (2006). Positivity of second order linear recurrent sequences. *Discrete Applied Mathematics*, 154(3):447–451.

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

[Hardy and Wright, 1999] Hardy, G. and Wright, E. (1999). An introduction to the theory of numbers. *Oxford*, 1:979.

[Harrison, 1969] Harrison, M. A. (1969). *Lectures on Linear Sequential Machines*. New York: Academic Press.

[Hurwitz, 1891] Hurwitz, A. (1891). Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche. *Mathematische Annalen*, 39(2):279–284.

[Kaltofen, 1982] Kaltofen, E. (1982). Polynomial factorization. In *(B. Buchberger, G. Collins, and R. Loos, editors) Computer Algebra*, pages 95–113. Springer.

[Kannan and Lipton, 1986] Kannan, R. and Lipton, R. (1986). Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821.

[Kannan and Lipton, 1980] Kannan, R. and Lipton, R. J. (1980). The orbit problem is decidable. In *Proceedings of the twelfth annual ACM symposium on Theory of computing*, STOC, pages 252–261. ACM.

[Khachiyan and Porkolab, 1997] Khachiyan, L. and Porkolab, L. (1997). Computing integral points in convex semi-algebraic sets. In *Foundations of Computer Science, 1997. Proceedings., 38th Annual Symposium on*, pages 162–171. IEEE.

[Khinchin, 1926] Khinchin, A. (1926). Zur metrischen Theorie der diophantischen Approximationen. *Mathematische Zeitschrift*, 24(1):706–714.

[Khinchin, 1961] Khinchin, A. (1961). Continued fractions. *Mat. Lit.*

[Khovanskii, 1980] Khovanskii, A. G. (1980). On a class of systems of transcendental equations. In *Soviet Math. Dokl*, volume 22, pages 762–765.

[Koiran et al., 1994] Koiran, P., Cosnard, M., and Garzon, M. (1994). Computability with low-dimensional dynamical systems. *Theoretical Computer Science*, 132(1):113–128.

[Kronecker, 1875] Kronecker, L. (1875). Zwei Sätze über Gleichungen mit ganzzahligen Koeffizienten. *J. Reine Angew. Math.*, 53:173–175.

[Lafferriere et al., 2001] Lafferriere, G., Pappas, G. J., and Yovine, S. (2001). Symbolic reachability computation for families of linear vector fields. *J. Symb. Comput.*, 32(3):231–253.

[Lagarias and Shallit, 1997] Lagarias, J. C. and Shallit, J. O. (1997). Linear fractional transformations of continued fractions with bounded partial quotients. *Journal de Théorie des Nombres de Bordeaux*, 9.

[Lang, 1966] Lang, S. (1966). Introduction to transcendental numbers. *Reading, Mass.*

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

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

[Lenstra et al., 1982] Lenstra, A. K., Lenstra, H. W., and Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534.

[Litow, 1997] Litow, B. (1997). A decision method for the rational sequence problem. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 4.

[Macintyre and Wilkie, 1996] Macintyre, A. and Wilkie, A. J. (1996). On the decidability of the real exponential field.

[Mahler, 1935] Mahler, K. (1935). Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen. *Proc. Akad. Wet. Amsterdam*, 38:51–60.

[Mahler and Cassels, 1956] Mahler, K. and Cassels, J. W. S. (1956). On the Taylor coefficients of rational functions. *Mathematical Proceedings of the Cambridge Philosophical Society*, 52:39–48.

[Marker, 2002] Marker, D. (2002). *Model Theory: An Introduction.* Graduate Texts in Mathematics. Springer.

[Markoff, 1879] Markoff, A. (1879). Sur les formes quadratiques binaires indéfinies. *Mathematische Annalen*, 15(3):381–406.

[Matiyasevich, 1993] Matiyasevich, Y. V. (1993). *Hilbert's tenth problem.* MIT Press.

[McMullen and Shephard, 1971] McMullen, P. and Shephard, G. C. (1971). *Convex polytopes and the upper bound conjecture*, volume 3. CUP Archive.

[Mesnard and Serebrenik, 2008] Mesnard, F. and Serebrenik, A. (2008). Recurrence with affine level mappings is p-time decidable for clp. *Theory and Practice of Logic Programming*, 8(01):111–119.

[Mignotte, 1982] Mignotte, M. (1982). Some useful bounds. *Computer Algebra*, pages 259–263.

[Mignotte et al., 1984] Mignotte, M., Shorey, T., and Tijdeman, R. (1984). The distance between terms of an algebraic recurrence sequence. *Jour. Reine Angew. Math.*, 349:63 – 76.

[Moore, 1990] Moore, C. (1990). Unpredictability and undecidability in dynamical systems. *Physical Review Letters*, 64(20):2354.

[Moore, 1991] Moore, C. (1991). Generalized shifts: unpredictability and undecidability in dynamical systems. *Nonlinearity*, 4(2):199.

[Nagasaka and Shiue, 1990] Nagasaka, K. and Shiue, J.-S. (1990). Asymptotic positiveness of linear recurrence sequences. *Fibonacci Quart*, 28(4):340–346.

[Ouaknine et al., 2015] Ouaknine, J., Pinto, J. a. S., and Worrell, J. (2015). On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 957–969. SIAM.

[Ouaknine and Worrell, 2012] Ouaknine, J. and Worrell, J. (2012). Decision problems for linear recurrence sequences. In Finkel, A., Leroux, J., and Potapov, I., editors, *Reachability Problems*, volume 7550 of *Lecture Notes in Computer Science*, pages 21–28. Springer Berlin Heidelberg.

[Ouaknine and Worrell, 2014a] Ouaknine, J. and Worrell, J. (2014a). On the positivity problem for simple linear recurrence sequences. In *Automata, Languages, and Programming*, pages 318–329. Springer.

[Ouaknine and Worrell, 2014b] Ouaknine, J. and Worrell, J. (2014b). Positivity problems for low-order linear recurrence sequences. In *Proceedings of SODA*, pages 366–379.

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

[Pan, 1996] Pan, V. (1996). Optimal and nearly optimal algorithms for approximating polynomial zeros. *Computers & Mathematics with Applications*, 31(12):97 – 138.

[Podelski and Rybalchenko, 2004] Podelski, A. and Rybalchenko, A. (2004). A complete method for the synthesis of linear ranking functions. In *Verification, model checking, and abstract interpretation*, pages 239–251. Springer.

[Renegar, 1992] Renegar, J. (1992). 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.

[Rice, 1953] Rice, H. G. (1953). Classes of recursively enumerable sets and their decision problems. *Transactions of the American Mathematical Society*, 74(2):pp. 358–366.

[Roth, 1955] Roth, K. F. (1955). Rational approximations to algebraic numbers. *Mathematika*, 2(1-20):58.

[Salomaa and Soittola, 1978] Salomaa, A. and Soittola, M. (1978). *Automata-theoretic aspects of formal power series*. Springer-Verlag Berlin.

[Schaefer and Štefankovic, 2011] Schaefer, M. and Štefankovic, D. (2011). Fixed points, nash equilibria, and the existential theory of the reals. *Submitted*.

[Schmidt, 1980] Schmidt, W. (1980). Diophantine approximation. 785.

[Schneider, 1935a] Schneider, T. (1935a). Transzendenzuntersuchungen periodischer Funktionen I. Transzendenz von Potenzen. *Journal für die reine und angewandte Mathematik*, 172:65–69.

[Schneider, 1935b] Schneider, T. (1935b). Transzendenzuntersuchungen periodischer Funktionen II. Transzendenzeigenschaften elliptischer Funktionen. *Journal für die reine und angewandte Mathematik*, 172:70–74.

[Schönhage, 1979] Schönhage, A. (1979). On the power of random access machines. In Maurer, H., editor, *Automata, Languages and Programming*, volume 71 of *Lecture Notes in Computer Science*, pages 520–529. Springer Berlin / Heidelberg.

[Siegelmann and Sontag, 1991] Siegelmann, H. T. and Sontag, E. D. (1991). Turing computability with neural nets. *Applied Mathematics Letters*, 4(6):77 – 80.

[Siegelmann and Sontag, 1995] Siegelmann, H. T. and Sontag, E. D. (1995). On the computational power of neural nets. *Journal of computer and system sciences*, 50(1):132–150.

[Skolem, 1934] Skolem, T. (1934). Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen. *Skand. Mat. Kongr.*, 8:163–188.

[Sohn and Van Gelder, 1991] Sohn, K. and Van Gelder, A. (1991). Termination detection in logic programs using argument sizes. In *Proceedings of the tenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems*, pages 216–226. ACM.

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

[Stewart and Tall, 2002] Stewart, I. and Tall, D. (2002). *Algebraic Number Theory and Fermat's Last Theorem*. A. K. Peters, 3rd edition.

[Tangsupphathawat et al., 2012] Tangsupphathawat, P., Punnim, N., and Laohakosol, V. (2012). The positivity problem for fourth order linear recurrence sequences is decidable. In *Colloq. Math*, volume 128.

[Tao, 2008] Tao, T. (2008). *Structure and randomness: pages from year one of a mathematical blog.* American Mathematical Society.

[Tarasov and Vyalyi, 2011] Tarasov, S. and Vyalyi, M. (2011). Orbits of linear maps and regular languages. In Kulikov, A. and Vereshchagin, N., editors, *Computer Science – Theory and Applications*, volume 6651 of *Lecture Notes in Computer Science*, pages 305–316. Springer Berlin Heidelberg.

[Tarski, 1951] Tarski, A. (1951). A decision method for elementary algebra and geometry.

[Tiwari, 2004] Tiwari, A. (2004). Termination of linear programs. In *Computer Aided Verification*, pages 70–82. Springer.

[Van der Poorten and Schlickewei, 1982] Van der Poorten, A. and Schlickewei, H. (1982). The growth conditions for recurrence sequences. *Macquarie Math. Reports*, 82:0041.

[van der Poorten, 1977] van der Poorten, A. J. (1977). Linear forms in logarithms in the p-adic case. *Transcendence Theory: Advances and Applications*, pages 29–57.

[Vereshchagin, 1985] Vereshchagin, N. (1985). Occurrence of zero in a linear recursive sequence. *Mathematical Notes*, 38:609–615.

[Wilkie, 1996] Wilkie, A. J. (1996). Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *Journal of the American Mathematical Society*, pages 1051–1094.

[Ziegler, 1995] Ziegler, G. M. (1995). *Lectures on polytopes*, volume 152. Springer.

[Zilber, 2002] Zilber, B. (2002). Exponential sums equations and the Schanuel conjecture. *Journal of the London Mathematical Society*, 65:27–44.

[Zippel, 1997] Zippel, R. (1997). Zero testing of algebraic functions. *Information Processing Letters*, 61(2):63 – 67.