Algorithmic Verification of Linear Dynamical Systems

Toghrul Karimov

Saarland University

A thesis submitted for the degree of

Doctor of Natural Sciences

December 2023

Abstract

Linear dynamical systems (LDS) are mathematical models widely used in engineering and science to describe systems that evolve over time. In this thesis, we study algorithms for various decision problems of discrete-time linear dynamical systems. Our main focus is the *Model-Checking Problem*, which is to decide, given a linear dynamical system and an *ω-regular* specification, whether the *trajectory* of the LDS satisfies the specification. Using tools from various mathematical disciplines, most notably algebraic number theory, Diophantine approximation, automata theory, and combinatorics on words, we prove decidability of the Model-Checking Problem for large classes of linear dynamical systems and ω-regular properties. We further exploit deep connections between linear dynamical systems and contemporary number theory to show that improving any of our decidability results would amount to major mathematical breakthroughs. Our results delineate the boundaries of decision problems of linear dynamical systems that, at the present time, can be solved algorithmically.

Zusammenfassung

Lineare dynamische Systeme (LdS) sind mathematische Modelle, die in den Ingenieurwissenschaften und in den Naturwissenschaften bei der Beschreibung von zeitabhängigen Beobachtungen weit verbreitet sind. In dieser Arbeit untersuchen wir Algorithmen für verschiedene Entscheidungsprobleme diskreter linearer dynamischer Systeme. Unser Hauptaugenmerk liegt auf dem *Model-Checking Problem*: Gegeben ein lineares dynamisches System und eine ω-*reguläre* Spezifikation, entscheiden, ob *die Trajektorie* des LdS die Spezifikation erfüllt. Durch Anwendung von Konzepten aus verschiedenen mathematischen Disziplinen, insbesondere algebraischer Zahlentheorie, diophantischer Approximation, Automatentheorie und Kombinatorik auf Wörtern, beweisen wir die Entscheidbarkeit des Model-Checking Problems für große Klassen linearer dynamischer Systeme und ω-regulärer Eigenschaften. Zusätzlich nutzen wir tiefe Verbindungen zwischen dem Model-Checking Problem und der modernen Zahlentheorie, um nachzuweisen, dass jede Erweiterung unserer Entscheidbarkeitsergebnisse wesentliche mathematische Durchbrüche bedeuten würde. Unsere Ergebnisse umreißen die Grenzen der Entscheidungsprobleme linearer dynamischer Systeme, die derzeit algorithmisch gelöst werden können.

Acknowledgements

I am deeply grateful to Joël Ouaknine and James Worrell, who have advised and supported me throughout my academic life. I could not have wished for better mentors. I am also thankful to Mahsa Shirmohammadi for everything she taught me when I was still an undergraduate.

Over the last four years, I have been fortunate to have many exciting scientific discussions with Amaury, Anne, Armand, Anton, David, Edon, Engel, Erfan, Filip, Gorav, Jakob, Joris, Julian, Mahmoud, Marcel, Markus, Martina, Mihir, Rajab, and many others. These interactions made my life as a PhD student so much fun that I never noticed the passage of time.

I am grateful to my examiners Rupak Majumdar (Qualifying and Area Exams), Holger Herrmans (Qualifying Exam), Michael Benedikt (Area Exam), as well as Valérie Berthé, Laura Kovács, Prakash Panangaden, and André Platzer (PhD Exam).

While pursuing my doctoral degree, I was employed at the Max Planck Institute for Software Systems in Saarbrücken, Germany, as a *wissenschaftlicher Mitarbeiter* (scientific employee). I would like to thank everyone at the MPI-SWS for creating a stimulating scientific environment and a wonderful workplace. Prior to my time in Saarbrücken, my undergraduate studies at the University of Oxford were funded by a scholarship of the Ministry of Education of the Republic of Azerbaijan.

My parents Fuad and Təranə, and my sister Mədinə have always been there for me. Without them, this thesis would not have been possible. I am also grateful to my dear Elif, whose love and companionship always inspires me.

To my grandparents Nəbi, Zülfiyyə, Ramiz və Gövhər.

Contents

Introduction

A *discrete-time linear dynamical system* (LDS) is given by an update matrix $M \in \mathbb{Q}^{d\times d}$ and a starting point $s \in \mathbb{Q}^d$. Such a system evolves according to the dynamics $x \mapsto Mx$. The *orbit* (also known as the *trajectory*) of (M, s) is the sequence $\mathcal{O}(M, s) \coloneqq (M^n s)_{n\in\mathbb{N}}$. In this thesis we study decision problems of linear dynamical systems and their orbits.

Linear dynamical systems are interesting both from the practical perspective, as they arise in many branches of engineering and science, and the theoretical standpoint, as their decidability problems straddle what is known (i.e. resolved) and what is believed to be out of reach at the moment. We illustrate the former by an example from program verification. A *linear loop* is a program fragment of the form

$$\begin{aligned} &\textbf{initialise}\ \ x \\ &\textbf{while}\ \ \neg\mathrm{P}(x)\ \ \textbf{do}\ \ x = M \cdot x \end{aligned}$$

where $x = (x_1, \ldots, x_d)$ is a tuple of d rational variables, $M \in \mathbb{Q}^{d\times d}$, and P is a condition specified using the variables $x_1, \ldots, x_d$, constants from $\mathbb{Q}$, arithmetic operations, inequalities, and logical connectives. The figure below depicts a concrete loop over two variables, where P is a conjunction of four linear inequalities.

$x_1 = 1$
$x_2 = 0$
while $\neg\mathrm{P}(x_1, x_2)$**:**

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0.22 \cdot \begin{pmatrix} 4x_1 + 3x_2 \\ -3x_1 + 4x_2 \end{pmatrix}$$

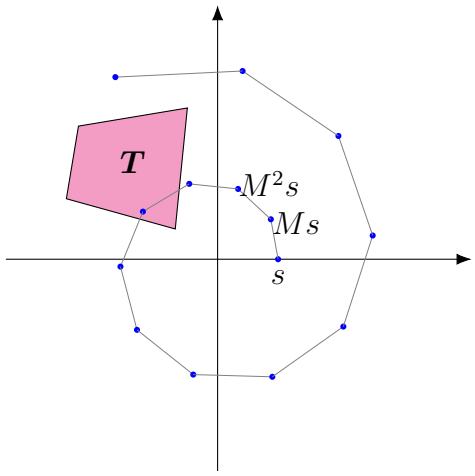

Figure 1: A linear loop and its geometric representation. The region T corresponds to the predicate P.

This loop can be modelled using the linear dynamical system given by

$$M = 0.22 \cdot \begin{bmatrix} 4 & 3 \\ -3 & 4 \end{bmatrix}, \quad s = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

With this definition, after n iterations of the loop body, the value of the variables (x_1, x_2) is equal to $M^n s$. Hence our loop terminates if and only if the orbit $\mathcal{O}(M, s)$ ever reaches the set $T = \{(x_1, x_2) \colon \mathrm{P}(x_1, x_2)\}$, depicted as the pink region in Figure 1. We see that the orbit, in fact, does reach T at time $n = 4$, and the loop terminates after 4 iterations. Generalising the example above, the termination problem for linear loops is Turing-equivalent to the following classical (and open) decidability problem about linear dynamical systems.

Reachability Problem. Given $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$, and a semialgebraic target set $T \subseteq \mathbb{R}^d$, decide whether the orbit $\mathcal{O}(M, s)$ reaches T, i.e. whether there exists $n \in \mathbb{N}$ such that $M^n s \in T$.

A subset of $\mathbb{R}^d$ is *semialgebraic* if it can be defined by a Boolean combination of polynomial inequalities with rational coefficients in variables $x_1, \ldots, x_d$. Semialgebraic sets include, among others, hyperplanes, halfspaces, bounded and unbounded polytopes, as well as algebraic varieties defined by polynomials over $\mathbb{Q}$. The class of semialgebraic targets corresponds exactly to the class of loop guards constructed from logical and arithmetic operations that we gave when defining linear loops.

From the perspective of formal verification, once a real-world system is modelled as a linear dynamical system, we can ask many different questions besides whether a configuration satisfying a certain condition is ever reached. For example, given (M, s) and semialgebraic sets T, T_1, T_2, we might want to decide whether, for example,

(a) $M^n s \in T$ for infinitely many $n \in \mathbb{N}$,

(b) for all n, if $M^n s \in T_1$ then there exists $k \geq 0$ such that $M^{n+k} s \in T_2$, or

(c) $M^n s \in T_1$ for all even n.

This leads us to consider the problem of deciding, given an LDS (M, s) and a specification φ, whether the orbit $\mathcal{O}(M, s)$ satisfies the specification.

But how can we represent the desired specification, and what kinds of specifications should we consider? Writing $\Sigma = 2^{\mathcal{T}}$, observe that determining whether the orbit $\mathcal{O}(M, s)$ satisfies a specification φ over a family of semialgebraic sets $\mathcal{T} = \{T_1, \ldots, T_\ell\}$

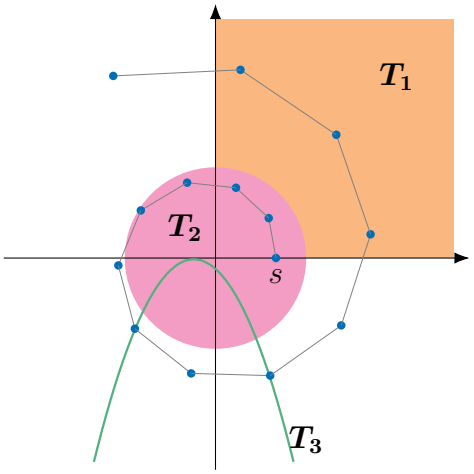

Figure 2: The orbit of (M, s) and the collection $\{T_1, T_2, T_3\}$ of target sets.

amounts to model checking the infinite *characteristic word* $\alpha \in \Sigma^\omega$ of (M, s) with respect to $\mathcal{T}$, defined by

$$T_i \in \alpha(n) \quad \Leftrightarrow \quad M^n s \in T_i$$

for all $1 \leq i \leq \ell$ and $n \in \mathbb{N}$. That is, the nth letter of α is the set of all semialgebraic targets from $\mathcal{T}$ which contain $M^n s$. Figure 2 depicts the orbit of (M, s) above as well as the collection of semialgebraic sets $\mathcal{T} = \{T_1, T_2, T_3\}$, where $T_1 = \{(x, y) \colon x, y \geq 0\}$, $T_2 = \{(x, y) \colon x^2 + y^2 < 1.2\}$, and $T_3 = \{(x, y) \colon y = -a(x - b)^2\}$ for $a \approx 1.23$ and $b \approx 0.35$. Note that the sets in $\mathcal{T}$ need not be disjoint, nor do they need to cover the entirety of the ambient space $\mathbb{R}^d$. We can read off from Figure 2 the characteristic word of (M, s) with respect to $\mathcal{T}$ as

$$\alpha = \{T_1, T_2\}\,\{T_1, T_2\}\,\{T_1, T_2\}\,\{T_2\}\,\{T_2\}\,\emptyset\,\{T_3\}\,\emptyset\,\{T_3\}\,\emptyset\,\{T_1\}\cdots .$$

Given a specification φ over $\mathcal{T}$ and a system (M, s), once we construct the characteristic word α of (M, s) with respect to $\mathcal{T}$, we can drop the original LDS and ask: Does the word α satisfy the property φ? Therefore, a natural way to represent φ is by a tuple $(\mathcal{T}, \mathcal{A})$, where $\mathcal{T}$ is a family of semialgebraic sets and $\mathcal{A}$ is an automaton over the alphabet $\Sigma = 2^{\mathcal{T}}$ that captures the property φ, in the sense that a word $\beta \in \Sigma^\omega$ satisfies φ if and only if it is accepted by $\mathcal{A}$. In this thesis, we work exclusively with *deterministic Muller automata*, which, just like non-deterministic Büchi automata, capture exactly all *ω-regular* specifications [11, Chapter 4]. In particular, ω-regular properties subsume reachability as well as the properties (a-c) above. We thus arrive at the following general verification problem for linear dynamical systems.

Model-Checking Problem (MCP). Given $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, a family $\mathcal{T}$ of semialgebraic subsets of $\mathbb{R}^d$, and a deterministic Muller automaton $\mathcal{A}$, decide whether $\mathcal{A}$ accepts the characteristic word α of (M, s) with respect to $\mathcal{T}$.

A large part of this thesis is dedicated to the study of the Model-Checking Problem from the perspective of decidability and complexity. Our main results in this direction can be summarised as follows.

(A) We give a novel framework in which decidability of various non-trivial classes of the Model-Checking Problem can be shown. Previously, decidability was only known for restricted classes of specifications (e.g. reachability [9] or infinite reachability [68]), or in the trivial cases where the characteristic word α is ultimately periodic (e.g. if M only has real eigenvalues, see Chapter 5).

(B) We show that any significant generalisation of the decidability results obtained through our framework would amount to major mathematical breakthroughs, therefore delineating the subclasses of the Model-Checking Problem for which decidability can be proven using contemporary mathematical tools.

In order to expound (A) and the "mathematical hardness" results alluded in (B), we need to introduce *linear recurrence sequences* (LRS), a fundamental class of sequences intimately related to linear dynamical systems. A sequence $(u_n)_{n\in\mathbb{N}}$ is a linear recurrence sequence over $\mathbb{Q}$ if there exist $d > 0$ and constants $a_0, \ldots, a_{d-1} \in \mathbb{Q}$ such that $u_0, \ldots, u_{d-1} \in \mathbb{Q}$ and

$$u_{n+d} = a_0 u_n + \ldots + a_{d-1} u_{n+d-1}$$

for all $n \in \mathbb{N}$. Equivalently, a sequence $(u_n)_{n\in\mathbb{N}}$ is an LRS over $\mathbb{Q}$ if and only if there exist $d > 0$, $M \in \mathbb{Q}^{d\times d}$ and $c, s \in \mathbb{Q}^d$ such that $u_n = c^\top M^n s$. Linear recurrence sequences will be discussed in detail in Chapter 2, but already from the latter characterisation of rational LRS a connection between LDS and LRS is immediate. Consider the Reachability Problem with (rational) hyperplane targets: given and LDS (M, s) and $c \in \mathbb{Q}^d$, decide whether the orbit of (M, s) ever reaches the hyperplane $H = \{x \mid c^\top x = 0\}$. Since $M^n s \in H$ if and only if $u_n \coloneqq c^\top M^n s = 0$, this problem is Turing-equivalent to the following.

Skolem Problem (for LRS over $\mathbb{Q}$). Given a rational LRS $(u_n)_{n\in\mathbb{N}}$, decide whether there exists n such that $u_n = 0$.

The Skolem Problem, despite having received significant attention since the 1980s, famously remains open. Decidability is currently known for sequences of order at most 4 (i.e. sequences that can be defined by a matrix $M \in \mathbb{Q}^{d\times d}$ for $d \leq 4$) by the result [61] of Mignotte, Shorey and Tijdeman proven in 1984. At order 5, the Skolem Problem remains open, although a recent result of Bilu et al. [16] shows decidability assuming certain well-known number-theoretic conjectures. In Section 8.3 we will show that the Skolem Problem for LRS of order 5 can, in fact, be reduced to the Reachability Problem for LDS in ambient space $\mathbb{R}^4$. The fact that the Skolem Problem is open at order 5, therefore, attests to the hardness of the Reachability Problem as well as the full Model-Checking Problem already in dimension $d = 4$.

Evidence of intractability of the Model-Checking Problem, however, goes much beyond reductions from the Skolem Problem. The following is another famous open problem about linear recurrence sequences subsumed by the Reachability Problem.

Positivity Problem (for LRS over $\mathbb{Q}$). Given a rational LRS $(u_n)_{n\in\mathbb{N}}$, decide whether $u_n \geq 0$ for all n.

Observe that for $u_n = c^\top M^n s$, deciding whether $u_n \geq 0$ for all n is equivalent to deciding whether there exists n such that $u_n < 0$. Hence the Positivity Problem is Turing-equivalent to deciding whether $\mathcal{O}(M, s)$ reaches a halfspace $H = \{x \mid c^\top x < 0\}$ where $c \in \mathbb{Q}^d$. Although not immediate at a first glance, the Skolem Problem is Turing-reducible to the Positivity Problem (Section 2.5). Independently from the Skolem Problem, the Positivity Problem is also hard with respect to certain open problems in Diophantine approximation: a decision procedure for the Positivity Problem for sequences of order 6 or more would entail algorithms for approximating *Lagrange constants* of a large class of transcendental numbers (Section 8.1), a result currently believed to be out of reach. Complementing this *Diophantine hardness*, [66, 67] show decidability of the Positivity Problem for sequences of order at most 5 and for diagonalisable sequences (i.e. sequences that can be defined by a diagonalisable matrix M) of order at most 9.

Linear recurrence sequences, however, do not only serve to formally prove the hardness of the Model-Checking Problem: They also form the backbone of every decidability result about the MCP. As an example, consider a semialgebraic target set $T \subseteq \mathbb{R}^d$ defined by a single inequality $p(x_1, \ldots, x_d)\ \Delta\ 0$, where p is a polynomial with rational coefficients. The orbit $\mathcal{O}(M, s)$ visits T at time $n \in \mathbb{N}$ if and only if $p(M^n s)\ \Delta\ 0$ holds. Since the sequence $u_n = p(M^n s)$ is a linear recurrence sequence over $\mathbb{Q}$ (see Chapter 2), understanding the time steps at which $\mathcal{O}(M, s)$ visits T

amounts to understanding the *sign pattern* $\sigma \in \{+, 0, -\}^\omega$ of the sequence $(u_n)_{n\in\mathbb{N}}$. A similar conclusion holds for a general semialgebraic target T defined by a Boolean combination of polynomial inequalities. In this case each inequality defining T gives rise to a separate sign pattern, and these sign patterns collectively determine the time steps at which $\mathcal{O}(M, s)$ visits T. We are now in a position to describe the results of this thesis pertaining to the Model-Checking Problem in more detail.

(✠) We introduce the class of *tame* semialgebraic sets, and show that the Model-Checking Problem is decidable if we assume all semialgebraic target sets in $\mathcal{T}$ are tame. A semialgebraic set is tame if it can be obtained, through standard set operations, from semialgebraic sets that either have dimension at most one, or are contained in a three-dimensional subspace. The sets of the former kind consist of finitely many components homeomorphic to a point or a line.

(★) We prove that the Model-Checking Problem is decidable if we restrict the matrix M to be diagonalisable and the automaton $\mathcal{A}$ to be *prefix-independent*. In this case, $\mathcal{T}$ is allowed to contain arbitrary semialgebraic sets. Intuitively, a prefix-independent automaton is such that whether a word α is accepted or not does not depend on any finite prefix of α. Prefix-independent properties constitute a strict subset of liveness properties. Importantly, infinite reachability properties are prefix-independent, but reachability properties are not. Somewhat surprisingly, we are also able to show that the full MCP for diagonalisable systems (i.e. without any restrictions on the set of targets $\mathcal{T}$ and the automaton $\mathcal{A}$) is decidable if we assume decidability of the Positivity Problem for *diagonalisable* linear recurrence sequences over $\mathbb{Q}$. Combining this result with the formulation of the Positivity Problem as an instance of the Reachability Problem described above, we conclude that for diagonalisable systems, the full Model-Checking Problem is Turing-reducible to the Reachability Problem.

To prove (✠) and (★), we use the framework of *toric* words. A toric word over an alphabet Σ is the *coding* of the trajectory $\langle x, f(x), f(f(x)), \ldots\rangle$ of a compact dynamical system $(\mathbb{T}^d, f)$, where $\mathbb{T}^d$ denotes the d-dimensional torus and f is a rotation, with respect to a collection $\mathcal{S}$ of open[1] subsets of $\mathbb{T}^d$ with $|\mathcal{S}| = |\Sigma|$. The nth letter of α is determined by the unique open set in $\mathcal{S}$ that contains $f^n(x)$. Variants of toric words have been extensively studied in symbolic dynamics and dynamical systems theory [69]. To capture characteristic words of linear dynamical systems, we introduce

[1] In the formal definition given in Chapter 4 we will also require each $S \in \mathcal{S}$ to have finitely many connected components, in order to avoid the situation where every word is toric.

the classes of *eventually toric* words and *eventually toric words with semialgebraic parameters*. As suggested by their names, the former class encloses the latter. We prove the following.

(a) The characteristic word of any linear dynamical system (M, s) with respect to a family $\mathcal{T}$ of tame sets is eventually toric with semialgebraic parameters. These parameters can be effectively computed given $M, s, \mathcal{T}$.

(b) The characteristic word of (M, s) for diagonalisable M with respect to any set $\mathcal{T}$ of semialgebraic targets is eventually toric with semialgebraic parameters. At the moment, we only know how to effectively determine only a subset of these parameters given $M, s, \mathcal{T}$.

The difference in the effectiveness of semialgebraic parameters (which arises because we use a deep but not fully constructive result when proving (b)) is ultimately the reason why for diagonalisable systems, in order to obtain decidability, we additionally impose the restriction that $\mathcal{A}$ be prefix-independent. In comparison, the proof of effectiveness of (a) involves solving the Skolem Problem for two new classes of linear recurrence sequences that can have arbitrarily large order (Section 2.7). We mention that the statement of (a) does not generalise beyond tame targets. In Chapter 8 we will give an example of $(M, s) \in \mathbb{Q}^{4\times 4} \times \mathbb{Q}^4$ and two-dimensional semialgebraic T such that the characteristic word of (M, s) with respect to $\mathcal{T} = \{T\}$ is not eventually toric.

Once we show that the characteristic words of linear dynamical systems we consider are eventually toric (with semialgebraic parameters), the punchline of our decidability results (✠) and (★) is that eventually toric words are *almost-periodic*, a notion due to Semënov [75]. An infinite word $\alpha \in \Sigma^\omega$ is almost-periodic if every finite word $u \in \Sigma^*$ either (i) occurs finitely often in α, or (ii) occurs infinitely often with bounded gaps. The word α is *effectively almost-periodic* if, given u, we can decide whether (i) or (ii) holds; Additionally, in case (i), we can determine all occurrences of u in α, and in case (ii) we can compute an upper bound on the gaps between consecutive occurrences of u in α. We will prove that eventually toric words with semialgebraic parameters are, in fact, effectively almost-periodic. The importance of effective almost periodicity lies in the result of Semënov [75, 64] to the effect that if α is effectively almost-periodic, then the following problem is decidable.

Acceptance Problem for the infinite word α. Given a deterministic Muller automaton $\mathcal{A}$, decide whether $\mathcal{A}$ accepts α.

Compare the statement of the Acceptance Problem to that of the Model-Checking Problem. The most important difference is that, in the former, the word α is fixed, and only the automaton $\mathcal{A}$ is given as the input. In the statement of the MCP, however, both the word α (represented by the triple $M, s, \mathcal{T}$) and the automaton $\mathcal{A}$ are part of the input. Despite this difference, we are able to utilise the concrete algorithm of Muchnik, Semënov and Ushakov ([64], see also Section 3.1) for the Acceptance Problem to show decidability of the MCP with tame targets. With few adaptations, the same algorithm can also be used to model check diagonalisable linear dynamical systems against prefix-independent properties. However, the aforementioned difference between the formulations of the Model-Checking Problem and the Acceptance Problem still results in the following discrepancy: The Acceptance Problem is decidable for characteristic words of diagonalisable LDS with respect to any set $\mathcal{T}$ of semialgebraic targets (Chapter 7), but the full MCP for diagonalisable systems (i.e. without the prefix-independence restriction on $\mathcal{A}$) is currently open and provably hard (Chapter 8).

The Acceptance Problem for certain combinatorial families of words (e.g. morphic words, the characteristic words of $\{f(n)\colon n \in \mathbb{N}\}$ for various functions including $f(n) = 2^n$, $f(n) = n^2$, $f(n) = n!$) has been studied in [34, 23, 70] in the light of its connection to the following fundamental problem in logic. For which unary predicates $P_1, \ldots, P_m \colon \mathbb{N} \to \{0,1\}$ is the *monadic second-order* (MSO) theory of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ decidable? We discuss the Monadic-Second Order logic in Section 1.9. Define the characteristic word of a predicate $P : \mathbb{N} \to \{0,1\}$ to be the word $\alpha \in \{0,1\}^\omega$ whose nth letter is equal to $P(n)$ for all $n \in \mathbb{N}$. By the reduction of Büchi in [21], where he showed decidability of the MSO theory of $\langle \mathbb{N}; < \rangle$ is decidable, the problem of determining whether a given MSO formula Φ is true in $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ is Turing-equivalent to the Acceptance Problem for the product word $\alpha = \alpha_1 \times \cdots \times \alpha_m \in \{0,1\}^m$. This equivalence has the following consequences.

(1) Suppose we are given an LDS (M, s) and a collection of semialgebraic sets $\mathcal{T} = \{T_1, \ldots, T_\ell\}$. For $1 \leq i \leq \ell$, let $P_i \colon \mathbb{N} \to \{0,1\}$ be the predicate defined by $P_i(n) = 1 \Leftrightarrow M^n s \in T_i$, and denote the characteristic word of P_i by α_i. Given a deterministic automaton $\mathcal{A}$, we can construct a formula Φ in a suitable monadic second-order language that holds in the structure $\langle \mathbb{N}; <, P_1, \ldots, P_\ell \rangle$ if and only if $\mathcal{A}$ accepts $\beta \coloneqq \alpha_1 \times \cdots \times \alpha_\ell$. Observe that β, up to a renaming of letters, is the same as the characteristic word α of (M, s) with respect to $\mathcal{T}$. Therefore, we can express the Model-Checking Problem in the parlance of monadic second-order logic.

(2) In Section 4.2 we will show that eventually toric words with semialgebraic parameters are closed under products. Consequently, if the characteristic word α_i of each P_i is toric with semialgebraic parameters, then the MSO theory of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ is decidable. In contrast, for all other well-known families of predicates, decidability is generally known only in case $m = 1$. For example, if P_1, P_2 are predicates whose characteristic words are morphic, then the MSO theories of both $\langle \mathbb{N}; <, P_1 \rangle$ and $\langle \mathbb{N}; <, P_2 \rangle$ are decidable, whereas decidability of the MSO theory of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ is, in general, unknown. See [15] for a survey of the state of the art regarding extensions of $\langle \mathbb{N}; < \rangle$ with decidable MSO theories.

Prior to discovering Semënov's work, in [48] and [7] we gave decidable subclasses of the Model-Checking Problem without using almost periodicity. Our methods were, in a sense, highly specialised versions of the algorithm of Muchnik et al. [64] for deciding whether an automaton accepts an effectively almost-periodic word. Remarkably, the theory of almost-periodic words not only unifies *all* decidability results to date pertaining to the Model-Checking Problem, but does so without deteriorating the complexity bounds on decision procedures compared to the ad hoc methods. The strong connection between Semënov's theory of almost-periodic words and decidability of the MCP will be further discussed in Chapter 3 and throughout this thesis.

By way of hardness, in Chapter 8 we will show that substantially improving any of our decidability results requires major mathematical breakthroughs. For example, we will prove that the Reachability Problem for $(M, s) \in \mathbb{Q}^{4\times 4} \times \mathbb{Q}^4$ and semialgebraic targets $T \subset \mathbb{R}^4$ of dimension 2 (which is also trivially contained in a linear subspace of dimension 4) is Diophantine-hard just like the Positivity Problem. Informally speaking, our hardness results show that tame targets essentially capture the class of semialgebraic sets for which the Reachability Problem can be shown to be decidable (without any restrictions on the system (M, s) or the automaton $\mathcal{A}$) using "conventional" number-theoretic methods. The fact that we can decide the full Model-Checking Problem for tame targets then suggests the following conjecture: If for a class of semialgebraic targets we can decide the Reachability Problem, then we can also decide the full Model-Checking Problem for the same class. Although this is not much more than a speculation, especially given that decidability of both the Reachability Problem and the Model-Checking Problem remain largely open, we are able to show in Chapter 7 that for LDS with a diagonalisable update matrix, the Model-Checking Problem is in fact Turing-reducible to the Reachability Problem. That is, for diagonalisable systems, deciding reachability is the only "difficult part" of model checking.

The final chapter of this thesis is markedly different from the others. There we consider the following verification problems of LDS that incorporate a notion of *robustness* to the Reachability Problem, and are more aligned with the classical, topological perspective on dynamical systems.

Topological Reachability Problem (TRP). Given an LDS (M, s) and a semialgebraic target T, decide if in every (open) neighbourhood of s there exists $\hat{s}$ such that the orbit $\mathcal{O}(M, \hat{s})$ reaches T.

Pseudo-Reachability Problem (PRP). Given an LDS (M, s) in ambient space $\mathbb{R}^d$ and a semialgebraic target $T \subseteq \mathbb{R}^d$, decide if for every $\epsilon > 0$, there exists a sequence $(u_n)_{n\in\mathbb{N}}$ of *control inputs* over $\mathbb{R}^d$ with the following properties.

(a) $\|u_n\|_2 < \epsilon$ for all $n \in \mathbb{N}$, and

(b) the trajectory $(x_n)_{n\in\mathbb{N}}$, defined by $x_0 = s$ and $x_{n+1} = Mx_n + u_n$, reaches T.

We show full decidability of the TRP and decidability of the PRP in case M is diagonalisable. Our results are based on a novel method of constructing a *continuous abstraction* $\mathcal{A}(t)$ of the orbit $\mathcal{O}(M, s)$. Here t ranges over $[0, \infty)$ and $M^n s \in \mathcal{A}(n)$ for all $n \in \mathbb{N}$. The continuous abstraction $\mathcal{A}(t)$ has many helpful properties not shared by the infinite discrete set $\mathcal{O}(M, s)$. Most importantly, $\mathcal{A}(t)$ can be computed from t using only arithmetic and real exponentiation, a result that allows us to deploy the powerful concept of *o-minimality* from model theory. In our context, o-minimality refers to the fact that every subset of $\mathbb{R}^d$ definable in first-order logic using arithmetic and exponentiation has finitely many connected components. One consequence of o-minimality is that when solving the TRP and the PRP, we can essentially pass from the orbit $\mathcal{O}(M, s)$ to the abstraction $\mathcal{A}(t)$. This cannot be done for the Reachability Problem due to the "exact" nature of the latter.

The abstraction-based technique unifies topological and pseudo-reachability with *inductive invariants* of linear dynamical systems. A set S is an inductive invariant of (M, s) if $s \in S$ and $MS \subseteq S$, which implies that $M^n s \in S$ for all n. Such invariants can be used to demonstrate non-reachability: given (M, s) and a target set T, if we can find S for which we can prove $s \in S$, $MS \subseteq S$, and $S \cap T = \emptyset$, then S certifies that $\mathcal{O}(M, s)$ does not reach T. The *Semialgebraic Invariant Problem*, shown decidable in [6], asks: Given (M, s) and semialgebraic T, decide whether there exists a semialgebraic inductive invariant of (M, s) that is disjoint from T. We show that decidability of the Semialgebraic Invariant Problem as well as the TRP and the PRP can be proven using the same approach. We are also able to show that if (M, s) does

not topologically reach T, then (M, s) has a semialgebraic invariant disjoint from T. Intuitively, for (M, s) such that $\mathcal{O}(M, s)$ does not reach T, whether an inductive invariant S disjoint from T exists and whether T is (not) topologically reachable depend on how well $\mathcal{O}(M, s)$ is separated from T.

The structure of this thesis. In Chapter 1 we provide necessary definitions and mathematical background, and develop algorithms for operating on algebraic numbers that will be required by our decision procedures. We dedicate significant attention to first-order theories of real and complex numbers as they offer us a common framework for algorithms operating on various types of mathematical objects. In Chapter 2 we study linear recurrence sequences in detail, recalling their classical theory as well as proving decidability of the Skolem Problem for certain novel families of sequences that arise from reachability problems of tame targets. In Chapter 3 we discuss effectively almost-periodic words. We give a detailed account of the algorithm of Muchnik et al. that decides whether a given automaton accepts a given effectively almost-periodic word, and modify it slightly to obtain a decision procedure for prefix-independent automata and certain kinds of almost-periodic words. Chapter 4 is dedicated to the study of toric words, which have significant overlap with the class of characteristic words of linear dynamical systems with respect to semialgebraic targets. We prove effective almost periodicity and various closure properties of toric words.

In Chapter 5 we apply the theory of toric and effectively almost-periodic words to show decidability of the Model-Checking Problem in ambient dimension at most three. This chapter is based on the work [48], presented at MFCS 2020. In Chapter 6 we extend decidability of the MCP to linear dynamical systems of arbitrary dimension and tame semialgebraic targets. The results of this chapter appeared in [47] (POPL 2022) and [46]. Chapter 7 studies the Model-Checking Problem for linear dynamical systems with a diagonalisable update matrix, proving decidability for prefix-independent properties ([7], POPL 2021) and full decidability assuming a Positivity oracle for diagonalisable linear recurrence sequences ([45], LICS 2022). In Chapter 8, by way of Diophantine and Skolem-hardness we show that none of our decidability results can be significantly improved without major mathematical breakthroughs.

Finally, in Chapter 9 we present our common solution based on continuous abstractions to the Semialgebraic Invariant Problem, the Topological Reachability Problem, and the Pseudo-Reachability Problem. These results appeared in the works [31] and [32], presented at MFCS 2021 and MFCS 2022, respectively. Chapter 9 can be read independently from the rest of this thesis with the exception of Chapter 1.

Chapter 1

Mathematical tools

Throughout this thesis, we will analyse algorithms that operate on linear dynamical systems, algebraic numbers, semialgebraic sets, automata and various other types of mathematical objects. In this chapter we describe how these objects will be represented (e.g. in computer memory), recall their basic properties, and analyse complexity of operations on them. A large part of our focus will be on the theory of algebraic numbers. In particular, we will use quantifier elimination and decision procedures from first-order logic to develop concrete algorithms with complexity bounds for performing various operations on a given set of algebraic numbers.

1.1 Notation and conventions

We write $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \overline{\mathbb{Q}}, \mathbb{C}$ for the sets of natural, integer, rational, real, algebraic and complex numbers, respectively. We denote by $\mathbb{T}$ the unit circle $\{z \in \mathbb{C} \colon |z| = 1\}$. For a ring R, $R^\times$ is the group of units in R. For example, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. We write $\boldsymbol{i}$ for the imaginary number, $\log \colon \mathbb{R}_{>0} \to \mathbb{R}$ for the natural logarithm, and $\operatorname{Log} \colon \mathbb{C}^\times \to \mathbb{C}$ for the principal branch of complex logarithm. For $x \in \mathbb{R}_{>0}$, $\operatorname{Log} x = \log x$.

We denote by $\mathbf{0}$ the vector or matrix of all zeros, whose dimensions will be clear from the context. The kth standard basis vector of $\mathbb{R}^d$, where d depends on the context, will be denoted by e_k. Given vectors $v_1, \ldots, v_m$, where $v_i \in \mathbb{C}^{d_i}$, we write $(v_1, \ldots, v_m)$ for the vector in $\mathbb{C}^{d_1+\ldots+d_m}$ obtained by concatenating $v_1, \ldots, v_m$ in the given order. For matrices $X_1, \ldots, X_m$, where $X_i \in \mathbb{C}^{a_i \times b_i}$, we define

$$\operatorname{diag}(X_1, \ldots, X_m) = \begin{bmatrix} X_1 & & \\ & \ddots & \\ & & X_m \end{bmatrix} \in \mathbb{C}^{(a_1+\ldots+a_m)\times(b_1+\ldots+b_m)}.$$

For a vector $v = (v_1, \ldots, v_d) \in \mathbb{C}^d$ and $p > 0$, we define $\|v\|_p = \sqrt[p]{|v_1|^p + \ldots + |v_d|^p}$. We further let $\|v\|_\infty = \max\{|v_i| : 1 \leq i \leq d\}$. We denote by $\mathcal{B}(z, \epsilon)$ the open ball

$$\{z \in R : \|x - z\|_2 < \epsilon\}$$

where R (usually either $\mathbb{R}^d$ or $\mathbb{C}^d$) will be understood from the context. Given a function $f : \mathbb{R}^d \to \mathbb{R}^l$ and $X \subset \mathbb{R}^d$, we write $f(X)$ for $\{f(x) \mid x \in \mathbb{R}^d\}$. For $X, Y \subseteq \mathbb{R}^d$, $c \in \mathbb{R}$, and an arithmetic operation $\circ$, we write $X \circ Y$ for the set $\{x \circ y \mid x \in X, y \in Y\}$ and cX for $\{cx \mid x \in X\}$.

When the topological space is clear from the context, we write $\mathrm{Cl}(X)$, $\mathrm{Int}(x)$, and ∂X for the closure, interior, and the boundary of X, respectively. In this thesis we will only work with the classical Euclidean and Zariski topologies, as well as the subset topologies they induce.

The function sign : $\mathbb{R} \to \{+, 0, -\}$ maps $\mathbb{R}_{>0}, \mathbb{R}_{<0}$ and $\{0\}$ to $+, -$ and 0, respectively. For an integer x, we write $\|x\|$ for the number of bits required to represent x in computer memory. More generally, for any object X we write $\|X\|$ for the description length of X, where the representation scheme will be clear from the type of the object. For example, since we represent semialgebraic sets by quantifier-free first-order formulas, $\|X\|$ for such a set is the bit length of the quantifier-free formula φ representing X. When we say that a class of objects $\{X_i \mid i \in I\}$ is effectively computable, we mean that there exists an algorithm that computes a representation of X_i given $i \in I$.

We write *Poly* for an absolute polynomial that does not depend on any other quantity. Every occurrence of *Poly* in this work can be (constructively) replaced by a concrete polynomial with integer coefficients, which we do not do in order to avoid notational clutter. For a function f, we denote by $f^n(x)$ the result of iteratively applying f to x a total of n times.

Finally, we mention that we will represent multivariate polynomials with rational coefficients by *flat first-order terms*, discussed in Section 1.3. Intuitively, the term $(x + 1)(y + 1)$ is not flat, whereas the equivalent term $xy + x + y + 1$ is.

1.2 Polynomials in one variable

We next recall some basic definitions and facts about univariate polynomials that will be useful throughout this work. Let $p(x) = \sum_{i=0}^{d} a_i x^i$ be a polynomial in $\mathbb{C}[x]$ with roots $\alpha_1, \ldots, \alpha_d$. We write $\deg(p)$ for the degree of p. The *height* of p, written $H(p)$, is defined as $\max_{0 \leq i \leq d} |a_i|$. The *Mahler measure* of p, denoted by $\mathcal{M}(p)$, is defined as

$|a_d| \prod_{k=1}^{d} \max\{1, |\alpha_i|\}$. We will use Mahler measure in a self-contained manner in this chapter, but refer the reader to [79, Section 3.3] for more details.

Consider an *integral* polynomial $p(x) = \sum_{i=0}^{\deg(p)} a_i x^i$, i.e. $p \in \mathbb{Z}[x]$. We represent p as a list of coefficients of length $\deg(p) + 1$. Hence $\deg(p) < \|p\|$, $H(\alpha) < 2^{\|p\|}$, and $\|p\| = O(\deg(p) \cdot \log H(p))$. In addition, if p is not the zero polynomial then $M(p) \geq |a_d| \geq 1$. We say that p is *primitive* if $\gcd(a_0, \ldots, a_d) = 1$. Using the algorithm of Lenstra, Lenstra and Lovász, an integral polynomial can be factored in polynomial time.

Theorem 1.2.1 (Main result of [53])**.** *Let $p \in \mathbb{Z}[x]$. In time polynomial in $\|p\|$ we can compute a factorisation $p = cp_1 \ldots p_m$, where $c = \gcd(a_0, \ldots, a_d)$ and for all $1 \leq i \leq m$, $p_i \in \mathbb{Z}[x]$ is primitive and irreducible over $\mathbb{Q}$.*

Next, we give a root separation bound for univariate polynomials due to Mignotte [62, Corollary of Theorem 5].

Theorem 1.2.2. *For square-free $p \in \mathbb{Z}[x]$ with distinct roots α and β,*

$$|\alpha - \beta| > \frac{\sqrt{3}}{(d+1)^{d+1} H^{d-1}}$$

where $d = \deg(p)$ and $H = H(p)$.

Corollary 1.2.3. *For $p(x) \in \mathbb{Q}[x]$ with distinct complex roots α and β,*

$$|\alpha - \beta| > 2^{-\textsc{Poly}(\|p\|)}.$$

Proof. Let $k \in \mathbb{N}$ with $k < 2^{\|p\|}$ be such that $q(x) \coloneqq kp(x) \in \mathbb{Z}[x]$. Observing that $\|q\|$ is at most polynomial in $\|p\|$, factorise $q(x) = cq_1(x) \cdots q_m(x)$ applying Theorem 1.2.1. It is classical that an irreducible polynomial in $\mathbb{Q}[x]$ is square-free. Moreover, two such polynomials either have identical roots, or do not share a common root. If α, β are roots of some q_i, then write $h = q_i$. Otherwise, let $i \neq j$ be such that $q_i(\alpha) = 0$ and $q_j(\beta) = 0$, and write $h = q_i q_j$. It remains to apply Theorem 1.2.2 to the square-free integral polynomial h. □

The following result of Cauchy, on the other hand, gives an upper on the magnitude of the roots of a polynomial.

Theorem 1.2.4. *Let $p(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{C}[x]$ with $a_d \neq 0$. If $p(\alpha) = 0$, then*

$$|\alpha| \leq 1 + \max_{0 \leq i \leq d} \frac{|a_i|}{|a_d|} \leq 1 + H(p).$$

We can also bound $|p(x)|$ from below for $|x|$ sufficiently large.

Lemma 1.2.5. *Let $p(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{C}[x]$ be a polynomial with degree d, $a_d \neq 0$, and height H. For all $x \in \mathbb{C}$ with $|x| \geq \frac{d \cdot H + 1}{a_d}$ it holds that*

$$|p(x)| > \min\{1, |a_0|/2\}.$$

Proof. If $d = 0$, then $|p(x)| = |a_0| > |a_0|/2$ for all x. Suppose $d > 0$. Since $|a_i| \leq H$ for all $0 \leq i \leq d$, $|\sum_{i=0}^{d-1} a_i t^i| < dHt^{d-1}$ for all $t > 1$. Hence if $t \geq \frac{dH+1}{a_d}$, which implies that $t > 1$, then

$$|p(t)| > |a_d| t^d - dHt^{d-1} = t^{d-1}(|a_d| t - dH) \geq 1. \qquad \square$$

1.3 First-order logic

We next establish most of the tools of the first-order logic that we will need. We refer the reader to [58, Chapters 2 and 3] for a comprehensive introduction to the concepts of this section.

A *first-order language* $\mathcal{L}$ is specified by a set F of function symbols, a set R of relation symbols, and a set C of constant symbols. We also assume an infinite set of variable symbols. A *term* in the language $\mathcal{L}$ is a well-formed expression built from the variable symbols and the symbols in F and C. Atomic formulas in $\mathcal{L}$ are of the form $r(t_1, \ldots, t_k)$, where $r \in R$ is a relation symbol with arity k, and $t_1, \ldots t_k$ are terms. The (well-formed) formulas in $\mathcal{L}$ are constructed from atomic formulas, quantifiers and logical connectives in the usual way. Finally, a *sentence* is a formula that does not contain free variables.

The (first-order) *language of rings*, denoted by $\mathcal{L}_r$, is given by the set of function symbols $F_r := \{+, -, \cdot\}$, the set of relation symbols $R_r := \{=, \neq\}$, and the set of constant symbols $C_r := \mathbb{Q}$. The (first-order) *language of ordered rings*, denoted by $\mathcal{L}_{or}$, is given by the triple $F_{or} = F_r$, $R_{or} := \{>, \geq, =, \neq, \leq, <\}$, and $C_{or} = C_r = \mathbb{Q}$. For example, $\varphi(x, y) := 5x^2 y + 3xz > 0$, which is a shorthand for $5 \cdot x \cdot x \cdot y + 3 \cdot x \cdot z > 0$, is an atomic formula in $\mathcal{L}_{or}$. With the exception of Chapter 9, we will be only working with the languages $\mathcal{L}_r$ and $\mathcal{L}_{or}$. Note that the terms of the two languages are identical. Hence we often do not specify whether a given first-order term belongs to $\mathcal{L}_r$ or $\mathcal{L}_{or}$.

Terms are purely syntactic objects. When working with $\mathcal{L}_{or}$ and $\mathcal{L}_r$, however, we will allow ourselves to substitute complex numbers in place of free variables in terms and formulas: for a term t with free variables $v_1, \ldots, v_m$ and complex numbers $\alpha_1, \ldots, \alpha_m$, we denote by $t(\alpha_1, \ldots, \alpha_m)$ the complex number obtained by performing the arithmetic operations specified in t on $\alpha_1, \ldots, \alpha_m$. We have therefore identified the term t with a polynomial function of type $\mathbb{C}^m \to \mathbb{C}$.

Let $\mathbb{R}_0$ and $\mathbb{C}_0$ denote the structures of real and complex numbers, respectively, equipped with the standard arithmetic operations and binary relations. The set $\mathbb{R}$ is the *universe* of the structure $\mathbb{R}_0$, and $\mathbb{C}$ is the universe of $\mathbb{C}_0$. We will be interpreting formulas of $\mathcal{L}_{or}$ and $\mathcal{L}_r$ in the structures $\mathbb{R}_0$ and $\mathbb{C}_0$, respectively.

Let $\mathbb{M}$ be a structure with universe M whose functions, relations and constants respectively match the function, relation and constant symbols of a language $\mathcal{L}$. We say that an $\mathcal{L}$-formula φ with free variables $x_1, \ldots, x_n$ *defines* $X \subseteq M^n$ if for all $a \coloneqq (a_1, \ldots, a_n) \in M^n$, $a \in X$ if and only if $\varphi(a_1, \ldots, a_n)$ holds in the structure $\mathbb{M}$. By the (first-order) *theory* of $\mathbb{M}$, denoted by $\mathrm{Th}(\mathbb{M})$, we mean the set of $\mathcal{L}$-sentences φ such that φ is true in $\mathbb{M}$, written $\mathbb{M} \models \varphi$. The theories $\mathrm{Th}(\mathbb{R}_0)$ and $\mathrm{Th}(\mathbb{C}_0)$ are known as the first-order theory of *real closed fields* and the the first-order theory of *algebraically closed fields of characteristic zero*, respectively. The theory $\mathrm{Th}(\mathbb{M})$ *admits quantifier elimination* if for every $\varphi(x_1, \ldots, x_n) \in \mathcal{L}$ there exists quantifier-free $\psi(x_1, \ldots, x_n) \in \mathcal{L}$ such that for all $a_1, \ldots, a_n \in M$, $\mathbb{M} \models \varphi(a_1, \ldots, a_n)$ if and only if $\mathbb{M} \models \psi(a_1, \ldots, a_n)$. We say that the formula ψ is *equivalent* to ϕ modulo $\mathbb{M}$. The theory $\mathrm{Th}(\mathbb{M})$ is *decidable* if, given an $\mathcal{L}$-sentence φ, it is decidable whether $\varphi \in \mathrm{Th}(\mathbb{M})$.

It is well-known that both $\mathrm{Th}(\mathbb{R}_0)$ and $\mathrm{Th}(\mathbb{C}_0)$ admit quantifier elimination. This immediately implies decidability of both theories: given a sentence Φ in $\mathcal{L}_{or}$ or $\mathcal{L}_r$, we can first compute an equivalent quantifier-free sentence Ψ, which will be a Boolean combination of atomic formulas without free variables containing constant symbols from $\mathbb{Q}$, arithmetic symbols, and relation symbols. Whether a sentence of this form is true in $\mathbb{R}_0$ and $\mathbb{C}_0$ can be easily verified. We next discuss the complexity of quantifier elimination and the decision problem for both theories.

1.3.1 Quantifier elimination in $\mathrm{Th}(\mathbb{R}_0)$

The first quantifier elimination algorithm for $\mathrm{Th}(\mathbb{R}_0)$ was given by Tarski in the 1940s. The running time of Tarski's algorithm is non-elementary, but the complexity of quantifier-elimination has since been refined to 2EXP. We refer the interested reader to [72, Section 1] for a detailed historical account. On the other hand, since the work of Fischer and Rabin [38] it is known that any quantifier elimination algorithm for $\mathrm{Th}(\mathbb{R}_0)$ must have at least doubly exponential complexity. In [30], for example, Davenport and Heintz construct an explicit class of formulas in $\mathcal{L}_{or}$ for which any equivalent quantifier-free formula has size at least doubly exponential in the length of the original formula. We will be using the quantifier elimination algorithm due to Renegar that has optimal complexity in the light of the lower bound above.

We refer to a term t as *flat* if it is of the form

$$\sum_{i \in I} c_i \prod_{j \in J} v_{i,j}$$

where $c_i \in \mathbb{Q}$ is a constant symbol, and $v_{i,j}$ is a variable symbol for all i, j, and for any distinct $a, b \in I$, the products $\prod_{j \in J} v_{a,j}$ and $\prod_{j \in J} v_{b,j}$ are distinct when viewed as monomials. Examples of non-flat terms include $(y_1 + 1) \cdots (y_n + 1)$ and $xy^2 + xy^2$. Flat terms correspond directly to multivariate polynomials with rational coefficients. As mentioned earlier, throughout this thesis **we assume that polynomials with rational coefficients are represented by flat terms**. In particular, for such p, $\deg(p)$ is bounded above by the description length of p.

We say that a formula φ in $\mathcal{L}_{or}$ is flat if all the terms appearing in φ are flat. In case of $\varphi \in \mathcal{L}_{or}$, this means that all the atomic formulas appearing in φ are of the form $t(x_1, \ldots, x_k)\ \Delta\ 0$ for a flat term t and a relation symbol Δ. Below is a summary of the quantifier elimination algorithm of Renegar that takes as an input a flat formula in prenex form (i.e. the formula consists of a block of quantifiers followed by a quantifier-free part) that has only integer constants.

Theorem 1.3.1 (Theorem 1.2 in [72])**.** *Let*

$$\Phi(\mathbf{y}) \coloneqq (Q_1 \mathbf{x}_1 \in \mathbb{R}^{n_1}) \cdots (Q_\omega \mathbf{x}_\omega \in \mathbb{R}^{n_\omega}) \colon \varphi(\mathbf{y}, \mathbf{x})$$

be a formula in $\mathcal{L}_{or}$ such that

(a) $Q_1, \ldots, Q_\omega \in \{\exists, \forall\}$,

(b) $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_\omega)$, *and* $\mathbf{y} = (y_1, \ldots, y_l)$ *are the free variables,*

(c) $\varphi(\mathbf{y}, \mathbf{x})$ *is flat and quantifier-free, and*

(d) all constants appearing in $\varphi(\mathbf{y}, \mathbf{x})$ *are integers.*

Let $n = \sum_{k=1}^{\omega} n_k$, *and denote by* $\|\Phi\|$ *the bit length of* Φ. *Using*

$$\|\Phi\|^{2^{O(\omega)}(n+l+1)\prod_{k=1}^{\omega} n_k}$$

sequential bit operations, one can compute a flat quantifier-free formula of the form

$$\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} h_{i,j}(y_1, \ldots, y_l)\ \Delta_{i,j}\ 0$$

equivalent to Φ *modulo* $\mathbb{R}_0$, *where each* $h_{i,j}$ *is a polynomial with integer coefficients and* $\Delta_{i,j} \in R_{or}$ *is a relation symbol.*

Note that in the formulation above, each $\mathbf{x}_i$ stands for a collection $x_{i,1}, \ldots, x_{i,n_i}$ of n_i bound variables, and $Q_i\mathbf{x}_i \in \mathbb{R}^{n_i}$ is a "syntactic sugar" for the block $Q_i x_{i,1} \ldots Q_i x_{i,n_i}$ of quantified variables. If $Q_i \neq Q_{i+1}$ for all i, then ω is the *quantifier alternation depth* of the formula Φ. Next, we give a well-known result about the *existential* fragment of the first-order theory of the reals.

Theorem 1.3.2 (Theorem 1.1 in [72])**.** *Let*

$$\Phi \coloneqq \exists x_1, \ldots, x_n \colon \varphi(x_1, \ldots, x_n)$$

be a sentence where $\varphi(x_1, \ldots, x_n)$ is flat, quantifier-free, and has only integer constants. Whether Φ holds in $\mathbb{R}_0$ can be decided in space polynomial in $\|\Phi\|$.

In order to be able to eliminate quantifiers from arbitrary formulas, we will need an algorithm to transform a given formula into the restricted form specified in Theorems 1.3.1 and 1.3.2. Any formula can be transformed into an equivalent formula in prenex form in polynomial time. Hence it remains to understand the complexity of "flattening" a formula and clearing out the denominators to replace rational constants with integer ones. We begin by analysing the process of performing an arithmetic operation on two multivariate polynomials.

Lemma 1.3.3. *Let $p_1, p_2 \in \mathbb{Z}[x_1, \ldots, x_n]$, $N_1, N_2 \in \mathbb{Z}$, and $q_i = \frac{1}{N_i} p_i \in \mathbb{Q}[x_1, \ldots, x_n]$ for $i \in \{1, 2\}$. Further let $N_3 = N_1 N_2$ and $q_3 = q_1 \circ q_2$, where $\circ \in \{+, -, \cdot\}$.*

(a) $q_3 = \frac{1}{N_3} p_3$ where $p_3 = p_1 p_2$ if $\circ$ is multiplication and $p_3 = N_2 p_1 + N_1 p_2$ otherwise.

(b) The number of distinct monomials appearing in p_i is at most $(1 + \deg(p_i))^n$ for all $i \in \{1, 2, 3\}$.

(c) $\deg(p_3) \leq \deg(p_1) + \deg(p_2)$.

(d) $H(p_3) \leq (N_1 + N_2) H(p_1) H(p_2) (1 + \deg(p_i))^n$ for $i \in \{1, 2\}$.

(e) (N_3, p_3) can be computed from (N_1, p_1) and (N_2, p_2) in time at most

$$\textsc{Poly}(\log N_1, \log N_2, \|p_1\|, \|p_2\|) \cdot (1 + \deg(p_1) + \deg(p_2))^n.$$

Proof. Statements (a-c) can be verified directly. To prove (d), for $i \in \{1, 2\}$, denote by m_i the number of distinct monomials with a non-zero coefficient appearing in p_i, and let $m = \min\{m_1, m_2\}$. If $\circ$ is multiplication, then each coefficient of a monomial

of p_3 is a sum of at most m integers with magnitude at most $H(p_1)H(p_2)$. Otherwise, $H(p_3)$ is bounded by $N_2H(p_1) + N_1H(p_2)$, and (d) follows.

Statement (e) follows from observing that there are at most $(1+\deg(p_1)+\deg(p_2))^n$ distinct monomials with non-zero coefficients in p_3. Since both multiplication and addition of integers can be performed in polynomial time, the coefficients of the monomials of p_3 (as well as the value N_3) each can be computed in time at most $\textsc{Poly}(\log N_1, \log N_2, \|p_1\|, \|p_2\|)$. □

We next lift the lemma above to flattening terms and formulas of $\mathcal{L}_{or}$ and $\mathcal{L}_r$. We say that terms $t_1(x_1, \ldots, x_n)$ and $t_2(x_1, \ldots, x_n)$ are *equivalent* if for all $a_1, \ldots, a_n \in \mathbb{C}$, $t_1(a_1, \ldots, a_n) = t_2(a_1, \ldots, a_n)$.

Lemma 1.3.4 (Flattening Lemma)**.** *Let T be a term and $n \geq 1$ be an upper bound on the number of distinct variable symbols appearing in T. Further let $\varphi \in \mathcal{L}$ be a formula of $\mathcal{L} \in \{\mathcal{L}_{or}, \mathcal{L}_r\}$. Write $\mathbb{M} = \mathbb{R}_0$ if $\mathcal{L} = \mathcal{L}_{or}$ and $\mathbb{M} = \mathbb{C}_0$ otherwise.*

(a) In time $\|T\|^{O(n)}$ we can compute a polynomial p with integer constants and $\deg(p) \leq \|T\|$, as well as $N \in \mathbb{Z}$, such that $\frac{1}{N}p$ is equivalent to T.

(b) In time $\|T\|^{O(n)}$ we can compute a flat formula $\psi \in \mathcal{L}$ with only integer constants that is equivalent to φ modulo $\mathbb{M}$.

Proof. We first give the algorithm for flattening a term t, i.e. constructing a polynomial p_t and integer N_t such that t is equivalent to $\frac{1}{N}p_t$. If t is a rational constant a/b, then $p_t = a$ and $N_t = b$. If t is a variable symbol, then $p_t = t$ and $N_t = 1$. Finally, if $t = t_1 \circ t_2$ for $\circ \in \{+, -, \cdot\}$, then first recursively compute p_{t_1}, N_{t_1} and p_{t_2}, N_{t_2} such that each $\frac{1}{N_{t_i}}p_i$ is equivalent to t_i. Thereafter, N_t and p_t can be computed from $p_{t_1}, N_{t_1}, p_{t_2}, N_{t_2}$ as described in Lemma 1.3.3.

Recall that for $a, b \in \mathbb{Z}$, $a \neq 0$, the height $H(a/b)$ of a/b is equal to $\max\{|a|, |b|\}$. Let $C = \max\{H(c) \mid c \text{ appears in } t \text{ as a constant}\}$. To analyse the complexity of our flattening algorithm applied to T, we will show by induction that for all intermediate sub-terms t of T,

(i) $\deg(p_t) \leq \|t\|$,

(ii) $N_t \leq C^{\|t\|}$,

(iii) $H(p_t) \leq 2^{\|t\|}(C(1 + \|t\|))^{n\|t\|^2}$.

In the base case, t is a constant or a variable symbol. All (i-iii) are immediate. In the inductive step, consider $t = t_1 \circ t_2$. Suppose we have already computed $p_{t_1}, p_{t_2}, N_{t_1}, N_{t_2}$. Observe that $\|t_1\| + \|t_2\| < \|t\|$, whence (i) follows. From $N_t = N_{t_1} N_{t_2}$ we deduce that $N_t \leq C^{\|t_1\|} C^{\|t_2\|} \leq C^{\|t\|}$. Finally, (iii) follows from Lemma 1.3.3 (d) and the inductive hypothesis.

We now prove (a). The output of the flattening algorithm is $p = p_T$ and $N = N_T$. From (i) we conclude that $\deg(p_T) \leq \|T\|$. Next, from (iii) we deduce that for every intermediate term t (including T itself), $\log(H(p_t)) < \textsc{Poly}(\|t\|)$. Since the number of distinct monomials in p_t is at most $(1 + \deg(p_t))^n$, we have $\|p_t\| < \|t\|^{O(n)}$. Applying Lemma 1.3.3 (e) to every step that flattens a sub-term t of T (of which there are at most $\|T\|$), we conclude that the running time of the algorithm is at most $\|T\|^{O(n)}$.

To prove (b), let $t(x_1, \ldots, x_n)\ \Delta\ 0$ be an atomic formula in φ. Using (a), compute in time $\|\varphi\|^{O(n)}$ a polynomial $p_t \in \mathbb{Z}[x_1, \ldots, x_n]$ and integer N_t such that t is equivalent to $\frac{1}{N_t} p_t$. Replacing $t(x_1, \ldots, x_n)\ \Delta\ 0$ in φ with $p_t(x_1, \ldots, x_n)\ \Delta\ 0$ we obtain a formula that is equivalent to $t(x_1, \ldots, x_n)\ \Delta\ 0$ modulo $\mathbb{M}$. It remains to apply this to every distinct atomic formula of φ, the number of which is at most $\|\varphi\|$. □

By the lemma above, if the total number of distinct variables in φ is fixed, then φ can be flattened in polynomial time. Such a result does not hold for arbitrary formulas, as illustrated by the family of formulas $\varphi_n(y_1, \ldots, y_n) \coloneqq (y_1 + 1) \cdots (y_n + 1) > 0$ for $n \in \mathbb{N}$. We are now ready to give the quantifier elimination result for general formulas. We say that a formula has *quantifier alternation* at most k if, once all instances of negation are pushed into the atomic predicates, each path in the syntax tree of the formula contains at most k alternating blocks of quantifiers.

Theorem 1.3.5. *Let $\Phi \in \mathcal{L}_{or}$ be a formula with N distinct (bound or free) variables.*

(a) A quantifier-free formula $\Psi \in \mathcal{L}_{or}$ equivalent to Φ modulo $\mathbb{R}_0$ can be constructed in time polynomial in $\|\Phi\|^{2^{\textsc{Poly}(N)}}$.

(b) If Φ has quantifier alternation bounded by an absolute constant k, then quantifier elimination can be performed in time polynomial in $\|\Phi\|^{\textsc{Poly}(N)}$.

(c) If Φ is a sentence, then whether Φ holds in $\mathbb{R}_0$ can be decided in time polynomial in $\|\Phi\|^{2^{\textsc{Poly}(N)}}$.

(d) If Φ is a flat sentence containing only existential quantifiers and no occurrences of the negation operator, then whether Φ holds in $\mathbb{R}_0$ can be decided in space polynomial in $\|\Phi\|$.

In cases (a) and (b), the formula Ψ is in disjunctive normal form, flat, and contains only integer constants.

Proof. In all cases, first compute (in polynomial time) a formula Φ_1 in prenex form that is equivalent to Φ. The formula Φ_1 has the same number of variables and the same quantifier alternation as Φ. Next, construct an equivalent flat formula Φ_2 as described in Lemma 1.3.4. This requires time at most $\|\Phi\|^{\textsc{Poly}(N)}$, and the resulting formula Φ_2 has only integer constants, same number of total variables as Φ, and is in prenex form. Statements (a-c), as well as the last statement about the shape of Ψ, follow from applying Theorem 1.3.1 to Φ_2. To prove (d), observe that in this case the formula Φ_1 is also flat, contains only existential quantifiers, and no instance of the negation operator. Hence we can clear out the denominators in polynomial time (in $\|\Phi_1\|$ and hence $\|\Phi\|$) and apply Theorem 1.3.2 to the resulting formula. □

1.3.2 Quantifier elimination in $\mathrm{Th}(\mathbb{C}_0)$

Quantifier elimination in $\mathrm{Th}(\mathbb{C}_0)$ has many parallels to its real counterpart described above. In particular, quantifier elimination algorithms for $\mathbb{C}_0$ also require at least doubly exponential space. See, for example, [42, Section 1]. Moreover, for both theories, quantifier elimination methods with optimal complexity are based on the same family of multivariate resultants. Lack of order relation on $\mathbb{C}_0$, however, makes the quantifier elimination and decision problems easier for certain special classes of $\mathcal{L}_r$-formulas. In this work we will only need the following quantifier elimination result about $\mathrm{Th}(\mathbb{C}_0)$, which is derived from the work [43] by Ierardi.

Theorem 1.3.6. *Let $\Phi \in \mathcal{L}_r$ be a formula with only existential quantifiers in which the negation operator does not occur. A flat quantifier-formula Ψ in disjunctive normal form and equivalent to Φ modulo $\mathbb{C}_0$ can be constructed in time $\|\Phi\|^{\textsc{Poly}(N)}$, where N is the total number of distinct (free and bound) variables in Φ.*

Proof. Similarly to the proof of Theorem 1.3.5, first construct, in time $\|\Phi\|^{O(N)}$ a formula Φ_2 that is flat, in prenex form, and equivalent to Φ. The formula Φ_2 will also contain only existential quantifiers, N distinct variables, and no occurrence of the negation operator. By [43, Corollary 16], a flat quantifier-free formula Ψ in disjunctive normal form that is equivalent to Φ_2 can be constructed in time $\|\Phi_2\|^{O(N)}$. Hence the total running time of quantifier elimination is bounded by $\|\Phi\|^{\textsc{Poly}(N)}$. □

1.4 Semialgebraic sets in $\mathbb{R}^d$ and $\mathbb{C}^d$

Recall that a formula $\varphi \in \mathcal{L}_{or}$ with free variables $x_1, \ldots, x_d$ defines $S \subseteq \mathbb{R}^d$ if for all $\mathbf{x} \in \mathbb{R}^d$, $\varphi(\mathbf{x})$ holds if and only if $\mathbf{x} \in S$. Subsets of $\mathbb{R}^d$ definable by a formula in $\mathcal{L}_{or}$ are called *semialgebraic*. By quantifier elimination, every semialgebraic set can in fact be defined by a flat quantifier-free formula of the form

$$\bigvee_{i \in I} \bigwedge_{j \in J} p_{i,j}(\mathbf{x}) \ \Delta_{i,j} \ 0. \tag{1.1}$$

Throughout this thesis we assume that **each semialgebraic set S is presented by a (not necessarily flat) quantifier-free formula φ defining S.** Operations on semialgebraic sets like checking the emptiness or taking a projection will be realised using quantifier elimination. If we were to represent semialgebraic sets with formulas of the form 1.1, which is more restrictive but common in the literature, then then complexity bounds we obtain for our algorithms would remain the same.

A semialgebraic set $S \subseteq \mathbb{R}^d$ is *algebraic* if it has a definition of the form 1.1 with the restriction that every $\Delta_{i,j}$ is the equality. Observe that

(a) $\bigwedge_{j \in J} p_{i,j}(\mathbf{x}) = 0$ is equivalent to $q_i(\mathbf{x}) = 0$ where $q_i = \sum_{j \in J} p_{i,j}^2$, and

(b) $\bigvee_{i \in I} q_i(\mathbf{x}) = 0$ is equivalent to $q(\mathbf{x}) = 0$ for $q = \prod_{i \in I} q_i$.

Hence every algebraic subset of $\mathbb{R}^d$ can be defined by a single polynomial equality.

Using cell decomposition (see [12, Chapter 5]), a semialgebraic set $S \subseteq \mathbb{R}^d$ can be written as a finite union of semialgebraic sets $S_1, \ldots, S_m$ where each S_i is homeomorphic to $(0,1)^{k_i}$ for some $k_i \leq d$. The dimension of S is equal to $\max_{1 \leq i \leq m} k_i$, which is independent of the decomposition $S = \bigcup_{1 \leq i \leq m} S_i$.

Analyses of linear dynamical systems, as well as our chosen representation for algebraic numbers, will often lead us to situations where we need to apply results pertaining to semialgebraic sets to sets of complex numbers. To formalise this, we say that $S \subseteq \mathbb{C}^d$ is semialgebraic if

$$\widetilde{S} \coloneqq \{(x_1, y_1, \ldots, x_d, y_d) \colon (x_1 + y_1 \boldsymbol{i}, \ldots, x_d + y_d \boldsymbol{i}) \in S\}$$

is a semialgebraic subset of $\mathbb{R}^{2d}$. Intuitively, we identify $\mathbb{C}^d$ with $\mathbb{R}^{2d}$ by taking real and imaginary parts of each coordinate of $z \in \mathbb{C}^d$. We represent S by a quantifier-free formula with $2d$ free variables that defines $\widetilde{S}$. We will revisit semialgebraic subsets of $\mathbb{C}^d$ in Lemma 1.5.5

1.5 Algebraic number theory

A number $\alpha \in \mathbb{C}$ is *algebraic* if there exists $p \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. Algebraic numbers form a subfield of $\mathbb{C}$ denoted by $\overline{\mathbb{Q}}$. The minimal polynomial of $\alpha \in \overline{\mathbb{Q}}$ is the (unique) monic polynomial $p \in \mathbb{Q}[x]$ of the smallest degree such that $p(\alpha) = 0$. An algebraic integer is an algebraic number whose minimal polynomial has integer coefficients. Algebraic integers form a subring of $\mathbb{C}$ denoted by $\mathcal{O}$. The ring $\mathcal{O}$ is *integrally closed*, meaning that every root of a monic polynomial whose coefficients are algebraic integers is itself an algebraic integer.

The *degree* of α, denoted by $\deg(\alpha)$, is the degree of the minimal polynomial of α. For each $\alpha \in \overline{\mathbb{Q}}$ there exists unique $P_\alpha(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ with $d = \deg(\alpha)$, called the *defining polynomial* of α, such that $P_\alpha(\alpha) = 0$ and $\gcd(a_0, \ldots, a_d) = 1$. The polynomial P_α and the minimal polynomial of α have identical roots and are *square-free*, meaning that all of their roots appear with multiplicity one. The *(naive) height* of α, denoted by $H(\alpha)$, is equal to $H(P_\alpha) = \max_{0 \le i \le d} |a_i|$. Write $P_\alpha(x) = a_d(x - \alpha_1) \cdots (x - \alpha_d)$. The algebraic numbers $\alpha_1, \ldots, \alpha_d$ (including α itself) are called the *(Galois) conjugates* of α.

A *canonical representation* of an algebraic number α is given by the polynomial P_α and an approximation $\xi \in \mathbb{Q}[\boldsymbol{i}]$, represented as a pair of rational numbers, with the property that $|\alpha - \xi| < |\beta - \xi|$ for every root $\beta \neq \alpha$ of P_α. That is, α is the nearest root of P_α to ξ. We represent algebraic numbers by their canonical representations. Other representations, e.g. based on the Primitive Element Theorem, are possible; see [28] for a detailed account. For $\alpha \in \overline{\mathbb{Q}}$ given by $(P_\alpha, u + v\boldsymbol{i})$, we write $\|\alpha\| = \|u\| + \|v\| + \|P_\alpha\|$ for the bit length of the particular canonical representation of α. Note that $\|\alpha\|$ is not a function of just α as it also depends on the choice of the representation. Throughout this thesis, when we make a statement about $\|\alpha\|$ without explicitly stating the representation, we mean that the statement holds for any canonical representation of α. The following lemma, for example, gives a lower bound on the distance between α and β in terms of bit lengths of any canonical representations thereof.

Lemma 1.5.1. *For every distinct* $\alpha, \beta \in \overline{\mathbb{Q}}$, $|\alpha - \beta| > 2^{-\textsc{Poly}(\|\alpha\| + \|\beta\|)}$.

Proof. Apply Mignotte's bound (Corollary 1.2.3) to $p = P_\alpha P_\beta \in \mathbb{Z}[x]$. □

1.5.1 The Weil height

In addition to the previously defined naive height $H(\cdot)$, we will make an extensive use of the *(absolute logarithmic) Weil height* of $\alpha \in \overline{\mathbb{Q}}$, defined as

$$h(\alpha) := \frac{1}{d}\log(M(P_\alpha)) = \frac{1}{d}\left(\log|a_d| + \sum_{i=1}^{d}\log\max\{1,|\alpha_i|\}\right)$$

where $d = \deg(\alpha)$, $\alpha_1, \ldots, \alpha_d$ are the Galois conjugates of α, and $M(P_\alpha)$ denotes the Mahler measure of α (see Section 1.2). Writing $P_\alpha(x) = \sum_{i=0}^{d} a_i x^i$, observe that the Weil height of $\alpha \neq 0$ is zero if and only if $a_d = 1$ (i.e. α is an algebraic integer) and all Galois conjugates of α have modulus at most 1. By a classical theorem of Kronecker, such numbers are exactly the roots of unity. It follows that $h(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity. On the other hand, if $h(\alpha) \neq 0$, then

$$h(\alpha) \geq \frac{1}{d}\log\left(1 + \frac{1}{52d\log 6d}\right) \geq \frac{1}{d + 52d^2\log 6d}$$

by a theorem of Blanksby and Montgomery [17]. In fact, Lehmer's famously open conjecture states that if $h(\alpha) \neq 0$, then $h(\alpha) > c/d$ for an absolute constant $c > 0$. Finally, for $\alpha = x/y \in \mathbb{Q}$ with $\gcd(x, y) = 1$, $h(\alpha) = \max\{\log|x|, \log|y|\}$.

The main utility of the Weil height for our purposes is that, compared to the naive height, it is easier to keep track of Weil heights of algebraic numbers obtained through arithmetic (and other) operations. Let $n \in \mathbb{Z}$ and $\alpha, \alpha_1, \alpha_2 \in \overline{\mathbb{Q}}$. The following bounds (and a detailed discussion of the Weil height) can be found in [79, Section 3].

(1) $h(\alpha_1 + \alpha_2) \leq h(\alpha_1) + h(\alpha_2) + \log 2$.

(2) $h(\alpha_1 \cdot \alpha_2) \leq h(\alpha_1) + h(\alpha_2)$.

(3) $h(\alpha^n) = |n|h(\alpha)$.

By the second equality, $h(-\alpha) = h(\alpha)$ for all $\alpha \in \overline{\mathbb{Q}}$. The last equality implies that $h(1/\alpha) = h(\alpha)$ for all $\alpha \neq 0$. Observing that $P_\alpha = P_{\overline{\alpha}}$ and hence $h(\alpha) = h(\overline{\alpha})$,

(4) $h(\mathrm{Re}(\alpha)) = h((\alpha + \overline{\alpha})/2) \leq 2(h(\alpha) + \log 2)$,

(5) $h(\mathrm{Im}(\alpha))) = h(\boldsymbol{i}(\alpha - \overline{\alpha})/2) \leq 2(h(\alpha) + \log 2)$,

(6) $h(|\alpha|) = h(\sqrt{\alpha\overline{\alpha}}\,) = h(\alpha\overline{\alpha})/2 \leq h(\alpha)$.

The Weil height is related to the naive height as follows [79, Lemma 3.11]. For all $\alpha \in \overline{\mathbb{Q}}$ with $\deg(\alpha) = d$ and $H(\alpha) = H$,

$$\frac{1}{d}\log H - \log 2 \leq h(\alpha) \leq \frac{1}{d}\log H + \frac{1}{2d}\log(d+1).$$

Hence for all $\alpha \neq 0$, $h(\alpha) \leq \|P_\alpha\| < \|\alpha\|$. We can use the Weil height to solve the following problem about power of algebraic numbers.

Lemma 1.5.2. *Let $\alpha, \beta \in \overline{\mathbb{Q}}$, where α is non-zero and not a root of unity. There exists effectively computable $N < \textsc{Poly}(\|\alpha\|, \|\beta\|)$ such that for all $n \geq N$, $\alpha^n \neq \beta$.*

Proof. Since $h(\alpha) > 0$ by the assumptions on α, and

$$\alpha^n = \beta \quad \Rightarrow \quad h(\alpha^n) = h(\beta) \quad \Leftrightarrow \quad nh(\alpha) = h(\beta),$$

we can choose $N \coloneqq \lceil h(\beta)/h(\alpha) \rceil$. Let $d = \max\{\deg(\alpha), \deg(\beta)\}$, and observe that

$$\frac{h(\beta)}{h(\alpha)} \leq \frac{\frac{1}{d}\log H(\beta) + \frac{1}{2d}\log(d+1)}{1/(d + 52d^2 \log 6d)} \leq \textsc{Poly}(\|\alpha\|, \|\beta\|). \qquad \square$$

Note that the bound $\textsc{Poly}(\|\alpha\| + \|\beta\|)$ above is on the magnitude of N. The bit length of N is poly-logarithmic in the input size $\|\alpha\| + \|\beta\|$. Nevertheless, the time required to compute N is linear in $\|\alpha\| + \|\beta\|$ as we need to look at every bit of the input.

1.5.2 Fields and rings of algebraic numbers

A *number field* is $\mathbb{K}$ is a subfield of $\mathbb{C}$ the form $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ where each α_i is an algebraic number. Our main reference for number fields is [57, Chapter 2]. Let $\mathbb{K}$ be a number field and denote by $D \coloneqq [\mathbb{K} : \mathbb{Q}]$ the *degree* of the field extension $\mathbb{K}/\mathbb{Q}$, defined as the dimension of $\mathbb{K}$ as a vector space over $\mathbb{Q}$. The degree D is always finite and by the Tower Law for field extensions, bounded above by $\prod_{i=1}^m \deg(\alpha_i)$. Moreover, the field $\mathbb{K}$ has exactly D distinct embeddings $\sigma_1, \ldots, \sigma_D$ into $\overline{\mathbb{Q}}$. If $\mathbb{K}/\mathbb{Q}$ is a *Galois extension*, meaning that there exists $p \in \mathbb{Q}[x]$ whose set of all roots $\{\alpha_1, \ldots, \alpha_d\}$ satisfies $\mathbb{K} = \mathbb{Q}(\beta_1, \ldots, \beta_d)$, then each σ_i is, in fact, a field automorphism of $\mathbb{K}$. These automorphisms constitute the *Galois group* of $\mathbb{K}/\mathbb{Q}$, denoted by $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

The *norm* of $\alpha \in \mathbb{K}$ in the number field $\mathbb{K}$ is defined as

$$N_{\mathbb{K}}(\alpha) \coloneqq \sigma_1(\alpha) \cdots \sigma_D(\alpha).$$

The norm $N_{\mathbb{K}}(\alpha)$ is zero if and only if $\alpha = 0$, and $N_{\mathbb{K}}(\alpha\beta) = N_{\mathbb{K}}(\alpha)N_{\mathbb{K}}(\beta)$ for all $\alpha, \beta \in \mathbb{K}$. Denote by $N_{abs}(\alpha)$ the product of all Galois conjugates of $\alpha \in \overline{\mathbb{Q}}$. It is related to the field norm as follows [57, Theorem 4].

$$N_{\mathbb{K}}(\alpha) = N_{abs}(\alpha)^{D/\deg(\alpha)}.$$

Let $\alpha \neq 0$ and $P_\alpha = \sum_{i=0}^{d} a_i x^i$ be the defining polynomial of α. Observe that $N_{abs}(\alpha) = \frac{a_0}{a_d}$ is always rational and has magnitude at most $H(\alpha)$. Hence $N_{\mathbb{K}}(\alpha)$ is also rational and satisfies $|N_{\mathbb{K}}(\alpha)| \leq H(\alpha)^D$.

Recall that $\mathcal{O}$ denotes the ring of algebraic integers. For a number field $\mathbb{K}$, we write $\mathcal{O}_{\mathbb{K}} \coloneqq \mathcal{O} \cap \mathbb{K}$ for the *ring of algebraic integers of* $\mathbb{K}$. By the Kummer-Dedekind theorem [57, Theorem 16], the ideals of $\mathcal{O}_{\mathbb{K}}$ have unique factorisation in terms of *prime ideals* of $\mathcal{O}_{\mathbb{K}}$.[1] Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ and $\mathfrak{a}$ be an ideal with prime factorisation $\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_n^{k_n}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are distinct prime ideals and $k_1, \ldots, k_n$ are positive integers. Define the *ideal counting function*

$$v_{\mathfrak{p}}(\mathfrak{a}) \coloneqq \begin{cases} n_i & \text{if } \mathfrak{p} = \mathfrak{p}_i \\ 0 & \text{otherwise.} \end{cases}$$

The function $v_{\mathfrak{p}}$ is analogous to the usual p-adic valuation defined on rationals, where p is an integer prime number.[2] For an algebraic integer $\beta \in \mathbb{K}$, denote by (β) the ideal in $\mathcal{O}_{\mathbb{K}}$ generated by β. For a prime ideal $\mathfrak{p}$ and $\beta \in \mathcal{O}_{\mathbb{K}}$, we define $v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}((\beta))$. Note that $v_{\mathfrak{p}}(\beta) \in \mathbb{N}$ for $\beta \in \mathcal{O}_{\mathbb{K}}$. We can then extend $v_{\mathfrak{p}}$ to the whole of $\mathbb{K}$ as follows. Let $\alpha \in \mathbb{K}$ with the defining polynomial $P_\alpha = \sum_{i=0}^{d} a_i x^i$. We will argue that $\beta = a_d \cdot \alpha$ is an algebraic integer. Observe that $\sum_{i=0}^{d} a_i a_d^{d-1} \alpha^i = 0$. Hence β is a root of

$$p(x) \coloneqq \sum_{i=0}^{d} a_d^{d-i-1} \cdot a_i x^i.$$

Since $a_d^{d-i-1} \cdot a_i = 1$ for $i = d$, we conclude that β is an algebraic integer. Recalling that $\alpha = \beta / a_d$, we define $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\beta) - v_{\mathfrak{p}}(a_d)$. Observe that $v_{\mathfrak{p}}(\beta)$ takes integer values. For $\alpha, \alpha_1, \alpha_2 \in \mathbb{K}$, α non-zero, $v_{\mathfrak{p}}(\cdot)$ has the following properties.

(a) $v_{\mathfrak{p}}(\alpha_1 \alpha_2) = v_{\mathfrak{p}}(\alpha_1) + v_{\mathfrak{p}}(\alpha_2)$.

(b) $v_{\mathfrak{p}}(\alpha + \beta) \geq \min\{v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)\}$.

(c) $v_{\mathfrak{p}}(1/\alpha) = -v_{\mathfrak{p}}(\alpha)$.

[1] The factorisation of the whole ring $\mathcal{O}_{\mathbb{K}}$ is the empty product.

[2] We recommend the lecture notes [63] by James Milne for a detailed introduction to the ideal counting function and the $\mathfrak{p}$-adic norms.

We now move onto norms of ideals. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$. The *norm* $N(\mathfrak{a})$ of $\mathfrak{a}$ is defined as the cardinality $|\mathcal{O}_{\mathbb{K}}/\mathfrak{a}|$ of the quotient ring $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$, which is always finite. By convention, the norm of the zero ideal is zero. The norm is multiplicative: For any two non-zero ideals $\mathfrak{a}, \mathfrak{b}$, it holds that

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

By [57, Theorem 22 (c)], for a principal ideal (β) where $\beta \in \mathcal{O}_{\mathbb{K}}$, it holds that

$$N((\beta)) = |N_{\mathbb{K}}(\beta)|.$$

Recall that $|N_{\mathbb{K}}(\alpha)| = N_{abs}(\alpha)^{D/\deg(\alpha)} \leq H(\alpha)^D$ for all $\alpha \in \mathbb{K}$, where $D = [\mathbb{K} : \mathbb{Q}]$. Hence $N((\beta)) \leq H(\beta)^D$ for all $\beta \in \mathcal{O}_{\mathbb{K}}$. For non-zero $x \in \mathbb{Z}$ we have that $N((x)) = x^D$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$. The ideal $\mathfrak{p}$ contains a unique rational prime p, and $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$ for some $f_{\mathfrak{p}} \in \mathbb{N}$. We say that $\mathfrak{p}$ *lies above* p, and call $f_{\mathfrak{p}}$ the *ramification degree* of $\mathfrak{p}$. Since $p \in \mathfrak{p}$, $(p) \subseteq \mathfrak{p}$. That is, $\mathfrak{p}$ divides (p). The value $e_{\mathfrak{p}} \coloneqq v_{\mathfrak{p}}((p))$ is called the *ramification index* of $\mathfrak{p}$. Both $f_{\mathfrak{p}}$ and $e_{\mathfrak{p}}$ are positive integers. Since $\mathfrak{p}^{e_{\mathfrak{p}}}$ divides (p), the latter is contained in $\mathfrak{p}^{e_{\mathfrak{p}}}$. Hence $N(\mathfrak{p}^{e_{\mathfrak{p}}}) \leq N((p))$. We therefore have

$$N(\mathfrak{p}^{e_{\mathfrak{p}}}) = N(\mathfrak{p})^{e_{\mathfrak{p}}} = p^{f_{\mathfrak{p}}e_{\mathfrak{p}}} \leq N((p)) = p^D.$$

It follows that $f_{\mathfrak{p}}e_{\mathfrak{p}} \leq D$ and $1 \leq e_{\mathfrak{p}}, f_{\mathfrak{p}} \leq D$.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ and $\lambda \in \mathbb{K}$ be such that $v_{\mathfrak{p}}(\lambda) > 0$. We next give bounds on $N(\mathfrak{p})$, the unique rational prime $p \in \mathbb{N}$ contained in $\mathfrak{p}$, as well as $|v_{\mathfrak{p}}(\alpha)|$ for $\alpha \in \mathbb{K}$ in terms of $\|\alpha\|$, $\|\lambda\|$ and D. These bounds will apply to *all* prime ideals $\mathfrak{p}$ satisfying $v_{\mathfrak{p}}(\lambda) > 0$. Since $\mathfrak{p}$ divides (λ),

$$N(\mathfrak{p}) \leq N((\lambda)) \leq H(\lambda)^D.$$

From $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$ and $1 \leq f_{\mathfrak{p}} \leq D$ we conclude that $p \leq H(\lambda)^D$. Next, consider $\alpha \in \mathbb{K}$. Write $\alpha = \beta/m$, where $\beta \in \mathcal{O}_{\mathbb{K}}$ and $m \in \mathbb{Z}$. As discussed earlier, we can take m to be the leading coefficient of P_α, the defining polynomial of α. Hence we can assume description lengths of β and m are at most polynomial in $\|\alpha\|$. By definition, $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(\beta) - v_{\mathfrak{p}}(m)$. Since $\mathfrak{p}^{v_{\mathfrak{p}}(\beta)}$ divides (β),

$$(N(\mathfrak{p}))^{v_{\mathfrak{p}}(\beta)} \leq N((\beta)) \leq H(\beta)^D.$$

Similarly, $(N(\mathfrak{p}))^{v_{\mathfrak{p}}(m)} \leq H(m)^D$. Since the ideal $\mathfrak{p}$ satisfies $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$, its norm $N(\mathfrak{p}) = |\mathcal{O}_{\mathbb{K}}/\mathfrak{p}|$ is at least two.[3] Therefore, $v_{\mathfrak{p}}(\beta) \leq D\log_2(H(\beta))$ and $v_{\mathfrak{p}}(m) \leq D\log_2(H(m))$. It follows that

$$|v_{\mathfrak{p}}(\alpha)| = |v_{\mathfrak{p}}(\beta) - v_{\mathfrak{p}}(m)| < \textsc{Poly}(D, \|\alpha\|).$$

[3]Recall that the whole of $\mathcal{O}_{\mathbb{K}}$ is not considered prime.

Finally, we show that for every $\alpha \in \mathbb{K} \setminus \mathcal{O}_{\mathbb{K}}$, there exists a prime ideal $\mathfrak{p}$ such such that $v_{\mathfrak{p}}(\alpha) \neq 0$. Write $\alpha = \beta/m$ as above for $\beta \in \mathcal{O}_{\mathbb{K}}$ and $m \in \mathbb{Z}$. We need to show existence of $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\beta) \neq v_{\mathfrak{p}}(m)$, which, by the unique factorisation theorem, is equivalent to $(\beta) \neq (m)$. Recall that two principal ideals are equal if and only if their generators are associates. Hence $(\beta) = (m)$ if and only if β/m is a unit of $\mathcal{O}_{\mathbb{K}}$. Since $\alpha = \beta/m$ and α does not belong $\mathcal{O}_{\mathbb{K}}$ by assumption, $(\beta) \neq (m)$ and the conclusion follows.

1.5.3 Defining algebraic numbers by first-order formulas

Rather than working with canonical representations directly (e.g. using resultants and root approximation algorithms), it will often be convenient to represent algebraic numbers by first-order formulas and perform operations thereon using quantifier elimination (Theorem 1.3.5) and flattening (Lemma 1.3.4). Recall from Section 1.4 that a formula $\varphi(x, y) \in \mathcal{L}_{or}$ defines $S \subset \overline{\mathbb{Q}}$ if

$$\{(x, y) \in \mathbb{R}^2 \colon \varphi(x, y)\} = \{(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha)) \colon \alpha \in S)\}.$$

We say that $\varphi(x, y)$ defines $\alpha \in \overline{\mathbb{Q}}$ if it defines $\{\alpha\}$. Similarly, $\varphi(x)$ defines $\alpha \in \mathbb{R} \cap \overline{\mathbb{Q}}$ if $\{x \in \mathbb{R} \colon \varphi(x)\} = \{\alpha\}$. We next discuss how to extract a formula defining α given its canonical representation.

Let $p(z) = \sum_{j=0}^{d} a_j z^j$ be a polynomial with rational coefficients. We first show how to compute, in time polynomial in $\|p\|$, $p_1, p_2 \in \mathbb{Q}[x, y]$ such that for all $x, y \in \mathbb{R}$,

$$p(x + y\boldsymbol{i}) = p_1(x, y) + p_2(x, y)\boldsymbol{i}.$$

Flatten the term $\sum_{j=0}^{d} a_j (x + yI)^j$, where I is a variable symbol that stands for the complex number $\boldsymbol{i}$. By Lemma 1.3.4, this requires time $\textsc{Poly}(\|p\|)$. In the resulting flat term, replace each occurrence of I^k, where $k \in \mathbb{N}$, respectively with $1, I, -1, -I$ depending on whether k is equal to $0, 1, 2$ or 3 modulo 4. The resulting term will be flat and of the form $t_1(x, y) + t_2(x, y)I$, where t_1, t_2 are flat terms themselves. We can then choose p_i as the polynomial corresponding to t_i for $i \in \{1, 2\}$. Observe that the formula

$$\Phi_p(x, y) \coloneqq\ t_1(x, y) = 0 \wedge t_2(x, y) = 0$$

defines the set of all roots of p. Let $\Psi_p(x, y, u, v)$ be the quantifier-free formula equivalent to

$$\Phi_p(x, y)\ \wedge\ \forall (x_1, y_1) \neq (x, y) \colon \Phi_p(x_1, y_1) \Rightarrow (x_1 - u)^2 + (y_1 - v)^2 > (x - u)^2 + (y - v)^2$$

computed in time polynomial in $\|p\|$ using Theorem 1.3.5. Observe that $\Psi_p(x, y, u, v)$ holds if and only if $x + y\boldsymbol{i}$ is the root of p that is closest to $u + v\boldsymbol{i}$. We therefore have the following.

Lemma 1.5.3. *Given a canonical representation (p, ξ) of $\alpha \in \overline{\mathbb{Q}}$, a quantifier-free formula $\varphi(x, y) \in \mathcal{L}_{or}$ defining α can be constructed in polynomial time.*

Proof. Recall that $\mathrm{Re}(\xi), \mathrm{Im}(\xi) \in \mathbb{Q}$. The quantifier-free formula $\Psi_p(x, y, \mathrm{Re}(\xi), \mathrm{Im}(\xi))$, which is obtained by substituting $\mathrm{Re}(\xi), \mathrm{Im}(\xi)$ respectively for variable symbols u, v in $\Psi_p(x, y, u, v)$, defines α. It remains to recall that Ψ_p is computed from p in polynomial time. □

Corollary 1.5.4. *Given canonical representations of $\alpha, \beta \in \overline{\mathbb{Q}}$, we can decide whether $\alpha = \beta$ in polynomial time.*

Proof. Let $\varphi(x, y), \psi(x, y)$ be two formulas defining α and β. The sentence

$$\exists x, y \colon \varphi(x, y) \ \wedge \ \psi(x, y)$$

holds in $\mathbb{R}_0$ if and only if $\alpha = \beta$. The former can be checked in polynomial time by Theorem 1.3.5. □

Having shown how to define algebraic numbers using first-order formulas, we now give our main tool for computing representations of semialgebraic subsets of $\mathbb{C}^d$ (see Section 1.4) that we will encounter.

Lemma 1.5.5. *Let $f \in \mathbb{C}(z_1, \ldots, z_k)$ be a rational function given by*

$$f(z_1, \ldots, z_k) = \sum_{j=1}^{A} h_j(\lambda_1, \ldots, \lambda_m) z_1^{\sigma_{j,1}} \cdots z_k^{\sigma_{j,k}}$$

where $\lambda_i \in \overline{\mathbb{Q}}$, $h_j \in \mathbb{Q}[x_1, \ldots, x_m]$, and $\sigma_{j,l} \in \mathbb{Z}$ for all i, j, l. Define

$$\mathcal{I} = \sum_{j=1}^{A} \|h_j\| + \sum_{i=1}^{m} \|\lambda_i\| + \sum_{j=1}^{A} \sum_{l=1}^{k} |\sigma_{j,l}|.$$

Let $\mathbb{D} \subseteq \mathbb{C}^k$ denote the set of all points on which f is well-defined. In time $\mathcal{I}^{\textsc{Poly}(m+k)}$ we can construct semialgebraic $S_>, S_=, S_< \subseteq \mathbb{D}$ such that

$$\mathrm{Re}(f(z)) \ \Delta \ 0 \quad \Leftrightarrow \quad z \in S_\Delta$$

for all $z \in \mathbb{D}$ and $\Delta \in \{>, =, <\}$.

Proof. Write θ_1, θ_2 and θ_3, respectively, for the collections of variables $a_1, b_1, \ldots, a_m, b_m$, $x_1, y_1, \ldots, x_k, y_k$, and $u_1, v_1, \ldots, u_k, v_k$. The variables $a_i, b_i, x_l, y_l, u_l, v_l$ respectively stand for

$$\mathrm{Re}(\lambda_i), \mathrm{Im}(\lambda_i), \mathrm{Re}(z_l), \mathrm{Im}(z_l), \mathrm{Re}(z_l^{-1}), \mathrm{Im}(z_l^{-1}).$$

We also use a variable I that stands for the complex number $\boldsymbol{i}$. For $1 \leq j \leq A$ and $1 \leq l \leq k$, let $t_{j,l}(\theta_2, \theta_3)$ denote the term $(x_l + y_l I)^{\sigma_{j,l}}$ if $\sigma_{j,l} \geq 0$ and $(u_l + v_l I)^{-\sigma_{j,l}}$ otherwise. For $\alpha \in \overline{\mathbb{Q}}$, write θ_α for $(\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$. With this notation, for all $z = (z_1, \ldots, z_k) \in \mathbb{D}$, $1 \leq j \leq A$, and $1 \leq l \leq k$,

$$t_{j,l}(\theta_{z_1}, \ldots, \theta_{z_k}, \theta_{1/z_1}, \ldots, \theta_{1/z_k}) = z_j^{\sigma_{j,l}}.$$

Next, consider the term

$$t(I, \theta_1, \theta_2, \theta_3) \coloneqq \sum_{j=1}^{A} h_j(a_1 + b_1 I, \ldots, a_m + b_m I) t_{j,1}(\theta_2, \theta_3) \cdots t_{j,k}(\theta_2, \theta_3).$$

For all $z_1, \ldots, z_k \in \mathbb{D}$,

$$f(z_1, \ldots, z_k) = t(\boldsymbol{i}, \theta_{\lambda_1}, \ldots, \theta_{\lambda_m}, \theta_{z_1}, \ldots, \theta_{z_k}, \theta_{1/z_1}, \ldots, \theta_{1/z_k}).$$

Flatten the term t in time $\mathcal{I}^{O(k+l)}$ using Lemma 1.3.4 to obtain an equivalent flat term $t_1(I, \theta_1, \theta_2, \theta_3)$ of the form

$$t_1(I, \theta_1, \theta_2, \theta_3) = \sum_{j=0}^{B} q_j(\theta_1, \theta_2, \theta_3) I^j$$

where each q_j has rational coefficients. Recall that $\boldsymbol{i}^{j_1} = \boldsymbol{i}^{j_2}$ if $j_1 \equiv j_2 \bmod 4$. Moreover, each summand $q_j(\theta_1, \theta_2, \theta_3) I^j$ represents either a real or purely imaginary number, depending only on the value of j. Hence we define

$$p(\theta_1, \theta_2, \theta_3) \coloneqq \sum_{j \equiv 0 \bmod 4} q_j(\theta_1, \theta_2, \theta_3) - \sum_{j \equiv 2 \bmod 4} q_j(\theta_1, \theta_2, \theta_3).$$

For any $\mu_1 \in \mathbb{R}^{2m}$ and $\mu_2, \mu_3 \in \mathbb{R}^{2k}$ it holds that

$$\mathrm{Re}(t(\boldsymbol{i}, \mu_1, \mu_2, \mu_3)) = p(\mu_1, \mu_2, \mu_3).$$

We are now ready to construct S_Δ for $\Delta \in \{>, =, <\}$.

For $1 \leq i \leq m$, let φ_i be a quantifier-free formula defining λ_i. By Lemma 1.5.3, we can assume $\|\varphi_i\| < \textsc{Poly}(\mathcal{I})$ for all i. Let $L = \{1 \leq l \leq k \mid \exists j \colon \sigma_{j,l} < 0\}$ and $\delta(\theta_2) \coloneqq \bigwedge_{l \in L}(x_l \neq 0 \vee y_l \neq 0)$, which defines $\mathbb{D}$. Finally, recall that

$$(x + y\boldsymbol{i})(u + v\boldsymbol{i}) = xu - yv + (yu + xv)\boldsymbol{i}$$

for all $x, y, u, v \in \mathbb{R}$. The formula

$$\begin{aligned}\Phi(\theta_2) \coloneqq \delta(\theta_2) \;\wedge\; \exists\theta_1, \theta_3 \colon & \bigwedge_{i=1}^{m} \varphi_i(a_i, b_i) \\ & \wedge \bigwedge_{l=1}^{k} (x_l u_l - y_l v_l = 1 \wedge y_l u_l + x_l v_l = 0) \\ & \wedge p(\theta_1, \theta_2, \theta_3) \;\Delta\; 0\end{aligned}$$

defines S_Δ. It remains to invoke Theorem 1.3.5 (b) to eliminate quantifiers from Φ in time $\mathcal{I}^{\textsc{Poly}(m+k)}$. □

Conversely to the two lemmas above, we can extract canonical representations of algebraic numbers from a formula that defines them. The idea is as follows. Given $\varphi(x, y)$ defining a finite set $S = \{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{C}$, we first compute the projections S_x, S_y of S onto the two coordinates. By factorising polynomials appearing in the definitions of S_x and S_y, we identify defining polynomials of $\mathrm{Re}(\alpha_k)$ and $\mathrm{Im}(\alpha_k)$ for all $1 \leq k \leq m$. We combine these polynomials using resultants to obtain the defining polynomial of each α_k. This, in particular, shows that every α_k is algebraic. It remains to compute numerical approximations to each α_k. To do this, we first compute a bounded box B around zero in $\mathbb{C}$ that is guaranteed to enclose S. The root separation bound (Corollary 1.2.3) tells us how close two distinct points in S can be. Hence we can partition B into a collection of small squares each of which can contain at most one $\alpha \in S$. Finally, we use binary search to sieve through square subsets of B efficiently and locate all $\alpha \in S$.

Lemma 1.5.6. *Let $\varphi(x, y) \in \mathcal{L}_{or}$ be a quantifier-free formula defining a finite set $S = \{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{C}$. Every α_k is algebraic, and in time $\textsc{Poly}(\|\varphi\|)$ we can compute a canonical representation (f_k, ξ_k) of each $\alpha_k \in S$, with the additional property that $\|\xi_k\| < \|f_k\|^C$ for an absolute constant C.*

Proof. Apply Theorem 1.3.5 to formulas $\exists y \colon \varphi(x, y)$ and $\exists x \colon \varphi(x, y)$, respectively, to compute, in polynomial time, equivalent flat quantifier-free formulas

$$\begin{aligned}\varphi_1(x) &\coloneqq \bigvee_{i \in I} \bigwedge_{j \in J} p_{i,j}(x) \;\Delta_{i,j}\; 0, \\ \varphi_2(y) &\coloneqq \bigvee_{i \in A} \bigwedge_{j \in B} q_{i,j}(y) \;\Delta_{i,j}\; 0.\end{aligned}$$

Here each $p_{i,j}$ and $q_{i,j}$ is a polynomial with integer coefficients. The formulas φ_1, φ_2 define $\{\mathrm{Re}(\alpha_k) \mid 1 \leq k \leq m\}$ and $\{\mathrm{Im}(\alpha_k) \mid 1 \leq k \leq m\}$, respectively. Since these

are two finite semialgebraic subsets of $\mathbb{R}$, they contain only real algebraic points. It follows that $\alpha_k \in \overline{\mathbb{Q}}$ for all $1 \leq k \leq m$.

We argue that $\mathrm{Re}(\alpha_k)$ for each $\alpha_k \in S$ must be a root of some $p_{i,j}$ Observe that $p_{i,j}(x) \geq 0$ can be written as $p_{i,j}(x) > 0 \vee p_{i,j}(x) = 0$, and $p_{i,j}(x) \leq 0$ can be expressed similarly. Hence there exists a formula $\bigvee_{n\in N} \bigwedge_{l\in L} h_{n,l}(x)\ \Delta_{n,l}\ 0$, equivalent to $\varphi_1(x)$ such that $\Delta_{n,l} \in \{>, =, <\}$ and each $h_{n,l}$ is either $p_{i,j}$ or $-p_{i,j}$ for some i, j. Each conjunct $\bigwedge_{l\in L} h_{n,l}(x)\ \Delta_{n,l}\ 0$ that defines a non-empty set must contain an equality, as otherwise φ_1 would define infinitely many points. Hence every $x \in \mathbb{R}$ satisfying $\bigwedge_{l\in L} h_{n,l}(x)\ \Delta_{n,l}\ 0$ must satisfy $p_{i,j}(x) = 0$ for some i, j. By the same argument, each $\mathrm{Im}(\alpha_k)$ is a root of some $q_{i,j}$.

We next factor each $p_{i,j}$ in polynomial time using Theorem 1.2.1, and collect all irreducible and primitive polynomials we obtain into the set Y_1. Similarly, we collect all such factors of polynomials appearing in φ_2 into Y_2. Observe that for all $\alpha_k \in S$, the defining polynomials of $\mathrm{Re}(\alpha_k)$ and $\mathrm{Im}(\alpha_k)$ belong to Y_1 and Y_2, respectively.

We will next compute from Y_1 and Y_2 a set of polynomials Y that the contains the defining polynomials of $\alpha_1, \ldots, \alpha_m$. Our main tool is the resultant. The resultant $\mathrm{Res}_x(q(x, y), h(x, y))$ of two polynomials in $\mathbb{Z}[x, y]$ is a polynomial $r \in \mathbb{Z}[y]$ with the property that for all $y \in \mathbb{R}$, $r(y) = 0$ if and only if there exists $x \in \mathbb{R}$ such that $q(x, y) = h(x, y) = 0$. Given polynomials q and h (represented by flat terms), we can compute r (also represented by a flat term) in polynomial time [12, Chapter 4.2]. Moreover, if α is a root of q and β is a root of h, then by [83, Chapter 9.4]

(a) $\beta\boldsymbol{i}$ is a root of $\mathrm{Res}_y(t^2y^2 + 1, h(y)) \in \mathbb{Z}[t]$, and

(b) $\alpha + b\boldsymbol{i}$ is a root of $f_{q,h}(z) \coloneqq \mathrm{Res}_t(q(z - t), \mathrm{Res}_y(t^2y^2 + 1, h(y))) \in \mathbb{Z}[z]$.

By Lemma 1.3.4, we can flatten $q(z - t)$ in polynomial time. Hence $f_{q,h}$ can be computed from q, h in polynomial time. The set Y is then the set of all integral and primitive polynomials that divide $f_{q,h}$ for some $q \in Y_1$ and $h \in Y_2$. Since factorisation of integral polynomials and computation of resultants are both done in polynomial time, Y can be computed in time polynomial in $\|Y_1\| + \|Y_2\|$ and hence $\|\varphi\|$.

It remains to identify the defining polynomials of $\alpha_1, \ldots, \alpha_m$ in Y and construct numerical approximations from $\mathbb{Q}[\boldsymbol{i}]$ to form the canonical representations. We iterate over all $f \in Y$. Fix such f and let $H \coloneqq H(f)$, $d \coloneqq \deg(f)$ and

$$\delta \coloneqq \frac{1}{2(d+1)^{d+1}H^{d-1}}.$$

By Theorem 1.2.4, the roots of f are contained in the box $B \coloneqq [-1 - H, 1 + H]^2$. Since f is irreducible by construction, it is square-free and by Theorem 1.2.2, the

distance between any two of its roots is at most $\frac{\sqrt{3}}{(d+1)^{d+1}H^{d-1}}$. Hence any square subset of B of side length δ can contain at most one root of f. We will look for approximations to the roots of f in the grid

$$G \coloneqq B \cap \{\delta(n + m\boldsymbol{i}) \colon n, m \in \mathbb{Z}\}.$$

Observe that there are $(1 + 4(1 + H)(d + 1)^{d+1}H^{d-1})^2$ points in G, all which have description length at most $\textsc{Poly}(\log H, d) < \textsc{Poly}(\|\varphi\|)$. Our algorithm for locating the roots of f is binary search on rectangular subsets of B of the form

$$R(z_1, z_2) \coloneqq \{z \in \mathbb{C} \colon \operatorname{Re}(z_1) \leq \operatorname{Re}(z) \leq \operatorname{Re}(z_2) \ \wedge \ \operatorname{Im}(z_1) \leq \operatorname{Im}(z) \leq \operatorname{Im}(z_2)\}$$

where $z_1, z_2 \in G$ satisfy $\operatorname{Re}(z_1) \neq \operatorname{Re}(z_2)$ and $\operatorname{Im}(z_1) \neq \operatorname{Im}(z_2)$. Intuitively, z_1, z_2 respectively specify the top-left and bottom-right corners of a rectangle that is not allowed to be a line or a point. The starting rectangle is the whole of B. At each step it is checked whether the current rectangle R is a square of length δ. If yes, then R must contain a root and we output any corner $z \in G$ of R as an approximation to a root of f. Observe that the distance from the root α of f inside R to any of the corners is at most $\sqrt{2}\delta$, which is less than half of the root separation bound of Corollary 1.2.3. Hence α is the closest root of f to z.

If R is not a square of side length δ, then the algorithm checks whether the current rectangle $R(z_1, z_2)$ contains a root of f. This is done by verifying, in time polynomial in $\|f\|$, the sentence

$$\exists x, y \colon \operatorname{Re}(z_1) \leq x \leq \operatorname{Re}(z_2) \ \wedge \ \operatorname{Im}(z_1) \leq y \leq \operatorname{Im}(z_2) \ \wedge \ \Phi_f(x, y)$$

where $\Phi_f(x, y)$ is the formula defining the set of all roots of f given on page 28. If the current rectangle does not contain a root, it is discarded. Otherwise, the algorithm divides the current rectangle into two (overlapping) sub-rectangles of (approximately) the same size along the grid G. The side lengths of the resulting rectangles remains a multiple of δ. The algorithm is then recursively applied to the two sub-rectangles.

The entire root-finding algorithm runs in time polynomial in $\|f\|$ and produces $\xi_1, \ldots, \xi_n \in G$ with the guarantee that for each $1 \leq i \leq n$, there exists a root β of f satisfying $|\beta - \xi_i| < \sqrt{2}\delta$. Hence each (f, ξ_i) is a canonical representation of some root of f. If f has a root β for which $\operatorname{Re}(\beta)$ or $\operatorname{Im}(\beta)$ belongs to G, then it is possible for β to have more than one (at most 4) canonical representations among $(f, \xi_1), \ldots, (f, \xi_n)$. Let φ_i be a formula defining the number represented by (f, ξ_i) as described in Lemma 1.5.3. Using Corollary 1.5.4 repeatedly, we can select $d = \deg(f)$

distinct canonical representations $(f, \xi_{\sigma(1)}), \ldots, (f, \xi_{\sigma(d)})$ of all roots of f. This step also requires time polynomial in $\|f\|$. Since the magnitude of denominators and numerators of $\mathrm{Re}(\xi_i), \mathrm{Im}(\xi_i)$ is at most $(1+H)/\delta$ for all $1 \leq i \leq n$, $\|\xi_i\| < (\|f\|)^C$ for an absolute constant C.

Finally, we have to determine which, if any, of the roots of f for which we computed canonical representations actually belong to S. This can be done by verifying the formula

$$\exists x, y \colon \varphi_{\sigma(i)}(x, y) \ \wedge \ \varphi(x, y)$$

for $1 \leq i \leq d$ in polynomial time (Theorem 1.3.5 (c), note that the number of variables $N = 2$ is fixed). The total running time of our algorithm is at most polynomial in $\|\varphi\|$. □

This result can be used to perform operations on algebraic numbers as follows. Suppose we are given canonical representations of $\alpha_1, \ldots, \alpha_m$, and want to compute a canonical representation for $\beta \coloneqq f(\alpha_1, \ldots, \alpha_m)$ for a "reasonable" function f. First compute for each $1 \leq i \leq m$, a formula φ_i that defines α_i. Next, write a formula ψ constructed from $\varphi_1, \ldots, \varphi_m$ defining β. Eliminate quantifiers from ψ to obtain an equivalent quantifier-free formula φ, and apply Lemma 1.5.6 to construct a canonical representation of β.

1.5.4 Algorithms for operating on algebraic numbers

We next discuss how to perform various operations on algebraic numbers effectively and the complexity of resulting algorithms. First, a lemma about computing a canonical representation of $f(\alpha_1, \ldots, \alpha_m)$ where f is constructed from field operations in a certain restricted way.

Lemma 1.5.7. *Let $X = \{\alpha_1, \ldots, \alpha_m\}$ be a set of algebraic numbers in canonical form, $h = \max_{1 \leq i \leq m} h(\alpha_i)$, $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, and $D = [\mathbb{K} : \mathbb{Q}]$. Suppose we are given n specifications of the form*

$$\alpha_{m+i} \coloneqq \alpha_{\sigma(i)} \circ_i \alpha_{\mu(i)}$$

where $\sigma(i) < m + i$, $\mu(i) \leq m$, $\alpha_{\mu(i)} \neq 0$ and $\circ_i$ is a field operation for all $1 \leq i \leq n$.

(a) For all $m < i \leq m + n$, $h(\alpha_i) \leq i(h + \log 2)$, and

(b) canonical representations of $\alpha_{m+1}, \ldots, \alpha_{m+n}$ can be computed in time at most $\textsc{Poly}(\|X\|, n, D)$.

Proof. Since $h(\alpha_{\mu(i)}) \leq h$ for all $1 \leq i \leq n$, (a) follows from the results of Section 1.5.1 that for any $x, y \in \overline{\mathbb{Q}}$,

$$h(x+y),\, h(x \cdot y),\, h(x-y) \;\leq\; h(x) + h(y) + \log 2$$

and $h(1/y) = h(y)$ assuming $y \neq 0$. Since $\alpha_i \in \mathbb{K}$ for all i, $\deg(\alpha_i) \leq D$. As described in Section 1.5.1, $\log H(\alpha_i) \leq \deg(\alpha_i)(h(\alpha_i) + \log 2)$ for all α_i. Hence the defining polynomial p_i of α_i satisfies $\|p_i\| < \textsc{Poly}(\|X\|, n, D)$ for all i.

Our algorithm for computing $\alpha_{m+1}, \ldots, \alpha_{m+n}$ is as follows. For $1 \leq i \leq m$, let $(p_i, \tilde{\xi}_i)$, denote the canonical representation of α_i given as part of the input, and compute a quantifier-free formula $\varphi_i(x, y)$ defining α_i using Lemma 1.5.3. Next, apply Lemma 1.5.6 to obtain a new canonical representation (p_i, ξ_i) of α_i for $1 \leq i \leq m$ that satisfies $\|\xi_i\| < (\|p_i\|)^C$, where C is the absolute constant of Lemma 1.5.6. For $j = m+1, \ldots, m+n$, we perform the following steps. Let $k = \sigma(j)$ and $l = \mu(j)$. From canonical representations (p_k, ξ_k) and (p_l, ξ_l) of α_k and α_l, compute quantifier-free formulas φ_k and φ_l defining α_k and α_l, respectively. Next, construct a formula $\varphi_j(x, y)$ defining $\alpha_k \circ_j \alpha_l$ as follows.

(a) If $\circ_j$ is addition or subtraction, then $\varphi_j(x, y)$ is

$$\exists x_1, y_1, x_2, y_2 \colon\; x_1 \circ_i x_2 = x \;\wedge\; y_1 \circ_i y_2 = y \;\wedge\; \varphi_k(x_1, y_1) \;\wedge\; \varphi_l(x_2, y_2).$$

(b) If $\circ_j$ is multiplication, then $\varphi_j(x, y)$ is

$$\exists x_1, y_1, x_2, y_2 \colon\; x_1x_2 - y_1y_2 = x \;\wedge\; x_1y_2 + x_2y_1 = y \;\wedge\; \varphi_k(x_1, y_1) \;\wedge\; \varphi_l(x_2, y_2).$$

(c) If $\circ_j$ is division, then $\varphi_j(x, y)$ is

$$\exists x_1, y_1, x_2, y_2 \colon\; xx_2 - yy_2 = x_1 \;\wedge\; xy_2 + x_2y = y_1 \;\wedge\; \varphi_k(x_1, y_1) \;\wedge\; \varphi_l(x_2, y_2).$$

Next, eliminate quantifiers in polynomial time by Theorem 1.3.5 (observe that the total number of variables in $\varphi_j(x, y)$ is always exactly 6), and compute a canonical representation (p_j, ξ_j) of α_j using Lemma 1.5.6. This way we maintain the invariant

$$\|\xi_j\| < (\|p_j\|)^C$$

for all j. The step of computing the canonical representation of α_j requires time at most $\textsc{Poly}(\|p_k\|, \|\xi_k\|, \|p_l\|, \|\xi_l\|)$. We argued above that $\|p_i\| < \textsc{Poly}(\|X\|, i, D)$ for all $1 \leq i \leq m+n$. Combining this with $\|\xi_i\| < \textsc{Poly}(\|p_i\|)$ we conclude that the total time required to compute $\alpha_{m+1}, \ldots, \alpha_{m+n}$ is bounded by $\textsc{Poly}(\|X\|, n, D)$. □

Observe that in the lemma above we only allow sequences of operations whose syntax tree is right-deep. In particular, in the syntax tree every node has at least one child that is a leaf. We can handle more general sequences of operations by invoking Lemma 1.5.7 more than once, illustrated below.

Corollary 1.5.8. *Let $p \in \mathbb{Q}[x_1, \ldots, x_m]$, $\alpha_1, \ldots, \alpha_m \in \overline{\mathbb{Q}}$, $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, and D be the degree of the extension $\mathbb{K}/\mathbb{Q}$. We can compute a canonical representation of $p(\alpha_1, \ldots, \alpha_m)$ in time at most $\textsc{Poly}(D, \|p\|, \sum_{i=1}^m \|\alpha_i\|)$.*

Proof. For each monomial $f(x_1, \ldots, x_m) \coloneqq cx_1^{k_1} \ldots x_m^{k_m}$ appearing in the definition of p, by Lemma 1.5.7 we can compute in time $\textsc{Poly}(D, \|p\|, \sum_{i=1}^m \|\alpha_i\|)$ a canonical representation of $\beta_f \coloneqq f(\alpha_1, \ldots, \alpha_m)$. Writing M for the set of all monomials appearing in p, it remains to apply Lemma 1.5.7 once again with $X = \{\beta_f \colon f \in M\}$ to compute $\sum_{f \in M} \beta_f$. □

We can use our results about algebraic numbers to give an algorithm for factorising a given polynomial with *algebraic* coefficients.

Lemma 1.5.9. *Let $p(x) = \sum_{j=0}^d h_j(\lambda_1, \ldots, \lambda_m)x^j$ where each λ_i is algebraic and $h_j \in \mathbb{Q}[x_1, \ldots, x_m]$. Write*

$$\mathcal{I} = \sum_{j=1}^{d} \|h_j\| + \sum_{i=1}^{m} \|\lambda_i\|.$$

In time $\mathcal{I}^{\textsc{Poly}(m)}$ we can compute $N \leq d$ and $\beta_0, \ldots, \beta_N \in \overline{\mathbb{Q}}$ such that

$$p(x) = \beta_0 \prod_{i=1}^{N} (x - \beta_i).$$

Proof. Let $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_m)$ and $D = [\mathbb{K} : \mathbb{Q}]$. By the Tower Law, $D < \mathcal{I}^{\textsc{Poly}(m)}$. By Corollary 1.5.8 we compute and compare against zero each $\delta_j \coloneqq h_j(\lambda_1, \ldots, \lambda_m)$ in time $\textsc{Poly}(\mathcal{I}, D) < \mathcal{I}^{\textsc{Poly}(m)}$. Assume p is not identically zero, as otherwise the factorisation is trivial. The value of N is equal to the largest integer j such that $\delta_j \neq 0$, and β_0 is equal to δ_N.

Next, applying Lemma 1.5.5 with $k = 1$ construct a quantifier-free formula defining $S = \{x \in \mathbb{C} \colon p(x) = 0\}$ in time $\mathcal{I}^{\textsc{Poly}(m)}$. The set S is finite by the assumption that $\deg(p) > 0$. By Lemma 1.5.6 in time $\mathcal{I}^{\textsc{Poly}(m)}$ we can compute representations of all distinct algebraic numbers in S, which are the distinct roots of p. It remains to determine the multiplicities of the roots, which can be done by taking the derivatives

$p^{(1)}(x), \ldots, p^{(N)}(x)$ and computing the distinct roots of $p^{(l)}(x)$ for all $1 \leq l \leq N$. To prove the complexity claim, observe that

$$p^{(l)}(x) = \sum_{j=0}^{N-l} (j+l) \cdots (j+1) h_j(\lambda_1, \ldots, \lambda_m) x^j$$

and hence the total description length of each $p^{(l)}$ above, viewed as a non-flat term, is at most polynomial in $\mathcal{I}$. □

One final operation we will frequently perform is computing the modulus of an algebraic number, which is algebraic itself.

Lemma 1.5.10. *Given $\alpha \in \overline{\mathbb{Q}}$, we can compute $|\alpha|$ in polynomial time.*

Proof. Let φ be a formula defining α, constructed from the given canonical representation of α in polynomial time using Lemma 1.5.3. Observe that $|\alpha|$ is defined by the formula

$$\psi(x) \coloneqq \exists x_1, y_1 \colon \varphi(x_1, y_1) \wedge x_1^2 + y_1^2 = x^2.$$

It remains to eliminate quantifiers from ψ and apply Lemma 1.5.6 to the resulting formula. □

1.6 Algebraic geometry

The *n-dimensional affine space* over $\mathbb{C}$, denoted by $\mathbb{A}^n$, is the set of all tuples $(x_1, \ldots, x_n)$ where $x_i \in \mathbb{C}$ for all $1 \leq i \leq n$. A set $V \subseteq \mathbb{A}^n$ is an *affine (algebraic) variety* if there exist polynomials $p_1, \ldots, p_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that

$$V = \{x \in \mathbb{A}^n \mid p_1(x) = \ldots = p_m(x) = 0\}.$$

Finite unions and arbitrary intersections of affine varieties are themselves affine varieties. We can therefore endow $\mathbb{A}^n$ with the *Zariski topology* where closed sets are precisely the affine varieties. The *Zariski closure* of $X \subseteq \mathbb{A}^n$ is the smallest closed subset of $\mathbb{A}^n$ containing X. We endow subsets of $\mathbb{A}^n$ with the induced subset topology. A set $X \subseteq \mathbb{A}^n$ is

(a) *irreducible* if, viewed as a topological space, it is not a union of two disjoint closed sets,

(b) *Zariski-dense* if its closure is $\mathbb{A}^n$, and

(c) a *quasi-affine variety* if it is an open subset of an affine variety.

Every affine variety is a finite union of irreducible affine varieties. All open subsets of $\mathbb{A}^n$ are Zariski-dense. Finally, the quasi-affine varieties we will encounter are all the form $\{x \in \mathbb{A}^n \mid p(x) \neq 0\}$ where $p \in \mathbb{C}[x_1, \ldots, x_n]$.

The *(complex) dimension* $\dim(V)$ of an affine variety V is the largest integer k such that there exist irreducible affine varieties $V_0, \ldots, V_k$ such that

$$V_0 \subset \ldots \subset V_k \subseteq V.$$

The affine space $\mathbb{A}^n$ has dimension n. The dimension $\dim(X)$ of arbitrary $X \subseteq \mathbb{A}^n$ is defined as the dimension of its Zariski closure. Hence $X \subseteq Y \Rightarrow \dim(X) \leq \dim(Y)$. Dimension of any $X \subseteq \mathbb{A}^n$ is at most n.

We have so far discussed the *objects* in our setting, namely the quasi-affine varieties. A *morphism* φ from a quasi-affine variety $V \subseteq \mathbb{A}^n$ to $\mathbb{A}$, also called a *regular function*, is a function such that for every $x \in V$, there exist an open subset O of V containing x, and polynomials $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ such that

1. g is non-zero on O, and
2. $\varphi(z) = f(z)/g(z)$ for all $z \in O$.

A morphism between quasi-affine varieties $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$, also called a *regular map*, is a map $\varphi : V \to W$ given by $x \mapsto (\varphi_1(x), \ldots, \varphi_m(x))$, where each φ_i is a regular function. Polynomial maps are examples of morphisms. The morphisms of quasi-affine maps are *continuous* with respect to the Zariski topology.

We will not need to work with dimensions of varieties directly. The main result we will need is the following theorem (analogous to the rank-nullity theorem from linear algebra) that describes how dimension of a quasi-affine variety behaves under the application of a morphism.[4]

Theorem 1.6.1 ([41, Thereom 11.12])**.** *Let V be an irreducible quasi-affine variety, $\varphi : V \to \mathbb{A}^m$ be a morphism of quasi-affine varieties, and W be the Zariski closure of $\varphi(V)$. For $x \in V$, write $\mu(x) = \dim(\varphi^{-1}(\varphi(x)))$. It holds that*

$$\dim(V) = \dim(W) + \min_{x \in V} \mu(x).$$

We will only encounter injective morphisms, for which the situation is simpler.

[4] In fact, this result holds for morphisms of *quasi-projective* varieties, which are more general than quasi-affine varieties.

Corollary 1.6.2. *Let $\varphi : V \to U$ be an injective morphism of quasi-affine varieties. It holds that*

$$\dim(V) = \dim(\varphi(V)) \leq \dim(U).$$

Proof. Let $V_1, \ldots, V_m$ be irreducible components of V. Denote by W the Zariski closure of $\varphi(V)$ and by W_i the Zariski closure of V_i for $1 \leq i \leq m$. Observe that $W = \cup_{i=1}^{m} W_i$. By injectivity, $\dim(\varphi^{-1}(\varphi(x))) = 0$ for all $x \in V$. By Theorem 1.6.1, $\dim(V_i) = \dim(W_i)$ for all i. Hence

$$\dim(V) = \max_{1 \leq i \leq m} \dim(V_i) = \max_{1 \leq i \leq m} \dim(W_i) = \dim(W) = \dim(\varphi(V)).$$

That $\dim(\varphi(V)) \leq \dim(U)$ follows from $\varphi(V) \subseteq U$. □

1.7 Jordan normal form

A *Jordan block* is a matrix of the form $\lambda I + N$, where $\lambda \in \mathbb{C}$ and N is the nilpotent matrix defined by

$$N_{i,j} = \begin{cases} 1, & \text{if } j = i+1 \\ 0, & \text{otherwise.} \end{cases}$$

A *real Jordan block* is of the form $\begin{bmatrix} \Lambda & I & & \\ & \ddots & \ddots & \\ & & \Lambda & I \\ & & & \Lambda \end{bmatrix}$ where either $\Lambda \in \mathbb{R}^{1\times 1}$, or $\Lambda = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$, $b \neq 0$. In the latter case, the matrix has precisely two eigenvalues $a + b\boldsymbol{i}$ and $a - b\boldsymbol{i}$, both non-real. A matrix J is in *(real) Jordan form* if $J = \mathrm{diag}(B_1, \ldots, B_m)$, where each B_k is a (real) Jordan block. It is classical that every square matrix M is similar to a matrix J in Jordan form. If M has rational entries, then J can in fact be computed in polynomial time.

Theorem 1.7.1 (Jin-Yi Cai, [22])**.** *Given $M \in \mathbb{Q}^{d\times d}$, in polynomial time one can compute the following.*

(a) Matrices S, J, P with algebraic entries such that J is in Jordan form, $S = P^{-1}$, and $M = SJP$;

(b) For each entry α of S, J or P, an eigenvalue λ of M and a polynomial $p \in \mathbb{Q}[x]$ such that $\alpha = p(\lambda)$.

Throughout this paper, unless stated otherwise, we make the following assumptions on the structure of S, J, P, permitted by Cai's algorithm. In particular, we assume that the first $2l_1$ blocks of J have two non-real eigenvalues, and the following l_2 blocks have a single real eigenvalue.

(1) $J = \mathrm{diag}(B_1, \ldots, B_{2l_1+l_2})$, where $l_1, l_2 \geq 0$ and $B_k = \lambda_k I + N \in \overline{\mathbb{Q}}^{d_k \times d_k}$ for all k.

(2) P is of the form $\begin{bmatrix} C_1 & \cdots & C_{2l_1+l_2} \end{bmatrix}$ and $S^\top$ is of the form $\begin{bmatrix} A_1 & \cdots & A_{2l_1+l_2} \end{bmatrix}$, where $C_k, A_k \in \overline{\mathbb{Q}}^{d \times d_k}$ for all $1 \leq k \leq 2l_1 + l_2$.

(3) For $1 \leq k \leq l_1$, λ_k is non-real, and A_{2k}, B_{2k}, C_{2k} are the entrywise complex conjugates of $A_{2k-1}, B_{2k-1}, C_{2k-1}$, respectively.

(4) For $l_1 < k \leq l_2$, A_k, B_k, C_k have real entries.

(5) There exists $1 \leq j \leq 2l_1 + l_2$ such that $\lambda_k \neq 0$ for all $k \leq j$ and $\lambda_j = 0$ for all $k > j$. That is, $J = \mathrm{diag}(J_1, J_2)$ where J_1 is invertible and J_2 is nilpotent.

Real Jordan Form. Given $M \in \mathbb{Q}^{d \times d}$, in polynomial time we can also compute $S_r, J_r, P_r \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ such that J_r is in real Jordan form, $S_r = (P_r)^{-1}$, and

$$M = S_r J_r P_r.$$

The construction follows the standard proof of existence of real Jordan forms. Assume we have already computed S, J, P and the blocks A_k, B_k, C_k for $1 \leq k \leq 2l_1 + l_2$ as above. For $1 \leq k \leq l_1$, let

$$\tilde{A}_k = \frac{1}{2}\begin{bmatrix} A_{2k-1} + A_{2k} & \boldsymbol{i}(A_{2k} - A_{2k-1}) \end{bmatrix},$$
$$\tilde{C}_k = \frac{1}{2}\begin{bmatrix} C_{2k-1} + C_{2k} & \boldsymbol{i}(C_{2k} - C_{2k-1}) \end{bmatrix},$$

and $\tilde{B}_k$ denote the real Jordan block belonging to $(\mathbb{R} \cap \overline{\mathbb{Q}})^{2d_k \times 2d_k}$ with eigenvalues $\lambda_k, \overline{\lambda_k}$. We can then choose

$$S_r^\top = \begin{bmatrix} \tilde{A}_1 & \cdots & \tilde{A}_{l_1} & A_{2l_1+1} & \cdots & A_{2l_1+l_2} \end{bmatrix}$$
$$P_r = \begin{bmatrix} \tilde{C}_1 & \cdots & \tilde{C}_{l_1} & C_{2l_1+1} & \cdots & C_{2l_1+l_2} \end{bmatrix}$$

and $J_r = \mathrm{diag}(\tilde{B}_1, \ldots, \tilde{B}_{l_1}, B_{2l_1+1}, \ldots, B_{2l_1+l_2})$. Finally, let J_r' be in real Jordan form and obtained from J_r through permutation of blocks. In polynomial time, we can compute S_r', P_r' (that are obtained by permuting of rows and columns of S_r and P_r, respectively) such that $S_r' = (P_r')^{-1}$ and $M = S_r' J_r' P_r'$.

Raising a matrix to an integer power. For $k \geq 0$, let

$$q_k(x) = \frac{1}{k!}x(x-1)\cdots(x-k+1).$$

It is well-known that for a Jordan block $B = \lambda I + N \in \overline{\mathbb{Q}}^{d\times d}$ with $\lambda \neq 0$,

$$(B^n)_{i,j} = \begin{cases} \lambda^{i-j}\lambda^n q_{j-i}(n) & \text{if } i \leq j, \\ 0 & \text{otherwise.} \end{cases} \tag{1.2}$$

Hence the entries of M^n for M invertible can be expressed in terms of n and the powers of the eigenvalues.

Lemma 1.7.2. *Let $M \in \overline{\mathbb{Q}}^{d\times d}$ be invertible with distinct non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$. For all $1 \leq i, k \leq d$, $(M^n)_{i,k}$ is of the form $\sum_{j=1}^{A} p_j(n)\lambda_j^n$ where each p_j has algebraic coefficients and $\sum_{j=1}^{A}(\deg(p_j)+1) \leq d$.*

Proof. Factorise $M = P^{-1}JP$ where $J = \operatorname{diag}(B_1, \ldots, B_l)$ is in Jordan form and each B_a for $1 \leq a \leq l$ is a Jordan block from $\overline{\mathbb{Q}}^{d_a\times d_a}$ with the non-zero eigenvalue λ_a. The entries of B_a^n are of the form $p(n)\lambda_a^n$ where p has algebraic coefficients and degree at most $d_a - 1$. It remains to recall $\sum_{i=1}^{l} d_a = d$. □

We now discuss the complexity of constructing the polynomials $p_1, \ldots, p_A$ in Lemma 1.7.2, and what to do in case M is not invertible. As shown in Equation (1.2), the entries of B^n, where $B = \lambda I + N \in \overline{\mathbb{Q}}^{d\times d}$ with $\lambda \neq 0$, are of the form $t(n, \lambda^{-1}, \lambda^n)$ for $0 \leq k < d$ and the non-flat term $t(x_1, x_2, x_3) \coloneqq x_2^k x_3 q_k(x_1)$. Let $\sum_{i=0}^{\deg(\lambda)} a_i x^i$ be the minimal polynomial of λ with $a_0, a_{\deg(\lambda)} \neq 0$. Observe that $\lambda^{-1} = \frac{1}{a_0}\sum_{i=1}^{\deg(\lambda)} a_i \lambda^{i-1}$. That is, λ^{-1} can be expressed as a rational linear combination of powers of λ. It follows that the entries of B^n can in fact be written as $s(n, \lambda, \lambda^n)$, where s is again a non-flat term. On the other hand, if $C \in \overline{\mathbb{Q}}^{d\times d}$ is nilpotent, then $C^n = \mathbf{0}$ for all $n \geq d$. We therefore arrive at the following.

Theorem 1.7.3. *Let $M \in \mathbb{Q}^{d\times d}$. Write $N = d$ if the Jordan form of M contains a non-diagonalisable nilpotent block and $N = 0$ otherwise. In time polynomial in $\|M\|$ we can compute the distinct non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$ of M as well as (non-flat) terms $t_{i,j}$ for $1 \leq i, j \leq d$ with the following property. For all i, j and $n \geq N$,*

(a) $(M^n)_{i,j} = t_{i,j}(\lambda_1, \ldots, \lambda_m, \lambda_1^n, \ldots, \lambda_m^n)$ if M is diagonalisable, and

(b) $(M^n)_{i,j} = t_{i,j}(\lambda_1, \ldots, \lambda_m, n, \lambda_1^n, \ldots, \lambda_m^n)$ otherwise.

Proof. First compute $S = P^{-1}, J, P$ in polynomial time as in Theorem 1.7.1 (a). Apply Theorem 1.7.1 (b) to express entries of P^{-1} and P in the form $p(\lambda)$ where $p \in \mathbb{Q}[x]$ and λ is an eigenvalue of M. The distinct non-zero eigenvalues of M can be read off from the diagonal J using Corollary 1.5.4.

Suppose M is diagonalisable. Then $N = 0$ and for all $1 \leq i, j \leq d$, $(J^n)_{i,j}$ is either identically zero or equal to λ_k^n for some k. It remains to compute each $t_{i,j}$ from the equality $(M^n)_{i,j} = e_i P^{-1} J^n P e_j^\top$.

Next, suppose M is non-diagonalisable. Choose $1 \leq i, j \leq d$. As discussed above, for $n \geq N$, $(J^n)_{i,j}$ is either always zero, or can be expressed as $h_{i,j}(n, \lambda_k, \lambda_k^n)$ for integer $1 \leq k \leq m$ and non-flat term $h_{i,j}$ that can be computed in polynomial time. It remains to once again compute $t_{i,j}$ from $(M^n)_{i,j} = e_i P^{-1} J^n P e_j^\top$. □

Note that the terms $t_{i,j}$ computed above are non-flat. If we want to turn them into *bona fide* polynomials using the Flattening Lemma, we incur the cost of $\|M\|^{O(d)}$, which is not polynomial in $\|M\|$.

1.8 Words and automata

We will work with finite and infinite words over a finite alphabet Σ. As usual, we write Σ^* for $\cup_{l \in \mathbb{N}} \Sigma^l$, and Σ^ω for the set of all infinite sequences over Σ. We denote the length of a finite word u by $|u|$. For a word u and $k \geq 0$, we write $u(k)$ for the kth letter of u. Hence for u with $|u| = l$,

$$u = u(0) \cdots u(l-1).$$

For $0 \leq k \leq j$ we define

(a) $u[k, j] = u(k) \cdots u(j)$,

(b) $u[k, j) = u(k) \cdots u(j-1)$, and

(c) for an infinite word u, $u[k, \infty) = u(k)u(k+1) \cdots$.

A finite word u occurs at a position k in (finite or infinite) α if the latter can be factorised as $\alpha = wu\beta$ where $|w| = k$. A *factor* u of a word α is a finite word that occurs at some position in α. Let α_i be an infinite word over Σ_i for $0 \leq i < L$. The *product* of $\alpha_0, \ldots, \alpha_{L-1}$, written $\alpha_0 \times \cdots \times \alpha_{L-1}$, is the word α over the product alphabet $\Sigma_0 \times \cdots \times \Sigma_{L-1}$ defined by $\alpha(n) = (\alpha_0(n), \ldots, \alpha_{L-1}(n))$ for all $n \in \mathbb{N}$. The *merge*, also known as *shuffling* or *interleaving* of $\alpha_0, \ldots, \alpha_{L-1}$, is the word α over the alphabet $\Sigma_0 \cup \cdots \cup \Sigma_{L-1}$ defined by $\alpha(qL + r) = \alpha_r(q)$ for all $0 \leq r < L$ and $q \in \mathbb{N}$.

A *property* or a *language* is a subset of Σ^ω. Recall that a property is *ω-regular* if it is precisely the set of all words accepted by a non-deterministic Büchi automaton. By McNaughton's theorem [60], every ω-regular property is the set of words accepted by a deterministic Muller automaton, which is a tuple $\langle Q, q_0, \delta, F\rangle$ comprising the following.

(i) Finite set of states Q;

(ii) Unique initial state $q_0 \in Q$;

(iii) Transition function $\delta\colon Q \times \Sigma \to Q$;

(iv) $F \subseteq \mathcal{P}(Q)$, called the *acceptance condition*.

Each word $\alpha \in \Sigma^\omega$ has a unique *run* $\mathcal{A}(\alpha) \in Q^\omega$ in a deterministic (Muller) automaton $\mathcal{A}$, which is the set of states visited when $\mathcal{A}$ reads α. The automaton $\mathcal{A}$ *accepts* α, written $\mathcal{A} \models \alpha$, if the set of states that appear infinitely often in $\mathcal{A}(\alpha)$ is present in F. The *property recognised by* $\mathcal{A}$ is the set of all words accepted by $\mathcal{A}$. In this thesis we will assume that all ω-regular properties, which will serve as specifications for linear dynamical systems, are presented by a deterministic Muller automaton.

A property $L \subseteq \Sigma^\omega$ is *prefix-independent* if for all infinite words α, β that can be obtained from one another through finitely many insertions and deletions, it holds that

$$\alpha \in L \qquad \Leftrightarrow \qquad \beta \in L.$$

Intuitively, a prefix-independent property is a set of words that share common *asymptotic* behaviour: It is not possible to change membership of a word in a prefix-independent language through finitely many modifications. Prefix-independent properties (excluding $L = \emptyset$) are special cases of *liveness* properties.

1.9 Monadic second-order logic

The monadic second-order logic is an extension of the first-order logic that allows quantification over subsets of the universe. Such subsets can be viewed as unary (that is, monadic) predicates. We will only be interpreting MSO formulas over extensions of the structure $\langle \mathbb{N}; < \rangle$. For a general perspective on MSO, see [18].

Let $\mathbb{S} \coloneqq \langle \mathbb{N}; <, P_1, \ldots, P_m\rangle$ be a structure where each $P_i : \mathbb{N} \to \{0, 1\}$ is a unary predicate. We associate a language $\mathcal{L}_\mathbb{S}$ of terms and formulas with $\mathbb{S}$ as follows. The

terms of $\mathcal{L}_{\mathbb{S}}$ are the elements $0, 1, 2, \ldots$ of $\mathbb{N}$, lowercase variable symbols that stand for elements of $\mathbb{N}$, and uppercase variable symbols that denote subsets of $\mathbb{N}$. The formulas of $\mathcal{L}_{\mathbb{S}}$ are the well-formed statements obtained from the built-in equality ($=$) and membership ($\in$) symbols, logical connectives, quantification over elements of $\mathbb{N}$ (written Qx for a quantifier Q), and quantification over subsets (written QX for a quantifier Q). The MSO theory of the structure $\mathbb{S}$ is the set of all sentences belonging to $\mathcal{L}_{\mathbb{S}}$ that are true in $\mathbb{S}$. The MSO theory of $\mathbb{S}$ is *decidable* if there exists an algorithm that, given a sentence $\varphi \in \mathcal{L}_{\mathbb{S}}$, decides if φ belongs to the MSO theory of $\mathbb{S}$. We give an example below.

Let $\mathbb{S} = \langle \mathbb{N}; <, P \rangle$, where P is the primes predicate: for all $n \in \mathbb{N}$, $P(n) = 1$ if and only if n is prime. Consider definitions

$$\varphi(X) \coloneqq 1 \in X \ \wedge\ 0, 2 \notin X \ \wedge\ \forall x.\, x \in X \Leftrightarrow s(s(s(x))) \in X$$
$$\psi \coloneqq \exists X \colon \varphi(X) \ \wedge\ \forall y.\, \exists z > y \colon z \in X \ \wedge\ P(z)$$

where $s(\cdot)$ is the successor function defined by $s(x) = y$ if and only if

$$x < y \quad \wedge \quad \forall z.\, x < z \Rightarrow y \leq z.$$

That is, $s(x) = x + 1$. The formula φ defines the subset $\{n \colon n \equiv 1 (\mathrm{mod}\ 3)\}$ of $\mathbb{N}$, and ψ is the sentence "there are infinitely many primes congruent to 1 modulo 3", which is trthe caseue. Another example of a number-theoretic statement expressible in our setting would be the Twin Primes Conjecture, which is given by the first-order sentence

$$\forall x.\, \exists y > x \colon P(y) \wedge P(s(s(y))).$$

Unsurprisingly, the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$, where P is the primes predicate, is not known to be decidable. However, it is not known to be undecidable either. We discuss extensions of $\langle \mathbb{N}; < \rangle$ with decidable MSO theories in Chapter 3.

Chapter 2

Linear recurrence sequences

In this chapter we recall the classical theory of linear recurrence sequences and describe the state of the art regarding their decision problems. We discuss tools for locating the zeros of LRS and estimating their growth rates, most notably the Skolem-Mahler-Lech theorem and Baker's theorem. Applying these techniques, in Section 2.7 we give a novel effective Skolem-Mahler-Lech theorem (and hence a decision procedure for the Skolem Problem) for certain families of sequences that arise when analysing the Model-Checking Problem with tame targets (Chapter 6).

A sequence $(u_n)_{n\in\mathbb{N}}$ over a ring $R \subseteq \mathbb{C}$ is a *linear recurrence sequence* (alternatively, a *constant-recursive*, *c-recursive*, or *c-finite* sequence) over R if there exists a positive integer d and a *recurrence relation* $(a_0, \ldots, a_{d-1}) \in \mathbb{R}^d$ such that

$$u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i}$$

for all $n \in \mathbb{N}$. The *order* of $(u_n)_{n\in\mathbb{N}}$ is the smallest $d > 0$ such that $(u_n)_{n\in\mathbb{N}}$ satisfies a recurrence relation in R^d. In this thesis we will work with linear recurrence sequences over the fields $\mathbb{Q}$, $\overline{\mathbb{Q}}$, and $\mathbb{R} \cap \overline{\mathbb{Q}}$. Examples of rational LRS (i.e. LRS over $\mathbb{Q}$) include the Fibonacci sequence, $u_n = p(n)$ for $p \in \mathbb{Q}[x]$, as well as $u_n = \cos(n\theta)$ for $\theta \in \{\arg(\lambda) \mid \lambda \in \mathbb{Q}(\boldsymbol{i})\}$. We refer the reader to the books by Everest et al. [35] and Kauers and Paule [49], which are the main references for this chapter, for a detailed discussion of linear recurrence sequences.

An LRS is *non-trivial* if it is not eventually identically zero. Let $(u_n)_{n\in\mathbb{N}}$ be a non-trivial LRS satisfying a recurrence relation $a = (a_0, \ldots, a_{d-1})$. If $a_0 = 0$, then $d > 1$ by non-triviality, and $b = (a_1, \ldots, a_{d-1})$ is a shorter recurrence relation satisfied by $(u_n)_{n\in\mathbb{N}}$. Hence we can assume that non-trivial sequences are always given by a recurrence relation whose first coefficient is non-zero.

In Section 2.2 we will show that each non-trivial LRS over $\overline{\mathbb{Q}}$ can be written uniquely in the *exponential polynomial* form

$$u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$$

where $A > 0$, each p_j is a non-zero polynomial with algebraic coefficients and $\lambda_1, \ldots, \lambda_A$, called the *eigenvalues* or *roots* of $(u_n)_{n\in\mathbb{N}}$, are non-zero and pairwise distinct algebraic numbers. An eigenvalue λ is *dominant* if for every eigenvalue λ', $|\lambda'| \leq |\lambda|$. We say that a non-trivial linear recurrence sequence is

(a) *simple* (also called *diagonalisable*) if each p_j is constant, and

(b) *non-degenerate* if λ_i/λ_j is not a root of unity for all $i \neq j$ and all real eigenvalues of $(u_n)_{n\in\mathbb{N}}$ are positive.[1]

Linear recurrence sequences over a field R are closed under multiplication by constants from R, ring operations [49, Theorem 4.2], taking subsequences of the form $v_n = u_{nL+r}$ for $L > 0$ and $r \in \mathbb{Z}$, and taking suffixes of the form $v_n = u_{n+k}$ for $k \geq 0$. Moreover, if the input sequences to all of these operations are diagonalisable, then so is the resulting sequence. Finally, by the Fatou Lemma [14, Chapters 6.1 and 7.2], if R is an integral domain, $\mathbb{K}$ is a field enclosing R, and $(u_n)_{n\in\mathbb{N}}$ is a sequence over R that is an LRS over $\mathbb{K}$, then $(u_n)_{n\in\mathbb{N}}$ is also an LRS over R.[2]

By [35, Theorem 1.2], for every LRS $(u_n)_{n\in\mathbb{N}}$ of order k there exists $L = 2^{O(k\sqrt{\log k})}$ such that the sequences $(u_{nL+r})_{n\in\mathbb{N}}$ for $0 \leq r < L$ are all either identically zero or non-degenerate. Hence by taking L subsequences we can reduce many problems of general LRS to problems about non-degenerate sequences.

2.1 Matrix representation of linear recurrence sequences

Linear recurrence sequences play a vital role in the analysis of linear dynamical systems. A link between LRS and LDS is immediate from the matrix representation of LRS. Let $(u_n)_{n\in\mathbb{N}}$ be an LRS over R satisfying a recurrence relation $a = (a_0, \ldots, a_{d-1}) \in R^d$.

[1] The classical definition of non-degeneracy only includes the first condition.

[2] In combination with closure of LRS over a field R under ring operations, the Fatou lemma implies that LRS over an arbitrary integral domain are closed under ring operations.

The matrix

$$C \coloneqq \begin{bmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ a_0 & a_1 & \cdots & a_{d-1} \end{bmatrix} \in R^{d \times d}$$

is called the *companion matrix* of the recurrence relation a. Writing $s = (u_0, \ldots, u_{d-1})$, we have that

$$C^n s = (u_n, \ldots, u_{n-d+1})$$

and $u_n = e_1 C^n s$ for all $n \in \mathbb{N}$, where e_i denotes the ith standard basis vector. Hence we can present any LRS $(u_n)_{n\in\mathbb{N}}$ over R in the form $u_n = c^\top M^n s$ where $M \in R^{d\times d}$ and $c, s \in R^d$. Observe that C is invertible if $a_0 \neq 0$, which we can assume for non-trivial sequences as discussed above. Conversely, any sequence $v_n = c^\top M^n s$, where $M \in R^{d\times d}$ and $c, s \in R^d$, is an LRS over R. To see this, let $p(x) \coloneqq \det(xI - M) = \sum_{i=0}^{d} b_i x^i$ be the characteristic polynomial of M, noting that $b_d = 1$ and $b_i \in R$ for all i. By the Cayley-Hamilton theorem, $p(M) = 0$. That is,

$$M^d = -\sum_{i=0}^{d-1} b_i M^i$$

and hence for all $n \in \mathbb{N}$,

$$c^\top M^{n+d} s = -\sum_{i=0}^{d-1} b_i c^\top M^{n+i} s.$$

That is, $v_{n+d} = b_0 v_n + \cdots + b_{d-1} v_{n+d-1}$ for all n. Therefore, $(v_n)_{n\in\mathbb{N}}$ is an LRS over R satisfying the recurrence relation $(-b_0, \ldots, -b_{d-1})$.

Using the matrix representation of LRS, decision problems about linear recurrence sequences can be formulated in a more geometric way in terms of linear dynamical systems. We say that a hyperplane or a halfspace is *rational* if it can be defined in the form $\{x \in \mathbb{R}^d \mid c^\top x \; \Delta \; 0\}$ where $\Delta \in \{\geq, >, =\}$ and $c \in \mathbb{Q}^d$.

(a) Recall that the **Skolem Problem** over $\mathbb{Q}$ is to decide, given a rational LRS $(u_n)_{n\in\mathbb{N}}$, whether $u_n = 0$ for some n. Writing $u_n = c^\top M^n s$, $u_n = 0$ for some n if and only if the orbit of (M, s) reaches the rational hyperplane $H = \{x \mid c^\top x = 0\}$. Conversely, the orbit of (M, s) reaches a rational hyperplane H with normal vector $c \in \mathbb{Q}^d$ if and only if the LRS $u_n = c^\top M^n s$ has a zero. Therefore, the Skolem Problem is Turing-equivalent to the Reachability Problem with rational hyperplane targets: given $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ and a rational hyperplane $H \subset \mathbb{R}^d$, decide whether the orbit of (M, s) reaches H.

(b) The **Positivity Problem** over $\mathbb{Q}$ is to decide, given a rational LRS $(u_n)_{n\in\mathbb{N}}$, whether $u_n \geq 0$ for all n. By the same argument as in (a), it is equivalent to deciding, given a linear dynamical system (M, s) and a rational halfspace $H = \{x \mid c^\top x \geq 0\}$, whether the orbit of (M, s) always remains in H.

(c) The **Ultimate Positivity Problem** over $\mathbb{Q}$ is to decide, given a rational LRS $(u_n)_{n\in\mathbb{N}}$, whether $u_n \geq 0$ for all sufficiently large n. In terms of LDS, it is equivalent to deciding whether the orbit of given (M, s) is eventually trapped in a rational halfspace $H = \{x \mid c^\top x \geq 0\}$.

We will discuss the decidability status of these problems in Sections 2.3 and 2.5.

2.2 Exponential polynomial representation of linear recurrence sequences

The Fibonacci sequence can be written in the form $u_n = \frac{1}{2}\varphi^n + \frac{1}{2}\Phi^n$, where $\varphi, \Phi \in \overline{\mathbb{Q}}$ are the roots of the characteristic polynomial $p(x) = x^2 - x - 1$ associated with the recurrence relation $u_{n+2} = u_{n+1} + u_n$. More generally, every non-trivial LRS $(u_n)_{n\in\mathbb{N}}$ over $\overline{\mathbb{Q}}$ can be written in the form

$$u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n \tag{2.1}$$

where $A > 0$, $\lambda_1, \ldots, \lambda_A \in \overline{\mathbb{Q}}$ are non-zero and pairwise distinct, and each p_j is a non-zero polynomial with algebraic coefficients. Moreover, if $(u_n)_{n\in\mathbb{N}}$ satisfies a recurrence relation $a = (a_0, \ldots, a_{d-1}) \in \overline{\mathbb{Q}}^d$, then $\sum_{j=1}^{A}(\deg(p_j) + 1) \leq d$. To prove these statements, let C be the companion matrix of the recurrence relation a and $s = (u_0, \ldots, u_{d-1})$. Recall that $u_n = e_1 C^n s$. As discussed above, by non-triviality of $(u_n)_{n\in\mathbb{N}}$ we can assume that C is invertible. It remains to express $C = P^{-1}JP$, where J is in Jordan form, and invoke Lemma 1.7.2. In the end, $\lambda_1, \ldots, \lambda_A$ form a subset of the eigenvalues of J. Moreover, if J is diagonalisable then $p_j \in \overline{\mathbb{Q}}$ for all j.

The right-hand side of Equation (2.1), with the restrictions that $\lambda_1, \ldots, \lambda_A$ are non-zero and pairwise distinct, and each p_j is not identically zero, is called an *exponential polynomial*. The exponential polynomial representation of an LRS is unique. This is a folklore result for which we provide a proof below in Theorem 2.2.2. The first step is to show that an exponential polynomial with $A > 0$ cannot be identically zero.

Lemma 2.2.1. *Let $u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$, where the right-hand side is an exponential polynomial with $A > 0$. The sequence $(u_n)_{n\in\mathbb{N}}$ is not identically zero. Specifically, there exists $0 \le n < d$, where $d = \sum_{j=1}^{A}(\deg(p_j)+1)$, such that $u_n \neq 0$.*

Proof. Let $v_n^{(0)} = u_n$ and $m = \sum_{j=1}^{A}\deg(p_j) = d - A$. We will inductively construct sequences $(v_n^{(0)})_{n\in\mathbb{N}}, \ldots, (v_n^{(m)})_{n\in\mathbb{N}}$ such that for all $0 \le k \le m$ the following hold.

(a) $v_n^{(k)}$ is of the form $\sum_{j=1}^{A} q_j^{(k)}(n)\lambda_j^n$, where each $q_j^{(k)}$ is a non-zero polynomial with algebraic coefficients;

(b) $\sum_{j=1}^{A}\deg(q_j^{(k)}) = d - k$;

(c) For all $n \in \mathbb{N}$, if $v_n^{(k)} \neq 0$ then at least one of $v_n^{(k)}, v_{n+1}^{(k)}$ is non-zero.

Suppose we have already constructed $(v_n^{(k)})_{n\in\mathbb{N}}$ for some $0 \le k < m$. By (b), $\sum_{j=1}^{A}\deg(q_j^{(k)}) = d - k > d - m = A$ and hence there exists $1 \le b \le A$ such that $\deg(q_b^{(k)}) \ge 1$. Consider the sequence

$$v_n^{(k+1)} = v_{n+1}^{(k)} - \lambda_b v_n^{(k)}.$$

Recall that for any polynomial $q \in \mathbb{C}[x]$ and $c \in \mathbb{C}$, the degree of $h(x) \coloneqq q(x+1) - cq(x)$ is equal to $\deg(q) - 1$ if $c = 1$ and $\deg(q)$ otherwise.[3] Hence

$$v_n^{(k+1)} = \sum_{j=1}^{A} \underbrace{\lambda_j\left(q_j^{(k)}(n+1) - \frac{\lambda_b}{\lambda_j}q_j^{(k)}(n)\right)}_{q_j^{(k+1)}(n)}\lambda_j^n$$

where $\deg(q_b^{(k+1)}) = \deg(q_b^{(k)}) - 1$ and $\deg(q_j^{(k+1)}) = \deg(q_j^{(k)})$ for $j \neq b$. In particular, $q_j^{(k+1)}$ is not the zero polynomial for all j. Since $v_n^{(k+1)} = v_{n+1}^{(k)} - \lambda_b v_n^{(k)}$, if $v_n^{(k+1)}$ is non-zero, then either $v_n^{(k)}$ or $v_{n+1}^{(k)}$ is non-zero.

At the end of the inductive construction we will obtain $(v_n^{(m)})_{n\in\mathbb{N}}$ of the form

$$v_n^{(m)} = \sum_{j=1}^{A} c_j\lambda_j^n$$

where each c_j is a non-zero algebraic number, with the property that if $v_n^{(m)}$ is non-zero, then at least one of $u_n, \ldots, u_{n+m}$ is non-zero. It remains to find a non-zero term of $v_n^{(m)}$. Consider the following system of equations

$$\sum_{j=1}^{A} x_i\lambda_j^n = 0 \qquad \text{for } 0 \le n < A$$

[3] By convention, the degree of the zero polynomial is -1.

in unknowns $x_1, \ldots, x_A$. We can write it in the form $Mx = \mathbf{0}$ where $x = (x_1, \ldots, x_A)$ and M is a Vandermonde matrix with $\det(M) = \prod_{j_1 \neq j_2}(\lambda_{j_1} - \lambda_{j_2})$. Since $\lambda_1, \ldots, \lambda_A$ are distinct by assumption, M is invertible and $Mx = 0$ if and only if $x = \mathbf{0}$. Since $c \neq \mathbf{0}$, $Mc \neq \mathbf{0}$. That is, c is not a solution to the system. Hence there exists $0 \leq k < A$ such that $v_k^{(m)} = \sum_{j=1}^{A} c_j \lambda_j^k$ is non-zero. By construction of $(v_n^{(m)})_{n \in \mathbb{N}}$, there exists

$$n \leq k + m < A + m = d$$

such that $u_n \neq 0$. □

Uniqueness of the exponential polynomial representation of a non-trivial linear recurrence sequence can now be proven.

Theorem 2.2.2. *Let $f(n) = \sum_{i \in I} p_i(n)\lambda_i^n$ and $g(n) = \sum_{j \in J} q_j(n)\gamma_j^n$ be two exponential polynomials satisfying $f(n) = g(n)$ for all $n \in \mathbb{N}$. Then $|I| = |J|$ and for each $i \in I$, there exists $j \in J$ satisfying $p_i = q_j$ and $\lambda_i = \gamma_j$.*

Proof. By Lemma 2.2.1, if I is empty, then $f(n)$ is identically zero, and hence J must also be empty. Suppose therefore $|I|, |J| > 0$. Define

$$h(n) \coloneqq f(n) - g(n) = \sum_{i \in I} p_i(n)\lambda_i^n - \sum_{j \in J} q_j(n)\gamma_j^n.$$

Since $h(n) = 0$ for all n, by Lemma 2.2.1 the right-hand side cannot be an exponential polynomial. Since p_i, q_j is non-zero for all i, j, and $\{\lambda_i \mid i \in I\}$ as well as $\{\gamma_j \mid j \in J\}$ are non-zero and pairwise distinct, the only possibility is that there exist $k \in I$ and $m \in J$ such that $\lambda_k = \gamma_m$. Let $I_1 = I \setminus \{k\}$, $J_1 = J \setminus \{m\}$, $\tilde{f}(n) = \sum_{i \in I_1} p_i(n)\gamma_i^n$, and $\tilde{g}(n) = \sum_{j \in J_1} q_j(n)\gamma_j^n$. Observe that both $\tilde{f}(n)$ and $\tilde{g}(n)$ are defined by exponential polynomials.

Our proof is by induction on $|I| + |J|$. In the base case, suppose $|I| = 1$ or $|J| = 1$. W.l.o.g. assume the former. Since $h(n) = f(n) - g(n)$ and $\lambda_k = \gamma_m$,

$$h(n) = p_k(n)\lambda_k^n - (q_m(n)\gamma_m^n + \tilde{g}(n)) = (p_k(n) - q_m(n))\lambda_k^n - \tilde{g}(n).$$

If $p_k(n) - q_m(n)$ is not the zero polynomial, then $(p_k(n) - q_m(n))\lambda_k^n - \tilde{g}(n)$ is an exponential polynomial that contradicts Lemma 2.2.1. Hence $p_k(n) = q_m(n)$ for all n. Since $h(n)$ vanishes by the assumption that $f(n) = g(n)$ for all n, it must be the case that $\tilde{g}(n)$ is also identically zero. From Lemma 2.2.1 it follows that J_1 must be empty. Hence $f(n)$ and $g(n)$ are in fact exactly the same.

In the inductive step, suppose $|I|, |J| > 1$. If $p_k(n) - q_m(n)$ is identically zero, then apply the inductive hypothesis to exponential polynomials $f'(n) \coloneqq \tilde{f}(n)$ and $\tilde{g}(n)$,

observing that $f'(n) = \tilde{g}(n)$ for all $n \in \mathbb{N}$. Otherwise, apply the inductive hypothesis to the exponential polynomials $f'(n) \coloneqq (p_k(n) - q_m(n))\lambda_k^n + \tilde{f}(n)$ and $\tilde{g}(n)$ that satisfy $f'(n) = \tilde{g}(n)$ for all n. Observe that the total number summands across $f'(n)$ and $\tilde{g}(n)$ is either 1 or 2 less than the total number of summands across $f(n)$ and $g(n)$. □

We can use the uniqueness of the exponential polynomial representation to characterise the exponential polynomial representations of LRS over $\mathbb{R}$.

Lemma 2.2.3. *A sequence $u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$, where the right-hand side is an exponential polynomial, satisfies $u_n \in \mathbb{R}$ for all $n \in \mathbb{N}$ if and only if for every $1 \leq i \leq A$ there exists k such that $\lambda_k = \overline{\lambda_i}$ and $p_k(n) = \overline{p_i(n)}$ for all $n \in \mathbb{N}$.*

Proof. The $\Rightarrow$ direction is immediate. To prove the $\Leftarrow$ direction, suppose u_n is real-valued and write $\gamma_j = \overline{\lambda_j}$ for all j. Since $u_n = \overline{u_n}$,

$$\sum_{j=1}^{A} p_j(n)\lambda_j^n = \sum_{j=1}^{A} \overline{p_j(n)}\,\gamma_j^n.$$

By uniqueness, the two exponential polynomials must be the same. □

When working with linear dynamical systems and semialgebraic targets, we will frequently encounter sequences of the form $u_n = p(M^n s)$, where p is a polynomial with rational coefficients. Recall that $u_n^{(i)} = e_i M^n s$ is an LRS for all $1 \leq i \leq d$. Since rational LRS are closed under addition and multiplication, $u_n = p(u_n^{(1)}, \ldots, u_n^{(d)})$ is a rational LRS. In the remainder of this section we study exponential polynomial representations of such sequences. Let $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, $p \in \mathbb{Q}[x_1, \ldots, x_d]$ and $u_n = p(M^n s)$. Write

$$\mathcal{I} = \|M\| + \|s\| + \|p\|.$$

Lemma 2.2.4. *In time $\mathcal{I}^{\textsc{Poly}(d)}$ we can compute*

(i) the non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$ of M,

(ii) integers $A \geq 0$ and $d_j \geq 0$ for $1 \leq j \leq A$,

(iii) non-zero and pairwise distinct $\Lambda_1, \ldots, \Lambda_A \in \overline{\mathbb{Q}}$,

(iv) polynomials $h_1, \ldots, h_A \in \mathbb{Q}[x_1, \ldots, x_m, y]$ such that $h_j(\lambda_1, \ldots, \lambda_m, n)$ is not zero for all n, and

(v) algebraic numbers $\alpha_{j,k}$ for $1 \leq j \leq A$, $0 \leq k \leq d_j$ with $\alpha_{j,d_j} \neq 0$ for all j

such that

$$u_n = \sum_{j=1}^{A} h(\lambda_1, \ldots, \lambda_m, n)\Lambda_j^n = \sum_{j=1}^{A} \sum_{k=0}^{d_j} \alpha_{j,k} n^k \Lambda_j^n$$

for all $n \geq d$.

The reason that the formula for u_n is guaranteed to hold for $n \geq d$ only is that M can have zero as a repeated eigenvalue. For $n \geq d$, however, all zero eigenvalues of M^n have multiplicity one. If $(u_n)_{n\in\mathbb{N}}$ is trivial, then our algorithm will produce $A = 0$.

Proof. First, in polynomial time compute J, P, P^{-1} such that J is in Jordan form and $M = P^{-1}JP$. We can then choose $\lambda_1, \ldots, \lambda_m$ as the non-zero diagonal entries of J. By Theorem 1.7.3, for $n \geq d$ the entries of M^n are of the form $t(\lambda_1, \ldots, \lambda_m, n, \lambda_1^n, \ldots, \lambda_m^n)$, where t is a (non-flat) first-order term of size $\textsc{Poly}(\|M\|)$. Hence

$$u_n = T(\lambda_1, \ldots, \lambda_m, n, \lambda_1^n, \ldots, \lambda_m^n)$$

for $n \geq d$ where $T(z_1, \ldots, z_{2m+1})$ is a (non-flat) term of size $\textsc{Poly}(\mathcal{I})$. Applying Lemma 1.3.4, in time $\mathcal{I}^{\textsc{Poly}(d)}$ we can construct a polynomial with rational coefficients

$$q(z_1, \ldots, z_{2m+1}) = \sum_{i=1}^{B} c_i z_1^{\sigma(i,1)} \cdots z_{2m+1}^{\sigma(i,2m+1)}$$

equivalent to T, where $\sigma(i,k) \in \mathbb{N}$ for all i, k.

Let $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_m)$ and $\Lambda_i = \lambda_1^{\sigma(i,m+1)} \cdots \lambda_d^{\sigma(i,2m+1)}$ for $1 \leq i \leq B$. By the Tower Law, $D = [\mathbb{K} : \mathbb{Q}] < \mathcal{I}^{\textsc{Poly}(d)}$, and hence by Corollary 1.5.8, each Λ_i can be computed in time $\mathcal{I}^{\textsc{Poly}(d)}$. So far we have

$$u_n = \sum_{i=1}^{B} c_i \lambda_1^{\sigma(i,1)} \cdots \lambda_m^{\sigma(i,m)} n^{\sigma(i,m+1)} \Lambda_i^n$$

for $n \geq d$. Collecting summands together, rewrite the right-hand side in the form

$$\sum_{i\in I} \sum_{0\leq k\leq \xi(i)} q_{i,k}(\lambda_1, \ldots, \lambda_m) n^k \Lambda_i^n$$

where $I \subseteq \{1, \ldots, B\}$, each $q_{i,k}$ is a polynomial with rational coefficients, $\{\Lambda_i \mid i \in I\}$ are non-zero and pairwise distinct, and $\xi(i) \in \mathbb{N}$ for all i. For each i, k, we can compute the algebraic number $q_{i,k}(\lambda_1, \ldots, \lambda_m)$ (and check whether it is zero) in time $\mathcal{I}^{\textsc{Poly}(d)}$ using Corollary 1.5.8. Hence we can express

$$\begin{aligned} u_n &= \sum_{i\in J} \sum_{k=0}^{d_i} \alpha_{i,k} n^k \Lambda_i^n \\ &= \sum_{i\in J} h_i(\lambda_1, \ldots, \lambda_m, n)\Lambda_i^n \end{aligned}$$

where $J \subseteq I$, $\{\Lambda_i \mid i \in J\}$ are non-zero and pairwise distinct, and for all i, $d_i \geq 0$, $\alpha_{i,d_i} \neq 0$, and $h_i(\lambda_1, \ldots, \lambda_m, n)$ is not the zero polynomial in n. It remains to take $A = |J|$ and rename the indices $i \in J$ to $j \in \{1, \ldots, A\}$. □

If M is diagonalisable, then we can give a specialised version of Lemma 2.2.4.

Lemma 2.2.5. *If M is diagonalisable, then in time $\mathcal{I}^{\text{POLY}(d)}$ we can compute the non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$ of M, an integer $A \geq 0$, non-zero and pairwise distinct $\Lambda_1, \ldots, \Lambda_A \in \overline{\mathbb{Q}}$, polynomials $h_1, \ldots, h_A \in \mathbb{Q}[x_1, \ldots, x_m]$ and non-zero $c_1, \ldots, c_A \in \overline{\mathbb{Q}}$ such that*

(a) $c_j = h_j(\lambda_1, \ldots, \lambda_m)$ for all j, and

(b) $u_n = \sum_{j=1}^{A} c_j \Lambda_j^n$ for all n.

Proof. Computing the Jordan form of M and the non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$, and invoking Theorem 1.7.3, we have that for all $n \in \mathbb{N}$,

$$u_n = T(\lambda_1, \ldots, \lambda_m, \lambda_1^n, \ldots, \lambda_m^n)$$

where $T(z_1, \ldots, z_{2m})$ is a (non-flat) term computed in polynomial time. Proceeding similarly to the proof of Lemma 2.2.4, in time $\mathcal{I}^{\text{POLY}(d)}$ we can write

$$u_n = \sum_{i \in I} h_i(\lambda_1, \ldots, \lambda_m) \Lambda_i^n$$

where each $h_i \in \mathbb{Q}[x_1, \ldots, x_m]$ and $\{\Lambda_i \mid i \in I\}$ are non-zero and pairwise distinct. Let $c_i = h_i(\lambda_1, \ldots, \lambda_m)$, which can be computed and compared against zero using Corollary 1.5.8. After discarding zero summands and renaming variables, we obtain $u_n = \sum_{j=1}^{A} c_j \Lambda_j^n$ as required. □

2.3 Zeros of linear recurrence sequences

We now discuss zero terms of linear recurrence sequences and the related Skolem Problem in detail. The most fundamental result about the distribution of zeros in a linear recurrence sequence is the Skolem-Mahler-Lech theorem, proven by Skolem [76] and and generalised by Mahler [56] and Lech [52]. The version we need (due to Mahler, see [40] for an elementary proof) states that for any LRS $(u_n)_{n \in \mathbb{N}}$ over $\overline{\mathbb{Q}}$, the set $Z = \{n \colon u_n = 0\}$ is of the form

$$F \cup (a_1 + b_1\mathbb{N}) \cup \ldots \cup (a_m + b_m\mathbb{N}) \tag{2.2}$$

where $F \subset \mathbb{N}$ is a finite set and $a_i, b_i \in \mathbb{N}$ with $0 \leq a_i < b_i$ for all $1 \leq i \leq m$. That is, Z is a union of a finite set and finitely many arithmetic progressions. Berstel and Mignotte have shown in [13] that if $(u_n)_{n\in\mathbb{N}}$ is non-degenerate, then Z is in fact finite. All known proofs of the Skolem-Mahler-Lech theorem rely on p-adic analysis and are not fully effective: From the proofs we can extract an algorithm to compute m and a_i, b_i for $1 \leq i \leq m$, but no algorithm is known for computing all elements of F or even determining if it is empty. Hence in contrast to checking whether a given LRS has a zero (which is exactly the Skolem Problem), whether it has infinitely many zeros can be easily determined by computing m and comparing it to zero.

The Skolem Problem for LRS over $R \subseteq \overline{\mathbb{Q}}$ is equivalent to the problem of determining all zeros of a given LRS over R. To see this, suppose we have access to a Skolem oracle that, given such an LRS, decides whether it has a zero. Let $(u_n)_{n\in\mathbb{N}}$ be an LRS over R and suppose we have already computed a_i, b_i for $1 \leq i \leq m$ as in 2.2. To determine all zeros of $(u_n)_{n\in\mathbb{N}}$, it remains to compute all elements of F. By taking sub-progressions of $a_1 + b_1\mathbb{N}, \ldots, a_m + b_m\mathbb{N}$ if necessary, we can assume that $b_1 = \ldots = b_m$. Take $b \coloneqq b_1$ subsequences of $(u_n)_{n\in\mathbb{N}}$ to obtain the sequences $u_n^{(r)} = u_{r+bn}$ for $0 \leq r < b$. It suffices to determine all zeros of each $(u_n^{(r)})_{n\in\mathbb{N}}$. Recall that $0 \leq a_i < b_i$ for all $1 \leq i \leq m$.

(a) If $r = a_i$ for some i, then $u_n^{(r)} = 0$ for all n.

(b) If $r \neq a_i$ for all i, then $u_n^{(r)}$ has only finitely many zeros. To determine all zeros of $(u_n^{(r)})_{n\in\mathbb{N}}$, first invoke the Skolem oracle to establish if $(u_n^{(r)})_{n\in\mathbb{N}}$ has a zero at all. If no, then terminate. If yes, then by checking sufficiently many initial terms of $(u_n^{(r)})_{n\in\mathbb{N}}$ find the smallest k such that $u_k^{(r)} = 0$. Construct the sequence $(u_{n+k+1})_{n\in\mathbb{N}}$ and apply the steps above until termination.

Therefore, **proving decidability of the Skolem Problem amounts to giving a fully effective version of the Skolem-Mahler-Lech theorem.**

We can apply the Skolem-Mahler-Lech theorem to the Reachability Problem where the target $T \subseteq \mathbb{R}^d$ is *algebraic*, i.e. defined by a Boolean combination of polynomial equalities with rational coefficients. Recall from Section 1.4 that by the squaring trick, such T can be defined by a single equation $p(x_1, \ldots, x_d) = 0$ where $p \in \mathbb{Q}[x_1, \ldots, x_d]$. For such T, $M^n s \in T$ if and only $p(M^n s) = 0$. Since $u_n = p(M^n s)$ is an LRS, the reachability set $\{n \colon M^n s \in T\}$ is of the form 2.2. Therefore, the characteristic word $\alpha \in \left(2^{\mathcal{T}}\right)^\omega$ of (M, s) with respect to a family of algebraic sets $\mathcal{T}$ is of the form uv^ω (i.e. ultimately periodic), with the caveat that we do not known how to effectively compute u due to the ineffectiveness of the Skolem-Mahler-Lech theorem. It is not

difficult to see that with an oracle for the Skolem Problem, we can compute u effectively and decide the full Model-Checking Problem for algebraic targets; see [54] for a proof.

We now give an overview of what is known about the Skolem Problem. Somewhat surprisingly, the Skolem Problem for LRS over $\overline{\mathbb{Q}}$ can be reduced to the Skolem Problem for LRS over $\mathbb{Q}$. Given an LRS $u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$ over $\overline{\mathbb{Q}}$, let $\mathbb{K}$ be a number field of finite degree enclosing $\lambda_1, \ldots, \lambda_A$ such that $\mathbb{K}/\mathbb{Q}$ is a Galois extension and $p_j \in \mathbb{K}[x]$ for all j. Recall that for any $\alpha \in \mathbb{K}$, the field norm is defined as

$$N_{\mathbb{K}}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})} \sigma(\alpha)$$

where $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ denotes the Galois group of the extension $\mathbb{K}/\mathbb{Q}$. The field norm has the properties that $N_{\mathbb{K}}(\alpha) \in \mathbb{Q}$ and $N_{\mathbb{K}}(\alpha) = 0 \Leftrightarrow \alpha = 0$ for all $\alpha \in \mathbb{K}$. We consider the sequence

$$v_n = N_{\mathbb{K}}(u_n) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})} \sum_{j=1}^{A} q_{\sigma,j}(n)\sigma(\lambda_j)^n$$

where $q_{\sigma,j} \in \mathbb{K}[x]$ is the polynomial satisfying $q_{\sigma,j}(n) = \sigma(q_j(n))$ for all n. By closure of linear recurrence sequences over $\overline{\mathbb{Q}}$ under multiplication, $(v_n)_{n\in\mathbb{N}}$ is an LRS over $\overline{\mathbb{Q}}$. Since $v_n \in \mathbb{Q}$ for all n, $(v_n)_{n\in\mathbb{N}}$ is also an LRS over $\mathbb{Q}$.[4] Moreover, $v_n = 0$ if and only if $N_{\mathbb{K}}(u_n) = 0$, which is equivalent to $u_n = 0$. Hence $(u_n)_{n\in\mathbb{N}}$ has a zero if and only if $(v_n)_{n\in\mathbb{N}}$ has a zero.

Known decidable subclasses of the Skolem Problem are due to Mignotte, Shorey, Tijdeman [61] and, independently, Vereschagin [78]. They showed the Skolem Problem is decidable

(A) for sequences over $\overline{\mathbb{Q}}$ with at most 3 dominant roots, and

(B) for sequences over $\mathbb{R} \cap \overline{\mathbb{Q}}$ of order at most 4.

By (A), the Skolem Problem is decidable for LRS over $\overline{\mathbb{Q}}$ of order at most 3. For LRS over $\mathbb{Q}$ (and hence over $\mathbb{R} \cap \overline{\mathbb{Q}}$ as well), the Skolem Problem is open for sequences of order 5 or more. However, there have been recent breakthroughs in the form of *conditional decidability* results, which we discuss next.

As shown in [65], the only open case of the Skolem Problem over $\mathbb{Q}$ at order 5 comprises diagonalisable sequences $(u_n)_{n\in\mathbb{N}}$ with 4 non-real dominant roots. That is, $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + b\gamma^n + \overline{b}\,\overline{\gamma^n} + c\rho^n$ where $c, \rho \in \mathbb{R}$ and $|\lambda| = |\gamma| > |\rho|$. Recently, Bilu et al. [16] proved decidability of the Skolem Problem for diagonalisable LRS assuming the Exponential Local-Global Principle and the p-adic version of Schanuel's

[4] This is a consequence of the Fatou Lemma; see the introduction to this chapter.

conjecture, two well-known conjectures in number theory. Their algorithm relies on the two conjectures only for termination: it can be proven unconditionally that whenever the algorithm terminates, it either produces n such that $u_n = 0$, or a verifiable certificate attesting that $u_n \neq 0$ for all $n \in \mathbb{N}$. In the latter case, the certificate consists of

(i) a partition of the input LRS $(u_n)_{n\in\mathbb{N}}$ into non-degenerate sequences $u_n^{(r)} = u_{nL+r}$ for $0 \leq r < L$, and

(ii) for each r, integers $m, k > 0$ such that $v_n = k^n u_n^{(r)}$ is an LRS over $\mathbb{Z}$ that is non-zero modulo m.

The algorithm of Bilu et al. has been implemented [1], and the Skolem Problem for diagonalisable LRS as well as LRS of order at most 5 is considered by some to be "solved in practice".

On the quantitative side, Chonev et al. [26, Theorem C.1] gave the following bounds on the largest zero of a non-degenerate sequence.

Theorem 2.3.1. *Let $u_{n+d} = \sum_{i=0}^{d-1} a_i u_{n+i}$ be a non-degenerate LRS over $\overline{\mathbb{Q}}$ with $d \leq 4$. Write $\mathcal{I} = \sum_{i=0}^{d-1} \|a_i\| + \|u_i\|$. If $d \leq 3$, or $a_i, u_i \in \mathbb{R} \cap \overline{\mathbb{Q}}$ for $0 \leq i < d$, then there exists effectively computable $N < 2^{\text{POLY}(\mathcal{I})}$ such that $u_n \neq 0$ for all $n \geq N$.*

This result can be seen as an effective Skolem-Mahler-Lech theorem for a class of low-order linear recurrence sequences. In Section 2.7 we will give new, effective bounds on the largest zero of LRS of the form $u_n = p(\lambda_1^n, \lambda_2^n)$ and $u_n = p(n, \lambda^n)$, where p is a polynomial. Note that these classes of sequences lie beyond (A) and (B) as neither their order nor the number of dominant roots is bounded by an absolute constant.

2.4 Bounds on rates of growth

Lower and upper bounds on the growth rate of $|u_n|$ for a linear recurrence sequence $(u_n)_{n\in\mathbb{N}}$ form the foundation of many decision procedures of LRS as well as LDS. We first discuss the (exponential) upper bounds, which are easy to obtain.

Lemma 2.4.1. *Let $(u_n)_{n\in\mathbb{N}}$ be given by*

$$u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$$

where λ_j is non-zero and algebraic and $p_j(x) = \sum_{i=0}^{\deg(p_j)} \alpha_{j,i}x^i \in \overline{\mathbb{Q}}[x]$ for all j. Write $d = \max_{1\leq j\leq A} \deg(p_j)$, $\rho = \max_{1\leq j\leq A} |\lambda_j|$, and

$$\mathcal{I} = \sum_{j=1}^{A}\Big(\|\lambda_j\| + \sum_{i=0}^{\deg(p_j)} \|\alpha_{j,i}\|\Big).$$

In time $\textsc{Poly}(\mathcal{I})$ we compute an integer K such that for all $n \geq 1$, $|u_n| < K\rho^n n^d$.

Proof. For $1 \leq j \leq A$, let $r_j = \max_i |\alpha_{j,i}|$ if $\alpha_{j,i} \neq 0$ for some i, and $r_j = 0$ otherwise. By Lemma 1.5.10, we can compute r_j for $1 \leq j \leq A$ in time polynomial in $\mathcal{I}$. We have $|p_j(n)\lambda_j^n| \leq (d+1)r_j n^d \rho^n$ for all j and $n \geq 1$. It remains to compute $K_j = (d+1)r_j$ for $1 \leq j \leq A$ and $K = K_1 + \ldots + K_A + 1$. Applying the triangle inequality, $|u_n| \leq \sum_{j=1}^{A} \left|p_j(n)\lambda_j^n\right| < K\rho^n n^d$. □

Establishing lower bounds on the growth of linear recurrence sequences, in comparison, is much harder. The following theorem, alongside the Skolem-Mahler-Lech theorem, is one of the most fundamental results about LRS. It is derived from Evertse's lower bound [36] on the sums of S-units; see [45, Theorem 11] for a proof.

Theorem 2.4.2. *Let $(u_n)_{n\in\mathbb{N}}$ be a non-degenerate LRS given by $u_n = \sum_{j=1}^{A} p_j(n)\lambda_j^n$, where $A > 0$, $p_1, \ldots, p_A \in \overline{\mathbb{Q}}[x]$ are not identically zero, and $\lambda_1, \ldots, \lambda_A \in \overline{\mathbb{Q}}$ are non-zero and pairwise distinct. Further let $\rho = \max_{1\leq i\leq m} |\lambda_i|$. For every $0 < r < \rho$ there exists N such that for all $n \geq N$, $|u_n| > r^n$.*

The value N above is not known to be effectively computable given the description of $(u_n)_{n\in\mathbb{N}}$. One consequence of this is that the Ultimate Positivity Problem is known to be decidable [67] for diagonalisable sequences, whereas the Positivity Problem is open for diagonalisable sequences of order 10 or more [67]. In the following section, we will discuss both problems in more detail.

We next give two straightforward results about growth rates that we will use extensively. First a bound on how long it takes for an exponential to overtake a polynomial.

Lemma 2.4.3. *Let $f(t) = C_1/t^k$ and $g(t) = C_2\rho^t$ where $\rho \in (0,1) \cap \overline{\mathbb{Q}}$, $k \in \mathbb{N}$, and C_1, C_2 are positive rationals. There exists a positive integer*

$$N < \textsc{Poly}(k, \log C_1, \log C_2, 1/(1-\rho))$$

computable in time $\textsc{Poly}(\|k\|, \|C_1\|, \|C_2\|, \|\rho\|)$ *such that* $f(t) > g(t)$ *holds for all* $t \in [N, \infty)$.

Proof. For all $t > 0$, $\log t < \sqrt{t}$ for $t > 0$ and hence

$$\begin{aligned} C_1/t^k > C_2\rho^t &\Leftrightarrow \log\frac{C_1}{C_2} > k\log t + t\log\rho \\ &\Leftarrow \log\frac{C_1}{C_2} > k\sqrt{t} + t\log\rho. \end{aligned}$$

We view the latter as a quadratic inequality in $\sqrt{t}$ which is satisfied for sufficiently large t as $\log\rho < 0$. Let $D = k^2 + 4\log\rho\log\frac{C_1}{C_2}$. If $D \leq 0$, then the quadratic inequality is satisfied for all $t > 0$ and we can choose $N = 0$. Otherwise, by the quadratic formula we can choose N to be any integer at least

$$\frac{-k-\sqrt{D}}{2\log\rho} = \frac{k+\sqrt{D}}{2\log 1/\rho} < \frac{k+1+D}{2\log 1/\rho} = \frac{1+k+k^2}{2\log 1/\rho} - 2\log\frac{C_2}{C_1}.$$

Since $\log 1/\rho \geq 1-\rho$ for all $\rho > 0$, it suffices to choose N to be any integer at least

$$\frac{1+k+k^2}{2(1-\rho)} - 2\log C_2 + 2\log C_1.$$

It remains to show how to compute N within the required time bound. By Corollary 1.5.8, we can compute the real algebraic number $\alpha \coloneqq \frac{1+k+k^2}{2(1-\rho)} > 0$ in time $\textsc{Poly}(\|\rho\|, \|k\|)$. Thereafter, an upper bound on α can be computed in time $\textsc{Poly}(\|\alpha\|)$ using Theorem 1.2.4. Finally, upper and lower bounds on $\log C_i$ for $i \in \{1, 2\}$ can be computed in polynomial time in $\|C_i\|$ as follows. First compute bounds on $\log_2 C_i$ using the binary representation of C_i. Then estimate $\log C_i$ as $\log 2 \cdot \log_2 C_i$. □

For linear recurrence sequences $(u_n)_{n\in\mathbb{N}}$ with only real eigenvalues, the asymptotic behaviour as well as the sign pattern are completely well-understood. Intuitively, for such sequences, for sufficiently large n, the nth powers of the dominant eigenvalues (of which there is at most two) completely determine the sign of u_n. Hence the sign pattern of $(u_n)_{n\in\mathbb{N}}$ is ultimately periodic with period either one or two. Possible sign patterns of such LRS are illustrated by the LRS $u_n = -3^n + 2^n$, $v_n = (-3)^n + 2^n$, and $w_n = 3^n + (-3)^n - 2^n$. The next result is about sign patterns of sequences with only positive eigenvalues, stated in continuous terms with a view towards later chapters.

Lemma 2.4.4. *Let* $r_1, \ldots, r_A \in \mathbb{R} \cap \overline{\mathbb{Q}}$ *be positive and pairwise distinct, and for* $1 \leq j \leq A$, *let* $p_j(x) = \sum_{i=0}^{\deg(p_j)} \alpha_{j,i}x^i \in (\mathbb{R} \cap \overline{\mathbb{Q}})[x]$ *be non-zero. Write*

$$\mathcal{I} = \sum_{j=1}^{A}\Big(\|r_j\| + \sum_{i=0}^{\deg(p_j)} \|\alpha_{j,i}\|\Big)$$

and consider

$$f(t) \coloneqq \sum_{j=1}^{A} p_j(t) r_j^t.$$

In time $\textsc{Poly}(\mathcal{I})$*, we can compute an integer* $N < 2^{\textsc{Poly}(\mathcal{I})}$ *and* $\Delta \in \{>, =, <\}$ *such that* $f(t)\ \Delta\ 0$ *for all* $t \in [N, \infty)$*.*

Proof. If $A = 0$, then the sequence is identically zero. Suppose therefore $A > 0$. By Lemma 1.5.10, we can compute $|r_1|, \ldots, |r_A|$ in polynomial time. Since $r_1, \ldots, r_A$ are positive and pairwise distinct, w.l.o.g. we can assume that $r_1 > \ldots > r_A$. Consider

$$g(t) \coloneqq \sum_{j=2}^{A} p_j(t) r_j^t.$$

By Lemma 1.2.5, in time $\textsc{Poly}(\mathcal{I})$ we can compute integers $K_1, N_1 < 2^{\textsc{Poly}(\mathcal{I})}$ such that

$$|p_1(t)| > 1/K_1$$

for all $t \in [N_1, \infty)$. Next, let $d = \max_{2 \leq j \leq A} \deg(p_j)$. Repeating the arguments of Lemma 2.4.1, in time $\textsc{Poly}(\mathcal{I})$ we can compute $K_2 \in \mathbb{N}$ such that $|g(t)| < K_2 t^d r_2^t$ for all $t \geq 1$. By Lemma 1.5.7, we can compute $r_2/r_1 \in \mathbb{R} \cap \overline{\mathbb{Q}}$ in time $\textsc{Poly}(\mathcal{I})$. Applying Lemma 2.4.3, in time $\textsc{Poly}(\mathcal{I})$ we can compute $N < 2^{\textsc{Poly}(\mathcal{I})}$ such that for $t \geq N$, $1 > K_1 K_2 t^d (r_2/r_1)^t$ and hence $|p_1(t) r_1^t| > |g(t)|$. Therefore, for $t \geq N$ it holds that $\operatorname{sign}(f(t)) = \operatorname{sign}(p_1(t) r_1^t)$. □

2.5 Positivity and related problems

Having discussed the Skolem Problem and zero terms of linear recurrence sequences, we move onto decision problems about the full sign pattern $\sigma \in \{+, 0, -\}^\omega$ of LRS. Recall that the Positivity Problem for LRS over $\mathbb{Q}$ is to decide, given such $(u_n)_{n \in \mathbb{N}}$, whether $u_n \geq 0$ for all $n \in \mathbb{N}$. It is trivially equivalent to deciding whether $u_n < 0$ for some n, which is an instance of the Reachability Problem with halfspace targets as discussed in Section 2.1. Similarly, the Ultimate Positivity Problem, which is to decide if $u_n \geq 0$ for all sufficiently large values of n, is equivalent to deciding whether $u_n < 0$ for infinitely many n. Note that since $u_n < 0 \Leftrightarrow -u_n > 0$, we can choose either of the strict inequality symbols.

We can reduce the Skolem Problem for sequences over $\overline{\mathbb{Q}}$ to the Positivity Problem for LRS over $\mathbb{Q}$. Given an LRS $(u_n)_{n \in \mathbb{N}}$ over $\overline{\mathbb{Q}}$, let $(v_n)_{n \in \mathbb{N}}$ be the LRS over $\mathbb{Q}$ constructed in Section 2.3 such that for all n, $u_n = 0 \Leftrightarrow v_n = 0$. Write $v_n = c^\top M^n s$, and let $r \in \mathbb{N}_{>0}$ be such that $w_n \coloneqq r^n v_n \in \mathbb{Z}$ for all n. We have $u_n = 0 \Leftrightarrow w_n = 0$.

Hence $(u_n)_{n\in\mathbb{N}}$ does not have a zero term if and only if the integer LRS $z_n = w_n^2 - 1$ satisfies $z_n \geq 0$ for all $n \in \mathbb{N}$.

More surprisingly, Positivity Problem for LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ can be reduced to the Positivity Problem for rational sequences; see [45] for a proof. The reduction additionally preserves diagonalisability.

The Positivity Problem and the Ultimate Positivity Problem are known to decidable for linear recurrence sequences over $\mathbb{Q}$ of order at most 5, whereas at order 6, both problems become hard with respect to certain open problems in Diophantine approximation [66]. We will discuss the issues surrounding *Diophantine hardness* in Chapter 8. For diagonalisable sequences, the Ultimate Positivity Problem is known to be decidable [68], whereas the Positivity Problem is known to be decidable only for sequences of order 9 or less [67]. As described in [67], at order 10 the open cases of the latter problem comprise the sequences $(u_n)_{n\in\mathbb{N}}$ with the following properties.

(a) $u_n = a\mu^n + b\rho^n + \sum_{i=1}^{4} c_i\lambda_i^n + \overline{c_i}\,\overline{\lambda_i^n}$ with $\mu, \rho \in \mathbb{R}$ and $|\rho| = |\lambda_1| = \cdots = |\lambda_4| > |\mu|$.

(b) There exist multiplicatively independent $\alpha, \beta \in \mathbb{C}$ such that for every λ_i, there exist k, m such that $\lambda_i = \alpha^k\beta^m$.

That is, at order 10 all hard cases of the Positivity Problem for diagonalisable sequences have 9 dominant roots, exactly one of which (i.e. ρ) is real, and the *group of multiplicative relations* of the dominant non-real eigenvalues $\lambda_1, \overline{\lambda_1}, \ldots, \lambda_4, \overline{\lambda_4}$ has rank exactly 2.

We conclude this section by showing how to decide the Ultimate Positivity Problem for diagonalisable and non-degenerate linear recurrence sequences over $\mathbb{R} \cap \overline{\mathbb{Q}}$.[5] Let $(u_n)_{n\in\mathbb{N}}$ be such an LRS with the exponential polynomial representation $u_n = \sum_{j=1}^{A} c_j\lambda_j^n$. We have to determine whether $u_n \geq 0$ for all sufficiently large n. The algorithm relies on the lower bound of Theorem 2.4.2. Let $\rho = \max_j |\lambda_j|$, $\mathcal{D} = \{j : |\lambda_j| = \rho\}$, $d_n = \sum_{j\in\mathcal{D}} c_j\lambda_j^n$, and $r_n = \sum_{j\notin\mathcal{D}} c_j\lambda_j^n$. Observe that $u_n = d_n + r_n$, and $(d_n)_{n\in\mathbb{N}}$ itself is a non-degenerate LRS. Due to the presence of conjugates in $\mathcal{D}$, $(d_n)_{n\in\mathbb{N}}$ is real-valued. Recall from Section 2.3 that a non-degenerate LRS has only finitely many zeros. Hence there exists N_1 such that for all $n \geq N_1$, $d_n \neq 0$. By Theorem 2.4.2, therefore, there exists $N_2 \geq N_1$ such that $|d_n| > |r_n|$ for all $n \geq N_2$. Hence it suffices to check whether $d_n \geq 0$ for sufficiently large n. Consider $w_n = d_n/\rho^n = \sum_{i=1}^{|\mathcal{D}|} c_i\gamma_i^n$, where each γ_i is equal to λ_j/ρ for some $j \in \mathcal{D}$. The sign of w_n is the same as the sign of d_n for all n. Using Kronecker's theorem in Diophantine approximation, we will

[5] For diagonalisable but degenerate sequences, the Ultimate Positivity Problem can be decided by taking non-degenerate subsequences and applying our decision procedure to each subsequence.

show in Section 4.1 that the closure $\mathbb{T}_\Gamma$ of $\{(\gamma_1^n, \ldots, \gamma_d^n) \mid n \in \mathbb{N}\}$ is semialgebraic and effectively computable. Moreover, $((\gamma_1^n, \ldots, \gamma_d^n))_{n\in\mathbb{N}}$ visits every open subset of $\mathbb{T}_\Gamma$ infinitely often. Therefore,

$$\begin{aligned} w_n \geq 0 \text{ for sufficiently large } n &\Leftrightarrow w_n \geq 0 \text{ for all } n \\ &\Leftrightarrow \sum_{i=1}^{d} c_i z_i \geq 0 \text{ for all } (z_1, \ldots, z_d) \in \mathbb{T}_\Gamma. \end{aligned}$$

The last condition can be verified using tools from semialgebraic geometry and first-order logic (Section 1.3).

2.6 Baker's theorem and its applications

A *linear form in logarithms* is an expression of the form $\Lambda = b_1 \operatorname{Log} \alpha_1 + \ldots + b_m \operatorname{Log} \alpha_m$ where $b_i \in \mathbb{Z}$ and $\alpha_i \in \overline{\mathbb{Q}}$ is non-zero for all $1 \leq i \leq m$. The celebrated theorem of Baker places a lower bound on $|\Lambda|$ in case $\Lambda \neq 0$. Baker's theorem and its p-adic analogue play a critical role in the proofs of decidability of the Skolem Problem [61, 78] and the Positivity Problem [66, 67] for low-order linear recurrence sequences. They will also be our main tool in Section 2.7. The version of Baker's theorem given below is a special case of the main theorem in [81]. Recall from Section 1.5 that $H(\alpha)$ and $h(\alpha)$ respectively denote the naive height and the absolute logarithmic Weil height of an algebraic number α.

Theorem 2.6.1. *Let $\Lambda = b_1 \operatorname{Log} \alpha_1 + \ldots + b_m \operatorname{Log} \alpha_m$ be a linear form in logarithms, $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_m) : \mathbb{Q}]$, and suppose $A, B \geq 3$ are such that $A \geq H(\alpha_i)$ and $B \geq |b_i|$ for all $1 \leq i \leq m$. If $\Lambda \neq 0$, then*

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

A direct consequence of Baker's theorem is the following [67, Corollary 8].

Lemma 2.6.2. *Let $\alpha \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and $\beta \in \overline{\mathbb{Q}}$. For all $n \geq 2$, if $\alpha^n \neq \beta$ then*

$$|\alpha^n - \beta| > n^{-\textsc{Poly}(\|\alpha\| + \|\beta\|)}.$$

This result already suffices for proving decidability of the Skolem Problem for real algebraic LRS of order at most three [26]. We can also place a bound on $|\alpha^n - \beta|$ that applies to all integers n.

Lemma 2.6.3. *Let $\alpha \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and $\beta \in \overline{\mathbb{Q}}$. For all $n \in \mathbb{Z}$, if $\alpha^n \neq \beta$ then*

$$|\alpha^n - \beta| > (\max\{2, |n|\})^{-\textsc{Poly}(\|\alpha\| + \|\beta\|)}.$$

Proof. Recall from Section 1.5.4 that, given α, we can compute a canonical representation of $\delta \coloneqq 1/\alpha$ satisfying $\|\delta\| < \textsc{Poly}(\|\alpha\|)$. Hence by Lemma 2.6.2, for $n \geq 2$, $|\alpha^n - \beta|, |\alpha^{-n} - \beta| < n^{-\textsc{Poly}(\|\alpha\|+\|\beta\|)}$. On the other hand, applying Lemma 1.5.1, $|\alpha - \beta|, |1 - \beta|, |1/\alpha - \beta| > 2^{-\textsc{Poly}(\|\alpha\|+\|\beta\|)}$. □

Next, we show how to use Baker's theorem to place a lower bound on $|u_n|$ for $u_n = p(\gamma^n)$, where $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and $p \in \overline{\mathbb{Q}}[x]$. The idea is to factorise $p(\gamma^n)$ and apply Lemma 2.6.2 to each linear factor.

Lemma 2.6.4. *Let $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$, $\lambda_1, \ldots, \lambda_m \in \overline{\mathbb{Q}}$, and*

$$p(x) = \sum_{j=0}^{B} h_j(\lambda_1, \ldots, \lambda_m) x^j \in \overline{\mathbb{Q}}[x]$$

where $h_j \in \mathbb{Q}[x_1, \ldots, x_m]$ for all j. Suppose γ is not a root of unity and p is not the zero polynomial. Write $\mathcal{I} \coloneqq \|\gamma\| + \sum_{j=0}^{B} \|h_j\| + \sum_{i=1}^{m} \|\lambda_i\|$. There exist integers $N, C < \mathcal{I}^{\textsc{Poly}(m)}$ computable in time $\mathcal{I}^{\textsc{Poly}(m)}$ such that for all $n \geq N$, $|p(\gamma^n)| > n^{-C}$.

Proof. Applying Lemma 1.5.9, in time $\mathcal{I}^{\textsc{Poly}(m)}$ we can factorise

$$p(x) = \beta_0(x - \beta_1) \cdots (x - \beta_k)$$

where $\beta_0, \ldots, \beta_k$ are algebraic and $\beta_0 \neq 0$ by the assumption that p is not identically zero. Since γ is not a root of unity, by Lemma 1.5.2 there exists an integer $N < \mathcal{I}^{\textsc{Poly}(m)}$ computable in polynomial time from $\gamma, \beta_1, \ldots, \beta_k$ such that for all $n \geq N$ and $1 \leq i \leq k$, $\gamma^n - \beta_i \neq 0$. By Lemma 2.6.2, for all $n \geq N$ and $1 \leq i \leq k$, $|\gamma^n - \beta_i| > n^{-\mathcal{I}^{\textsc{Poly}(m)}}$. Since $|\beta_0| > 2^{-\mathcal{I}^{\textsc{Poly}(m)}}$ (e.g. by Lemma 1.5.1), for all $n \geq N$

$$|p(\gamma^n)| = |\beta_0| \prod_{i=1}^{k} |\gamma^n - \beta_i| > n^{-\mathcal{I}^{\textsc{Poly}(m)}} = n^{-C}.$$

It remains to observe that C can be computed in time $\mathcal{I}^{\textsc{Poly}(m)}$. □

The following is the p-adic analogue of Baker's theorem due to Yu [82]. Alongside Theorem 2.6.1, it is crucial to the proof of decidability of the Skolem Problem for linear recurrence sequences over $\mathbb{Q}$ of order 4. See Section 1.5.2 for relevant definitions.

Theorem 2.6.5. *Let $\alpha_1, \ldots, \alpha_m$ be non-zero algebraic numbers, $b_1, \ldots, b_m \in \mathbb{Z}$, and $\Xi \coloneqq \alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1$. Further let $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, $D = [\mathbb{K} : \mathbb{Q}]$, $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ lying over a rational prime $p \in \mathbb{N}$, $B \geq 3$ be an upper bound on $b_1, \ldots, b_m$, and $h = \max\{h(\alpha_1), \ldots, h(\alpha_m), \log p\}$. If $\Xi \neq 1$, then*

$$v_{\mathfrak{p}}(\Xi) < 19(20\sqrt{m+1}D)^{2(m+1)} e_{\mathfrak{p}}^{m-1} \cdot \frac{N(\mathfrak{p})}{(f_{\mathfrak{p}} \operatorname{Log} p)^2} \cdot h^m \log(e_{\mathfrak{p}}^5 mD) \log B.$$

To see that Theorem 2.6.5 is really analogous to Baker's theorem, recall that the latter establishes a lower bound on $|\Lambda|$ for $\Lambda = b_1 \operatorname{Log} \alpha_1 + \ldots + b_m \operatorname{Log} \alpha_m$ of the form $e^{-f(m,D,A,B)}$ when $\Lambda \neq 0$. Consider $e^{\Lambda} = \alpha_1^{b_1} \cdots \alpha_m^{b_m}$. We have that $|e^{\Lambda}| = |\alpha_1^{\beta_1} \cdots \alpha_m^{b_m}|$ is bounded below by $e^{e^{-f(m,D,A,B)}}$, which itself is greater than 1. Hence we can view Theorem 2.6.1 as stating a lower bound on the Euclidean norm $|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1|$. On the other hand, Theorem 2.6.5 can be equivalently stated as a lower bound on the $\mathfrak{p}$-adic norm $|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1|_{\mathfrak{p}}$. We will use the p-adic version of Baker's theorem in the next section through the following lemma.

Lemma 2.6.6. *Let $\mathbb{K}$ be a number field, $D = [\mathbb{K} : \mathbb{Q}]$, $\lambda, \alpha \in \mathbb{K}$ be non-zero, and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$. Write $\mathcal{I} = \|\alpha\| + \|\lambda\|$. For $n \in \mathbb{N}$, if $\alpha\lambda^n \neq 0$ then*

$$v_{\mathfrak{p}}(\alpha\lambda^n - 1) < \mathcal{I}^{\textsc{Poly}(D)} \log n.$$

Proof. We invoke Theorem 2.6.5 with $m = 2$, $\alpha_1 = \alpha, \alpha_2 = \lambda, b_1 = 1$ and $b_2 = n$. It remains to recall that $h(\alpha) \leq \|\alpha\|$, $h(\lambda) \leq \|\lambda\|$ (Section 1.5.1), and $f_{\mathfrak{p}}, e_{\mathfrak{p}} \leq D$, $N(\mathfrak{p}) \leq \|\lambda\|^D$ (Section 1.5.2). □

2.7 Effective Skolem-Mahler-Lech theorems

We now show how to compute, for non-degenerate linear recurrence sequences of the form $u_n = p(\lambda_1^n, \lambda_2^n)$ and $u_n = p(n, \lambda^n)$, effective bounds on the finitely many zero terms. Such sequences arise when we analyse semialgebraic targets of dimension one in Chapter 6. As they can have arbitrarily high order and number of dominant roots, they lie outside the scope of decidability results of [61, 78] discussed in Section 2.3. Our main tools are Baker's theorem, its p-adic analogue, and the Weil height.

For $p \in \overline{\mathbb{Q}}[z_1, z_2]$ of the form $\sum_{(i,j)\in X} c_{i,j} z_1^i z_2^j$ given by the set X and the canonical representations of the algebraic coefficients $\{c_{i,j} \mid (i,j) \in X\}$, define

$$\|p\| = \deg(p) + \sum_{(i,j)\in X} \|c_{i,j}\|.$$

Theorem 2.7.1. *Let $\lambda_1, \lambda_2 \in \overline{\mathbb{Q}}$ be non-zero and multiplicatively independent, and $p \in \overline{\mathbb{Q}}[z_1, z_2]$ be given by*

$$p(z_1, z_2) = \sum_{(i,j)\in X} c_{i,j} z_1^i z_2^j$$

where $|X| > 0$ and $c_{i,j} \neq 0$ for all $(i,j) \in X$. Consider the sequence $u_n = p(\lambda_1^n, \lambda_2^n)$. Writing $\mathcal{I} = \|p\| + \|\lambda_1\| + \|\lambda_2\|$, there exists effectively computable

$$N < \exp^4(\textsc{Poly}(\mathcal{I}))$$

such that $u_n \neq 0$ for all $n \geq N$.

Proof. We write $d = \deg(p) > 0$. Recall that multiplicative independence means that for any $(m_1, m_2) \in \mathbb{Z}^2$, if $\lambda_1^{m_1}\lambda_2^{m_2} = 1$ then $m_1 = m_2 = 0$. As a consequence, both λ_1 and λ_2 are not a root of unity, and $\lambda_1^{i_1}\lambda_2^{i_1} \neq \lambda_1^{i_2}\lambda_2^{j_2}$ for any distinct $(i_1, j_1), (i_2, j_2) \in X$. Let $\mathbb{K}$ be the smallest number field containing, $\lambda_1, \lambda_2, |\lambda_1|, |\lambda_2|$ as well as $c_{i,j}$ for all $(i, j) \in X$, such that $\mathbb{K}/\mathbb{Q}$ is a Galois extension. By the Tower Law, $D \coloneqq [\mathbb{K} : \mathbb{Q}]$ is bounded above by $\mathcal{I}^{\textsc{Poly}(d)}$.

We can replace λ_i with $1/\lambda_i$ in polynomial time if needed. For example, to replace λ_1 with $1/\lambda_1$, let $q(z_1, z_2) = \sum_{(i,j)\in X} c_{i,j} z_1^{d-i} z_2^j$. Then $q((1/\lambda_1)^n, \lambda_2^n) = \lambda_1^{-nd} p(\lambda_1^n, \lambda_2^n)$ and hence $p(\lambda_1^n, \lambda_2^n) = 0 \Leftrightarrow q((1/\lambda_1)^n, \lambda_2^n) = 0$. Observe that $1/\lambda_1$ and λ_2 are also multiplicatively independent. We now move onto the proof.

Case 1. Suppose $|\lambda_i| \neq 1$. W.l.o.g. we can take $i = 1$. By replacing λ_1 with $1/\lambda_1$ if necessary, we can assume $|\lambda_1| > 1$. Define $L = \max\{|\lambda_1^i\lambda_2^j| \colon (i, j) \in X\}$, $\mathcal{D} = \{(i, j) \colon |\lambda_1^i\lambda_2^j| = L\}$, and $\mathcal{R} = \{(i, j) \colon |\lambda_1^i\lambda_2^j| < L\}$. Write

$$p(\lambda_1^n, \lambda_2^n) = \underbrace{\sum_{(i,j)\in\mathcal{D}} c_{i,j}(\lambda_1^i\lambda_2^j)^n}_{v_n} + \underbrace{\sum_{(i,j)\in\mathcal{R}} c_{i,j}(\lambda_1^i\lambda_2^j)^n}_{r_n}$$

where $(v_n)_{n\in\mathbb{N}}$ is the *dominant part* of $(u_n)_{n\in\mathbb{N}}$. By Lemma 2.2.1, and the assumption of multiplicative independence, v_n is not identically zero.

We will first show that v_n can be written in the form $L^n\alpha^n \sum_{k=0}^d b_k\gamma^{kn}$, where $\alpha, \gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and $b_k \in \overline{\mathbb{Q}}$. If $v_n = c_{i,j}(\lambda_1^i\lambda_2^j)^n$ for some i, j, then we can simply choose $\alpha = \lambda_1^i\lambda_2^j/L$, $\gamma = 1$, $b_0 = c_{i,j}$, and $b_1, \ldots, b_d = 0$. Therefore, suppose v_n has at least two summands. Consider the free abelian group

$$G = \{(m_1, m_2) \in \mathbb{Z}^2 \colon |\lambda_1|^{m_1}|\lambda_2|^{m_2} = 1\}.$$

By the assumption that v_n has at least two summands, $|\lambda_1|$ and $\lambda_2|$ are multiplicatively dependent and hence G contains an element other than $(0, 0)$. On the other hand, since $|\lambda_1| \neq 1$, $G \neq \mathbb{Z}^2$. It follows that G has rank exactly 1. That is, there exists $(m_1, m_2) \in G$ satisfying $\gcd(m_1, m_2) = 1$ such that every element of G is an integer multiple of (m_1, m_2). Let $\gamma = \lambda_1^{m_1}\lambda_2^{m_2}$ and $\Lambda_{i,j} = \lambda_1^i\lambda_2^j$ for $(i, j) \in \mathcal{D}$. As every element of G is an integer multiple of (m_1, m_2), for all $(i_1, j_1), (i_2, j_2) \in \mathcal{D}$ it holds that $\Lambda_{i_2,j_2}/\Lambda_{i_1,j_1} = \lambda_1^{i_2-i_1}\lambda_2^{j_2-j_1}$ is of the form $(\lambda_1^{m_1}\lambda_2^{m_2})^k = \gamma^k$ for some k. Since $0 \leq i_1, i_2, j_1, j_2 \leq d$, we conclude that $|k|, |m_1|, |m_2| \leq d$. Hence there exists $(r, s) \in \mathcal{D}$ such that for any $(i, j) \in \mathcal{D}$, $\Lambda_{i,j} = \Lambda_{r,s}\gamma^{k_{i,j}}$ for some $0 \leq k_{i,j} \leq d$. Writing $\Lambda \coloneqq \Lambda_{r,s}$ and $\alpha = \Lambda/L$, we obtain that

$$\Lambda_{i,j}^n = \Lambda^n \left(\gamma^{k_{i,j}}\right)^n = L^n\alpha^n \left(\gamma^{k_{i,j}}\right)^n$$

for all $(i,j) \in \mathcal{D}$. Therefore,

$$v_n = \sum_{(i,j)\in\mathcal{D}} c_{i,j}\Lambda_{i,j}^n = L^n\alpha^n \sum_{k=0}^{d} b_k\gamma^{kn}$$

where each b_k is either zero or equal to $c_{i,j}$ for some i,j.

We now bound the description lengths of the algebraic numbers computed above. Since $c_{i,j}$ is part of the input for all i,j, $\|b_k\| < \mathcal{I}$ for all k. Next, recall that $\alpha = \Lambda_{i,j}/L$ and $L = |\lambda_1^i\lambda_2^j|$ for some $(i,j) \in \mathcal{D}$. Applying Corollary 1.5.8 and Lemma 1.5.10, $\|L\|, \|\alpha\| < \textsc{Poly}(\mathcal{I}, D)$. To bound $\|\gamma\|$, suppose v_n has at least two summands, as otherwise $\gamma = 1$. Recall that $\gamma = \lambda_1^{m_1}\lambda_2^{m_2}$. As discussed above, $|m_1|, |m_2| \le d$. Therefore, by Corollary 1.5.8, $\|\gamma\| < \textsc{Poly}(\mathcal{I}, D)$.

Applying Lemma 2.6.4 with $m = d$ to the non-zero polynomial $q(x) = \sum_{k=0}^{d} b_k x^k$ and γ, which satisfy $v_n = L^n\alpha^n q(\gamma^n)$ for all n, we conclude that there exist effectively computable $N_1, K_1 < 2^{\textsc{Poly}(\mathcal{I},D)}$ such that for $n \ge N_1$, $|v_n| > L^n/n^{K_1}$. We will compare this to the growth rate of $|r_n|$. Let $L_1 = \max_{(i,j)\in\mathcal{R}} |\lambda_1^i\lambda_2^j|$, which can be computed in time $\textsc{Poly}(\mathcal{I}, D)$ by Corollary 1.5.8 and lemma 1.5.10. By Lemma 2.4.1 there exists $K_2 < 2^{\textsc{Poly}(\mathcal{I},D)}$ such that for $n \ge 1$, $|r_n| < K_2 L_1^n$. By Lemma 1.5.1, $L - L_1 > 2^{-\textsc{Poly}(\mathcal{I},D)}$ and hence $L/(L - L_1) < 2^{\textsc{Poly}(\mathcal{I},D)}$. Applying Lemma 2.4.3 to $f(n) \coloneqq 1/n^{K_1}$ and $g(n) \coloneqq K_2(L_1/L)^n$ yields effectively computable

$$N < 2^{\textsc{Poly}(\mathcal{I},D)} < \exp^2(\textsc{Poly}(\mathcal{I}))$$

such that for all $n \ge N$, $|v_n| > |r_n|$ and therefore $u_n \neq 0$.

Case 2. Suppose $|\lambda_1| = |\lambda_2| = 1$ and λ_i is an algebraic integer; w.l.o.g. we can take $i = 1$. By a theorem of Kronecker (Section 1.5.2), an algebraic integer of modulus 1 that is not a root of unity has a Galois conjugate of modulus greater than 1. Hence there exists an automorphism $\sigma\colon \mathbb{K} \to \mathbb{K}$ such that $|\sigma(\lambda_1)| > 1$. Consider

$$q(z_1, z_2) = \sum_{(i,j)\in X} \sigma(c_{i,j})\sigma(\lambda_1)^i\sigma(\lambda_2)^j.$$

Since σ maps each element of $\mathbb{K}$ to one of its Galois conjugates, $\|\sigma(c_{i,j})\|$ for all i,j, as well as $\|\sigma(\lambda_1)\|$ and $\|\sigma(\lambda_2)\|$ are bounded by a polynomial in $\mathcal{I}$.[6] Moreover, $p(\lambda_1^n, \lambda_2^n) = 0$ if and only if $q(\sigma(\lambda_1)^n, \sigma(\lambda_2)^n) = 0$. Hence Case 1 applies.

Case 3. Finally, suppose λ_i is not an algebraic integer for some i. W.l.o.g. take $i = 1$. Recall that we can replace λ_1, λ_2, respectively, with $1/\lambda_1, 1/\lambda_2$ if necessary.

[6] We can compute canonical representations of all Galois conjugates of a given algebraic number in polynomial time using Lemma 1.5.6.

For $m \coloneqq (m_1, m_2) \in \{-1, 1\}^2$, let $p_m \in \overline{\mathbb{Q}}[z_1, z_2]$ be a non-zero polynomial such that $\|p_m\| < \textsc{Poly}(\mathcal{I})$ and for all $n \in \mathbb{N}$,

$$p(\lambda_1^n, \lambda_2^n) = 0 \quad \Leftrightarrow \quad p_m((\lambda_1^{m_1})^n, (\lambda_2^{m_2})^n) = 0.$$

If some p_m belongs to $\overline{\mathbb{Q}}[z_1]$, then $u_n = p_m(\lambda_1^n, \lambda_2^n)$ is of the form $\sum_{i \in Y} c_i (\lambda_1^{m_1})^{in}$. Applying Lemma 2.6.4, there exists $N < 2^{\textsc{Poly}(\mathcal{I})}$ such that $u_n \neq 0$ for all $n \geq N$. Suppose therefore no p_m for $m \in \{-1, 1\}^2$ belongs to $\overline{\mathbb{Q}}[z_1]$. By dividing each p_m through a power of z_1 if necessary, we can assume that

$$p_m(z_1, z_2) = z_1 q_m(z_1, z_2) + h_m(z_2)$$

for $q_m \in \overline{\mathbb{Q}}[z_1, z_2]$ and non-zero $h_m \in \overline{\mathbb{Q}}[z_1]$. The latter is of the form $\sum_{i=0}^{d_m} a_i z_1^i$, where each a_i is equal to one of the coefficients of p given as part of the input and $d_m = \deg(h_m) > 0$.

Applying Lemma 1.5.9, in time $\mathcal{I}^{\textsc{Poly}(|X|)}$ we can factorise each h_m and compute $A_m, \beta_1^{(m)}, \ldots, \beta_{d_m}^{(m)} \in \overline{\mathbb{Q}}$ such that $h_m(z) = A_m \prod_{i=1}^{d_m} (z - \beta_i^{(m)})$. Let $\mathbb{L}$ be the smallest extension of $\mathbb{K}$ containing $\beta_i^{(m)}$ for all m and $1 \leq i \leq d_m$. By the Tower Law and the fact that $d_m \leq d$ for all m,

$$D_1 \coloneqq [\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{Q}] \leq D \cdot \prod_{i,m} \deg(\beta_i^{(m)}) < 2^{2^{\textsc{Poly}(\mathcal{I})}}.$$

As discussed in Section 1.5.2, there exists a prime ideal $\mathfrak{p}$ of the ring $\mathcal{O}_{\mathbb{L}}$ of algebraic integers of $\mathbb{L}$ such that $v_{\mathfrak{p}}(\lambda_1) \neq 0$. Recalling that $v_{\mathfrak{p}}(\lambda_i^{-1}) = -v_{\mathfrak{p}}(\lambda_i)$, choose $m = (m_1, m_2) \in \{-1, 1\}^2$ such that $v_{\mathfrak{p}}(\lambda_1^{m_1}) > 0$ and $v_{\mathfrak{p}}(\lambda_2^{m_2}) \geq 0$. Define $\gamma_i \coloneqq \lambda_i^{m_i}$ for $i \in \{1, 2\}$, $\beta_i \coloneqq \beta_i^{(m)}$ for all $1 \leq i \leq d_m$, $P \coloneqq p_m$, $q \coloneqq q_m$, $h \coloneqq h_m$, and $A \coloneqq A_m$. In the end, we obtain that $u_n = 0$ if and only if

$$P(\gamma_1^n, \gamma_2^n) = \gamma_1^n q(\gamma_1^n, \gamma_2^n) + h(\gamma_2^n) = 0$$

where $v_{\mathfrak{p}}(\gamma_1) > 0$ and $v_{\mathfrak{p}}(\gamma_2) \geq 0$. The polynomials $P(z_1, z_2)$ and $q(z_1, z_2)$ are of the form $\sum_{(i,j) \in Y} b_{i,j} z_1^i z_2^j$ and $\sum_{(i,j) \in Z} a_{i,j} z_1^i z_2^j$, respectively, where each $b_{i,j}$ and $a_{i,j}$ is a coefficient of the original polynomial p. Hence both $\|P\|$ and $\|q\|$ are bounded by $\textsc{Poly}(\mathcal{I})$.

Since $P(\gamma_1^n, \gamma_2^n) = 0$ is equivalent to $\gamma_1^n q(\gamma_1^n, \gamma_2^n) = -h(\gamma_2^n)$, our approach will be to compare $v_{\mathfrak{p}}(\gamma_1^n q(\gamma_1^n, \gamma_2^n))$ to $v_{\mathfrak{p}}(-h(\gamma_2^n))$. Recall from Section 1.5.2 that $v_{\mathfrak{p}}(\cdot)$ is integer-valued, and for any $\alpha \in \mathbb{L}$ and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{L}}$,

$$|v_{\mathfrak{p}}(\alpha)| < \textsc{Poly}(D_1, \|\alpha\|).$$

Case 3.1. Suppose $v_{\mathfrak{p}}(\gamma_2) = 0$. Recall from Section 1.5.2 that $v_{\mathfrak{p}}(\alpha\beta) = v_{\mathfrak{p}}(\alpha) + v_{\mathfrak{p}}(\beta)$ and $v_{\mathfrak{p}}(\alpha + \beta) \geq \min\{v_{\mathfrak{p}}(\alpha), v_{\mathfrak{p}}(\beta)\}$ for all $\alpha, \beta \in \mathbb{L}$. Therefore,

$$v_{\mathfrak{p}}(\gamma_1^n q(\gamma_1^n, \gamma_2^n)) = n v_{\mathfrak{p}}(\gamma_1) + v_{\mathfrak{p}}(q(\gamma_1^n, \gamma_2^n))$$

for all $n \in \mathbb{N}$. Since $v_{\mathfrak{p}}(\gamma_1) > 0$ and $v_{\mathfrak{p}}(\gamma_2) = 0$,

$$\begin{aligned} v_{\mathfrak{p}}(q(\gamma_1^n, \gamma_2^n)) &\geq \min_{i,j} v_{\mathfrak{p}}(a_{i,j}\gamma_1^{in}\gamma_2^{jn}) \\ &\geq \min_{i,j} v_{\mathfrak{p}}(a_{i,j}). \end{aligned}$$

Since $\|a_{i,j}\| < \mathcal{I}$, we conclude that there exists a constant C_1 with $|C_1| < \textsc{Poly}(\mathcal{I}, D_1)$ such that $v_{\mathfrak{p}}(q(\gamma_1^n, \gamma_2^n)) \geq C_1$. Therefore, $v_{\mathfrak{p}}(\gamma_1^n q(\gamma_1^n, \gamma_2^n)) \geq n + C_1$ for all $n \in \mathbb{N}$. On the other hand,

$$v_{\mathfrak{p}}(-h(\gamma_2^n)) = v_{\mathfrak{p}}(-A) + \sum_{i=0}^{d_m} v_{\mathfrak{p}}(\gamma_2^n - \beta_i).$$

Let $N_1 < \mathcal{I}^{\textsc{Poly}(D_1)}$ be such that for $n \geq N_1$, $\gamma_2^n \neq \beta_i$ for all i, as in Lemma 1.5.2. If $\beta_i = 0$, then $v_{\mathfrak{p}}(\gamma_2^n) = n v_{\mathfrak{p}}(\gamma_2) = 0$. Otherwise, by Lemma 2.6.6 for all $n \geq N_1$,

$$v_{\mathfrak{p}}(\gamma_2^n - \beta_i) = v_{\mathfrak{p}}(\beta_i(\beta_i^{-1}\gamma_2^n - 1)) = v_{\mathfrak{p}}(\beta_i) + v_{\mathfrak{p}}(\beta_i^{-1}\gamma_2^n - 1) \leq \mathcal{I}^{\textsc{Poly}(D_1)} \log n.$$

Hence there exists a constant $0 < C_2 < \mathcal{I}^{\textsc{Poly}(D_1)}$ such that $v_{\mathfrak{p}}(-h(\gamma_2^n)) < C_2 \log n$ for all $n \geq N_1$. By Lemma 2.4.3, there exists $N = \textsc{Poly}(C_1, C_2) < \exp^3(\textsc{Poly}(\mathcal{I}))$ such that for all $n \geq N$, $3^{n+C_1} > n^{C_2}$. It follows that for $n \geq N$, $n + C_1 > C_2 \log n$ and hence $v_{\mathfrak{p}}(q(\gamma_1^n, \gamma_2^n)) > v_{\mathfrak{p}}(-h(\gamma_2^n))$, which implies that $u_n \neq 0$.

Case 3.2. Finally, suppose $v_{\mathfrak{p}}(\gamma_i) > 0$ for both γ_1 and γ_2. Let $L = v_{\mathfrak{p}}(\gamma_1) \cdot v_{\mathfrak{p}}(\gamma_2) \in \mathbb{N}$. Since $v_{\mathfrak{p}}(\gamma_i) < \textsc{Poly}(\mathcal{I}, D)$ (Section 1.5.2), $L \leq \textsc{Poly}(D, \mathcal{I})$. Consider the sequences

$$v_n^{(r)} = P(\gamma_1^{nL+r}, \gamma_2^{nL+r})$$

for $0 \leq r < L$. It suffices to show that for each r there exists computable N_r such that for $n \geq N_r$, $v^{(r)} \neq 0$. We can then choose $N = L \max_{0 \leq r < L} N_r$.

Let $\Lambda_1 = \gamma_1^{v_{\mathfrak{p}}(\gamma_2)}$ and $\Lambda_2 = \gamma_2^{v_{\mathfrak{p}}(\gamma_1)}$, noting that $v_{\mathfrak{p}}(\Lambda_1) = v_{\mathfrak{p}}(\Lambda_2) = L > 0$ and

$$\gamma_i^{nL} = (\Lambda_i^n)^{v_{\mathfrak{p}}(\gamma_i)}$$

for $i \in \{1, 2\}$. Recall that $P(z_1, z_2) \in \overline{\mathbb{Q}}[z_1, z_2]$ is of the form $\sum_{(i,j) \in Y} b_{i,j} z_1^i z_2^j$ with

$\|P\| < \textsc{Poly}(\mathcal{I})$. Writing $a_{i,j} = \gamma_1^{ir}\gamma_2^{jr}b_{i,j}$, it holds that

$$\begin{aligned} v_n^{(r)} &= P(\gamma_1^{nL+r}, \gamma_2^{nL+r}) \\ &= \sum_{(i,j)\in Y} a_{i,j}\gamma_1^{niL}\gamma_2^{njL} \\ &= \sum_{(i,j)\in Y} a_{i,j}\Lambda_1^{niv_\mathfrak{p}(\gamma_1)}\Lambda_2^{njv_\mathfrak{p}(\gamma_2)} \\ &= \sum_{(i,j)\in Y} a_{i,j}\Lambda_1^{n(iv_\mathfrak{p}(\gamma_1)+jv_\mathfrak{p}(\gamma_2))}(\Lambda_2/\Lambda_1)^{njv_\mathfrak{p}(\gamma_2)}. \end{aligned}$$

Hence for

$$S(z_1, z_2) \coloneqq \sum_{(i,j)\in Y} a_{i,j} z_1^{iv_\mathfrak{p}(\gamma_1)+jv_\mathfrak{p}(\gamma_2)} z_2^{jv_\mathfrak{p}(\gamma_2)}$$

it holds that for all $n \in \mathbb{N}$,

$$u_n = 0 \;\Leftrightarrow\; P(\gamma_1^{nL+r}, \gamma_2^{nL+r}) = 0 \;\Leftrightarrow\; S(\Lambda_1^n, (\Lambda_2/\Lambda_1)^n) = 0.$$

Observe that $v_\mathfrak{p}(\Lambda_1/\Lambda_2) = v_\mathfrak{p}(\Lambda_1) - v_\mathfrak{p}(\Lambda_2) = 0$ and $v_\mathfrak{p}(\Lambda_1) > 0$. Moreover, Λ_1 and Λ_2/Λ_1 are multiplicatively independent. To see this, let $a, b \in \mathbb{Z}$ be such that $\Lambda_1^a = (\Lambda_2/\Lambda_1)^b$. That is,

$$\gamma_1^{(a+b)v_\mathfrak{p}(\gamma_2)} = \gamma_2^{bv_\mathfrak{p}(\gamma_1)}.$$

Since γ_1 γ_2 are multiplicatively independent, $(a+b)v_\mathfrak{p}(\gamma_2) = 0$ and $bv_\mathfrak{p}(\gamma_1) = 0$. From $v_\mathfrak{p}(\gamma_1), v_\mathfrak{p}(\gamma_2) > 0$ it follows that $a = b = 0$. Therefore, we can use our analysis in Case 3.1 to bound the zeros of $S(\Lambda_1^n, (\Lambda_2/\Lambda_1)^n)$. It remains to observe that $\|S\|, \|\Lambda_1\|, \|\Lambda_1/\Lambda_2\| < 2^{\textsc{Poly}(\mathcal{I})}$, whence the required bound $N < \exp^4(\textsc{Poly}(\mathcal{I}))$ follows. □

Note that Cases 1-2 and 3 overlap in the proof above. In Case 3 we use the assumption that λ_1 is not an algebraic integer when asserting existence of a prime ideal $\mathfrak{p}$ for which $v_\mathfrak{p}(\lambda_1) \neq 0$. If neither λ_i is an algebraic integer, then it is possible that $v_\mathfrak{p}(\lambda_1) = v_\mathfrak{p}(\lambda_2) = 0$ for every prime ideal $\mathfrak{p}$. This happens, for example, if λ_1, λ_2 are both units of $\mathcal{O}_\mathbb{K}$, which need not be roots of unity.

Lifting the restriction that λ_1, λ_2 be multiplicatively independent in the statement of Theorem 2.7.1 does not make the analysis of zeros of u_n more difficult. However, it becomes possible that $u_n = 0$ for infinitely many n. As an example, suppose λ_1, λ_2 are multiplicatively dependent with $\lambda_1^a\lambda_2^b = 1$ where $(a, b) \neq (0, 0)$. Let $L = ab$ and consider the sequences $u_n^{(r)} = u_{nL+r}$ for $0 \leq r < L$. Each $u_n^{(r)}$ can be written in the form $q((\lambda_1^a)^n)$, where $q \in \overline{\mathbb{Q}}[x]$. If λ_1^a is a root of unity, then we can determine all zeros of $(u_n^{(r)})_{n\in\mathbb{N}}$ by inspection. Otherwise, we can employ Lemma 2.6.4.

Theorem 2.7.1 also solves the Skolem Problem for LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ of the form $u_n = a\lambda^n + \overline{a}\overline{\lambda}^n + b\gamma^n + \overline{b}\overline{\gamma}^n$ satisfying $|\lambda| = |\gamma|$. By scaling, u_n if necessary, we can assume that $|\lambda| = |\gamma| = 1$. Since $\overline{\lambda} = 1/\lambda$ and $\overline{\gamma} = 1/\gamma$, $u_n = 0$ if and only if

$$a\lambda^{2n}\gamma^n + \overline{a}\gamma^n + b\gamma^{2n}\lambda^n + \overline{b}\lambda^n = 0$$

which can be expressed as $p(\lambda^n, \gamma^n) = 0$ for a polynomial p with algebraic coefficients. The case of the Skolem Problem described above is exactly the one that requires the p-adic version of Baker's theorem. The remaining cases at order 4 can be solved using only the classical version of Baker's theorem.

We will next consider sequences of the form $u_n = p(n, \lambda^n)$. First, a small lemma.

Lemma 2.7.2. *For all $t \geq 0$ and integers $k > 0$, $\log t < kt^{\frac{1}{k}}$.*

Proof. For $0 < t < 1$, this is immediate. Let $f(t) \coloneqq kt^{\frac{1}{k}} - \log t$. It holds that

$$f'(t) = \frac{1}{\sqrt[k]{t^{k-1}}} - \frac{1}{t} = \frac{1}{t}(\sqrt[k]{t} - 1).$$

It remains to observe that $f'(t) > 0$ for all $t > 1$ and $f(1) > 0$. □

Theorem 2.7.3. *Let $\lambda \in \overline{\mathbb{Q}}$ be non-zero and $p(z_1, z_2) \in \overline{\mathbb{Q}}[z_1, z_2]$ be given by*

$$p(z_1, z_2) = \sum_{(i,j) \in X} c_{i,j} z_1^i z_2^j$$

where $|X| > 0$ and $c_{i,j} \neq 0$ for all $(i, j) \in X$. Suppose λ is not a root of unity. Write $\mathcal{I} = \|\lambda\| + \|p\|$ and consider the LRS $u_n = p(n, \lambda^n)$. There exists effectively computable $N < 2^{\textsc{Poly}(\mathcal{I})}$ such that for all $n \geq N$, $u_n \neq 0$.

Proof. If $p \in \overline{\mathbb{Q}}[z_1]$, then by Theorem 1.2.4 there exists $N < 2^{\textsc{Poly}(\mathcal{I})}$ such that $u_n \neq 0$ for $n \geq N$. Similarly, if $p \in \overline{\mathbb{Q}}[z_2]$, then we can invoke Lemma 2.6.4 to construct $N < 2^{\textsc{Poly}(\mathcal{I})}$ with the desired property. Hence assume $p \notin \overline{\mathbb{Q}}[z_1], \overline{\mathbb{Q}}[z_2]$ and write

$$p(n, \lambda^n) = \sum_{i=0}^{K} \lambda^{in} q_i(n)$$

where $k \leq \deg(p)$, each $q_i \in \overline{\mathbb{Q}}[z]$ and q_K is not identically zero. By Theorem 1.2.4, there exists $N_1 < 2^{\textsc{Poly}(\mathcal{I})}$ such that for all $n \geq N_1$, $q_K(n) \neq 0$ and hence $h_n(z) \coloneqq p(n, z)$ is not identically zero. For $n \geq N_1$, let

$$Z_n = \{z \colon p(n, z) = 0\}$$

which is a finite set of algebraic numbers. We will argue that the largest value of $\log(H(\alpha))$ for a point $\alpha \in Z_n$ grows poly-logarithmically in n, whereas $\log(H(\lambda^n))$ grows linearly in n. Therefore, for sufficiently large values of n, λ^n cannot possibly belong to Z_n.

Applying Lemma 1.5.9, there exists an absolute constant $C < \textsc{Poly}(\mathcal{I})$ such that we can compute all elements of Z_n for $n \geq 1$ in time $(\mathcal{I} + \log n)^C$. Hence there exists $B < \textsc{Poly}(\mathcal{I})$ such that for all $n \geq 2$,

$$\log H(\alpha) < (\mathcal{I} \log n)^B = \mathcal{I}^B (\log n)^B$$

for every $\alpha \in Z_n$. On the other hand, as discussed in Section 1.5.1, for all $n \in \mathbb{N}$,

$$\log H(\lambda^n) \geq dh(\lambda^n) - \frac{\log(d+1)}{2} = dnh(\lambda) - \frac{\log(d+1)}{2}$$

where $d = \deg(\lambda)$, $h(\lambda)$ is the absolute logarithmic Weil height of λ, and the last equality follows from $h(\lambda^n) = nh(\lambda)$. Recall from Section 1.5.1 that

$$h(\lambda) \geq \frac{1}{d + 52d^2 \log 6d}.$$

Hence there exist positive integers $A, N_2 < \textsc{Poly}(\mathcal{I})$ such that

$$\log(H(\lambda^n)) > \frac{n}{A}$$

for all $n \geq N_2$. It remains to compare $\mathcal{I}^B (\log n)^B$ to n/A. Applying Lemma 2.7.2 with $k = 2B$, we obtain that $(\log n)^B < (2B)^B \sqrt{n}$ for $n \geq 1$. Let $N_3 = (\mathcal{I} \cdot 2B)^{2B} A^2$, which is at most $2^{\textsc{Poly}(\mathcal{I})}$. We have that for all $n \geq N_3$,

$$\mathcal{I}^B (\log n)^B < \frac{n}{A}.$$

It remains to take $N = \max\{N_1, N_2, N_3\}$. □

Chapter 3

Almost-periodic words

In his seminal work [21], Büchi showed decidability of the monadic second-order theory (see Section 1.9) of the structure $\langle \mathbb{N}; < \rangle$ by establishing a correspondence between MSO formulas and non-deterministic Büchi automata. Shortly thereafter, Elgot and Rabin [34] asked: Which unary predicates $P_1, \ldots, P_m$ can be added to $\langle \mathbb{N}; < \rangle$ while maintaining decidability of the MSO theory? It turns out that using Büchi's method, this question can also be cast into automata-theoretic terms. Recall the following problem from the Introduction.

Acceptance Problem for the infinite word α. Given a deterministic Muller automaton $\mathcal{A}$, decide whether $\mathcal{A}$ accepts α.

For a predicate $P_i \colon \mathbb{N} \to \{0,1\}$, denote by $\alpha_i \in \{0,1\}^\omega$ its characteristic word defined by $\alpha_i(n) = P_i(n)$ for all $n \in \mathbb{N}$. By [21] and the fact that deterministic Muller automata are equivalent to non-deterministic Büchi automata, the MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ is decidable if and only if the Acceptance Problem for the product word $\alpha \coloneqq \alpha_1 \times \cdots \times \alpha_m$ is decidable. This characterisation has allowed decidability of the MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ to be studied through combinatorial properties of the word α. In contrast, it was known even before Büchi's decidability result that augmenting $\langle \mathbb{N}; < \rangle$ with addition or even the doubling function results in a structure with undecidable MSO theory [73, 77].

We now give an overview of predicates (resp. characteristic words) for which decidability of the MSO theory (resp. the Acceptance Problem) is known. In [34], Elgot and Rabin used a *contraction method* to show decidability of the MSO theory of $\langle \mathbb{N}; <, P \rangle$ for the following predicates P, where m is an arbitrary positive integer.

(a) $P(n) = 1 \Leftrightarrow n = k!$ for some k;

(b) $P(n) = 1 \Leftrightarrow n = k^m$ for some k;

(c) $P(n) = 1 \Leftrightarrow n = m^k$ for some k.

More recently, Carton and Thomas [23] showed via a *semigroup* approach that the Acceptance Problem is decidable for *morphic* words. Morphic words include characteristic words of the predicates (b-c) above, as well a large number other words like the Thue-Morse sequence (viewed as an infinite word over $\{0, 1\}$) and the characteristic word $\alpha \in \{0, 1\}^\omega$ of the Fibonacci sequence defined by

$$\alpha(n) = 1 \quad \Leftrightarrow \quad n \text{ is a term of the Fibonacci sequence.}$$

The most interesting (for our purposes) class of words with decidable MSO properties, however, is due to Semënov. He showed in [75] that the Acceptance Problem is decidable for *effectively almost-periodic* words. We refer to this result as **Semënov's theorem**. A word $\alpha \in \Sigma^\omega$ is *almost-periodic* if for every finite word $u \in \Sigma^*$ there exists $k_u \in \mathbb{N}$ such that either

(a) u does not occur in $\alpha[k_u, \infty)$, or

(b) u occurs infinitely often in α and within every contiguous subword (i.e. factor) of length k_u.

An almost-periodic word α is effectively almost-periodic if there exist

($\star$) a program $\mathcal{P}_1$ that computes $\alpha(n)$ given $n \in \mathbb{N}$, and

($\star\star$) a program $\mathcal{P}_2$ that, given a finite word u, computes an integer k_u with the property above.

We dedicate the rest of this chapter to almost-periodic words and Semënov's theorem.

Recall that the Model-Checking Problem is to decide, given a linear dynamical system (M, s), a family of semialgebraic targets $\mathcal{T}$, and a deterministic automaton $\mathcal{A}$, whether $\mathcal{A}$ accepts the characteristic word α of (M, s) with respect to $\mathcal{T}$. Let $\mathcal{K}$ be a class of triples $\langle M, s, \mathcal{T}\rangle$. Suppose we have an algorithm for computing, on input $\langle M, s, \mathcal{T}\rangle \in \mathcal{K}$, the programs $\mathcal{P}_1$ and $\mathcal{P}_2$ described above for the characteristic word α of (M, s) with respect to $\mathcal{T}$.[1] In particular, we have proven that each characteristic word

[1] Given $M, s, \mathcal{T}$, constructing $\mathcal{P}_1$ is trivial: on input n, compute $M^n s$ and check which polynomial inequalities defining $\mathcal{T}$ are satisfied.

α associated with $\langle M, s, \mathcal{T}\rangle \in \mathcal{K}$ is effectively almost-periodic. Invoking Semënov's theorem, it follows that the Model-Checking Problem is decidable for the family of instances

$$\{\langle M, s, \mathcal{T}, \mathcal{A}\rangle \colon \langle M, s, \mathcal{T}\rangle \in \mathcal{K}\}.$$

That the programs $\mathcal{P}_1, \mathcal{P}_2$ are computable from $\langle M, s, \mathcal{T}\rangle$ is important. In Chapter 7 we will see that for the class $\mathcal{K}_D = \{\langle M, s, \mathcal{T}\rangle \colon M \text{ is diagonalisable}\}$, every characteristic word α associated with $\langle M, s, \mathcal{T}\rangle \in \mathcal{K}_D$ is provably effectively almost-periodic. In particular, for such α there exists *some* program $\mathcal{P}_2$ that computes k_u on u. But we do not have a way of determining $\mathcal{P}_2$ given $M, s, \mathcal{T}$. Consequently, we are unable to prove decidability of the full Model-Checking Problem for diagonalisable linear dynamical systems.

The approach described in the previous paragraph is the one we take throughout this thesis. That is, we prove decidability results for the Model-Checking Problem by showing, for various classes $\mathcal{K}$ of triples $\langle M, s, \mathcal{T}\rangle$, effective almost periodicity of the characteristic word α associated with every $\langle M, s, \mathcal{T}\rangle \in \mathcal{K}$ and how to construct the programs $\mathcal{P}_1$ and $\mathcal{P}_2$ for α given $M, s, \mathcal{T}$. The relationship between Semënov's theorem and decidability of the Model-Checking Problem, however, is much deeper. Firstly, every non-trivial decidability result about the MCP known to the author can be explained by an argument based on almost periodicity. In particular, the approach to the Model-Checking Problem based on Semënov's theorem captures *all* decidability results for the MCP that we have given to date [7, 47, 48]; We explicitly used Semënov's theorem only in [47]. Moreover, relying on effective almost periodicity and Semënov's theorem as opposed to *ad hoc* approaches does not seem to deteriorate the complexity of the resulting decision procedures. For example, in [48] we proved, using specialised methods, that given an LDS (M, s) in ambient space $\mathbb{R}^3$, a family of semialgebraic sets $\mathcal{T}$, and a formula φ in the language of Linear Temporal Logic, it is decidable whether the characteristic word α of (M, s) with respect to $\mathcal{T}$ satisfies φ. The complexity upper bound that we could prove for our algorithm was EXPSPACE. In Chapter 5, we will show that the full Model-Checking Problem for three-dimensional systems is decidable with the same complexity bound.

In Section 3.1, we prove Semënov's theorem and quantitatively analyse the resulting decision procedure, The latter has not been done so far but is required for bounding complexity of our algorithms. Our starting point is the ingenious proof of Muchnik, Semënov and Ushakov [64] that, given a deterministic automaton $\mathcal{A}$ and an effectively almost-periodic word α (represented by the programs $\mathcal{P}_1$ and $\mathcal{P}_2$), it is decidable whether $\mathcal{A}$ accepts α. Apart from obtaining complexity bounds, another benefit of

giving a detailed account of the proof of [64] is that we can use the intermediate steps to give an algorithm that, under some assumptions, decides whether a given *prefix-independent* automaton $\mathcal{A}$ accepts a word α that has a an almost-periodic suffix (Section 3.2). This is the specific result we use to show decidability of the Model-Checking Problem restricted to diagonalisable systems and prefix-independent properties (Chapter 7), which we originally proved in [7] using specialised arguments.

We mention that almost-periodic words generalise *uniformly recurrent words* that are well-known in symbolic dynamics and combinatorics on words. A word α is uniformly recurrent if for every finite word u appearing in α, there exists $k_u \in \mathbb{N}$ such that u appears in every factor of α of length k_u. In particular, each finite word u either does not occur in a uniformly recurrent word α, or occurs infinitely often. Muchnik et al. [64] refer to uniformly recurrent words as *strongly almost-periodic*.

3.1 Model checking effectively almost-periodic words

In this section we prove Semënov's theorem. The main step of the proof is to show that if α is effectively almost-periodic, then so is the sequence of states $\mathcal{A}(\alpha)$ obtained when a deterministic automaton $\mathcal{A}$ reads α. Once we know that $\mathcal{A}(\alpha)$ is effectively almost-periodic, we can determine the set of states that are visited infinitely often as follows. For a state q of $\mathcal{A}$, let k be such that either q does not occur in $\mathcal{A}[k, \infty)$, or it occurs in every subword of $\mathcal{A}(\alpha)$ of length k. The state q occurs infinitely often in $\mathcal{A}(\alpha)$ if and only if it occurs in $\mathcal{A}[k, 2k)$, which can be checked effectively.

For an effectively almost-periodic word α and a finite word u, let $\mathcal{W}_\alpha(u)$ denote the smallest $m \in \mathbb{N}$ satisfying the following property: either u does not appear in $\alpha[m, \infty)$, or it appears at least twice in every contiguous substring of α of length m.[2] The quantity $\mathcal{W}_\alpha(u)$ is slightly different (but ultimately more convenient) than the quantity k_u that we gave when defining almost-periodic words. In particular, $k_u \leq \mathcal{W}_\alpha(u) \leq 2k_u$ for every u. For $l \in \mathbb{N}$, we define

$$\mathcal{W}_\alpha(l) = \max_{u \in \Sigma^l} \mathcal{W}_\alpha(u).$$

We will write $\mathcal{W}(u)$ and $\mathcal{W}(l)$ when α is clear from the context. We denote by $\mathcal{W}^n$ the nth functional power of $\mathcal{W}$, defined inductively as $\mathcal{W}^0 = \mathrm{id}$ and $\mathcal{W}^{n+1} = \mathcal{W} \circ \mathcal{W}^n$ for $n \geq 0$. Observe that $\mathcal{W}$ is monotonic by definition and hence $\mathcal{W}^n(l) \geq \mathcal{W}^m(l)$ for $n \geq m$. Moreover, $\mathcal{W}(l) \geq l + 1$ for all $l \in \mathbb{N}$. Finally, we say that $\widetilde{\mathcal{W}} \colon \mathbb{N} \to \mathbb{N}$ is

[2] We take $\mathcal{W}(\varepsilon) = 1$, where ε is the empty word. The exact definition of $\mathcal{W}(\varepsilon)$ is immaterial to our results.

a *window function* for an effectively almost-periodic word α if $\widetilde{\mathcal{W}}(u) \geq \mathcal{W}_\alpha(u)$ and $\widetilde{\mathcal{W}}(l) \geq \mathcal{W}_\alpha(l)$ for all $u \in \Sigma^*$ and $l \in \mathbb{N}$. For an effectively almost-periodic word α, as discussed above, we have the window function $\widetilde{\mathcal{W}}(u) = 2k_u$. Conversely, to prove that a computable word α is effectively almost-periodic it suffices to construct an explicit window function for α.

We begin our analysis of the sequence of states $\mathcal{A}(\alpha)$ for α effectively almost-periodic. The following lemma states that in an almost-periodic word, if a finite word occurs sufficiently far to the right, then it must have an earlier occurrence. Its proof follows directly from the definition of almost periodicity.

Lemma 3.1.1. *Let α be an almost-periodic word, and $\alpha[i, j]$ be a subword of length l. If $i \geq \mathcal{W}(l)$, then there exist $i' < i$ and $j' < j$ such that $|\alpha[i', j]| \leq \mathcal{W}(l)$ and $\alpha[i', j'] = \alpha[i, j]$.*

The next lemma can be seen as lifting the statement of Lemma 3.1.1 from α to $\mathcal{A}(\alpha)$. Recall that $|u|$ denotes the length of u.

Lemma 3.1.2. *Let α be almost periodic, $\mathcal{A}$ be a deterministic automaton with the set of states Q, and $u \in Q^*$ be a finite sequence of states with $|u| = l > 0$. If u occurs in $\mathcal{A}(\alpha)$ at a position $i \geq 2\mathcal{W}^{|Q|+1}(l)$, then it has another occurrence in $\mathcal{A}(\alpha)$ at a position $i' < i$ with $|\mathcal{A}(\alpha)[i', j]| \leq \mathcal{W}^{|Q|}(l)$.*

Proof. Let $i_1 := i$ and $j_1 := i_1 + l - 1$ denote the endpoints of u in $\mathcal{A}(\alpha)$, i.e. $\mathcal{A}(\alpha)[i_1, j_1] = u$. The proof relies on constructing a finite sequence of pairs of indices

$$(i_1, j_1), \ldots, (i_{|Q|+1}, j_{|Q|+1})$$

with the following properties. Write $v_k = \alpha[i_k, j_1]$, $l_k = |v_k|$ and $q_k = \mathcal{A}(\alpha)(i_k)$ for $k \geq 1$. For all $k \geq 1$ and $m < k$,

(1) $i_k \leq j_k$, $i_k < i_m$, and $l_m > l_k$,

(2) v_m is a prefix of v_k,

(3) $l_k \leq \mathcal{W}^{k-1}(l)$, and

(4) $i_k > \mathcal{W}(l_k)$.

Properties 1 and 2 follow from $\alpha[i_k, j_k]$ being a "retraction" (i.e. an earlier occurrence) of $\alpha[i_{k-1}, j_1] = v_{k-1}$ in α. Property 4 will allow us to repeatedly apply Lemma 3.1.1 to $\alpha[i_k, j_1]$. Fig. 3.1 depicts construction of $(i_1, j_1), (i_2, j_2), (i_3, j_3)$ and Properties 1 and 2.

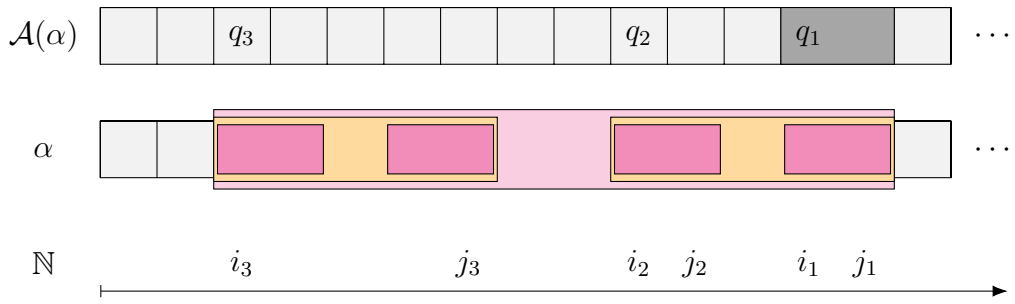

Figure 3.1: Constructing (i_2, j_2) and (i_3, j_3) from $u \coloneqq \alpha[i_1, j_1]$. ▭, ▭, ▭, ▭ represent the finite words u, v_1, v_2, v_3, respectively. Observe that v_1 is a prefix of v_2, which itself is a prefix of v_3.

Once we have constructed $(i_1, j_1), \ldots, (i_{|Q|+1}, j_{|Q|+1})$ with the desired properties, the statement of the lemma follows. By the pigeonhole principle, there must exist $1 \leq m < k \leq |Q| + 1$ such that $q_k = q_m$. Since v_m is a prefix of v_k and $\mathcal{A}$ is deterministic, reading v_k from the state q_k and reading v_m from the state q_m will produce the same sequence of $l_m = |v_m|$ states. Formally,

$$\mathcal{A}(\alpha)[i_k, i_k + l_m - 1] = \mathcal{A}(\alpha)[i_m, j_1].$$

Since $\mathcal{A}(\alpha)[i_1, j_1] = u$ and $i_m \leq i_1$, $\mathcal{A}(\alpha)[i_m, j_1]$ ends in u. Hence $\mathcal{A}(\alpha)[i_k, i_k + l_m - 1]$ also ends in u. That is,

$$\mathcal{A}(\alpha)[i_k + l_m - l, i_k + l_m - 1] = u.$$

Since $i_k + l_m - 1 < i_k + l_k - 1$, this occurrence of u in $\mathcal{A}(\alpha)$ is different from $\mathcal{A}(\alpha)[i_1, j_1] = u$. We can therefore choose $i' = i_k + l_m - l_1$. That $|\mathcal{A}(\alpha)[i', j]| \leq \mathcal{W}^{|Q|}(l)$ follows from $i_{|Q|+1} \leq i'$ and

$$|\mathcal{A}(\alpha)[i_{|Q|+1}, j]| = l_{|Q|+1} \leq \mathcal{W}^{|Q|}(l)$$

where the inequality follows from Property 3.

We now proceed with our (inductive) construction. Observe that all properties are satisfied for $k = 1$, i.e. for the finite sequence (i_1, j_1). Now suppose we have constructed $(i_1, j_1), \ldots, (i_k, j_k)$ satisfying Properties 1-4 for some $k \leq |Q|$. To construct (i_{k+1}, j_{k+1}), consider the finite word $v_k = \alpha[i_k, j_1]$. Since α is almost-periodic and $i_k > \mathcal{W}(l_k)$ by the inductive hypothesis, invoking Lemma 3.1.1 there exist i_{k+1}, j_{k+1} such that $i_{k+1} < i_k$ and

$$|\alpha[i_{k+1}, j_1]| \leq \mathcal{W}(l_k).$$

Let $v_{k+1} = \alpha[i_{k+1}, j_{k+1}]$ and $l_{k+1} = |v_{k+1}| = j_1 - i_{k+1} + 1$. By the inductive hypothesis,

$$l_{k+1} \leq \mathcal{W}(l_k) \leq \mathcal{W}(\mathcal{W}^{k-1}(l)) = \mathcal{W}^k(l).$$

So far we have shown Properties 1 and 3. For all $m < k$, by the inductive hypothesis, v_m is a prefix of v_k. Since v_k itself is a prefix of v_{k+1} by construction, we conclude that v_m is a prefix of v_{k+1} for all $m < k+1$ (Property 2).

To show that $i_{k+1} > \mathcal{W}(l_{k+1})$ as in Property 4, observe that by construction, $i_{k+1} = j_1 - l_{k+1} + 1 > i_1 - l_{k+1}$. Since $i_1 \geq 2\mathcal{W}^{|Q|+1}(l)$ by assumption and $l_{k+1} \leq \mathcal{W}^k(l)$ as argued above,

$$i_{k+1} > 2\mathcal{W}^{|Q|+1}(l) - \mathcal{W}^k(l) = \mathcal{W}^{|Q|+1}(l) + (\mathcal{W}^{|Q|+1}(l) - \mathcal{W}^k(l)).$$

Since $k \leq |Q|$ and $\mathcal{W}(l) \geq l + 1$ for all $l \in \mathbb{N}$,

$$\mathcal{W}^{|Q|+1}(l) = \mathcal{W}(\mathcal{W}^{|Q|}(l)) > \mathcal{W}^k(l)$$

Therefore,

$$i_{k+1} > \mathcal{W}^{|Q|+1}(l).$$

On the other hand, since $l_{k+1} \leq \mathcal{W}^k(l)$ and $k + 1 \leq |Q| + 1$,

$$\mathcal{W}(l_{k+1}) \leq \mathcal{W}^{k+1}(l) \leq \mathcal{W}^{|Q|+1}(l) < i_{k+1}. \qquad \square$$

We are now ready to state and prove the main result of this section. Recall that to prove that an almost-periodic word α is effectively almost-periodic, it suffices to give two algorithms: one that computes $\alpha(n)$ given n, and another one that computes an upper bound on $\mathcal{W}(l)$ given l.

Theorem 3.1.3. *Let α be almost-periodic, $\mathcal{A}$ be a deterministic automaton with set of states Q, and $\widetilde{\mathcal{W}} : \mathbb{N} \to \mathbb{N}$ be an effectively computable function satisfying $\widetilde{\mathcal{W}}(l) \geq \mathcal{W}_\alpha(l)$ for all $l \in \mathbb{N}$. Define $N(l) \coloneqq 2\widetilde{\mathcal{W}}^{|Q|+1}(l) + l$ and $H(l) \coloneqq 2\widetilde{\mathcal{W}}^{|Q|+1}(N(l))$.*

(a) A word $u \in Q^l$ occurs infinitely often in $\mathcal{A}(\alpha)$ if and only if it occurs at least once in every contiguous substring of $\mathcal{A}(\alpha)$ of length $N(l)$.

(b) A word $u \in Q^l$ does not occur infinitely often in $\mathcal{A}(\alpha)$ if and only if it does not occur in $\mathcal{A}(\alpha)[H(l), \infty)$.

(c) The word $\mathcal{A}(\alpha)$ is almost-periodic with $\mathcal{W}_{\mathcal{A}(\alpha)}(l) \leq 2H(l)$ for all $l \in \mathbb{N}$. Moreover, if α is effectively almost-periodic, then so is $\mathcal{A}(\alpha)$.

Proof. We will need the following observation to relate $\widetilde{\mathcal{W}}^k(\cdot)$ to $\mathcal{W}_\alpha^k(\cdot)$ for $k \in \mathbb{N}$. Let $g, f\colon \mathbb{N} \to \mathbb{N}$ be such that f is monotonic and $g(n) \geq f(n)$ for all n. Then for all $k, x \in \mathbb{N}$, $g^k(x) \geq f^k(x)$. To prove this by induction, first observe that for $k = 0$, $g^k(x) = f^k(x) = x$. For $k \geq 1$,

$$g^k(x) = g(g^{k-1}(x)) \geq f(g^{k-1}(x)) \geq f(f^{k-1}(x)) = f^k(x).$$

In particular, $\widetilde{\mathcal{W}}^k(l) \geq \mathcal{W}_\alpha^k(l)$ for all $k, l \in \mathbb{N}$.

Let u be a word of length l. We first prove (a). Suppose u occurs infinitely often in $\mathcal{A}(\alpha)$. Let $0 \leq k_1 < k_2 < \cdots$ denote all the indices at which u occurs in $\mathcal{A}(\alpha)$, and $k_0 = 0$. By Lemma 3.1.2, for all $n \in \mathbb{N}$,

$$k_{n+1} - k_n < 2\mathcal{W}_\alpha^{|Q|+1}(l) \leq 2\widetilde{\mathcal{W}}^{|Q|+1}(l).$$

It follows that u occurs in every subword of $\mathcal{A}(\alpha)$ of length

$$2\widetilde{\mathcal{W}}^{|Q|+1}(l) + l = N(l).$$

To prove (b), suppose u does not occur infinitely often in $\mathcal{A}(\alpha)$. Let v be a word of length $N(l)$ appearing infinitely often in $\mathcal{A}(\alpha)$ in which u does not occur. By Lemma 3.1.2, the earliest occurrence of v in $\mathcal{A}(\alpha)$ is at a position k satisfying

$$k \leq 2\mathcal{W}_\alpha^{|Q|+1}(|v|) \leq 2\widetilde{\mathcal{W}}^{|Q|+1}(N(l)) = H(l).$$

Let $\beta = \alpha[k, \infty)$, $w = \mathcal{A}(\alpha)[k, \infty)$ and $\mathcal{B}$ be the automaton with start state $\mathcal{A}(\alpha)(k)$ that is identical to $\mathcal{A}$ otherwise. Observe that $w = \mathcal{B}(\beta)$. Applying Lemma 3.1.2 to β and $\mathcal{B}$, if u occurs in w then it must occur at a position m with

$$m < 2\mathcal{W}_\beta^{|Q|+1}(l) \leq 2\widetilde{\mathcal{W}}^{|Q|+1}(l) \leq N(l).$$

Here we used the fact that since β is a suffix of α, $\mathcal{W}_\beta(l)$ is bounded above by $\mathcal{W}_\alpha(l)$. In particular, $\widetilde{\mathcal{W}}$ is a window function for β as well. Since v is a prefix of β of length $N(l)$ and u does not appear in v by construction, we conclude that u does not appear in $\mathcal{A}(\alpha)[k, \infty)$. It remains to recall that $k \leq H(l)$.

Finally, to prove (c), first of all observe that if α is effectively almost-periodic, its letters can be effectively determined. Hence $\mathcal{A}(\alpha)(n)$ can be effectively computed for all $n \in \mathbb{N}$ by simply simulating $\mathcal{A}$ on α. Next, consider $u \in Q^*$ of length l. If u appears infinitely often in $\mathcal{A}(\alpha)$, then by (a) it appears at least twice in any substring of $\mathcal{A}(\alpha)$ of length $2N(l)$. Since $\widetilde{\mathcal{W}}(l) \geq \mathcal{W}_\alpha(l) \geq l$ for all $l \in \mathbb{N}$, we have $N(l) \leq H(l)$ and hence $2N(l) \leq 2H(l)$. It follows that u occurs at least twice in every substring of $\mathcal{A}(\alpha)$ of length at least $2H(l)$. If, on the other hand, u does not occur infinitely often in $\mathcal{A}(\alpha)$, then by (b) it does not occur in $\mathcal{A}(\alpha)[H(l), \infty)$ and hence in $\mathcal{A}(\alpha)[2H(l), \infty)$ □

Corollary 3.1.4. *Let α be effectively almost-periodic with the window function $\widetilde{\mathcal{W}}$, and $\mathcal{A}$ be a deterministic automaton. Suppose $H(1)$ is computed from $\widetilde{\mathcal{W}}$ as above. A state q occurs infinitely often in $\mathcal{A}(\alpha)$ if and only if it occurs in $\mathcal{A}(\alpha)[H(1), 2H(1))$.*

Proof. Immediate from Theorem 3.1.3 (a-b) and that $N(l) \leq H(l)$ for all $l \in \mathbb{N}$. □

We therefore have the following conceptually simple algorithm for deciding whether a given deterministic automaton $\mathcal{A}$ accepts a word α that is effectively almost-periodic. Let $\widetilde{\mathcal{W}}$ be a computable function such that for all $l \in \mathbb{N}$, $\widetilde{\mathcal{W}}(l) \geq \mathcal{W}_\alpha(l)$, which exists by effective almost periodicity. First compute the value of $m = \widetilde{\mathcal{W}}^{|Q|+1}(1)$ and

$$H(1) = 2\widetilde{\mathcal{W}}^{|Q|+1}(2m+1).$$

The set S of states appearing in $\mathcal{A}(\alpha)[H(1), 2H(1))$ comprises exactly the states visited infinitely often when $\mathcal{A}$ reads α. It remains to check S against the acceptance condition of the automaton. Observe that because $H(1)$ depends non-elementarily on the number of states in $\mathcal{A}$, the running time of this algorithm can be elementary only if $\widetilde{\mathcal{W}}(l)$ is "small" in terms of l. We are able to ensure this in our proof of the decidability of the Model-Checking Problem with tame targets (Chapter 6) by constructing $\widetilde{\mathcal{W}}(l)$ that is polynomial in l.

3.2 Words with an almost-periodic suffix

Recall from Section 1.8 that a prefix-independent automaton has the property that whether a word α is accepted or not does not change if we perform finitely many insertions and deletions on α. Suppose we want to decide whether a given deterministic and prefix-independent Muller automaton $\mathcal{A}$ with state set Q accepts a word α with the following properties.

(a) The word α has an almost-periodic suffix β.

(b) We have access to a window function $\widetilde{\mathcal{W}}$ for β, but cannot necessarily compute $\beta(n)$ given n. In other words, we do not know the starting index of β in α.

(c) We have access to an oracle that, given $l \in \mathbb{N}$, returns a word u of length l that occurs infinitely often in β and hence also in α.

That is, the input is the automaton $\mathcal{A}$ and the oracles described (b-c). This setting, however esoteric it may sound, is encountered when analysing characteristic words of

diagonalisable linear dynamical systems with respect to semialgebraic targets. We can decide whether $\mathcal{A}$ accepts α as follows.

As the first step, compute $N = 2\widetilde{\mathcal{W}}^{|Q|+1}(1) + 1$ and $H = 2\widetilde{\mathcal{W}}^{|Q|+1}(N)$. In the notation of the previous section, $H = H(1)$. Next, using the oracle from (c), determine a word w of length $2H$ that occurs infinitely often in β. Thereafter, simulate $\mathcal{A}$ on w, recording the set S of states in $\mathcal{A}(w)[H, 2H)$. The algorithm returns "yes" if and only $S \in F$, where F is the acceptance condition of $\mathcal{A}$ (Section 1.8). To prove correctness of this procedure, consider factorisations $\alpha = u\beta$ and $\beta = vw\gamma$, where u, v, w are finite words and γ is infinite. Since $w\gamma$ is a suffix of β, the word $w\gamma$ is almost-periodic and $\widetilde{\mathcal{W}}$ is a window function for $w\gamma$ as well. Applying Theorem 3.1.3 (a-b) to $w\gamma$, we conclude that a set q appears infinitely often in $\mathcal{A}(w\gamma)$ if and only if it appears in $\mathcal{A}(w)[H, 2H)$. That is, S is exactly the set of states that appear infinitely often in $\mathcal{A}(w\gamma)$. Hence our algorithm returns "yes" if and only if $\mathcal{A}$ accepts $w\gamma$. Because $\mathcal{A}$ is prefix-independent, it accepts $w\gamma$ if and only if it accepts α.

Chapter 4

Toric words

In this chapter we study *toric words*, a class of almost-periodic words generated by a compact dynamical system on a torus. Toric words will play a prominent role in our analysis of linear dynamical systems. Recall that we denote by $\mathbb{T}$ the one-dimensional torus $\{z \in \mathbb{C} \colon |z| = 1\}$, viewed as an abelian group under multiplication. We equip $\mathbb{C}^d$ with the Euclidean topology and $\mathbb{T}^d$ with the induced subset topology for every $d > 0$. A word $\alpha \in \Sigma^\omega$ is *toric* if there exist an integer $d > 0$, $\Gamma = (\gamma_1, \ldots, \gamma_d) \in \mathbb{T}^d$, and a family $\mathcal{S} = \{S_\sigma \colon \sigma \in \Sigma\}$ of pairwise disjoint open subsets of $\mathbb{T}^d$ such that each S_σ has finitely many connected components, and for all $n \in \mathbb{N}$ and $\sigma \in \Sigma$,

$$\alpha(n) = \sigma \quad \Leftrightarrow \quad \Gamma^n \in S_\sigma. \tag{4.1}$$

The definition implies that the sequence $(\Gamma^n)_{n\in\mathbb{N}}$ is contained in the open subset $\bigcup_{\sigma\in\Sigma} S_\sigma$ of $\mathbb{T}^d$. We say that α is the toric word *generated by* $(\Gamma, \mathcal{S})$. To determine the nth letter of a toric word α, it suffices to determine the unique $\sigma \in \Sigma$ such that $\Gamma^n = (\gamma_1^n, \ldots, \gamma_d^n)$ "falls into" (i.e. belongs to) S_σ. In the dynamical systems literature, the toric word α generated by $(\Gamma, \mathcal{S})$ is referred to as the *coding* of the orbit $(\Gamma^n)_{n\in\mathbb{N}}$ with respect to $\mathcal{S}$.

We refer to a word $\alpha \in \Sigma$ as *eventually toric* with parameters $(\Gamma, N, \mathcal{S})$, where $N \in \mathbb{N}$, $\Gamma \in \mathbb{T}^d$ and $\mathcal{S}$ consists of open semialgebraic sets with finitely many connected components, if Equation (4.1) holds for all $n \geq N$ and $\sigma \in \Sigma$. We say that a triple $(\Gamma, N, \mathcal{S})$ is *semialgebraic* if $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ for some $d > 0$ and $\mathcal{S}$ consists of semialgebraic subsets of $\mathbb{T}^d$. Eventually toric words with semialgebraic parameters will be crucial to our decidability proofs for various subclasses of the Model-Checking Problem. In particular, all characteristic words of linear dynamical systems for which we will prove eventual toricity will be eventually toric with semialgebraic parameters. In Section 4.3 we will show that the eventually toric words are *effectively* almost-periodic. For arbitrary toric words, in comparison, we are able to only show almost periodicity.

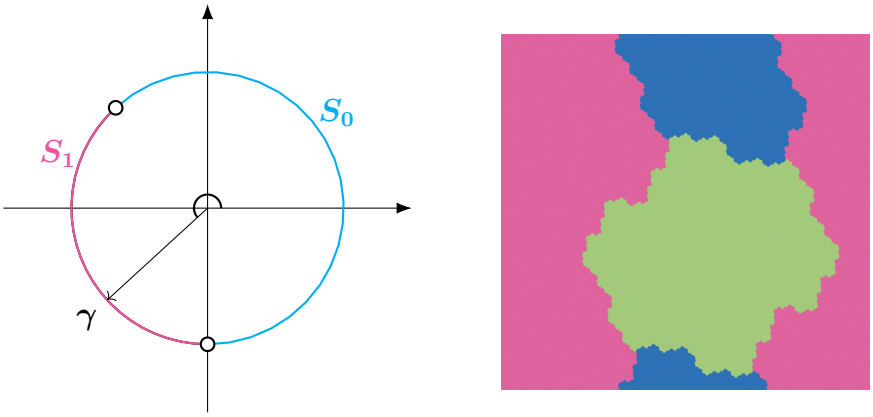

Figure 4.1: Target sets for the Fibonacci and Tribonacci words. On the right, the embeddings of $S_1, S_2, S_3 \subset \mathbb{T}^2$ into $[0,1)^2 \subset \mathbb{R}^2$ are depicted. Pink, green, and blue sets correspond to S_1, S_2, S_3, respectively.

The toric word α generated by $(\Gamma, \mathcal{S})$ is eventually toric with parameters $(\Gamma, 0, \mathcal{S})$. In fact, eventually toric words are the same as words with a toric suffix. To see this, let α be eventually toric with parameters $(\Gamma, N, \mathcal{S})$. Then $\beta := \alpha[N, \infty)$ is the toric word generated by $(\Gamma, \{\Gamma^{-N} S_\sigma : \sigma \in \Sigma\})$. Conversely, if $\alpha[N, \infty)$ is the toric word generated by $(\Gamma, \mathcal{S})$, then α is eventually toric with parameters $(\Gamma, N, \{\Gamma^N S_\sigma : \sigma \in \Sigma\})$.

In addition to their relevance to linear dynamical systems, (eventually) toric words appear frequently in the study of combinatorics on words. We next give a few examples.

(a) Recall that *sign pattern* α of a real-valued sequence $(u_n)_{n\in\mathbb{N}}$ is the infinite word over $\Sigma = \{+, 0, -\}$ such that $\alpha(n)$ corresponds to $\operatorname{sign}(u_n)$ for all n. Let $\gamma = e^{i\theta} \in \mathbb{T}$ be not a root of unity and consider the linear recurrence sequence

$$u_n = \gamma^n + \overline{\gamma^n} = 2\cos(n\theta).$$

By the assumption on γ, for all n, $u_n \neq 0$. Moreover, $u_n > 0$ if and only if $\operatorname{Log}(\gamma^n) \in (-\pi/2, \pi/2)$. Hence the sign pattern $\alpha \in \Sigma^\omega$ of $(u_n)_{n\in\mathbb{N}}$ is the toric word generated by $(\gamma, \{S_+, S_0, S_-\})$ where $S_+ = \{z \in \mathbb{T} : |\operatorname{Log}(z)| < \pi/2\}$, $S_0 = \emptyset$, and $S_- = \{z \in \mathbb{T} : |\operatorname{Log}(z)| > \pi/2\}$.

(b) Let $\Sigma = \{0, 1\}$ and consider the morphism $\tau : \Sigma^* \to \Sigma^*$ given by $\tau(0) = 01$ and $\tau(1) = 0$. Suppose we start with $w_0 = 0$ and iteratively apply the morphism τ to generate the sequence $w_{n+1} = \tau(w_n)$. In particular, $w_1 = \tau(w_0) = 01$, $w_2 = \tau(w_1) = 010$, $w_3 = \tau(w_2) = 01001$, and so on. We have that $w_n = \tau^n(u)$, and for all $k, n \in \mathbb{N}$, w_n is a prefix w_{n+k}. The limit word $\alpha_F = 01001010010\cdots$ that has every w_n as a prefix is the famous *Fibonacci word*. It has many equivalent

definitions, one of them as a toric word. Denote by $\varphi \approx 1.618$ the golden ratio and by $\Phi = \varphi - 1$ its multiplicative inverse, and let $\gamma = e^{\boldsymbol{i}2\pi/\varphi}$. The long-run ratio of zeros to ones in α_F is equal to $1/\Phi$, and α_F is the toric word generated by $(\gamma, \{S_0, S_1\})$ where S_0, S_1 are open interval subsets of $\mathbb{T}$ with lengths $2\pi/\varphi$ and $2\pi\Phi/\varphi$, respectively. See Figure 4.1.

(c) The *Tribonacci word* $\alpha_T = 121312112131\cdots$ is generated by iteratively applying the morphism $1\to 12$, $2 \to 13$, $3 \to 1$ to the starting letter 1. Let $\beta \approx 1.839$ be the real root of $x^3 - x^2 - x - 1$ and $\Gamma = (e^{\boldsymbol{i}2\pi/\beta}, e^{\boldsymbol{i}2\pi/\beta^2}) \in \mathbb{T}^2$. Rauzy [71] showed that the word α_T is, in fact, the toric word generated by $(\Gamma, \{S_1, S_2, S_3\})$ where S_1, S_2, S_3 have fractal boundaries. Figure 4.1 depicts the images of S_1, S_2, S_3 (pink, green, and blue sets, respectively) under the isomorphism $f\colon \mathbb{T}^2 \to [0,1)^2$ given by $f(z_1, z_2) = (g(z_1), g(z_2))$ where $g(z) = \frac{\mathrm{Log}(z)}{\boldsymbol{i}2\pi} + \frac{1}{2}$. The Fibonacci and Tribonacci words are examples of *morphic words*. Understanding which morphic words are also toric is one of the central problems in symbolic dynamics [15, 2].

Using the morphic and toric characterisations above, we can prove that the Tribonacci word is effectively almost-periodic. However, for toric words generated by $(\Gamma, \mathcal{S})$, where, for example, $\mathcal{S}$ has complicated (e.g. fractal) geometry, there is no general way to decide occurrence of a finite pattern, let alone prove effective almost periodicity. We will see that almost periodicity of arbitrary toric words, on the other hand, can be proven using topological arguments.

(d) A word α over the binary alphabet $\Sigma = \{0, 1\}$ is *Sturmian* if for every $n \in \mathbb{N}$, the number of distinct factors of α of length n is exactly $n + 1$. It is known that if a word has n or fewer distinct factors of length n for at least one value of n, then it must be ultimately periodic. Hence Sturmian words have the lowest possible factor complexity among words that are not ultimately periodic. We refer the reader to [4, Chapter 10.5] for a detailed introduction to Sturmian words. Each Sturmian word can be represented by two parameters $\gamma, \xi \in \mathbb{T}$, where γ is not a root of unity, as follows. For $z_1, z_2 \in \mathbb{T}$, denote by $J(z_1, z_2)$ the open interval subset of $\mathbb{T}$ obtained by starting at z_1 and rotating counter-clockwise until z_2 is reached. The Sturmian word α with parameters (γ, ξ) has the property that for all n, $\alpha(n) = 1$ if and only if $\gamma^n \in \{\xi\} \cup J(\xi, \xi\gamma)$.[1] In other words, a Sturmian word is the coding of $(\gamma^n)_{n\in\mathbb{N}}$, where γ is not a root of unity, with respect to two semi-open interval subsets I_0, I_1 of $\mathbb{T}$ such that $I_0 \cup I_1 = \mathbb{T}$ and the length of I_1

[1] Since $\gamma^n \in \{\xi\} \cup J(\xi, \xi\gamma)$ if and only if $\overline{\gamma^n} \in J(\overline{\xi\gamma}, \overline{\xi}) \cup \{\overline{\xi}\}$, we do not need to consider bothopen-closed and closed-open intervals separately when defining Sturmian words.

is exactly $|\operatorname{Log}(\gamma)|$. Since γ is not a root of unity, $\gamma^n = \xi$ holds for at most one value of n. Therefore, writing $S_0 = J(\xi\gamma, \xi)$ and $S_1 = J(\xi, \xi\gamma)$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, $\alpha(n) = 1$ if and only if $\gamma^n \in S_1$ and $\alpha(n) = 0$ if and only if $\gamma^n \in S_0$. That is, the Sturmian word α is eventually toric with parameters $(\gamma, N, \{S_0, S_1\})$.

Recall that the Model-Checking Problem is to decide, given a linear dynamical system (M, s), a collection of semialgebraic sets $\mathcal{T}$, and a deterministic Muller automaton $\mathcal{A}$, whether $\mathcal{A}$ accepts the characteristic word α of (M, s) with respect to $\mathcal{T}$. Throughout this thesis, our main way of showing that the Model-Checking Problem is decidable for a particular class of instances $\langle M, s, \mathcal{T}, \mathcal{A}\rangle$ is to show, using number-theoretic arguments, that the characteristic word α of (M, s) with respect to $\mathcal{T}$ is a merge (also known as an interleaving, see Section 1.8) of eventually toric words with semialgebraic parameters. In the remainder of this chapter we lay the foundations of this approach by showing that (eventually) toric words have strong closure and almost periodicity properties. This will allow us to apply algorithms for model checking effectively almost-periodic words based on Semënov's theorem (Chapter 3) to model checking toric characteristic words of linear dynamical systems. Our main results are summarised below.

(A) In Section 4.2 we will prove that a merge of eventually toric words (with semialgebraic parameters) is itself eventually toric (with semialgebraic parameters). This is in contrast to the more general class of almost-periodic words, which is not closed under merges [64]. We mention that closure under merges and effective almost periodicity imply decidability of the MSO theory of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_m\rangle$, where each $P_i \colon \mathbb{N} \to \{0, 1\}$ is a predicate whose characteristic word is eventually toric with semialgebraic parameters. We discuss this result in Section 4.3.

(B) Let α be eventually toric with parameters $(\Gamma, N, \mathcal{S})$. By a simple topological argument it can be shown that α is almost-periodic (Theorem 4.3.1 and corollary 4.3.2). If Γ has algebraic entries and each $S_\sigma \in \mathcal{S}$ is semialgebraic, then the same proof shows effective almost periodicity of α. The topological approach, however, is not fully constructive in the sense that it does not give us any *a priori* bounds on the gaps between occurrences of a finite word u in α. In Section 4.3 we use a quantitative version of Kronecker's theorem to give a bound on the window function $\mathcal{W}_\alpha(l)$ for α that is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$ in terms of l, N and (the description lengths) of $\Gamma, \mathcal{S}$. Such a result is necessary to produce upper bounds on the complexity of our model-checking algorithms.

(C) In Section 4.4 using Baker's theorem we give specialised bounds on $\mathcal{W}_\alpha(l)$ for α that is eventually toric with parameters $(\Gamma, N, \mathcal{S})$ where $\Gamma \in \mathbb{T}$. Eventually toric words of this kind arise in the low-dimensional instances of the Model-Checking Problem considered in Chapters 5 and 6.

(D) In Chapter 7 we will prove that the characteristic word α of a diagonalisable LDS with respect to a collection $\mathcal{T}$ of semialgebraic targets is eventually toric with semialgebraic parameters $(N, \Gamma, \mathcal{S})$, where Γ and $\mathcal{S}$ can be computed effectively given $M, s, \mathcal{T}$, but the value of N is ineffective. In Section 4.3 we will show that even though we do not have access to the value of N, we can still establish an upper bound on $\mathcal{W}_\beta(l)$ for all $l \in \mathbb{N}$, where $\beta = \alpha[N, \infty)$. This result plays a vital role in the algorithm of Chapter 7 for model checking characteristic words of diagonalisable LDS against *prefix-independent* properties.

4.1 Orbits in $\mathbb{T}^d$

Toric words arise from discrete-time dynamical systems on the torus $\mathbb{T}^d$ whose dynamics is given by $z \to \Gamma z$ for $\Gamma \in \mathbb{T}^d$. In order to understand patterns occurring in toric words, we have to understand the time steps at which the orbit $\mathcal{O}(\Gamma) \coloneqq (\Gamma^n)_{n\in\mathbb{N}}$ visits a given subset of $\mathbb{T}^d$. In this section we will show unlike the discrete orbit $\mathcal{O}(\Gamma)$, its Euclidean closure $\mathbb{T}_\Gamma \coloneqq \mathrm{Cl}(\mathcal{O}(\Gamma))$ is semialgebraic and effectively computable. Moreover, $\mathcal{O}(\Gamma)$ visits every open subset of $\mathbb{T}_\Gamma$ infinitely often.

The key to proving the aforementioned results is the notion of a *multiplicative relation*. We say that $(a_1, \ldots, a_d) \in \mathbb{Z}^d$ is multiplicative relation of $(z_1, \ldots, z_d) \in (\mathbb{C}^\times)^d$ if $z_1^{a_1} \cdots z_d^{a_d} = 1$. Given $z = (z_1, \ldots, z_d) \in (\mathbb{C}^\times)^d$,

$$G(z) \coloneqq \{(a_1, \ldots, a_d) \in \mathbb{Z}^d \mid z_1^{a_1} \cdots z_d^{a_d} = 1\}$$

is called the *group of multiplicative relations* of z. For all z, $G(z)$ is a free abelian group under addition with a basis containing at most d vectors from $\mathbb{Z}^d$. If the entries of z are all algebraic, then such a basis can be effectively computed using the following theorem due to Masser [59].

Theorem 4.1.1. *Let $\mathbb{K}$ be an algebraic number field of (finite) degree D, and $\gamma_1, \ldots, \gamma_d$ be non-zero elements of $\mathbb{K}$ of absolute logarithmic Weil height at most h. There exists an absolute constant c such that $G((\gamma_1, \ldots, \gamma_d))$ has a basis $v_1, \ldots, v_m \in \mathbb{Z}^d$ satisfying $m \leq d$ and for all $1 \leq i \leq m$,*

$$\|v_i\|_\infty < (cdh)^{d-1} D^{d-1} \frac{(\log(D+2))^{3d-3}}{(\log\log(D+2))^{3d-4}}.$$

We write $M(d, h, D)$ for the right-hand side of Masser's bound. Observe that the bound is on the *magnitude* of the entries in the basis as opposed to their bit length.

Corollary 4.1.2. *Given $\Gamma = (\gamma_1, \ldots, \gamma_d) \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$, a basis of $G(\Gamma)$ can be computed in polynomial space.*

Proof. Let $\mathbb{K} = \mathbb{Q}(\gamma_1, \ldots, \gamma_d)$, $D = [\mathbb{K} : \mathbb{Q}]$ and $h = \max_i h(\gamma_i)$. Since $h(\gamma_i) \leq \|\gamma_i\|$ for all $1 \leq i \leq d$ (see Section 1.5.1) and $D \leq \prod_{i=1}^{d} \deg(\gamma_i) \leq \|\Gamma\|^d$ by the Tower Law (Section 1.5.2), we have that $M(d, h, D) < \|\Gamma\|^{\textsc{Poly}(d)}$.

The algorithm starts with $B = \emptyset$ and constructs increasingly larger linearly independent (over $\mathbb{Z}$) subsets of $G(\Gamma)$. It enumerates all $v \in \mathbb{Z}^d$ such that

$$\|v\|_\infty < M(d, h, D).$$

The total description length of such v is at most $\textsc{Poly}(\|\Gamma\|)$. For each $v = (v_1, \ldots, v_d)$, the algorithm first determines whether $\gamma_1^{v_1} \cdots \gamma_d^{v_d} = 1$, i.e. whether $v \in G(\Gamma)$. Using iterative squaring[2] we can write a first-order sentence

$$\varphi \coloneqq \exists \mathbf{x} \in \mathbb{R}^l \colon \psi(\mathbf{x})$$

in the language $\mathcal{L}_{or}$, where l is some positive integer, such that $\|\varphi\|$ is polynomial in $\|\Gamma\|$, the formula ψ is quantifier-free, and φ holds if and only if $\gamma_1^{v_1} \cdots \gamma_d^{v_d} = 1$; see Section 1.5 for how to encode statements about arithmetic on algebraic numbers as first-order formulas. By Theorem 1.3.5, we can decide the truth of φ in space polynomial in $\|\Gamma\|$. If $v \in G(\Gamma)$, it remains to check whether $\{v\} \cup B$ is linearly independent and add v to B if this is the case. This can be done in polynomial time using, for example, the Hermite normal form [28, Section 2.4]. Once all candidate $v \in \mathbb{Z}^d$ have been enumerated, B is a basis of $G(\Gamma)$. □

In order to compute a representation of $\mathbb{T}_\Gamma$, we will use multiplicative relations in combination with Kronecker's theorem. For $x, y \in \mathbb{R}$, denote by $[\![x]\!]_y$ the distance from x to a nearest integer multiple of y. Further write $[\![x]\!]$ for $[\![x]\!]_1$. The following is a classical version of Kronecker's theorem (see, for example, [39]) in simultaneous Diophantine approximation.

[2]Iterative squaring refers to the following. Suppose we want to express $x^{12} = 1$ in first-order logic. We can do so using the formula $\exists x_2, x_4, x_8 \colon x_2 = x \cdot x \ \wedge\ x_4 = x_2 \cdot x_2 \ \wedge\ x_8 = x_4 \cdot x_4 \ \wedge\ x_8 \cdot x_4 = 1$. This way $x^n = 1$ can be expressed by a formula of size $\Theta(\log n)$, whereas $\underbrace{x \cdot \ldots \cdot x}_{12 \text{ times}} = 1$ has size $\Theta(n)$.

Theorem 4.1.3. *Let $x = (x_1, \ldots, x_d) \in \mathbb{R}^d$ and $y = (y_1, \ldots, y_d) \in \mathbb{R}^d$ be such that for all $b \in \mathbb{Z}^d$,*

$$b \cdot x \in \mathbb{Z} \quad \Rightarrow \quad b \cdot y \in \mathbb{Z}.$$

For every $\varepsilon > 0$ there exist infinitely many values $n \in \mathbb{N}$ satisfying

$$\sum_{j=1}^{d} [\![nx_j - y_j]\!] < \varepsilon.$$

Writing $X = (e^{\boldsymbol{i}2\pi x_1}, \ldots, e^{\boldsymbol{i}2\pi x_d})$ and $Y = (e^{\boldsymbol{i}2\pi y_1}, \ldots, e^{\boldsymbol{i}2\pi y_d})$, the condition that for all $b \in \mathbb{Z}^d$, $b \cdot x \in \mathbb{Z} \Rightarrow b \cdot y \in \mathbb{Z}$ is equivalent to $G(X) \subseteq G(Y)$. That is, "every multiplicative relation of X is also a multiplicative relation of Y". We can now prove the main result of this section.

Theorem 4.1.4. *Let $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$.*

(a) If $z \in \mathbb{T}^d$ is such that $G(\Gamma) \subseteq G(z)$, then for every open subset O of $\mathbb{T}^d$ containing z there exist infinitely many values $n \in \mathbb{N}$ such that $\Gamma^n \in O$.

(b) The set $\mathbb{T}_\Gamma$ is equal to $\{z \in \mathbb{T}^d \colon G(\Gamma) \subseteq G(z)\}$, semialgebraic, and computable in polynomial space given Γ.

Proof. Let $z = (z_1, \ldots, z_d)$ be such that $G(\Gamma) \subseteq G(z)$. Define $x_j = \frac{\operatorname{Log}(\gamma_j)}{\boldsymbol{i}2\pi}$ and $y_j = \frac{\operatorname{Log}(z_j)}{\boldsymbol{i}2\pi}$ for $1 \le j \le d$, noting that $x_j, y_j \in (-1/2, 1/2]$. For all $n \in \mathbb{N}$,

$$\begin{aligned}
\|\Gamma^n - z\|_1 &= \sum_{j=1}^{d} |\gamma_j^n - z_j| \\
&\le \sum_{j=1}^{d} |\operatorname{Log}(\gamma_j^n / z_j)| \\
&= \sum_{j=1}^{d} [\![n \operatorname{Log}(\gamma_j)/\boldsymbol{i} - \operatorname{Log}(z_j)/\boldsymbol{i}]\!]_{2\pi} \\
&= 2\pi \sum_{j=1}^{d} [\![nx_j - y_j]\!]
\end{aligned}$$

where the last equality follows from the fact that $[\![x]\!]_{2\pi} = 2\pi [\![x/(2\pi)]\!]$ for all $x \in \mathbb{R}$. Applying Kronecker's theorem, for each $\varepsilon > 0$ there exist infinitely many values n such that $\|\Gamma^n - z\|_1 < \varepsilon$. This proves (a).

To prove (b), let $B = \{v_1, \ldots, v_m\}$ be a basis of $G(\Gamma)$ where $1 \le m \le d$. As discussed earlier, such basis can be computed in polynomial space given Γ. For $1 \le k \le m$, write $v_k = (v_{k,1}, \ldots, v_{k,d})$. Since for all $z = (z_1, \ldots, z_d)$

$$G(\Gamma) \subseteq G(z) \quad \Leftrightarrow \quad \bigwedge_{k=1}^{m} z_1^{v_{k,1}} \cdots z_d^{v_{k,d}} = 1,$$

the set $\{z \in \mathbb{T}^d \colon G(\Gamma) \subseteq G(z)\}$ is closed and semialgebraic. It moreover contains the orbit $\mathcal{O}(\Gamma)$ as $G(\Gamma) \subseteq G(\Gamma^n)$ for all $n \in \mathbb{N}$. Finally, by (a) the orbit $\mathcal{O}(\Gamma)$ is dense in $\{z \in \mathbb{T}^d \colon G(\Gamma) \subseteq G(z)\}$. Hence the latter must be exactly the closure of $\mathcal{O}(\Gamma)$. □

4.2 Closure properties of eventually toric words

Let $\alpha_r \in \Sigma_r^\omega$ for $0 \leq r < L$. Recall that the product word $\alpha = \alpha_0 \times \cdots \times \alpha_{L-1}$ is defined by $\alpha(n) = (\alpha_0(n), \ldots, \alpha_{L-1}(n))$. We next show that eventually toric words (with semialgebraic parameters) are closed under products.

Lemma 4.2.1. *Let $\alpha_r \in \Sigma_r^\omega$ for $0 \leq r < L$ be eventually toric with parameters $(\Gamma_r, N_r, \mathcal{S}_r)$, and $\alpha = \alpha_0 \times \cdots \times \alpha_{L-1} \in \Sigma^\omega$, where $\Sigma = \Sigma_0 \times \cdots \times \Sigma_{L-1}$.*

(a) The word α is eventually toric.

(b) If each $(\Gamma_r, N_r, \mathcal{S}_r)$ is semialgebraic, then α is also eventually toric with semialgebraic parameters.

Proof. Suppose for all $0 \leq r < L$, $\Gamma_r \in \mathbb{T}^{d_r}$ and $\mathcal{S}_r$ is of the form $\{S_\sigma^{(r)} \colon \sigma \in \Sigma_r\}$, and let $d = d_0 + \ldots + d_{L-1}$. Define $\Gamma = (\Gamma_0, \ldots, \Gamma_{L-1}) \in \mathbb{T}^d$. The word α is eventually toric with parameters $(\Gamma, N, \{S_\sigma \colon \sigma \in \Sigma\})$ where $N = \max_r N_r$ and $S_\sigma = \prod_{r=0}^{L-1} S_{x_r}^{(r)}$ for all $\sigma = (x_0, \ldots, x_{L-1})$. This proves (a). To prove (b), observe that if $\Gamma_r \in (\mathbb{T} \cap \overline{\mathbb{Q}})^{d_r}$ and $\mathcal{S}$ contains only semialgebraic sets for all $0 \leq r < L$, then $(\Gamma, N, \mathcal{S})$ is semialgebraic. □

Observe that if $N_r = 0$ for all r above, i.e. every α_r is toric, then $N = 0$ and α is also toric. We next show that eventually toric words are closed under renamings of letters, a straightforward property that will later be useful.

Lemma 4.2.2. *Let Σ, Π be alphabets, $\alpha \in \Sigma^\omega$ be eventually toric with parameters $(\Gamma, N, \{S_\sigma \colon \sigma \in \Sigma\})$, and $f \colon \Sigma \to \Pi$. Consider $\beta \in \Pi^\omega$ defined by $\beta(n) = f(\alpha(n))$ for all $n \in \mathbb{N}$.*

(a) The word β is eventually toric with parameters $(\Gamma, N, \{\mathcal{K}_\pi \colon \pi \in \Pi\})$, where

$$\mathcal{K}_\pi = \bigcup_{\sigma \colon f(\sigma) = \pi} S_\sigma.$$

(b) If $(\Gamma, N, \mathcal{S})$ is semialgebraic, then so is $(\Gamma, N, \{\mathcal{K}_\pi \colon \pi \in \Pi\})$.

Recall that the *merge* (i.e. the interleaving) of $\alpha_0, \ldots, \alpha_{L-1}$ is defined by

$$\alpha(qL + r) \coloneqq \alpha_r(q)$$

for all $q, r \in \mathbb{N}$ with $0 \leq r < L$. In the remainder of this section we show that a merge of eventually toric words is eventually toric.

Theorem 4.2.3. *Let $L > 0$, and for $0 \leq r < L$, $\alpha_r \in \Sigma_r^\omega$ be an eventually toric word with parameters $(\Gamma_r, N_r, \mathcal{S}_r)$, where $\Gamma_r \in \mathbb{T}^{d_r}$. Write $d = d_0 + \ldots + d_{L-1}$ and $N = L \max_{0 \leq r < L} N_r$. Let α be the merge of $\alpha_0, \ldots, \alpha_{L-1}$.*

(a) There exist $\Gamma \in \mathbb{T}^{d+1}$ and $\mathcal{S}$ such that the word α is eventually toric with parameters $(\Gamma, N, \mathcal{S})$.

(b) Suppose $(\Gamma_r, N_r, \mathcal{S}_r)$ is semialgebraic for every $0 \leq r < L$. Write

$$\mathcal{I} = \sum_{r=0}^{L-1} \big(\|\Gamma_r\| + \|\mathcal{S}_r\| \big).$$

The word α is is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$, where $\|\mathcal{S}\| < \mathcal{I}^{\textsc{Poly}(d)}$ and $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^{d+1}$ with $\|\Gamma\| < \textsc{Poly}(\mathcal{I})$.

Observe that if $\alpha_0, \ldots, \alpha_{L-1}$ are all toric (i.e. $N_0 = \ldots = N_{L-1} = 0$), then $N = 0$ and hence α is also toric. To prove Theorem 4.2.3 we will need the following lemma.

Lemma 4.2.4. *Let $\Gamma = (\gamma_1, \ldots, \gamma_d) \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$, $S \subseteq \mathbb{T}^d$ be semialgebraic, and $k \in \mathbb{Z}$. We can compute a quantifier-free formula defining $\Gamma^k S$ in time $(|k| + \|\Gamma\| + \|S\|)^{\textsc{Poly}(d)}$.*

Proof. We define $\Gamma^k S$ via the characterisation

$$x \in \Gamma^k S \quad \Leftrightarrow \quad \Gamma^{-k} x \in S.$$

For $1 \leq j \leq d$, compute $\xi_j = \gamma_j^{-k}$. By Lemma 1.5.7, $\|\xi_j\| < \textsc{Poly}(\|\gamma_j\|, |k|)$. Let Φ be the quantifier-free formula (given as part of the input) defining S, and for $1 \leq j \leq d$, let φ_j be a quantifier-free formula of size at most $\textsc{Poly}(\|\xi_j\|)$ defining ξ_j (Lemma 1.5.3). Write $\mathbf{u}$ and $\mathbf{v}$ for the collections of variables $u_1, \ldots, u_d$ and $v_1, \ldots, v_d$, respectively. The variables u_j, v_j stand for $\mathrm{Re}(\xi_j)$ and $\mathrm{Im}(\xi_j)$, respectively. Let $r_j \coloneqq x_j u_j - y_j z_j$ and $c_j \coloneqq x_j v_j + y_j u_j$ for $1 \leq j \leq d$, where r_j, c_j are terms with free variables x_j, y_j, u_j, v_j. These represent respectively the real and imaginary parts of $(x_j + y_j \boldsymbol{i})(u_j + v_j \boldsymbol{i})$. The set $\Gamma^k S = \{x \colon \Gamma^{-k} x \in S\}$ is defined by the formula

$$\exists \mathbf{u}, \mathbf{v} \colon \bigwedge_{i=1}^{d} \varphi_j(u_j, v_j) \ \wedge \ \Phi(r_1, c_1, \ldots, r_d, c_d)$$

with free variables $x_1, y_1, \ldots, x_d, y_d$. Since the formula contains only existential quantifiers and $2d$ distinct variables in total, and is of size at most $\textsc{Poly}(|k|, \|\Gamma\|, \|S\|)$, an equivalent quantifier-free formula can be computed in time $(|k| + \|\Gamma\| + \|S\|)^{\textsc{Poly}(d)}$ by Theorem 1.3.5. □

We can now prove Theorem 4.2.3. Let $\Sigma = \Sigma_0 \cup \cdots \cup \Sigma_{L-1}$. For $0 \le r < L$, write $\mathcal{S}_r = \{S_\sigma^{(r)} \colon \sigma \in \Sigma_r\}$. That is, the open set in $\mathcal{S}_r$ corresponding to the letter $\sigma \in \Sigma_r$ is $S_\sigma^{(r)}$. Further let $S_\sigma^{(r)} = \emptyset$ for all $0 \le r < L$ and $\sigma \in \Sigma \setminus \Sigma_r$, and $\Lambda \in \mathbb{T}^d$ be the concatenation of $\Gamma_0, \ldots, \Gamma_{L-1}$ For all $0 \le r < L$ and $\sigma \in \Sigma$, define

$$\widetilde{S}_\sigma^{(r)} \coloneqq \prod_{j=0}^{r-1} \mathbb{T}^{d_j} \times S_\sigma^{(r)} \times \prod_{j=r+1}^{L-1} \mathbb{T}^{d_j}$$

and $\widetilde{\mathcal{S}}_r = \{\widetilde{S}_\sigma^{(r)} \colon \sigma \in \Sigma\}$. Each α_r, viewed as a word over the larger alphabet Σ, is eventually toric with parameters $(\Lambda, N_r, \widetilde{\mathcal{S}}_r)$. In particular, $\alpha_0, \ldots, \alpha_{L-1} \in \Sigma^\omega$ are all codings of the same rotation Λ.

Recall that $N = L \max_{0 \le r < L} N_r$. For $n \in \mathbb{N}$, define $q(n) = \lfloor n/L \rfloor$ and $r(n) = n - q(n)L$. By construction of α,

$$\alpha(n) = \sigma \quad \Leftrightarrow \quad \alpha_{r(n)}(q(n)) = \sigma$$

for all $\sigma \in \Sigma$ and $n \ge N$. To express α as an eventually toric word, our strategy will be to "slow down Λ by a factor of L" and "add a counter that counts modulo L". Let ω be a primitive Lth root of unity, and $B_0, \ldots, B_{L-1} \subset \mathbb{C}$ be disjoint semialgebraic open balls around $1, \omega, \ldots, \omega^{L-1}$, respectively. Write $\Lambda = (\gamma_1, \ldots, \gamma_d)$ and let $\xi_j = e^{\operatorname{Log}(\gamma_j)/L}$ for $1 \le j \le d$. Let $X = (\xi_1, \ldots, \xi_d)$, noting that for all $n \in \mathbb{N}$, $X^n = \Lambda^{q(n)} X^{r(n)}$. We can now define $\Gamma = (\omega, \xi_1, \ldots, \xi_L)$ and $\mathcal{S} \coloneqq \{S_\sigma \colon \sigma \in \Sigma\}$, where, for all $\sigma \in \Sigma$,

$$S_\sigma = \bigcup_{0 \le r < L} B_r \times X^r \widetilde{S}_\sigma^{(r)}.$$

For all $\sigma \in \Sigma$ and $n \ge N$,

$$\begin{aligned}
\Gamma^n \in S_\sigma &\Leftrightarrow \exists r \in \{0, \ldots, L-1\} \colon \omega^n \in B_r \ \wedge \ X^n \in X^r \widetilde{S}_\sigma^{(r)} \\
&\Leftrightarrow \Lambda^{q(n)} \in \widetilde{S}_\sigma^{(r(n))} \\
&\Leftrightarrow \alpha_{r(n)}(q(n)) = \sigma \\
&\Leftrightarrow \alpha(n) = \sigma.
\end{aligned}$$

Therefore, the word α is eventually toric with parameters $(\Gamma, N, \mathcal{S})$. This proves (a).

To prove (b), observe that under the assumptions that each $(\Gamma_r, N_r, \mathcal{S}_r)$ is semialgebraic, $(\Gamma, N, \mathcal{S})$ constructed above is semialgebraic. It remains to bound description

lengths of Γ and $\mathcal{S}$. For algebraic $\gamma \neq 0$, and $L > 0$, invoking Lemma 1.5.5 with $m = 0$ and $k = 1$, in time $\textsc{Poly}(\|\gamma\|, L) < \textsc{Poly}(\mathcal{I})$ we can compute a quantifier-free formula φ defining the finite set of all Lth roots of γ. Applying Lemma 1.5.6, entries of Γ can be computed in time $\textsc{Poly}(\|\Lambda\|, L) < \textsc{Poly}(\mathcal{I})$. By the same argument, canonical representations of $\omega^0, \ldots, \omega^{L-1}$ can be computed in time $\textsc{Poly}(\mathcal{I})$. We can then define B_r, also in polynomial time, as the open ball of radius $1/L$ around ω^r for $0 \leq r < L$. Finally, applying Lemma 4.2.4, for each $0 \leq r < L$ and $\sigma \in \Sigma$ we can compute $X^r \widetilde{S}_\sigma^{(r)}$ in time at most $(L + \|X\| + \|\mathcal{S}_r\|)^{\textsc{Poly}(d)}$. It follows that $\mathcal{S}$ can be computed in time $\mathcal{I}^{\textsc{Poly}(d)}$.

4.3 Almost-periodicity of toric words

Muchnik et al. [64] gave a topological proof that, under some assumptions, the coding of the trajectory of a compact dynamical system with respect to open sets is almost-periodic. We adapt their arguments to show almost periodicity of (eventually) toric words.

Theorem 4.3.1. *Let $\alpha \in \Sigma^\omega$ be the toric word generated by $(\Gamma, \mathcal{S})$, where $\Gamma \in \mathbb{T}^d$.*

(a) The word α is strongly almost-periodic.

(b) If $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ and $\mathcal{S}$ consists of semialgebraic sets, then α is strongly and effectively almost-periodic.

Proof. Let $u \in \Sigma^l$ be a word of length l. It occurs at the position n of α if and only if

$$\begin{aligned} \bigwedge_{k=0}^{l-1} \alpha(n+k) = u(k) &\Leftrightarrow \bigwedge_{k=0}^{l-1} \Gamma^{n+k} \in S_{u(k)} \\ &\Leftrightarrow \bigwedge_{k=0}^{l-1} \Gamma^n \in \Gamma^{-k} S_{u(k)} \\ &\Leftrightarrow \Gamma^n \in \bigcap_{k=0}^{l-1} \Gamma^{-k} S_{u(k)}. \end{aligned}$$

Recall that $\mathbb{T}_\Gamma \subseteq \mathbb{T}^d$ denotes the closure of $(\Gamma^n)_{n \in \mathbb{N}}$, and let

$$S_u = \mathbb{T}_\Gamma \cap \bigcap_{k=0}^{l-1} \Gamma^{-k} S_{u(k)}.$$

Observe that S_u is an open subset of $\mathbb{T}_\Gamma$. If S_u is empty, then u does not occur in α. Suppose therefore that S_u is non-empty. By Theorem 4.1.4, there exist infinitely

many $n \in \mathbb{N}$ such that $\Gamma^n \in S$. Hence u occurs infinitely often in α. We will show that the gaps between consecutive occurrences of u in α are bounded.

Consider $f\colon \mathbb{T}^d \to \mathbb{T}^d$, $f(z) = \Gamma^{-1}z$. We will prove that $\{f^k(S_u)\colon k \in \mathbb{N}\}$ is an open cover of $\mathbb{T}_\Gamma$. Let $z \in \mathbb{T}_\Gamma$. We need to show existence of $k \in \mathbb{N}$ such that $z \in f^k(S_u)$, i.e. $\Gamma^k z \in S_u$. Choose a point $y \in S_u$, and let ε be such that

$$\mathcal{B}(y, 2\varepsilon) \cap \mathbb{T}_\Gamma \subset \mathbb{T}_\Gamma$$

where $\mathcal{B}(y, 2\varepsilon)$ denotes the ℓ_2-ball of radius 2ε around y in $\mathbb{C}^d$. By Theorem 4.1.4 (a), there exist $n_1, n_2 \in \mathbb{N}$ such that $n_1 < n_2$, $\|\Gamma^{n_1} - z\|_2 < \varepsilon$ and $\|\Gamma^{n_2} - y\|_2 < \varepsilon$. Observe that $\|\Gamma^{n_1} - z\|_2 = \|\Gamma^{n_2} - \Gamma^{n_2-n_1}z\|_2$. Applying the triangle inequality, $\|\Gamma^{n_2-n_1}z - y\|_2 < 2\varepsilon$, i.e. $\Gamma^k z \in S_u$ where $k = n_2 - n_1$.

By compactness of $\mathbb{T}_\Gamma$, there exists K such that $\bigcup_{k=0}^K f^k(S_u)$ covers $\mathbb{T}_\Gamma$. It follows that for every $m \in \mathbb{N}$, there exists $n \in \{m, \ldots, m+K\}$ such that $\Gamma^n \in S_u$. Since u occurs at position n in α if and only if $\Gamma^n \in S_u$, we conclude that u occurs in every contiguous subword of α of length at least $K + l$. This proves (a).

It remains to prove that α is effectively almost-periodic assuming every $S \in \mathcal{S}$ is semialgebraic. Recall the programs $\mathcal{P}_1$ and $\mathcal{P}_2$ described in the definition of effective almost periodicity given on page 72.

(a) Given $n \in \mathbb{N}$, $\alpha(n)$ can be computed effectively by first computing the algebraic number Γ^n and then determining the unique semialgebraic $S \in \mathcal{S}$ containing Γ^n. This gives us $\mathcal{P}_1$.

(b) Given $u \in \Sigma^l$, the program $\mathcal{P}_2$ first computes (e.g. using tools of first-order logic) a formula defining S_u and checks the emptiness of the latter. If $S_u = \emptyset$, then it outputs $k_u = 0$, as the word u does not appear in α. Otherwise, the program computes a formula defining the semialgebraic set $\mathbb{T}_\Gamma$ (Theorem 4.1.4). Thereafter, it checks for increasing values of K whether $\bigcup_{k=0}^K f^k(S_u)$ covers $\mathbb{T}_\Gamma$. Since every $f^k(S_u)$ is semialgebraic, this step can also be implemented using first-order formulas. Once the value of K is found, the program outputs $k_u = K + l$: The word u occurs in every factor of α of length at least $K + l$. □

It follows that eventually toric words are almost-periodic. Note, however, that unlike toric words, eventually toric words need not be strongly almost periodic. For example, a finite word u can occur only once in an eventually toric word α but outside the toric suffix $\alpha[N, \infty)$, i.e. at a position $n \in \{0, \ldots, N-1\}$.

Corollary 4.3.2. *Let α be eventually toric with parameters $(\Gamma, N, \mathcal{S})$.*

(a) The word α is almost-periodic.

(b) If $(\Gamma, N, \mathcal{S})$ is semialgebraic, then α is effectively almost-periodic.

Proof. Recall that $\beta = \alpha[N, \infty)$ is the toric word generated by $(\Gamma, \{\Gamma^{-N} S_\sigma : \sigma \in \Sigma\})$. By Theorem 4.3.1 (a), the word β is almost-periodic. Since β is a suffix of α, the latter is also almost-periodic.

Now suppose $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ and $\mathcal{S}$ is a collection of semialgebraic sets. By Theorem 4.3.1 (a), the word β is effectively almost-periodic. To prove effective almost periodicity of α, we have to give the two programs $\mathcal{P}_1$ and $\mathcal{P}_2$ that compute $\alpha(n)$ on $n \in \mathbb{N}$ and k_u on $u \in \Sigma^*$, respectively.

(i) The program $\mathcal{P}_1$ simply stores the values of $\alpha(0), \ldots, \alpha(N-1)$, and on input $n \geq N$, returns the value of $\beta(n - N)$ using the respective program for β.

(b) On input $u \in \Sigma^l$, the program $\mathcal{P}_2$ first computes, using the respective program for β, a value k such that either u does not occur in $\beta[k, \infty)$, or it occurs in every factor of β of length k. Thereafter, $\mathcal{P}_2$ simply outputs $k_u = N + k$. □

The three facts that eventually toric words with semialgebraic parameters are effectively almost-periodic, closed under merges, and closed under products will play a critical role throughout this thesis in our decidability results for the Model-Checking Problem. Before that, let us briefly revisit decidability of the MSO theory (see Section 1.9) of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$, where each $P_i : \mathbb{N} \to \{0, 1\}$ is a unary predicate.

Theorem 4.3.3. *For $1 \leq i < m$, let α_i be eventually toric with semialgebraic parameters. Denote by β and γ the merge and the product of $\alpha_1, \ldots, \alpha_m$, respectively.*

(A) The Acceptance Problem is decidable for all of $\beta, \gamma, \alpha_1, \ldots, \alpha_m$.

(B) For $1 \leq r \leq m$, let $P_i : \mathbb{N} \to \{0, 1\}$ be defined by $P_i(n) = \alpha_i(n)$. The MSO theory of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ is decidable.

Proof. By Theorem 4.2.3 and lemma 4.2.1, the words β and γ are eventually toric with semialgebraic parameters. By Corollary 4.3.2, the words $\beta, \gamma, \alpha_1, \ldots, \alpha_m$ are effectively almost-periodic. To prove (A), recall that by Semënov's theorem, the Acceptance Problem is decidable for effectively almost-periodic words. To prove (B), recall from the Introduction that by Büchi's construction in [21], the MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ is decidable if and only if the Acceptance Problem is decidable for the word γ. □

Let α be eventually toric with parameters $(\Gamma, N, \mathcal{S})$, where $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ and $\mathcal{S}$ consists of semialgebraic sets. As mentioned earlier, the topological proofs of Theorem 4.3.1 and corollary 4.3.2 have the drawback that they not give us any *a priori* bounds on the gaps between consecutive occurrences of a finite word of length l in α in terms of $l, N, \|\Gamma\|$ and $\|\mathcal{S}\|$. We address this issue next.

In the proof of Theorem 4.1.4, we gave a trial-and-error procedure that computes a value K such that

$$\bigcup_{k=0}^{K} f^k(S_u) \supseteq \mathbb{T}_\Gamma,$$

where S_u is the semialgebraic set associated with the finite word u. That is, the procedure finds K such that for all $z \in \mathbb{T}_\Gamma$, there exists $0 \leq n \leq K$ such that $\Gamma^n z \in S_u$. We will show how to bound K in terms of the description length of S_u and $\|\Gamma\|$, which will then be used to prove the following. Recall that for an almost-periodic word α and $l \in \mathbb{N}$, $\mathcal{W}_\alpha(l)$ is the smallest integer m with the property that every $u \in \Sigma^l$ either does not occur in $\alpha[m, \infty)$, or occurs at least twice in every contiguous subword of α of length m.

Theorem 4.3.4. *Let $\alpha \in \Sigma^\omega$ be eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$, where $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$. Further let $\beta \coloneqq \alpha[N, \infty)$. Both α and β are effectively almost-periodic with*

$$\mathcal{W}_\beta(l) < 2^{(l+\|\Gamma\|+\|\mathcal{S}\|)^{\text{Poly}(d)}}$$

and $\mathcal{W}_\alpha(l) \leq N + \mathcal{W}_\beta(l)$ for all $l \in \mathbb{N}$.

We prove Theorem 4.3.4 in the remainder of this section. Once we establish almost periodicity of β and the bound on $\mathcal{W}_\beta(l)$, almost periodicity of α and the bound on $\mathcal{W}_\alpha(l)$ follow immediately. Hence we analyse β first. For $S \subseteq \mathbb{T}^d$ and $\Gamma \in \mathbb{T}^d$, define

$$\mathcal{R}(\Gamma, S) = \sup \{m \in \mathbb{N} \mid \exists n \in \mathbb{N}.\, \forall k \in \{n, \ldots, n+m-1\} \colon \Gamma^k \notin S\}.$$

Intuitively, $\mathcal{R}(\Gamma, S)$ is the largest number of steps it takes for a term of the sequence $(\Gamma^n)_{n\in\mathbb{N}}$ to reach S when we repeatedly apply the transformation $z \to \Gamma z$. We refer to $\mathcal{R}(\Gamma, S)$ as the *return time* of $(\Gamma^n)_{n\in\mathbb{N}}$ in S. Proving Theorem 4.3.4 amounts to proving a bound on $\mathcal{R}(\Gamma, S)$ for semialgebraic S and Γ with algebraic entries in terms of $\|\Gamma\|$ and $\|S\|$. We will do this in two steps. First we will analyse the case where S is an open ball. Thereafter we will show how to construct, given open semialgebraic S, an open ε-ball B contained in S. Since $S \supseteq B$ implies $\mathcal{R}(\Gamma, S) \leq \mathcal{R}(\Gamma, B)$, to bound $\mathcal{R}(\Gamma, S)$ it suffices to bound $\mathcal{R}(\Gamma, B)$.

Step 1. Bounding the return time in an ε-ball. Our main tool is the following quantitative version of Kronecker's theorem due to Chen [24, Special case of Theorem 1]. Recall that $[\![x]\!]$ denotes the distance from x to a nearest integer.

Theorem 4.3.5. *Let $x \coloneqq (x_1, \dots, x_d), y \coloneqq (y_1, \dots, y_d) \in (-1, 1)^d$ be such that $x \neq \mathbf{0}$ and for all $b \in \mathbb{Z}^d$, if $b \cdot x \in \mathbb{Z}$ then $b \cdot y \in \mathbb{Z}$. Further let $L, M \geq 2$ be integers. In any interval $I \subseteq \mathbb{R}_{>0}$ of length L there exists a natural number n such that*

$$\sum_{j=1}^{d} [\![nx_j - y_j]\!]^2 < \frac{d}{4} \sin^2\left(\frac{\pi}{2(M+1)}\right) + \frac{dM^d}{8\Lambda(M)L}$$

where $\Lambda(M) = \min\{[\![b \cdot x]\!] \colon b \in \mathbb{Z}^d,\ \|b\|_\infty < M,\ b \cdot x \notin \mathbb{Z}\}$.

See [39, Theorem 5.1] for a discussion of this theorem. Note that as $x \neq \mathbf{0}$ and $M \geq 2$, the quantity $\Lambda(M)$ is always finite. Writing $X = (e^{\boldsymbol{i}2\pi x_1}, \dots, e^{\boldsymbol{i}2\pi x_d})$ and $Y = (e^{\boldsymbol{i}2\pi y_1}, \dots, e^{\boldsymbol{i}2\pi y_d})$, Chen's theorem tells us that Y is an ω-limit point of $(X^n)_{n\in\mathbb{N}}$ assuming Y satisfies all multiplicative relations of X. We can use Chen's theorem as follows to construct $n \in \mathbb{N}$ such that the distance between X^n and Y is less than some $\varepsilon > 0$. First choose M such that $\frac{d}{4}\sin^2\left(\frac{\pi}{2(M+1)}\right) \ll \varepsilon$. Then compute $\Lambda(M)$ and choose L such that $\frac{dM^d}{8\Lambda(M)L} \ll \varepsilon$. Chen's theorem guarantees that for every $k \in \mathbb{N}$, there exists $n \in \{k, k+1, \dots, k+L-1\}$ such that X^n is ε-close to Y. The next lemma formalises this argument. We write $\mathcal{B}(z, \varepsilon)$ for the open ℓ_2-ball of radius ε around $z \in \mathbb{C}^d$.

Lemma 4.3.6. *Let $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ and $\varepsilon \in \mathbb{Q} \cap (0, 1)$. There exists an effectively computable integer $L(\varepsilon, \Gamma) < (2/\varepsilon)^{\textsc{Poly}(\|\Gamma\|)^d}$ with the following property. For every $z \in \mathbb{T}_\Gamma$ and $k \in \mathbb{N}$, there exists $k \leq n < k + L(\varepsilon, \Gamma)$ such that $\Gamma^n \in \mathcal{B}(z, \varepsilon)$.*

Proof. Write $\Gamma = (\gamma_1, \dots, \gamma_d)$ and $z = (z_1, \dots, z_d)$. If $\gamma_j = 1$ for all j, then $\mathbb{T}_\Gamma$ consists of a single point and the result is immediate. Otherwise, for $1 \leq j \leq d$, let $x_j = \frac{\operatorname{Log}(\gamma_j)}{\boldsymbol{i}2\pi}$ and $y_j = \frac{\operatorname{Log}(z_j)}{\boldsymbol{i}2\pi}$ for $1 \leq j \leq d$. Observe that $x_j, y_j \in (-1/2, 1/2]$ for all j, and $(x_1, \dots, x_d) \neq \mathbf{0}$. Similarly to the proof of Theorem 4.1.4,

$$\begin{aligned}
\|\Gamma^n - z\|_2^2 &= \sum_{j=1}^{d} |\gamma_j^n - z_j|^2 \\
&\leq \sum_{j=1}^{d} (\operatorname{Log}(\gamma_j^n / z_j))^2 \\
&= \sum_{j=1}^{d} [\![n \operatorname{Log}(\gamma_j)/\boldsymbol{i} - \operatorname{Log}(z_j)/\boldsymbol{i}]\!]_{2\pi}^2 \\
&= 4\pi^2 \sum_{j=1}^{d} [\![nx_j - y_j]\!]^2
\end{aligned}$$

for all $n \in \mathbb{N}$. By Chen's theorem, if we choose M, L such that

$$\frac{d}{4}\sin^2\left(\frac{\pi}{2(M+1)}\right) + \frac{dM^d}{8\Lambda(M)L} < \frac{\varepsilon^2}{4\pi^2}$$

then in every interval subset of $\mathbb{R}_{>0}$ of length L there exists n such that $\Gamma^n \in \mathcal{B}(z, \varepsilon)$. Since $\sin^2 x \leq x$ for non-negative x, it suffices to choose M, L such that both $\frac{d\pi}{8(M+1)}$ and $\frac{dM^d}{8\Lambda(M)L}$ are less than $\frac{\varepsilon^2}{8\pi^2}$. Therefore, applying Chen's theorem with

$$M = \left\lceil \frac{\pi^3 d}{\varepsilon^2} \right\rceil, \quad L = \left\lceil \frac{d\pi^2 M^d}{\Lambda(M)\varepsilon^2} \right\rceil$$

we have that any interval subset of $\mathbb{R}_{>0}$ of length L contains $n \in \mathbb{N}$ such that $\Gamma^n \in \mathcal{B}(z, \varepsilon)$. It remains to compute an upper bound $L(\varepsilon, \Gamma)$ on L in terms of $\|\Gamma\|$ and ε. To do this, we have to bound $\Lambda(M)$ from below.

Write $y = (y_1, \ldots, y_d)$. Since $|b \cdot x| < Md$ for every $b \in \mathbb{Z}^d$ with $\|b\|_\infty < M$, it holds that $\Lambda(M) = |c \cdot x - v|$ for some $c \in \mathbb{Z}^d$ and $v \in \mathbb{Z}$ satisfying $\|c\|_\infty < M$, $|v| \leq Md$, and $c \cdot x \neq v$. Writing $c = (c_1, \ldots, c_d)$,

$$\begin{aligned} |c \cdot x - v| &= |c_1 x_1 + \ldots + c_d x_d - v| \\ &= \left| \frac{c_1 \operatorname{Log}(\gamma_1)}{2\pi \boldsymbol{i}} + \ldots + \frac{c_d \operatorname{Log}(\gamma_d)}{2\pi \boldsymbol{i}} - v \right| \\ &= \frac{1}{2\pi} |c_1 \operatorname{Log}(\gamma_1) + \ldots + c_d \operatorname{Log}(\gamma_d) - 2v \operatorname{Log}(-1)|. \end{aligned}$$

Let $D < \|\Gamma\|^d$ be the degree of the number field $\mathbb{Q}(\gamma_1, \ldots, \gamma_d)$. Applying Baker's theorem (Section 2.6) with the bounds on $|v|$ and $|c_i|$ above,

$$|\Lambda(M)| = |c \cdot y - x| > e^{(-\log M) \cdot \textsc{Poly}(D, \|\Gamma\|)^d} = M^{-\textsc{Poly}(D, \|\Gamma\|)^d}.$$

Since $\varepsilon < 1$, from the choice of M, L it follows that exists effectively computable $L(\varepsilon, \Gamma) < (2/\varepsilon)^{\textsc{Poly}(\|\Gamma\|)^d}$ such that $L < L(\varepsilon, \Gamma)$. □

Step 2. Constructing an open ball inside an open semialgebraic set. Let $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$, $\Phi_1 \in \mathcal{L}_{or}$ be a quantifier-free formula defining $\mathbb{T}_\Gamma$, and S be an open semialgebraic subset of $\mathbb{T}_\Gamma$ defined by a quantifier-free formula $\Phi_2 \in \mathcal{L}_{or}$. Consider

$$R = \{\varepsilon > 0 \mid \exists z \in S\colon\ \mathcal{B}(z, \varepsilon) \cap \mathbb{T}_\Gamma \subset S\}$$

and define $\rho = \sup R$. The value 2ρ is the "diameter" of S inside $\mathbb{T}_\Gamma$. Intuitively, the larger this value, the more frequently $(\Gamma^n)_{n \in \mathbb{N}}$ visits S. We next argue that ρ is

algebraic and compute bounds on its magnitude. Write θ_1 and θ_2 for the collections of variables $x_1, y_1, \ldots, x_d, y_d$ and $u_1, v_1, \ldots, u_d, v_d$, respectively. The formula

$$\begin{aligned}\Psi_1(e) \coloneqq e > 0 \ \wedge \\ \exists \theta_1 \colon \Phi_2(\theta_1) \ \wedge \\ \forall \theta_2 \colon \Phi_1(\theta_2) \ \wedge \ \sum_{i=1}^{d} (u_i - x_i)^2 + (v_i - y_i)^2 < e^2 \Rightarrow \Phi_2(\theta_2)\end{aligned}$$

defines the set R. Hence ρ can be defined by the formula

$$\Psi_2(r) \coloneqq \forall e > 0, e \neq r \colon \Psi_1(e) \Leftrightarrow e < r.$$

By Theorem 4.1.4, $\|\Phi_1\| < \textsc{Poly}(\|\Gamma\|)$. Hence Ψ_2 has size $\textsc{Poly}(\|\Gamma\|, \|S\|)$, contains $O(d)$ distinct variables, and has bounded quantifier elimination. Invoking Theorem 1.3.5 an equivalent quantifier-free formula can be constructed in time $(\|\Gamma\| + \|S\|)^{\textsc{Poly}(d)}$. By Lemma 1.5.6, $\|\rho\| < (\|\Gamma\| + \|S\|)^{\textsc{Poly}(d)}$. Finally, from Lemma 1.5.1 we conclude that $\rho > 2^{-(\|\Gamma\|+\|S\|)^{\textsc{Poly}(d)}}$.

Proof of Theorem 4.3.4. We can now combine Steps 1 and 2 to finalise the proof. Write $\Gamma = (\gamma_1, \ldots, \gamma_d)$ and $\mathcal{S} = \{S_\sigma \colon \sigma \in \Sigma\}$. A finite word u of length l occurs at a position $n \geq N$ in α if and only if

$$\begin{aligned}\bigwedge_{k=0}^{l-1} \alpha(n+i) = u(k) \Leftrightarrow \bigwedge_{k=0}^{l-1} \Gamma^{n+k} \in S_{u(k)} \\ \Leftrightarrow \Gamma^n \in \bigcap_{k=0}^{l-1} \Gamma^{-k} S_{u(k)}.\end{aligned}$$

Let $S_u = \mathbb{T}_\Gamma \cap \bigcap_{k=0}^{l-1} \Gamma^{-k} S_{u(k)}$. By Theorem 4.1.4 and Lemma 4.2.4,

$$\|S_u\| < (l + \|\Gamma\| + \|\mathcal{S}\|)^{\textsc{Poly}(d)}.$$

If S_u is empty, then u does not appear in β, and hence $\mathcal{W}_\beta(u) = 0$. Suppose therefore that S_u is not empty. As discussed above, there exist $r > 2^{-(l+\|\Gamma\|+\|\mathcal{S}\|)^{\textsc{Poly}(d)}}$ and $z \in \mathbb{T}_\Gamma$ such that $\mathcal{B}(z, r) \cap \mathbb{T}_\Gamma \subseteq S_u$. By Lemma 4.3.6,

$$\mathcal{R}(\Gamma, \mathcal{B}(z, r)) < 2^{(l+\|\Gamma\|+\|\mathcal{S}\|)^{\textsc{Poly}(d)}}.$$

This bound applies to $\mathcal{R}(\Gamma, S_u)$ as well since $\mathcal{R}(\Gamma, \mathcal{B}(z, \varepsilon)) \leq \mathcal{R}(\Gamma, S_u)$. By the definition of the return time $\mathcal{R}(\cdot, \cdot)$, for every $n \geq N$ there exists $0 \leq k \leq \mathcal{R}(\Gamma, S_u)$

such that $\Gamma^{n+k} \in S_u$, i.e. the word u occurs in β at the position $n+k$. Hence u occurs at least twice in every subword of β of length at least $2\mathcal{R}(\Gamma, S_u) + 2l$. Therefore,

$$\mathcal{W}_\beta(u) \leq 2\mathcal{R}(\Gamma, S_u) + 2l < 2^{(l+\|\Gamma\|+\|\mathcal{S}\|)^{\text{POLY}(d)}}.$$

Recalling that $\mathcal{W}_\beta(l) = \max_{u\in\Sigma^l} \mathcal{W}_\beta(u)$, we have proven the desired bound on $\mathcal{W}_\beta(l)$. As mentioned earlier, the bound on $\mathcal{W}_\alpha(l)$ follows from the bound on $\mathcal{W}_\beta(l)$ and the definition of effective almost periodicity.

Model-checking eventually toric words with semialgebraic parameters. Recall from Corollary 3.1.4 that in order to decide whether a deterministic automaton $\mathcal{A}$ with the set of states Q accepts an effectively almost-periodic word α with a window function $\widetilde{\mathcal{W}}$, we need to compute up to $2H$ first letters of $\mathcal{A}(\alpha)$, where

$$H = 2\widetilde{\mathcal{W}}^{|Q|+1}(2m+1),$$

$m = \widetilde{\mathcal{W}}^{|Q|+1}(1)$ and $\mathcal{A}(\alpha)$ is the sequence of states obtained when $\mathcal{A}$ reads α. Suppose α is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$. With our bound on $\mathcal{W}_\alpha(l)$ from Theorem 4.3.4, the quantity H is non-elementary in terms of $\|\mathcal{A}\|+\|\Gamma\|+\|\mathcal{S}\|+N$, even if we fix the dimension d of Γ. As a result, the best complexity bound we can prove for deciding whether a given automaton accepts a given eventually toric word with semialgebraic parameters is TOWER. In the next section we will show that if we fix $d = 1$ (which, as it turns out, suffices for many of our purposes) then we can prove much better bounds on $\mathcal{W}_\alpha(l)$ compared to Theorem 4.3.4 using a specialised application of Baker's theorem.

4.4 Toric words generated by a one-dimensional rotation

When working with low-dimensional instances of the Model-Checking Problem, we will encounter a very specific scenario: we will need to decide whether a given deterministic automaton $\mathcal{A}$ accepts the merge α of eventually toric words $\alpha_0, \ldots, \alpha_{L-1}$ **all generated by the same one-dimensional rotation** $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$. That is, we have a single algebraic number γ of modulus one such that for all $0 \leq r < L$ and sufficiently large values of n, $\alpha_r(n)$ is the coding of γ^n with respect to some family of open semialgebraic subsets of $\mathbb{T}$. In this section, we will prove specialised bounds on $\mathcal{W}_\alpha(l)$ for eventually toric words of this kind. This will give us decision procedures with elementary complexity in the following two chapters. The key idea is that to analyse

$(\gamma^n)_{n\in\mathbb{N}}$ for $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$, we can employ Baker's theorem instead of Chen's quantitative version Kronecker's theorem, which produces much stronger bounds on the return time of $(\gamma^n)_{n\in\mathbb{N}}$ in semialgebraic $S \subset \mathbb{T}$.

By an interval subset of $\mathbb{T}$ we mean a set of the form $\{e^{iz} \mid z \in I\}$ where $I \subset \mathbb{R}$ is an interval. By an interval component of $S \subseteq \mathbb{T}$ we mean an interval $S_1 \subseteq S$ such that for any interval $S_2 \subseteq \mathbb{T}$, if $S_2 \supseteq S_1$ then $S_2 = S_1$. We next discuss how Baker's theorem can be used to bound return times of $(\gamma^n)_{n\in\mathbb{N}}$ in an interval subset of $\mathbb{T}$. Compare the following result to Lemma 4.3.6.

Lemma 4.4.1. *Let $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ be not a root of unity and J be an interval subset of $\mathbb{T}$ of length $|J| > 0$ For every $N \in \mathbb{N}$ there exists n satisfying*

$$N \leq n < N + \left(\frac{4\pi}{|J|}\right)^{\textsc{Poly}(\|\gamma\|)}$$

such that $\gamma^n \in J$.

Recall that $\textsc{Poly}(\cdot)$ stands for an absolute polynomial. Hence the exponent $\textsc{Poly}(\|\gamma\|)$ appearing above does not depend on J or N.

Proof. It suffices to prove the claim in case J is open. Let $l = \left\lfloor \frac{2\pi}{|J|} \right\rfloor$ and consider the intervals $\{J, \ldots, \gamma^l J\}$ on $\mathbb{T}$. Since $(l+1)|J| > 2\pi$, there exist $0 \leq m < s \leq l$ such that $\gamma^m J$ intersects $\gamma^s J$. Let $k = s - m$ and $\theta = |\operatorname{Log}(\gamma^k)|$. It holds that $0 \leq k \leq l$ and $\theta < |J|$. Since γ is not a root of unity, $\gamma^m \neq \gamma^s$ and hence $\theta > 0$. We next compute a lower bound on θ. Observe that $\theta > |\gamma^k - 1|$. Applying Lemma 2.6.3,

$$\theta > |\gamma^k - 1| > (\max\{2, k\})^{-\textsc{Poly}(\|\gamma\|)}.$$

Since $k \leq l < 4\pi/|J|$ and $2 \leq 4\pi/|J|$, we conclude that

$$\theta > (4\pi/|J|)^{-\textsc{Poly}(\|\gamma\|)}.$$

Let $L = \lceil 2\pi/\theta \rceil$. By the lower bound on θ above, $L < (4\pi/|J|)^{\textsc{Poly}(\|\gamma\|)}$.

Consider the sequence $(z_n)_{n\in\mathbb{N}}$ of points on $\mathbb{T}$ given by $z_n = \gamma^{N+kn}$. It holds that $z_{n+1} = \gamma^k z_n$ and hence $|z_{n+1} - z_n| < |J|$ for all n. Moreover, the finite sequence $\langle z_0, \ldots, z_L \rangle$ winds around $\mathbb{T}$ at least once. Hence there exists

$$0 \leq r < L$$

such that $z_r \in J$. That is, $\gamma^n \in J$ for $n = N + kr$. It remains to observe that $N \leq N + kr < N + kL$, and recall the bounds on k and L. □

We are now ready to prove the main result of this section. Compare the bound of the following theorem on $\mathcal{W}_\alpha$ with that of Theorem 4.3.4.

Theorem 4.4.2. *Let $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and for $0 \leq r < L$, $\alpha_r \in \Sigma_r^\omega$ be eventually toric with semialgebraic parameters $(\gamma, N_r, \mathcal{S}_r)$. Define $\mathcal{I} = \|\gamma\| + \sum_{r=0}^{L-1} \|\mathcal{S}_r\|$ and $N = \max_{0\leq r<L} N_r$. The merge α of $\alpha_0, \ldots, \alpha_{L-1}$ is effectively almost-periodic with*

$$\mathcal{W}_\alpha(l) \leq NL + l^{\textsc{Poly}(\mathcal{I})}$$

for $l > 1$.

Proof. Write $\mathcal{S}_r = \{S_\sigma^{(r)} \colon \sigma \in \Sigma_r\}$. That is, the open set in $\mathcal{S}_r$ corresponding to the letter σ is $S_\sigma^{(r)}$. For $n \in \mathbb{N}$, let $q(n) = \lfloor n/L \rfloor$ and $r(n) = n - q(n)L$. A letter σ appears at a position $n \geq NL$ of α if and only if

$$\alpha_{r(n)}(q(n)) = \sigma. \tag{4.2}$$

Since $q(n) \geq N_r$, Equation (4.2) holds if and only if $\gamma^{q(n)} \in S_\sigma^{r(n)}$. Note that if γ is a root of unity of order k, then $\mathbb{T}_\Gamma = \{1, \ldots, \gamma^{k-1}\}$. Otherwise, $\mathbb{T}_\Gamma = \mathbb{T}$.

Let u be a finite word of length $l > 1$. We have to show that $\mathcal{W}_\alpha(u) < NL + l^{\textsc{Poly}(\mathcal{I})}$. The word u appears at a position $n \geq NL$ in α if and only if

$$\begin{aligned}\bigwedge_{j=0}^{l-1} \alpha_{r(n+j)}(q(n+j)) = u(j) \;&\Leftrightarrow\; \bigwedge_{j=0}^{l-1} \gamma^{q(n+j)} \in S_{u(j)}^{(r(n+j))} \\ &\Leftrightarrow\; \gamma^{q(n)} \in \bigcap_{j=0}^{l-1} \gamma^{q(n)-q(n+j)} S_{u(j)}^{(r(n+j))}.\end{aligned}$$

For $n \in \mathbb{N}$, let $O_n = \bigcap_{j=0}^{l-1} \gamma^{q(n)-q(n+j)} S_{u(j)}^{(r(n+j))}$, which is an open and semialgebraic subset of $\mathbb{T}$. For all $j \in \mathbb{N}$ and $n_1, n_2 \in \mathbb{N}$ such that $n_1 \equiv n_2 \pmod{L}$, we have the equalities $q(n_1) - q(n_1 + j) = q(n_2) - q(n_2 + j)$ and $r(n_1 + j) = r(n_2 + j)$. Therefore, $O_{n_1} = O_{n_2}$ for such n_1, n_2. It follows that u appears at a position $n \geq N$ of α if and only if $\gamma^{q(n)} \in O_{r(n)}$. Hence it suffices to only consider $O_0, \ldots, O_{L-1}$.

If $O_r \cap \mathbb{T}_\Gamma$ is empty for all $0 \leq r < L$, then w does not appear in $\alpha[NL, \infty)$. Otherwise, suppose $0 \leq r < L$ is such that $O \coloneqq O_r \cap \mathbb{T}_\Gamma$ is non-empty. First consider the case where γ is a root of unity of order $k \geq 1$. There must exist $0 \leq m < k$ such that $\gamma^m \in O_r$. Therefore, u occurs in α at the position $(nk + m)L + r$ for all $n \in \mathbb{N}$. It is classical that the degree of kth primitive root of unity is exactly $\Phi(k) \geq \sqrt{k/2}$, where Φ denotes Euler's totient function. Hence $k \leq 2\deg(\gamma)^2 \leq 2\|\gamma\|^2$, and the required bounds on $\mathcal{W}_\alpha(u)$ and $\mathcal{W}_\alpha(l)$ follow.

Next, suppose γ is not a root of unity. If $O = \mathbb{T}$, then w occurs in α at all positions $n \equiv r (\mathrm{mod}\, L)$, and the bound on $\mathcal{W}_\alpha(u)$ follows. Suppose therefore $O \neq \mathbb{T}$. Since O is open and semialgebraic, it consists of finitely many disjoint open interval subsets of $\mathbb{T}$. Moreover, by construction, every boundary point of O is of the form $\gamma^{-k} z$ where $0 \leq k < l$ and z is a boundary point of some $S_\sigma^{(r)}$. We will next compute a lower bound on the length of an interval component of O.

Let $\varphi_\sigma^{(r)}$ be the quantifier-free formula defining $S_\sigma^{(r)}$, given as part of the input. For $0 \leq r < L$ and $\sigma \in \Sigma_r$, let $E_\sigma^{(r)} \coloneqq \partial S_\sigma^{(r)}$ be the finite set of boundary points of $S_\sigma^{(r)}$ in $\mathbb{T}$. The set $E_\sigma^{(r)}$ can be defined by the following formula with free variables x, y.

$$\begin{aligned} \forall \varepsilon.\, \exists x_1, x_2, y_1, y_2 \colon\, & (x - x_1)^2 + (y - y_1)^2 < \varepsilon \\ & \wedge\, (x - x_2)^2 + (y - y_2)^2 < \varepsilon \\ & \wedge\, \varphi_\sigma^{(r)}(x_1, y_1) \\ & \wedge\, \neg \varphi_\sigma^{(r)}(x_2, y_2). \end{aligned}$$

Eliminating quantifiers using Theorem 1.3.5, we obtain a representation of $E_\sigma^{(r)}$ with $\|E_\sigma^{(r)}\| < \textsc{Poly}(\mathcal{I})$. By Lemma 1.5.6, every $\alpha \in E_\sigma^{(r)}$ is algebraic with $\|\alpha\| < \textsc{Poly}(\mathcal{I})$. Define

$$E = \bigcup_{\substack{0 \leq r < L \\ \sigma \in \Sigma_r}} E_\sigma^{(r)}.$$

Recall that the endpoints of any interval component of O are of the form $\gamma^{-k} z$ for some $z \in E$ and $0 \leq k < l$. Let $\gamma^{-k_1} z_1, \gamma^{-k_2} z_2 \in E$ be two distinct endpoints of an interval component $I \subset \mathbb{T}$ of O. W.l.o.g. we can assume $k_2 \geq k_1$. Consider

$$\delta \coloneqq |\gamma^{k_1} z_1 - \gamma^{k_2} z_2| = |z_1 / z_2 - \gamma^{k_2 - k_1}|.$$

By Lemma 1.5.7, $\|z_1 / z_2\| < \textsc{Poly}(\mathcal{I})$. Since $k_2 - k_1 < l$, applying Lemma 2.6.3 yields

$$\delta > (\max\{2, l\})^{-\textsc{Poly}(\|\gamma\|)}.$$

By assumption, $l > 1$. Hence $\delta > l^{-\textsc{Poly}(\|\gamma\|)}$. We have thus proven that every interval component of O has length at least $l^{-\textsc{Poly}(\|\gamma\|)}$. Applying Lemma 4.4.1, for every $n \geq NL$ there exists $0 \leq k < l^{\textsc{Poly}(\mathcal{I})}$ such that $\gamma^{n+k} \in O$. It follows that $\mathcal{W}_{\alpha[NL,\infty)}(u) < l^{\textsc{Poly}(\mathcal{I})}$ and $\mathcal{W}_\alpha(u) < NL + l^{\textsc{Poly}(\mathcal{I})}$. □

Chapter 5

The Model-Checking Problem in dimension at most three

We will now use the theory of toric and effectively almost-periodic words that we have developed so far to prove decidability of the Model-Checking Problem for linear dynamical systems in ambient space $\mathbb{R}^d$ for $d \leq 3$. Our approach will be to show that the characteristic word α of such (M, s) with respect to any family of semialgebraic sets $\mathcal{T}$ is an interleaving of eventually toric words with semialgebraic parameters, all generated by the same $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$. From the results of Section 4.2 it follows that α itself is eventually toric with semialgebraic parameters and hence effectively almost-periodic. The restriction that $d \leq 3$ is crucial for a proof of this kind to be possible: In Chapter 8 we will construct $M \in \mathbb{Q}^{4\times 4}$, $s \in \mathbb{Q}^4$, and a collection $\mathcal{T}$ of semialgebraic sets such that the characteristic word of (M, s) with respect to $\mathcal{T}$ is not almost-periodic, which implies that it is not eventually toric either.

We can increase the dimension of an LDS freely by adding coordinates that are always zero. Suppose therefore that we are given $(M, s) \in \mathbb{Q}^{3\times 3} \times \mathbb{Q}^3$ and a collection $\mathcal{T}$ of semialgebraic subsets of $\mathbb{R}^3$. Denote by α the characteristic word of (M, s) with respect to $\mathcal{T}$. To prove eventual toricity of α, we will show that the sign pattern of the linear recurrence sequence $u_n = p(M^n s)$, where $p \in \mathbb{Q}[x_1, x_2, x_3]$, is an interleaving of eventually toric words and hence eventually toric. Such sequences can have arbitrarily large order and number of dominant roots, and therefore lie beyond the well-known classes of LRS for which the Skolem Problem (Section 2.3) and the Positivity Problem (Section 2.5) are known to be decidable. Nevertheless, we are able to apply Baker's theorem to analyse the sign pattern of $(u_n)_{n\in\mathbb{N}}$, exploiting the fact that eigenvalues of $(u_n)_{n\in\mathbb{N}}$ are multiplicatively generated by $\{\gamma, r_1, \ldots, r_m\}$ for some m, where $\gamma \in \overline{\mathbb{Q}} \cap \mathbb{T}$ and each r_i is real algebraic.

Once we have established the aforementioned properties of α, we can utilise the generic model-checking algorithm for eventually toric words with semialgebraic parameters (page 98) to verify properties of α. The result is the following conceptually simple algorithm. Given be $M \in \mathbb{Q}^{3\times 3}$, $s \in \mathbb{Q}^3$, a set of semialgebraic targets $\mathcal{T}$, and a deterministic automaton $\mathcal{A}$.

1. From $M, s, T, \mathcal{A}$, compute a large integer H.
2. Simulate $\mathcal{A}$ on α for the first $2H$ letters, and record the set S of states that occur in $\mathcal{A}(\alpha)[H, 2H)$.
3. The set of states appearing infinitely often in the run of $\mathcal{A}$ on α is exactly S. Check S against the acceptance condition of $\mathcal{A}$ to determine whether $\mathcal{A} \models \alpha$.

Write $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\| + \|\mathcal{A}\|$ for the total input length. The integer H above can be computed as $2^{2^{R(\mathcal{I})}}$ for an absolute polynomial $R \in \mathbb{Z}[x]$ that can be extracted from our proofs. That is, to compute H we only need to look at the input size. In Section 5.4 we will discuss two decision procedures with EXPSPACE complexity for the Model-Checking Problem in dimension at most three, one of them comprising exactly the steps (1-3) above.

We say that a linear dynamical system (M, s) is *non-degenerate* if all real eigenvalues of M are non-negative, and for any two distinct eigenvalues λ_1, λ_2, the ratio λ_1/λ_2 is not a root of unity. Compare this to the definition of non-degeneracy for linear recurrence sequences (page 46). We will first analyse (eventual) toricity of characteristic words of non-degenerate systems. In Sections 5.1 and 5.2 we prove the following.

Theorem 5.0.1. *Let $(M, s) \in \mathbb{Q}^{3\times 3} \times \mathbb{Q}^3$ be non-degenerate. There exists $\gamma \in \overline{\mathbb{Q}} \cap \mathbb{T}$ that only depends on M with the following properties.*

(a) A representation of γ can be computed in polynomial time given M.

(b) Let $\mathcal{T}$ be a set of semialgebraic targets, α be the characteristic word of (M, s) with respect to $\mathcal{T}$, and $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\|$. Given $M, s, \mathcal{T}$, in time $\textsc{Poly}(\mathcal{I})$ we can compute an integer N and a collection $\mathcal{S}$ of semialgebraic subsets of $\mathbb{T}$ such that α is eventually toric with semialgebraic parameters $(\gamma, N, \mathcal{S})$.

In Sections 5.3 and 5.4 we will show how to handle general matrices and give the model-checking procedure. The results of this chapter illustrate all important aspects of how we prove decidability of various subclasses of the Model-Checking Problem throughout this thesis.

5.1 Non-degenerate M with a non-real eigenvalue

In this section we prove Theorem 5.0.1 for non-degenerate $M \in \mathbb{Q}^3$ with a non-real eigenvalue. We begin by analysing sequences of the form $u_n \coloneqq p(M^n s)$ where p is a polynomial with rational coefficients. The lemma below shows that if this sequence is not identically zero, then for sufficiently large values of n, the sign of u_n can be determined from γ^n, where $\gamma = \lambda/|\lambda|$ for an eigenvalue λ of M.

Lemma 5.1.1. *Let $M \in \mathbb{Q}^{3\times 3}$ be non-degenerate with non-real eigenvalues $\lambda, \overline{\lambda}$ and real eigenvalue $\rho > 0$. Further let $s \in \mathbb{Q}^3$ and $p \in \mathbb{Q}[x_1, x_2, x_3]$. Write $\gamma = \lambda/|\lambda|$ and $\mathcal{I}$ for the total input size $\|M\| + \|s\| + \|p\|$. Either $p(M^n s) = 0$ for all $n \in \mathbb{N}$, or there exist open semialgebraic $S \subseteq \mathbb{T}$ and $N \in \mathbb{N}$, both computable in time $\textsc{Poly}(\mathcal{I})$, with the following properties.*

(a) For all $n \geq N$, $p(M^n s) \neq 0$.

(b) For all $n \geq N$, $p(M^n s) > 0 \Leftrightarrow \gamma^n \in S$.

Proof. Since M is non-degenerate, $(\lambda/\overline{\lambda})^k = \gamma^k \neq 1$ for all non-zero $k \in \mathbb{Z}$. Hence γ is not a root of unity. Let $\mathbb{K} = \mathbb{Q}(\lambda, \overline{\lambda}, \rho, |\lambda|)$ and $D = [\mathbb{K} : \mathbb{Q}]$. Since $\deg(\lambda), \deg(\rho) \leq 3$ and $\deg(|\lambda|) < \textsc{Poly}(\deg(\lambda))$, the degree D is bounded above by an absolute constant that does not depend on M. All algebraic numbers we will need are elements of $\mathbb{K}$.

Let $u_n = p(M^n s)$. Since M is diagonalisable, we can apply Lemma 2.2.5 with $d = 3$ to compute in time polynomial in $\mathcal{I}$ the representation

$$u_n = \sum_{j=1}^{A} h_j(\lambda, \overline{\lambda}, \rho)\Lambda_j^n \tag{5.1}$$

where $\Lambda_1, \ldots, \Lambda_A$ are non-zero and pairwise distinct, $h_j \in \mathbb{Q}[x_1, x_2, x_3]$, and $h_j(\lambda, \overline{\lambda}, \rho)$ is non-zero for all j. If $A = 0$, then $p(M^n s)$ is identically zero, and we are done. Suppose therefore $A \geq 1$. Observe that $\lambda = |\lambda|\gamma$ and $\overline{\lambda} = |\lambda|\gamma^{-1}$. Since each entry of M^n is linear in $\lambda^n, \overline{\lambda^n}, \rho^n$, for all $1 \leq j \leq A$,

$$\Lambda_j = \lambda^{k_{j,1}}\overline{\lambda}^{k_{j,2}}\rho^{k_{j,3}}$$

where $k_{j,1}, k_{j,2}, k_{j,3} \in \mathbb{N}$ and $k_{j,1} + k_{j,2} + k_{j,3} \leq \deg(p)$. Hence $\Lambda_j = r_j\gamma^{k_j}$ where $k_j = k_{j,1} - k_{j,2}$ with $|k_j| \leq \deg(p)$ and $r_j = \rho^{k_{j,3}}|\lambda|^{k_{j,1}+k_{j,2}} > 0$ is real algebraic. Applying Corollary 1.5.8 and Lemma 1.5.10, every r_j can be computed in time polynomial in $\mathcal{I}$. We have thus shown that u_n is of form $q(\gamma^n, \gamma^{-n}, r_1^n, \ldots, r_A^n)$ for a polynomial q with algebraic coefficients.

Let $R = \max_{1 \leq j \leq A} r_j$, $\mathcal{D} = \{j \colon r_j = R\}$ and $\mathcal{R} = \{j \colon r_j < R\}$. Consider the sequence $v_n \coloneqq p(M^n s)/R^n$. Clearly, $(v_n)_{n \in \mathbb{N}}$ and $(u_n)_{n \in \mathbb{N}}$ have identical sign patterns. Moreover,

$$v_n = \underbrace{\sum_{j \in \mathcal{D}} h_j(\lambda, \overline{\lambda}, \rho) \gamma^{k_j n}}_{d_n} + \underbrace{\sum_{j \in \mathcal{R}} h_j(\lambda, \overline{\lambda}, \rho) \gamma^{k_j n} \left(\frac{r_j}{R}\right)^n}_{r_n}. \tag{5.2}$$

Here d_n is the *dominant* part of v_n, since all eigenvalues of $(d_n)_{n \in \mathbb{N}}$ have modulus exactly one, whereas the eigenvalues of $(r_n)_{n \in \mathbb{N}}$, if any, have modulus less than one. Our approach will be to show existence of N such that for $n \geq N$, $|d_n|$ is much larger than $|r_n|$ and hence the sign of $p(M^n s)$ can be recovered from the sign of d_n.

Consider $w_n \coloneqq \gamma^{n \deg(p)} d_n$. Observe that $|w_n| = |d_n|$ for all n. Since $|k_j| \leq \deg(p)$ for all $j \in \mathcal{D}$, we have that $w_n = q(\gamma^n)$ for a non-zero polynomial $q \in \overline{\mathbb{Q}}[x]$ of degree at most $2 \deg(p)$ whose non-zero coefficients are of the form $h_j(\lambda, \overline{\lambda}, \rho)$ for some $1 \leq j \leq A$. Applying Lemma 2.6.4 with $m = 3$, there exist $N_1, C < \textsc{Poly}(\mathcal{I})$ computable in time $\textsc{Poly}(\mathcal{I})$ such that for all $n \geq N_1$,

$$|w_n| = |d_n| > n^{-C}.$$

Let us next consider

$$r_n = \sum_{j \in \mathcal{R}} h_j(\lambda, \overline{\lambda}, \rho) \gamma^{k_j n} \left(\frac{r_j}{R}\right)^n.$$

By Lemma 1.5.7 and corollary 1.5.8 we can compute canonical representations of algebraic numbers $h_j(\lambda, \overline{\lambda}, \rho)$, r_j/R and $|r_j/R|$ in time $\textsc{Poly}(\mathcal{I})$. Let $R_1 = \max_{j \in \mathcal{R}} |r_j/R|$. Applying Lemma 2.4.1, there exists $K < 2^{\textsc{Poly}(\mathcal{I})}$ computable in time $\textsc{Poly}(\mathcal{I})$ such that

$$|r_n| < K R_1^n$$

for all n. It remains to compare this to the lower bound on $|d_n|$ above. Since $\|r_j/R\| < \textsc{Poly}(\mathcal{I})$ for all j, by Lemma 1.5.1

$$1 - R_1 > 2^{-\textsc{Poly}(\mathcal{I})}.$$

Applying Lemma 2.4.3, in time $\textsc{Poly}(\mathcal{I})$ we can compute an integer $N \geq N_1$ such that for all $n \geq N$,

$$|d_n| > n^{-C} > K R_1^n > |r_n|.$$

Recall from Lemma 2.2.3 that since u_n is a real-valued LRS, the summands of the exponential polynomial in Equation (5.1) are closed under conjugation. Since the magnitudes of z and $\overline{z}$ are equal for all $z \in \mathbb{C}$, the summands of both d_n and r_n in Equation (5.2) are also closed under conjugation. Hence both $(d_n)_{n \in \mathbb{N}}$ and $(u_n)_{n \in \mathbb{N}}$

are real-valued LRS, although unlike $(u_n)_{n\in\mathbb{N}}$, they need not to take values in $\mathbb{Q}$. It follows that for $n \geq N$, $v_n \neq 0$ and $\operatorname{sign}(v_n) = \operatorname{sign}(d_n)$.

So far we have constructed integer N such that for $n \geq N$, $p(M^n s) \neq 0$ and $p(M^n s) > 0 \Leftrightarrow f(\gamma^n) > 0$, where

$$f(z) = \sum_{j\in\mathcal{D}} h_j(\lambda, \overline{\lambda}, \rho) z^{k_j n} \in \mathbb{R}.$$

We can therefore define $S = \{z \in \mathbb{C} \colon f(z) > 0\} \cap \mathbb{T}$. Applying Lemma 1.5.5 with $m = 3$ and $k = 1$, a representation of S can be computed in time polynomial in $\mathcal{I}$. □

Let (M, s) be as in the statement of Lemma 5.1.1, and $\mathcal{T}$ be a set of semialgebraic subsets of $\mathbb{R}^3$. We can already prove that the characteristic word of (M, s) with respect to $\mathcal{T}$ is eventually toric with semialgebraic parameters, which is essentially the statement of Theorem 5.4.2, using the closure properties of such words studied in Chapter 4. Let $p_1, \ldots, p_K \in \mathbb{Q}[x_1, x_2, x_3]$ be polynomials defining $\mathcal{T}$, and for $1 \leq i \leq K$, let $\alpha_i \in \{+, 0, -\}^\omega$ be the sign pattern of the LRS $p(M^n s)$. By Lemma 5.1.1, each α_i is eventually toric with semialgebraic parameters $(\gamma, N_i, \mathcal{S}_i)$ for some N_i and $\mathcal{S}_i$. The characteristic word α of (M, s) with respect to $\mathcal{T}$ is the result fo applying a renaming $f \colon \{+, 0, -\}^K \to 2^{\mathcal{T}}$ to the product word $\alpha_1 \times \cdots \times \alpha_K$. Applying Lemmas 4.2.1 and 4.2.2, and noting that every α_i is the coding of the same rotation γ, we conclude that α is eventually toric with semialgebraic parameters $(\gamma, N, \mathcal{S})$ for some N and $\mathcal{S}$.

In order to accurately keep track of complexity bounds, we will prove Theorem 5.4.2 for (M, s) with a non-real eigenvalue directly, rather than using the argument above based on closure under products and renamings. First we lift the statement of Lemma 5.1.1 to semialgebraic sets defined by more than one polynomial inequality.

Lemma 5.1.2. *Let M, s, λ be as in the statement of Lemma 5.1.1, $\gamma = \lambda/|\lambda|$, and $T \subseteq \mathbb{R}^3$ be semialgebraic. Denote by $\mathcal{I}$ the total input size $\|M\| + \|s\| + \|T\|$. In time $\textsc{Poly}(\mathcal{I})$ we can compute $N(T) \in \mathbb{N}$ and open semialgebraic $S(T) \subseteq \mathbb{T}$ such that for all $n \geq N(T)$, $M^n s \in T$ if and only if $\gamma^n \in S(T)$.*

Proof. Let $\psi(x_1, x_2, x_3)$ be the quantifier-free input formula defining T. Applying Theorem 1.3.5, in polynomial time we can compute

$$\varphi(x_1, x_2, x_3) \coloneqq \bigwedge_{i\in I} \bigvee_{j\in J} p_{i,j}(x_1, x_2, x_3) \; \Delta_{i,j} \; 0$$

equivalent to $\psi(x_1, x_2, x_3)$, where each $p_{i,j}$ is a polynomial with rational coefficients.[1] By multiplying the inequalities through -1 when necessary, we can assume that $\Delta_{i,j} \in \{\geq, >, =\}$ for all i, j. For every i, j, perform the following.

(1) Using Lemmas 2.2.1 and 2.2.5 check in polynomial time whether $p_{i,j}(M^n s)$ is identically zero.

(2) If $p_{i,j}(M^n s)$ is identically zero, define $N_{i,j} = 0$ and

$$S_{i,j} = \begin{cases} \mathbb{T} & \text{in case } \Delta_{i,j} \in \{\geq, =\}, \\ \emptyset & \text{otherwise.} \end{cases}$$

(3) If $p_{i,j}(M^n s)$ is not identically zero, apply Lemma 5.1.1 to compute in time $\textsc{Poly}(\mathcal{I})$ open semialgebraic $S_{i,j} \subseteq \mathbb{T}$ and a time bound $N_{i,j}$ such that for all $n \geq N_{i,j}$, $p_j(M^n s) \neq 0$ and

$$p_{i,j}(M^n s) > 0 \Leftrightarrow \gamma^n \in S_{i,j}.$$

We have that for all i, j and $n \geq N_{i,j}$, the inequality $p_{i,j}(x_1, x_2, x_3)\ \Delta_{i,j}\ 0$ holds if and only if $\gamma^n \in S_{i,j}$. Moreover, each $S_{i,j}$ is an open subset fo $\mathbb{T}$. It remains to define $N(T) \coloneqq \max_{i,j} N_{i,j}$ and

$$S(T) \coloneqq \bigcap_{i \in I} \bigcup_{j \in J} S_{i,j}$$

which can be computed in time $\textsc{Poly}(\mathcal{I})$. □

We can now prove Theorem 5.0.1 in case M has non-real eigenvalues $\lambda, \overline{\lambda}$ and a real eigenvalue ρ. Let $\gamma = \lambda/|\lambda|$, which can be computed in polynomial time given M using the results of Section 1.5.4. Write $\mathcal{T} = \{T_1, \ldots, T_\ell\}$. For each letter $\sigma \in 2^{\mathcal{T}}$, define $X_\sigma = \bigcap_{i=1}^{\ell} Y_i$, where

$$Y_i = \begin{cases} T_i & \text{if } T_i \in \Sigma, \\ \mathbb{R}^3 \setminus T_i & \text{otherwise.} \end{cases}$$

Observe that each X_σ is semialgebraic and computable in polynomial time. Moreover, for all $n \in \mathbb{N}$, $\alpha(n) = \sigma$ if and only if $M^n s \in X_\sigma$. Apply Lemma 5.1.2 to each X_σ to compute in polynomial time integer N_σ and semialgebraic $S_\sigma \subset \mathbb{T}$ such that for all $n \geq N$, $M^n s \in X_\sigma$ if and only if $\gamma^n \in S_\sigma$. Taking $N = \max_{\sigma \in \Sigma} N_\sigma$, the word α is eventually toric with parameters $(\gamma, N, \{S_\sigma : \sigma \in \Sigma\})$.

[1] Here we used the quantifier elimination algorithm to transform ψ, which was already quantifier-free, into the desired shape in conjunctive normal form.

5.2 Non-degenerate M with only real eigenvalues

In this section let $M \in \mathbb{Q}^{3\times 3}$ be non-degenerate with real eigenvalues ρ_1, ρ_2, ρ_3, and $s \in \mathbb{Q}^3$ be a starting point. Recall from the definition of non-degeneracy (page 103) that each ρ_i must be non-negative. We will show that the characteristic word α of the orbit $(M^n s)_{n\in\mathbb{N}}$ with respect to any collection $\mathcal{T}$ of semialgebraic sets is ultimately constant.

Lemma 5.2.1. *Let T be a semialgebraic set and $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\|$. In time $\textsc{Poly}(\mathcal{I})$ we can compute integer N such that either $M^n s \in T$ for all $n \geq N$, or $M^n s \notin T$ for all $n \geq N$.*

Proof. Let $\varphi(x_1, x_2, x_3)$ be the input quantifier-free formula defining T. Apply Theorem 1.3.5 to compute in polynomial time equivalent formula

$$\bigvee_{i\in I} \bigwedge_{k\in K} q_{i,k}(x_1, x_2, x_3)\ \Delta_{i,k}\ 0$$

in the disjunctive normal form. Fix $i \in I$ and $k \in K$. By Lemma 2.2.4, in time $\textsc{Poly}(\|M\| + \|s\| + \|p\|) < \textsc{Poly}(\mathcal{I})$ we can compute the exponential polynomial

$$f(n) \coloneqq \sum_{j=1}^{A} p_j(n) r_j^n$$

such that $f(n) = q_{i,k}(M^n s)$ for $n \geq 3$. Recall that $r_1, \ldots, r_A$ are non-zero and pairwise distinct, and each p_j is a non-zero polynomial. Each p_j will, in fact, have real algebraic coefficients. This can be seen by writing $M^n = P^{-1} J^n P$, where J is in real Jordan form, and invoking uniqueness of the exponential polynomial solution (Theorem 2.2.2). Since each r_j is of the form $\rho_1^a \rho_2^b \rho_3^c$ for $a, b, c \in \mathbb{N}$, $r_j \geq 0$. Applying Lemma 2.4.4 to $f(n)$, in time $\textsc{Poly}(\mathcal{I})$ we can compute an integer $N_{i,k}$ and $\Delta \in \{>, =, <\}$ such that for all $n \geq N_{i,k}$, $q_{i,k}(M^n s)\ \Delta\ 0$. It remains to apply this to every $q_{i,k}$ for $i \in I, k \in K$, and take $N = \max_{i,k} N_{i,k}$. □

To prove Theorem 5.0.1 for M with only real eigenvalues, first recall from page 107 that for each letter $\sigma \in \Sigma$ in polynomial time we can compute semialgebraic X_σ such that $\alpha(n) = \sigma \Leftrightarrow M^n s \in X_\sigma$ for all n. Applying the lemma above, for each X_σ there exists N_σ, computable in polynomial time, such that either $M^n s \in X_\sigma$ for all $n \geq N_\sigma$, or $M^n s \notin X_\sigma$ for all $n \geq N_\sigma$. Writing $N = \max_{\sigma\in\Sigma} N_\sigma$, therefore, $\alpha[N, \infty) = a^\omega$ for a letter $a \in \Sigma$. Equivalently, α is eventually toric with parameters $(\gamma, N, \mathcal{S})$ where $S_a = \mathbb{T}$, $S_\sigma = \emptyset$ for all $\sigma \neq a$, and γ can be taken to be 1 (or any other $z \in \mathbb{T} \cap \overline{\mathbb{Q}}$).

5.3 Handling degenerate instances

Recall that M is non-degenerate if

(a) all real eigenvalues of M are non-negative, and

(b) for any distinct eigenvalues λ_1, λ_2 of M, the ratio λ_1/λ_2 is not a root of unity.

We can eliminate degeneracy by raising the matrix M to a sufficiently large power. First, a lemma about roots of unity. For a root of unity z, write $\mathrm{ord}(z)$ for the smallest positive integer k such that $z^k = 1$.

Lemma 5.3.1. *Let $\mathbb{K}$ be a number field of degree D. Every root of unity in $\mathbb{K}$ has order at most $2D^2$.*

Proof. Let $z \in \mathbb{K}$ be a root of unity with $\mathrm{ord}(z) = k$. It is classical that

$$\deg(z) = \Phi(k) \geq \sqrt{k/2}$$

where Φ denotes Euler's totient function. Hence

$$k \leq 2\deg(z)^2 \leq 2D^2. \qquad \square$$

The main result of this section is the following.

Lemma 5.3.2. *For every $M \in \mathbb{Q}^{d\times d}$, there exists $L < 2^{\textsc{Poly}(d)}$ such that M^L is non-degenerate.*

Proof. Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of M, $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_d)$, and $D = [\mathbb{K} : \mathbb{Q}]$. By the Tower Law,

$$D \leq \prod_{1\leq i\leq d} \deg(\lambda_i) \leq d^d.$$

Let $\omega_{i,j} = \lambda_i/\lambda_j$ for $1 \leq i, j \leq d$, and define

$$k_{i,j} = \begin{cases} \mathrm{ord}(\omega_{i,j}) & \text{if } \omega_{i,j} \text{ is a root of unity,} \\ 1 & \text{otherwise.} \end{cases}$$

We can then take

$$L = 2\prod_{1\leq i,j\leq d} k_{i,j}.$$

Suppose λ_i^L/λ_j^L is a root of unity for some $1 \leq i, j \leq d$. Then λ_i/λ_j is also a root of unity, which, by construction of L, implies that $\lambda_i^L = \lambda_j^L$. Since the eigenvalues of M^L are exactly $\lambda_1^L, \ldots, \lambda_d^L$, and L is even, M^L is non-degenerate. It remains to bound the magnitude of L. By Lemma 5.3.1, $k_{i,j} \leq 2D^2$ for all i, j. Therefore, $L \leq 2(2D^2)^{d(d-1)/2} \leq 2^{\textsc{Poly}(d)}$. $\square$

Given (M, s), constructing non-degenerate LDS $(M^L, M^r s)$ for $0 \leq r < L$ is a recurring theme in analysis of linear linear dynamical systems. Observe that the orbit $(M^n s)_{n\in\mathbb{N}}$ of (M, s) is the merge of the orbits of $(M^L, s), \ldots, (M^L, M^{L-1}s)$. Hence, for example, if we could decide the Reachability Problem for non-degenerate LDS, then we could also decide the full Reachability Problem by reducing it to L instances involving non-degenerate LDS.

5.4 The model-checking algorithm

We are now ready to prove eventual toricity of the characteristic word and give the model-checking algorithm for three-dimensional linear dynamical systems. First, we will need a subroutine that, given (M, s), a collection of semialgebraic sets $\mathcal{T}$, and $n \in \mathbb{N}$, computes $\alpha(n)$, i.e. the set of targets $T \in \mathcal{T}$ such that $M^n s \in T$.

Lemma 5.4.1. *Given M and s with rational entries, $n \in \mathbb{N}$, and semialgebraic T, whether $M^n s \in T$ can be determined in $\textsc{Poly}(\|M\|, \|s\|, \|T\|, \log n)$ space.*

Proof. Denote by φ the quantifier-free formula defining T given as part of the input. Using iterative squaring,[2] we can write a sentence $\psi \in \mathcal{L}_{or}$ of the form $\exists x_1, \ldots, x_m \colon \mu(x_1, \ldots, x_m)$, where $m = O(\log n)$ and μ is quantifier-free, such that $\|\psi\| < \textsc{Poly}(\|M\|, \|s\|, \|T\|, \log n)$ and ψ holds if and only if $M^n s \in T$. It remains apply Theorem 1.3.5 to verify ψ. □

Our main result is as follows.

Theorem 5.4.2. *Let $d \leq 3$, $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ be a set of semialgebraic targets, $\Sigma = 2^{\mathcal{T}}$, and $\mathcal{A}$ be a deterministic automaton over Σ.*

- (✠) *The characteristic word α of (M, s) with respect to $\mathcal{T}$ is eventually toric with semialgebraic parameters.*
- (★) *It is decidable whether $\mathcal{A}$ accepts α, with complexity in* EXPSPACE.

Proof. If $d < 3$, then we can make the problem instance three-dimensional by adding one or two new coordinates. Suppose therefore $d = 3$, and write $\mathcal{I} \coloneqq \|M\| + \|s\| + \|\mathcal{T}\| + \|\mathcal{A}\|$. As discussed in Section 5.3, there exists $L < 2^{\textsc{Poly}(d)} < \textsc{Poly}(\mathcal{I})$ such that M^L is non-degenerate. We consider the family of non-degenerate systems

$$(M^L, s), (M^L, Ms), \ldots, (M^L, M^{L-1}s).$$

[2] See the footnote on page 86.

Denote the characteristic word of $(M^L, M^r s)$ with respect to $\mathcal{T}$ by α_r, and observe that $\|M^L\|, \|M^r s\| = \textsc{Poly}(\mathcal{I})$. Applying Theorem 5.0.1 to $(M^L, M^r s)$ for $0 \leq r < L$, in time $\textsc{Poly}(\mathcal{I})$ we can compute $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$, integers $N_0, \ldots, N_{L-1}$, and collections $\mathcal{S}_0, \ldots, \mathcal{S}_{L-1}$ of semialgebraic subsets of $\mathbb{T}$ such that each α_r is eventually toric with semialgebraic parameters $(\gamma, N_r, \mathcal{S}_r)$. From Theorem 4.2.3 it follows that α is also eventually toric with semialgebraic parameters, proving (✠).

Let $N = L \max_{0 \leq r < L} N_r$, observing that $N < 2^{\textsc{Poly}(\mathcal{I})}$. By Theorem 4.4.2, there exists an absolute polynomial P such that the word $\beta \coloneqq \alpha[N, \infty)$ is effectively almost-periodic with

$$\mathcal{W}_\beta(l) < l^{2^{P(\mathcal{I})}}$$

for $l \geq 2$. Since $\mathcal{W}_\beta(1) \leq \mathcal{W}_\beta(2)$,

$$\widetilde{\mathcal{W}}(l) = \begin{cases} 2^{2^{P(\mathcal{I})}}, & \text{if } l = 1, \\ l^{2^{P(\mathcal{I})}}, & \text{otherwise} \end{cases}$$

is an over-approximation of $\mathcal{W}_\beta(l)$, i.e. a window function for β. We mention that since $\beta = \alpha[N, \infty)$ and $N < 2^{\textsc{Poly}(\mathcal{I})}$, there exists an absolute polynomial $Q \in \mathbb{Z}[x]$ such that α is effectively almost-periodic with $\mathcal{W}_\alpha(l) < l^{2^{Q(\mathcal{I})}}$ for all $l \geq 2$.

Let q be the state of $\mathcal{A}$ after reading the first N letters of α, which can be determined in polynomial space by Lemma 5.4.1. Further let $\mathcal{B}$ be the deterministic automaton that has q as the start state and is identical to $\mathcal{A}$ otherwise. By construction, $\mathcal{A}$ accepts α if and only if $\mathcal{B}$ accepts β. Let

$$H = 2\widetilde{\mathcal{W}}^{|Q|+1}(2\widetilde{\mathcal{W}}^{|Q|+1}(1) + 1) < 2^{2^{\textsc{Poly}(\mathcal{I})}}. \tag{5.3}$$

By Theorem 3.1.3 and Corollary 3.1.4, the set of states that appear infinitely often in β is exactly the set of letters that appear in $w \coloneqq \mathcal{B}(\beta)[H, 2H)$. Applying Lemma 5.4.1, the set of states appearing in w can be determined in space $2^{\textsc{Poly}(\mathcal{I})}$, proving (★). □

The algorithm of Theorem 5.4.2 computes L, representations of eventually toric words α_r for $0 \leq r < L$, and so on. These are the steps that an efficient real-world implementation of the model-checking procedure would take. As mentioned in the introduction to this chapter, we can also give a simple alternative algorithm with the same worst-case complexity bound.[3] Let $d \leq 3$, $M \in \mathbb{Q}^{d \times d}$, $s \in \mathbb{Q}^d$, $\mathcal{T}$ be a set of semialgebraic subsets of $\mathbb{R}^d$, and $\mathcal{A}$ be a deterministic automaton. We showed in the

[3]The alternative algorithm we present is slightly more involved than the generic model-checking algorithm for toric words given on page 98, as the complexity bound for the latter on our problem instances is worse than EXPSPACE.

proof of Theorem 5.4.2 that there exists an absolute polynomial $Q \in \mathbb{Z}[x]$ such that the characteristic word α of (M, s) with respect to $\mathcal{T}$ is effectively almost-periodic with $\mathcal{W}_\alpha(l) < l^{2^{Q(\mathcal{I})}}$ for all $l \geq 2$. Define

$$f(l) = \begin{cases} 2^{2^{Q(\mathcal{I})}}, & \text{if } l = 1, \\ l^{2^{Q(\mathcal{I})}}, & \text{otherwise} \end{cases}$$

similarly to the proof of Theorem 5.4.2, and let $R \in \mathbb{Z}[x]$ be a polynomial such that

$$2f^n\left(2f^n\left(1\right) + 1\right) < 2^{2^{R(n)}}$$

for all $n \geq 1$, where $f^n(x)$ denotes $\underbrace{f(f(\cdots(f(x))))}_{n \text{ times}}$.[4] Observe that R is fully effective in the sense that it can be extracted from our results. Corollary 3.1.4 guarantees that a state of $\mathcal{A}$ is appears infinitely often in $\mathcal{A}(\alpha)$ if and only if it appears in $\mathcal{A}(\alpha)[H, 2H)$, where $H = 2^{2^{R(\mathcal{I})}}$ and $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\| + \|\mathcal{A}\|$. Hence in order to decide whether $\mathcal{A}$ accepts α, we can compute H, simulate $\mathcal{A}$ on α for $2H$ steps, record the set S of states appearing in $\mathcal{A}(\alpha)[H, 2H)$, and finally compare S against the acceptance condition of $\mathcal{A}$.

[4] Compare this with Equation (5.3), noting that for all inputs $M, s, \mathcal{T}, \mathcal{A}$, $|Q| + 1 < \mathcal{I}$ where Q is the number of states in $\mathcal{A}$.

Chapter 6

The Model-Checking Problem with tame targets

In this chapter we consider instances of the Model-Checking Problem where the semialgebraic target sets belonging to $\mathcal{T}$ have relatively simple geometry. We say that a semialgebraic set $T \subseteq \mathbb{R}^d$ is

(A) *low-dimensional* if it has semialgebraic dimension at most one, or is contained in a three-dimensional subspace of $\mathbb{R}^d$, and

(B) *tame* if it can be obtained from a set of low-dimensional sets through finitely many intersections, unions, and complements.

We will show that the Model-Checking Problem is decidable for arbitrary (M, s) assuming all targets in $\mathcal{T}$ are tame.

It will be more convenient to work with low-dimensional targets directly rather than with tame targets. Let (M, s) be a linear dynamical system, $\mathcal{T}_1$ be a set of tame targets and $\mathcal{A}_1$ be a deterministic automaton over $\Sigma_1 \coloneqq 2^{T_1}$. In Section 6.4 we will give an algorithm for computing a set $\mathcal{T}_2$ of low-dimensional targets from which every $T \in \mathcal{T}_1$ can be generated using the standard set operations. Let $\Sigma_2 \coloneqq 2^{\mathcal{T}_2}$, and denote by α_1, α_2 the characteristic words of (M, s) with respect to $\mathcal{T}_1$ and $\mathcal{T}_2$, respectively. We can construct a deterministic automaton $\mathcal{A}_2$ that accepts α_2 if and only if $\mathcal{A}_1$ accepts α_1. To do this, observe that there exists a renaming $f \colon \Sigma_2 \to \Sigma_1$ (that can be computed from the sequence of set operations on $\mathcal{T}_2$ that generate $\mathcal{T}_1$) such that for all $n \in \mathbb{N}$, $f(\alpha_2(n)) = \alpha_1(n)$. The automaton $\mathcal{A}_2$ has the same set of states as $\mathcal{A}_1$. Let p, q be two states, and $\sigma_1, \ldots, \sigma_k$ be all distinct labels of transitions from p to q in $\mathcal{A}_1$. In $\mathcal{A}_2$, the set of all labels of all transitions from p to q is $f^{-1}(\{\sigma_1, \ldots, \sigma_k\})$. We have thus reduced the MCP with tame targets to the MCP with low-dimensional

targets. Until Section 6.4 we will assume that we are given a set $\mathcal{T}$ of low-dimensional sets as part of the input when considering the MCP.

In the preceding chapter we saw that, for a three-dimensional linear dynamical system (M, s) and a set $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ of semialgebraic predicates, by understanding sufficiently well the time steps at which the orbit $(M^n s)_{n\in\mathbb{N}}$ visits every T_i (e.g. using toricity), we can model check the orbit of (M, s) against ω-regular properties over $\mathcal{T}$. We next illustrate how the low-dimensionality assumption on targets helps us obtain decidability results for arbitrary LDS in a similar way. For simplicity, let us restrict our attention to diagonalisable systems. For $(M, s) \in \mathbb{Q}^{3\times 3} \times \mathbb{Q}^3$, whether $M^n s \in T$ is determined by polynomial inequalities of the form $p(\lambda_1^n, \lambda_2^n, \lambda_3^n)\ \Delta\ 0$, where $\lambda_1, \lambda_2, \lambda_3$ are the eigenvalues of M. In other words, to understand reachability in T we have to understand sign patterns of linear recurrence sequences of the form $u_n = p(\lambda_1^n, \lambda_2^n, \lambda_3^n)$, with the restriction that $\Lambda \coloneqq \{\lambda_1, \lambda_2, \lambda_3\}$ is closed under Galois conjugation. LRS of this form are at the boundary of what we can handle: For example, deciding whether $u_n = p(\lambda_1^n, \lambda_2^n, \lambda_3^n)$ is ever zero without assuming closure of Λ under Galois conjugation is equivalent to the Skolem Problem at order 5, which is currently open.[1]

Now suppose $M \in \mathbb{Q}^{d\times d}$ is diagonalisable, and let $s \in \mathbb{Q}^d$, T be a one-dimensional semialgebraic target, and V be a three-dimensional subspace of $\mathbb{R}^d$. Since every semialgebraic set of dimension at most one is contained in a semialgebraic set of dimension exactly 1 (assuming $d > 0$), the sets T and V are prototypical "container" sets for low-dimensional targets. We can find $d - 1$ "independent" polynomials $p_1, \ldots, p_{d-1} \in \mathbb{Q}[x_1, \ldots, x_d]$ such that $x \in T$ if and only if $p_i(x) = 0$ for all i. In terms of the eigenvalues $\lambda_1, \ldots, \lambda_d$ of M, for all $n \in \mathbb{N}$,

$$M^n s \in T \ \Leftrightarrow \bigwedge_{i=1}^{d-1} h_i(\lambda_1^n, \ldots, \lambda_d^n) = 0$$

where each h_i has algebraic coefficients and satisfies $h_i(\lambda_1^n, \ldots, \lambda_d^n) = p_i(M^n s)$. Assuming $h_1, \ldots, h_{d-1}$ are also sufficiently "independent", for each $1 \le j < k \le d$ using variable elimination a polynomial q can be computed such that $M^n s \in T \Rightarrow q(\lambda_j^n, \lambda_k^n) = 0$. Hence we have to understand the zero terms of linear recurrence sequences of the form $u_n = q(\lambda_j^n, \lambda_k^n)$. This brings us back to the realm of LRS of low complexity that we can handle: Recall that we gave effective Skolem-Mahler-Lech theorems for sequences of the form $u_n = p(\alpha^n, \beta^n)$ and $u_n = p(n, \alpha^n)$, where $p \in \overline{\mathbb{Q}}[x_1, x_2]$, in Section 2.7.

[1] The only open case of the Skolem Problem at order 5 is $u_n = a\lambda^n + \overline{a}\,\overline{\lambda^n} + b\gamma^n + \overline{b}\,\overline{\gamma^n} + \rho^n$, where w.l.o.g. we can assume $|\lambda| = |\gamma| = 1$ and $|\rho| < 1$; see Section 2.3. Since $\overline{\lambda} = \lambda^{-1}$ and $\overline{\gamma} = \gamma^{-1}$, $v_n = \lambda^n \gamma^n u_n$ is of the form $p(\lambda^n, \gamma^n, \rho^n)$ for $p \in \overline{\mathbb{Q}}[x_1, x_2, x_3]$. Note that $u_n = 0 \Leftrightarrow v_n = 0$.

Bounds on the zeros of sequences of the latter type will be used when we perform the aforementioned variable elimination on non-diagonalisable systems.

Similarly, for the target V, for all $n \in \mathbb{N}$,

$$M^n s \in V \Leftrightarrow \bigwedge_{i=1}^{d-3} f_i(\lambda_1^n, \ldots, \lambda_d^n) = 0$$

where each f_i is a linear polynomial with algebraic coefficients. Eliminating variables carefully, we can compute $u_n = \sum_{i=1}^{4} c_i \lambda_i^n$ such that $(u_n)_{n\in\mathbb{N}}$ is a real-valued linear recurrence sequence, and $M^n s \in T \Rightarrow u_n = 0$ for all $n \in \mathbb{N}$, Since the Skolem Problem is known to be decidable for real algebraic LRS of order at most 4, zeros of $(u_n)_{n\in\mathbb{N}}$ can all be effectively determined.

In this chapter we will carry out the variable elimination described above to show that the characteristic word α of (M, s) with respect to a set $\mathcal{T}$ of tame predicates is eventually toric with semialgebraic parameters and hence effectively almost-periodic. We will move from $\mathbb{R}^d$ to $\mathbb{C}^d$ by taking the *complexification* of the semialgebraic target T, which is the smallest affine algebraic variety containing T. Thereafter we will use tools from first-order logic (see Section 1.3.2) to implement necessary procedures from algebraic geometry, most notable projections. In the end, we will have shown that characteristic words of LDS with respect to tame targets are not too different from characteristic words of three-dimensional systems, in the sense that α is again an interleaving of eventually toric words all generated by the same $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$. In Chapter 8 we will prove that the decidability results of this section are tight: For example, it will be shown that reachability problems for targets that have semialgebraic dimension two, or, for that matter, are contained in a four-dimensional subspace, subsume open cases of the Skolem and Positivity problems.

Just like in Chapter 5, our results in this chapter imply an algorithm of the following shape for deciding the Model-Checking Problem restricted to tame targets.

1. Given $M, s, T, \mathcal{A}$, compute a large integer H.

2. Denote by α the characteristic word of (M, s) with respect to $\mathcal{T}$. Simulate $\mathcal{A}$ on α for the first $2H$ letters, and record the set S of states that occur in $\mathcal{A}(\alpha)[H, 2H)$.

3. The set of states appearing infinitely often in the run of $\mathcal{A}$ on α is exactly S. Check S against the acceptance condition of $\mathcal{A}$.

In Section 6.4, we will give a more interpretable algorithm that behaves efficiently in various special cases.

Our plan for this chapter is as follows. In Section 6.1 we will discuss how to transform given (M, s) into a family of *full-dimensional* systems before deploying algebraic and semialgebraic geometry to carry out the variable elimination described above. This pre-processing step is necessary to deal with systems like

$$M = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad s = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

whose "true dimension" (in this case 2, as the last coordinate is always zero) is less than their syntactic dimension. In sections 6.2 and 6.3 we show that the characteristic word of a full-dimensional and non-degenerate system with respect to a single low-dimensional target is eventually toric. Finally, in Section 6.4 we bring everything together and give the model-checking algorithm.

6.1 Full-dimensional systems

We next define the notion of a full-dimensional linear dynamical system and show how to translate a given instance of the Model-Checking Problem to one involving only full-dimensional systems. Full-dimensional systems are free from various kinds of degenerate behaviour exhibited by general LDS.

6.1.1 The inherent linear dimension of an orbit

In this section let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ and $J = PMP^{-1}$ be in Jordan form with $J = \mathrm{diag}(J_1, J_2)$, where $J_i \in \overline{\mathbb{Q}}^{d_i \times d_i}$ for $i \in \{1, 2\}$, J_1 is invertible, and J_2 is nilpotent. Write $\tilde{s} \coloneqq Ps = (\tilde{s}_1, \tilde{s}_2)$ where each $\tilde{s}_i \in \overline{\mathbb{Q}}^{d_i}$.

We define

$$\dim(A, x) \coloneqq \dim_{\mathbb{R}}(\mathrm{span}_{\mathbb{R}}(\{x, Ax, A^2x, \ldots\}))$$

for any matrix A and vector x, both with complex entries. That is, $\dim(A, x)$ is the dimension of the smallest real vector space enclosing $(A^n x)_{n\in\mathbb{N}}$. We say that (A, x) *has stable dimension* if there exists μ such that for all $n \in \mathbb{N}$, $\dim(A, A^n x) = \mu$. Such a system is *full-dimensional* if μ is as large as possible, i.e. $A \in \mathbb{C}^{\mu\times\mu}$. Observe that if the matrix A is invertible, then (A, x) has stable dimension.

As the dimension of a vector space is preserved under invertible linear maps,

$$\dim(M, M^k s) = \dim(PM, PM^k s) = \dim(J, J^k \tilde{s})$$

for all $k \in \mathbb{N}$. Since J_1 is invertible $J_2^n = \mathbf{0}$ for $n \geq d$, both $(J, J^d\tilde{s})$ and $(M, M^d s)$ have stable dimension. That is, once we discard the first d terms of the orbit of (M, s), we obtain a new orbit that has stable dimension. The next lemma describes what happens when we combine discarding the prefix with taking subsequences.

Lemma 6.1.1. *Let $L > 0$. There exists $\mu \leq d$ such for all $0 \leq r < L$, $(M^L, M^{d+r}s)$ has stable dimension and $\dim(M^L, M^{d+r}s) = \mu$.*

Proof. By the observations above,

$$\dim(M^L, M^{d+r}s) = \dim(J^L, J^{d+r}\tilde{s}) = \dim(J_1^L, J_1^{d+r}\tilde{s})$$

for all $0 \leq r < L$. Because J_1^L is invertible, $(J_1^L, J_1^{d+r}\tilde{s})$ has stable dimension. Since J_1^r is invertible, $\dim(J_1^L, J_1^{d+r}\tilde{s}) = \dim(J_1^L, J_1^d\tilde{s}) = \dim(M^L, M^d s)$. Writing $\mu = \dim(M^L, M^d s)$, we have

$$\dim(M^L, M^{d+r}s) = \mu$$

for all $0 \leq r < L$. □

Given an LDS (M_1, s_1) with stable dimension and a set $\mathcal{T}_1$ of low-dimensional predicates, through a change of basis one can construct full-dimensional (M_2, s_2) and a new set of low-dimensional predicates $\mathcal{T}_2$ such that the characteristic word of (M_1, s_1) with respect to $\mathcal{T}_1$ is, up to a renaming of letters, the same as the characteristic word of (M_2, s_2) with respect to $\mathcal{T}_2$. Lemma 6.1.2 and corollary 6.1.3 show that when this is done simultaneously on L sub-orbits of (M, s), we can choose all L full-dimensional systems to be the same. Recall that e_k stands for the kth standard basis vector.

Lemma 6.1.2. *Let $L > 0$, $0 \leq r < L$, and $T \subseteq \mathbb{R}^d$ be low-dimensional. Write*

$$u_n = M^{nL+r+d}s = \left(M^L\right)^n M^{d+r}s.$$

In time $\textsc{Poly}(\mathcal{I})$, where $\mathcal{I} = \|M\| + \|s\| + \|T\| + L$, we can compute $\mu \leq d$, $R \in \mathbb{Q}^{\mu\times\mu}$, $t \in \mathbb{Q}^\mu$, and a low-dimensional semialgebraic set $\widetilde{T} \subseteq \mathbb{R}^\mu$ with the following properties.

(a) (R, t) only depends on M, L, s, and is full-dimensional.

(b) The eigenvalues of R form a subset of the eigenvalues of M^L.

(c) For all $n \in \mathbb{N}$,

$$u_n \in T \Leftrightarrow R^n t \in \widetilde{T}.$$

Proof. Applying Lemma 6.1.1, in time $\textsc{Poly}(\mathcal{I})$ we can compute $m \leq d$ such that both $(M^L, M^d s)$ and $(M^L, M^{d+r} s)$ have stable dimension with

$$\dim(M^L, M^{d+r} s) = \dim(M^L, M^d s) = m. \tag{6.1}$$

If $m = 0$, then choose $\mu = 1$, $R = [1]$, $t = 1$, and $\widetilde{T} = \{1\}$ if $\mathbf{0} \in T$ and $\widetilde{T} = \emptyset$ otherwise. Suppose $m > 0$, and let $\mu = m$. Since $\dim(M^L, M^{d+r} s) = \mu$ and M, s have rational entries, there exist $c_0, \ldots, c_{\mu-1} \in \mathbb{Q}$ such that $u_\mu = \sum_{i=0}^{\mu-1} c_i u_i$. We will need to understand rational linear dependence between consecutive terms of $(u_n)_{n\in\mathbb{N}}$. Define

$$v_n = M^{nL} M^d s.$$

It holds that $u_n = M^r v_n$ for all n. Let $k \geq 0$ and $b_0, \ldots, b_k \in \mathbb{Q}$. Since J_1 is invertible and $J_2^l = \mathbf{0}$ for $l \geq d$, for all $n \in \mathbb{N}$,

$$\begin{aligned}
\sum_{i=0}^{k} b_i u_{n+i} = \mathbf{0} &\Leftrightarrow \sum_{i=0}^{k} b_i J^{(n+i)L+r+d}\, \tilde{s} = \mathbf{0} \\
&\Leftrightarrow \sum_{i=0}^{k} b_i J_1^{(n+i)L+r+d}\, \tilde{s}_1 = \mathbf{0} \\
&\Leftrightarrow \sum_{i=0}^{k} b_i J_1^{iL+d}\, \tilde{s}_1 = \mathbf{0} \\
&\Leftrightarrow \sum_{i=0}^{k} b_i J^{iL+d}\, \tilde{s} = \mathbf{0} \\
&\Leftrightarrow \sum_{i=0}^{k} b_i v_i = \mathbf{0}.
\end{aligned}$$

In particular, for all $b_0, \ldots, b_k$ and $n, m \in \mathbb{N}$,

$$\sum_{i=0}^{k} b_i u_{n+i} = \mathbf{0} \Leftrightarrow \sum_{i=0}^{k} b_i u_{m+i} = \mathbf{0}.$$

Since $\dim(M^L, M^{d+r} s) = \dim_{\mathbb{R}} \{u_n : n \in \mathbb{N}\} = \mu$, we conclude that $\{u_0, \ldots, u_{\mu-1}\}$ is a basis of $U \coloneqq \operatorname{span}_{\mathbb{R}}\{u_n : n \in \mathbb{N}\}$, and $\{v_0, \ldots, v_{\mu-1}\}$ is a basis of $\operatorname{span}_{\mathbb{R}}\{v_n : n \in \mathbb{N}\}$. We next show how to compute the unique recurrence relation[2] $a = (a_0, \ldots, a_\mu) \in \mathbb{Q}^{\mu+1}$ such that $a_\mu = 1$ and $\sum_{i=0}^{\mu} a_i u_i = \mathbf{0}$. We will then use recurrence relation a to perform a change of basis and compute (R, t). The particular choice of a will be crucial to proving property (b). We make the following definitions.

[2]Sequences $(u_n)_{n\in\mathbb{N}}$ and $(v_n)_{n\in\mathbb{N}}$ are not linear recurrence sequences according to our definition: Recall that the terms of an LRS and the coefficients of a defining recurrence relation must belong to the same ring R.

(i) $\mathcal{R}_1 \coloneqq \bigcup_{k\in\mathbb{N}} \{(b_0,\ldots,b_k) \in \mathbb{Q}^{k+1} \mid \sum_{i=0}^{k} b_i \left(M^L\right)^i = \mathbf{0}\}$.

(ii) $\mathcal{R}_2 \coloneqq \bigcup_{k\in\mathbb{N}} \{(b_0,\ldots,b_k) \in \mathbb{Q}^{k+1} \mid \sum_{i=0}^{k} b_i u_i = \mathbf{0}\}$.

(iii) $\mathcal{R}_3 \coloneqq \bigcup_{k\in\mathbb{N}} \{(b_0,\ldots,b_k) \in \mathbb{Q}^{k+1} \mid \sum_{i=0}^{k} b_i v_i = \mathbf{0}\}$.

Recall that $\sum_{i=0}^{k} b_i u_i = \mathbf{0} \Leftrightarrow \sum_{i=0}^{k} b_i v_i = \mathbf{0}$. Hence $\mathcal{R}_2 = \mathcal{R}_3$, and we write $\mathcal{R} \coloneqq \mathcal{R}_3$. Observe that $\mathcal{R}_1 \subseteq \mathcal{R}$. We will show that both $\mathcal{R}$ and $\mathcal{R}_1$ are generated by a single recurrence relation.

Define $\varphi\colon \bigcup_{k\geq 1} \mathbb{Q}^k \to \mathbb{Q}[x]$ to be the bijection $(b_0,\ldots,b_{k-1}) \mapsto \sum_{i=0}^{k-1} b_i x^i$. Let $K = \varphi(\mathcal{R})$ and $K_1 = \varphi(\mathcal{R}_1)$. It can be verified directly that both K and K_1 are ideals of $\mathbb{Q}[x]$. Since every ideal of $\mathbb{Q}[x]$ is principal, there exist unique monic polynomials $p, p_1 \in \mathbb{Q}[x]$ such that K and K_1 are the principal ideals generated by p and p_1, respectively. The polynomial p_1 is the *minimal polynomial* of the matrix M^L, which is a factor of the characteristic polynomial of M^L. Since $K_1 \subseteq K$, the polynomial p must divide p_1 in $\mathbb{Q}[x]$. This will be the critical property for proving (b).

We are now ready to compute the polynomial p generating the ideal K and hence the desired recurrence relation $a \in \mathbb{Q}^{\mu+1}$. Since $L < \mathcal{I}$, we can compute M^L and $v_0,\ldots,v_\mu$ in time $\textsc{Poly}(\mathcal{I})$. Thereafter, in time polynomial in $\mathcal{I}$, using Gaussian elimination we can compute $a = (a_0,\ldots,a_\mu) \in \mathbb{Q}^d$ such that $a_\mu = 1$ and $\sum_{i=0}^{\mu} a_i v_i = \mathbf{0}$. In particular, $a \in \mathcal{R}$. Since $\{v_0,\ldots,v_{\mu-1}\}$ is a basis of $\operatorname{span}_{\mathbb{R}}\{v_n \colon n \in \mathbb{N}\}$, the lowest degree of a polynomial in the ideal K is μ. Hence there exists a unique monic polynomial $p \in K$ with $\deg(p) = \mu$. The polynomial p, moreover, generates K. Observe that $\varphi(a)$ is a monic polynomial of degree μ in K. Therefore, $\varphi(a) = p$. That is, $p(x) = \sum_{i=0}^{\mu} a_i x^i$ generates K.

By the earlier argument, $\sum_{i=0}^{\mu} a_i v_i = \mathbf{0}$ implies that $\sum_{i=0}^{\mu} a_i v_{n+i} = \mathbf{0}$ and hence $v_{n+\mu} = \sum_{i=0}^{\mu-1} -a_i v_{n+i}$ for all $n \in \mathbb{N}$. Since $\mathcal{R}_2 = \mathcal{R}_3$,

$$u_{n+\mu} = \sum_{i=0}^{\mu-1} -a_i u_{n+i}.$$

Writing $w_a = (-a_0,\ldots,-a_{\mu-1}) \in \mathbb{Q}^d$, we are thus led to defining $t = e_1$ and

$$R = [e_2 \ \cdots \ e_\mu \ w_a] \in \mathbb{Q}^{\mu\times\mu}.$$

Observe that $R^\top$ is the companion matrix of the recurrence relation $(-a_0,\ldots,-a_{\mu-1})$ defined in Section 2.1, and the characteristic polynomial of R is exactly p. Since p divides p_1, the eigenvalues of R form a subset of the eigenvalues of M. This proves (b).

Recall that $U = \operatorname{span}_{\mathbb{R}}\{u_n \colon n \in \mathbb{N}\}$ has $u_0, \ldots, u_{\mu-1}$ as a basis. Construct in time $\textsc{Poly}(\mathcal{I})$ change-of-basis matrices $\Pi \colon U \to \mathbb{R}^{\mu\times\mu}$ and $Y \colon \mathbb{R}^{\mu\times\mu} \to U$ such that $\Pi(u_k) = e_k$ for $0 \leq k < \mu$. For all $n \in \mathbb{N}$,

$$\Pi \cdot u_n = R^n t$$

for all n. It follows that for every $0 \leq r < L$ and $n \in \mathbb{N}$,

$$u_n \in T \;\Leftrightarrow\; R^n t \in \Pi \cdot (T \cap U).$$

Hence we can choose $\widetilde{T} \coloneqq \Pi \cdot (T \cap U)$, which is a low-dimensional semialgebraic set under the low-dimensionality assumption on T. This proves (c). To prove (a), first recall that $t = e_1$ and observe that R was constructed from $(v_n)_{n\in\mathbb{N}}$, which neither depends on the value of r nor on T. Full-dimensionality of (R, t) follows from the fact that R is invertible and

$$\dim_{\mathbb{R}}\{R^n t \mid n \in \mathbb{N}\} = \dim_{\mathbb{R}}\{u_n \mid n \in \mathbb{N}\} = \mu.$$

It remains to show how to compute a representation of $\widetilde{T}$ in polynomial time. Let φ be the quantifier-free formula defining T given as part of the input. It holds that $\widetilde{T} = \{x \in \mathbb{R}^{\mu\times\mu} \mid Yx \in T\}$. Write $b_k \in \mathbb{Q}^\mu$ for the kth row of Y for $1 \leq k \leq \mu$. The formula

$$\psi(\mathbf{x}) \coloneqq \varphi(b_1 \cdot \mathbf{x}, \ldots, b_\mu \cdot \mathbf{x}),$$

where $\mathbf{x} = (x_1, \ldots, x_\mu)$, defines $\widetilde{T}$. □

Corollary 6.1.3. *Let $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$ and $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ be a collection of semialgebraic sets in $\mathbb{R}^d$. Write*

$$\mathcal{I} = \|M\| + \|s\| + \|T\|.$$

In time $2^{\textsc{Poly}(\mathcal{I})}$ we can compute $L < 2^{\textsc{Poly}(\mathcal{I})}$, $\mu \leq d$, a non-degenerate and full-dimensional linear dynamical system $(R, t) \in \mathbb{Q}^{\mu\times\mu} \times \mathbb{Q}^\mu$, and low-dimensional semi-algebraic sets $T_i^{(r)} \subseteq \mathbb{R}^{\mu\times\mu}$ for $0 \leq r < L$ and $1 \leq i \leq \ell$ such that for every $n \geq 0$, $1 \leq i \leq \ell$ and $0 \leq r < L$,

$$M^{nL+r+d} s \in T_i \;\Leftrightarrow\; R^n t \in T_i^{(r)}.$$

Proof. Let $L < 2^{\textsc{Poly}(\mathcal{I})}$ be such that M^L is non-degenerate (Lemma 5.3.2). Apply Lemma 6.1.2 to M, L, r, T_i for every $0 \leq r < L$ and $T_i \in \mathcal{T}$. Observe that (R, t) is non-degenerate since every eigenvalue of R is also an eigenvalue of M^L. □

Consider $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ and a set of semialgebraic predicates $\mathcal{T} = \{T_1, \ldots, T_\ell\}$. Denote by α the characteristic word of (M, s) with respect to $\mathcal{T}$, and apply Corollary 6.1.3 to compute L, R, t, as well as the low-dimensional semialgebraic sets $T_i^{(r)}$ for $0 \leq r < L$ and $1 \leq i \leq \ell$. Let $\beta \coloneqq \alpha[d, \infty)$ and β_r for $0 \leq r < L$ be such that β is the merge of $\beta_0, \ldots, \beta_{L-1}$. Corollary 6.1.3 tells us that each β_r, up to a renaming of letters, is the characteristic word of (R, t) with respect to the collection $\{T_1^{(r)}, \ldots, T_\ell^{(r)}\}$ of low-dimensional targets. We will show in Sections 6.2 and 6.3 that each β_r is, in fact, eventually toric. Thereafter we will use the results of Chapter 4 to model check the words β and α.

Next we will show that for a full-dimensional system (M, s) im ambient space $\mathbb{R}^d$ with non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$, we can define a well-behaved map F such that $M^n s = F(n, \lambda_1^n, \ldots, \lambda_m^n)$ for all $n \geq d$. This will allow us to translate the condition $M^n s \in T$ for a semialgebraic target T into a system of inequalities in $n, \lambda_1^n, \ldots, \lambda_m^n$, which we will solve for n.

6.1.2 Expressing $M^n s$ as a function of $n, \lambda_1^n, \ldots, \lambda_m^n$

Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ be full-dimensional and $J = PMP^{-1}$ be in Jordan form, computed by some fixed algorithm.[3] Write $J = \operatorname{diag}(B_1, \ldots, B_m)$ as in Section 1.7, where each $B_k \in \overline{\mathbb{Q}}^{d_k \times d_k}$ is a Jordan block with the (only) eigenvalue λ_k. Recall that $m = 2l_1 + l_2$, the first $2l_1$ blocks of J all have a non-real eigenvalue, the remaining l_2 blocks have a real eigenvalue, and B_{2k} is the entrywise complex conjugate of B_{2k-1} for $1 \leq k \leq l_1$. Write $\tilde{s} \coloneqq Ps$ in the form $(\tilde{s}_1, \ldots, \tilde{s}_m)$, where $\tilde{s}_k \in \overline{\mathbb{Q}}^{d_k}$ for all k. Finally, write $\tilde{s}_k = (x_1^{(k)}, \ldots, x_{d_k}^{(k)})$ for $1 \leq k \leq m$. Our goal is to construct injective entrywise polynomial functions $f_{M,s}, F_{M,s}$ such that for all $n \in \mathbb{N}$,

$$M^n s = \begin{cases} f_{M,s}(\lambda_1^n, \ldots, \lambda_m^n) & \text{if } M \text{ is diagonalisable,} \\ F_{M,s}(n, \lambda_1^n, \ldots, \lambda_m^n) & \text{otherwise.} \end{cases} \tag{6.2}$$

Since (M, s) is full-dimensional, we have the following.

Lemma 6.1.4. *The matrix M is invertible. Moreover, for all $1 \leq k \leq m$, $x_{d_k}^{(k)} \neq 0$. That is, the last coordinate of each $\tilde{s}_k$ is non-zero.*

Proof. Recall that M is invertible if and only if $\lambda_1, \ldots, \lambda_m \neq 0$. We give a proof by contradiction. First suppose $x_{d_k}^{(k)} = 0$ or $\lambda_k = 0$ for some $k > 2l_1$. Then $e_K J^n \tilde{s}$ for

[3] We need the assumption that the algorithm be fixed to ensure that the functions $f_{M,s}$ and $F_{M,s}$, which depend on the particular choice of J in Jordan form, are uniquely defined.

$K = \sum_{i=1}^{k} d_i$ (i.e. the Kth coordinate of $J^n\tilde{s}$) is identically zero. Hence $\dim(J, \tilde{s}) < d$, which contradicts full-dimensionality of (M, s) since $\dim(M, s) = \dim(J, \tilde{s})$.

Suppose $x_{d_k}^{(k)} = 0$ or $\lambda_k = 0$ for some $k \leq 2l_1$. Since B_{2j} is the entrywise complex conjugate of B_{2j-1}, and $\tilde{s}_{2j}$ is the entrywise complex conjugate of $\tilde{s}_{2j-1}$ for all $1 \leq j \leq l_1$, w.l.o.g. we can assume k is even. By the aforementioned conjugacy relations, if $x_{d_k}^{(k)} = 0$ then $x_{d_{k-1}}^{(k-1)} = 0$. Otherwise, $\lambda_{k-1} = 0$. Therefore, $e_K J^n \tilde{s}$ and $e_M J^n \tilde{s}$, where $K = \sum_{i=1}^{k} d_i$ and $M = \sum_{i=1}^{k-1} d_i$, are both identically zero.

For all $1 \leq j \leq l_1$ and $n \in \mathbb{N}$, $B_{2j}^n \tilde{s}_{2j}$ is the entrywise conjugate of $B_{2j-1}^n \tilde{s}_{2j-1}$. Let $T \in \{\boldsymbol{i}, -1, -\boldsymbol{i}, 1\}^{d \times d}$ be such that for all $y_1, z_1 \in \overline{\mathbb{Q}}^{d_1}, \ldots, y_{l_1}, z_{l_1} \in \overline{\mathbb{Q}}^{d_{l_1}}$ and $w \in \mathbb{R}^{l_2}$,

$$T \cdot (y_1, z_1, \ldots, y_l, z_l, w) = \frac{1}{2}(y_1 + z_1, \boldsymbol{i}(z_1 - y_1), \ldots, y_{l_1} + z_{l_1}, \boldsymbol{i}(z_{l_1} - y_{l_1}), w).$$

The matrix T is invertible and satisfies $TJ^n\tilde{s} \in \mathbb{R}^d$ for all $n \in \mathbb{N}$. Writing δ for the dimension of $\operatorname{span}_{\mathbb{R}}((TJ^n\tilde{s})_{n\in\mathbb{N}})$ as a subspace of $\mathbb{R}^d$, we have that $\dim(M, s) = \delta$. On the other hand, since $e_K J^n \tilde{s}$ and $e_M J^n \tilde{s}$ are identically zero, by construction of T the sequences $e_K T J^n \tilde{s}$ and $e_M T J^n \tilde{s}$ are also identically zero. Therefore, $\delta < d$. This contradicts full-dimensionality of (M, s). □

We are now ready to give the main construction on this section. Keep in mind that all of $\lambda_1, \ldots, \lambda_m$ are non-zero. For $z \in \mathbb{C}$ and $k \in \mathbb{N}$, write

$$\binom{z}{k} \coloneqq \frac{z(z-1)\cdots(z-k+1)}{k!}.$$

For $\lambda \in \overline{\mathbb{Q}}$ not zero, r a positive integer, and $u, v \in \mathbb{C}$, define

$$J_r^{\lambda}(u, v) = v \begin{bmatrix} 1 & u\lambda^{-1} & \cdots & \binom{u}{r-1}\lambda^{-r+1} \\ & 1 & \cdots & \binom{u}{r-2}\lambda^{-r+2} \\ & & \ddots & \vdots \\ & & & 1 \end{bmatrix} \in \mathbb{C}^{r \times r}.$$

The (i, j)th entry of $J_r^{\lambda}(u, v)$ for $j \geq i$ is $\binom{u}{j-i}\lambda^{i-j}v$. With this definition, $J_r^{\lambda}(n, \lambda^n)$ is exactly the nth power of Jordan block of dimension $r \times r$ with the eigenvalue λ. Note that if M is diagonalisable, then $m = d$. Mirroring $J = \operatorname{diag}(B_1, \ldots, B_m)$, define

(a) $g_{M,s} \colon (\mathbb{C}^{\times})^m \to \mathbb{C}^{d \times d}$,

$$g_{M,s}(z_1, \ldots, z_m) \coloneqq \operatorname{diag}(z_1, \ldots, z_m)$$

if M is diagonalisable, and

(b) $G_{M,s}\colon \mathbb{C} \times (\mathbb{C}^\times)^m \to \mathbb{C}^{d\times d}$,

$$G_{M,s}(z_0, \ldots, z_m) \coloneqq \operatorname{diag}(J_{d_1}^{\lambda_1}(z_0, z_1), \ldots, J_{d_m}^{\lambda_m}(z_0, z_m))$$

if M is non-diagonalisable.

In case (a), $J^n = g_{M,s}(\lambda_1^n, \ldots, \lambda_m^n)$, and in case (b), $J^n = G_{M,s}(n, \lambda_1^n, \ldots, \lambda_m^n)$ for all $n \in \mathbb{N}$. Finally, we define

$$f_{M,s}(z_1, \ldots, z_m) \coloneqq P^{-1} g_{M,s}(z_1, \ldots, z_m) Ps$$

in case M is diagonalisable, and

$$F_{M,s}(z_0, \ldots, z_m) \coloneqq P^{-1} G_{M,s}(z_0, \ldots, z_m) Ps$$

otherwise. With the definitions, Equation (6.2) holds for all $n \in \mathbb{N}$.

We view $f_{M,s}$ and $M_{M,s}$ as (entrywise polynomial) functions with types $(\mathbb{C}^\times)^m \to \mathbb{C}^d$ and $\mathbb{C} \times (\mathbb{C}^\times)^m \to \mathbb{C}^d$, respectively. Recall from Section 1.7 that each entry of P and P^{-1} is of the form $p(\lambda)$, where $\lambda \in \{\lambda_1, \ldots, \lambda_m\}$ and p is a polynomial with rational coefficients that, alongside canonical representations of algebraic entries of P, P^{-1}, J, can be computed in polynomial time given M. Moreover, if $q(x) = \sum_{i=0}^{\deg(\lambda)} a_i x^i$ is the minimal polynomial of λ, then $a_0 \neq 0$ (as $\lambda \neq 0$), $-a_0 = \sum_{i=1}^{\deg(\lambda)} a_i \lambda^i$, and hence

$$\lambda^{-1} = \sum_{i=1}^{\deg(\lambda)} (-a_i/a_0)\lambda^{i-1}.$$

That is, λ^{-1} can be expressed in the form $h(\lambda)$ for a polynomial p with rational coefficients. Consequently, we have the following.

(a) Suppose M is diagonalisable. Given M, s, using the definition of $f_{M,s}$ above in time $\textsc{Poly}(\|M\|, \|s\|)$ we can compute (non-flat) terms $f_1, \ldots, f_d \in \mathcal{L}_r$ such that

$$e_i M^n s = f_i(\lambda_1, \ldots, \lambda_m, \lambda_1^n, \ldots, \lambda_m^n)$$

for all $1 \leq i \leq d$ and $n \in \mathbb{N}$.

(b) Similarly, if M is non-diagonalisable, then again in time $\textsc{Poly}(\|M\|, \|s\|)$ we can compute non-flat terms $F_1, \ldots, F_d \in \mathcal{L}_r$ such that

$$e_i M^n s = F_i(\lambda_1, \ldots, \lambda_m, n, \lambda_1^n, \ldots, \lambda_m^n)$$

for all i and n.

Finally, we show that the functions $f_{M,s}$ and $F_{M,s}$ map injectively from their respective domains (where the powers of the eigenvalues and the value n live) into $\mathbb{C}^d$, where the points of the orbit $(M^n s)_{n\in\mathbb{N}}$ live.[4]

Lemma 6.1.5. *If M is diagonalisable, then $f_{M,s}$ is injective. If M is non-diagonalisable, then $F_{M,s}$ is injective.*

Proof. Suppose M is diagonalisable. Let $z = (z_1, \ldots, z_m), y = (y_1, \ldots, y_m) \in (\mathbb{C}^\times)^m$ and suppose $f_{M,s}(z) = f_{M,s}(y)$. Then $g_{M,s}(z)\tilde{s} = g_{M,s}(y)\tilde{s}$ and hence $g_{M,s}(z-y)\tilde{s} = \mathbf{0}$. Since all entries of $\tilde{s}$ are non-zero by Lemma 6.1.4, and

$$g_{M,s}(z-y) = \operatorname{diag}(z_1 - y_1, \ldots, z_m - y_m),$$

we conclude that $z - y = \mathbf{0}$.

Suppose M is non-diagonalisable. It suffices to prove that for each $1 \le k \le m$, the function $(u, v) \mapsto J_{d_k}^{\lambda_k}(u, v)\tilde{s}_k$ is injective on $\mathbb{C} \times \mathbb{C}^\times$. Suppose

$$J_{d_k}^{\lambda_k}(u_1, v_1)\tilde{s}_k = J_{d_k}^{\lambda_k}(u_2, v_2)\tilde{s}_k$$

for $u_1, v_1 \in \mathbb{C}$ and $u_2, v_2 \in \mathbb{C}^\times$. By equating the values of the last (i.e. the d_kth) coordinate we obtain $v_1 x_{d_k}^{(k)} = v_2 x_{d_k}^{(k)}$. From Lemma 6.1.4 it follows that $v_1 = v_2$. If $d_k = 1$, then we are done. Otherwise, equating the values of the $(d_k - 1)$th coordinate we obtain

$$v_1 x_{d_k-1}^{(k)} + u_1\lambda_k^{-1} v_1 x_{d_k}^{(k)} = v_2 x_{d_k-1}^{(k)} + u_2\lambda_k^{-1} v_2 x_{d_k}^{(k)}$$

which implies that $u_1\lambda_k^{-1} v_1 x_{d_k}^{(k)} = u_2\lambda_k^{-1} v_2 x_{d_k}^{(k)}$. Since $v_1 = v_2$ as shown above and v_1, v_2 are non-zero by assumption, we conclude that $u_1 = u_2$. □

6.2 Semialgebraic targets contained in a three-dimensional subspace

Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ be full-dimensional and non-degenerate, and T be a set contained in a subspace V of $\mathbb{R}^d$ of dimension $k < d$. Suppose V is defined by equations $c_1^\top \cdot x = \cdots = c_{d-k}^\top \cdot x = 0$ for $c_1, \ldots, c_{d-k} \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$. Let $V_i = \{x \mid c_i^\top x = 0\}$. For all $n \in \mathbb{N}$ and $1 \le i \le d-k$, $M^n s \in V_i$ if and only if $c_i^\top M^n s = 0$. By full-dimensionality, the orbit $(M^n s)_{n\in\mathbb{N}}$ cannot be contained in any V_i. Hence for all i, the sequence $u_n^{(i)} = c_i^\top M^n s$ is not identically zero. The eigenvalues of each LRS $(u_n^{(i)})_{n\in\mathbb{N}}$ will be

[4] Terms of $(M^n s)_{n\in\mathbb{N}}$ live in $\mathbb{R}^d$, but it will be more convenient to apply algebraic geometry if we move to the algebraically closed field $\mathbb{C}$.

a subset of the eigenvalues of M. Since M is non-degenerate by assumption, every $(u_n^{(i)})_{n\in\mathbb{N}}$ is non-degenerate. Recall from Chapter 2 that a non-degenerate[5] LRS has only finitely many zero terms. It follows that the orbit of (M, s) visits each V_i and hence T only finitely many times. This example demonstrates that understanding the (finitely many) time steps at which the orbit of a full-dimensional and non-degenerate system visits a target set of lower linear dimension ought to be easy, provided that we can effectively solve the system of linear equations $c_1^\top M^n s = \cdots = c_{d-k}^\top M^n s = 0$ in $n \in \mathbb{N}$. The latter is an instance of the Skolem Problem.[6] We will now show how to determine all elements of $\{n \mid M^n \in T\}$ effectively in case $k = 3$. Our (only) result in this section is the following.

Theorem 6.2.1. *Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ be non-degenerate and full-dimensional with $d > 3$, and $T \subset \mathbb{R}^d$ be a semialgebraic set contained in a three-dimensional subspace. There exists an absolute absolute polynomial $P \in \mathbb{Z}[x]$ such that for every $n \geq 2^{2^{P(\mathcal{I})}}$, where $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\|$, it holds that $M^n s \notin T$.*

We mention that the polynomial P is fully constructive and can be extracted from the proof below. Once we have Theorem 6.2.1, given T and full-dimensional and non-degenerate (M, s), we can determine all n such that $M^n s \in T$ by simply checking the first $N = 2^{2^{P(\mathcal{I})}}$ terms of the orbit $(M^n s)_{n\in\mathbb{N}}$.

Proof. Our strategy is to show existence of a non-degenerate linear recurrence sequence $(u_n)_{n\in\mathbb{N}}$ over $\mathbb{R} \cap \overline{\mathbb{Q}}$ of order at most 4 such that for all n, $M^n s \in T$ only if $u_n = 0$. Such LRS have finitely many zeros that can be effectively determined (Theorem 2.3.1).

Write $M = P^{-1}JPs$, where J is in real Jordan form. By permuting the blocks of J if necessary, we can assume that J is of the form $\mathrm{diag}(J_1, J_2)$ where J_1, J_2 are in real Jordan form, all blocks of J_1 are in $\mathbb{R}^{(2k+1)\times(2k+1)}$ for some $k \in \mathbb{N}$, and all blocks of J_2 are in $\mathbb{R}^{2k\times 2k}$ for some $k \in \mathbb{N}$. Writing $\tilde{s} = Ps$ and $\widetilde{T} = PT$, for all $n \in \mathbb{N}$ it holds that

$$M^n s \in T \;\Leftrightarrow\; J^n \tilde{s} \in \widetilde{T}.$$

Next, write

$$J = \begin{bmatrix} X & Y \\ \mathbf{0} & Z \end{bmatrix}$$

so that $Z \in \mathbb{R}^{4\times 4}$. Observe that Z is in real Jordan form. Define $\Pi\colon \mathbb{R}^d \to \mathbb{R}^4$ by

$$\Pi(x_1, \ldots, x_d) = (x_{d-3}, \ldots, x_d),$$

[5] By definition, a non-degenerate sequence must be not identically zero.

[6] Using the squaring trick we can construct $(v_n)_{n\in\mathbb{N}}$ such that for all $n \in \mathbb{N}$, $v_n = 0$ if and only if $c_1^\top M^n s = \cdots = c_{d-k}^\top M^n s = 0$.

and let $V \subset \mathbb{R}^4$ be a three-dimensional subspace enclosing $\Pi(\widetilde{T})$ with a normal vector $c \in (\mathbb{R} \cap \overline{\mathbb{Q}})^4$. It holds that

$$M^n s \in T \;\Leftrightarrow\; J^n \tilde{s} \in \widetilde{T} \;\Rightarrow\; Z^n \Pi(\tilde{s}) \in V.$$

Observe that $(Z, \Pi(\tilde{s}))$ is itself non-degenerate and full-dimensional. Next, consider the linear recurrence sequence $u_n = c^\top Z^n \Pi(\tilde{s})$ over $\mathbb{R} \cap \overline{\mathbb{Q}}$, satisfying

$$u_n = 0 \;\Leftrightarrow\; Z^n \Pi(\tilde{s}) \in V.$$

As Z is non-degenerate and the eigenvalues of $(u_n)_{n\in\mathbb{N}}$ form a subset of the eigenvalues of Z, the sequence $(u_n)_{n\in\mathbb{N}}$ is either identically zero or non-degenerate. Because $(Z, \Pi(\tilde{s}))$ is full-dimensional, $(Z^n \Pi(\tilde{s}))_{n\in\mathbb{N}}$ cannot be contained in the hyperplane V. It follows that $(u_n)_{n\in\mathbb{N}}$ is not identically zero and hence is non-degenerate. As $Z \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{4\times 4}$, $(u_n)_{n\in\mathbb{N}}$ is an LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ of order at most 4. Therefore, by Theorem 2.3.1 there exists effectively computable N such that for all $n \geq N$, $u_n \neq 0$ and $Z^n \Pi(\tilde{s}) \notin V$. We conclude that $M^n s \notin T$ for $n \geq N$. It remains to bound N in terms of $\mathcal{I}$.

We first bound the description lengths of $\widetilde{T}$ and $\tilde{s}$. Let Φ be a quantifier-free formula defining T, and for $1 \leq i, j \leq d$, let $\varphi_{i,j}(u_{i,j})$ be a quantifier-free formula defining the real algebraic number $P^{-1}_{i,j}$. Since algebraic entries of P^{-1}, J, P can be computed in polynomial time given M, invoking Lemma 1.5.3 we can assume $\|\varphi_{i,j}\| < \textsc{Poly}(\mathcal{I})$. Write $\mathbf{x}$ and $\mathbf{u}$ for the collections of variables $x_1, \ldots, x_{d-4}$ and $u_{i,j}$ for $1 \leq i, j \leq d$, respectively, For all $y \in \mathbb{R}^4$,

$$y \in \Pi(\widetilde{T}) \;\Leftrightarrow\; \exists w \in \mathbb{R}^{d-4} \colon P^{-1} \cdot (w, y) \in T.$$

We can therefore define $\Pi(\widetilde{T})$ by the formula

$$\exists \mathbf{x}, \mathbf{u} \colon \bigwedge_{i,j} \varphi_{i,j}(u_{i,j}) \wedge \Phi\left(\sum_{j=1}^{d} x_j u_{1,j}, \ldots, \sum_{j=1}^{d} x_j u_{d,j}\right)$$

with free variables $x_{d-3}, \ldots, x_d$. Eliminating quantifiers using Theorem 1.3.5, we conclude that there exists a quantifier-free formula Φ_1 with $\|\Phi_1\| < \mathcal{I}^{\textsc{Poly}(d)}$ that defines $\Pi(\widetilde{T})$. By a similar argument, algebraic entries of $\Pi(\tilde{s})$ each can be defined by a quantifier-free formula of size at most $\mathcal{I}^{\textsc{Poly}(d)}$.

Next, consider the set

$$W = \{(b_1, \ldots, b_4) \in \mathbb{R}^4 \mid \forall x_1, \ldots, x_4 \colon \Phi_1(x_1, \ldots, x_4) \Rightarrow b_1 x_1 + \ldots + b_4 x_4 = 0\}$$

of all vectors orthogonal to $\Pi(\widetilde{T})$. Since $\Pi(\widetilde{T})$ is contained in a three-dimensional subspace, W is non-empty. Since W is defined using 8 bound and free variables in total, invoking Theorem 1.3.5, there exists a quantifier-free formula Φ_2 of bit length at most $\textsc{Poly}(\|\Pi(\widetilde{T})\|) < \mathcal{I}^{\textsc{Poly}(d)}$ that defines W. We will shortly show that W must contain $c \in (\mathbb{R} \cap \overline{\mathbb{Q}})^4$ with total description length at most $\mathcal{I}^{\textsc{Poly}(d)}$. Assuming existence of such c, consider the sequence $u_n = c^\top Z^n \Pi(\tilde{s})$, which is an LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ of order at most 4. Applying Corollary 1.5.8, algebraic numbers $u_0, \ldots, u_3$ have canonical representations of size at most $\mathcal{I}^{\textsc{Poly}(d)}$. To apply Theorem 2.3.1, it remains to bound the description length of a recurrence relation satisfied by $(u_n)_{n \in \mathbb{N}}$. Let

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + x^4 \in \overline{\mathbb{Q}}[x]$$

be the characteristic polynomial of Z. As $Z \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{4 \times 4}$ and $\|Z\| < \textsc{Poly}(\mathcal{I})$, by Corollary 1.5.8 each a_i has a canonical representation of size at most $\textsc{Poly}(\mathcal{I})$. Applying the Cayley-Hamilton theorem, $u_{n+4} = a_0 u_n + \ldots + a_3 u_{n+3}$ for all $n \in \mathbb{N}$. Finally, invoking Theorem 2.3.1, there exists $N < 2^{\mathcal{I}^{\textsc{Poly}(d)}} < 2^{2^{P(\mathcal{I})}}$, where $P \in \mathbb{Z}[x]$ is an absolute polynomial, such that $u_n \neq 0$ for all $n \geq N$. It follows that $u_n \neq 0$ and hence $M^n s \notin T$ for all $n \geq 2^{2^{P(\mathcal{I})}}$.

It remains to prove the claim about the description length of $c = (c_1, \ldots, c_4) \in W$. We will give an inductive algorithm that constructs such c. First, consider non-empty and semialgebraic $X \subseteq \mathbb{R}$ defined by a quantifier-free formula φ. We can sample $x \in (\mathbb{R} \cap \overline{\mathbb{Q}}) \cap X$ as follows. If $X = \mathbb{R}$, which can be checked in polynomial time by Theorem 1.3.5, then we can select $x = 0$. Otherwise, compute in time polynomial in $\|X\|$ a quantifier-free formula ψ equivalent to

$$\varphi(x) \quad \wedge \quad \forall \epsilon > 0.\, \exists y \colon (x - y)^2 < \epsilon \wedge \neg \varphi(y)$$

which defines the finite set ∂X of boundary points of X. We can then use Lemma 1.5.6 to compute in polynomial time canonical representations of all numbers belonging to ∂X. Hence X contains $x \in \mathbb{R} \cap \overline{\mathbb{Q}}$ with $\|x\| < \textsc{Poly}(\|X\|)$.

Let Φ be a quantifier-free formula defining W. To sample c_1, let φ be a quantifier-free formula equivalent to $\exists x_2, x_3, x_4 \colon \Phi(x_1, \ldots, x_4)$, which can be computed in polynomial time. Write $X = \{x \in \mathbb{R} \mid \varphi(x)\}$. Applying the argument above to X, we can construct c_1 in time polynomial in $\|\Phi\|$. In particular, $c_1 \in \mathbb{R} \cap \overline{\mathbb{Q}}$ with $\|c_1\| < \textsc{Poly}(\mathcal{I})$.

Next, suppose for some $k < 4$ we have computed $c_1, \ldots, c_k \in \mathbb{R} \cap \overline{\mathbb{Q}}$ each with description length at most $\textsc{Poly}(\mathcal{I})$. Let φ_i be a quantifier-free formula of size at

most $\textsc{Poly}(\mathcal{I})$ defining c_i for $1 \leq i \leq k$, computed using Lemma 1.5.3. Consider $X \subseteq \mathbb{R}$ defined by

$$\exists x_1, \ldots, x_k, x_{k+2}, \ldots, x_4 \colon \bigwedge_{i=1}^{k} \varphi(x_i) \ \wedge \ \Phi(x_1, \ldots, x_4)$$

which has a single free variable x_{k+1}. A quantifier-free formula φ defining X can be computed in polynomial time, and applying the argument above, there exists $c_{k+1} \in (\mathbb{R} \cap \overline{\mathbb{Q}}) \cap X$ with $\|c_{k+1}\| < \textsc{Poly}(\mathcal{I})$. □

6.3 Semialgebraic targets of dimension one

In this section we will analyse the reachability set $\{n \in \mathbb{N} \colon M^n s \in T\}$ for a non-degenerate and full-dimensional system (M, s) and a one-dimensional semialgebraic target T. We will show that this set is either finite of co-finite, unless the system (M, s) is of *Type 1*, which is a very strong restriction.

Definition 6.3.1. *A linear dynamical system (M, s) is of Type 1 if M is diagonalisable, all eigenvalues of M have modulus 1, and every pair λ_i, λ_j of eigenvalues of M is multiplicatively dependent. It is of Type 2 otherwise.*

Type 1 systems generalise two-dimensional linear dynamical systems whose update matrix is a rotation. For such systems it is not difficult to construct T for which the reachability set is neither finite nor co-finite. Take

$$M = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in \mathbb{Q}^{2\times 2},$$

$s = (1, 0)$ and $T = \{(x, y) \in \mathbb{R}^2_{>0} \mid x^2 + y^2 = 1\}$ for example. However, in this case the reachability set is well-structured in a different way:

$$M^n s \in T \ \Leftrightarrow \ \gamma^n \in J$$

where $\gamma = e^{i\theta}$ and $J = \{z \in \mathbb{T} \mid \mathrm{Re}(z), \mathrm{Im}(z) > 0\}$. In other words, the characteristic word α_T defined by

$$\alpha(n) = 1 \ \Leftrightarrow \ M^n s \in T$$

is toric. The next lemma generalises this observation.

Lemma 6.3.2. *Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ be non-degenerate and of Type 1. Write $\mathcal{I} = \|M\| + \|s\|$. There exist effectively computable $L \in \mathbb{N}$ and $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ not a root of unity with the following properties.*

(a) $\|\gamma\| < \textsc{Poly}(\mathcal{I})$, $L < 2^{\textsc{Poly}(\mathcal{I})}$, *and* γ *only depends on* M.

(b) *Let* T *be semialgebraic. Writing* $\mathcal{I}_T = \mathcal{I} + \|T\|$, *there exist open semialgebraic* $S_0, \ldots, S_{L-1} \subseteq \mathbb{T}$ *with description lengths at most* $2^{\textsc{Poly}(\mathcal{I}_T)}$ *and* $N < 2^{\textsc{Poly}(\mathcal{I}_T)}$ *such that for all* $0 \leq r < L$ *and* $n \geq N$,

$$M^{nL+r}s \in T \Leftrightarrow \gamma^n \in S_r.$$

Proof. Denote the (possibly non-distinct) eigenvalues of M by $\lambda_1, \ldots, \lambda_d$, and let $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_d)$. By the Tower Law, $D \coloneqq [\mathbb{K} : \mathbb{Q}] < \mathcal{I}^{\textsc{Poly}(d)}$.

Since M is non-degenerate by assumption, λ_i is not a root of unity for all i. We will choose $\gamma = \lambda_1$. For $1 \leq i \leq d$, let l_i, k_i be non-zero integers such that $\lambda_1^{l_i} = \lambda_i^{k_i}$. By Masser's bound (Theorem 4.1.1), we can take k_i, l_i to have absolute value at most polynomial in $\|\lambda_1\| + \|\lambda_i\|$. Let $L = \operatorname{lcm}(k_1, \ldots, k_d) < \mathcal{I}^{\textsc{Poly}(d)}$. We will consider the family of linear dynamical systems $(M^L, M^r s)$ for $0 \leq r < L$. Note that $\|M^L\|, \|M^r s\| < \mathcal{I}^{\textsc{Poly}(d)}$.

From the input quantifier-free formula defining T, using Lemma 1.3.4 compute an equivalent flat quantifier-formula

$$\varphi(x_1, \ldots, x_d) \coloneqq \bigwedge_{a \in A} \bigvee_{b \in B} p_{a,b}(x_1, \ldots, x_d)\ \Delta_{a,b}\ 0$$

with $\|\varphi\| < \|T\|^{O(d)}$. W.l.o.g. we can assume $\Delta_{a,b} \in \{\geq, >, =\}$ for all $a \in A$ and $b \in B$. Fix $0 \leq r < L$. We will show how to construct S_r. For $a \in A, b \in B$ define

$$u_n^{a,b} = p_{a,b}(M^{nL+r}s).$$

Observe that for all $n \in \mathbb{N}$, $M^{nL+r}s \in T$ if and only if

$$\bigwedge_{a \in A} \bigvee_{b \in B} u_n^{a,b}\ \Delta_{a,b}\ 0.$$

We will show that the sign pattern of each $(u_n^{a,b})_{n \in \mathbb{N}}$ is eventually toric and generated by γ. Applying Lemma 2.2.5 to p, M^L and $M^r s$, for all a, b we can write

$$u_n^{a,b} = \sum_{j=1}^{K} f_j(\lambda_1^L, \ldots, \lambda_d^L)(\lambda_1^{nL})^{e_{j,1}} \cdots (\lambda_d^{nL})^{e_{j,d}}$$

where $K < \mathcal{I}_T^{\textsc{Poly}(d)}$ and $f_j \in \mathbb{Q}[x_1, \ldots, x_d]$ with $\|f_j\| < \mathcal{I}_T^{\textsc{Poly}(d)}$ for all j. Recall that for $1 \leq i \leq d$, $\lambda_i^{k_i} = \lambda_1^{l_i}$ and hence $\lambda_i^L = \gamma^{l_i L/k_i}$. Therefore,

$$u_n^{a,b} = \sum_{j=1}^{K} f_j(\lambda_1^L, \ldots, \lambda_d^L)\gamma^{nh_j} \tag{6.3}$$

where for all $1 \leq j \leq K$,

$$h_j = L \sum_{i=1}^{d} \frac{e_{j,i}\, l_i}{k_i} < \mathcal{I}_T^{\textsc{Poly}(d)}.$$

By Corollary 1.5.8, there exists a canonical representation of $\xi_i = \lambda_i^L$ satisfying $\|\xi_i\| < \mathcal{I}^{\textsc{Poly}(d)}$ for $1 \leq i \leq d$. If $u_n^{a,b}$ is identically zero, i.e. $f_j(\lambda_1^L, \ldots, \lambda_d^L) = 0$ for all j, let $N_{a,b} = 0$, and $S_{a,b} = \mathbb{T}$ in case $\Delta_{a,b}$ is $\geq$ and $S_{a,b} = \emptyset$ otherwise. If $u_n^{a,b}$ is not identically zero, let $N_{a,b} < \mathcal{I}_T^{\textsc{Poly}(d)}$ be such that $u_n^{a,b} \neq 0$ for $n \geq N_{a,b}$ (Lemma 2.6.4), and applying Lemma 1.5.5 to Equation (6.3), compute open semialgebraic $S_{a,b} \subseteq \mathbb{T}$ with $\|S_{a,b}\| < \mathcal{I}_T^{\textsc{Poly}(d)}$ such that for all $n \in \mathbb{N}$,

$$u_n^{a,b} > 0 \;\Leftrightarrow\; \gamma^n \in S_{a,b}.$$

Writing $N = \max_{(a,b)\in A\times B} N_{a,b}$, for all $n \geq N$ and $(a,b) \in A \times B$ the (in)equality $u_n^{a,b}\ \Delta_{a,b}\ 0$ holds if and only if $\gamma^n \in S_{a,b}$. Therefore, we can define

$$S_r := \bigwedge_{a\in A} \bigvee_{b\in B} S_{a,b}$$

with the property that $M^{nL+r}s \in T$ if and only if $\gamma^n \in S_r$. Observe that S_r is open, semialgebraic, and has bit length at most $\mathcal{I}_T^{\textsc{Poly}(d)}$. □

The lemma above shows that the characteristic word α of a non-degenerate Type 1 system (M, s) with respect to a set $\mathcal{T}$ of semialgebraic targets of dimension 1 is an interleaving of L eventually toric words with semialgebraic parameters, all generated by the same rotation $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$. From Theorem 4.2.3 it follows that α itself is eventually toric with semialgebraic parameters.

To analyse Type 2 systems next, we will need the notion of the *complexification* of semialgebraic $T \subseteq \mathbb{R}^d$. The complexification of semialgebraic T, written $C(T)$, is the smallest affine variety enclosing T. The complex dimension of $C(T)$ (i.e. its dimension over $\mathbb{C}$ as a variety) is the same as the semialgebraic dimension of T [74, Section 1].

Lemma 6.3.3 (Roy and Vorobjov, [74], Theorem 3)**.** *Let $T \subseteq \mathbb{R}^d$ be a semialgebraic set and $C(T)$ be its complexification. For each irreducible component W of $C(T)$ there exist $k \leq d$, $p_1, \ldots, p_k \in \mathbb{Q}[y, z_1, \ldots, z_d]$ and $\alpha_1, \ldots, \alpha_k \in \mathbb{R} \cap \overline{\mathbb{Q}}$ such that $\|p_i\|, \|\alpha_i\| < \|T\|^{\textsc{Poly}(d)}$ for all $1 \leq i \leq k$, and for all $z = (z_1, \ldots, z_d) \in \mathbb{C}^d$,*

$$z \in W \;\Leftrightarrow\; \bigwedge_{1\leq i\leq k} p_i(\alpha_k, z_1, \ldots, z_d) = 0.$$

We will not actually need to compute the complexification of a given semialgebraic set. Rather, we need the bounds above on the description length of the complexification and its irreducible components. In the next lemma we carry out the variable elimination described in the introduction of this chapter to show that the set of time steps at which a full-dimensional, non-degenerate LDS of Type 2 visits a semialgebraic target of dimension at most one is either finite or co-finite.

Lemma 6.3.4. *Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ be non-degenerate, full-dimensional and of Type 2, and $T \subseteq \mathbb{R}^d$ be a semialgebraic set of dimension at most 1. There exists effectively computable $N < \exp^5(\textsc{Poly}(\mathcal{I}))$, where $\mathcal{I} = \|M\| + \|s\| + \|T\|$, such that $M^n s \in T$ either holds for all $n \geq N$, or does not hold for any $n \geq N$.*

We prove Lemma 6.3.4 in the remainder of this section. Recall from Lemma 6.1.4 that full-dimensionality of (M, s) implies M is invertible, i.e. every eigenvalue of M is non-zero. Let $\lambda_1, \ldots, \lambda_m$ denote the eigenvalues of M, which are non-zero by full-dimensionality, and $J = P^{-1}MP$ be in Jordan normal form. Write $\boldsymbol{\lambda}$ for the collection of numbers $\lambda_1, \ldots, \lambda_m$. We will carry out a case analysis based on the eigenvalues of M. In Cases 1 and 2 we will show that for each irreducible component W of the complexification $C(T)$ there exists $N < \exp^5(\textsc{Poly}(\mathcal{I}))$ such that for all $n \geq N$, $M^n s \notin W$. Since the bound applies to all irreducible components of $C(T)$, we can conclude that for $n \geq N$, $M^n s \notin C(T)$ and hence $M^n s \notin T$. Case 3 is simpler and does not involve the complexification.

Case 1. Suppose M is diagonalisable and has two multiplicatively independent eigenvalues. W.l.o.g. assume λ_1, λ_2 are multiplicatively independent. Let W be an irreducible component of $C(T)$, and let polynomials $p_1, \ldots, p_k$ and real algebraic $\alpha_1, \ldots, \alpha_k$ define W as described in Lemma 6.3.3. As mentioned earlier, the complex dimension of W is at most 1. We will argue that $M^n s \in W$ forces a polynomial relation between λ_1^n and λ_2^n, after which we can construct the desired N using Theorem 2.7.1.

As in Section 6.1.2, let $f_1, \ldots, f_d$ be first-order terms[7] with rational coefficients and $2m$ free variables such that for $1 \leq i \leq d$,

$$f_i(\boldsymbol{\lambda}, \lambda_1^n, \ldots, \lambda_m^n) = e_i M^n s.$$

Write $\mathbf{z}$ for the collection of variables $z_1, \ldots, z_m$. Since (M, s) is full-dimensional and M is diagonalisable by assumption, by Lemma 6.1.5 the function $f\colon \mathbb{C}^m \to \mathbb{C}^d$,

$$f(\mathbf{z}) = (f_1(\boldsymbol{\lambda}, \mathbf{z}), \ldots, f_d(\boldsymbol{\lambda}, \mathbf{z}))$$

[7]Recall from Section 1.3 that we identified first-order terms with polynomial functions. We can determine the polynomial equivalent (as a function) to a given first-order term through flattening (Lemma 1.3.4).

is injective on $(\mathbb{C}^\times)^m$. Let $V \coloneqq f^{-1}(W) \cap (\mathbb{C}^\times)^m$ and $X \subseteq \mathbb{C}^2$ be the projection of V onto the first two coordinates. It holds that

$$M^n s \in W \;\Leftrightarrow\; (\lambda_1^n, \dots, \lambda_m^n) \in V \;\Rightarrow\; (\lambda_1^n, \lambda_2^n) \in X.$$

Observe that $f^{-1}(W)$ is an affine variety, and

$$V = f^{-1}(W) \setminus \{(z_1, \dots, z_m) \in \mathbb{C}^m \mid z_i = 0 \text{ for some } 1 \le i \le m\}$$

is quasi-affine. Hence the restriction $\tilde{f}\colon V \to W$ of f to V is an injective morphism of quasi-affine varieties. Invoking Corollary 1.6.2, $\dim(V) \le \dim(f(V)) \le \dim(W) \le 1$. As X is a projection of W, $\dim(X) \le \dim(V) \le 1$. We are almost done: Let $Y \supseteq X$ be a hypersurface in $\mathbb{C}^2$ defined as the locus of a non-zero polynomial $q \in \overline{\mathbb{Q}}[z_1, z_2]$. It holds that $(\lambda_1^n, \lambda_2^n) \in X \Rightarrow q(\lambda_1^n, \lambda_2^n) = 0$, and we can invoke Theorem 2.7.1 to construct the required N. We next show how to compute such polynomial q and establish bounds on the magnitude of N.

Write $\mathbf{l}$ and $\mathbf{a}$ for the collections of variables $l_1, \dots, l_m$ and $a_1, \dots, a_k$, respectively, and $\boldsymbol{\alpha}$ for the collection of numbers $\alpha_1, \dots, \alpha_k$. The variables l_i, a_j stand for λ_i and α_j, respectively. Let

$$\begin{aligned}\Phi(\mathbf{a}, \mathbf{l}, \mathbf{z}) &\coloneqq \bigwedge_{j=1}^{k} p_j(a_i, f_1(\mathbf{l}, \mathbf{z}), \dots, f_d(\mathbf{l}, \mathbf{z})) = 0,\\ \Psi(\mathbf{a}, \mathbf{l}, z_1, z_2) &\coloneqq \exists z_3, \dots, z_d\colon \Phi(\mathbf{a}, \mathbf{l}, \mathbf{z}).\end{aligned}$$

Observe that $(z_1, z_2) \in X$ if and only if $\Psi(\boldsymbol{\alpha}, \boldsymbol{\lambda}, z_1, z_2)$ holds. Recall from Section 6.1.2 that $\|f_i\| < \textsc{Poly}(\|M\|)$ for all i, and by Lemma 6.3.3, $\|p_j\|, \|\alpha_j\| < 2^{\textsc{Poly}(\|T\|)}$ for all j. Hence $\|\Psi\| < 2^{\textsc{Poly}(\mathcal{I})}$. Viewing Ψ as a formula in $\mathcal{L}_r$ (i.e. the language of ordered rings) and eliminating quantifiers using Theorem 1.3.6, we obtain that $(z_1, z_2) \in X$ if and only if

$$\bigvee_{1 \le i \le I} \bigwedge_{1 \le j \le J_i} h_{i,j}(\boldsymbol{\alpha}, \boldsymbol{\lambda}, z_1, z_2) \sim_{i,j} 0 \tag{6.4}$$

where $h_{i,j}$ is a polynomial (i.e. a flat term) with rational coefficients, $\|h_{i,j}\| < 2^{\textsc{Poly}(\mathcal{I})}$, and $\sim_{i,j} \in \{=, \neq\}$ for all i, j. Let

$$q_{i,j}(z_1, z_2) = h_{i,j}(\boldsymbol{\alpha}, \boldsymbol{\lambda}, z_1, z_2) \in \overline{\mathbb{Q}}[z_1, z_2]$$

for all i, j. The coefficients of $q_{i,j}$ are obtained through arithmetic operations in $\mathbb{K} = \mathbb{Q}(\boldsymbol{\alpha}, \boldsymbol{\lambda})$. By the Tower Lemma, $D \coloneqq [\mathbb{K} : \mathbb{Q}] < 2^{\textsc{Poly}(\mathcal{I})}$. Invoking Lemma 1.5.7, the total description length of the coefficients of $q_{i,j}$ is bounded by $2^{\textsc{Poly}(\mathcal{I})}$.

If $q_{i,j}$ is identically zero for some i, j, then $h_{i,j}(\boldsymbol{\alpha}, \boldsymbol{\lambda}, z_1, z_2) \sim_{i,j} 0$ holds either everywhere or nowhere on $\mathbb{C}^2$, depending on $\sim_{i,j} \in \{=, \neq\}$. By removing all such i, j from Equation (6.4), we can w.l.o.g. assume that $q_{i,j}$ is not identically zero for all i, j. It follows that I cannot be zero, as this would imply that $X = \mathbb{C}^2$, contradicting $\dim(X) \leq 1$. Next, fix a value $1 \leq i \leq I$ and let

$$q(z_1, z_2) = q_{i,1}(z_1, z_2) \cdots q_{i,J_i}(z_1, z_2).$$

We will show that there exists j such that $\sim_{i,j}$ is the equality. Suppose $\sim_{i,j}$ is the inequality sign for all $1 \leq j \leq J_i$. Then $X \supseteq \{(z_1, z_2) \colon q(z_1, z_2) \neq 0\} \coloneqq Y$, where Y is non-empty and open. Since non-empty open sets are Zariski-dense, $\dim(X) \geq \dim(Y) = 2$, again contradicting $\dim(X) \leq 1$.

We have proven that each disjunct in Equation (6.4) contains at least one equality. That means there exist non-zero polynomials $q_1, \ldots, q_I \in \overline{\mathbb{Q}}[z_1, z_2]$ such that

$$(z_1, z_2) \in X \Rightarrow \bigvee_{i=1}^{I} q_i(z_1, z_2) = 0.$$

Hence for all $n \in \mathbb{N}$, $M^n s \in W \Rightarrow q_i(\lambda_1^n, \lambda_2^n) = 0$ for some $1 \leq i \leq I$. Applying Theorem 2.7.1 to each $1 \leq i \leq I$, there exists $N < \exp^5(\textsc{Poly}(\mathcal{I}))$ such that for all $n \geq N$, $q_i(\lambda_1^n, \lambda_2^n) \neq 0$ for all $1 \leq i \leq I$, which implies $M^n s \notin T$.

Case 2. Suppose M is non-diagonalisable with an eigenvalue $\lambda \neq 1$. W.l.o.g. assume $\lambda_1 \neq 1$. We proceed similarly to Case 1, this time with the end goal of applying Theorem 2.7.3. Let $W, p_1, \ldots, p_k$ and $\boldsymbol{\alpha}$ be as in Case 1. As in Section 6.1.2, let $F_1, \ldots, F_d$ be first-order terms with rational coefficients and $2m + 1$ free variables such that for all $1 \leq i \leq d$,

$$F_i(\boldsymbol{\lambda}, n, \lambda_1^n, \ldots, \lambda_m^n) = e_i M^n s.$$

Writing $\mathbf{z}$ for the collection of variables $z_0, \ldots, z_m$, recall that $F \colon \mathbb{C}^{m+1} \to \mathbb{C}^d$,

$$F(\mathbf{z}) = (F_1(\boldsymbol{\lambda}, \mathbf{z}), \ldots, F_d(\boldsymbol{\lambda}, \mathbf{z}))$$

is injective on $\mathbb{C} \times (\mathbb{C}^\times)^m$, Consider

$$V \coloneqq F^{-1}(W) \cap \left(\mathbb{C} \times (\mathbb{C}^\times)^m\right),$$

and let X be the projection of V onto the first two coordinates. It holds that

$$M^n s \in W \;\Leftrightarrow\; (n, \lambda_1^n, \ldots, \lambda_m^n) \in V \;\Rightarrow\; (n, \lambda_1^n) \in X.$$

We again need to show that $\dim(V) \leq 1$, which implies $\dim(X) \leq 1$. To this end, consider the restriction $\widetilde{F}\colon V \to W$ of F to V. Observe that F is an entrywise polynomial map, and since W is an affine variety, so is $F^{-1}(W)$. Therefore,

$$V = F^{-1}(W) \setminus \{(z_0, \ldots, z_m) \in \mathbb{C}^{m+1} \mid z_i = 0 \text{ for some } 1 \leq i \leq m\}$$

is a quasi-affine variety, and $\widetilde{F}$ is a morphism of quasi-affine varieties. Applying Corollary 1.6.2 yields that $\dim(V) \leq \dim(W) \leq 1$.

The rest of the argument is essentially the same as in Case 1. Because $\dim(X) \leq 1$, there exist polynomials $q_1, \ldots, q_I \in \overline{\mathbb{Q}}[z_1, z_2]$, with $\|q_i\| < 2^{\textsc{Poly}(\mathcal{I})}$ for all $1 \leq i \leq I$, such that for all $n \in \mathbb{N}$,

$$(n, \lambda_1^n) \in X \Rightarrow \bigvee_{i=1}^{I} q_i(n, \lambda_1^n) = 0.$$

Since $\lambda_1 \neq 1$ by assumption, invoking Theorem 2.7.3 we conclude that there exists $N < \exp^2(\textsc{Poly}(\mathcal{I}))$ such that for all $n \geq N$, $q_i(n, \lambda_1^n) \neq 0$ for all $1 \leq i \leq I$, and hence $(n, \lambda_1^n) \notin X$. The latter implies $M^n s \notin T$.

Case 3. Suppose M only has real eigenvalues. Let $p \in \mathbb{Q}[x_1, \ldots, x_d]$ be a polynomial appearing in the definition of T. By Lemma 2.2.4, in time $\mathcal{I}^{\textsc{Poly}(d)}$ we can compute the exponential-polynomial representation $p(M^n s) = \sum_{j=1}^{A} q_j(n)\Lambda_j^n$, where each Λ_j is real algebraic and q_j has real algebraic coefficients.[8] Applying Lemma 2.4.4, there exists $N < \exp^2(\textsc{Poly}(\mathcal{I}))$ such that the sign of $p(M^n s)$ is stable for $n \geq N$. Since the bound N applies to all polynomials appearing in the definition of T, it follows that either $M^n s \in T$ for all $n \geq N$, or $M^n s \notin T$ for all $n \geq N$.

Together Cases 1-3 cover all the possibilities. If M is not diagonalisable, then either Case 2 or Case 3 applies. Suppose M is diagonalisable. If M has two multiplicatively independent eigenvalues, then Case 1 applies. Suppose therefore that any two eigenvalues of M are multiplicatively dependent. Since M is of Type 2 by assumption, this means M has an eigenvalue ρ with $|\rho| \neq 1$. Since for all $z \notin \mathbb{T}$, z and $\overline{z}$ are not multiplicatively dependent, and we assumed that every two eigenvalues of M are multiplicatively dependent, it follows that ρ is real. By the same argument, M cannot have non-real eigenvalues λ, $\overline{\lambda}$ with $|\lambda| = 1$. Suppose μ is an eigenvalue of M with $|\mu| = 1$. Since μ is not a root of unity by the assumption that M is non-degenerate, μ is multiplicatively dependent with ρ if and only if $\mu = 1$. Hence M cannot have a non-real eigenvalue, and Case 3 applies.

[8] The latter can be seen by expressing $M^n = P^{-1}J^nP$, where J is in real Jordan form and P^{-1}, P have real algebraic entries.

6.4 Decidability of the model-checking problem

We can now combine the results we have developed in this chapter to show how to model check linear dynamical systems against ω-regular specifications over low-dimensional, and by extension, tame targets. We first focus on low-dimensional targets. Our main result is the following.

Theorem 6.4.1. *Let $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ be a set of low-dimensional predicates, $\Sigma = 2^{\mathcal{T}}$, and $\mathcal{A}$ be a deterministic automaton over Σ.*

(✠) *The characteristic word α of (M, s) with respect to $\mathcal{T}$ is eventually toric with semialgebraic parameters.*

(★) *It is decidable whether $\mathcal{A}$ accepts α, with complexity in* 5EXPSPACE.

Proof. Denote by $\mathcal{I} = \|M\| + \|s\| + \|\mathcal{T}\| + \|\mathcal{A}\|$ the total input size. Let q be the state of $\mathcal{A}$ after reading the first d letters of α, and $\mathcal{B}$ be the automaton over Σ with the start state q that is identical to $\mathcal{A}$ otherwise. The automaton $\mathcal{B}$ can be constructed in polynomial time, and $\mathcal{A}$ accepts α if and only if $\mathcal{B}$ accepts $\beta \coloneqq \alpha[d, \infty)$. Moreover, the word β is eventually toric with semialgebraic parameters if and only if α is eventually toric with semialgebraic parameters. Writing $w \coloneqq M^d s$, note that β is the characteristic word of (M, w) with respect to $\mathcal{T}$.

Apply Corollary 6.1.3 to $M, s, \mathcal{T}$ to compute in time $2^{\textsc{Poly}(\mathcal{I})}$ positive integers $L < 2^{\textsc{Poly}(\mathcal{I})}$, $\mu \leq d$, a non-degenerate and full-dimensional linear dynamical system $(R, t) \in \mathbb{Q}^{\mu\times\mu} \times \mathbb{Q}^\mu$, as well as low-dimensional semialgebraic $T_i^{(r)}$ for $0 \leq r < L$, $1 \leq i \leq \ell$ with the following property. For all $n \in \mathbb{N}$ and $0 \leq r < L$,

$$M^{nL+r} w \in T_i \;\Leftrightarrow\; R^n t \in T_i^{(r)}.$$

Let $\mathcal{T}_r = \{T_1^{(r)}, \ldots, T_\ell^{(r)}\}$, and $\beta_0, \ldots, \beta_{L-1}$ be the L words whose merge is β. We have that each β_r, up to a renaming of letters, is the characteristic word of (R, t) with respect to $\mathcal{T}_r$. Note that $\|R\|, \|t\|, \|\mathcal{T}_r\| < 2^{\textsc{Poly}(\mathcal{I})}$.

Case 1. Suppose $\mu \leq 3$. In this case our analysis of three-dimensional linear dynamical systems from chapter 5 applies. By Theorem 5.0.1, there exists $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$ satisfying $\|\gamma\| < 2^{\textsc{Poly}(\mathcal{I})}$ and the following property. For each $0 \leq r < L$, there exist $N_r < \exp^2(\textsc{Poly}(\mathcal{I}))$ and a collection $\mathcal{S}_r$ of open subsets of $\mathbb{T}$ with $\|\mathcal{S}_r\| < 2^{\textsc{Poly}(\mathcal{I})}$ such that each β_r is eventually toric with semialgebraic parameters $(\gamma, N_r, \mathcal{S}_r)$. Note that we were able to choose the same γ for every $0 \leq r < L$ because the words $\beta_0, \ldots, \beta_{L-1}$ are all generated by the same LDS (R, t). By Theorem 4.2.3, the word β

is eventually toric with semialgebraic parameters. To prove (✠), recall that eventually toric words are the same as words with an eventually toric suffix (Chapter 4).

Applying Theorem 4.4.2, the word β is effectively almost-periodic with

$$\mathcal{W}_\beta(l) < l^{2^{\textsc{Poly}(\mathcal{I})}}$$

for $l \geq 2$. By Corollary 3.1.4, there exists effectively computable $H < \exp^2(\textsc{Poly}(\mathcal{I}))$ such that a state q appears infinitely often in $\mathcal{B}(\beta)$ if and only if it appears in $\mathcal{B}(\beta)[H, 2H)$. Finally, recall from Lemma 5.4.1 that using iterative squaring, whether $R^n t \in T$ for semialgebraic T can be decided in time $\textsc{Poly}(\|R\|, \|t\|, \|T\|, \log n)$. Therefore, the set of states occurring in $\mathcal{B}(\beta)[H, 2H)$ and hence whether $\mathcal{B}$ accepts β can be determined in EXPSPACE. This proves (★).

Case 2. Suppose $\mu > 3$ and M is of Type 1. Apply Lemma 6.3.2 to (R, t) to construct $K \in \mathbb{N}$ and $\lambda \in \overline{\mathbb{Q}} \cap \mathbb{T}$ satisfying $\|\lambda\| < 2^{\textsc{Poly}(\mathcal{I})}$, $K < \exp^2(\textsc{Poly}(\mathcal{I}))$, and the following property. For each semialgebraic T and $0 \leq m < K$, there exists open semialgebraic $S(m, T) \subseteq \mathbb{T}$ and positive integer $N(m, T)$ with

$$N(m, T), \|S(m, T)\| < 2^{\textsc{Poly}(\|R\|+\|t\|+\|T\|)}$$

such that for all $n \geq N(m, T)$,

$$R^{nK+m} t \in T \;\Leftrightarrow\; \lambda^n \in S(m, T).$$

Recall that each β_r is the characteristic word of (R, t) with respect to $\mathcal{T}_r$. Intuitively, each β_r itself is the merge of K eventually toric words with semialgebraic parameters. It follows that β is the merge of $L \cdot K$ eventually toric words with semialgebraic parameters all generated by λ, and Theorem 4.4.2 applies. We next prove these statements formally.

For $0 \leq r < L$, let $\beta_{r,0}, \ldots, \beta_{r,K-1}$ be the K words whose merge is β_r. Hence β is the merge of

$$\beta_{0,0}, \beta_{1,0}, \ldots, \beta_{K-1,0}, \beta_{0,1}, \ldots, \beta_{L-1,K-1}.$$

We will show that each $\beta_{r,m}$ is an eventually toric word with semialgebraic parameters. Fix r, m. Recall that all $n \in \mathbb{N}$ and $T_i \in \mathcal{T}$,

$$T_i \in \beta_r(n) \;\Leftrightarrow\; R^n t \in T_i^{(r)}.$$

Hence for all $1 \leq i \leq \ell$ and $n \in \mathbb{N}$,

$$T_i \in \beta_{r,m}(n) \;\Leftrightarrow\; R^{nK+m} t \in T_i^{(r)}.$$

For $\sigma \in \Sigma$, define

$$X_\sigma = \bigcap_{T_i \in \sigma} T_i^{(r)} \cap \bigcap_{T_i \notin \sigma} \mathbb{R}^d \setminus T_i^{(r)}.$$

We have that each X_σ is open and semialgebraic with $\|X_\sigma\| < 2^{\textsc{Poly}(\mathcal{I})}$, and for all n,

$$\beta_{r,m}(n) = \sigma \;\Leftrightarrow\; R^{nK+m} \in X_\sigma.$$

Let $N_{r,m} = \max_\sigma N(m, X_\sigma)$ and $S_\sigma^{(r,m)} = S(m, X_\sigma)$ for all $\sigma \in \Sigma$. Observe that each $S_\sigma^{(r,m)}$ is open and semialgebraic with bit length at most $\exp^2(\textsc{Poly}(\mathcal{I}))$, and $N_{r,m} < \exp^2(\textsc{Poly}(\mathcal{I}))$. Moreover, for $n \geq N$, $\beta_{r,m}(n) = \sigma$ if and only of $\lambda^n \in S_\sigma^{(r,m)}$. Therefore, each $\beta_{r,m}$ is eventually toric with semialgebraic parameters $(\lambda, N_{r,m}, \mathcal{S}_{r,m})$ where $\mathcal{S}_{r,m} = \{S_\sigma^{(r,m)} \colon \sigma \in 2^{\mathcal{T}}\}$. To prove (✠) it remains to apply Theorem 4.2.3.

Applying Theorem 4.4.2, we conclude that β is effectively almost-periodic with

$$\mathcal{W}_\beta(l) < l^{\exp^2(\textsc{Poly}(\mathcal{I}))}$$

for $l \geq 2$. By Corollary 3.1.4, there exists effectively computable $H < \exp^3(\textsc{Poly}(\mathcal{I}))$ such that a state q appears infinitely often in $\mathcal{B}(\beta)$ if and only if it appears in $\mathcal{B}(\beta)[H, 2H)$. Therefore, using Lemma 5.4.1 whether $\mathcal{B}$ accepts β can be decided in 2EXPSPACE.

Case 3. Finally, suppose $\mu > 3$ and M is of Type 2. We will show that each β_r is ultimately constant and hence β is ultimately periodic with period L. Fix $0 \leq r < L$, and consider $T_i^{(r)} \in \mathcal{T}_r$. If $T_i^{(r)}$ is contained in a three-dimensional subspace of $\mathbb{R}^d$, then by Theorem 6.2.1 there exists

$$N_i^{(r)} < \exp^2\Big(\textsc{Poly}(\|R\| + \|t\| + \|T_i^{(r)}\|)\Big) < \exp^3(\textsc{Poly}(\mathcal{I}))$$

such that either $R^n t \in T_i^{(r)}$ or $R^n t \notin T_i^{(r)}$ holds for all $n \geq N_i^{(r)}$. On the other hand, if $T_i^{(r)}$ is not contained in a three-dimensional subspace, then it must be of semialgebraic dimension 1. By Lemma 6.3.4, there exists

$$N_i^{(r)} < \exp^5\Big(\textsc{Poly}(\|R\| + \|t\| + \|T_i^{(r)}\|)\Big) < \exp^6(\textsc{Poly}(\mathcal{I}))$$

with the same property as above. We conclude that there exists $N_r < \exp^6(\textsc{Poly}(\mathcal{I}))$ such that $\beta_r[N_r, \infty)$ is constant. Therefore, for

$$N = L \max_{0 \leq r \leq L} N_r < \exp^6(\textsc{Poly}(\mathcal{I}))$$

it holds that β is of the form uv^ω for $u \in \Sigma^N$ and $v \in \Sigma^L$. It follows that β is eventually toric with semialgebraic parameters $(\gamma, N, \mathcal{S})$ where γ is an Lth root of unity. Hence α is eventually toric with semialgebraic parameters $(\gamma, N + d, \{\gamma^d S_\sigma \colon S_\sigma \in \mathcal{S}\})$.

To prove (★), let h be the state of $\mathcal{B}$ after reading u, and $\mathcal{C}$ be the deterministic automaton with the start state h that is otherwise identical to $\mathcal{B}$. Using Lemma 5.4.1, the automaton $\mathcal{C}$ and the word w can be constructed in $\exp^5(\textsc{Poly}(\mathcal{I}))$ space. It holds that β is accepted by $\mathcal{B}$ if and only if v^ω is accepted by $\mathcal{C}$, which can be determined in space in $\textsc{Poly}(\|\mathcal{C}\|, \|v\|)$. Hence the problem of deciding whether $\mathcal{B}$ accepts β is in 5EXPSPACE. □

To extend the decidability result above to the class of tame predicates, as discussed in the introduction to this chapter, it suffices to give an algorithm that, given a set $\mathcal{T}$ of tame targets, constructs a set of low-dimensional sets that generate $\mathcal{T}$. We start by giving a characterisation of tame sets.

Lemma 6.4.2. *A set $T \subseteq \mathbb{R}^d$ is tame if and only if either T or $\mathbb{R}^d \setminus T$ is a union of low-dimensional sets.*

Proof. The ''if" direction follows from the definition of tame targets. To prove the other direction, suppose T is tame. Recall that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus B)$, $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus B)$, and $A \setminus (A \setminus B) = A \cap B$. Hence we can express T in the form

$$\bigcup_{i \in I} \bigcap_{j \in J} W_{i,j} \tag{6.5}$$

where each $W_{i,j}$ is either low-dimensional or a complement of a low-dimensional set. Define $V_{i,j} \coloneqq \mathbb{R}^d \setminus W_{i,j}$ for all i, j. Observe that the intersection of a low-dimensional set with any semialgebraic set is low-dimensional. Fix $i \in I$. If $W_{i,j}$ is low-dimensional for some $j \in J$ then $\cap_{j \in J} W_{i,j}$ is also low-dimensional. The other possibility is that for every $j \in J$, $W_{i,j}$ is a complement of a low-dimensional set. That is, $V_{i,j}$ is low-dimensional for all $j \in J$. In this case we can write

$$\bigcap_{j \in J} W_{i,j} = \mathbb{R}^d \setminus \bigcup_{j \in J} V_{i,j}.$$

Note that $\bigcup_{j \in J} V_{i,j}$ is a union of low-dimensional sets. We have so far shown that for every conjunct $U_i \coloneqq \cap_{j \in J} W_{i,j}$ in Equation (6.5), either (a) U_i is low-dimensional, or (b) the complement of U_i is low-dimensional. Write I_1 for the set of all $i \in I$ such that U_i is of Type (a), and $I_2 = I \setminus I_1$.

Suppose $a, b \in I_2$, i.e. $V_{a,j}, V_{b,j}$ are low-dimensional for all $j \in J$. We have

$$\begin{aligned} U_a \cup U_b &= \mathbb{R}^d \setminus \Big(\bigcup_{j \in J} V_{a,j} \cap \bigcup_{j \in J} V_{b,j} \Big) \\ &= \mathbb{R}^d \setminus \bigcup_{k,l \in J} (V_{a,k} \cap V_{b,l}). \end{aligned}$$

Since $V_{a,k} \cap V_{b,l}$ itself is low-dimensional, the complement of $U_a \cup U_b$ is a union of low-dimensional sets. We therefore conclude that T is a union of $X = \bigcup_{i \in I_1} U_i$ and $Y = \bigcup_{i \in I_2} U_i$ where X and the complement of Y are unions of low-dimensional sets.

If $X = \emptyset$ or $Y = \emptyset$, then the statement of the lemma follows. Suppose X, Y are both non-empty. Write $Y = \mathbb{R}^d \setminus \bigcup_{k \in K} A_k$ and $Z = \bigcup_{k \in K} A_k$, where each A_k s low-dimensional. Observe that

$$\begin{aligned} Y \cup X &= \mathbb{R}^d \setminus (Z \setminus X) \\ &= \mathbb{R}^d \setminus \bigcup_{k \in K} (A_k \setminus \bigcup_{i \in I_1} U_i) \\ &= \mathbb{R}^d \setminus \bigcup_{k \in K} \bigcap_{i \in I_1} A_k \setminus U_i \end{aligned}$$

Since each $A_k \setminus U_i$ is low-dimensional, by closure under intersections $\bigcap_{i \in I_1} A_k \setminus U_i$ is low-dimensional for every k. That is, the complement of $T = Y \cup X$ is a union of low-dimensional sets. This concludes the proof. □

Therefore, to decide whether a given semialgebraic target T is tame, we have to check whether T or its complement can be written as a union of low-dimensional sets.

Lemma 6.4.3. *Given semialgebraic $T \subseteq \mathbb{R}^d$, we can decide if it can be written as a union of low-dimensional sets. If yes, then we can effectively compute low-dimensional $S_1, \ldots, S_m$ such that $T = \bigcup_{i=1}^m S_i$.*

Proof. Using cell decomposition (Section 1.4), decompose T into disjoint semialgebraic $C_1, \ldots, C_l$ such that each C_i is homeomorphic to $(0,1)^{m_i}$ for some $m_i \in \mathbb{N}$. It suffices to check if each cell can be written as a union of low-dimensional sets and compute such a union when possible.

Suppose C_i can be written as a union $\bigcup_{j \in J} B_j$ of low-dimensional sets. Then C_i is contained in $\bigcup_{j \in J} \mathrm{Cl}(B_j)$, where $\mathrm{Cl}(B_j)$ is the Euclidean closure of B_j. Since C_i is irreducible, it is contained in $\mathrm{Cl}(B_j)$ for some j. Since $\mathrm{Cl}(B_j)$ is low-dimensional, so is C_i. Therefore, C_i can be written as a union of low-dimensional sets if and only if it is low-dimensional itself. We therefore have the following algorithm. Given T, compute $C_1, \ldots, C_l$. Each C_i is low-dimensional if and only if $m_i \leq 1$, or the subspace $\{x \in \mathbb{R}^d \mid \forall y \in C_i \colon x \cdot y = 0\}$ has dimension at least $d - 3$. If every C_i is low-dimensional, output $m = l$ and $S_i = C_i$ for $1 \leq i \leq m$. Otherwise, conclude that T cannot be written as a union of low-dimensional sets. □

Corollary 6.4.4. *Given set $T \subseteq \mathbb{R}^d$, we can decide if it is tame. If yes, we can effectively compute low-dimensional sets $S_1, \ldots, S_m$ such that either $T = \bigcup_{i=1}^m S_i$, or $T = \mathbb{R}^d \setminus \bigcup_{i=1}^m S_i$.*

Proof. Apply Lemma 6.4.3 to both T and $\mathbb{R}^d \setminus T$. □

We can now extend Theorem 5.4.2 to tame targets.

Theorem 6.4.5. *Let $M \in \mathbb{Q}^{d\times d}$, $s \in \mathbb{Q}^d$, $\mathcal{T} = \{T_1, \dots, T_\ell\}$ be a set of tame predicates, $\Sigma = 2^{\mathcal{T}}$, and $\mathcal{A}$ be a deterministic automaton over Σ.*

(✠) *The characteristic word α of (M, s) with respect to $\mathcal{T}$ is eventually toric with semialgebraic parameters.*

(★) *It is decidable whether $\mathcal{A}$ accepts α.*

Proof. First compute, using Corollary 6.4.4, a set $\mathcal{T}_1$ of low-dimensional predicates such that for each $T \in \mathcal{T}$, either T or $\mathbb{R}^d \setminus T$ is a union of sets from $\mathcal{T}_1$. Let $\Sigma_1 = 2^{\mathcal{T}_1}$, α_1 be the characteristic word of (M, s) with respect to $\mathcal{T}_1$, and $f\colon \Sigma_1 \to \Sigma$ be a renaming of letters such that $\alpha(n) = f(\alpha_1(n))$ for all $n \in \mathbb{N}$. We will construct an automaton $\mathcal{A}_1$ that accepts α_1 if and only if $\mathcal{A}$ accepts α, as described on page 113. The set of states, the initial state, and the acceptance condition of both $\mathcal{A}$ and $\mathcal{A}_1$ are identical. Let p, q be two states and $L \subseteq \Sigma$ be the set of all letters that, when read in $\mathcal{A}$ in state p, lead to state q. In $\mathcal{A}_1$, the set of all labels of all transitions from p to q is $f^{-1}(L)$.

Applying Theorem 6.4.1, α_1 is eventually toric with semialgebraic parameters $(\Gamma, N, \{S_\sigma\colon \sigma \in \Sigma_1\})$. The word α is then eventually toric with semialgebraic parameters $(\Gamma, N, \{\bigcup_{f(\mu)=\sigma} S_\mu\colon \sigma \in \Sigma\})$ by Lemma 4.2.2. This proves (✠). To prove (★), observe that $\mathcal{A}$ accepts α if and only if $\mathcal{A}_1$ accepts α_1, and invoke Theorem 6.4.1. □

Chapter 7

Diagonalisable systems and prefix-independent properties

In this chapter we study the Model-Checking Problem for *diagonalisable* linear dynamical systems, i.e. systems (M, s) where the matrix M is diagonalisable. Our main results are as follows. First, we show that the characteristic word α of such (M, s) with respect any set $\mathcal{T}$ of semialgebraic targets is eventually toric with semialgebraic parameters. We then use this result to give a procedure for deciding, in arbitrary ambient dimension, whether a given diagonalisable linear dynamical system satisfies a given *prefix-independent* property. Recall from Section 1.8 that these are the properties that do not depend on any finite prefix, i.e. whether an infinite word w satisfies a prefix-independent property φ does not change if we perform finitely many insertions and deletions on w. Finally, we show that the full Model-Checking Problem for diagonalisable systems (i.e. without the restriction to prefix-independent properties) is decidable if we assume decidability of the Positivity Problem for diagonalisable linear recurrence sequences over $\mathbb{Q}$.

Let (M, s) be a diagonalisable LDS, $\mathcal{T}$ be a collection of semialgebraic sets, and denote by α the characteristic word of (M, s) with respect to $\mathcal{T}$. The arguments we use to prove eventual toricity of α are quite different from the arguments of the preceding chapter showing eventual toricity of characteristic words of LDS with respect to tame targets. In particular, our main tool in this section is the fundamental lower bound of Theorem 2.4.2 on the growth rate of linear recurrence sequences. Due to the non-constructive nature of Theorem 2.4.2, our result has the following caveat. Given (M, s) and $\mathcal{T}$ as above, we show how to construct $d > 0, \Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$, and a collection $\mathcal{S}$ of semialgebraic subsets of $\mathbb{T}^d$ such that α is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$ for *some* integer N. In particular, we do not have an algorithm for determining a value for N given (M, s) and $\mathcal{T}$. Nevertheless, we are

able to prove decidability of the Model-Checking Problem restricted to diagonalisable systems and prefix-independent properties using the application of Semënov's theorem described in Section 3.2.[1] Our final model-checking algorithm is of the following form. Given be a diagonalisable LDS (M, s), a set of semialgebraic targets $\mathcal{T}$, and a prefix-independent automaton $\mathcal{A}$. Denote by α the characteristic word of (M, s) with respect to $\mathcal{T}$.

1. From $M, s, \mathcal{T}$ and $\mathcal{A}$ compute a large integer H.
2. Compute a word w of length $2H$ that occurs infinitely often in α.
3. Simulate $\mathcal{A}$ on w and record the set S of states that occur in $\mathcal{A}(w)[H, 2H)$. These are precisely the states that are visited infinitely often when $\mathcal{A}$ reads α.
4. Check S against the acceptance condition of $\mathcal{A}$.

As mentioned earlier, we will also show that for diagonalisable systems, the full Model-Checking Problem can be reduced to the Positivity Problem for diagonalisable linear recurrence sequences over $\mathbb{Q}$. Stated in geometric terms, if we can decide the Reachability Problem restricted to diagonalisable LDS and halfspace targets of the form $\{x \in \mathbb{R}^d \mid c^\top x \geq 0\}$ where $c \in \mathbb{Q}^d$, then we can decide the full MCP for diagonalisable systems.[2] A distinct step in our reduction is the non-trivial result of [45] that the Positivity Problem for LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ reduces to the Positivity Problem for LRS over $\mathbb{Q}$. We mention that for non-diagonalisable systems, it is not known whether the MCP can be reduced to the Reachability Problem.

The starting point of our proofs is the result of Ouaknine and Worrell [68] that, in stark contrast to the Positivity Problem, the Ultimate Positivity Problem is decidable for diagonalisable linear recurrence sequences (see Section 2.5). Recall the following geometric characterisation of the Ultimate Positivity Problem from Section 2.1. The LRS $u_n = c^\top M^n s$, where $c, s \in \mathbb{Q}^d$ and $M \in \mathbb{Q}^{d \times d}$, satisfies $u_n \geq 0$ for all sufficiently large n if and only if the the orbit $(M^n s)_{n \in \mathbb{N}}$ of the LDS (M, s) is eventually trapped in the halfspace $H = \{x \mid c^\top x \geq 0\}$. The latter, in turn, is a prefix-independent (and a liveness) property of the orbit of (M, s). In this chapter, we generalise the decidability result of Ouaknine and Worrell from the property of being eventually trapped in a halfspace to the class of prefix-independent properties over semialgebraic sets. Liveness properties turn out to be too general to be tractable,

[1] See [7] for our original proof that used specialised arguments instead of Semënov's theorem.
[2] See Section 2.1 for the equivalence between the Positivity and halfspace reachability problems.

as these already include reachability properties. Recall from Section 2.1 that the Reachability Problem for diagonalisable LDS subsumes the Skolem and Positivity problems for diagonalisable LRS, both of which are currently open.

We move onto proving the three main results of this chapter. Our first step will be to understand sign patterns of linear recurrence sequences of the form $u_n = p(M^n s)$, where M is diagonalisable and p is a polynomial.

Lemma 7.0.1. *Let $\lambda_1, \ldots, \lambda_m \in \overline{\mathbb{Q}}$ be non-zero, $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_m)$, $D = [\mathbb{K} : \mathbb{Q}]$, $L = (2D^2)!$, and $\Gamma = (\gamma_1, \ldots, \gamma_m)$ where $\gamma_i = \lambda_i/|\lambda_i|$ for all $1 \leq i \leq m$. Consider a real-valued sequence $u_n = p((\lambda_1^L)^n, \ldots, (\lambda_m^L)^n)$ that is not identically zero, where p is a polynomial with algebraic coefficients.*

(a) There exist N and effectively computable open semialgebraic sets $O_>, O_< \subseteq \mathbb{T}^m$ such that for all $n \geq N$, $u_n \neq 0$ and

$$u_n \,\Delta\, 0 \quad \Leftrightarrow \quad \Gamma^n \in O_\Delta$$

for $\Delta \in \{>, <\}$.

(b) Assuming decidability of the Positivity Problem for diagonalisable LRS over $\mathbb{Q}$, a value N as above can be effectively computed.

Note that according to the statement (a) above, we can effectively compute representations of $\Gamma, O_>$ and $O_<$, whereas nothing is promised about the effectiveness of N. The value of L is chosen to guarantee non-degeneracy of $(u_n)_{n\in\mathbb{N}}$.

Proof. Write $u_n = \sum_{j=1}^{A} c_j \Lambda_j^n$ where $\Lambda_1, \ldots, \Lambda_A$ pairwise distinct and c_j, Λ_j are non-zero algebraic numbers for all j. As discussed in Section 2.2, $A = 0$ if and only if u_n is identically zero. Since u_n is not identically zero by assumption, $A > 0$. Since u_n is real-valued, by Lemma 2.2.3 for each j there exists i such that $\overline{c_j} = c_i$ and $\overline{\Lambda_j} = \Lambda_i$.

We can express each Λ_j in the form

$$\Lambda_j = r_j \left(\gamma_1^{k_{1,j}} \cdots \gamma_m^{k_{m,j}}\right)^L$$

where $k_{1,j}, \ldots, k_{m,j}$ are non-negative and $r_j = |\Lambda_j| > 0$ is real algebraic. Define $R = \max_{1\leq j\leq A} r_j$, $\mathcal{D} = \{j : r_j = R\}$ and $\mathcal{R} = \{j : r_j < R\}$, and write

$$u_n = \underbrace{\sum_{j\in\mathcal{D}} c_j \Lambda_j^n}_{d_n} + \underbrace{\sum_{j\in\mathcal{R}} c_j \Lambda_j^n}_{r_n}.$$

Here d_n is the *dominant* part of v_n. Since $\mathcal{D}$ is non-empty, d_n is not identically zero. Since $(u_n)_{n\in\mathbb{N}}$ is real-valued and Λ_j has the same magnitude as $\overline{\Lambda_j}$, all conjugates are present in the expression for d_n, and $(d_n)_{n\in\mathbb{N}}$ is also real-valued (see Lemma 2.2.3). Define R_1 to be 0 if $\mathcal{R}$ is empty and $\max_{j\in\mathcal{R}} R_j$ otherwise. We next argue that $(d_n)_{n\in\mathbb{N}}$ is non-degenerate and hence by the result of Berstel and Mignotte (Section 2.7), $d_n \neq 0$ for sufficiently large n.

Let $j_1, j_2 \in \mathcal{D}$. Observe that $\Lambda_{j_1}/\Lambda_{j_2}$ is of the form γ^L where $\gamma = \gamma_1^{k_1} \cdots \gamma_m^{k_m}$ for some $k_1, \ldots, k_m \in \mathbb{Z}$. Moreover, $\Lambda_{j_1}/\Lambda_{j_2}$ is a root of unity if and only if γ is a root of unity. Since γ belongs to $\mathbb{K}$, by Lemma 5.3.1, if it is a root of unity then its order is at most $2D^2$ and hence divides L. Therefore, γ is a root of unity if and only if $\gamma^L = 1$, i.e. $\Lambda_{j_1} = \Lambda_{j_2}$. Moreover, since L is even, for al $j \in \mathcal{D}$, if $\Lambda_j \in \mathbb{R}$ then $\Lambda_j > 0$. We conclude that d_n is not identically zero and non-degenerate.

Let $M = (R + R_1)/2$. Applying Theorem 2.4.2 to $(d_n)_{n\in\mathbb{N}}$, there exists N_1 such that for all $n \geq N_1$, $|d_n| > M^n$. Since $M > R_1 \geq 0$, there exists $N \geq N_1$ such that for all $n \geq N$, $M^n > |r_n|$ and hence $|d_n| > |r_n|$. Since the sequence $(d_n)_{n\in\mathbb{N}}$ is real-valued, it follows that for $n \geq N$, both d_n and u_n are non-zero and $\operatorname{sign} d_n = \operatorname{sign} u_n$.

It remains to express $\operatorname{sign} d_n$ in terms of Γ^n for $n \geq N$. For $j \in \mathcal{D}$, let

$$f_j(z_1, \ldots, z_m) \coloneqq c_j \left(z_1^{k_{1,j}} \cdots z_m^{k_{m,j}}\right)^L.$$

With this definition, for all $n \in \mathbb{N}$,

$$d_n = R^n \sum_{j\in\mathcal{D}} c_j f_j(\gamma_1^n, \ldots, \gamma_m^n).$$

We can therefore define

$$O_\Delta = \{(z_1, \ldots, z_m) \in \mathbb{T} \mid \sum_{i\in\mathcal{D}} c_i f_i(z_1, \ldots, z_m) \;\Delta\; 0\}$$

for $\Delta \in \{>, <\}$. Observe that each O_Δ is open and semialgebraic. In particular, an effective representation of O_Δ can be computed using Lemma 1.5.5. This completes the proof of (a).

We now prove (b). As mentioned earlier, [45] shows that the Positivity Problem for sequences over $\mathbb{R} \cap \overline{\mathbb{Q}}$ reduces to the Positivity Problem for sequences over $\mathbb{Q}$. Hence we assume an oracle for the former problem. Let $M = (R + R_1)/2$ as above. By the choice of M, we can effectively compute $N_1 \in \mathbb{N}$ such that for all $n \geq N_1$, $M^n > |r_n|$. On the other hand, by Theorem 2.4.2, there exists N_2 such that for all $n \geq N_2$, $|d_n| > M^n$. Such N_2 can be determined using a Positivity oracle for diagonalisable LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$ as follows. Let $w_n = d_n^2 - M^{2n}$ and $w_n^{(k)} = w_{n+k}$ for

$k \geq 0$. Since $d_n \in \mathbb{R} \cap \overline{\mathbb{Q}}$ for all n and $M \in \mathbb{R} \cap \overline{\mathbb{Q}}$, $(w_n)_{n\in\mathbb{N}}$ is an LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$. As discussed in Chapter 2, for all k the sequence $(w_n^{(k)})_{n\in\mathbb{N}}$ is diagonalisable. Finally, by construction, $w_n \geq 0$ for sufficiently large n. Hence the smallest possible value for N_2 can be determined by asking the Positivity oracle whether $w_n^{(k)} \geq 0$ for all $n \in \mathbb{N}$ for increasing values of k, starting with $k = 0$. Finally, we select $N = \max\{N_1, N_2\}$. □

We next lift the previous lemma to show that characteristic words of diagonalisable systems with respect to sets of semialgebraic targets are eventually toric.

Lemma 7.0.2. *The characteristic word α of diagonalisable $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ with respect to any family $\mathcal{T}$ of semialgebraic targets is eventually toric with semialgebraic parameters $(N, \Gamma, \mathcal{S})$, where*

(a) representations of $\Gamma, \mathcal{S}$ can be effectively computed, and

(b) N can be effectively computed using an oracle for the Positivity Problem for diagonalisable linear recurrence sequences over $\mathbb{Q}$.

Proof. Denote by $\lambda_1, \ldots, \lambda_m$ the non-zero eigenvalues of M and write $\mathcal{T} = \{T_1, \ldots, T_\ell\}$. Let $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_m)$, $D = [\mathbb{K} : \mathbb{Q}]$, $L = (2D^2)!$, and

$$\Gamma = (\lambda_1/|\lambda_1|, \ldots, \lambda_m/|\lambda_m|).$$

We will consider the L sequences $\alpha_0, \ldots, \alpha_{L-1}$, defined by $\alpha_r(q) = \alpha(qL + r)$ for $0 \leq r < L$ and $q \in \mathbb{N}$. Note that the merge of $\alpha_0, \ldots, \alpha_{L-1}$ is α.

Write $\mathcal{T} = \{T_1, \ldots, T_\ell\}$. By flattening each $\mathcal{T}_i$ using Lemma 1.3.4, we can construct polynomials $p_1, \ldots, p_K \in \mathbb{Q}[x_1, \ldots, x_d]$ that define $\mathcal{T}$. Fix $0 \leq r < L$. For $1 \leq i \leq K$, let $u_n^{(i)} = p_i(M^{nL+r}s)$, and denote by $\beta_i \in \{+, 0, -\}^\omega$ the sign pattern of $(u_n^{(i)})_{n\in\mathbb{N}}$. We can compute the exponential polynomial representation of each $u_n^{(i)}$ using Lemma 2.2.5 and check whether $u_n^{(i)}$ is identically zero using Lemma 2.2.1.

Since each $u_n^{(i)}$ is of the form $h_i(\lambda_1^{nL}, \ldots, \lambda_m^{nL})$ for a polynomial h_i with algebraic coefficients, by Lemma 7.0.1 each β_i is eventually toric with parameters $(\Gamma, N_i, \mathcal{S}_i)$, where $\mathcal{S}_i = \{S_+^{(i)}, S_0^{(i)}, S_-^{(i)}\}$ consists of open semialgebraic subsets of $\mathbb{T}^m$, and N_i can be effectively computed using an oracle for the Positivity Problem for diagonalisable LRS over $\mathbb{Q}$.[3] Since $\mathcal{T}$ is defined by inequalities involving $p_1, \ldots, p_K$, there exists

$$f\colon \{+, 0, -\}^K \to 2^{\mathcal{T}}$$

[3] If $(p_i(M^n s))_{n\in\mathbb{N}}$ is identically zero, then $N_i = 0$ and $S_+^{(i)} = S_-^{(i)} = \emptyset$ and $S_0^{(i)} = \mathbb{T}$.

such that for all $n \in \mathbb{N}$,

$$f(\beta_1(n), \ldots, \beta_K(n)) = \alpha_r(n).$$

Applying Lemmas 4.2.1 and 4.2.2, we conclude that α_r is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$ where $\mathcal{S}$ can be effectively computed and N can be effectively computed assuming decidability of the Positivity Problem for diagonalisable sequences. It remains to invoke Theorem 4.2.3 to conclude that α is also eventually toric with semialgebraic parameters. □

Interestingly, the lemma above implies that the word α is *effectively* almost-periodic. That is, there exists *some* program $\mathcal{P}_2$ that, given a finite word u, decides whether u occurs in α and computes a bound on the gaps between consecutive occurrences of u in α (see page 72). As a result, there exists *some* algorithm that decides the Acceptance Problem[4] for α.

Theorem 7.0.3. *Let α be the characteristic word of diagonalisable (M, s) with respect to a collection $\mathcal{T}$ of semialgebraic targets.*

(a) The word α is effectively almost-periodic.

(b) The Acceptance Problem for α is decidable.

Proof. Lemma 7.0.2 shows that α is eventually toric with semialgebraic parameters. To prove (a), recall that eventually toric words with semialgebraic parameters are effectively almost-periodic (Theorem 4.3.1). Statement (b) follows from (a) and Semënov's theorem (Chapter 3). □

The statements (a-b) of Theorem 7.0.3 also hold for any α that is the characteristic word of an arbitrary LDS (M, s) with respect to a collection $\mathcal{T}$ of tame targets; Such α was shown to be eventually toric with semialgebraic parameters in the preceding chapter. However, in this case, the word α is eventually toric with parameters $(\Gamma, N, \mathcal{S})$ all of which can be effectively computed given $M, s, \mathcal{T}$. Hence the Model-Checking Problem for tame targets and the Acceptance Problem for any characteristic word of an LDS with respect to a set of tame targets are both decidable.

We now state and prove conditional decidability of the Model-Checking Problem for diagonalisable systems and unconditional decidability of the MCP restricted to diagonalisable systems and prefix-independent properties.

[4]Recall from the Introduction that the Acceptance Problem for α is to decide whether a given automaton $\mathcal{A}$ accepts α.

Theorem 7.0.4.

(✠) *Given a diagonalisable linear dynamical system (M, s), a set $\mathcal{T}$ of semialgebraic predicates, and a prefix-independent automaton $\mathcal{A}$, it is decidable whether $\mathcal{A}$ accepts the characteristic word α of (M, s) with respect to $\mathcal{T}$.*

(★) *If we assume the Positivity Problem is decidable for diagonalisable linear recurrence sequences over $\mathbb{Q}$, then the full Model-Checking Problem is decidable for diagonalisable systems.*

Proof. We first prove (★). Let α be the characteristic word of diagonalisable (M, s) with respect to a collection of semialgebraic sets $\mathcal{T}$. By Lemma 7.0.2, α is eventually toric with semialgebraic parameters $(\Gamma, N, \mathcal{S})$, where $\mathcal{S} = \{S_\sigma \mid \sigma \in \Sigma\}$ and $\Sigma = 2^{\mathcal{T}}$. Under the assumption that the Positivity Problem is decidable for diagonalisable LRS over $\mathbb{Q}$, the value of N can be effectively computed. Thereafter, using Theorem 4.3.4 we can compute (e.g. as a formula) a window function $\widetilde{\mathcal{W}}$ for α satisfying $\widetilde{\mathcal{W}}(l) \geq \mathcal{W}(l)$ for all $l \in \mathbb{N}$. We can then use the algorithm of Corollary 3.1.4 to decide whether $\mathcal{A}$ accepts α.

It remains to show how to unconditionally determine whether a prefix-independent automaton accepts α above that is eventually toric with parameters $(\Gamma, N, \mathcal{S})$. Recall from Lemma 7.0.2 that we can effectively compute representations of Γ and $\mathcal{S}$. By Theorem 4.3.4, the word $\beta \coloneqq \alpha[N, \infty)$ is almost-periodic with the window function

$$\widetilde{\mathcal{W}}(l) = 2^{(l+||\Gamma||+||\mathcal{S}||)^{\textsc{Poly}(d)}}$$

for all $l \in \mathbb{N}$. That is, even though we do not where β begins in α, we can effectively compute an upper bound on $\mathcal{W}_\beta(l)$ for all l.

We gave the following algorithm in Section 3.2 for deciding whether a prefix-independent automaton $\mathcal{A}$ with the set of states Q accepts α.

1. Compute
$$H = 2\widetilde{\mathcal{W}}^{|Q|+1}(2\widetilde{\mathcal{W}}^{|Q|+1}(1) + 1).$$
2. Compute a word w of length $2H$ that occurs infinitely often in α.
3. Simulate $\mathcal{A}$ on w and record the set S of states that occur in $\mathcal{A}(w)[H, 2H)$. The set S is exactly the set of states that are visited infinitely often when $\mathcal{A}$ reads α.
4. Check S against the acceptance condition of $\mathcal{A}$.

It remains to show how to implement Step 2. For this, it suffices to give a procedure that determines whether a given finite word u of length $2H$ occurs infinitely often in β. By definition of eventually toricity, u occurs at a position $n \geq N$ in α if and only if

$$\begin{aligned}\bigwedge_{k=0}^{2H-1} \alpha(n+k) = u(k) &\Leftrightarrow \bigwedge_{k=0}^{2H-1} \Gamma^{n+k} \in S_{u(k)} \\ &\Leftrightarrow \bigwedge_{k=0}^{2H-1} \Gamma^{n} \in \Gamma^{-k} S_{u(k)} \\ &\Leftrightarrow \Gamma^n \in \bigcap_{k=0}^{2H-1} \Gamma^{-k} S_{u(k)}.\end{aligned}$$

Let $S_u = \mathbb{T}_\Gamma \cap \bigcap_{k=0}^{2H-1} \Gamma^{-k} S_{u(k)}$, where $\mathbb{T}_\Gamma$, as in Theorem 4.1.4, is the Euclidean closure of $(\Gamma^n)_{n\in\mathbb{N}}$ Observe that S_u is semialgebraic and an open subset of $\mathbb{T}_\Gamma$. By Theorem 4.1.4, $\Gamma^n \in S_u$ for infinitely many values of n if and only if $S_u \neq \emptyset$. Hence determining whether u occurs infinitely often in β is equivalent to checking whether the semialgebraic set S_u is non-empty. □

The complexity bound we can prove for (★) is TOWER, i.e. non-elementary. The main reason for this is that the window function $\widetilde{\mathcal{W}}(l)$ for β guaranteed by Theorem 4.3.4 is not polynomial in l.[5] This makes the quantity $\widetilde{\mathcal{W}}^{|Q|+1}(1)$ non-elementary in the input size. As long as we use the framework of almost periodicity and Semënov's theorem, an algorithm with elementary complexity seems unlikely. In fact, the original ad hoc (i.e. not directly based on almost periodicity) model-checking algorithm that we gave in [7] also has non-elementary complexity.

As discussed in Chapter 2, we currently do not know how to decide the Positivity Problem for diagonalisable sequences, or whether this is at all possible. For non-diagonalisable systems almost none of the methods we used in this section are applicable. For example, consider $u_n = p(M^n s)$ not identically zero, where M is non-diagonalisable. Scaling u_n by the magnitude of the largest eigenvalue and applying Theorem 2.4.2, we can conclude that there exists N such that for all $n \geq N$, the sign of u_n is the same as the sign of $d_n = \sum_{j=1}^{A} p_j(n)\gamma_j^n$ where $\gamma_j \in \mathbb{T} \cap \overline{\mathbb{Q}}$ and $p_j \in \overline{\mathbb{Q}}[x]$ for all j. We will show in the following chapter that the sign pattern of $(d_n)_{n\in\mathbb{N}}$ can in fact be not toric and not almost-periodic. Hence the statement of Lemma 7.0.2 does not hold for non-diagonalisable systems.

[5] This is in contrast to the window functions for toric words generated by a single rotation $\Gamma \in \mathbb{T}$, which appeared in Chapters 5 and 6.

Chapter 8

Hard instances of the Model-Checking Problem

Recall that the Model-Checking Problem in its full generality is to decide, given a linear dynamical system (M, s), a set $\mathcal{T}$ of semialgebraic targets, and a deterministic automaton $\mathcal{A}$, whether $\mathcal{A}$ accepts the characteristic word α of (M, s) with respect to $\mathcal{T}$. We have shown decidability of the MCP in the following two cases.

(A) All semialgebraic targets in $\mathcal{T}$ are *low-dimensional*, i.e. every $T \in \mathcal{T}$ is either of semialgebraic dimension at most 1 or contained in a linear subspace of dimension at most 3.[1]

(B) M is diagonalisable and $\mathcal{A}$ is prefix-independent.

In this chapter we will show that substantially improving either (A) or (B) would lead to major mathematical breakthroughs. Specifically, we will use *Diophantine hardness* (Section 8.1) and reductions from open cases of the Skolem and Positivity problems as evidence of intractability. Below is a summary of our results.

(1) Already in the ambient space $\mathbb{R}^4$, both reachability and infinite reachability problems of the class of semialgebraic sets of dimension 2 are Diophantine-hard. Note that infinite reachability is a prefix-independent property. Since every subset of $\mathbb{R}^4$ is trivially contained in a four-dimensional subspace, it follows that the reachability and infinite reachability problems of the class of semialgebraic sets contained in a four-dimensional subspace are also Diophantine-hard. Therefore, the MCP for both aforementioned generalisations of low-dimensional targets is intractable, even if we restrict $\mathcal{A}$ to be prefix-independent.

[1] Recall from Chapter 6 that we also showed decidability for tame targets by reducing the MCP with tame targets to the MCP with low-dimensional targets.

(2) The Reachability Problem for diagonalisable systems subsumes the Skolem and Positivity problems for diagonalisable sequences. In ambient dimension 4, the Reachability Problem is at least as hard as the Skolem Problem for sequences of order 5. Recall that reachability properties are not prefix-independent. Therefore, in (B) above, if we drop (only) the prefix-independence restriction, then the resulting model-checking problem subsumes the Skolem and Positivity problems, becoming intractable already in ambient dimension 4. If we drop the diagonalisability restriction in (B), then we obtain a Diophantine-hard problem already in ambient dimension 4 as discussed in (1).

We will also show that the characteristic word of a linear dynamical system (M, s) with respect to a single target of semialgebraic dimension 2 or a single target contained in a four-dimensional space can be not be almost-periodic and hence not eventually toric. This makes all approaches based on Semënov's theorem and the theory of toric words inapplicable to model checking problems involving such targets, further substantiating hardness of generalising (A).

8.1 Overview of Diophantine hardness

Let $x \in \mathbb{R}$. The *Lagrange constant* (or the *homogenous Diophantine approximation constant*) of x is defined as

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

Writing $[\![y]\!]$ for the distance from $y \in \mathbb{R}$ to a nearest integer, $L_\infty(x) < b$ means that for infinitely many integers $n > 0$, there exists $m \in \mathbb{N}$ such that $|nx - m| < b/n$, which is equivalent to $[\![nx]\!] < b/n$. Hence we can equivalently define

$$L_\infty(x) = \liminf_{n\to\infty} n[\![nx]\!].$$

The Lagrange constant, alongside the *irrationality measure*, is actively studied in Diophantine approximation. Nevertheless, we only know how to compute $L_\infty(x)$ to arbitrary precision only for a very restricted class of real numbers x.

Dirichlet proved, using the Pigeonhole Principle, that for every $x \in \mathbb{R}$ there exist infinitely many integers n, m such that $|x - m/n| \leq 1/n^2$. That is, $L_\infty(x) \leq 1$ for all x. Hurwitz showed that for every irrational $x \in \mathbb{R}$, $L_\infty(x) \leq 1/\sqrt{5}$, which is the best possible as the Lagrange constant of the golden ratio is exactly $1/\sqrt{5}$. The Lagrange constant of x is usually studied through its *continued fraction expansion*.

For algebraic numbers of degree at most 2, as well as certain special transcendental numbers (e.g. Euler's constant), the continued fraction expansion can be described in a finitary manner and hence the Lagrange constant can be computed exactly. For other numbers, no general method is known that, given x and a threshold c, compares $L_\infty(x)$ against c. We do know, however, that the *Lagrange spectrum* $\{L_\infty(x) \mid x \in \mathbb{R} \setminus \mathbb{Q}\}$ contains countably many numbers in the interval $(1/3, 1/\sqrt{5})$ called *Lagrange numbers*, as well as the whole interval $(0, 1/F]$ where $F \approx 4.52783$ is Freiman's constant. We refer the reader to the wonderful book [19] by Borwein et al. for an introduction to Diophantine approximation and the theory of continued fractions.

We next define the (*homogenous Diophantine approximation*) *type* of x as

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

Observe that $L(x) \leq L_\infty(x)$ for all x. In fact, if $u_n = p_n/q_n$ is the sequence of *convergents* of x (i.e. rational approximations of x of increasing quality satisfying $\lim_{n\to\infty} \frac{p_n}{q_n} = x$) obtained from the continued fraction expansion of x, then

$$L_\infty(x) = \limsup_{n\geq 0} \left(q_n|q_n x - p_n|\right)^{-1}$$

and

$$L(x) = \sup_{n\geq 0} \left(q_n|q_n x - p_n|\right)^{-1}.$$

See [51] for a discussion of $L_\infty(x)$ and $L(x)$, as well as their relationship to various other quantities from Diophantine approximation. For our purposes, we will only need the fact it is only known how to compute or even estimate $L(x)$ or $L_\infty(x)$ for very specific values of x. Hence finding an algorithm to compute $L(x)$ or $L_\infty(x)$ to arbitrary precision for a large class of numbers would amount to a major mathematical breakthrough. The Positivity Problem and the Ultimate Positivity Problem are two well-known examples of decision problems that are Diophantine-hard in this sense. Recall that we denote by $\mathbb{T}$ the unit circle in $\mathbb{C}$, and let

$$\begin{aligned}\mathcal{G} &= \{p + q\boldsymbol{i} \mid p, q \in \mathbb{Q}\} \cap \mathbb{T},\\ \mathcal{L} &= \{\mathrm{Log}(\alpha)/(\boldsymbol{i}2\pi) \colon \alpha \in \mathcal{G}\}.\end{aligned}$$

The set $\mathcal{L}$ is dense in $(-1/2, 1/2]$, and contains transcendental numbers with the only exceptions $-1/4$, 0, $1/4$, $1/2$. Consider linear recurrence sequences of the form

$$\begin{aligned}u_n^{\lambda,r} &= -n1^n + \frac{1}{2}(n - ri)\lambda^n + \frac{1}{2}(n + ri)\overline{\lambda^n}\\ &= r\,\mathrm{Im}(\lambda^n) - n(1 - \mathrm{Re}(\lambda^n)).\end{aligned}$$

where $r \in \mathbb{Q}$ and $\lambda \in \mathbb{T} \cap \mathbb{Q}(\boldsymbol{i})$. Each $(u_n^{\lambda,r})_{n\in\mathbb{N}}$ is an LRS over $\mathbb{Q}$ of order at most 6. The following are established in [66].

Theorem 8.1.1 (Diophantine hardness of Positivity)**.** *Suppose it is decidable, given $\lambda \in \mathcal{G}$ and $r \in \mathbb{R}$, whether $u_n^{\lambda,r} \geq 0$ for all n. Then $L(x)$ can be computed to arbitrary precision for any $x \in \mathcal{L}$.*

Theorem 8.1.2 (Diophantine hardness of Ultimate Positivity)**.** *Suppose it is decidable, given $\lambda \in \mathcal{G}$ and $r \in \mathbb{R}$, whether there exists N such that $u_n^{\lambda,r} \geq 0$ for all $n \geq N$. Then for any $x \in \mathcal{L}$, $L_\infty(x)$ can be computed to arbitrary precision.*

In the following section we will prove Diophantine hardness by showing that solving various special cases of the Model-Checking Problem (that lie just outside the scope of our decidability results) would give us means to estimate $L(x)$ or $L_\infty(x)$ for the class $\mathcal{L}$ above.

8.2 Targets that are not low-dimensional

For target sets of semialgebraic dimension 2, already in ambient dimension 4 every approach we have used so far to decide the Model-Checking Problem is shattered, and we are faced with Diophantine hardness. Let

$$\mathcal{H} \coloneqq \{T \subseteq \mathbb{R}^4 \mid T \text{ is semialgebraic with dimension } 2\}$$

and recall the definition of $\mathcal{L}$ above. We will prove the following.

Theorem 8.2.1 (Diophantine hardness of reachability)**.** *Suppose it is decidable, given $(M, s) \in \mathbb{Q}^{4\times4} \times \mathbb{Q}^4$ and $T \in \mathcal{H}$, whether there exists $n \in \mathbb{N}$ such that $M^n s \in T$. Then $L(x)$ can be approximated to arbitrary precision for every $x \in \mathcal{L}$.*

Theorem 8.2.2 (Diophantine hardness of infinite reachability)**.** *Suppose it is decidable, given $(M, s) \in \mathbb{Q}^{4\times4} \times \mathbb{Q}^4$ and $T \in \mathcal{H}$, whether there exist infinitely many values n such that $M^n s \in T$. Then $L_\infty(x)$ can be approximated to arbitrary precision for every $x \in \mathcal{L}$.*

We will also give an example of $T \in \mathcal{H}$ and $(M, s) \in \mathbb{Q}^{4\times4} \times \mathbb{Q}^4$ such that the characteristic word of (M, s) with respect to $\mathcal{T} = \{T\}$ is not almost-periodic and hence not eventually toric either. Observe that every $T \in \mathcal{H}$ is trivially contained in a four-dimensional subspace. Hence for the class

$$\widehat{\mathcal{H}} \coloneqq \bigcup_{k\in\mathbb{N}} \{T \subseteq \mathbb{R}^k \mid T \text{ is contained in a subspace of } \mathbb{R}^k \text{ of dimension at most } 4\}$$

it also holds that if reachability (resp. infinite reachability) were decidable, then $L(x)$ (resp. $L_\infty(x)$) can be approximated to arbitrary precision for every $x \in \mathcal{L}$. Note that "the orbit $(M^n s)_{n\in\mathbb{N}}$ visits T infinitely often" is a prefix-independent property. Hence both reachability and prefix-independent model-checking are Diophantine-hard for the classes $\mathcal{H}$ and $\widehat{\mathcal{H}}$ of targets.

For $r \in \mathbb{R}$ and $\lambda \in \mathcal{G}$, where $\mathcal{G} = \mathbb{Q}(i) \cap \mathbb{T}$ as above, define

$$v_n^{\lambda,r} = u_n^{\lambda,r} \cdot (\operatorname{Im}(\lambda^n))^2 = r\,(\operatorname{Im}(\lambda^n))^3 - n\,(\operatorname{Im}(\lambda^n))^2\,(1 - \operatorname{Re}(\lambda^n)).$$

Assuming λ is not a root of unity, $\operatorname{Im}(\lambda^n) \neq 0$ and hence $\operatorname{sign}(u_n^{\lambda,r}) = \operatorname{sign}(v_n^{\lambda,r})$ for all $n \geq 1$. It will be more convenient to work with $(v_n^{\lambda,r})_{n\in\mathbb{N}}$. For $\lambda \in \mathcal{G}$, let

$$R_\lambda = \begin{bmatrix} \operatorname{Re}(\lambda) & -\operatorname{Im}(\lambda) \\ \operatorname{Im}(\lambda) & \operatorname{Re}(\lambda) \end{bmatrix}$$

and

$$M_\lambda = \begin{bmatrix} R_\lambda & I \\ & R_\lambda \end{bmatrix}.$$

Further let $s = (0, 0, 0, 1)$, and for $\lambda \in \mathcal{G}$ and $n \in \mathbb{N}$ write

$$z(\lambda, n) \coloneqq (-\operatorname{Im}(\lambda^n), \operatorname{Re}(\lambda^n)).$$

It holds that

$$M_\lambda^n s = (-n \operatorname{Im}(\lambda^{n-1}), n \operatorname{Re}(\lambda^{n-1}), -\operatorname{Im}(\lambda^n), \operatorname{Re}(\lambda^n)) = (nR_\lambda^{-1} \cdot z(\lambda, n), z(\lambda, n)).$$

In particular, for every $(x_1, x_2, x_3, x_4) = M_\lambda^n s$ for some n, (x_3, x_4) lies on the unit circle and

$$(x_1, x_2) = nR_\lambda^{-1}(x_3, x_4). \tag{8.1}$$

Writing $p_\lambda(x_1, x_2, x_3, x_4) \coloneqq \operatorname{Re}(\lambda)x_1 - \operatorname{Im}(\lambda)x_2$ we have that

$$p_\lambda(M_\lambda^n s) = -n \operatorname{Im}(\lambda^n). \tag{8.2}$$

Intuitively, p_λ multiplies (x_1, x_2) by the rotation matrix R_λ and then extracts x_1. Writing $q_{\lambda,r}(x_1, x_2, x_3, x_4) \coloneqq -rx_3^3 + p_\lambda(x_1, x_2, x_3, x_4)x_3(1 - x_4)$, we obtain

$$v_n(\lambda, r) = q_{\lambda,r}(M_\lambda^n s).$$

If we choose T to be $\{x \in \mathbb{R}^4 \colon q_{\lambda,r}(x) < 0\}$, then for all n, $u_n^{\lambda,r} < 0$ (and hence $v_n^{\lambda,r} < 0$) for some n if and only if $M_\lambda^n s \in T$. We have thus related the condition $v_n \geq 0$ to non-reachability in T. Observe that T need not be two-dimensional. To remedy this,

we will construct, for every $\lambda \in \mathcal{G}$, a semialgebraic set $S_\lambda \subset \mathbb{R}^4$ of dimension 2 that contains the orbit of (M_λ, s). We can then consider reachability in $T \cap S_\lambda$ and $S_\lambda \setminus T$, both of which have semialgebraic dimension at most 2.

Let $x(t) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ and recall that the unit circle in $\mathbb{R}^2$ can be expressed in the parametric form as $\{(-1,0)\} \cup \{x(t) \colon t \in \mathbb{R}\}$. We make the following definitions.

$$\begin{aligned} f_\lambda(s,t) &= (sR_\lambda^{-1} \cdot x(t), x(t)) \\ A_\lambda &= \{f(s,t) \colon s,t \in \mathbb{R}\} \\ B_\lambda &= \{(sR_\lambda^{-1}(-1,0), -1, 0) \colon s \in \mathbb{R}\} \\ S_\lambda &= A_\lambda \cup B_\lambda. \end{aligned}$$

Recall (from Equation (8.1)) that for every $\lambda \in \mathcal{G}$ and $(x_1, x_2, x_3, x_4) = M_\lambda^n s$ occurring in the orbit of (M_λ, s), (x_3, x_4) lies on the unit circle and

$$(x_1, x_2) = nR_\lambda^{-1}(x_3, x_4).$$

Hence $M_\lambda^n s \in S_\lambda$ for all λ and n. Since S_λ is rationally parametrised using two parameters, it has dimension at most (in fact exactly) 2. Another way to see this is to observe that f_λ maps $\mathbb{R}^2$ onto A_λ homeomorphically. Similarly, B_λ is homeomorphic to $\mathbb{R}$. Since dimension of semialgebraic sets is preserved under homeomorphisms, $\dim(A_\lambda) = 2$, $\dim(B_\lambda) = 1$, and $\dim(S_\lambda) = \max\{\dim(A_\lambda), \dim(B_\lambda)\} = 2$.

Proof of Theorem 8.2.1. Suppose the Reachability Problem is decidable in ambient dimension 4 for the class of targets $\mathcal{H}$. By Theorem 8.1.1, it suffices to show that given $r \in \mathbb{R}$ and $\lambda \in \mathcal{G}$, we can decide whether $u_n^{\lambda,r} \geq 0$ for all $n \in \mathbb{N}$. First suppose λ is a root of unity. Since $\lambda \in \mathbb{Q}(i)$, it must be one of $1, \boldsymbol{i}, -1, \boldsymbol{i}$, in which case whether $u_n^{\lambda,r} \geq 0$ holds for all n can be verified directly. Suppose therefore λ is not a root of unity. As mentioned earlier, $\operatorname{sign}(v_n^{\lambda,r}) = \operatorname{sign}(u_n^{\lambda,r})$ for $n \geq 1$; Moreover, $v_0^{\lambda,r} = 0$. If $u_0^{\lambda,r} < 0$, then we are done. Suppose $u_0^{\lambda,r} \geq 0$. It remains to determine whether $v_n^{\lambda,r} \geq 0$ for all $n \in \mathbb{N}$. Let $M = M_\lambda$, $s = (0,0,0,1)$, and

$$T = S_\lambda \cap \{x \in \mathbb{R}^4 \colon q_{\lambda,r}(x) < 0\}.$$

The set T is semialgebraic and has dimension at most 2 as $\dim(S_\lambda) = 2$. Hence $T \in \mathcal{H}$. Since $M^n s \in S_\lambda$ for all n,

$$M^n s \in T \quad \Leftrightarrow \quad q_{\lambda,r}(M^n s) < 0. \tag{8.3}$$

Recall that $q_{\lambda,r}(M^n s) = v_n^{\lambda,r}$. Hence $v_n^{\lambda,r} \geq 0$ for all n if and only if the orbit of (M, s) does not reach T, i.e. there does not exist n such that $M^n s \in T$. □

Proof of Theorem 8.2.2. Similar to the above. First assume that its is decidable whether the orbit of a given LDS visits a given target from $\mathcal{H}$ infinitely often. By Theorem 8.1.2, it suffices to show that given $r \in \mathbb{R}$ and $\lambda \in \mathcal{G}$, we can decide whether there exists N such that $u_n^{\lambda,r} \geq 0$ for all $n \geq N$. Assume λ is not a root of unity, as otherwise the problem is trivial. Observe that $u_n^{\lambda,r} \geq 0$ for sufficiently large n if and only if $v_n^{\lambda,r} \geq 0$ for sufficiently large n. That is, we have to decide whether $(v_n^{\lambda,r})_{n\in\mathbb{N}}$ has only finitely many negative terms. Let $M, s, q_{\lambda,r}, T$ be as in the proof of Theorem 8.2.1. Recalling that $v_n^{\lambda,r} = q_{\lambda,r}(M^n s)$ and applying Equation (8.3), $v_n^{\lambda,r} < 0$ holds only for finitely many n if and only if the orbit of (M, s) does not visit T infinitely often. □

These two theorems tell us that we cannot extend our result that the MCP is decidable for arbitrary LDS and low-dimensional targets to neither the class $\mathcal{H}$ of targets of semialgebraic dimension 2, nor to the class $\widehat{\mathcal{H}}$ of targets contained in a four-dimensional subspace. In fact, by Theorem 8.2.2 even the restriction to prefix-independent properties does not help.As promised, we conclude this section by showing that the characteristic word of a four-dimensional system (M, s) with respect to a set of targets $\mathcal{T} \subset \mathcal{H}$ need not be almost-periodic.

Let $\lambda \in \mathcal{G}$ be not a root of unity, e.g. $\lambda = 0.6 + 0.8\boldsymbol{i}$, and consider the LRS

$$u_n = 8 - (n \operatorname{Im}(\lambda^n))^2.$$

We will show that the sign pattern of $(u_n)_{n\in\mathbb{N}}$ is not almost-periodic and at the same time, up to a renaming of letters, the characteristic word of an LDS with respect to $\{T\}$ for $T \in \mathcal{H}$ defined below. Let $s = (0, 0, 0, 1)$ and M_λ, p_λ be as above. By Equation (8.2),

$$u_n = 8 - p_\lambda(M_\lambda^n s)^2.$$

If we define

$$T = \{(x_1, x_2, x_3, x_4) \colon p_\lambda(x_1, x_2, x_3, x_4)^2 < 8\}$$

then $M_\lambda^n s \in T$ if and only if $u_n > 0$.

Theorem 8.2.3. *The characteristic word of (M_λ, s) with respect to $\mathcal{T} = \{T\}$ is not almost-periodic.*

Proof. First let us show that T is visited infinitely often by the orbit of (M_λ, s). Let

$$x = \frac{\operatorname{Log}(\lambda)}{\boldsymbol{i}2\pi}$$

and observe that since λ is not a root of unity, x is irrational and lies in $(-1/2, 1/2]$. For all $n \in \mathbb{N}$ it holds that

$$|\operatorname{Log}(\lambda^n)/\boldsymbol{i}| = [\![2\pi n x]\!]_{2\pi} = 2\pi[\![nx]\!].$$

By Hurwitz's theorem (see Section 8.1), there exist infinitely many positive integers n such that

$$[\![nx]\!] < \frac{1}{\sqrt{5}n}.$$

We conclude that

$$|\mathrm{Log}(\lambda^n)/\boldsymbol{i}| < \frac{2\pi}{\sqrt{5}n} \tag{8.4}$$

holds for infinitely many integers $0 < n_1 < n_2 < \cdots$. Recall that for $z \in \mathbb{T}$, $|\operatorname{Log}(z)/\boldsymbol{i}| \in [0, \pi]$ is the length of the (smallest) arc of the unit circle extended by the complex numbers 1 and z. Observe that for $z \in \mathbb{T}$ with $\mathrm{Log}(z)/\boldsymbol{i} \in [-\pi/2, \pi/2]$,

$$|\operatorname{Log}(z)/\boldsymbol{i}| \geq |\operatorname{Im}(z)|.$$

Moreover, for all $n_i \geq 2$ it holds that $\frac{2\pi}{\sqrt{5}n_i} \leq \pi/2$. Applying Equation (8.4), for al $n_i \geq 2$,

$$|\operatorname{Im}(\lambda^{n_i})| < \frac{2\pi}{\sqrt{5}n_i}$$

which is equivalent to $(\operatorname{Im}(\lambda^{n_i}))^2 < \frac{4\pi^2}{5n^2}$. We conclude that

$$(n \operatorname{Im}(\lambda^n))^2 < \frac{4\pi^2}{5} < 8$$

and hence $u_n > 0$ for infinitely many values of n.

We next show that for every k, there exists m such that for all $m < n \leq m + k$, $M_\lambda^n s \notin T$. That is, the gaps between consecutive visits of $(M^n s)_{n\in\mathbb{N}}$ to T can be arbitrarily large. Equivalently, the characteristic word α of (M_λ, s) with respect to $\mathcal{T} = \{T\}$ contains arbitrarily large blocks of the letter $\emptyset$. From the fact that the letter $\{T\}$ occurs infinitely often in α it will then follow that α is not almost-periodic.

For $z \in \mathbb{T}$ and $\varepsilon > 0$ we write $\mathcal{B}(z, \varepsilon) = \{y \in \mathbb{T} \colon |z - y| < \varepsilon\}$. For $n \in \mathbb{N}$, let

$$T_n = \{z \in \mathbb{C} \colon |\operatorname{Im}(z)| < 8/n\}.$$

Observe that $M_\lambda^n \in T$ if and only if $\lambda^n \in T_n$. Moreover, the sequence $(T_n)_{n\in\mathbb{N}}$ of sets shrinks uniformly to the finite set $\{-1, 1\}$. Intuitively, due to the shrinkage it takes longer and longer for $(\lambda^n)_{n\in\mathbb{N}}$ to fall into T_n as $n \to \infty$. Given k, we construct m described above as follows. Since λ is not a root of unity, $\lambda^n \neq 1, -1$ for all $n > 1$. Let $\varepsilon > 0$ be such that

$$\lambda, \ldots, \lambda^k \notin \mathcal{B}(1, 2\varepsilon) \cup \mathcal{B}(-1, 2\varepsilon).$$

Then for all $z \in \mathcal{B}(1, \varepsilon) \cap \mathbb{T}$,

$$\lambda z, \ldots, \lambda^k z \notin \mathcal{B}(1, \varepsilon) \cup \mathcal{B}(-1, \varepsilon).$$

Let N be such that for all $n \geq N$, $T_n \subseteq \mathcal{B}(1,\varepsilon) \cup \mathcal{B}(-1,\varepsilon)$, and $m \geq N$ be such that $\lambda^m \in \mathcal{B}(1,\varepsilon)$. Such m exists by the density of $(\lambda^n)_{n\in\mathbb{N}}$ in $\mathbb{T}$ (Theorem 4.1.4). By construction, $\lambda^{m+1}, \ldots, \lambda^{m+k} \notin \mathcal{B}(1,\varepsilon) \cup \mathcal{B}(-1,\varepsilon)$, which encloses T_n for all $n \geq m$. Hence for all $m < n \leq m+k$, $\lambda^n \notin T_n$ and $M_\lambda^n s \notin T$. □

8.3 Hardness results for diagonalisable systems

We now look at possible extensions of our result that the Model-Checking Problem is decidable for diagonalisable (M, s) and prefix-independent properties. First of all, recall from Theorem 8.2.2 that it is Diophantine-hard to decide whether the orbit of a given LDS $(M, s) \in \mathbb{Q}^{4\times4} \times \mathbb{Q}^4$ visits a given semialgebraic set T infinitely often. Noting that "$T \in \alpha(n)$ for infinitely many n" is a prefix-independent property of the characteristic word α, we conclude that the Model-Checking Problem with prefix-independent properties (without the diagonalisability assumption) is Diophantine-hard already in ambient dimension 4.

Now let us look at what happens if we only remove the restriction to prefix-independent properties. That is, we consider the full Model-Checking Problem for diagonalisable LDS (M, s), without any restrictions on the target sets $\mathcal{T}$ or the automaton $\mathcal{A}$. By the correspondence between halfspace (resp. hyperplane) reachability and the Positivity (resp. Skolem) Problem given in Section 2.1, the MCP for diagonalisable systems immediately subsumes the Skolem and Positivity problems for diagonalisable sequences, both open at the moment. We will next show that already in dimension 4, the Reachability Problem with affine subspace targets is at least as hard as the Skolem Problem at order 5.

Theorem 8.3.1. *The Skolem Problem for rational linear recurrence sequences of order 5 reduces to the following problem. Given diagonalisable $M \in \mathbb{Q}^{4\times4}$ and $c \in \mathbb{Q}^4$, decide if the orbit of (M, s) reaches the affine plane $T = \{x \mid c^\top x = 1\}$.*

Proof. Recall from Section 2.3 that at order 5 the Skolem Problem for LRS over $\mathbb{Q}$ is open only for sequences of the form

$$u_n = b^\top P^n t = \alpha\lambda^n + \overline{\alpha}\,\overline{\lambda^n} + \beta\gamma^n + \overline{\beta}\,\overline{\gamma^n} + \delta\rho^n$$

where $b, t \in \mathbb{Q}^5$, $P \in \mathbb{Q}^{5\times5}$, λ and γ are non-real and distinct, δ and ρ are positive, and

$$|\lambda| = |\gamma| > |\rho|.$$

Moreover, $\lambda, \overline{\lambda}, \gamma, \overline{\gamma}, \rho$ are exactly the roots of the characteristic polynomial $p \in \mathbb{Q}[x]$ of P. Let $\mathbb{K} = \mathbb{Q}(\lambda, \overline{\lambda}, \gamma, \overline{\gamma}, \rho)$ and $D = [\mathbb{K} : \mathbb{Q}]$. Note that $\mathbb{K}/\mathbb{Q}$ is a Galois extension, and $\alpha, \beta, \delta \in \mathbb{K}$.

We will next argue that ρ must be rational, i.e. the polynomial p is reducible with a linear factor. Let $\sigma_1, \ldots, \sigma_D$ denote all distinct automorphisms of the number field $\mathbb{K}$. Recall that as $\mathbb{K}$ is the splitting field of p, each σ_i acts bijectively on the roots of p. Observe that $\lambda\overline{\lambda} = \gamma\overline{\gamma}$ and hence

$$\sigma_i(\lambda)\sigma_i(\overline{\lambda}) = \sigma_i(\gamma)\sigma_i(\overline{\gamma})$$

for all $1 \leq i \leq D$. Since σ_i permutes the roots and $|\rho| < |\lambda|, |\gamma|$, the equation above can only hold if σ_i permutes $\{\lambda, \overline{\lambda}, \gamma, \overline{\gamma}\}$. We conclude that every automorphism σ_i of $\mathbb{K}$ fixes ρ, which implies that ρ is rational.

We consider δ next. Since $u_n \in \mathbb{Q}$ for all n, $\sigma_i(u_n) = u_n$ for all i and n. By the uniqueness of the exponential polynomial representation (Section 2.2),

$$\sigma_i(u_n) = \sigma_i(\alpha)(\sigma_i(\lambda))^n + \ldots + \sigma_i(\delta)(\sigma_i(\rho))^n$$

must be syntactically the same exponential polynomial as $\alpha\lambda^n + \overline{\alpha}\,\overline{\lambda^n} + \beta\gamma^n + \overline{\beta}\,\overline{\gamma^n} + \delta\rho^n$. Since $\rho \in \mathbb{Q}$, $\sigma_i(\rho) = \rho$ hence $\sigma_i(\delta) = \delta$ for all $1 \leq i \leq D$. It follows that $\delta \in \mathbb{Q}$.

Let $v_n = \alpha\lambda^n + \overline{\alpha}\,\overline{\lambda^n} + \beta\gamma^n + \overline{\beta}\,\overline{\gamma^n}$, and $h(x) = a_0 + a_1x + \ldots + a_4x^4 \in \mathbb{Q}[x]$, $a_4 \neq 0$ be a factor of p whose roots are exactly $Z \coloneqq \{\lambda, \overline{\lambda}, \gamma, \overline{\gamma}\}$. For each $z \in Z$ and $n \in \mathbb{N}$,

$$z^{n+4} = \sum_{i=0}^{3} \frac{a_i}{a_4} z^{n+i}.$$

Therefore,

$$v_n = \sum_{i=0}^{3} \frac{a_i}{a_4} v_{n+i}$$

That is, $(v_n)_{n\in\mathbb{N}}$ is an LRS over $\mathbb{Q}$ of order 4. Let $a, s \in \mathbb{Q}^4$ and $R \in \mathbb{Q}^{4\times4}$ be such that $v_n = a^\top R^n s$ for all n. We have that $u_n = 0$ if and only if $-a^\top R^n s = \delta\rho^n$, which is equivalent to

$$-(a/\delta)^\top (R/\rho)^n s = 1$$

Taking $M = (R/\rho) \in \mathbb{Q}^{4\times4}$, $c = -a/\delta \in \mathbb{Q}^4$, and $T = \{x \in \mathbb{R}^4 \mid c^\top x = 1\}$, we obtain that $u_n = 0$ if and only if $M^n s \in T$. This completes the reduction. □

We claimed in Section 2.3 that the Skolem Problem for sequences of order 5 has been "solved in practice" due to the conditional decidability result [16] of Bilu et al. This is far from the case when it comes to the Model-Checking Problem

for diagonalisable systems. Intuitively, this is because for a four-dimensional liner dynamical system (M, s) and a polynomial p, the LRS $u_n = p(M^n s)$ can have high order (that depends on the degree of p) and many dominant and non-dominant roots. In fact, a significant open subclass of the Positivity Problem for diagonalisable linear recurrence sequences of order 10 (see Section 2.5) can be reduced to the Reachability Problem for diagonalisable systems of dimension 4. We give an example.

Let $\lambda = 1 + 2\boldsymbol{i}$, $\gamma = 2 + 3\boldsymbol{i}$, and consider the sequence

$$u_n = (\lambda^n \gamma^n + \overline{\lambda^n}\,\overline{\gamma^n} + 2\overline{\lambda^n}\gamma^n + 2\lambda^n\overline{\gamma^n})^2 - 2^n.$$

It has been verified that $u_n \geq 0$ for all $0 \leq n \leq 10^6$, but, to the best of our knowledge, no proof is known that $u_n \geq 0$ for all $n \in \mathbb{N}$.[2] Let $v_n = u_{2n}$ and $w_n = u_{2n+1}$. We will reduce the problem of deciding whether $v_n \geq 0$ for all n to an instance of the Reachability Problem in dimension 4 with a diagonalisable LDS. Whether $w_n \geq 0$ for all n can be reduced to an instance of the Reachability Problem similarly. Note that $u_n \geq 0$ for all n if and only if $v_n, w_n \geq 0$ for all n.

Write $\alpha = \lambda^2/2 = -(3 + 4\boldsymbol{i})/2$ and $\beta = \gamma^2/2 = -(5 + 12\boldsymbol{i})/2$. Both α and β are quadratic irrationals belonging to $\mathbb{Q}(\boldsymbol{i})$. It holds that

$$\frac{v_n}{4^n} = (\alpha^n \beta^n + \overline{\alpha}^n\,\overline{\beta^n} + 2\overline{\alpha^n}\beta^n + 2\alpha^n\overline{\beta^n})^2 - 1.$$

Let $s = (0, 1, 0, 1)$, $R(z) = \begin{bmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{bmatrix}$ for $z \in \mathbb{C}$, and

$$M = \begin{bmatrix} R(\alpha) & \\ & R(\beta) \end{bmatrix} \in \mathbb{Q}^{4\times 4}$$

which has eigenvalues $\alpha, \overline{\alpha}, \beta, \overline{\beta}$. For every $n \in \mathbb{N}$,

$$M^n = \begin{bmatrix} R(\alpha^n) & \\ & R(\beta^n) \end{bmatrix}.$$

Hence there exists $p \in \mathbb{Q}[x_1, \ldots, x_4]$ such that $p(M^n s) = v_n/4^n$ for all n. Writing $T = \{x \in \mathbb{R}^4 \colon p(x) < 0\}$, $v_n \geq 0$ for all n if and only if $(M^n s)_{n\in\mathbb{N}}$ does not reach T.

[2] Personal communication with Joël Ouaknine.

Chapter 9

Abstraction-based verification of linear dynamical systems

In the preceding chapters we mainly focussed on the Model-Checking Problem for linear dynamical systems. Our approach was to translate various instances of the MCP to problems about sign patterns of linear recurrence sequences. To reason about these sign patterns we used bounds from algebraic number theory as well as tools from Diophantine approximation. When going back from sign patterns of LRS to the orbit of (M, s), we applied the theory of toric words, whose origins lie in symbolic dynamics. Finally, Semënov's algorithm for model-checking effectively almost-periodic words was the punchline of our proofs that various classes of the Model-Checking Problem are decidable. The *classical* perspective on dynamical systems, on the other hand, often involves the study of various *topological* properties of dynamical systems as well as their asymptotic behaviour. In this chapter we shift gears and study three problems in computer science that arise from the latter view of (linear) dynamical systems. It turns out that these problems, despite looking fairly different, can all be solved using the same technique: constructing a *continuous abstraction* of the orbit of (M, s).

Pseudo-Reachability Problem (PRP). A fundamental notion in the theory of dynamical systems is that of *pseudo-orbits*. A sequence $(x_n)_{n\in\mathbb{N}}$ over $\mathbb{R}^d$ is an ε-pseudo-orbit of (M, s) if $x_0 = s$ and $\|x_{n+1} - Mx_n\|_2 < \varepsilon$ for all $n \in \mathbb{N}$. The study of pseudo-orbits dates back to the works Anosov [10], Bowen [20] and Conley [29]. We will consider the *Pseudo-Reachability Problem*:[1] given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$, and a semialgebraic target T, decide if for every $\varepsilon > 0$ there exist an ε-pseudo-orbit $(x_n)_{n\in\mathbb{N}}$ of (M, s) that reaches T, i.e. $x_n \in T$ for some $n \in \mathbb{N}$. We write PRP for the set of all $\langle M, s, T\rangle$ that are positive instances of this problem. In Section 9.7 we will

[1] Note that here we allow M,s to have real algebraic entries, which is different from the preceding chapters. This is to make intermediate steps involving real Jordan form more convenient.

use the aforementioned continuous abstraction technique to show that the PRP is decidable for diagonalisable M.

We can also view the PRP through the lens of control theory. Let (M, s) be as above, and $U \subset \mathbb{R}^d$ be a set of accessible *control inputs*. Consider the dynamics $x_0 = s$ and $x_{n+1} = Mx_n + u_n$ for $n \in \mathbb{N}$, where $u_n \in U$ for all n. The Reachability Problem for Linear Time-Invariant Systems [37] is to decide, given M, s, U as above and a target set T, whether there exists a sequence $(u_n)_{n\in\mathbb{N}}$ of control inputs from U such that the sequence $(x_n)_{n\in\mathbb{N}}$ reaches T. We can therefore interpret $\langle M, s, T\rangle \in \mathsf{PRP}$ as "For any set U of control inputs containing a ball of positive radius around the origin, $\langle M, s, U, T\rangle$ is a positive instance of the Reachability Problem for LTI systems".

Previously, we have studied decidability of the PRP in two papers. In the earlier work [31] we showed that the PRP is decidable for all LDS assuming the target T is either a hyperplane, a halfspace, or a bounded semialgebraic set. We will comment on these results in Section 9.7, but do not focus on them in this thesis as they are based on a specialised (but relatively straightforward) technique. Instead, we will show decidability of the PRP for diagonalisable linear dynamical systems and arbitrary semialgebraic targets using the continuous abstraction technique we developed in the later work [32].

Topological Reachability Problem (TRP). This is the problem of deciding, given (M, s) and T as above, whether in every neighbourhood of s there exists a point $\hat{s}$ such that the orbit of $(M, \hat{s})$ reaches T. Observe that in comparison to the PRP, here we are allowed a single control input that is applied *before* the first multiplication by M. We write TRP for the set of all positive instances $\langle M, s, T\rangle$ of the Topological Reachability Problem. Unless $s \in \partial T \setminus T$, that is, s lies at the boundary of T but is not in T, if $\langle M, s, T\rangle \in \mathsf{TRP}$ then $\langle M, s, T\rangle \in \mathsf{PRP}$. To see why the qualification $s \notin \partial T \setminus T$ is necessary, suppose T is open, s lies at the boundary of T, and $\langle M, s, T\rangle \notin \mathsf{PRP}$. In this case, due to the way we defined topological reachability, $\langle M, s, T\rangle \in \mathsf{TRP}$. On the other hand, suppose $s \notin \partial T \setminus T$ and $\langle M, s, T\rangle \in \mathsf{TRP}$. If $s \in T$, then $\langle M, s, T\rangle \in \mathsf{PRP}$. Suppose $s \notin T$. Then for every open O containing s, there exist $\hat{s}$ and $n \geq 1$ such that $M^n\hat{s} \in T$. It follows that for every $\varepsilon > 0$, there exists an ε-pseudo-orbit of (M, s) of the form $x_1 = Ms + u_0$ and $x_{n+1} = Mx_n$ for $n \geq 1$ that reaches T. Finally, we mention that $\langle M, s, T\rangle \in \mathsf{PRP}$ in general does not imply $\langle M, s, T\rangle \in \mathsf{TRP}$. This is illustrated by M that is a 2×2 rotation matrix, any starting point s and closed semialgebraic T that does not intersect $\{x \in \mathbb{R}^2 \colon |x| = |s|\}$.

The (equivalent) dual problem of the TRP, sometimes referred to as the Robust Avoidance Problem, is to decide, given (M, s) and T as above, whether there exists

an open neighbourhood O containing s such that the sequence $(M^n O)_{n\in\mathbb{N}}$ avoids T. Robust avoidance is a relatively strong form of non-reachability that rules out instances where the orbit of (M, s), in some sense, comes arbitrarily close to the target T without ever reaching it.

Decidability of the TRP for hyperplane and halfspace targets was first shown by Akshay et al. in [3]. We illustrate their idea for hyperplane targets; halfspace targets are handled in the same way. Given a hyperplane $T = \{x \colon c^\top x = 0\}$ and (M, s), the linear recurrence sequence $u_n = c^\top M^n s$ has the property that for all n, $M^n s \in T$ if and only if $u_n = 0$. Suppose $(u_n)_{n\in\mathbb{N}}$ has order k and satisfies a recurrence relation $a = (a_0, \ldots, a_{k-1}) \in \mathbb{R}^k$. That is, $u_{n+k} = a_0 u_n + \ldots + a_{d-1} u_{n+k-1}$ for all $n \in \mathbb{N}$. If we change s to a close point $\hat{s}$, we obtain a new sequence $v_n = c^\top M^n \hat{s}$ that has order at most k and also satisfies the recurrence relation a. That is, moving from s to t corresponds to slightly modifying the starting values of $(u_n)_{n\in\mathbb{N}}$. Therefore, for hyperplane targets, the TRP is equivalent to the following problem about LRS: Given $(u_n)_{n\in\mathbb{N}}$ satisfying a recurrence relation $a \in \mathbb{R}^k$, decide whether for every $\varepsilon > 0$ it is possible to perturb the initial values $u_0, \ldots, u_{k-1}$ by at most ε to obtain a sequence $(v_n)_{n\in\mathbb{N}}$ such that $v_n = 0$ for some n. The latter problem, in turn, can be solved using the classical theory of linear recurrence sequences. The approach of [3] is specific to targets defined by a single linear (in)equality. In Section 9.6 we will use a different, geometric approach to prove decidability of the TRP in full generality.

Semialgebraic Invariant Problem (SIP). Somewhat surprisingly, we will show that the two reachability problems given above are related to *inductive invariants* of linear dynamical systems. An inductive invariant of (M, s) is a set S such that $MS \subseteq S$ and $s \in S$. Two trivial inductive invariants of S are the whole ambient space $\mathbb{R}^d$ and the orbit of (M, s) itself. Given a semialgebraic target T, if we can synthesise a semialgebraic inductive invariant S of (M, s) that is disjoint from T then we have a *certificate* that the orbit of (M, s) does not reach T. This makes inductive invariants a crucial tool for proving non-reachability, especially in the light of the following result of [6].

Theorem 9.0.1. *Given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$ and semialgebraic $T \subseteq \mathbb{R}^d$, it is decidable whether there exists a semialgebraic inductive invariant of (M, s) that is disjoint from T. In case such an invariant exists, it can be computed effectively.*

We refer to the decision problem of determining whether a semialgebraic invariant disjoint from T exists as the *Semialgebraic Invariant Problem* (SIP) and write SIP for the set of all positive instances $\langle M, s, T\rangle$ thereof. To prove Theorem 9.0.1, the

authors first show that $\langle M, s, T\rangle \in \mathsf{SIP}$ if and only there exists an inductive invariant S that is disjoint from T and can be defined using arithmetic operations as well as *real exponentiation*. Note that this class invariants is strictly larger than the class of semialgebraic invariants. Existence of a desired invariant in the larger class was already shown to be decidable in [5] using *o-minimality* of the structure of real numbers equipped with arithmetic operations and exponentiation, which we will discuss shortly.

We mention that non-reachability cannot always be proven using invariants. As an example, let M be a 2×2 rotation matrix, $s = (1, 0)$, T be a semialgebraic subset of the unit circle containing finitely many points, and suppose the orbit of (M, s) is dense in the unit circle but avoids T. Any inductive invariant of (M, s) that has finitely many connected components must contain the whole unit circle. Hence no such invariant can be disjoint from T. Nevertheless, we will show in Section 9.8 that $\overline{\mathsf{TRP}} \subset \mathsf{SIP}$. That is, if the orbit of M, s is sufficiently well-separated from T (i.e. there exists a neighbourhood O of s such that $(M^n O)_{n\in\mathbb{N}}$ avoids T), then we can always prove non-reachability by synthesising a semialgebraic invariant.

Recall that exact verification problems of linear dynamical systems like the Skolem Problem,[2] the Positivity Problem, and the Model-Checking Problem are known to be decidable in low dimension and are open or provably "mathematically intractable" in higher dimensions. The results of this chapter, in comparison, are applicable in all dimensions. However, in Section 9.9 we will show that the if we try to generalise our decidability results for the TRP and the PRP from reachability properties to arbitrary ω-regular properties, the resulting problems are at least as hard as the Positivity Problem for linear recurrence sequences. We mention that, another comparison to the problems of LDS considered in preceding chapters is that in this chapter we use "soft" tools like o-minimality as opposed "hard" tools like Baker's theorem.

We next introduce o-minimality and model-theoretic properties of real numbers with exponentiation. These are of vital importance to us as the continuous abstraction, which is our common tool for attacking the TRP, the PRP and the SIP, is defined using not only polynomials but also the exponential function.

9.1 Model theory of real exponentiation

Recall that $\mathcal{L}_{or}$ denotes the language of ordered rings, and formulas $\varphi \in \mathcal{L}_{or}$ with d free variables define precisely the semialgebraic subsets of $\mathbb{R}^d$. We write $\mathcal{L}_e$ for the

[2] See Section 2.1 for the formulation of the Skolem and Positivity problems in terms of linear dynamical systems.

first-order language given by the set of function symbols $F_e \coloneqq \{+, -, \cdot, \exp\}$, the set of relation symbols $R_e \coloneqq \{>, \geq, =, \neq, \leq, <\}$, and the set of constant symbols $C_e \coloneqq \mathbb{Q}$. We denote by $\mathbb{R}_{\exp}$ the structure of real numbers equipped with the usual arithmetic operations and the exponentiation function $x \mapsto e^x$. We will be interpreting formulas of $\mathcal{L}_e$ in $\mathbb{R}_{\exp}$. Observe that in the structure $\mathbb{R}_{\exp}$, for every positive $r \in (\mathbb{R} \cap \overline{\mathbb{Q}})$ we can define the function $y = r^x = e^{x \log r}$ by the $\mathcal{L}_e$-formula

$$\varphi(x, y) \coloneqq \exists z \colon \exp(z) = r \wedge y = \exp(x \cdot z).$$

The structure $\mathbb{R}_{\exp}$ has been studied intensively over decades. Already in 1948, having proved decidability of $\mathrm{Th}(\mathbb{R}_0)$, Tarski asked: is $\mathrm{Th}(\mathbb{R}_{\exp})$ decidable? Here $\mathrm{Th}(\mathbb{R}_{\exp})$ denotes the set of all $\mathcal{L}_e$-sentences that are true in $\mathbb{R}_{\exp}$. In 1996, Macintyre and Wilkie [55] gave a positive answer to Tarski's question subject to Schanuel's famous conjecture in transcendental number theory.

Schanuel's conjecture. For $\lambda_1, \ldots, \lambda_m \in \mathbb{C}$ that are linearly independent over $\mathbb{Q}$, the transcendence degree of the field extension $\mathbb{Q}(\lambda_1, \ldots, \lambda_m, e^{\lambda_1}, \ldots, e^{\lambda_m})/\mathbb{Q}$ is at least m.

Schanuel's conjecture has wide implications in transcendence theory, but is currently believed to be out of reach. We refer the reader to [79] for a detailed introduction. The aforementioned proof of Macintyre and Wilkie requires Schanuel's conjecture only for $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$. For $\lambda_1, \ldots, \lambda_m \in \overline{\mathbb{Q}}$, Schanuel's conjecture has been proven as the Lindemann-Weierstrass theorem.

We say that $S \subseteq \mathbb{R}^d$ is *definable in* $\mathbb{R}_{\exp}$ *with parameters from* $X \subseteq \mathbb{R}$ if there exist $k \geq 0$, a formula $\varphi \in \mathcal{L}_e$ with $k + d$ free variables, and $c_1, \ldots, c_k \in X$ such that for all $\mathbf{x} \in \mathbb{R}^d$,

$$\mathbf{x} \in S \Leftrightarrow \varphi(c_1, \ldots, c_k, \mathbf{x}).$$

We say that S is *definable in* $\mathbb{R}_{\exp}$ if it is definable in $\mathbb{R}_{\exp}$ with parameters from $\mathbb{R}$, and $\mathcal{L}_e$*-definable* if it is definable in $\mathbb{R}_{\exp}$ with parameters from $X = \emptyset$. Semialgebraic sets, for example, are $\mathcal{L}_e$-definable. Wilkie has shown [80] that the structure $\mathbb{R}_{\exp}$ is

(a) *o-minimal*, meaning that every set S definable in $\mathbb{R}_{\exp}$ has finitely many connected components in the Euclidean topology, and

(b) *model-complete*, meaning that every $\mathcal{L}_e$-formula is equivalent to an existential formula modulo $\mathrm{Th}(\mathbb{R}_{\exp})$.

Both results are independent of Schanuel's conjecture. **That $\mathbb{R}_{\exp}$ is o-minimal is the cornerstone of our decidability results in this chapter.**

The $\mathcal{L}_e$-definable sets, just like the more special class of semialgebraic sets, admit *cell decomposition* [33, Chapter 3]. In this chapter by a cell we mean an $\mathcal{L}_e$-definable set that is homeomorphic to $(0,1)^m$ for some m. Let S be $\mathcal{L}_e$-definable, and $A_1, \ldots, A_l$ be a collection of disjoint cells such that $S = \bigcup_{1 \leq i \leq l} A_i$. Suppose each A_i is homeomorphic to $(0,1)^{m_i}$. We define the dimension of S, written $\dim(S)$, to be $\max_{1 \leq i \leq l} m_i$. The dimension of S is independent of its decomposition into cells.

We conclude this section by applying o-minimality to give a convergence theorem for families of $\mathcal{L}_e$-definable sets. In the following, $\mathcal{B}(x, \varepsilon)$ denotes the open ℓ_2-ball of radius ε around $x \in \mathbb{R}^d$.

Lemma 9.1.1. *Let $(S_t)_{t \geq 0}$ be a family of sets contained in a compact set $C \subset \mathbb{R}^d$ given by a formula $\varphi(y, x_1, \ldots, x_d) \in \mathcal{L}_e$ such that for all $\mathbf{x} \in \mathbb{R}^d$ and $t \geq 0$, $\mathbf{x} \in S_t$ if and only if $\varphi(t, \mathbf{x})$ holds. If $S_t \neq \emptyset$ for all sufficiently large t, then there exists non-empty and closed $L \subseteq C$, called the limit shape of $(S_t)_{t \geq 0}$, with the following properties.*

(a) For every $\varepsilon > 0$, there exists N such that for all $t \geq N$, $S_t \subseteq L + \mathcal{B}(\mathbf{0}, \varepsilon)$.

(b) For all $x \in L$ and $\varepsilon > 0$, $\mathcal{B}(x, \varepsilon)$ intersects S_t for all sufficiently large t.

Proof. The limit shape is

$$L \coloneqq \{x \in C \colon \liminf_{t \to \infty} d(x, S_t) = 0\}$$

where $d(x, S_t)$ denotes the shortest Euclidean distance from x to a point in S_t. By an elementary argument, L is closed. As the sequence $(S_n)_{n \in \mathbb{N}}$ is eventually non-empty and C is compact, by the Bolzano-Weierstrass theorem L is non-empty.

We prove (a) by contradiction. Suppose there exist $\varepsilon > 0$, an increasing and unbounded sequence $(t_n)_{n \in \mathbb{N}}$ of time steps over $\mathbb{R}_{\geq 0}$, and a sequence $(x_n)_{n \in \mathbb{N}}$ over C such that $x_n \in S_{t_n}$ but $x_n \notin L + \mathcal{B}(\mathbf{0}, \varepsilon)$ for all n. Let x be an accumulation point of $(x_n)_{n \in \mathbb{N}}$. Since $x_n \notin L + \mathcal{B}(\mathbf{0}, \varepsilon)$ for all n, $x \notin L$. However, since $x_n \in S_{t_n}$ for all n,

$$\liminf_{t \to \infty} d(x, S_t) = 0.$$

This implies that $x \in L$, a contradiction. To prove (b), fix $x \in L$ as well as $\varepsilon > 0$, and consider

$$Z \coloneqq \{t \geq 0 \colon x + B(\mathbf{0}, \varepsilon) \text{ intersects } S_t\}.$$

Since Z is definable in $\mathbb{R}_{\exp}$ with parameters from $\mathbb{R}$, by o-minimality, it consists of finitely many intervals. Since $x \in L$, the set Z is unbounded. Hence it must contain an interval of the form $[N, \infty)$, i.e. $x + \mathcal{B}(\mathbf{0}, \varepsilon)$ intersects S_t for all sufficiently large t. $\square$

9.2 The main idea through an example

Our objective in this section is to give an intuitive explanation of the idea behind the continuous abstraction that we will use to solve the TRP, the PRP, and the SIP. Consider $M = \begin{bmatrix} \Lambda & \\ & \rho_2 \end{bmatrix} \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{3\times 3}$ where $\Lambda = \rho_1 \Gamma$,

$$\Gamma = \begin{bmatrix} \mathrm{Re}(\gamma) & -\mathrm{Im}(\gamma) \\ \mathrm{Im}(\gamma) & \mathrm{Re}(\gamma) \end{bmatrix},$$

$\rho_1, \rho_2 \in \mathbb{R} \cap \overline{\mathbb{Q}}$ with $\rho_1, \rho_2 > 1$, and $\gamma \in \mathbb{T} \cap \overline{\mathbb{Q}}$. Let $s = (1, 0, 1)$ be the starting point and $T \subseteq \mathbb{R}^3$ be a semialgebraic target. We will show how to solve our three problems for such $\langle M, s, T\rangle$, illustrating the main ideas of our decidability proofs. It will be convenient to first reformulate the TRP and the PRP in terms of linear dynamical systems equipped with control inputs.

Lemma 9.2.1. *Let B be a bounded open set containing $\mathbf{0}$.*

(a) The TRP is equivalent to the following problem. Given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, a starting point $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$ and semialgebraic T, decide if for every $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $M^n s + \varepsilon M^n B$ intersects T.

(b) The PRP is equivalent to the following problem. Given (M, s) and T as above, decide if for every $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that

$$M^n s + \varepsilon \sum_{i=0}^{n-1} M^i B$$

intersects T.

Proof. We first prove (a). Observe that $M^n s + \varepsilon M^n B = M^n(\{s\} + \varepsilon B)$. Suppose $\langle M, s, T\rangle \in \mathsf{TRP}$. Then there exist $n \in \mathbb{N}$ and $\hat{s}$ in the neighbourhood $O \coloneqq \{s\} + \varepsilon B$ of s such that $M^n \hat{s} \in T$, which implies that $M^n s + \varepsilon M^n B$ intersects T. Conversely, suppose $\langle M, s, T\rangle \notin \mathsf{TRP}$, i.e. there exists an open set O containing s such that $M^n O$ does not intersect T for all n. Let $\varepsilon > 0$ be such that $s + \varepsilon B \subseteq O$. It holds that $M^n(\{s\} + \varepsilon B) \subseteq M^n O$ does not intersect T for all n.

To prove (b), denote by $\mathcal{B}$ the unit ℓ_2-ball and let k_1, k_2 be such that $k_1\mathcal{B} \subseteq B \subseteq k_2\mathcal{B}$. For all $\varepsilon > 0$ and $n \in \mathbb{N}$ it holds that

$$M^n s + k_1\varepsilon \sum_{i=0}^{n-1} M^n \mathcal{B} \subseteq M^n s + \varepsilon \sum_{i=0}^{n-1} M^n B \subseteq M^n s + k_2\varepsilon \sum_{i=0}^{n-1} M^n \mathcal{B}.$$

It remains to observe that the set of points that are reachable at exactly time n by an ε-pseudo-orbit is $M^n s + \varepsilon \sum_{i=0}^{n-1} M^i \mathcal{B}$. □

Next, we construct a continuous abstraction of the orbit of (M, s). Factorise $M = CD$ where $C = \mathrm{diag}(\rho_1, \rho_1, \rho_2)$, $D = \mathrm{diag}(\Gamma, 1)$, C has only real eigenvalues, and all eigenvalues of D lie on the unit circle. We have thus decomposed the linear map given by M into a scaling and a rotation. Observe that for all $n \in \mathbb{N}$,

$$M^n = C^n D^n.$$

Applying Kronecker's theorem (see Section 4.1) and identifying $\mathbb{R}^{3\times3}$ with $\mathbb{R}^9$, we can compute compact semialgebraic $\mathcal{D} \subset \mathbb{R}^{3\times3}$ such that

(a) $(D^n)_{n\in\mathbb{N}}$ is dense in $\mathcal{D}$, and

(b) for each $Z \in \mathcal{D}$ and $\varepsilon > 0$, there exist infinitely many values $n \in \mathbb{N}$ such that $\|D^n - Z\|_2 < \varepsilon$.

In our case if γ is not a root of unity, then $\mathcal{D} = \{(x, y, 1) \mid x^2 + y^2 = 1\}$. Otherwise, $\mathcal{D}$ is finite.

By an *abstraction* of $(M^n s)_{n\in\mathbb{N}}$ we mean a function $\mathcal{A}$ that, give $t \geq 0$, computes a subset of $\mathbb{R}^3$ with the property that for all $n \in \mathbb{N}$, $M^n s \in \mathcal{A}(n)$. The abstraction we will need is

$$\mathcal{A}(t) = C^t \mathcal{D} s$$

where $C^t = \mathrm{diag}(\rho_1^t, \rho_1^t, \rho_2^t)$ for all $t \geq 0$. We refer to

$$R(Z) \coloneqq \{C^t Z s \mid t \geq 0\}$$

as the *trajectory ray* of Z. Figure 9.1 illustrates the situation.

Topological Reachability Problem. Recall that by Lemma 9.2.1 we have to decide whether

$$\forall \varepsilon > 0.\, \exists n\colon (M^n s + \varepsilon M^n B) \cap T \neq \emptyset$$

where we are free to choose any open, bounded B containing a neighbourhood around $\mathbf{0}$. The best choice for our purposes is

$$B \coloneqq \mathcal{B}((0, 0), 1) \times (-1, 1).$$

With this definition, $M^n s + \varepsilon M^n B = M^n s + \varepsilon C^n B$. Because C only has real eigenvalues, the set $C^n B$ is significantly simpler than $M^n B$. We still, however, need one more trick. Recall that $M^n s \in \mathcal{A}(n)$ for all $n \in \mathbb{N}$. We will study, for each $\varepsilon > 0$, the set

$$V(\varepsilon) \coloneqq \{t \geq 0 \mid \mathcal{A}(t) + \varepsilon C^t B \cap T \neq \emptyset\}.$$

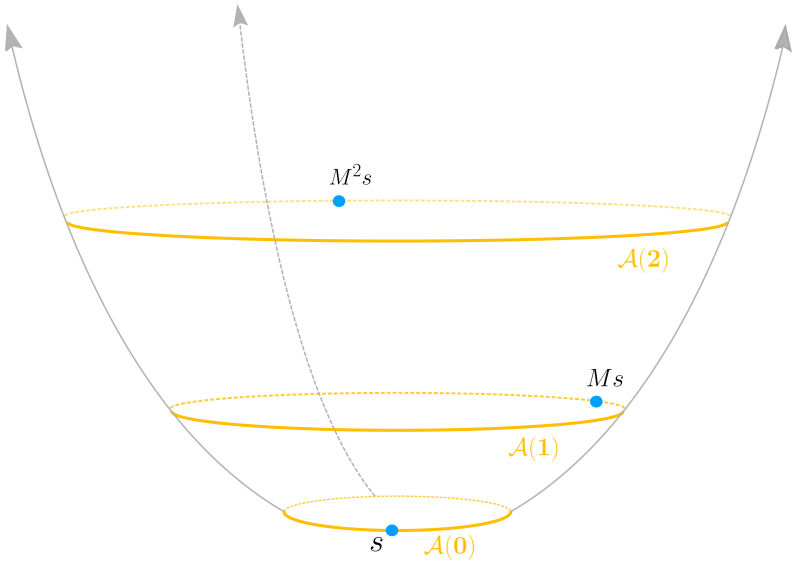

Figure 9.1: The orbit of (M, s), its abstraction, and three trajectory rays.

Note that every $n \in \mathbb{N}$ for which $M^n s + \varepsilon M^n B$ intersects T belongs to $V(\varepsilon)$. Since for each $\varepsilon \geq 0$, $V(\varepsilon)$ is definable in $\mathbb{R}_{\text{exp}}$ with parameters from $\mathbb{R}$, by o-minimality it consists of finitely many intervals. That is, either $V(\varepsilon)$ is bounded, or it contains an interval of the form $[N, \infty)$. Moreover, if $V(\varepsilon)$ is bounded by $N \in \mathbb{N}$ then so is $V(e)$ for $e < \varepsilon$. Hence there are two possibilities.

(A) For every $\varepsilon > 0$, $V(\varepsilon)$ is unbounded. In particular, $\mathcal{A}(n) + \varepsilon C^n B$ intersects T for infinitely many $n \in \mathbb{N}$.

(B) There exists ε and N such that for all $e \leq \varepsilon$, $V(\varepsilon)$ is bounded by N. That is, for all $n > N$ and $e \leq \varepsilon$, $\mathcal{A}(n) + eC^n B$ and hence $M^n s + eC^n B$ do not intersect T.

We will show in Section 9.6 how to decide which case holds. If (A) holds, then we will show that, in fact, $\langle M, s, T \rangle \in \mathsf{TRP}$. Otherwise, we will show how to effectively compute a value N as in (B). It remains to decide whether

$$\forall \varepsilon > 0.\, \exists n \leq N \colon (M^n s + \varepsilon C^n B) \cap T \neq \emptyset$$

which is equivalent to $\exists n \in \{0, \ldots, N\} \colon M^n s \in \mathrm{Cl}(T)$. The latter is verified directly.

Pseudo-Reachability Problem. Recall that the PRP is to decide whether

$$\forall \varepsilon > 0.\, \exists n \colon (M^n s + \varepsilon \sum_{i=0}^{n-1} M^i B) \cap T \neq \emptyset.$$

Again, by Lemma 9.2.1, we are free to choose B, which we take to be exactly as above. Let $r_1(t) = \frac{\rho_1^t - 1}{\rho_1 - 1}$ and $r_2(t) = \frac{\rho_2^t - 1}{\rho_2 - 1}$ for $t \geq 0$, and

$$B(t) \coloneqq \mathcal{B}((0,0), r_1(t)) \times (-r_2(t), r_2(t)).$$

Since $M^i B = C^i B$ for all $i \in \mathbb{N}$,

$$\sum_{i=0}^{n-1} M^i B = \sum_{i=0}^{n} \mathcal{B}((0,0), \rho_1^i) \times (-\rho_2^i, \rho_2^i) = B(n).$$

Proceeding similarly to our analysis of the TRP, we define

$$V(\varepsilon) \coloneqq \{t \geq 0 \mid \mathcal{A}(t) + \varepsilon B(n) \cap T \neq \emptyset\}.$$

The dichotomy (A-B) remains true. We will show in Section 9.7 that in case (A), $\langle M, s, T\rangle \in \mathsf{PRP}$. Otherwise, we will once again reduce the problem to checking a finite prefix $\langle s, \ldots, M^N s\rangle$ of the orbit.

Semialgebraic Invariant Problem. Let us now discuss possible invariants of (M, s), and whether we can find one that is disjoint from a given semialgebraic target T. By a result of [6], (M, s) has a semialgebraic invariant disjoint from T if and only if it has an $\mathcal{L}_e$-definable invariant with the same property. Hence it suffices to restrict our attention to the latter, broader class of invariants.

Since $M\mathcal{A}(t) = \mathcal{A}(t+1)$ and $s \in \mathcal{A}(0)$, the bowl-shaped set $S_0 \coloneqq \cup_{t \geq 0} \mathcal{A}(t)$ is an $\mathcal{L}_e$-definable invariant of (M, s). We can construct stronger (i.e. smaller) $\mathcal{L}_e$-definable invariants of (M, s) by taking $\tau > 0$ and

$$S_\tau \coloneqq \{s, \ldots, M^{\lfloor \tau \rfloor} s\} \cup \bigcup_{t \geq \tau} \mathcal{A}(t).$$

We will show in Section 9.8 that any $\mathcal{L}_e$-definable invariant of (M, s), in fact, must contain S_N for some $N \in \mathbb{N}$. Hence the SIP can be decided as follows. First check if $\mathcal{A}(t)$ is disjoint from T for sufficiently large t. If not, then the required invariant does not exist. Otherwise, compute τ such that $\mathcal{A}(t) \cap T = \emptyset$ for all $t \geq \tau$. It remains to check whether $s, \ldots, M^{\lfloor \tau \rfloor} s \notin T$, in which case S_τ is the desired $\mathcal{L}_e$-definable invariant.

9.3 Constructing the abstraction

In this section, let $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ be in real Jordan form and $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$. We will factorise $M = CD$ into a scaling and a rotation component as we did in our example in the previous section, and then construct an abstraction $\mathcal{A}$ for the orbit of (M, s)

with the property that $M^n s \in \mathcal{A}(n)$ for all $n \in \mathbb{N}$. Write $M = \operatorname{diag}(J_1, \dots, J_l)$, where each J_i is a real Jordan block.

We start by factorising a single block J_i. If J_i is not invertible (i.e. its only eigenvalue is zero), we simple take $J_i = C_i D_i$ with $C_i = J_i$ and $D_i = I$. Next, consider invertible J_i. We write

$$J_i = \begin{bmatrix} \Lambda_i & I & & \\ & \ddots & \ddots & \\ & & \Lambda_i & I \\ & & & \Lambda_i \end{bmatrix} = \begin{bmatrix} \Gamma_i & & & \\ & \ddots & & \\ & & \Gamma_i & \\ & & & \Gamma_i \end{bmatrix} \cdot \rho_i \begin{bmatrix} I & \Lambda_i^{-1} & & \\ & \ddots & \ddots & \\ & & I & \Lambda_i^{-1} \\ & & & I \end{bmatrix} \coloneqq D_i \cdot C_i$$

where $D = \operatorname{diag}(\Gamma_i, \dots, \Gamma_i)$. Here Λ_i, Γ_i, I are all either 2×2 or 1×1 matrices, $\rho_i > 0$ is the spectral radius of Λ_i, and $\Lambda_i = \rho_i \Gamma_i$. If J_i has two non-real eigenvalues, then Γ_i is a rotation matrix. Otherwise, $\Gamma_i = [1]$ and D_i is the identity matrix. Note that the eigenvalues of D_i (which are exactly the eigenvalues of Γ_i) lie on the unit circle, whereas the single eigenvalue of C_i is $\rho_i \in \mathbb{R}$. It remains to define $C = \operatorname{diag}(C_1, \dots, C_l)$ and $D = \operatorname{diag}(D_1, \dots, D_l)$, which yields

$$M^n = C^n D^n = \operatorname{diag}(C_1^n D_1^n, \dots, C_l^n D_l^n)$$

for all $n \in \mathbb{N}$.

We are now in a position to define the continuous abstraction of the orbit of (M, s). Let $r_1, \dots, r_m$ denote the distinct non-zero eigenvalues of C. We write $\mathcal{D}$ for the Euclidean closure of $\{D^n \colon n \in \mathbb{N}\}$, which is analogous to the closure $\mathbb{T}_\Gamma$ of $(\Gamma^n)_{n \in \mathbb{N}}$ for $\Gamma \in (\mathbb{T} \cap \overline{\mathbb{Q}})^d$ that we considered in Section 4.1.

Lemma 9.3.1. *The set $\mathcal{D}$ is semialgebraic and can be effectively computed. Moreover, for each $Z \in \mathcal{D}$ and $\varepsilon > 0$, there exist infinitely many values $n \in \mathbb{N}$ such that $\|D^n - Z\|_2 < \varepsilon$. Finally, $(D^{-n})_{n \in \mathbb{N}}$ is also dense in $\mathcal{D}$.*

Proof. We can diagonalise D to obtain $D = P^{-1} G P$, where

$$G = \operatorname{diag}(\gamma_1, \dots, \gamma_d)$$

is a diagonal matrix whose eigenvalues all lie on $\mathbb{T}$. Applying Theorem 4.1.4, we can compute the semialgebraic closure $\mathbb{T}_G \subseteq \mathbb{T}^d$ of the sequence $(G^n)_{n \in \mathbb{N}}$ with the property that for every $z \in \mathbb{T}_G$ and $\varepsilon > 0$ there exist infinitely many values $n \in \mathbb{N}$ such that $\|G^n - z\|_2 < \varepsilon$. It remains to observe that $\mathcal{D} = P^{-1} \mathbb{T}_G P$.

It remains to prove the last statement. Observe that $D^{-1} = P^{-1} G^{-1} P$ where $G = \operatorname{diag}(\gamma_1^{-1}, \dots, \gamma_d^{-1})$. Since $(\gamma_1, \dots, \gamma_d)$ and $(\gamma_1^{-1}, \dots, \gamma_d^{-1})$ satisfy exactly the same multiplicative relations, the closure of $(G^{-n})_{n \in \mathbb{N}}$ is also equal to $\mathbb{T}_G$. Hence the closure of $(D^{-n})_{n \in \mathbb{N}}$ is $P^{-1} \mathbb{T}_G P = \mathcal{D}$. □

For $n \in \mathbb{N}$, we can now define the abstraction $\mathcal{A}(n) \coloneqq C^n \mathcal{D}s$, which contains $M^n s$ as intended. To apply o-minimality of $\mathbb{R}_{\exp}$, however, we need to make the abstraction depend on its argument continuously. To this end, we first define $C(t)$ for $t \geq 0$ to abstract $(C^n)_{n\in\mathbb{N}}$. Recall that $C = \operatorname{diag}(C_1, \ldots, C_l)$. For invertible $C_i \in \mathbb{R}^{\mu_i\sigma_i \times \mu_i\sigma_i}$, where $\mu_i \in \{1, 2\}$ is such that $\Lambda_i \in \mathbb{R}^{\mu_i \times \mu_i}$ and σ_i is the multiplicity of C_i,

$$C_i^n = \rho_i^n \begin{bmatrix} I & n\Lambda_i^{-1} & \dots & \binom{n}{\sigma_i - 1}\Lambda_i^{1-\sigma_i} \\ & \ddots & \ddots & \vdots \\ & & I & n\Lambda_i^{-1} \\ & & & I \end{bmatrix}$$

where the $\mu_i \times \mu_i$ block at the position (a, b) is $\binom{n}{b-a}\Lambda^{a-b}$ for $b \geq a$. Let

$$p_k(x) = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

for $k \in \mathbb{N}$ and $x \in \mathbb{R}$. We define $C_i(t)$ as the matrix consisting of $\mu_i \times \mu_i$ blocks that, for $1 \leq a, b \leq d$, has at the (a, b)th position $p_{b-a}(t)\Lambda^{a-b}$ if $b \geq a$ and $\mathbf{0}$ otherwise. On the other hand, if J_i is nilpotent, then we set $C_i(t) = C_i^t$ for $t \in \{0, \ldots, d-1\}$ and $C_i(t) = \mathbf{0}$ for all other values of t. It remains to define $C(t) = \operatorname{diag}(C_1(t), \ldots, C_l(t))$ for all $t \geq 0$, with the property that $C(n) = C^n$ for all $n \in \mathbb{N}$. Observe for each $1 \leq a, b \leq$ there exists a formula φ such that for all $t \geq 0$ and $x \in \mathbb{R}$, $(C(t))_{a,b} = x$ if and only if $\varphi(x, t, r_1^t, \ldots, r_m^t)$ holds.

We can now define the continuous abstraction as $\mathcal{A}(t) = C(t)\mathcal{D}s$ for $t \geq 0$. We refer to

$$\mathcal{A}(t, Z) \coloneqq C(t)\mathcal{D}s$$

for $Z \in \mathcal{D}$ as the *specialisation* of $\mathcal{A}(t)$ at the point Z. By construction, for all $n \in \mathbb{N}$,

$$M^n s = \mathcal{A}(n, D^n) \in \mathcal{A}(n).$$

We have the following further properties.

Lemma 9.3.2. *There exists a formula $\varphi \in \mathcal{L}_{or}$ such that for all $t \geq 0$ and $\mathbf{x} \in \mathbb{R}^d$, $\mathbf{x} \in \mathcal{A}(t)$ if and only if $\varphi(\mathbf{x}, t, r_1^t, \ldots, r_m^t)$ holds.*

Proof. As mentioned above, for each $1 \leq a, b \leq d$ there exists $\varphi_{a,b} \in \mathcal{L}_{or}$ such that $x = (C(t))_{a,b} \Leftrightarrow \varphi_{a,b}(x, t, r_1^t, \ldots, r_m^t)$ for all x and $t \geq 0$. Recalling that $\mathcal{D}$ is semialgebraic, we can construct the desired φ from $\{\varphi_{a,b} \mid 1 \leq a, b \leq d\}$ via the definition $\mathcal{A}(t) = C(t)\mathcal{D}s$. □

Lemma 9.3.3. *For all $Z \in \mathcal{D}$ and $t \geq 0$,*

(a) $M\mathcal{A}(t, Z) = \mathcal{A}(t+1, DZ)$, and

(b) $M\mathcal{A}(t) = \mathcal{A}(t+1)$.

Proof. It can be directly verified that $CC(t) = C(t+1)$ for all $t \geq 0$. Hence

$$\mathcal{A}(t+1, DZ) = C(t+1)DZs = CD \cdot C(t)Zs = M \cdot C(t)Zs = M\mathcal{A}(t, Z).$$

To prove (b), first deduce from Lemma 9.3.1 that $D\mathcal{D} = \mathcal{D}$. We have

$$\mathcal{A}(t+1) = C(t+1)\mathcal{D}s = CC(t) \cdot D\mathcal{D}s = CD \cdot C(t)\mathcal{D}s = M\mathcal{A}(t). \qquad \square$$

Lemma 9.3.3 will be used to show that bowl-shaped sets of the form $\bigcup_{t \geq \tau} \mathcal{A}(t)$, where $\tau \geq 0$, are inductive invariants of (M, s).

9.4 Choosing the control set

We saw already through the example given in Section 9.2 by choosing the set B carefully, we can obtain simple closed-form expressions for $M^n B$ and $\sum_{i=0}^{n-1} M^i B$. In this section let $M = \operatorname{diag}(J_1, \ldots, J_l) \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ be in real Jordan form where each J_i is a real Jordan block. Compute the factorisation $M = CD$, $C = \operatorname{diag}(C_1, \ldots, C_l)$ and $D = \operatorname{diag}(D_1, \ldots, D_l)$ as prescribed in Section 9.3. If J_i has two non-real eigenvalues and $J_i \in \mathbb{R}^{2\sigma_i \times 2\sigma_i}$, let

$$B_i \coloneqq \prod_{k=1}^{\sigma_i} \mathcal{B}((0,0), 1) \subset \mathbb{R}^{2\sigma_i}.$$

Otherwise, let σ_i be such that $J_i \in \mathbb{R}^{\sigma_i \times \sigma_i}$ and choose

$$B_i \coloneqq \prod_{k=1}^{\sigma_i} \mathcal{B}(0, 1) = (-1, 1)^{\sigma_i} \subset \mathbb{R}^{\sigma_i}.$$

The suitable generalisation of the construction in Section 9.2 is

$$B \coloneqq \prod_{i=1}^{l} B_i.$$

This choice of the control set affords us the following important property

Lemma 9.4.1. *Let $r_1, \ldots, r_m \in \mathbb{R}$ be the non-zero eigenvalues of C. There exist $\varphi_1, \varphi_2 \in \mathcal{L}_{or}$ with the following properties.*

(a) For all $n \in \mathbb{N}$,

$$\mathbf{x} \in J^n B \quad \Leftrightarrow \quad \varphi_1(\mathbf{x}, n, r_1^n, \ldots, r_m^n).$$

(b) If M is diagonalisable, then for all $n \in \mathbb{N}$,

$$\mathbf{x} \in \sum_{i=0}^{n-1} J^i B \quad \Leftrightarrow \quad \varphi_2(\mathbf{x}, n, r_1^n, \ldots, r_m^n).$$

Proof. Since a 2×2 rotation matrix fixes the ℓ_2-ball $\mathcal{B}((0,0),1) \subset \mathbb{R}^2$ and the identity matrix in $\mathbb{R}^{1\times 1}$ fixes the interval $(-1,1)$, we have that $D_i B_i = B_i$ for all $1 \leq i \leq l$ and hence $D^n B = B$ for all n. Therefore,

$$J^n B = C^n D^n B = C^n B = \prod_{i=1}^{l} C_i^n B_i$$

for all n. To prove (a), recall from the previous section that for each $1 \leq a, b \leq d$ there exists a formula $\varphi_{a,b}$ such that $x = (C^n)_{a,b} \Leftrightarrow \varphi_{a,b}(x, n, r_1^n, \ldots, r_m^n)$ for all $x \in \mathbb{R}$ and $n \in \mathbb{N}$. The required formula φ_1 constructs B as a semialgebraic set, $(C^n)_{a,b}$ for all $1 \leq a, b \leq d$, and defines $J^n B$ as $C^n B$.

We move on to (b). For all n,

$$\sum_{k=0}^{n-1} J^k B = \sum_{k=0}^{n-1} C^k B = \sum_{k=0}^{n-1} \prod_{i=1}^{l} C_i^k B_i = \prod_{i=1}^{l} \sum_{k=0}^{n-1} C_i^k B_i.$$

Since M is assumed to be diagonalisable, $\sigma_i = 1$ for all $1 \leq i \leq l$ and each B_i is either the one-dimensional or the two-dimensional unit ℓ_2-ball. Writing $P_i(n) \coloneqq \sum_{k=0}^{n-1} C_i^k B_i$, it suffices to construct a formula ψ_i for $1 \leq i \leq l$ such that

$$\mathbf{x} \in P_i(n) \quad \Leftrightarrow \quad \psi_i(\mathbf{x}, n, r_1^n, \ldots, r_m^n)$$

for all n. If C_i is nilpotent, then by diagonalisability $C_i = [0]$ and hence $P_i(n) = \{0\}$ for all n. Otherwise, $C_i = \rho I$, where ρ is the positive real eigenvalue of C_i and I is either the 2×2 or 1×1 identity matrix. Therefore, $C_i^k B_i = \rho^k B_i = \mathcal{B}(\mathbf{0}, \rho^k)$ for all $k \geq 0$ and

$$P_i(n) = r(n) B_i = \mathcal{B}(\mathbf{0}, r(n))$$

where $r(n) = n$ if $\rho = 1$ and $r(n) = \frac{\rho^n - 1}{\rho - 1}$ otherwise. It remains to observe that there exists $\psi \in \mathcal{L}_{or}$ such that for all $n \in \mathbb{N}$ and $y \in \mathbb{R}$, $\psi(n, y)$ holds if and only if $y = r(n)$. □

We will also need the following properties of B, which, intuitively, behaves like an ordinary ball.

Lemma 9.4.2. *For every $a, b > 0$, $(a+b)B = aB + bB$.*

Proof. Recall that B is a product of (two or one-dimensional) ℓ_2-balls $B_1, \ldots, B_l$. For any ℓ_2-ball A and $a, b > 0$, $aA + bA = (a+b)A$. Hence

$$aB + bB = \prod_{i=1}^{l}(aB_i + bB_i) = \prod_{i=1}^{l}(a+b)B_i = (a+b)\sum_{i=1}^{l} B_i. \qquad \square$$

Lemma 9.4.3. *For every $\varepsilon_1 \geq \varepsilon_2 > 0$ and $n \in \mathbb{N}$,*

(a) $\varepsilon_1 J^n B \supseteq \varepsilon_2 J^n B$, *and*

(b) $\varepsilon_1 \sum_{k=0}^{n-1} J^k B \supseteq \varepsilon_2 \sum_{k=0}^{n-1} J^k B$.

Proof. The claim (b) follows from (a), which itself is immediate from $\varepsilon_1 B \supseteq \varepsilon_2 B$. $\square$

9.5 A general decidability result

In this section we prove a general decidability result that abstracts our method from Section 9.2 and will be used in the following chapters to prove decidability results for the TRP and the PRP. First, a technical lemma showing that in the setting where we will apply o-minimality, we can do so effectively.

Lemma 9.5.1. *Let $r_1, \ldots, r_m$ be positive and real algebraic, and $\varphi \in \mathcal{L}_{or}$ be a formula with $m + k + 2$ free variables.*

(a) For each $\varepsilon > 0$ and $\mathbf{x} \in \mathbb{R}^k$, the statement $\varphi(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t)$ either holds for all sufficiently large $t \in \mathbb{R}$, or does not hold for all sufficiently large t.

(b) We can compute a formula $\psi \in \mathcal{L}_{or}$ such that for all $\varepsilon > 0$ and $\mathbf{x} \in \mathbb{R}^k$, $\psi(\varepsilon, \mathbf{x})$ holds if and only if $\varphi(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t)$ holds for all sufficiently large t.

(c) If $k = 0$, then given $\varepsilon \in \mathbb{Q}$, we an effectively compute $N \in \mathbb{N}$ such that either (i) $\varphi(\varepsilon, t, r_1^t, \ldots, r_m^t)$ holds for all $t \geq N$, or (ii) it does not hold for all $t \geq N$. Whether case (i) or case (ii) holds can also be determined effectively.

Proof. Sice $\varphi \in \mathcal{L}_{or}$, after flattening (Lemma 1.3.4) it can be written as a Boolean combination

$$\bigwedge_{i \in I} \bigvee_{j \in J} p_{i,j}(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t) \ \Delta_{i,j} \ 0$$

of polynomial inequalities. We can further write each $p_{i,j}$ in the form

$$p_{i,j}(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t) = \sum_{1 \leq l \leq L} q_l(\varepsilon, \mathbf{x}) h_l(t) R^t$$

where $R_1 > \ldots > R_L$ are positive and real algebraic, and q_l and h_l are non-zero polynomials with rational coefficients for all l. If $L = 0$, then the inequality defined by $p_{i,j}$ either holds for all $\varepsilon, \mathbf{x}, t$, or does not hold for all $\varepsilon, \mathbf{x}, t$. Suppose therefore $L > 0$. Since $q_l(\varepsilon, \mathbf{x})h_l(t) = -q_l(\varepsilon, \mathbf{x}) \cdot -h_l(t)$, w.l.o.g. we can also assume that for all l, $h_l(t) > 0$ for sufficiently large t. For $\varepsilon > 0$ and $\mathbf{x} \in \mathbb{R}^k$, denote by $\sigma(\varepsilon, \mathbf{x})$ the largest integer $y \leq L$ such that $q_l(\varepsilon, \mathbf{x})$ is identically zero for all $l < y$. Observe that once we fix ε and $\mathbf{x}$, for sufficiently large values of t the sign of $p_{i,j}(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_k^t)$ is stable and equal to the sign of $q_{\sigma(\varepsilon,\mathbf{x})}(\varepsilon, \mathbf{x})$. Applying this argument to every i, j proves (a).

Having proven (a), to prove (b) it suffices to construct, for every i, j, a formula $\psi_{i,j} \in \mathcal{L}_{or}$ such that for all $\varepsilon > 0$ and $\mathbf{x} \in \mathbb{R}^k$, $\psi_{i,j}(\varepsilon, \mathbf{x})$ holds if and only if $p_{i,j}(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t)\ \Delta_{i,j}\ 0$ holds for all sufficiently large values of t. If $L = 0$, then $\psi_{i,j}(\varepsilon, \mathbf{x})$ is either a formula that is vacuously true or a formula that is vacuously false. Suppose $L > 0$. Construct formulas $\psi_1, \ldots, \psi_L \in \mathcal{L}_{or}$ such that for all $\varepsilon \in \mathbb{R}, \mathbf{x} \in \mathbb{R}^d$ and $1 \leq l \leq L$, $\psi_l(\varepsilon, \mathbf{x})$ holds if and only if $\sigma(\varepsilon, \mathbf{x}) = l$. We can then define $\psi_{i,j}(\varepsilon, \mathbf{x})$ using the formulas $\psi_1, \ldots, \psi_L$ and a finite case analysis.

Finally, suppose $k = 0$. Each $p_{i,j}(\varepsilon, t, r_1^t, \ldots, r_m^t)$ is of the form

$$\sum_{1 \leq l \leq L} q_l(\varepsilon)h_l(t)R^t.$$

Given rational $\varepsilon > 0$, we can apply Lemma 2.4.4 to compute $N_{i,j} \in \mathbb{N}$ such that the sign of this expression is constant over $[N_{i,j}, \infty)$. To prove (c), it remains to apply this argument to each $p_{i,j}$ and take $N = \max_{i,j} N_{i,j}$. □

We are now ready to state and prove the main result of this section.

Lemma 9.5.2. *Let $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$, $J \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d}$ be in real Jordan form with non-zero eigenvalues $\lambda_1, \ldots, \lambda_m$, $r_i = |\lambda_i|$ for $1 \leq i \leq m$, T be a semialgebraic set, and $(P(n))_{n \in \mathbb{N}}$ be a sequence of sets in $\mathbb{R}^d$ given by a formula $\varphi \in \mathcal{L}_{or}$ such that for all $\mathbf{x} \in \mathbb{R}^d$ and $n \in \mathbb{N}$,*

$$\mathbf{x} \in P(n) \quad \Leftrightarrow \quad \varphi(\mathbf{x}, n, r_1^n, \ldots, r_m^n).$$

Let $C, D, \mathcal{D}, \mathcal{A}$ be constructed from (J, s) as described in Section 9.3, and assume the following hold.

(A) For all $n \in \mathbb{N}$ and $\varepsilon_1, \varepsilon_2 > 0$,

$$\varepsilon_1 \geq \varepsilon_2 \quad \Rightarrow \quad \varepsilon_1 P(n) \supseteq \varepsilon_2 P(n).$$

(B) *There exists* $N \in \mathbb{N}$ *with the following property. For every* $\varepsilon_1 > 0$ *there exist* $\delta, \varepsilon_2 > 0$ *such that for all* $n \geq N$ *and* $X, Y \in \mathcal{D}$,

$$\|X - Y\|_2 < \delta \quad \Rightarrow \quad \mathcal{A}(n, X) + \varepsilon_1 P(n) \supseteq \mathcal{A}(n, Y) + \varepsilon_2 P(n).$$

It is decidable whether for all $\varepsilon > 0$ *there exists* $n \in \mathbb{N}$ *such that* $J^n s + \varepsilon P(n)$ *intersects* T.

To understand (B) intuitively, assume for a moment that N is always zero and $\varepsilon_2 = \varepsilon_1/2$. When trying to prove that $J^n s + \varepsilon_1 P(n) = \mathcal{A}(n, D^n) + \varepsilon_1 P(n)$ intersects T, from (B) we know that it is sufficient to prove that $\{\mathcal{A}(n, X) \colon \|X - D^n\|_2 < \delta\} + \varepsilon_2 P(n)$ intersects T. In the latter case, we can work with the sequence $(\mathcal{B}(D^n, \delta) \cap \mathcal{D})_{n \in \mathbb{N}}$ of open subsets of $\mathcal{D}$, which is more amenable to topological arguments than the sequence $(D^n)_{n \in \mathbb{N}}$ of points in $\mathcal{D}$.

Proof. Recall that $r_1, \ldots, r_m$ are exactly the non-zero eigenvalues of C, all eigenvalues of D lie on the unit circle, and $\mathcal{D}$ is the Euclidean closure of $(D^n)_{n \in \mathbb{N}}$ that is semialgebraic. Using quantifier elimination (Theorem 1.3.5), construct A, B and polynomials $p_{a,b}$ with rational coefficients for $a \in A, b \in B$ such that

$$\mathbf{x} \in P(n) \Leftrightarrow \bigwedge_{a \in A} \bigvee_{b \in B} p_{a,b}(\mathbf{x}, n, r_1^n, \ldots, r_m^n) \; \Delta_{a,b} \; 0.$$

for all n. For $t \geq 0$, let $P(t)$ denote the set of all $\mathbf{x} \in \mathbb{R}^d$ satisfying

$$\bigwedge_{a \in A} \bigvee_{b \in B} p_{a,b}(\mathbf{x}, t, r_1^t, \ldots, r_m^t) \; \Delta_{a,b} \; 0.$$

We have thus embedded the sequence $(P(n))_{n \in \mathbb{N}}$ into the family of sets $(P(t))_{t \geq 0}$. For $\varepsilon > 0$ and $t \geq 0$, define

$$Z_t^{(\varepsilon)} := \{Z \in \mathcal{D} \mid (\mathcal{A}(t, Z) + \varepsilon P(t)) \cap T \neq \emptyset\}.$$

Observe that $Z_t^{(\varepsilon)} = \emptyset$ if and only if $\mathcal{A}(t) + \varepsilon P(t)$ does not intersect T. Invoking Lemma 9.3.2, we can construct a formula Φ such that for all $\varepsilon > 0$, $t \geq 0$ and $\mathbf{x}$, $\Phi(\varepsilon, \mathbf{x}, t, r_1^t, \ldots, r_m^t)$ holds if and only if $\mathbf{x} \in Z_t^{(\varepsilon)}$. Hence we can further construct φ such that $\varphi(\varepsilon, t, r_1^t, \ldots, r_m^t)$ holds if and only if $Z_t^{(\varepsilon)} = \emptyset$. Applying Lemma 9.5.1 (a) with $k = 0$, we conclude that for every $\varepsilon > 0$, $Z_t^{(\varepsilon)}$ is either empty for sufficiently large t or non-empty for sufficiently large t. Hence either

(1) for all $\varepsilon > 0$, $Z_t^{(\varepsilon)}$ is non-empty for sufficiently large t, or

(2) there exists $e > 0$ and N such that $Z_t^{(e)}$ is empty for all $t \geq N$.

We can decide which case holds as follows. Invoking Lemma 9.5.1 (b), let ψ be a formula such that for all $\varepsilon > 0$, $\psi(\varepsilon)$ holds if and only if $Z_t^{(\varepsilon)}$ is non-empty for all sufficiently large t. Case 1 holds if and only if the $\mathcal{L}_{or}$-sentence $\forall \varepsilon > 0 \colon \psi(\varepsilon)$ is true, which can be verified using a decision procedure for the first-order theory of reals numbers (Theorem 1.3.5). If the sentence $\forall \varepsilon > 0 \colon \psi(\varepsilon)$ is false, then by trial-and-error we can first compute rational $e > 0$ for which $\psi(e)$ does not hold. We can then use Lemma 9.5.1 (c) to compute N such that for all $t \geq N$, $Z_t^{(e)} = \emptyset$.

Suppose Case 2 holds. Since $Z_t^{(e)} = \emptyset$ implies that $(M^n s + eP(n)) \cap T = \emptyset$, we have that that $\langle M, s, T \rangle \in \mathsf{TRP}$ if and only if for all $\varepsilon > 0$, there exists $n < N$ such that $M^n s + \varepsilon P(n)$ intersects T. This can be expressed as a first-order $\mathcal{L}_{or}$-sentence and verified using Theorem 1.3.5.

Suppose Case 1 holds. We will show that for each $\varepsilon_1 > 0$ there exists n such that $M^n s + \varepsilon_1 P(n)$ intersects T. Fix $\varepsilon_1 > 0$ and let δ, ε_2 be as in (B). By reducing the value fo ε_2 if necessary, w.l.o.g. we can assume that ε_2 is rational. Consider the family of sets $(Z_t^{(\varepsilon_2)})_{t \geq 0}$, defined by

$$\mathbf{x} \in Z_t^{(\varepsilon_2)} \Leftrightarrow \Phi(\varepsilon_2, \mathbf{x}, t, r_1^t, \ldots, r_m^t).$$

Since $Z_t^{(\varepsilon_2)} \neq \emptyset$ for all sufficiently large $t \geq 0$ by the assumption that Case 1 holds, by Lemma 9.1.1 the sequence $(Z_t^{(\varepsilon_2)})_{t \geq 0}$ has a non-empty limit shape $L \subseteq \mathcal{D}$. Choose any point $X \in L$, and invoking Lemma 9.3.1, let $n \geq N$ be such that $\|X - D^n\|_2 < \delta/2$. Applying Lemma 9.1.1 (b), let $Y \in \mathcal{D}$ be such that

(a) $\|X - Y\|_2 < \delta/2$, and

(b) $Y \in Z_n^{(\varepsilon_2)}$, i.e. $\mathcal{A}(n, Y) + \varepsilon_2 P(n)$ intersects T.

We have $\|Y - D(n)\|_2 < \delta$ by the triangle inequality. Applying (B),

$$M^n s + \varepsilon_1 P(n) = \mathcal{A}(n, D^n) + \varepsilon_1 P(n) \supseteq \mathcal{A}(n, Y) + \varepsilon_2 P(n).$$

Since the latter intersects T by construction, we conclude that $M^n s + \varepsilon_1 P(n)$ also intersects T. □

In the following two sections we will apply Lemma 9.5.2 to prove decidability results for the TRP and the PRP. The next corollary will be used to show that $\overline{\mathsf{TRP}} \subseteq \mathsf{SIP}$.

Corollary 9.5.3. *Let $J, s, T, (P(n))_{n\in\mathbb{N}}$ be as above, and suppose $\mathbf{0} \in P(n)$ for all n. If there exists $\varepsilon > 0$ such that $M^n s + \varepsilon P(n)$ does not intersect T for all $n \in \mathbb{N}$, then there exists effectively computable $N \in \mathbb{N}$ such that*

(a) $\mathcal{A}(t)$ does not intersect T for all $t \geq N$, and

(b) $M^n s \notin T$ for $0 \leq n \leq N$.

Proof. Under the assumption that for all sufficiently small $\varepsilon > 0$, $M^n s + \varepsilon P(n)$ does not intersect T for all $n \in \mathbb{N}$, Case 1 cannot hold in the proof of Lemma 9.5.2. Hence Case 2 holds, and as discussed in the proof, there exist effectively computable $N \in \mathbb{N}$ and $\varepsilon \in \mathbb{Q}_{>0}$ such that $\mathcal{A}(t) + \varepsilon P(n)$ does not intersect T for all $t \geq N$. From $\mathbf{0} \in P(n)$ it follows that $\mathcal{A}(t)$ does not intersect T for $t \geq N$. To prove (b), observe that by $\mathbf{0} \in P(n)$, $M^n s \notin T$ for all $n \in \mathbb{N}$. □

9.6 Topological Reachability Problem

Using the results we have developed so far we can now prove the following.

Theorem 9.6.1. *The Topological Reachability Problem is decidable.*

Proof. Suppose we are given $M \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$, $\tilde{s} \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$, and a semialgebraic target $\widetilde{T}$. Write $M = P^{-1}JP$, where $J = \mathrm{diag}(J_1, \ldots, J_l)$ is in real Jordan form and each J_i is a real Jordan block. Further let $s = P\tilde{s}$, $T = P\widetilde{T}$, $B = \prod_{i=1}^{l} B_i$ be the control set we gave for J in Section 9.4, and define $A = P^{-1}B$. Observe that A is a bounded open set containing $\mathbf{0}$ and hence by Lemma 9.2.1, $\langle M, s, \widetilde{T}\rangle \in \mathsf{TRP}$ if and only if for all $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $M^n\tilde{s} + \varepsilon M^n A$ intersects $\widetilde{T}$. The latter is equivalent to

$$\forall \varepsilon > 0.\, \exists n \in \mathbb{N}\colon J^n s + J^n B \text{ intersects } T \tag{9.1}$$

since $M^n A = P^{-1}J^n PA = P^{-1}J^n B$. Factorise $J = CD$, $C = \mathrm{diag}(C_1, \ldots, C_l)$ as in Section 9.3, recalling that all eigenvalues of C are real and all eigenvalues of D lie on the unit circle. Let $\mathcal{D}$ be the Euclidean closure of $(D^n)_{n\in\mathbb{N}}$ and $\mathcal{A}(t)$ be the abstraction of the orbit of (J, s) described in Section 9.3. Finally, define $P(n) = J^n B$ for all $n \in \mathbb{N}$. We will use Lemma 9.5.2 to prove that whether 9.1 holds is decidable.

By Lemma 9.4.1 (a), there exists $\varphi \in \mathcal{L}_{or}$ such that

$$\mathbf{x} \in P(n) \quad \Leftrightarrow \quad \varphi(\mathbf{x}, n, r_1^n, \ldots, r_m^n)$$

Condition (A) of Lemma 9.5.2 is satisfied by Lemma 9.4.3 (a). We next show that condition (B) is met with $N = 0$. Given $\varepsilon_1 > 0$, let $\varepsilon_2 = \varepsilon_1/2$ and δ be such that for all $1 \leq i \leq l$,

$$\mathcal{B}(\mathbf{0}, \delta) \subseteq \frac{\varepsilon_1}{2} B_i.$$

Such δ exists because every B_i contains an open set around the origin. Recall that $\mathcal{D} \subset \mathbb{R}^{d \times d}$, and let $X, Y \in \mathcal{D}$ be such that $\|X - Y\|_2 < \delta$. Write $X = \operatorname{diag}(X_1, \ldots, X_l)$ and $Y = \operatorname{diag}(Y_1, \ldots, Y_l)$, so that the dimensions of each X_i, Y_i matches those of C_i. That is, $C^n X = \operatorname{diag}(C_1^n X_1, \ldots, C_l^n X_l)$ and $C^n Y = \operatorname{diag}(C_1^n Y_1, \ldots, C_l^n Y_l)$ for all $n \in \mathbb{N}$. We need to prove that for all $n \in \mathbb{N}$,

$$\mathcal{A}(n, X) + \varepsilon_1 C^n B \supseteq \mathcal{A}(n, Y) + \frac{\varepsilon_1}{2} C^n B$$

which is equivalent to

$$\prod_{i=1}^{l} C_i^n (X_i - Y_i) + \varepsilon_1 \prod_{i=1}^{l} C_i^n B_i \supseteq \frac{\varepsilon_1}{2} \prod_{i=1}^{l} C_i^n B_i$$

since $C^n B = \prod_{i=1}^{l} C_i^n B_i$ and $\mathcal{A}(n, Z) = C^n Z$ for all $Z \in \mathcal{D}$. As

$$\prod_{i=1}^{l} C_i^n (X_i - Y_i) + \varepsilon_1 \prod_{i=1}^{l} C_i^n B_i = \prod_{i=1}^{l} \Big(C_i^n (X_i - Y_i) + \varepsilon_1 C_i^n B_i \Big)$$

it suffices to prove that for all $1 \leq i \leq l$,

$$C_i^n (X_i - Y_i) + \varepsilon_1 C_i^n B_i \supseteq \frac{\varepsilon_1}{2} C_i^n B_i.$$

Observe that $\|X_i - Y_i\|_2 < \delta$ since $\|X - Y\|_2 < \delta$. Moreover, by construction of δ, it holds that $\mathbf{0} \in X_i - Y_i + \frac{\varepsilon_1}{2} B_i$. Hence

$$C_i^n (X_i - Y_i) + \frac{\varepsilon_1}{2} C_i^n B_i = C_i^n (X_i - Y_i + \frac{\varepsilon_1}{2} B_i) \ni \mathbf{0}$$

for all $n \in \mathbb{N}$. Recalling from Lemma 9.4.2 that $B_i = \frac{1}{2} B_i + \frac{1}{2} B_i$, we conclude that for all $n \in \mathbb{N}$,

$$\begin{aligned} C_i^n (X_i - Y_i) + \varepsilon_1 C_i^n B_i &= C_i^n (X_i - Y_i) + \frac{\varepsilon_1}{2} C_i^n B_i + \frac{\varepsilon_1}{2} C_i^n B_i \\ &\supseteq \frac{\varepsilon_1}{2} C_i^n B_i \end{aligned}$$

as required. □

Applying Corollary 9.5.3 to $(P(n))_{n \in \mathbb{N}}$ defined above we obtain the following.

Lemma 9.6.2. *If $\langle M, s, T \rangle \notin \mathsf{TRP}$, then there exists effectively computable $N \in \mathbb{N}$ such that*

(a) $\mathcal{A}(t)$ does not intersect T for all $t \geq N$, and

(b) $M^n s \notin T$ for $0 \leq n \leq N$.

9.7 Pseudo-Reachability Problem

Analysis of pseudo-reachability is more nuanced than that of topological reachability. In [31], we studied the Pseudo-Reachability Problem for targets T that are either a point, a hyperplane, or a halfspace. Writing $\mathcal{O}(M,s)$ for $\{M^n s\colon n \in \mathbb{N}\}$ and $\widetilde{\mathcal{O}}(M,s)$ for the set of points that are pseudo-reachable (i.e. $x \in \widetilde{\mathcal{O}}(M,s)$ if and only if $\langle M, s, \{x\}\rangle \in \mathsf{PRP}$), we gave the following characterisation .

Theorem 9.7.1. *$\widetilde{\mathcal{O}}(M,s) = \mathcal{O}(M,s) \cup \Delta$ for a semialgebraic set Δ that can be effectively determined.*

Recall that by the result [44] of Kannan and Lipton, it is decidable whether a given point x belongs to the orbit $\mathcal{O}(M,s)$. Hence decidability of the PRP with point targets follows immediately from our characterisation. We also used theory of linear recurrence sequences to show decidability of the PRP with hyperplane and halfspace targets by analysing the expression $c^\top M^n s + \varepsilon c^\top \sum_{k=0}^{n-1} M^k B$ for arbitrarily small values of $\varepsilon > 0$, where $c \in \mathbb{Q}^d$ and B is a conveniently shaped ball. Note that this result does not place any restrictions on (M,s). Unfortunately, the methods of [31] do not generalise to any significantly larger class of target sets. We can, however, use our abstraction-based approach to prove the following.

Theorem 9.7.2. *The Pseudo-Reachability Problem is decidable for diagonalisable M.*

Proof. We follow the same strategy as the proof of Theorem 9.6.1. Suppose we are given the instance $\langle M, \tilde{s}, \widetilde{T}\rangle$. Write $M = P^{-1}JP$, where $J = \operatorname{diag}(J_1, \ldots, J_l)$ is in real Jordan form and J_i is a real Jordan block for all i. Let $s = P\tilde{s}$, $T = P\widetilde{T}$, $B = \prod_{i=1}^{l} B_i$ be the control set corresponding to J as described in Section 9.4, and define $A = P^{-1}B$. Since A is bounded and contains a neighbourhood around $\mathbf{0}$, by Lemma 9.2.1 $\langle M, \tilde{s}, \widetilde{T}\rangle \in \mathsf{PRP}$ if and only if for all $\varepsilon > 0$ there exists $n \in \mathbb{N}$ such that $M^n\tilde{s} + \sum_{k=0}^{n-1} M^k A$ intersects $\widetilde{T}$. Since $M^n A = P^{-1}J^n PA$, the latter is equivalent to

$$\forall \varepsilon > 0.\ \exists n \in \mathbb{N}\colon\ (J^n s + \sum_{k=0}^{n-1} J^k B) \cap T \neq \emptyset. \tag{9.2}$$

As described in Section 9.3, factorise $J = CD$, where $C = \operatorname{diag}(C_1, \ldots, C_l)$. Construct the semialgebraic $\mathcal{D}$, which is the Euclidean closure of $(D^n)_{n\in\mathbb{N}}$, and the abstraction $\mathcal{A}(t)$ of the orbit of (J,s). Finally, define $P(n) = \sum_{k=0}^{n-1} J^k B$ for all $n \in \mathbb{N}$. We will prove that the statement 9.2 is decidable using Lemma 9.5.2.

By Lemma 9.4.1 (b), there exists $\varphi \in \mathcal{L}_{or}$ such that

$$\mathbf{x} \in P(n) \quad \Leftrightarrow \quad \varphi(\mathbf{x}, n, r_1^n, \ldots, r_m^n)$$

Condition (A) of Lemma 9.5.2 is satisfied by Lemma 9.4.3 (b). It remains to prove that condition (B) is met. We choose $N = 1$. Given $\varepsilon_1 > 0$, let $\varepsilon_2 = \varepsilon_1/2$ and δ be such that for all $1 \leq i \leq l$,

$$C_i \cdot \mathcal{B}(\mathbf{0}, \delta) \subseteq \frac{\varepsilon_1}{2} B_i.$$

Such δ exists because every B_i contains an open set around the origin. Let $X, Y \in \mathcal{D}$ be such that $\|X - Y\|_2 < \delta$. Write $X = \text{diag}(X_1, \ldots, X_l)$ and $Y = \text{diag}(Y_1, \ldots, Y_l)$ in a way that the dimension of each X_i, Y_i matches those of C_i. That is, $C^n X = (C_1^n X_1, \ldots, C_l^n X_l)$ and $C^n Y = (C_1 Y_1^n, \ldots, C_l^n Y_l^n)$ for all $n \in \mathbb{N}$. We need to prove that for all $n \geq 1$,

$$\mathcal{A}(n, X) + \varepsilon_1 \sum_{k=0}^{n-1} C^k B \supseteq \mathcal{A}(n, Y) + \frac{\varepsilon_1}{2} \sum_{k=0}^{n-1} C^k B$$

which is equivalent to

$$\prod_{i=1}^{l} C_i^n (X_i - Y_i) + \varepsilon_1 \prod_{i=1}^{l} \sum_{k=0}^{n-1} C_i^n B_i \supseteq \frac{\varepsilon_1}{2} \prod_{i=1}^{l} \sum_{k=0}^{n-1} C_i^n B_i$$

since $\mathcal{A}(n, Z) = C^n Z$ for all $Z \in \mathcal{D}$. It suffices to prove that for all $1 \leq i \leq l$ and $n \geq 1$,

$$C_i^n (X_i - Y_i) + \varepsilon_1 \sum_{k=0}^{n-1} C_i^k B_i \supseteq \frac{\varepsilon_1}{2} \sum_{k=0}^{n-1} C_i^k B_i.$$

Since $\|X - Y\|_2 < \delta$, $\|X_i - Y_i\|_2 < \delta$. By construction of δ, it therefore holds that $C_i(X_i - Y_i) \in \frac{\varepsilon_1}{2} B_i$. Hence

$$C_i^n (X_i - Y_i) + \frac{\varepsilon_1}{2} C_i^{n-1} B_i = C_i^{n-1} (C_i (X_i - Y_i) + \frac{\varepsilon_1}{2} B_i) \ni \mathbf{0}$$

for all $n \geq 1$ by the construction of δ. As shown in Lemma 9.4.2, $B_i = \frac{1}{2} B_i + \frac{1}{2} B_i$. Therefore, for $n \geq 1$,

$$\begin{aligned} C_i^n (X_i - Y_i) + \varepsilon_1 \sum_{k=0}^{n-1} C_i^k B_i &= C_i^n (X_i - Y_i) + \varepsilon_2 \sum_{k=0}^{n-1} C_i^k B_i + \varepsilon_2 \sum_{k=0}^{n-1} C_i^k B_i \\ &\supseteq C_i^n (X_i - Y_i) + \varepsilon_2 C_i^{n-1} B_i + \varepsilon_2 \sum_{k=0}^{n-1} C_i^k B_i \\ &\supseteq \varepsilon_2 \sum_{k=0}^{n-1} C_i^k B_i \end{aligned}$$

as required. □

For non-diagonalisable systems, the PRP remains open. An immediate obstacle to applying the abstraction-based method is the following. Let J be in real JNF and B be the bounded open set constructed for in Section 9.4. We showed in Lemma 9.4.1 that $J^n B$ is semialgebraic in $n, r_1^n, \ldots, r_m^n$, where $r_1, \ldots, r_m$ are real algebraic. However, we are unable to prove the same for $P(n) \coloneqq \sum_{k=0}^{n-1} J^k B$, which is required by Lemma 9.5.2.

9.8 Semialgebraic Invariant Problem

In this section our objective is to prove that $\overline{\mathsf{TRP}} \subseteq \mathsf{SIP}$. That is, if there exists a neighbourhood O of s such that $(M^n O)_{n\in\mathbb{N}}$ avoids a semialgebraic set T, then (M, s) has a semialgebraic invariant S disjoint from T. As a side effect, we will also have produced a proof based on the continuous abstraction that that it is decidable, given $\langle M, s, T\rangle$, whether there exists an $\mathcal{L}_e$-definable invariant S of (M, s) that is disjoint from T. This result is the first step of the proof of [6] that the SIP is decidable. The second step is the following.

Theorem 9.8.1 (Lemma 5.2 of [6])**.** $\langle M, s, T\rangle \in \mathsf{SIP}$ *if and only if there exists an inductive invariant* S *of* (M, s) *that is definable in* $\mathbb{R}_{\exp}$ *and disjoint from* T*.*

In order to link topological reachability with semialgebraic invariants we will need to reprove, in terms of the continuos abstraction, certain results of [5] pertaining to $\mathcal{L}_e$-definable invariants of linear dynamical systems. Our goal is the following.

Theorem 9.8.2. *Let* $J \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d\times d}$ *be in real Jordan form,* $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$*, and* T *be a semialgebraic target. Denote by* $\mathcal{A}$ *be the abstraction of the orbit of* (J, s) *defined in Section 9.3. For any inductive,* $\mathcal{L}_e$*-definable invariant* S *of* (J, s) *there exists* $N \in \mathbb{N}$ *such that* $\mathcal{A}(t) \subseteq S$ *for all* $t \geq N$*.*

Since $J^n s \in S$ for $0 \leq n \leq N$ by the definition of an invariant, the statement of Theorem 9.8.2 implies that any $\mathcal{L}_e$-definable invariant of (J, s) must contain the prefix $s, \ldots, M^N s$ of the orbit and the bowl-shaped set $\bigcup_{t\geq N} \mathcal{A}(t)$ for some $N \geq 0$. On the other hand, since $J\mathcal{A}(t) = \mathcal{A}(t + 1)$ by Lemma 9.3.3, for every N the set

$$S_N \coloneqq \{s, \ldots, M^N s\} \cup \bigcup_{t\geq N} \mathcal{A}(t)$$

is an inductive invariant of (J, s). Therefore, when searching for an $\mathcal{L}_e$-definable invariant of (J, s) disjoint from a target set T, it will suffice to only consider the family $\{S_N \colon N \in \mathbb{N}\}$ of invariants.

To prove Theorem 9.8.2, we will need the following lemmas. We say that a function $f \colon \mathbb{R}^d \to \mathbb{R}$ is *$\mathcal{L}_e$-definable* if its graph $\{(x, y) \colon f(x) = y\}$ is an $\mathcal{L}_e$-definable subset of $\mathbb{R}^{d+1}$.

Lemma 9.8.3 (Lemma 10 in [5])**.** *If* X, Y *are* $\mathcal{L}_e$*-definable and dense subsets of* $\mathcal{L}_e$*-definable* $\mathcal{D}$*, then* $X \cap Y$ *is non-empty.*

Lemma 9.8.4. *Let $\mathcal{D} \subseteq \mathbb{R}^d$ be $\mathcal{L}_e$-definable and $f\colon \mathcal{D} \to \mathbb{R}$ be an $\mathcal{L}_e$-definable function. Then f is bounded on some open subset O of $\mathcal{D}$.*

Proof. Let $\Gamma = \{(x, f(x)) \mid x \in \mathbb{R}^d\}$ be the graph of f and $m = \dim(\Gamma)$. Decompose Γ into cells $A_1, \ldots, A_k$, where each A_i is homeomorphic to $(0,1)^{m_i}$. Denoting by $\Pi : \mathbb{R}^{d+1} \to \mathbb{R}^d$ the projection map onto the first d coordinates, let $B_i = \Pi(A_i)$ for all $1 \leq i \leq k$. Since each A_i is a cell, f is continuous on every B_i, and hence B_i is also homeomorphic to $(0,1)^{m_i}$. Moreover, $\{B_1, \ldots, B_k\}$ is a cell decomposition of $\mathcal{D}$ and hence $\dim(\mathcal{D}) = \dim(\Gamma)$. Let $m = \max_{1 \leq i \leq k} m_i$ and l be such that $m = m_l$.

Since $\mathcal{D}$ is closed and $\mathcal{L}_e$-definable, by [33, Chapter 4, 1.12] the cell decomposition $\{B_1, \ldots, B_k\}$ is a *stratification*. That is, the boundary points of each B_i in $\mathcal{D}$ are contained in a union of cells of dimension less than m_i. In particular, B_l does not contain any of its boundary points in $\mathcal{D}$. Hence B_l is open in $\mathcal{D}$.

If $m = 0$, then $\mathcal{D}$ is finite and we can take $O = \mathcal{D}$. Suppose $m > 0$. Since B_l is homeomorphic to $(0,1)^m$, we can construct $O \subset C \subset B_l$ such that O is an open subset of both B_l and $\mathcal{D}$, and C is a closed subset of B_l and $\mathcal{D}$. By compactness, f attains its maximum and minimum over C and hence is bounded over O. □

Proof of Theorem 9.8.2. Let S be an $\mathcal{L}_e$-definable invariant of (J, s). Factorise $J = CD$ and define the abstraction $\mathcal{A}(t)$ of the orbit of (J, s) as specified in Section 9.3. Recall that $\mathcal{D}$ is the topological closure of $(D^n)_{n \in \mathbb{N}}$, $\mathcal{A}(t, Z) = C(t)Zs$ for all $Z \in \mathcal{D}$ and $t \geq 0$, and $\mathcal{A}(t) = C(t)\mathcal{D}s$. We will consider *trajectory rays* of the form $(\mathcal{A}(t, Z))_{t \geq 0}$. For each $Z \in \mathcal{D}$, the set

$$V(Z) \coloneqq \{t \geq 0 \colon \mathcal{A}(t, Z) \in S\}$$

is definable in $\mathbb{R}_{\exp}$ with parameters from $\mathbb{R}$. By o-minimality, each $V(Z)$ is a finite union of intervals. That is, $\mathcal{A}(t, Z)$ either belongs to S for all sufficiently large t, or is outside S for all sufficiently large t. We write

(a) $R_1 \coloneqq \{Z \in \mathcal{D} \mid V(Z) \text{ is bounded}\}$, and

(b) $R_2 \coloneqq \{Z \in \mathcal{D} \mid V(Z) \text{ is unbounded}\}$.

Both sets are definable in $\mathbb{R}_{\exp}$ with parameters from $\mathbb{R}$. For $Z \in \mathcal{D}$, further define

$$f(Z) \coloneqq \inf \{\tau \geq 0 \mid t \in V(Z) \text{ for all } t \geq \tau, \text{ or } t \notin V(Z) \text{ for all } t \geq \tau\}$$

to be the earliest time from which onwards the ray $\mathcal{A}(t, Z)$ does not enter or leave S. We first show that $R_1 = \emptyset$ and $R_2 = \mathcal{D}$. An intermediate step is the following lemma.

Lemma 9.8.5. *Either $R_1 = \emptyset$ or $R_2 = \emptyset$.*

Proof. Suppose $R_1, R_2 \neq \emptyset$, and consider $Z \in R_1$. Consider $Z_n \coloneqq D^{-n}Z$ for $n \in \mathbb{N}$, and recall from Lemma 9.3.3 that $M\mathcal{A}(t, Z) = \mathcal{A}(t+1, DZ)$. If $\mathcal{A}(t, Z_n) \in S$, then, because S satisfies $MS \subseteq S$,

$$M^n\mathcal{A}(t, Z_n) = \mathcal{A}(t+n, D^nZ_n) = \mathcal{A}(t+n, Z)$$

must also belong to S.Hence $Z_n \in R_2$ implies $Z \in R_2$ for all $n \in \mathbb{N}$. Since $Z \in R_1$ by assumption, we conclude that $Z_n \in R_1$ for all $n \in \mathbb{N}$.

As shown in Lemma 9.3.1, $(D^{-n})_{n\in\mathbb{N}}$ is dense in $\mathcal{D}$. Recall from Section 9.3 that by construction, every $Z \in \mathcal{D}$ is a block-diagonal matrix whose blocks are either 2×2 rotation matrices or identity matrices. Therefore, $x \mapsto xZ$ is an isometry of $\mathcal{D}$. It follows that $(Z_n)_{n\in\mathbb{N}}$ and hence R_1 are dense in $\mathcal{D}$.

Now consider $Y \in R_2$. Let $\tau \geq 0$ be such that $\mathcal{A}(t, Y) \in S$ for all $t \geq \tau$. From $MS \subseteq S$ we conclude that $M\mathcal{A}(t, Y) = \mathcal{A}(t+1, DY) \in S$ for all $t \geq \tau$ and hence $Y_n \coloneqq D^nY \in R_2$ for all $n \in \mathbb{N}$. Since $(Y_n)_{n\in\mathbb{N}}$ is dense in $\mathcal{D}$, R_2 is also dense in $\mathcal{D}$.

Since R_1 and R_2 are definable in $\mathbb{R}_{\exp}$ (with parameters from $\mathbb{R}$) and dense in $\mathcal{D}$ as shown above, by Lemma 9.8.3 they must have non-empty intersection. This is a contradiction as, R_1, R_2 are disjoint by construction. We conclude that at least one of R_1, R_2 must be empty. □

Suppose $R_1 = \mathcal{D}$ and $R_2 = \emptyset$. That is, for all $Z \in \mathcal{D}$, $\mathcal{A}(t, Z) \notin S$ for sufficiently large t. Recall that $MS \subseteq S$. In particular, if $\mathcal{A}(t, Z) \in S$ then

$$M\mathcal{A}(t, Z) = \mathcal{A}(t+1, DZ) \in S.$$

Hence for all $Z \in \mathcal{D}$,

$$f(Z) \leq \max\{0, f(DZ) - 1\} \leq f(DZ).$$

By Lemma 9.8.4, there exist an open subset O of $\mathcal{D}$ and $b \in \mathbb{N}$ such that $f(Z) \leq b$ for all $Z \in O$. Consider $(D^{-n}O)_{n\in\mathbb{N}}$, By density of $(D^{-n})_{n\in\mathbb{N}}$ in $\mathcal{D}$,

$$\bigcup_{n\in\mathbb{N}} D^{-n}O$$

is an open cover of $\mathcal{D}$. By compactness, there exists K such that $\bigcup_{n=0}^{K} D^{-n}O = \mathcal{D}$. That is, for every $Z \in \mathcal{D}$ there exists $0 \leq n \leq K$ such that $D^nZ \in O$. Hence

$$f(Z) \leq f(DZ) \leq \ldots \leq f(D^nZ) \leq b.$$

Therefore, $f(Z) \leq b$ for all $Z \in \mathcal{D}$. But this cannot be the case: let $n > b$ and consider $M^n s = \mathcal{A}(n, D^n)$. Together $R_1 = \mathcal{D}$ and $f(D^n) \leq b$ imply that $D^n \in R_1$ and $\mathcal{A}(n, D^n) \notin S$. However, $M^n s = \mathcal{A}(n, D^n) \in S$ since S is an invariant of (M, s). Arriving at a contradiction, we conclude that it is not the case that $R_1 = \mathcal{D}$ and $R_2 = \emptyset$. From Lemma 9.8.5 it follows that $R_1 = \emptyset$ and $R_2 = \mathcal{D}$.

It remains establish existence of N such that $\mathcal{A}(t) \subseteq S$ for all $t \geq N$. That is, we have to establish an upper bound N on $f(Z)$ for $Z \in \mathcal{D}$. Applying Lemma 9.8.4, there exist an open subset O of $\mathcal{D}$ and $b \in \mathbb{N}$ such that $f(Z) \leq b$ for all $Z \in O$. This time consider $\bigcup_{n \in \mathbb{N}} D^n O$, which is an open cover of $\mathcal{D}$ by density of $(D^n)_{n \in \mathbb{N}}$ in $\mathcal{D}$. By compactness, there exists K such that

$$\mathcal{D} = \bigcup_{n=0}^{K} D^n O.$$

Recall that for all $Z \in \mathcal{D}$, if $\mathcal{A}(t, Z) \in S$ then $\mathcal{A}(t+1, DZ) \in S$. Hence $f(DZ) \leq f(Z) + 1$ for all Z. Fix $Z \in \mathcal{D}$, and let $0 \leq n \leq K$ be such that $Z \in D^n O$. We have

$$f(Z) \leq f(D^{-1}Z) + 1 \leq \cdots \leq f(D^{-n}Z) + n.$$

Since $D^{-n}Z \in O$, we conclude that $f(Z) \leq b + n$. Hence for all $Z \in \mathcal{D}$, $f(Z) \leq b + K$. Since the choice of Z was arbitrary, we can take $N = b + K$. This concludes the proof of Theorem 9.8.2. □

Using Theorem 9.8.2, if we are given $\langle M, s, T \rangle$, we can decide whether (M, s) has an $\mathcal{L}_e$-definable invariant S disjoint from T as follows. Write $M = P^{-1}JP$, where J is in Jordan form. We have $MS \subseteq S \Leftrightarrow J(PS) \subseteq (PS)$. Moreover, $S \cap T = \emptyset$ if and only if $PS \cap PT = \emptyset$. Hence it suffices to decide whether (J, s) has an $\mathcal{L}_e$-definable invariant disjoint from PT. Consider the formula

$$\Phi(t) \coloneqq \mathcal{A}(t) \cap PT = \emptyset$$

which, by Lemma 9.3.2, can be written in the form $\varphi(t, r_1^t, \ldots, r_m^t)$ for $\varphi \in \mathcal{L}_{or}$ and positive $r_1, \ldots, r_m \in \mathbb{R} \cap \overline{\mathbb{Q}}$. Applying Lemma 9.5.1 (c), we can effectively compute integer N such that either $\Phi(t)$ holds for all $t \geq N$, or it does not hold for all $t \geq N$. By Theorem 9.8.2, the desired $\mathcal{L}_e$-definable invariant exists if and only if the first case holds and $M^n s \notin PT$ for all $0 \leq n \leq N$.

We are finally in a position to prove $\overline{\mathsf{TRP}} \subseteq \mathsf{SIP}$.

Theorem 9.8.6. *If $\langle M, s, T \rangle \notin \mathsf{TRP}$, then there exists a semialgebraic inductive invariant S of (M, s) that is disjoint from T.*

Proof. Write $M = P^{-1}JP$ where J is in real Jordan form, and let $\mathcal{A}$ be the abstraction of the orbit of (J, Ps). As discussed in Section 9.6, $\langle M, s, T\rangle \notin \mathsf{TRP}$ is equivalent to $\langle J, Ps, PT\rangle \notin \mathsf{TRP}$. Applying Lemma 9.6.2, there exists effectively computable integer N such that

(a) $J^n Ps \notin PT$ for all $0 \leq n \leq N$, and

(b) $\mathcal{A}(t)$ does not intersect PT for all $t \geq N$.

By Theorem 9.8.2, there exists an $\mathcal{L}_e$-definable invariant S of (J, Ps) disjoint from T. By Theorem 9.8.1, $\langle J, Ps, PT\rangle \in \mathsf{SIP}$, which implies $\langle M, s, T\rangle \in \mathsf{SIP}$. □

The converse inclusion, however, does not hold. Writing

$$R(\theta) \coloneqq \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

consider $M = 2R(\pi/2)$, which is already in real Jordan form. Let $s = (1, 0)$ and $T = \{(x, 1) \mid x \geq 1\}$. Clearly, T is not reached by the orbit of (M, s). Moreover,

$$\mathcal{A}(t) = 2^t\{(1, 0), (0, 1), (-1, 0), (-1, 1)\}$$

which is disjoint from T for all $t \geq 0$. Hence

$$S = \bigcup_{t\geq 0} \mathcal{A}(t) = \{(0, y) \colon |y| \geq 1\} \cup \{(x, 0) \colon |x| \geq 1\}$$

is an inductive invariant of (M, s) certifying non-reachability in T.

However, T is topologically reachable. For $n \geq 1$, let x_n be the point in T such that $|x_n| = 2^n$. We can define $R_n \coloneqq R(\theta_n)$ with $\theta_n \to 0$ as $n \to \infty$ such that $x_n = 2^n R_n s$ for all n. Given an open set O around s, first choose $\theta > 0$ such that for all $0 \leq \theta' < \theta$, $(\cos(\theta'), \sin(\theta')) \in O$. Then find n divisible by 4 such that $\theta_n < \theta$, and let $\hat{s} \coloneqq (\cos\theta_n, \sin\theta_n) = R_n s \in O$. As 4 divides n, $M^n t\hat{s} = 2^n \hat{s}t$, which is equal to x_n by construction. Note that $x_n \in T$. We conclude that in every neighbourhood of s there exists $\hat{s}$ whose orbit under M reaches T.

9.9 Hardness results

We now discuss hardness results for various problems conceptually related to the TRP and the PRP. One of the most salient patterns appearing in the preceding chapters was that for various classes of LDS and semialgebraic targets, a good understanding of reachability properties suffices for being able to decide the full Model-Checking

Problem. In Chapter 7 we even formally showed that for diagonalisable systems, the Model-Checking Problem is Turing-reducible to the Reachability Problem. The situation for pseudo-orbits, however, is markedly different.

Theorem 9.9.1. *Let $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$ and $H \subset \mathbb{R}^d$ be a halfspace defined by $x \in H \Leftrightarrow c^\top x \geq 0$ for $c \in \mathbb{Q}^d$. The following problems are at least as hard as the Positivity Problem for LRS over $\mathbb{Q}$.*

(A) Decide whether for every $\varepsilon > 0$, there exists $\hat{s} \in \mathcal{B}(s, \varepsilon)$ such that the orbit of $(M, \hat{s})$ remains in H.

(B) Decide whether for every $\varepsilon > 0$, there exists an ε-pseudo-orbit of (M, s) that remains in H.

Proof. Let $(u_n)_{n\in\mathbb{N}}$ be an LRS over $\mathbb{Q}$ with companion matrix $M \in \mathbb{Q}^{d\times d}$. As discussed in Section 2.1, $u_n = e_1^\top M^n s$, where $s = (u_0, \ldots, u_{d-1})$. Observe that $u_n \geq 0$ for all $n \in \mathbb{N}$ if and only if the orbit $(M^n s)_{n\in\mathbb{N}}$ remains in H. Given $(u_n)_{n\in\mathbb{N}}$, our many-one reduction to Problem (A) is to return $\langle M, s, H\rangle$. To prove the correctness of this reduction, suppose $u_n \geq 0$ for all $n \in \mathbb{N}$. Let $\hat{s} = s$. Clearly, the orbit of $(M, \hat{s})$ remains in H. Next, suppose there exists $k \in \mathbb{N}$ such that $u_k < 0$. It holds that $M^k s \notin H$. Since H is closed, there exists $\varepsilon_1 > 0$ such that $M^k s + \varepsilon_1 M^k \mathcal{B}(\mathbf{0}, 1)$ does not intersect H. Hence for ε_1, there does not exist $x \in \mathcal{B}(s, \varepsilon_1)$ such that $\mathcal{O}(M, x)$ remains in H.

Given $(u_n)_{n\in\mathbb{N}}$, our many-one reduction to Problem (B) also returns $\langle M, s, H\rangle$. If $u_n \geq 0$ for all $n \in \mathbb{N}$, then for all $\varepsilon > 0$ we can choose $(M^n s)_{n\in\mathbb{N}}$ itself as the ε-pseudo-orbit that remains in H. If $u_k < 0$ for some $k \in \mathbb{N}$, let $\varepsilon > 0$ be sufficiently small such that $M^k s + \varepsilon \sum_{i=0}^{k-1} \mathcal{B}(\mathbf{0}, 1)$ does not intersect T. We have that all ε-pseudo-orbits of (M, s) leave H at time k. □

Let φ denote the LTL formula $\Box H$, meaning "H holds at all times". Problem (A) is to decide whether in every neighbourhood of s there exists a point $\hat{s}$ such that the orbit $\mathcal{O}(M, \hat{s})$ satisfies φ. Problem (B), on the other hand, is to decide whether for every $\varepsilon > 0$, the LDS (M, s) has an ε-pseudo-orbit that satisfies φ. The theorem above shows that the generalisation of either the TRP or the PRP from reachability properties to ω-regular properties (while maintaining the existential quantification over starting points and pseudo-orbits, respectively) immediately runs into the open Positivity Problem for linear recurrence sequences.

Another way to modify the TRP would be to remove the universal quantification over $\varepsilon > 0$, which amounts to making the set of all possible starting points part of the

input. If we also stay within the realm of semialgebraic sets, the result is the following problem.

Semialgebraic Orbit Problem. Given $M \in \mathbb{Q}^{d\times d}$ and semialgebraic $B, T \subseteq \mathbb{R}^d$, decide if there exist $s \in B$ and $n \in \mathbb{N}$ such that $M^n s \in T$.

This problem is decidable [9] for $d \leq 3$ and Diophantine-hard at order $d = 4$ if we restrict B to contain a single point and T to be a polytope [25]. Requiring the starting set B set to have non-zero measure does not help: In [3] it is shown that if we restrict B to balls of positive radius and H to hyperplanes, the Semialgebraic Orbit Problem remains Diophantine-hard. Further restricting B to be open or closed does not make a difference either.

We can also modify the PRP in the same way as above by making the set of allowed perturbations at each step a part of the input. The result is the following well-known problem in control theory.

Reachability Problem for Linear Time-Invariant Systems. Given $M \in \mathbb{Q}^{d\times d}$, a starting point $s \in \mathbb{Q}^d$, and semialgebraic sets B, T, decide if there exists a sequence $(u_n)_{n\in\mathbb{N}}$ of control inputs from B such that the trajectory defined by $x_0 = s$ and $x_{n+1} = Mx_n + u_n$ for $n \in \mathbb{N}$ reaches T.

In [37] it is shown that the Reachability Problem for linear time-invariant systems is undecidable for B that is a finite union of affine subspaces of $\mathbb{R}^d$, and Positivity-hard if we restrict B to be a bounded polytope.

Discussion

In this thesis we presented various decidable fragments of the Model-Checking Problem for discrete-time linear dynamical systems, and showed that significantly extending any of our decidability results requires solving open cases of at least one of the Skolem, Positivity and Ultimate Positivity problems.[3] Among these problems of linear recurrence sequences, the Skolem Problem appears to be the most tractable. In particular, for diagonalisable LRS over $\mathbb{Q}$, the Skolem Problem is arguably "solved in practice": As discussed in Section 2.3, an algorithm is given in [16] that

(a) always terminates assuming the Skolem Conjecture (also called the Exponential Local-Global Principle) and the p-adic Schanuel Conjecture, and

(b) upon termination, is (unconditionally) guaranteed to produce either a zero of the input LRS, or a certificate showing that no zero exists.

The Positivity and Ultimate Positivity problems, on the other hand, have not seen much progress since the works [66, 67, 68] of Ouaknine and Worrell, which prove decidability of both problems at low orders and full decidability of Ultimate Positivity for diagonalisable sequences. We mention the recent the work [50] by Kenison et al. that shows decidability of the Positivity Problem for the special class of *reversible* sequences of order at most 11.

Speaking hypothetically, if we assume that the Skolem Problem is decidable for LRS over $\mathbb{Q}$, then the Model-Checking Problem becomes decidable for arbitrary linear dynamical systems (M, s) and $\mathcal{T}$ containing only *algebraic* targets; see [54] and Section 2.3. This is not surprising as for each algebraic set T and LDS (M, s), there exists an LRS $(u_n)_{n\in\mathbb{N}}$ over $\mathbb{Q}$ such that for all $n \in \mathbb{N}$, $u_n = 0$ if and only if $M^n s \in T$.

Recall from Chapter 7 that if we assume decidability of the Positivity Problem for diagonalisable LRS over $\mathbb{Q}$, then the full Model-Checking Problem for diagonalisable systems becomes decidable. Non-diagonalisable LDS, in comparison, are much more

[3] Recall that the Diophantine-hard instances of the MCP that we gave in Chapter 8 are subsumed by the Positivity Problem.

intricate. For example, if we assume full decidability of both the Positivity and Ultimate Positivity problems, then it is not clear that we can prove full decidability of the MCP, or, for that matter, decidability of the MCP with prefix-independent properties. The main culprit behind this is the loss of (eventual) toricity and almost-periodicity: Recall that in Section 8.2 we constructed non-diagonalisable $(M, s) \in \mathbb{Q}^{4\times 4} \times \mathbb{Q}^4$ and a polynomial p with rational coefficients such that the sign pattern of $u_n = p(M^n s)$ is not almost-periodic and hence not eventually toric either. As a result, we have the following obstacles to proving decidability of the MCP in dimension 4 or higher.

(1) Since the sign pattern α_u of $(p(M^n s))_{n\in\mathbb{N}}$ is not necessarily almost-periodic, if we have means to decide whether a finite pattern $u \in \{+, 0, -\}^*$ occurs in α_u, we still would not know how to decide if a given deterministic automaton accepts α_u.

(2) Let q be another polynomial with rational coefficients, $v_n = q(M^n s)$, and α_v be the sign pattern of $(v_n)_{n\in\mathbb{N}}$. Suppose we want to model check the characteristic word α of (M, s) with respect to a semialgebraic target T defined by inequalities involving polynomials p and q. Even if we know "everything" individually about α_u and α_v, without toricity we do not how how to deduce properties of α from the properties of the two sign patterns. In Chapters 5 to 7 we relied on the argument that if the sign patterns of $p_1(M^n s), \ldots, p_k(M^n s)$ are eventually toric, where $p_1, \ldots, p_k$ are the polynomials defining a collection $\mathcal{T}$ of semialgebraic sets, then the characteristic word of (M, s) with respect to $\mathcal{T}$ is also eventually toric.

At the time of writing, it is possible (and conceivable) that both the Positivity and Ultimate Positivity problems are decidable, whereas the full Model-Checking Problem for linear dynamical systems is undecidable.

To the best of our knowledge, no undecidability result is known for natural model-checking problems of linear dynamical systems that only involve the single orbit $(M^n s)_{n\in\mathbb{N}}$. However, [46] shows that the following multi-path problem about LDS is undecidable. Given an update matrix M, a semialgebraic starting set S, a positive integer k, and a target hyperplane H, decide if there exists $s \in S$ such that the orbit $(M^n s)_{n\in\mathbb{N}}$ reaches H at least k times. The undecidability proof is based on a reduction from Hilbert's 10th problem, and involves only matrices of the form $I + N$, where N is nilpotent.

Recently, model-checking problems have been studied for *continuous-time* linear dynamical systems. Such a system, just like a discrete-time LDS, is given by a pair $(M, s) \in \mathbb{Q}^{d\times d} \times \mathbb{Q}^d$, but its trajectory is described by $x(0) = s$ and $x(t) = e^{Mt}x(0)$

for $t \in \mathbb{R}_{>0}$. All problems considered in this thesis have analogous, continuous-time formulations, The Skolem Problem for continuous-time LDS, for example, is to decide, given (M, s) and a target hyperplane H, whether there exists $t \geq 0$ such that $x(t) \in H$. This problem is known to be decidable in dimension $d \leq 9$ assuming Schanuel's conjecture. Overall, the mathematical tools used across the two settings to obtain decidability results for exact verification problems are fairly different [27]. In contrast, the "inexact" (alternatively, robust) verification problems that we considered in Chapter 9 are solved in the discrete and the continuous settings in the same way; see [8, 32]. This correspondence is completely unsurprising since we used a continuous abstraction technique (Chapter 9) to solve the Topological Reachability, Pseudo-Reachability, and Semialgebraic Invariant problems for discrete-time LDS.

All decidability results of this thesis also apply to orbits $(M^n s)_{n\in\mathbb{N}}$ where M, s have real algebraic entries. Our complexity analyses, however, become invalid, primarily because the degrees of the eigenvalues of $M \in (\mathbb{R}\cap\overline{\mathbb{Q}})^{d\times d}$ need not be bound by d. If we assume Schanuel's conjecture, the decidability results of Chapter 9 can be generalised from semialgebraic targets to $\mathcal{L}_e$-definable sets, i.e. targets that can be defined using real exponentiation as well as arithmetic and logical operations. Schanuel's conjecture is needed to decide whether, given (M, s), positive integer n, and $\mathcal{L}_e$-definable target T, whether $M^n s \in T$.

Bibliography

[1] SKOLEM: Solves the Skolem Problem for Simple Integer Linear Recurrence Sequences. skolem.mpi-sws.org/, 2023. [Online; accessed on 13 November 2023].

[2] S. Akiyama, M. Barge, V. Berthé, J.-Y. Lee, and A. Siegel. On the Pisot Substitution Conjecture. In *Mathematics of Aperiodic Order*, pages 33–72. Springer Basel, 2015.

[3] S. Akshay, Hugo Bazille, Blaise Genest, and Mihir Vahanwala. On Robustness for the Skolem and Positivity Problems. In Petra Berenbrink and Benjamin Monmege, editors, *39th International Symposium on Theoretical Aspects of Computer Science (STACS 2022)*, volume 219 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 5:1–5:20, Dagstuhl, Germany, 2022. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[4] Jean-Paul Allouche and Jeffrey Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.

[5] Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-minimal Invariants for Linear Loops. In Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella, editors, *45th International Colloquium on Automata, Languages, and Programming (ICALP 2018)*, volume 107 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 114:1–114:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[6] Shaull Almagor, Dmitry Chistikov, Joël Ouaknine, and James Worrell. O-Minimal Invariants for Discrete-Time Dynamical Systems. *ACM Trans. Comput. Logic*, 23(2), Jan 2022.

[7] Shaull Almagor, Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. Deciding ω-Regular Properties on Linear Recurrence Sequences. *Proc. ACM Program. Lang.*, 5(POPL):1–24, 2021.

[8] Shaull Almagor, Edon Kelmendi, Joël Ouaknine, and James Worrell. Invariants for Continuous Linear Dynamical Systems. In Artur Czumaj, Anuj Dawar, and Emanuela Merelli, editors, *47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)*, volume 168 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 107:1–107:15, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[9] Shaull Almagor, Joël Ouaknine, and James Worrell. First-Order Orbit Queries. *Theor. Comp. Sys.*, 65(4):638–661, May 2021.

[10] D. V. Anosov. Geodesic Flows on Closed Riemannian Manifolds of Negative Curvature. *Proc. Steklov Inst. Math.*, 90, 1967.

[11] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, 2008.

[12] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*. Springer Berlin Heidelberg, 2006.

[13] Jean Berstel and Maurice Mignotte. Deux Propriétés Décidables des Suites Récurrentes Linéaires. *Bulletin de la Societe mathematique de France*, 79:175–184, 1976.

[14] Jean Berstel and Christophe Reutenauer. *Noncommutative Rational Series with Applications*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010.

[15] Valérie Berthé, Toghrul Karimov, Joël Ouaknine, Mihir Vahanwala, and James Worrell. The Monadic Theory of Toric Words. arxiv.org/abs/2311.04895, 2023.

[16] Yuri Bilu, Florian Luca, Joris Nieuwveld, Joël Ouaknine, David Purser, and James Worrell. Skolem Meets Schanuel. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria*, volume 241 of *LIPIcs*, pages 20:1–20:15. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2022.

[17] P. Blanksby and H. Montgomery. Algebraic Integers Near the Unit Circle. *Acta Arithmetica*, 18(1):355–369, 1971.

[18] Achim Blumensath. Monadic Second-Order Model Theory. www.fi.muni.cz/~blumens/, 2023. [Online; accessed on 09 November 2023].

[19] Jonathan Borwein, Alf van der Poorten, Jeffrey Shallit, and Wadim Zudilin. *Neverending Fractions: An Introduction to Continued Fractions*. Australian Mathematical Society Lecture Series. Cambridge University Press, 2014.

[20] R. Bowen. *Equilibrium States and the Ergodic Theory of Axiom A Diffeomorphisms*, volume 470 of *Lecture Notes in Mathematics*. Springer-Verlag, 1975.

[21] J. R. Büchi. On a Decision Method in Restricted Second Order Arithmetic. In *The Collected Works of J. Richard Büchi*, pages 425–435. Springer New York, 1990.

[22] Jin-Yi Cai. Computing Jordan Normal Forms Exactly for Commuting Matrices in Polynomial Time. *International Journal of Foundations of Computer Science*, 05(03n04):293–302, 1994.

[23] Olivier Carton and Wolfgang Thomas. The Monadic Theory of Morphic Infinite Words and Generalizations. *Information and Computation*, 176(1):51–65, 2002.

[24] Yong-Gao Chen. The Best Quantitative Kronecker's Theorem. *Journal of the London Mathematical Society*, 61(3):691–705, 2000.

[25] Ventsislav Chonev, Joël Ouaknine, and James Worrell. The Polyhedron-Hitting Problem. SODA '15, page 940–956, USA, 2015. Society for Industrial and Applied Mathematics.

[26] Ventsislav Chonev, Joël Ouaknine, and James Worrell. On the Complexity of the Orbit Problem. *J. ACM*, 63(3), Jun 2016.

[27] Ventsislav Chonev, Joel Ouaknine, and James Worrell. On the Zeros of Exponential Polynomials. *J. ACM*, 70(4), aug 2023.

[28] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer Berlin Heidelberg, 1993.

[29] C. Conley. *Isolated Invariant Sets and the Morse Index*, volume 25 of *CBMS Regional Conference Series in Mathematics*. American Mathematical Society, 1978.

[30] James H. Davenport and Joos Heintz. Real Quantifier Elimination is Doubly Exponential. *Journal of Symbolic Computation*, 5(1):29–35, 1988.

[31] Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, Sadegh Soudjani, and James Worrell. The Pseudo-Skolem Problem is Decidable. In Filippo Bonchi and Simon J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science (MFCS 2021)*, volume 202 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 34:1–34:21, Dagstuhl, Germany, 2021. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[32] Julian D'Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamati, and James Worrell. The Pseudo-Reachability Problem for Diagonalisable Linear Dynamical Systems. In Stefan Szeider, Robert Ganian, and Alexandra Silva, editors, *47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022)*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 40:1–40:13, Dagstuhl, Germany, 2022. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[33] L. P. D. van den Dries. *Tame Topology and O-minimal Structures*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1998.

[34] Calvin C. Elgot and Michael O. Rabin. Decidability and Undecidability of Extensions of Second (First) Order Theory of (Generalized) Successor. *The Journal of Symbolic Logic*, 31(02):169–181, 1966.

[35] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*. American Mathematical Society, 2003.

[36] Jan-Hendrik Evertse. On Sums of S-Units and Linear Recurrences. *Compositio Mathematica*, 53(2):225–244, 1984.

[37] Nathanaël Fijalkow, Joël Ouaknine, Amaury Pouly, João Sousa-Pinto, and James Worrell. On the Decidability of Reachability in Linear Time-Invariant Systems. HSCC '19, page 77–86, New York, NY, USA, 2019. Association for Computing Machinery.

[38] Michael J. Fischer and Michael O. Rabin. Super-Exponential Complexity of Presburger Arithmetic. In Bob F. Caviness and Jeremy R. Johnson, editors,

Quantifier Elimination and Cylindrical Algebraic Decomposition, pages 122–135, Vienna, 1998. Springer Vienna.

[39] Steven M. Gonek and Hugh L. Montgomery. Kronecker's Approximation Theorem. *Indagationes Mathematicae*, 27(2):506–523, 2016. In Memoriam J.G. Van der Corput (1890–1975) Part 2.

[40] G. Hansel. A simple Proof of the Skolem-Mahler-Lech Theorem. In *Automata, Languages and Programming*, pages 244–249. Springer-Verlag.

[41] Joe Harris. *Algebraic Geometry*. Springer New York, 1992.

[42] Joos Heintz. Definability and Fast Quantifier Elimination in Algebraically Closed Fields. *Theoretical Computer Science*, 24(3):239–277, 1983.

[43] D. Ierardi. Quantifier Elimination in the Theory of an Algebraically-Closed Field. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 138–147, New York, NY, USA, 1989. Association for Computing Machinery.

[44] Ravindran Kannan and Richard J. Lipton. The Orbit Problem is Decidable. In *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing*, STOC '80, page 252–261, New York, NY, USA, 1980. Association for Computing Machinery.

[45] Toghrul Karimov, Edon Kelmendi, Joris Nieuwveld, Joël Ouaknine, and James Worrell. The Power of Positivity. In *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–11, 2023.

[46] Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. What's Decidable About Discrete Linear Dynamical Systems? In *Lecture Notes in Computer Science*, pages 21–38. Springer Nature Switzerland, 2022.

[47] Toghrul Karimov, Engel Lefaucheux, Joël Ouaknine, David Purser, Anton Varonka, Markus A. Whiteland, and James Worrell. What's Decidable about Linear Loops? *Proc. ACM Program. Lang.*, 6(POPL), Jan 2022.

[48] Toghrul Karimov, Joël Ouaknine, and James Worrell. On LTL Model Checking for Low-Dimensional Discrete Linear Dynamical Systems. In Javier Esparza and Daniel Kráĺ, editors, *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*, volume 170 of *Leibniz International*

Proceedings in Informatics (LIPIcs), pages 54:1–54:14, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[49] Manuel Kauers and Peter Paule. *The Concrete Tetrahedron*. Springer Vienna, 2011.

[50] George Kenison, Joris Nieuwveld, Joël Ouaknine, and James Worrell. Positivity Problems for Reversible Linear Recurrence Sequences. In Kousha Etessami, Uriel Feige, and Gabriele Puppis, editors, *50th International Colloquium on Automata, Languages, and Programming (ICALP 2023)*, volume 261 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 130:1–130:17, Dagstuhl, Germany, 2023. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[51] J.C. Lagarias and J.O. Shallit. Linear Fractional Transformations of Continued Fractions with Bounded Partial Quotients. *Journal de Théorie des Nombres de Bordeaux*, 9(2):267–279, 1997.

[52] Christer Lech. A Note on Recurring Series. *Arkiv för Matematik*, 2(5):417–421, Aug 1953.

[53] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[54] Florian Luca, Joël Ouaknine, and James Worrell. Algebraic Model Checking for Discrete Linear Dynamical Systems. In *Lecture Notes in Computer Science*, pages 3–15. Springer International Publishing, 2022.

[55] Angus Macintyre and Alex J. Wilkie. On the Decidability of the Real Exponential Field. In Piergiorgio Odifreddi, editor, *Kreiseliana. About and Around Georg Kreisel*, pages 441–467. A K Peters, 1996.

[56] Kurt Mahler. An Arithmetic Property of Taylor Coefficients of Rational Functions (1935). In Michael Baake, Yann Bugeaud, and Michael Coons, editors, *The Legacy of Kurt Mahler*, pages 437–448. EMS Press, 2019.

[57] Daniel A. Marcus. *Number Fields*. Springer International Publishing, 2018.

[58] D. Marker. *Model Theory: An Introduction*. Graduate Texts in Mathematics. Springer New York, 2002.

[59] D. W. Masser. *Linear Relations on Algebraic Groups*, page 248–262. Cambridge University Press, 1988.

[60] Robert McNaughton. Testing and Generating Infinite Sequences by a Finite Automaton. *Information and control*, 9(5):521–530, 1966.

[61] M. Mignotte, T. N. Shorey, and R. Tijdeman. The Distance Between Terms of an Algebraic Recurrence Sequence. *Journal für die reine und angewandte Mathematik*, 349, 1984.

[62] Maurice Mignotte. *Some Useful Bounds*, pages 259–263. Springer Vienna, Vienna, 1982.

[63] James S. Milne. Algebraic Number Theory (v3.08). www.jmilne.org/math/, 2020.

[64] An. Muchnik, A. Semenov, and M. Ushakov. Almost Periodic Sequences. *Theoretical Computer Science*, 304(1-3):1–33, 2003.

[65] Joël Ouaknine and James Worrell. Decision Problems for Linear Recurrence Sequences. In *Lecture Notes in Computer Science*, pages 21–28. Springer Berlin Heidelberg, 2012.

[66] Joël Ouaknine and James Worrell. Positivity Problems for Low-Order Linear Recurrence Sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, 12 2013.

[67] Joël Ouaknine and James Worrell. On the Positivity Problem for Simple Linear Recurrence Sequences. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, pages 318–329, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[68] Joël Ouaknine and James Worrell. Ultimate Positivity is Decidable for Simple Linear Recurrence Sequences. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Proceedings, Part II*, volume 8573 of *Lecture Notes in Computer Science*, pages 330–341. Springer, 2014.

[69] M. Queffélec. *Substitution Dynamical Systems–Spectral Analysis*, volume 1294 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, second edition, 2010.

[70] Alexander Rabinovich. On Decidability of Monadic Logic of Order Over the Naturals Extended by Monadic Predicates. *Information and Computation*, 205(6):870–889, 2007.

[71] G. Rauzy. Nombres Algébriques et Substitutions. *Bull. Soc. Math. France*, 110(2):147–178, 1982.

[72] James Renegar. On the Computational Complexity and Geometry of the First-Order Theory of the Reals. Part I: Introduction. Preliminaries. The Geometry of Semi-Algebraic Sets. The Decision Problem for the Existential Theory of the Reals. *Journal of symbolic computation*, 13(3):255–299, 1992.

[73] Raphael M Robinson. Restricted Set-Theoretical Definitions in Arithmetic. *Proceedings of the American Mathematical Society*, 9(2):238–242, 1958.

[74] Marie-Françoise Roy and Nicolai Vorobjov. Computing the Complexification of a Semi-Algebraic Set. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, ISSAC '96, page 26–34, New York, NY, USA, 1996. Association for Computing Machinery.

[75] A. L. Semënov. Logical Theories of One-Place Functions on the Set of Natural Numbers. *Mathematics of the USSR-Izvestiya*, 22(3):587–618, 1984.

[76] Th. Skolem. Einige Sätze über p-Adische Potenzreihen mit Anwendung auf Gewisse Exponentielle Gleichungen. *Mathematische Annalen*, 111(1):399–424, Dec 1935.

[77] B. A. Trahtenbrot. Finite Automata and the Logic of One-place Predicates. In Russian. *Siberian Mathematical Journal*, 3:103–131, 1962.

[78] N. K. Vereshchagin. Occurrence of Zero in a Linear Recursive Sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38(2):609–615, Aug 1985.

[79] Michel Waldschmidt. *Heights of Algebraic Numbers*, pages 65–114. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.

[80] A. J. Wilkie. 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*, 9(4):1051–1094, 1996.

[81] G. Wüstholz and A. Baker. Logarithmic Forms and Group Varieties. *Journal für die reine und angewandte Mathematik*, 442:19–62, 1993.

[82] Kunrui Yu. p-Adic Logarithmic Forms and Group Varieties II. *Acta Arithmetica*, 89(4):337–378, 1999.

[83] Richard Zippel. *Effective Polynomial Computation*. Springer US, 1993.