The Power of Positivity

Toghrul Karimov*, Edon Kelmendi†, Joris Nieuwveld*, Joël Ouaknine*, and James Worrell‡
*Max Planck Institute for Software Systems, Germany
{toghs, jnieuwve, joel}@mpi-sws.org
†Queen Mary University of London, UK
e.kelmendi@qmul.ac.uk
‡Department of Computer Science, University of Oxford, UK
jbw@cs.ox.ac.uk

2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS) | 979-8-3503-3587-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/LICS56636.2023.10175758

***Abstract*—The Positivity Problem for linear recurrence sequences over a ring R of real algebraic numbers is to determine, given an LRS $(u_n)_{n\in\mathbb{N}}$ over R, whether $u_n \geq 0$ for all n. It is known to be Turing-equivalent to the following reachability problem: given a linear dynamical system $(M, s) \in R^{d\times d} \times R^d$ and a halfspace $H \subseteq \mathbb{R}^d$, determine whether the orbit $(M^n s)_{n\in\mathbb{N}}$ ever enters H. The more general model-checking problem for LDS is to determine, given (M, s) and an ω-regular property φ over semialgebraic predicates $T_1, \ldots, T_\ell \subseteq \mathbb{R}^d$, whether the orbit of (M, s) satisfies φ.**

In this paper, we establish the following:

1) **The Positivity Problem for LRS over real algebraic numbers reduces to the Positivity Problem for LRS over the integers; and**
2) **The model-checking problem for LDS with diagonalisable M is decidable subject to a Positivity oracle for simple LRS over the integers.**

In other words, the full semialgebraic model-checking problem for diagonalisable linear dynamical systems is no harder than the Positivity Problem for simple integer linear recurrence sequences. This is in sharp contrast with the situation for arbitrary (not necessarily diagonalisable) LDS and arbitrary (not necessarily simple) integer LRS, for which no such correspondence is expected to hold.

***Index Terms*—Linear recurrence sequences, Positivity Problem, linear dynamical systems, model checking.**

I. Introduction

Dynamical systems are a fundamental modelling paradigm in many branches of science, and have been the subject of extensive research for many decades. A *real-algebraic discrete linear dynamical system (LDS)* in ambient space $\mathbb{R}^d$ is given by a square $d \times d$ matrix M with entries in $\mathbb{R} \cap \overline{\mathbb{Q}}$, together with a starting point $s \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$. The *orbit* of (M, s) is the infinite trajectory $(s, Ms, M^2 s, \ldots)$.

One of the most natural and fundamental computational questions concerning linear dynamical systems is the *Point-to-Point Reachability Problem*, also known as the *Kannan-Lipton Orbit Problem*: given a d-dimensional LDS (M, s) together with a point target $t \in (\mathbb{R} \cap \overline{\mathbb{Q}})^d$, does the orbit of the LDS ever hit the target? The decidability of this question was settled affirmatively in the 1980s in the seminal work of Kannan and Lipton [1], [2].

Interestingly, one of Kannan and Lipton's motivations was to propose a line of attack to the well-known *Skolem Problem*, which had itself been famously open since the 1930s (and remains so to this day). Phrased in the language of linear dynamical systems, the Skolem Problem asks whether it is decidable, given (M, s) as above, together with a $(d-1)$-dimensional subspace T of $\mathbb{R}^d$, to determine if the orbit of (M, s) ever hits T. Kannan and Lipton suggested that, in ambient space $\mathbb{R}^d$ of arbitrary dimension, the problem of hitting a low-dimensional subspace might be decidable. Indeed, this was eventually substantiated by Chonev *et al.* for linear subspaces of dimension at most 3 [3], [4].

If one replaces the linear-subspace target T by a full-dimensional halfspace target $H \subseteq \mathbb{R}^d$, one obtains a computational question equivalent to the well-known *Positivity Problem* for linear recurrence sequences, also famously open to this day, and to which we shall return shortly.

Subsequent research focussed on the decidability of hitting targets of increasing complexity, such as polytopes [5]–[7] and semialgebraic sets [8], [9]. In recent years, motivated in part by verification questions for stochastic systems and linear while loops, researchers have begun investigating more sophisticated decision problems for linear dynamical systems, such as *model checking*. In this setting, let us assume we are given a finite partition $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ of $\mathbb{R}^d$. Given a d-dimensional LDS (M, s), the *characteristic word* of the orbit of (M, s) relative to partition $\mathcal{T}$ is the infinite word $\alpha \in \mathcal{T}^\omega$ such that, for each $n \in \mathbb{N}$, the n-th element of the orbit of (M, s) lies in $\alpha(n)$: $M^n s \in \alpha(n)$. A *specification* over $\mathcal{T}$ is a (possibly infinite) collection of infinite words $\varphi \subseteq \mathcal{T}^\omega$, and we say that the LDS (M, s) *satisfies* the specification φ if the characteristic word of its orbit belongs to the specification: $\alpha \in \varphi$.

The elements of the partition $\mathcal{T}$ are known as *predicates*. Instances of the model-checking problem are characterised by: (i) the class of dynamical systems under consideration, (ii) the kinds of predicates allowed, and (iii) the formalism used to describe the specification. For example, the paper [10] studies LTL model checking of low-dimensional linear dynamical systems with semialgebraic predicates,[1] whereas [11] focusses on semialgebraic model checking for diagonalisable linear dynamical systems in arbitrary dimension against prefix-

[1]Semialgebraic predicates correspond to Boolean combinations of polynomial equalities and inequalities.

979-8-3503-3587-3/23/$31.00 ©2023 IEEE

independent MSO properties.[2] The paper [12], on the other hand, investigates semialgebraic MSO model checking of linear dynamical systems in which the dimensions of predicates obey particular constraints. Other relevant papers include [13], [14]; we refer the reader to [15] for a recent survey of the state of the art on model checking for linear dynamical systems.

It is worth recalling once more that, in general, the model-checking problem for linear dynamical systems is *not* known to be decidable, since longstanding open reachability questions, such as the Skolem and Positivity Problems, can straightforwardly be phrased as model-checking queries (with either polytopic or semialgebraic predicates). This in turn leads to the following natural question: ***What could be achieved assuming the existence of Skolem or Positivity oracles?*** Or, in other words: ***Exactly how powerful are such oracles?***

The question is not entirely academic; aside from sheer intellectual curiosity, recent work has established, for example, that Skolem oracles for simple linear recurrence sequences could be designed, assuming certain classical conjectures in number theory [16].[3] In turn, this enabled the authors of [16] to show that full algebraic MSO model checking[4] of diagonalisable linear dynamical systems is decidable, subject to the same number-theoretic assumptions, and to exhibit a corresponding decision procedure for this task.

Linear recurrence sequences (LRS), such as the Fibonacci numbers, are properly introduced and defined in the next section; the present brief discussion will therefore remain relatively informal. For the purposes of this paper, we wish to consider classes of LRS defined over both real algebraic numbers and integers; and distinguish between *simple* LRS (whose characteristic polynomials have no repeated roots) and arbitrary ones. The *Skolem Problem* for an LRS $(u_n)_{n\in\mathbb{N}}$ asks whether it has a zero term, i.e., whether there exists $n \in \mathbb{N}$ such that $u_n = 0$, whereas the *Positivity Problem* asks whether all terms of the sequence are non-negative. As mentioned earlier, whether the Skolem or Positivity Problems are decidable are longstanding open questions [17]–[28]; this remains so even when restricting to simple LRS. It is folklore that the Skolem Problem is 'easier' than the Positivity Problem: the former reduces to the latter, and the same again holds when restricting to simple LRS. It is also known that the Skolem Problem over real-algebraic LRS reduces to its counterpart over integer sequences, and likewise when restricting to simple LRS [16]. Finally, the paper [26] shows, by way of hardness, that establishing decidability for the Positivity Problem over integer LRS would necessarily entail major breakthroughs in analytic number theory, more precisely in the field of Diophantine approximation of transcendental numbers. The same is however not known (or believed) to hold when restricting to *simple* LRS. We shall return to these matters in Section VI.

We are now in a position to state the major contributions of this paper. We establish the following:

1) The Positivity Problem for LRS over real algebraic numbers is Turing-equivalent to the Positivity Problem for LRS over the integers; and likewise when restricting to simple LRS.
2) The semialgebraic MSO model-checking problem for real-algebraic diagonalisable LDS is decidable subject to a Positivity oracle for simple LRS over the integers.

In other words, the full semialgebraic MSO model-checking problem for diagonalisable linear dynamical systems is no harder than the Positivity Problem for simple integer linear recurrence sequences. As we argue in Section VI, this appears to be in sharp contrast with the situation for non-diagonalisable LDS (and non-simple LRS), for which the existence of a Positivity oracle does not seem to have a bearing on the solvability of various basic instances of LDS model checking.

II. Preliminaries

A. Linear recurrence sequences

A *linear recurrence sequence* (LRS) of order $d > 0$ over a ring $R \subseteq \overline{\mathbb{Q}}$ is given by a recurrence relation

$$u_{n+d} = a_1 u_{n+d-1} + \ldots + a_d u_n$$

and initial values $u_0, \ldots, u_{d-1} \in R$, where $a_i \in R$ for $1 \leq i \leq d$. We give the most important properties of LRS and refer the reader to the book [23] by Everest *et al.* for a comprehensive introduction. The *characteristic polynomial* $p \in R[x]$ of such a sequence is $p(x) = x^d - \sum_{i=1}^{d} a_i x^{d-i}$. Each LRS that is not identically zero has a unique solution (up to reordering of summands) in the *exponential polynomial form* given by

$$u_n = \sum_{k=1}^{m} p_k(n)\Lambda_k^n \tag{1}$$

where each Λ_i is a root of the characteristic polynomial of $(u_n)_{n\in\mathbb{N}}$, $\Lambda_i \neq \Lambda_j$ for $i \neq j$, and for all k, $\Lambda_k \neq 0$ and $p_k \in \overline{\mathbb{Q}}[z]$ is not identically zero. The value Λ_i is called a *dominant root of* $(u_n)_{n\in\mathbb{N}}$ if $|\Lambda_i| \geq |\Lambda_j|$ for all j, and the *spectral radius* ρ of $(u_n)_{n\in\mathbb{N}}$ is equal to $|\Lambda_i|$ for a dominant root Λ_i.

An LRS given by Equation (1) is

- *simple* (or *diagonalisable*) if $p_k(n)$ is constant for all k,
- *non-degenerate* if Λ_i/Λ_j is not a root of unity for $i \neq j$.
- *positive* if $u_n \in \mathbb{R}_{\geq 0}$ for all $n \in \mathbb{N}$, and
- *ultimately positive* if $u_n \in \mathbb{R}_{\geq 0}$ for sufficiently large n.

If $(u_n)_{n\in\mathbb{N}}$ is degenerate, then there exists a computable integer L such the subsequences $(u_{nL+r})_{n\in\mathbb{N}}$ for $0 \leq r < L$ are all non-degenerate.

The Skolem-Mahler-Lech theorem states that the set $\mathcal{Z}$ of zeroes of a non-degenerate LRS is finite. Unfortunately, all known proofs of the theorem are non-constructive. In fact, the problem of computing $\mathcal{Z}$ is equivalent to the Skolem Problem.

[2]Monadic Second-Order Logic (MSO) is a highly expressive specification formalism that subsumes the vast majority of temporal logics employed in the field of automated verification, such as Linear Temporal Logic (LTL). "Prefix independence" is a quality of properties that are *asymptotic* in nature.

[3]In fact, such oracles have been implemented as algorithms and can be experimented with; see https://skolem.mpi-sws.org/.

[4]*Algebraic* model checking refers to the setting in which predicates correspond to arbitrary Boolean combinations of *algebraic* sets, i.e., sets defined by polynomial equalities.

A consequence of the Cayley-Hamilton theorem is that

$$u_n = c^\top M^n s \tag{2}$$

where $c \in R^d$, $M \in R^{d\times d}$ and $s \in R^d$, defines an LRS over R. The characteristic polynomial of $(u_n)_{n\in\mathbb{N}}$ is exactly $\det(xI - M)$, which is the characteristic polynomial of M. Conversely, every LRS $(u_n)_{n\in\mathbb{N}}$ over R can be written in the form of Equation (2). The matrix M is then called the *companion matrix* of the sequence.

Let $u_n = \sum_{k=1}^{m} p_k(n)\Lambda_k^n$ define a real-valued LRS, i.e. $\overline{u_n} = u_n$ for all $n \in \mathbb{N}$. Then $u_n = \sum_{k=1}^{m} \overline{p_k(n)}\,\overline{\Lambda_k}^n$. By the uniqueness of the exponential polynomial representation, it follows that for each k there exists k' such that $\Lambda_{k'} = \overline{\Lambda_k}$ and $p_{k'}(n) = \overline{p_k(n)}$. That is, the summands of the exponential polynomial solution of a real-valued LRS are closed under complex conjugation.

B. Algebraic numbers

A complex number α is *algebraic* if it is a root of a polynomial with rational coefficients. For such α there exists a unique irreducible polynomial $p(x) = \sum_{i=0}^{d} a_i x^{d-i} \in \mathbb{Q}[x]$ of the smallest degree, called the *minimal polynomial* of α, such that $a_0 = 1$ and $p(\alpha) = 0$. The *degree* $\deg(\alpha)$ of α is equal to d. The polynomial p has d distinct roots $\alpha_1, \ldots, \alpha_d$ called the *Galois conjugates of* α. Let $b \in \mathbb{N}$ be such that $ba_i \in \mathbb{Z}$ for all $1 \le i \le d$ and $\gcd(ba_0, \ldots, ba_d) = 1$. The *height* of α is defined as $H(\alpha) \coloneqq \max_{0\le i\le d} |ba_i|$.

The set of all algebraic numbers, denoted $\overline{\mathbb{Q}}$, forms a field. An *algebraic integer* is an algebraic number whose minimal polynomial has integer coefficients. Algebraic integers form a ring, denoted $\mathcal{O}$. Each algebraic number α can be written in the form β/m, where $\beta \in \mathcal{O}$ and $m \in \mathbb{Z}$.

By a *number field* we mean an algebraic extension $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_m) \subset \overline{\mathbb{Q}}$ of $\mathbb{Q}$, where $\alpha_1, \ldots, \alpha_m$ are algebraic numbers. We write $[\mathbb{K} : \mathbb{Q}]$ for the degree of the field extension $\mathbb{K}/\mathbb{Q}$, which is equal to the dimension of $\mathbb{K}$ as a vector space over $\mathbb{Q}$. For a number field $\mathbb{K}$, $D \coloneqq [\mathbb{K} : \mathbb{Q}]$ is always finite, and there exist exactly D embeddings $\sigma_1, \ldots, \sigma_D : \mathbb{K} \hookrightarrow \mathbb{C}$. A number $\alpha \in \mathbb{K}$ is rational if and only if it is fixed by every σ_i. Hence an LRS given by Equation (1) is rational if and only if the summands are closed under taking Galois conjugates: for every $1 \le k \le m$ and $1 \le i \le D$, there exists $1 \le k_i \le m$ such that $p_{k_i}(n) = \sigma_i(p_k(n))$ and $\Lambda_{k_i} = \sigma_i(\Lambda_k)$.

We denote by $\mathbb{T}$ the set $\{z \in \mathbb{C} : |z| = 1\}$. When talking about a semialgebraic subset of $\mathbb{C}^d$, we identify $\mathbb{C}$ with $\mathbb{R}^2$ (and hence $\mathbb{C}^d$ with $\mathbb{R}^{2d}$) in the standard way.

III. A lower bound on the growth rate of LRS

In this section we describe a lower bound on the magnitude of the terms of an LRS over algebraic numbers (Theorem 2), originally due to Everest, van der Poorten, Shparlinski and Ward. This result, alongside the Skolem-Mahler-Lech theorem, is one of the cornerstones of the theory of linear recurrence sequences. For example, a weaker version of Theorem 2 is the most crucial ingredient in the proof of [29] that Ultimate Positivity is decidable for diagonalisable LRS over $\mathbb{R}\cap\overline{\mathbb{Q}}$. The statement of Theorem 2 appears in [23][5], but to the best of our knowledge, no written proof has been published. We give a proof based on Theorem 1 of Evertse on the sums of S-units.[6]

We begin by introducing the necessary mathematical concepts. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}_{\ge 0}$ that satisfies the following properties:

1) $|\alpha| = 0$ if and only if $\alpha = 0$;
2) $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in K$;
3) $|\alpha| + |\beta| \ge |\alpha + \beta|$ for all $\alpha, \beta \in K$.

An absolute value is called *non-archimedean* if, in addition, $|\alpha + \beta| \ge \max\{|\alpha|, |\beta|\}$ for all $\alpha, \beta \in K$. For example, on $K = \mathbb{Q}$, we have the usual (archimedean) absolute value (denoted by $|\cdot|$ or $|\cdot|_\infty$) as well as the p-adic absolute value $|\cdot|_p$ for each prime $p \in \mathbb{N}$, defined as $|a/b|_p = (1/p)^{\mathrm{ord}_p(a)-\mathrm{ord}_p(b)}$. Here $\mathrm{ord}_p(x)$ is equal to the largest $k \in \mathbb{N}$ such that p^k divides x. See [30] for a detailed discussion of absolute values on $\mathbb{Q}$. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are considered *equivalent* if there exists real $r > 0$ such that $|x|_1 = |x|_2^r$ for all $x \in K$. By Ostrowski's theorem, every non-trivial absolute value on $\mathbb{Q}$ (i.e. an absolute value that is not equal to 1 everywhere on $\mathbb{Q} \setminus \{0\}$) is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for a prime p. Finally, the product rule for absolute values on $\mathbb{Q}$ reads

$$\prod_{p\in\mathcal{P}} |\alpha|_p = 1 \tag{3}$$

where $\alpha \ne 0$ and $\mathcal{P} = \{p \in \mathbb{N} : p \text{ is prime}\} \cup \{\infty\}$.

To prove Theorem 2, we will need to generalise the notions above to arbitrary number fields. We refer the reader to the lecture notes on algebraic number theory by James Milne [31] for a detailed introduction to absolute values on number fields.

Let $\mathbb{K}$ be a number field and $\mathcal{O}_\mathbb{K} = \mathcal{O} \cap \mathbb{K}$ be the ring of its algebraic integers. By the Kummer-Dedekind theorem [32, Theorem 16], each non-zero ideal of $\mathcal{O}_\mathbb{K}$ has a unique factorisation (up to reordering of factors) in prime ideals. Let $N(\mathfrak{p})$ denote the *norm* of the ideal $\mathfrak{p}$, defined as the cardinality of the finite field $\mathcal{O}_\mathbb{K}/\mathfrak{p}$. Denote by (α) the ideal generated by an algebraic integer α in $\mathcal{O}_\mathbb{K}$. Given a prime ideal $\mathfrak{p}$ and $\alpha \in \mathcal{O}_\mathbb{K}$ with the prime factorisation $(\alpha) = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_m^{k_m}$, we define the *normalised* $\mathfrak{p}$*-adic absolute value* of α as

$$|\alpha|_\mathfrak{p} = \begin{cases} (1/N(\mathfrak{p}))^{k_i} \text{ if } \mathfrak{p} = \mathfrak{p}_i, \\ 1 \text{ otherwise.} \end{cases}$$

We can extend $|\cdot|_\mathfrak{p}$ to the whole of $\mathbb{K}$ by setting $|\alpha|_\mathfrak{p} = |\beta|_\mathfrak{p}/|m|_\mathfrak{p}$ where $\beta \in \mathcal{O}_\mathbb{K}$ and $m \in \mathbb{Z}$ are such that $\alpha = \beta/m$.

The definition above provides all the possible non-archimedean absolute values on $\mathbb{K}$ up to equivalence. We next describe the archimedean absolute values. Let $D \coloneqq [\mathbb{K} : \mathbb{Q}]$ and denote by $\sigma_1, \ldots, \sigma_D$ all the distinct embeddings of $\mathbb{K}$

[5]Unfortunately, the version of the bound stated in the book is slightly inaccurate, as it does not hold for LRS of spectral radius at most 1.

[6]We would like to thank Jan-Hendrik Evertse for the very helpful personal communication.

into $\mathbb{C}$. For each such embedding σ, we define the *normalised absolute value*

$$|\alpha|_\sigma = \begin{cases} |\sigma(\alpha)| \text{ if } \sigma(\mathbb{K}) \subseteq \mathbb{R}, \\ |\sigma(\alpha)|^2 \text{ otherwise.} \end{cases}$$

We are now ready to give the generalisation of Equation (3) to an arbitrary number field $\mathbb{K}$. A *place* on $\mathbb{K}$ is an equivalence class of absolute values on $\mathbb{K}$. For each prime ideal $\mathfrak{p}$, we denote the corresponding place by $v_\mathfrak{p}$ and refer to the places obtained in this way as *finite*. For each embedding σ, we define a place v_σ and refer to the resulting places as *infinite*. For a place v, let

$$|\cdot|_v = \begin{cases} |\cdot|_\mathfrak{p} \text{ if } v = v_\mathfrak{p}, \\ |\cdot|_\sigma \text{ if } v = v_\sigma. \end{cases}$$

Denote the set of all places of $\mathbb{K}$ by $\mathcal{P}$, and the set of all infinite places by $\mathcal{P}^\infty$. The product rule reads

$$\prod_{v \in \mathcal{P}} |\alpha|_v = 1$$

for all $\alpha \neq 0$.

We are now in a position to state the aforementioned theorem of Evertse. For a vector $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{K}^m$, define

$$||\mathbf{x}|| = \max_{\substack{1 \leq k \leq m \\ 1 \leq j \leq D}} |\sigma_j(x_k)|.$$

Theorem 1 (Theorem 2, Evertse, [33])**.** *Let $S \subset \mathcal{P}$ be a finite set of places on a number field $\mathbb{K}$ enclosing $\mathcal{P}^\infty$, $T \subseteq S$ be non-empty, and $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{K}^m$. Suppose for every non-empty $I \subseteq \{1, \ldots, m\}$, $\Sigma_{k \in I} x_k \neq 0$. For every $\epsilon > 0$ there exists $C > 0$, depending only on $\mathbb{K}, S, T, \epsilon$ and m, such that*

$$\left(\prod_{k=1}^{m} \prod_{v \in S} |x_k|_v \right) \prod_{v \in T} |x_1 + \ldots + x_k|_v \geq C \left(\prod_{v \in T} \max_{1 \leq k \leq m} |x_k|_v \right) ||\mathbf{x}||^{-\epsilon}.$$

We apply this theorem to obtain the following main result of this section.

Theorem 2. *Let $u_n = \sum_{k=1}^{m} p_k(n) \lambda_k^n$ be a non-degenerate LRS with $\rho = |\lambda_1| \geq \cdots \geq |\lambda_m| > 0$ and $p_k \in \overline{\mathbb{Q}}[z]$, $p_k \neq 0$ for all k. For every $0 < r < \rho$, there exists $N \in \mathbb{N}$ such that*

$$|u_n| > r^n$$

for all $n > N$.

Proof. We first argue that it suffices to prove the theorem assuming $\lambda_1, \ldots, \lambda_m$, as well as all the coefficients of $p_1, \ldots, p_m$, are algebraic integers. Since each algebraic number can be written as a ratio of an algebraic integer and a rational integer, there exist non-zero $A, B \in \mathbb{N}$ such that for all k, $B\lambda_k$ and the coefficients of the polynomial $A \cdot p_k$ are algebraic integers. Consider $v_n = AB^n u_n$, and suppose for each $0 < \mu < B\rho$, there exists N_μ such that for all $n > N_\mu$, $|v_n| > \mu^n$. Given $0 < r < \rho$, choose $\mu \in (Br, B\rho)$ and observe that $\mu/B > r$. Let N be sufficiently large that for all $n > N$, $(\mu/B)^n > Ar^n$. Then for all $n > \max\{N, N_\mu\}$,

$$|u_n| = |v_n|/(AB^n) \geq \frac{\mu^n}{AB^n} \geq r^n.$$

We now prove the theorem under the assumption above. Let $\mathbb{K}$ be a non-real number field containing $\lambda_1, \ldots, \lambda_m$, as well as the coefficients of $p_1, \ldots, p_m$, and $D = [\mathbb{K} : \mathbb{Q}]$. Let $\mathcal{P}$ denote the set of all places of $\mathbb{K}$ and $\mathcal{P}_\infty$ denote the set of all infinite places. Choose S to be the smallest set enclosing $\mathcal{P}_\infty$ and containing $v_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ that appears in the prime factorisation of (λ_k) for some k. Observe that $|\lambda_k^n|_v = 1$ for all $v \notin S$ by the choice of S, and, because $p_k(n)$ is an algebraic integer, $|p_k(n)|_v \leq 1$ for all $v \notin \mathcal{P}^\infty$. Choose $T = \{v_\sigma\}$ where $\sigma(\alpha) = \alpha$ is the identity map. Because $\mathbb{K} \not\subseteq \mathbb{R}$, $|z|_{v_\sigma} = |z|^2$ for all $z \in \mathbb{K}$. Let $||u_n|| = ||(p_1(n)\lambda_1^n, \ldots, p_m(n)\lambda_m^n)||$ and observe that $||u_n|| \geq \max_{1 \leq k \leq m} |p_k(n)\lambda_k^n|$.

To show the existence of the desired N for a given r, let $N_1 \in \mathbb{N}$ and $c \in \mathbb{Q}$ be such that for all $n > N_1$, no (non-empty) sub-sum of $\sum_{k=1}^{m} p_k(n)\lambda_k^n$ is zero and $|p_k(n)| > c$ for all k. To see that such N_1 exists, observe that every such sub-sum is itself a non-degenerate LRS, and invoke the Skolem-Mahler-Lech theorem. Further observe that for $n > N_1$, $||u_n|| \geq c\rho^n$. Next, let $\epsilon > 0$ be such that $\rho^{1-\epsilon/2} > r$. Applying Theorem 1 with S, T, ϵ as described above to the sum $\sum_{k=1}^{m} p_k(n)\lambda_k^n$, let C be such that

$$\left(\prod_{k=1}^{n} \prod_{v \in S} |p_k(n)\lambda_k^n|_v \right) |u_n|^2 \geq C \max_{1 \leq k \leq m} |p_k(n)\lambda_k^n|^2 ||u_n||^{-\epsilon}$$

for all $n > N_1$. Observe that

$$\prod_{k=1}^{n} \prod_{v \in S} |p_k(n)\lambda_k^n|_v = \underbrace{\prod_{k=1}^{n} \prod_{v \in S} |\lambda_k^n|_v}_{a_n} \cdot \underbrace{\prod_{k=1}^{n} \prod_{v \in S} |p_k(n)|_v}_{b_n}.$$

Since $\prod_{v \in \mathcal{P}} |\lambda_k^n|_v = 1$ by the product rule and $|\lambda_k^n|_v = 1$ for all $v \notin S$ as discussed above, $a_n = 1$ for all n. Since $|p_k(n)|_v \leq 1$ for every finite place v,

$$\begin{aligned} \prod_{v \in S} |p_k(n)|_v &\leq \prod_{v \in \mathcal{P}^\infty} |p_k(n)|_v \\ &= \prod_{j=1}^{D} |\sigma_j(p_k(n))|^2 \\ &\leq H(p_k(n))^{2D} \end{aligned}$$

for all $1 \leq k \leq m$ and $n \in \mathbb{N}$. Since the height $H(p_k(n))$ is at most polynomial in n (see, for example, [34, Chapter 3.2]), there exists a polynomial q such that $b_n < q(n)$. Combining all of the inequalities above we obtain

$$q(n)|u_n|^2 \geq C(c\rho^n)^2(c\rho^n)^{-\epsilon} = C(c\rho^n)^{2-\epsilon}$$

for $n > N_1$. By taking square roots,

$$|u_n| \geq \sqrt{\frac{C}{q(n)}} c^{1-\epsilon/2} \rho^{(1-\epsilon/2)n}.$$

Recalling that $\rho^{1-\epsilon/2} > r$, it remains to choose $N > N_1$ such that $\sqrt{C/q(n)}c^{1-\epsilon/2}\rho^{(1-\epsilon/2)n} > r^n$ for all $n > N$. □

The constant C in the statement of Theorem 1 and hence the value N above are non-constructive. Nevertheless, such N can be effectively computed using a Positivity oracle, which can be taken to be for integer LRS by the results of Section IV.

Theorem 3. *Let u_n and ρ be as in the statement of Theorem 2. Given a Positivity oracle for real algebraic LRS, for every $0 < r < \rho$ we can effectively compute N such that $|u_n| > r^n$ for all $n > N$.*

Proof. Let $\mu \in (r, \rho) \cap \mathbb{Q}$ and consider the sequence $v_n = |u_n|^2 - \mu^{2n}$. Since $|u_n|^2 = u_n\overline{u_n}$, the sequence $(v_n)_{n\in\mathbb{N}}$ is an LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$. Applying Theorem 2 to $(|u_n|^2)_{n\in\mathbb{N}}$, there exists N such that $|u_n|^2 > \mu^{2n}$ for all $n \geq N$ and hence the sequence $v_n^{(N)} = (v_{n+N})_{n\in\mathbb{N}}$ is positive. Such N can be computed by repeatedly invoking the Positivity oracle on suffixes of v_n. It remains to observe that positivity of $v^{(N)}$ implies that $|u_n| > |r^n|$ for all $n > N$. □

IV. From algebraic to rational positivity

In this section, we will show that a Positivity oracle for rational LRS is sufficient to decide the Positivity Problem for real algebraic LRS. As a rational LRS can be transformed into an integer LRS by a simple scaling that preserves the sign of u_n, it follows that a Positivity oracle for integer LRS is equally powerful.

Theorem 4. *Given a Positivity oracle for LRS over $\mathbb{Q}$, the Positivity Problem is decidable for LRS over $\mathbb{R} \cap \overline{\mathbb{Q}}$. Moreover, if the input LRS is simple then a Positivity oracle for simple rational LRS suffices.*

To sketch an outline of the proof of this theorem, let $(u_n)_{n\in\mathbb{N}}$ be a real algebraic LRS. We construct three new LRS $(v_n)_{n\in\mathbb{N}}$, $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$. Here, $(v_n)_{n\in\mathbb{N}}$ is real algebraic and positive if and only if u_n is positive, and $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$ are rational LRS such that (i) $|v_n - v_n^+|$ and $|v_n - v_n^-|$ grow much slower than v_n itself, and (ii) v_n is "squeezed" between v_n^- and v_n^+. That is, for sufficiently large n (for which a threshold is effectively computable), $v_n^- \leq v_n \leq v_n^+$. As the terms of v_n grow according to Theorem 2, we can conclude that understanding positivity of suffixes of $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$ is sufficient to understand positivity of $(v_n)_{n\in\mathbb{N}}$ and therefore, $(u_n)_{n\in\mathbb{N}}$.

To prove this theorem, two technical lemmas are required. The first shows that the powers of an algebraic number form a $\overline{\mathbb{Q}}$-linear combination of rational LRS.

Lemma 5. *Let λ be an algebraic integer with the minimal polynomial $p(x) = \sum_{i=0}^{d} a_i x^{d-i}$, where $a_0 = 1$. One can construct simple rational LRS $u_n^{(0)}, \ldots, u_n^{(d-1)}$ such that for all $n \geq 0$,*

$$\lambda^n = \sum_{i=0}^{d-1} \lambda^i u_n^{(i)}.$$

Proof. Let $L = (1, \lambda, \ldots, \lambda^{d-1}) \in \overline{\mathbb{Q}}^d$. For $c \in \mathbb{Z}[\lambda]$ with $c(\lambda) = c_{d-1}\lambda^{d-1} + \cdots + c_0$, we have $c(\lambda) = L^\top M\mathbf{c}$, where $\mathbf{c} = (c_0, \ldots, c_{d-1}) \in \mathbb{Z}^d$ and

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}.$$

is the companion matrix of p. Let e_i denote ith standard unit vector. If $\lambda^k = c_0 + \cdots + c_{d-1}\lambda^{d-1}$, then

$$\lambda^{k+1} = -c_{d-1}a_0 + (c_0 - c_{d-1}a_1)\lambda + \cdots + (c_{d-2} - c_{d-1}a_{d-1})\lambda^{d-1},$$

and hence by induction it can be shown that the d coefficients of $1, \ldots, \lambda^{d-1}$ in the expression for λ^n are exactly $e_1^T M^n e_1, \ldots, e_d^T M^n e_1$, respectively. For $1 \leq i \leq d$, $(u_n^{(i)})_{n\in\mathbb{N}} := (e_i^T M^n e_1)_{n\in\mathbb{N}}$ is a rational LRS that is simple, as M has no repeated eigenvalues: the eigenvalues of M are exactly the roots of p, which is a minimal polynomial with d distinct roots. □

The second technical lemma shows that every algebraic number can be approached exponentially fast by the quotient of two rational LRS.

Lemma 6. *Let α be a real algebraic number and $0 < r < 1$. One can construct simple, ultimately positive rational LRS $(c_n)_{n\in\mathbb{N}}$ and $(d_n)_{n\in\mathbb{N}}$, as well as $b \in \mathbb{Q}_{>0}$ and $N \in \mathbb{N}$, such that $(d_n)_{n\in\mathbb{N}}$ has exactly one dominant root, and for all $n \geq N$,*

$$\left|\alpha - \frac{c_n}{d_n}\right| < b \cdot r^n.$$

Proof. If $\alpha \in \mathbb{Q}$, choosing $c_n = \alpha$, $d_n = 1$, and $b = 1$ suffices. Hence assume α is irrational and let $\alpha_1, \ldots, \alpha_k$ denote the Galois conjugates of α with $\alpha_1 = \alpha$.

First, we will find $p, q \in \mathbb{Z}$ and $s \in \{-1, 1\}$ such that, writing $f(x) = \frac{s}{x - p/q}$, $f(\alpha) \in \mathbb{R}_{>0}$ and $f(\alpha) > |f(\alpha_i)|$ for $i = 2, \ldots, k$.

Let $d = \min(|\alpha - \alpha_2|, \ldots, |\alpha - \alpha_k|)$ and $0 < \epsilon < d/2$. As $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists effectively computable $\frac{p}{q} \in \mathbb{Q}$ such that $|\alpha - \frac{p}{q}| < \epsilon$. Let $f_1(x) = x - \frac{p}{q}$. Then, for $i = 2, \ldots, k$,

$$|f_1(\alpha_i)| = \left|\alpha_i - \frac{p}{q}\right| \geq |\alpha_i - \alpha_1| + \left|\alpha_1 - \frac{p}{q}\right| \geq d - \epsilon > \epsilon,$$

which is larger than $f(\alpha)$. Thus, $f_1(\alpha)$ is closer to the origin than $f_1(\alpha_i)$, but $f_1(\alpha) \neq 0$ as α is irrational.

Let $s = \operatorname{sgn}(\alpha - p/q)$ and $f(x) = \frac{s}{f_1(x)}$. For all $i = 2, \ldots, k$, $|f(\alpha)| > |f(\alpha_i)|$, and by the choice of s, $f(\alpha) > 0$. Therefore, f has the desired properties stated above.

Define the LRS $(c_n)_{n\in\mathbb{N}}$ and $(d_n)_{n\in\mathbb{N}}$ as follows:

$$c_n = \sum_{i=1}^{k} \alpha_i f(\alpha_i)^n \quad \text{and} \quad d_n = \sum_{i=1}^{k} f(\alpha_i)^n.$$

As both c_n and d_n are closed under Galois automorphisms and $f(x) \in \mathbb{Q}(x)$, we have that $(c_n)_{n\in\mathbb{N}}$ and $(d_n)_{n\in\mathbb{N}}$ are

simple rational linear recurrence sequences. It is easily seen that $(d_n)_{n\in\mathbb{N}}$ is ultimately strictly positive and has exactly one dominant root.

Let $b_1 = \sum_{i=2}^{k} |\alpha - \alpha_i|$, $r_1 = \max_{i=2}^{k} |f(\alpha_i)|$. Then $r_1 < f(\alpha)$, and we can compute N as the smallest integer n such that $(k-1)\left(\frac{f(\alpha)}{r_1}\right)^n > 2$. Recall that for $x \geq 2$, $1/(x-1) \leq 2/x$. Therefore, for all $n \geq N$,

$$\begin{aligned}\left|\alpha - \frac{c_n}{d_n}\right| &= \left|\frac{\sum_{i=1}^{k}(\alpha_1-\alpha_i)f(\alpha_i)^n}{\sum_{i=1}^{k} f(\alpha_i)^n}\right| \\ &= \left|\frac{\sum_{i=2}^{k}(\alpha-\alpha_i)f(\alpha_i)^n}{f(\alpha)^n + \sum_{i=2}^{k} f(\alpha_i)^n}\right| \\ &\leq \left|\frac{b_1 r_1^n}{f(\alpha)^n - (k-1)r_1^n}\right| \\ &= b_1(k-1)\left|\frac{1}{(k-1)\left(\frac{f(\alpha)}{r_1}\right)^n - 1}\right| \\ &\leq b_1(k-1)\left|\frac{2}{k-1}\left(\frac{r_1}{f(\alpha)}\right)^n\right| = 2b_1\left(\frac{r_1}{f(\alpha)}\right)^n.\end{aligned}$$

It remains to choose for b a rational number larger than $2b_1$, and let $\ell \geq 1$ be a number such that $r_1^\ell < r$. Then, choosing the LRS $(c_{\ell n})_{n\in\mathbb{N}}$ and $(d_{\ell n})_{n\in\mathbb{N}}$ gives that

$$\left|\alpha - \frac{c_{\ell n}}{d_{\ell n}}\right| < b \cdot r^n.$$

and so the premise is satisfied. □

Proof of Theorem 4. Let $(u_n)_{n\in\mathbb{N}}$ be an LRS over $\mathbb{R}\cap\overline{\mathbb{Q}}$ with the exponential polynomial solution $\sum_{k=1}^{m} p_k(n)\Lambda_i^n$. By considering non-degenerate subsequences if necessary, without loss of generality, we can assume that $(u_n)_{n\in\mathbb{N}}$ is non-degenerate. Moreover, as in the proof of Theorem 2, by scaling the LRS if necessary we can assume that Λ_k is an algebraic integer for all k. By the discussion in Section II-A, for each i there exists j such that $\Lambda_j = \overline{\Lambda_i}$ and $p_j(n) = \overline{p_i(n)}$. Therefore, we can rewrite u_n as

$$u_n = \sum_{k\in\mathcal{R}} n^{\sigma(k)}\gamma_k\Lambda_k^n + \sum_{k'\in\mathcal{C}} n^{\sigma(k')}(\gamma_{k'}\Lambda_{k'}^n + \overline{\gamma_{k'}}\,\overline{\Lambda_{k'}}^n)$$

where $\Lambda_k, \gamma_k \in \mathcal{R}$ for $k \in \mathcal{R}$. Next, for $k' \in \mathcal{C}$, applying Lemma 5, to $u_n^{(k)} = \Lambda_k^n$ for $k \in \mathcal{R}$, we obtain that $u_n = \sum_{i=0}^{d-1} \Lambda_k^i v_n^{(i)}$ for simple rational LRS $v_n^{(0)}, \ldots, v_n^{(d-1)}$ where d is the degree of Λ_k. Next, observe that $\Lambda_{k'}$ and $\overline{\Lambda_{k'}}$ have the same minimal polynomial. Hence applying Lemma 5, we obtain that for each k' there exist simple rational LRS $v_n^{(0)}, \ldots, v_n^{(d-1)}$ for some $d > 0$ such that $\Lambda_{k'}^n = \sum_{i=0}^{d-1} \Lambda_{k'}^i v_n^{(i)}$ and $\overline{\Lambda_{k'}}^n = \sum_{i=0}^{d-1} \overline{\Lambda_{k'}}^i v_n^{(i)}$. Hence we have

$$\gamma_{k'}\Lambda_k^n + \overline{\gamma_{k'}}\,\overline{\Lambda_k^n} = \sum_{i=0}^{d-1}(\gamma_{k'}\Lambda_{k'}^i + \overline{\gamma_{k'}}\,\overline{\Lambda_{k'}}^i)v_n^{(i)}.$$

Therefore, we can write

$$u_n = \sum_{k=1}^{\ell} n^{\ell_k}\beta_k u_n^{(k)}$$

for some $\ell, \ell_k \geq 0$, $\beta_k \in \overline{\mathbb{Q}}$, and simple rational LRS $(u_n^{(k)})_{n\in\mathbb{N}}$.

Let R denote the spectral radius of $(u_n)_{n\in\mathbb{N}}$ and let $r \in \mathbb{Q}$ satisfy $0 < r < \min(1, 1/R)$. Then, for each $1 \leq k \leq \ell$, invoke Lemma 6 with $\alpha = \beta_k$ and r to obtain rational LRS $(c_n^{(k)})_{n\in\mathbb{N}}$ and $(d_n^{(k)})_{n\in\mathbb{N}}$, the rational numbers $b_k \geq 0$, and the threshold N_k. As $(d_n^{(k)})_{n\in\mathbb{N}}$ is an ultimately positive LRS with one dominant root, we can compute a M_k such that $d_n^{(k)} > 0$ for all $n \geq M_k$. Let $\tilde{r} \in \mathbb{Q}$ satisfy $r < \tilde{r} < 1$ and

$$\tilde{r}^n \geq 2\left(\sum_{k=1}^{\ell} b_k |u_n^{(k)}| n^{\ell_k} r^n\right)$$

for all $n \geq N'$, where N' is effectively computable. Note that $1/r$ is bigger than any eigenvalue of any $(u_n^{(k)})_{n\in\mathbb{N}}$, which is R, so $\tilde{r}$ indeed exists. Define $N = \max(N_1, \ldots, N_\ell, M_1, \ldots, M_\ell, N')$, $D_n = d_n^{(1)} \cdots d_n^{(\ell)}$, and

$$\begin{aligned} v_n &= D_n \sum_{k=1}^{\ell} n^{\ell_k}\beta_k u_n^{(k)}, \\ v_n^+ &= D_n\left(\frac{1}{2}\tilde{r}^n + \sum_{k=1}^{\ell}\frac{c_n^{(k)}}{d_n^{(k)}} n^{\ell_k} u_n^{(k)}\right), \\ v_n^- &= D_n\left(-\frac{1}{2}\tilde{r}^n + \sum_{k=1}^{\ell}\frac{c_n^{(k)}}{d_n^{(k)}} n^{\ell_k} u_n^{(k)}\right). \end{aligned}$$

Then, by construction, for all $n \geq N$,

$$\begin{aligned} |v_n^+ - v_n| &\leq |D_n|\left(\frac{1}{2}\tilde{r}^n + \sum_{k=1}^{\ell} n^{\ell_k}\left|\beta_k - \frac{c_n}{d_n}\right| |u_n^{(k)}|\right) \\ &\leq |D_n|\left(\frac{1}{2}\tilde{r}^n + \sum_{k=1}^{\ell} n^{\ell_k} r^n b_k |u_n^{(k)}|\right) \\ &\leq |D_n|\left(\frac{1}{2}\tilde{r}^n + \frac{1}{2}\tilde{r}^n\right) = |D_n|\tilde{r}^n \end{aligned}$$

can grow exponentially, but this exponent is strictly smaller than the spectral radius of $(v_n)_{n\in\mathbb{N}}$. Moreover, it can be seen that $v_n^- \leq v_n \leq v_n^+$ holds for all $n \geq N$ and v_n^+ and v_n^- are rational LRS as the class of LRS is closed under addition and pointwise multiplication. As each $d_n^{(k)}$ is strictly positive for $n \geq N$, so is D_n. Hence $v_n > 0$ if and only if $u_n > 0$.

Therefore, by Theorem 2, there exists $N'' \geq N$ such that for all $n \geq N''$, $|v_n|, |v_n^+|, |v_n^-| \geq |D_n|\tilde{r}^n$. It follows that, for all $n \geq N''$, the signs of v_n, v_n^+ and v_n^- are identical. In particular, v_n is ultimately positive if and only if both v_n^+ and v_n^- are ultimately positive.

As such, we can decide positivity for v_n using the Positivity oracle on v'_n. If there is a $0 \leq n \leq N$ such that $u_n < 0$, conclude that v_n is not positive. Else, apply the Positivity oracle on $(v_{n+N}^+)_{n\in\mathbb{N}}$ and $(v_{n+N}^-)_{n\in\mathbb{N}}$. If both sequences are positive, then $(v_n)_{n\in\mathbb{N}}$ and thus $(u_n)_{n\in\mathbb{N}}$ is positive. Otherwise, enumerate v_n^+ and v_n^- until a negative term is found in one of them, say at index n', and check whether $v_{n'} < 0$. If so, $(v_n)_{n\in\mathbb{N}}$, and thus also $(u_n)_{n\in\mathbb{N}}$, is not positive.

Finally, repeat this process with Positivity oracles starting from $n = n' + 1$.

This process will terminate because if $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$ are both ultimately positive, then they have only finitely many negative values and therefore Positivity oracles will be applied only finitely often. Otherwise, $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$ are both not ultimately positive. Hence a value n exists such that $v_n^+ < 0$ and, as $v_n \leq v_n^+$, $(v_n)_{n\in\mathbb{N}}$ is not positive. This proves the first claim in the statement of Theorem 4.

To prove the second claim, note that if $(u_n)_{n\in\mathbb{N}}$ is simple, $(v_n^+)_{n\in\mathbb{N}}$ and $(v_n^-)_{n\in\mathbb{N}}$ are also simple. Hence our reduction only involves Positivity oracles for simple rational LRS. □

V. The model-checking problem

Recall that the semialgebraic MSO model-checking problem is to determine, given a real algebraic LDS (M, s), a semialgebraic partition $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ of the ambient space, and an MSO specification φ, whether the orbit of (M, s) satisfies φ. We assume that φ is given as a deterministic (e.g. Rabin or Mueller) automaton $\mathcal{A}$. Hence the problem is to decide whether the characteristic word $\alpha \in \mathcal{T}^\omega$ of the orbit of (M, s) relative to $\mathcal{T}$, defined by $\alpha(n) = T_i \Leftrightarrow M^n s \in T_i$, is accepted by $\mathcal{A}$. In this section we show that the semialgebraic MSO model-checking problem for diagonalisable LDS is decidable subject to a Positivity oracle for simple LRS, which by the previous section can be taken to be for integer sequences. Our main tools are toric words and their effective almost-periodicity.

Recall that we denote by $\mathbb{T}$ the set $\{z \in \mathbb{C} : |z| = 1\}$. We say that $S \subseteq \mathbb{C}^d$ is *semialgebraic* if the set

$$\{(x_1, y_1, \ldots, x_d, y_d) : (x_1 + y_1 i, \ldots, x_d + y_d i) \in S\}$$

is a semialgebraic subset of $\mathbb{R}^{2d}$. Let $\Sigma = \{x_1, \ldots, x_\ell\}$ be a finite alphabet. An infinite word $\alpha \in \Sigma^\omega$ is *toric* if there exists a tuple $(d, \Gamma, O_1, \ldots, O_\ell)$ such that

- $\Gamma = (\gamma_1, \ldots, \gamma_d) \in (\overline{\mathbb{Q}} \cap \mathbb{T})^d$,
- $O_1, \ldots, O_\ell$ are open semialgebraic subsets of $\mathbb{T}^d$,
- $\Gamma^n \in \cup_{i=1}^{\ell} O_i$ for all $n \in \mathbb{N}$, where $\Gamma^k = (\gamma_1^k, \ldots, \gamma_d^k)$ for $k \in \mathbb{Z}$, and
- for all $n \in \mathbb{N}$ and i, $\alpha(n) = x_i$ if and only if $\Gamma^n \in O_i$.

We say that α is *generated by* Γ.

An infinite word $\alpha \in \Sigma^\omega$ is *effectively almost-periodic* if for every finite word $u \in \Sigma^*$, there exists a computable window size w_u such that either u does not appear in $\alpha(w_u, \infty)$, or it appears in every contiguous subword of α of length at least w_u. Such α is *strongly effectively almost-periodic* if, in addition, every finite word u either occurs infinitely often, or does not occur in α. The MSO theory of the structure $\langle \mathbb{N}; \leq, f\rangle$, where $f : \mathbb{N} \to \Sigma$ is defined by $f(n) = \alpha(n)$ for an effectively almost-periodic word $\alpha \in \Sigma^\omega$, is known to be decidable by the work of Semënov [35]. We will be using the following equivalent result from [36] by Muchnik *et al.*

Theorem 7. *Given a deterministic automaton $\mathcal{A}$ over an alphabet Σ, and an effectively almost-periodic word $\alpha \in \Sigma^\omega$, it is decidable whether $\mathcal{A}$ accepts α.*

In [36], the authors introduce a family of words similar to toric words (generated by $\Gamma \in e^{i\overline{\mathbb{Q}}}$ as opposed to by $\Gamma \in \mathbb{T}$) and show their effective almost-periodicity. The same approach can be used to prove the following.

Theorem 8. *Toric words are strongly effectively almost-periodic.*

Proof. Let α be a toric word given by $(d, \Gamma, O_1, \ldots, O_\ell)$, $\Gamma = (\gamma_1, \ldots, \gamma_d)$, and let $u \in \Sigma^*$ be a finite word. Define $\Gamma^k z = (\gamma_1^k z_1, \ldots, \gamma_d^k z_d)$ for $k \in \mathbb{Z}$ and $z = (z_1, \ldots, z_d) \in \mathbb{T}^d$, and let $\Gamma X = \{\Gamma z : z \in X\}$ for $X \subseteq \mathbb{C}^d$. Observe that u occurs at the position n of α if and only if

$$\begin{aligned}\bigwedge_{k=0}^{|u|-1} \alpha(n+k) = u(k) &\Leftrightarrow \bigwedge_{k=0}^{|u|-1} \Gamma^{n+k} \in O_{i_k} \\ &\Leftrightarrow \bigwedge_{k=0}^{|u|-1} \Gamma^{n} \in \Gamma^{-k} O_{i_k} \\ &\Leftrightarrow \Gamma^n \in \bigcap_{k=0}^{|u|-1} \Gamma^{-k} O_{i_k}\end{aligned}$$

where O_{i_k} is the open set corresponding to the letter $u(k)$ of u at the position $0 \leq k \leq |u| - 1$. Let $O_u = \bigcap_{k=0}^{|u|-1} \Gamma^{-k} O_{i_k}$. If O_u is empty, then u does not occur in α. Suppose O_u is non-empty. We will show that u must occur infinitely often in α and in every contiguous subword of length w_u that is effectively computable.

Let $\mathbb{T}_\Gamma \subseteq \mathbb{T}^d$ denote the topological closure of $(\Gamma^n)_{n\in\mathbb{N}}$. By Kronecker's theorem in Diophantine approximation, for any $N \in \mathbb{N}$ the sequence $(\Gamma^{n+N})_{n\in\mathbb{N}}$ is dense in $\mathbb{T}_\Gamma$. Moreover, $\mathbb{T}_\Gamma$ is semialgebraic and can be determined effectively; see Corollary 6 in [27] for a proof. Let $f(z) = \Gamma^{-1} z$. To compute w_u we will first show that $\bigcup_{k\in\mathbb{N}} f^k(O_u)$ is an open cover of $\mathbb{T}_\Gamma$. To see this, let $z \in \mathbb{T}_\Gamma$. We need to determine $k \in \mathbb{N}$ such that $z \in f^k(O_u)$, i.e. $\Gamma^k z \in O_u$. Choose a point $y \in O_u$, and let ϵ be such that for all $x \in \mathbb{T}_\Gamma$, $|x - y| < 2\epsilon \Rightarrow x \in O_u$. By the aforementioned density, there exist $n_1, n_2 \in \mathbb{N}$ such that $n_1 < n_2$, $|\Gamma^{n_1} - z| < \epsilon$ and $|\Gamma^{n_2} - y| < \epsilon$. Since the map $x \mapsto \Gamma x$ is an isometry, it follows that $\Gamma^{n_2 - n_1} z \in O_u$.

By compactness of $\mathbb{T}_\Gamma$, there exists K such that $\bigcup_{k=0}^{K} f^k(O_u) \supseteq \mathbb{T}_\Gamma$. Such K can be effectively computed by trial-and-error. It follows that in every interval $[a, b] \subset \mathbb{N}$ of length at least $K + 1$, there exists n such that $\Gamma^n \in O_u$. Since u occurs at position n in α if and only if $\Gamma^n \in O_u$, it follows that u occurs in every contiguous subword of α of size at least $w_u = K + |u|$. □

In [36], the authors show that the interleaving (i.e. the merge) of almost-periodic words need not be almost-periodic. We show that the more special class of toric words does, in fact, have such a closure property.

Theorem 9. *Let $\alpha_0, \ldots, \alpha_{L-1}$ be toric words. Their merge α, defined by $\alpha(qL + r) = \alpha_r(q)$ for $0 \leq r < L$ and $q > 0$, is toric.*

Proof. Suppose α_r is given by $(d_r, \Gamma^{(r)}, O_1^{(r)}, \ldots, O_\ell^{(r)})$. By taking $d = \sum_{r=0}^{L-1} d_r$ and artificially enlarging each $\Gamma^{(r)}$ into an element of $\mathbb{T}^d$ if necessary, we can assume that $d_0 = \ldots = d_{L-1} = d$ and $\Gamma^{(0)} = \ldots = \Gamma^{(L-1)} = \tilde{\Gamma}$ for some $d > 0$ and $\tilde{\Gamma} = (\gamma_1, \ldots, \gamma_d)$. Our approach is to "slow down" $\tilde{\Gamma}$ by a factor of L and add a "$\bmod L$ counter". Let $\gamma = e^{i2\pi/L}$, $\gamma'_j = e^{\mathrm{Log}(\gamma_j)/L}$ for $1 \leq j \leq d$, where Log denotes the principal branch of the complex logarithm, $\Gamma_0 = (\gamma'_1, \ldots, \gamma'_d)$ and $\Gamma = (\gamma, \gamma'_1, \ldots, \gamma'_d)$. Observe that γ is a root of unity of order L. Let $B_0, \ldots, B_{L-1} \subset \mathbb{C}$ be disjoint open balls centred around $\gamma^0, \ldots, \gamma^{L-1}$, respectively. We define

$$O_i = \bigcup_{0 \leq r < L} B_r \times \Gamma_0^r \, O_i^{(r)}$$

for $1 \leq i \leq \ell$. Let $n = qL + b$ with $q > 0$ and $0 \leq b < L$, and observe that for all $1 \leq i \leq \ell$,

$$\begin{aligned}
\Gamma^n \in O_i &\Leftrightarrow \exists r : \gamma^n \in B_r \wedge \Gamma_0^n \in \Gamma_0^r O_i^{(r)} \\
&\Leftrightarrow r = b \wedge \Gamma_0^{qL} \in O_i^{(r)} \\
&\Leftrightarrow \tilde{\Gamma}^n \in O_i^{(b)} \\
&\Leftrightarrow \alpha_b(n) = x_i \\
&\Leftrightarrow \alpha(n) = x_i
\end{aligned}$$

where x_i denotes the letter corresponding to O_i. It follows that α is the toric word given by $(d, \Gamma, O_1, \ldots, O_\ell)$. □

In Theorem 11 we will prove that the characteristic word of a diagonalisable LDS has a toric (and hence effectively almost-periodic) suffix that can be effectively determined using a Positivity oracle for simple LRS. Let $\mathrm{sign} : \mathbb{R} \to \{>, =, <\}$ denote the usual sign function on real numbers.

Lemma 10. *Let $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$, $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_d)$, $D = [\mathbb{K} : \mathbb{Q}]$, $L = (4D^2)!$ and $\Gamma = (\gamma_1, \ldots, \gamma_d)$ where $\gamma_i = \lambda_i/|\lambda_i|$.*

(a) *Let $u_n = p((\lambda_1^L)^n, \ldots, (\lambda_d^L)^n)$, where $p \in \overline{\mathbb{Q}}[z]$. If $(u_n)_{n \in \mathbb{N}}$ is not identically zero, then it is non-degenerate.*

(b) *Let u_n be a diagonalisable, non-degenerate LRS over $\mathbb{K} \cap \mathbb{R}$ that is not identically zero. There exist N that can be effectively computed using a Positivity oracle for simple LRS, and open semialgebraic sets $O_>, O_< \subseteq \mathbb{T}^d$ such that for all $n > N$, $u_n \neq 0$ and $\mathrm{sign}\, u_n = \Delta \Leftrightarrow \Gamma^n \in O_\Delta$ for $\Delta \in \{>, <\}$.*

Proof. To prove (a), let $\sum_{i=1}^m c_i (\Lambda_i^L)^n$ be the exponential polynomial representation of u_n with $\Lambda_i \in \mathbb{K}$ and $c_i \in \overline{\mathbb{Q}}$. Suppose $(\Lambda_i/\Lambda_j)^L$ is a root of unity. Then Λ_i/Λ_j must also be a root of unity. It is well-known that the degree of the kth primitive root of unity is exactly $\Phi(k)$, where Φ is the Euler's totient function. Since $\Phi(k) \geq \sqrt{k}/2$, it follows that the order of Λ_i/Λ_j as a root of unity is at most $4D^2$. But this implies that $(\Lambda_i/\Lambda_j)^L = 1$, which, by the definition of an exponential polynomial representation (see Section II), implies that $i = j$.

To prove (b), let $\sum_{i=1}^m c_i \Lambda_i^n$ be an exponential polynomial representation of u_n, $\rho = \max_{1 \leq i \leq m} |\Lambda_i|$, $\mathcal{D} = \{i : |\Lambda_i| = \rho\}$ and $\mathcal{R} = \{i : |\Lambda_i| < \rho\}$. Write

$$u_n = \underbrace{\sum_{i \in \mathcal{D}} c_i \Lambda_i^n}_{d_n} + \underbrace{\sum_{j \in \mathcal{R}} c_j \Lambda_j^n}_{r_n}.$$

Let $\mu < \rho$ be such that $|\Lambda_j| < \mu$ for all $j \in \mathcal{R}$. For sufficiently large n, $|r_n| < \mu^n$. Applying Theorem 3, there exists N, computable using a Positivity oracle for simple LRS, such that for all $n > N$, $|d_n| > \mu^n > |r_n|$ and hence $u_n \neq 0$.

By the discussion in Section II-A, for each $i \in \mathcal{R}$ there exists $i' \neq i$ such that $\sigma(c_i) = c_{i'}$ and $\sigma(\Lambda_i) = \Lambda_{i'}$. Since $|\sigma(\Lambda_i)| = \rho$ for $i \in \mathcal{D}$, the summands of d_n are also closed under conjugation and d_n is real-valued. Therefore, for $n > N$, $\mathrm{sign}\, u_n = \mathrm{sign}\, d_n \in \{>, <\}$.

Finally, we express $\mathrm{sign}\, d_n$ in terms of Γ^n. Consider $v_n = u_n/\rho^n$, and for $i \in \mathcal{D}$, write $\Lambda_i/\rho^n = f_i(\gamma_1, \ldots, \gamma_d)$ for a monomial f_i, observing that Λ_i/ρ^n belongs to the multiplicative group generated by $\gamma_1, \ldots, \gamma_d$. We can then define

$$O_\Delta = \{z \in \mathbb{T} : \sum_{i \in \mathcal{D}} c_i f_i(z) \, \Delta \, 0\}$$

for $\Delta \in \{>, <\}$. □

We are now ready to prove that the characteristic word of a diagonalisable system relative to a semialgebraic partition has a toric suffix. In the sequel, by $\delta(N, \infty)$ we mean the word $\sigma(N)\sigma(N+1)\ldots$ where σ is an an infinite word and $N \in \mathbb{N}$.

Theorem 11. *Let $(M, s) \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d} \times (\mathbb{R} \cap \overline{\mathbb{Q}})^d$ be a diagonalisable LDS, $\mathcal{T} = \{T_1, \ldots, T_\ell\}$ be a semialgebraic partition of $\mathbb{R}^d$, and $\alpha \in \mathcal{T}^\omega$ denote the characteristic word of the orbit of (M, s) relative to $\mathcal{T}$. There exist N, effectively computable using a Positivity oracle for simple LRS, and $\Gamma, O_1, \ldots, O_\ell$ that can be determined effectively, such that $\beta = \alpha(N, \infty)$ is the toric word given by $(d, \Gamma, O_1, \ldots, O_\ell)$.*

Proof. Let $\lambda_1, \ldots, \lambda_d$ denote the eigenvalues of M, $\mathbb{K} = \mathbb{Q}(\lambda_1, \ldots, \lambda_d)$, $D = [\mathbb{K} : \mathbb{Q}]$, $L = (4D^2)!$ and $\Gamma = (\gamma_1, \ldots, \gamma_d)$ where $\gamma_i = \lambda_i/|\lambda_i|$. For $0 \leq r < L$ and $n \geq 0$, define $\alpha_r \in \mathcal{T}^\omega$ by

$$\alpha_r(n) = \alpha(nL + r).$$

Observe that α is the merge of $\alpha_0, \ldots, \alpha_{L-1}$. We first prove the following intermediate results.

(*) For each $0 \leq r < L$ and $T_k \in \mathcal{T}$, there exists $N_{r,k}$ (computable using a Positivity oracle for simple LRS) and an open semialgebraic set $O_{r,k}$ such that for all $n > N_{r,k}$, $\alpha_r(n) \in T_k \Leftrightarrow \Gamma^n \in O_{r,k}$.

(**) There exists N_1 computable using a Positivity oracle for simple LRS such that the suffix $\beta_r = \alpha_r(N_1, \infty)$ is toric for every $0 \leq r < L$.

To prove $(*)$, let

$$\bigvee_{i \in I} \bigwedge_{j \in J} p_{i,j}(x_1, \ldots, x_d) \, \Delta_{i,j} \, 0$$

be a formula in disjunctive normal form defining T_k, where w.l.o.g. we can assume $\Delta_{i,j} \in \{\geq, >\}$. We have that $\alpha_r(n) = T_k$ if and only if

$$\bigvee_{i \in I} \bigwedge_{j \in J} p_{i,j}(M^{nL+r}s)\, \Delta_{i,j}\, 0.$$

Let $u_n^{(i,j)} = p_{i,j}(M^{nL+r}s)$. Writing

$$M^{nL+r}s = P^{-1}\,\mathrm{diag}(\lambda_1^{nL}, \ldots, \lambda_d^{nL})PM^r s$$

where $P \in \overline{\mathbb{Q}}^{d \times d}$ is an invertible change-of-basis matrix, observe that $u_n^{(i,j)} = q_{i,j}(\lambda_1^{nL}, \ldots, \lambda_d^{nL})$ for a polynomial $q_{i,j} \in \overline{\mathbb{Q}}[z_1, \ldots, z_d]$. If $(u_n^{(i,j)})_{n \in \mathbb{N}}$ is identically zero, then the condition $p_{i,j}(M^{nL+r}s)\, \Delta_{i,j}\, 0$ either holds for all $n \in \mathbb{N}$, or does not hold for all $n \in \mathbb{N}$. Such conditions can be replaced by true or false. Hence we can assume that no sequence $(u_n^{(i,j)})_{n \in \mathbb{N}}$ is identically zero. By Lemma 10 (a), every $(u_n^{(i,j)})_{n \in \mathbb{N}}$ is non-degenerate. Applying Lemma 10 (b), let $N_{i,j}$ and $O_{i,j}$ be such that for $n > N_{i,j}$,

- $u_n^{(i,j)} \neq 0$, and
- $u_n^{(i,j)} > 0$ if and only if $\Gamma^n \in O_{i,j}$.

Note that each $N_{i,j}$ can be effectively determined using a Positivity oracle for simple LRS. Let $N_{r,k} = \max_{(i,j) \in I \times J} N_{i,j}$ and

$$O_{r,k} = \bigcup_{i \in I} \bigcap_{j \in J} O_{i,j}.$$

For $n > N_{r,k}$, it holds that $\alpha_r(n) = T_k$ if and only if $\Gamma^n \in O_{r,k}$.

To prove $(**)$, let $N_{r,k}$ and $O_{r,k}$ be as in $(*)$ and define $N_1 = 1 + \max\{N_{r,k} : 0 \leq r < L \wedge 1 \leq k \leq \ell\}$. Consider $\beta_r = \alpha_r(N_1, \infty)$. For $n \in \mathbb{N}$ and $1 \leq k \leq \ell$,

$$\begin{aligned} \beta_r(n) = T_k &\Leftrightarrow \alpha_r(n + N_1) \in T_k \\ &\Leftrightarrow \Gamma^{n+N_1} \in O_{r,k} \\ &\Leftrightarrow \Gamma^n \in \Gamma^{-N_1} O_{r,k}. \end{aligned}$$

Hence β_r is the toric word given by

$$(d, \Gamma, \Gamma^{-N_1}O_{r,1}, \ldots, \Gamma^{-N_1}O_{r,\ell}).$$

We are now ready to prove Theorem 11. Let $N = N_1 L$, and consider $\beta = \alpha(N, \infty)$. The word β is the merge of $\beta_0, \ldots, \beta_{L-1}$ where $\beta_r = \alpha_r(N_1, \infty)$. Applying Theorem 9 to $\beta_0, \ldots, \beta_{L-1}$, we obtain that their merge β is toric.

Note that all the semialgebraic sets above that are used in defining a toric word are fully effective in the sense that we can write down their definition (for example, as a disjunction of conjunction of polynomial inequalities) without needing a Positivity oracle. The oracle is only required for computing $N_{r,k}$ for $0 \leq r < L$ and $1 \leq k \leq \ell$. □

The decidability result for diagonalisable systems subject to existence of a Positivity oracle follows immediately.

Theorem 12. *Let $(M, s) \in (\mathbb{R} \cap \overline{\mathbb{Q}})^{d \times d} \times (\mathbb{R} \cap \overline{\mathbb{Q}})^d$ be a diagonalisable LDS, $\mathcal{T}$ be a semialgebraic partition of $\mathbb{R}^d$, and $\mathcal{A}$ be a deterministic automaton. Subject to existence of a Positivity oracle for simple integer LRS, it is decidable whether $\mathcal{A}$ accepts the characteristic word $\alpha \in \mathcal{T}^\omega$ of the orbit of (M, s) with respect to $\mathcal{T}$.*

Proof. Let N be as in the statement of Theorem 11, which can be computed using a Positivity oracle for simple LRS, and q be the state of $\mathcal{A}$ after reading the first N letters of α. The suffix $\beta = \alpha(N, \infty)$ is toric (given by $(d, \Gamma, O_1, \ldots, O_\ell)$ that can be determined fully effectively) and hence effectively almost-periodic by Theorem 8. Let $\mathcal{B}$ denote the deterministic automaton that has q as the start state and is identical to $\mathcal{A}$ otherwise. Observe that $\mathcal{A}$ accepts α if and only if $\mathcal{B}$ accepts β, which can be decided by Theorem 7. □

VI. Concluding Remarks

In this final section, let us briefly comment on what are perhaps the two most natural and pressing questions arising from our work: (i) can our main model-checking result, Theorem 12, be extended to arbitrary (i.e., not necessarily diagonalisable) LDS, assuming a Positivity oracle for arbitrary (not necessarily simple) LRS? And (ii) are there any foreseeable prospects of actually designing Positivity oracles for simple integer LRS, subject perhaps to some number-theoretic conjectures?

Let us begin by pointing out a major obstacle to extending our current proof techniques to non-diagonalisable LDS. As observed in [11, Sec. 4], in contrast to their diagonalisable siblings, non-diagonalisable LDS can unfortunately give rise to characteristic words that fail to be almost-periodic. This in turn dooms our entire present approach, which is predicated on the pivotal results of Muchnik *et al.* [36].

A second substantial difficulty arises by considering the *Ultimate Positivity Problem* for LRS: an LRS $(u_n)_{n \in \mathbb{N}}$ is ultimately positive if it harbours at most finitely many negative terms, i.e., there is some threshold $T \in \mathbb{N}$ such that, for all $n \geq T$, $u_n \geq 0$. The Ultimate Positivity Problem for LRS is easily seen to be equivalent to the model-checking problem which asks, for a given LDS (M, s) and full-dimensional half-space H, whether the orbit of (M, s) is eventually forever trapped in H. It is interesting to note that, whilst Ultimate Positivity is decidable for all simple LRS [29], not only is it not known to be decidable for arbitrary (non-simple) LRS, but in fact one can show that the existence of an Ultimate Positivity oracle for arbitrary LRS would entail major breakthroughs in Diophantine approximation: the ability to approximate arbitrarily closely the *Lagrange constant* (or *homogeneous Diophantine approximation constant*) $L_\infty(t)$ for a countable class of transcendental numbers t consisting of ratios of logarithms of complex algebraic numbers; such a task is considered by experts to be vastly beyond the capabilities of contemporary number theory. We refer the reader to [26, Sec. 5] for details.

Now the authors of [26] also show that, should a Positivity oracle for arbitrary LRS exist, one could approximate arbitrarily closely the *homogeneous Diophantine approximation type* $L(t)$ for the same class of transcendental numbers t. Nevertheless, essentially the only known relationships between

these quantities are that, for all transcendentals t, $0 \leq L(t) \leq L_\infty(t) \leq 1/3$, and also $L(t) = 0$ iff $L_\infty(t) = 0$. It is moreover widely believed by number theorists that, for the class of transcendental numbers at hand, $L(t) = 0$ (although this likely can never be established, even with a Positivity oracle, since the latter only provides us with *approximation* capabilities). In other words, the ability to approximate $L(t)$ to arbitrary precision does not appear to yield any visible benefits as regards approximating $L_\infty(t)$, and *a fortiori* as regards deciding Ultimate Positivity for arbitrary LRS.

One might of course argue that there could be other, currently unforeseen, ways in which to make use of a Positivity oracle to establish Ultimate Positivity. But frontal attempts do not seem to lead anywhere. We therefore continue to hold that Ultimate Positivity of arbitrary LRS remains a formidably difficult computational problem, even with the help of a Positivity oracle.

We also conjecture that the following algorithmic problem remains intractably difficult, even assuming a Positivity oracle: given two LRS $(u_n)_{n\in\mathbb{N}}$ and $(v_n)_{n\in\mathbb{N}}$, is there some $n \in \mathbb{N}$ such that both $u_n < 0$ and $v_n < 0$? We speculate that one can in fact construct an infinite hierarchy of such problems, where determining the existence of an index for which a $(k+1)$-fold combination of LRS simultaneously take on negative values remains difficult, even assuming the existence of an oracle for the k-fold version of the problem. It is moreover easily checked that each problem in this hierarchy can straightforwardly be encoded as an LDS model-checking query.

Turning to (ii), it is conceivable, on the other hand, that Positivity oracles for *simple* LRS might eventually be achievable. One immediate avenue towards this goal would be to obtain an effective version of the Subspace Theorem. Even though, in the present state of knowledge, this too appears to be a daunting number-theoretic task, several mathematicians in recent years have attempted to make progress on that front.

VII. Acknowledgements

Toghrul Karimov and Joël Ouaknine were supported by DFG grant 389792660 as part of TRR 248 (see https://perspicuous-computing.science). Joël Ouaknine is also affiliated with Keble College, Oxford as emmy.network Fellow. James Worrell was supported by EPSRC Fellowship EP/X033813/1.

References

[1] R. Kannan and R. J. Lipton, "The Orbit Problem is decidable," in *Proceedings of the 12th Annual ACM Symposium on Theory of Computing 1980*. ACM, 1980, pp. 252–261.

[2] ——, "Polynomial-time algorithm for the Orbit Problem," *J. ACM*, vol. 33, no. 4, pp. 808–821, 1986.

[3] V. Chonev, J. Ouaknine, and J. Worrell, "The Orbit Problem in higher dimensions," in *Symposium on Theory of Computing Conference, STOC'13*. ACM, 2013, pp. 941–950.

[4] ——, "On the complexity of the orbit problem," *J. ACM*, vol. 63, no. 3, jun 2016. [Online]. Available: https://doi.org/10.1145/2857050

[5] S. P. Tarasov and M. N. Vyalyi, "Orbits of linear maps and regular languages," in *Computer Science - Theory and Applications - 6th International Computer Science Symposium in Russia, CSR 2011*, ser. Lecture Notes in Computer Science, vol. 6651. Springer, 2011, pp. 305–316.

[6] V. Chonev, J. Ouaknine, and J. Worrell, "The Polyhedron-Hitting Problem," in *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015*. SIAM, 2015, pp. 940–956.

[7] S. Almagor, J. Ouaknine, and J. Worrell, "The Polytope-Collision Problem," in *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017*, ser. LIPIcs, vol. 80. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017, pp. 24:1–24:14.

[8] ——, "The semialgebraic orbit problem," in *36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019, March 13-16, 2019, Berlin, Germany*, ser. LIPIcs, R. Niedermeier and C. Paul, Eds., vol. 126. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, pp. 6:1–6:15. [Online]. Available: https://doi.org/10.4230/LIPIcs.STACS.2019.6

[9] ——, "First-order orbit queries," *Theory Comput. Syst.*, vol. 65, no. 4, pp. 638–661, 2021.

[10] T. Karimov, J. Ouaknine, and J. Worrell, "On LTL model checking for low-dimensional discrete linear dynamical systems," in *45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020, LIPIcs 170*, 2020.

[11] S. Almagor, T. Karimov, E. Kelmendi, J. Ouaknine, and J. Worrell, "Deciding ω-regular properties on linear recurrence sequences," *Proc. ACM Program. Lang.*, vol. 5, no. POPL, pp. 1–24, 2021. [Online]. Available: https://doi.org/10.1145/3434329

[12] T. Karimov, E. Lefaucheux, J. Ouaknine, D. Purser, A. Varonka, M. A. Whiteland, and J. Worrell, "What's decidable about linear loops?" *Proc. ACM Program. Lang.*, vol. 6, no. POPL, pp. 1–25, 2022.

[13] D. Beauquier, A. M. Rabinovich, and A. Slissenko, "A logic of probability with decidable model checking," *J. Log. Comput.*, vol. 16, no. 4, pp. 461–487, 2006. [Online]. Available: https://doi.org/10.1093/logcom/exl004

[14] M. Agrawal, S. Akshay, B. Genest, and P. S. Thiagarajan, "Approximate verification of the symbolic dynamics of markov chains," *J. ACM*, vol. 62, no. 1, pp. 2:1–2:34, 2015.

[15] T. Karimov, E. Kelmendi, J. Ouaknine, and J. Worrell, "What's decidable about discrete linear dynamical systems?" in *Principles of Systems Design - Essays Dedicated to Thomas A. Henzinger on the Occasion of His 60th Birthday*, ser. Lecture Notes in Computer Science, J. Raskin, K. Chatterjee, L. Doyen, and R. Majumdar, Eds., vol. 13660. Springer, 2022, pp. 21–38. [Online]. Available: https://doi.org/10.1007/978-3-031-22337-2_2

[16] F. Luca, J. Ouaknine, and J. Worrell, "Algebraic model checking for discrete linear dynamical systems," in *Formal Modeling and Analysis of Timed Systems - 20th International Conference, FORMATS 2022, Warsaw, Poland, September 13-15, 2022, Proceedings*, ser. Lecture Notes in Computer Science, S. Bogomolov and D. Parker, Eds., vol. 13465. Springer, 2022, pp. 3–15. [Online]. Available: https://doi.org/10.1007/978-3-031-15839-1_1

[17] M. Soittola, "On D0L synthesis problem," in *Automata, Languages, Development*, A. Lindenmayer and G. Rozenberg, Eds. North-Holland, 1976.

[18] A. Salomaa, "Growth functions of Lindenmayer systems: Some new approaches," in *Automata, Languages, Development*, A. Lindenmayer and G. Rozenberg, Eds. North-Holland, 1976.

[19] J. Berstel and M. Mignotte, "Deux propriétés décidables des suites récurrentes linéaires," *Bull. Soc. Math. France*, vol. 104, 1976.

[20] R. Tijdeman, M. Mignotte, and T. Shorey, "The distance between terms of an algebraic recurrence sequence," *Journal für die reine und angewandte Mathematik (Crelles Journal)*, vol. 1984, no. 349, pp. 63–76, 1984. [Online]. Available: https://doi.org/10.1515/crll.1984.349.63

[21] N. Vereshchagin, "The problem of appearance of a zero in a linear recurrence sequence," *Mat. Zametki*, vol. 38, no. 2, pp. 609–615, 1985.

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

[23] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence Sequences*, ser. Mathematical Surveys and Monographs. American Mathematical Society, 2003. [Online]. Available: http://dx.doi.org/10.1090/surv/104

[24] V. Halava, T. Harju, and M. Hirvensalo, "Positivity of second order linear recurrent sequences," *Discret. Appl. Math.*, vol. 154, no. 3, pp. 447–451, 2006.
[25] V. Laohakosol and P. Tangsupphathawat, "Positivity of third order linear recurrence sequences," *Discret. Appl. Math.*, vol. 157, no. 15, pp. 3239–3248, 2009.
[26] J. Ouaknine and J. Worrell, "Positivity problems for low-order linear recurrence sequences," in *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, 12 2014. [Online]. Available: https://doi.org/10.1137/1.9781611973402.27
[27] ——, "On the positivity problem for simple linear recurrence sequences," in *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, ser. Lecture Notes in Computer Science, J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, Eds., vol. 8573. Springer, 2014, pp. 318–329.
[28] ——, "On linear recurrence sequences and loop termination," *ACM SIGLOG News*, vol. 2, no. 2, pp. 4–13, 2015.
[29] ——, "Ultimate positivity is decidable for simple linear recurrence sequences," in *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Proceedings, Part II*, ser. Lecture Notes in Computer Science, vol. 8573. Springer, 2014, pp. 330–341.
[30] F. Q. Gouvêa, *p-adic Numbers*. Springer International Publishing, 2020. [Online]. Available: https://doi.org/10.1007%2F978-3-030-47295-5
[31] J. S. Milne, "Algebraic number theory (v3.08)," p. 166, 2020, available at www.jmilne.org/math/.
[32] D. A. Marcus, *Number Fields*. Springer International Publishing, 2018. [Online]. Available: https://doi.org/10.1007%2F978-3-319-90233-3
[33] J.-H. Evertse, "On sums of s-units and linear recurrences," *Compositio Mathematica*, vol. 53, no. 2, pp. 225–244, 1984. [Online]. Available: http://eudml.org/doc/89685
[34] M. Waldschmidt, *Heights of Algebraic Numbers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 65–114. [Online]. Available: https://doi.org/10.1007/978-3-662-11569-5_3
[35] A. L. Semënov, "Logical theories of one-place functions on the set of natural numbers," *Mathematics of the USSR-Izvestiya*, vol. 22, no. 3, pp. 587–618, 1984. [Online]. Available: https://doi.org/10.1070/im1984v022n03abeh001456
[36] A. Muchnik, A. Semenov, and M. Ushakov, "Almost periodic sequences," *Theoretical Computer Science*, vol. 304, no. 1-3, pp. 1–33, 2003. [Online]. Available: https://doi.org/10.1016/s0304-3975(02)00847-2