

On Expansions of Monadic Second-Order Logic with Dynamical Predicates

Joris Nieuwveld 

Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany

Joël Ouaknine 

Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany

Abstract

Expansions of the monadic second-order (MSO) theory of the structure $\langle \mathbb{N}; < \rangle$ have been a fertile and active area of research ever since the publication of the seminal papers of Büchi and Elgot & Rabin on the subject in the 1960s. In the present paper, we establish decidability of the MSO theory of $\langle \mathbb{N}; <, P \rangle$, where P ranges over a large class of unary “dynamical” predicates, i.e., sets of non-negative values assumed by certain integer linear recurrence sequences. One of our key technical tools is the novel concept of (*effective*) *prodisjunctivity*, which we expect may also find independent applications further afield.

2012 ACM Subject Classification Theory of computation $\rightarrow$ Logic and verification; Theory of computation $\rightarrow$ Formal languages and automata theory; Mathematics of computing $\rightarrow$ Discrete mathematics

Keywords and phrases Monadic second-order logic, linear recurrence sequences, decidability, Baker’s theorem

Digital Object Identifier 10.4230/LIPIcs.MFCS.2025.80

Related Version *Full Version:* <https://arxiv.org/abs/2507.16581>

Funding *Joël Ouaknine:* Also affiliated with Keble College, Oxford as emmy.network Fellow, and supported by ERC grant DynAMiCs (101167561) and DFG grant 389792660 as part of TRR 248.

1 Introduction

The monadic second-order (MSO) theory of the structure $\langle \mathbb{N}; < \rangle$ has been a foundational pillar of the field of automated verification, and more generally the area of logic in computer science, for many decades. Arguably the most important paper on the topic is due to Büchi [6], who in the early 1960s established decidability of this theory through a deep and fecund connection between logic and automata theory.

Shortly thereafter, in yet another seminal piece of work [11], Elgot and Rabin devised the *contraction method* to establish decidability of expansions of this base theory by various “arithmetic” unary predicates $P \subseteq \mathbb{N}$.¹ In particular, they proved decidability of the MSO theory of $\langle \mathbb{N}; <, P \rangle$, where P could for example be taken to be the set $2^{\mathbb{N}}$ of powers of 2, or the set Sq of perfect squares, or the set Fac of factorial numbers, and so on.

Much progress followed in the ensuing decades, notably thanks to Semënov [24], who introduced the notion of *effective almost periodicity*, and Carton and Thomas [8], who substantially refined Elgot and Rabin’s contraction method into the notion of *effective profinite ultimate periodicity*. Other notable works in this area include articles by Rabinovich [22], Rabinovich and Thomas [23], and Berthé et al. [3].

¹ In this paper, we adopt the convention that the set $\mathbb{N}$ of natural numbers contains 0. We also use the adjective “positive” with the meaning of “non-negative”.



In the present paper, we significantly extend this line of research by considering a large class of “dynamical” predicates derived from integer linear recurrence sequences (LRS).² The complexity of an LRS can be measured in various ways; chief among them are the number of distinct *dominant characteristic roots* of the LRS, and whether the LRS is *simple* or not.³ For P the set of positive values of an LRS having a single dominant root, such as the set of Fibonacci numbers, the decidability of the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is readily established via Elgot and Rabin’s contraction method;⁴ see also [3] in which expansions of $\langle \mathbb{N}; < \rangle$ by adjoining multiple predicates obtained from such LRS are thoroughly investigated. Unfortunately, virtually nothing is known when considering LRS having more than a single dominant characteristic root.

Our main contribution is the following result:

► **Theorem 1.** *Let $P = \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$ for $\langle u_n \rangle_{n=0}^\infty$ a non-degenerate, simple, integer-valued linear recurrence sequence with two dominant roots. Then the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is decidable.*

An example of an LRS satisfying the hypotheses of Thm. 1 is the sequence $\langle u_n \rangle_{n=0}^\infty$ defined by

$$u_{n+3} = 6u_{n+2} - 13u_{n+1} + 10u_n \quad (1)$$

and $u_0 = 2, u_1 = 4$, and $u_2 = 7$. Its subsequent values are: 10, 9, -6 , -53 , -150 , -271 , -206 , 787, 4690, 15849, 41994, 92827, 169530, 230369, 106594, $\dots$. One can readily verify that $\langle u_n \rangle_{n=0}^\infty$ satisfies the formula

$$u_n = \frac{1}{2}(2+i)^n + \frac{1}{2}(2-i)^n + 2^n, \quad (2)$$

and that u_n is both infinitely often positive and infinitely often negative. Moreover, although $\lim_{n \rightarrow \infty} |u_n| = +\infty$, $|u_n|$ is *not* monotonically increasing: for all $N \in \mathbb{N}$ there is an $n \in \mathbb{N}$ such that $|u_{n+N}| < |u_n|$.

For our LRS $\langle u_n \rangle_{n=0}^\infty$, let P be as per Thm. 1. Viewing P as an ordered set, we have:

$$P = \{u_0, u_1, u_2, u_4, u_3, u_{10}, u_{11}, u_{12}, u_{13}, u_{14}, u_{17}, u_{15}, u_{16}, u_{24}, u_{25}, u_{26}, u_{27}, u_{28}, u_{30}, \dots\}.$$

One immediately notices that there are two complications at play here. The first one is that we are “throwing away” all the negative values of our LRS (this is of course necessary since we are working over domain $\mathbb{N}$ rather than $\mathbb{Z}$). This restriction is, however, entirely benign in view of the following result:

► **Corollary 2.** *Let $\bar{P} = \{u_n : n \in \mathbb{N}\}$ for $\langle u_n \rangle_{n=0}^\infty$ a non-degenerate, simple, integer-valued linear recurrence sequence with two dominant roots. Then the MSO theory of the structure $\langle \mathbb{Z}; 0, <, \bar{P} \rangle$ is decidable.*

² The “dynamical” moniker was chosen to reflect the close kinship of these predicates with discrete-time linear dynamical systems; see, e.g., [1, 2, 9, 14–16, 18].

³ These notions are properly defined in Sec. 2.3.

⁴ LRS having a single positive dominant root are particularly well behaved: they are either constant, or effectively ultimately monotonically increasing (or decreasing), effectively procyclic, and effectively sparse (see [3] for precise definitions of these notions and a proper account of these facts). In the case of a negative dominant root, essentially the same behaviour is observed by restricting to the positive terms.

This result is straightforwardly obtained from Thm. 1 via an application of Shelah’s celebrated “composition method” in model theory [25]. In the case at hand, one can directly invoke, for example, [26, Cor. 6], since the structure $\langle \mathbb{Z}; 0, <, \overline{P} \rangle$ is isomorphic to the ordered sum $\langle \mathbb{Z} - \mathbb{N}; <, P^- \rangle + \langle \mathbb{N}; <, P \rangle$, where the second summand is as per Thm. 1, and the first structure is obtained by setting $P^- = \{u_n : n \in \mathbb{N}\} \cap (\mathbb{Z} - \mathbb{N})$. Intuitively speaking, MSO sentences over $\langle \mathbb{Z}; <, \overline{P} \rangle$ can be faithfully decomposed into component subformulas dealing exclusively with either positive or negative values of our LRS, with the truth value of the original sentence obtained by appropriately piecing together truth values of each of the sub-sentences within their respective structures.

The second complication is that, as noted earlier, the ordering of the positive values of our LRS does not respect the index ordering of the LRS. This ostensibly precludes the direct application of classical techniques such as Elgot and Rabin’s contraction method (or more generally Carton and Thomas’s effective profinite ultimate periodicity criterion), or Semënov’s toolbox of effective almost periodicity.

In order to prove Thm. 1, we therefore rely instead on a new concept, that of (*effective*) *prodisjunctivity*, which we introduce shortly. Prodisjunctivity is itself predicated on the notion of disjunctivity, whose application to the decidability of logical theories (under the alternative terminology of “weak normality”) was pioneered by Berthé et al. [3]. In particular, Berthé et al. study the MSO theory of the structure $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \text{Sq} \rangle$, and establish decidability assuming that the binary expansion of $\sqrt{2}$ is disjunctive, i.e., contains every finite bit pattern as a factor infinitely often.

The hypothesis that $\sqrt{2}$ is disjunctive in base 2 is widely expected by number theorists to be true, but remains a major unsolved problem. Irrational algebraic numbers, along with most known transcendental numbers such as e and π , are in fact believed to satisfy a stronger property, that of being *normal* in every integer base: a real number α is normal in base b provided that every finite word $w \in \{0, \dots, b-1\}^*$ appears with frequency $b^{-|w|}$ in the base- b expansion of α . And although Borel [5] showed over a century ago that non-normal real numbers have null Lebesgue measure, establishing normality (or even disjunctivity) of everyday irrational numbers has remained fiercely elusive; see [7, 13, 17, 21] for more detailed accounts of results, research, and open problems in this area.

Given a finite alphabet Σ together with a subset $S \subseteq \Sigma$, we say that an infinite sequence in Σ^ω is *disjunctive relative to S* if every finite word over S appears infinitely often as a factor in the sequence. We are now in a position to define (effective) prodisjunctivity:

► **Definition 3.** Let $\langle p_m \rangle_{m=0}^\infty$ be an infinite integer-valued sequence. For any integer $M \geq 2$, let S_M be the set of residue classes modulo M that appear infinitely often in $\langle p_m \rangle_{m=0}^\infty$:

$$S_M = \{s \in \{0, \dots, M-1\} : \exists^\infty m \in \mathbb{N} : p_m \equiv s \pmod{M}\}. \quad (3)$$

We say that the sequence $\langle p_m \rangle_{m=0}^\infty$ is **prodisjunctive** if, for all $M \geq 2$, the sequence of residues $\langle p_m \bmod M \rangle_{m=0}^\infty$ is disjunctive relative to S_M .

For **effectiveness**, we require in addition that the sequence $\langle p_m \bmod M \rangle_{m=0}^\infty$ be computable and that, for each M , the set S_M , together with the smallest index threshold N_M beyond which all residue classes of the sequence lie in S_M (i.e., for all $m \geq N_M$, $(p_m \bmod M) \in S_M$), also be computable.

Let us now sketch how prodisjunctivity relates to Thm. 1. Recall from (1) our LRS $\langle u_n \rangle_{n=0}^\infty$, along with its infinite set P of positive values (as per the notation of Thm. 1), and let $\langle p_m \rangle_{m=0}^\infty$ be a strictly increasing enumeration of P ; in other words, p_{m-1} is the m th smallest element in P . We will establish the following instrumental result:

► **Theorem 4.** *Let $\langle p_m \rangle_{m=0}^\infty$ be as above, i.e., the strictly increasing sequence of positive terms of some non-degenerate, simple, integer-valued LRS having two dominant roots. Then $\langle p_m \rangle_{m=0}^\infty$ is effectively prodisjunctive.*

Let us return to our example and set $M = 5$. Then one easily shows that

$$u_n \bmod 5 = \begin{cases} 0 & \text{if } n \equiv 3 \pmod{4} \\ 2 & \text{if } n = 0, \text{ or if } n \equiv 2 \pmod{4} \\ 4 & \text{otherwise.} \end{cases} \quad (4)$$

It follows that $S_5 = \{0, 2, 4\}$, $N_5 = 0$, and

$$\langle p_m \bmod 5 \rangle_{m=0}^\infty = \langle 2, 4, 2, 4, 0, 2, 0, 4, 2, 4, 0, 4, 4, 2, 0, 4, 2, 4, 2, 0, 4, 4, 2, 0, 4, 4, 2, \dots \rangle$$

is in $\{0, 2, 4\}^\omega$.

Computing the first million terms of $\langle p_m \bmod 5 \rangle_{m=0}^\infty$, one does not encounter the factor $\langle 0, 0, 0 \rangle$ once within that initial segment. Nevertheless, according to Thm. 4, it should appear infinitely often! Indeed, we prove this in Sec. 3.2, and moreover construct an index of roughly $2.18 \cdot 10^{59}$ where this occurs. A more involved calculation (not shown here) can however establish that the very first occurrence of $\langle 0, 0, 0 \rangle$ within $\langle p_m \bmod 5 \rangle_{m=0}^\infty$ is at index 8479226.

The above discussion suggests that, whilst the sequence $\langle p_m \rangle_{m=0}^\infty$ is provably disjunctive, it is by all accounts not normal, i.e., a given factor $w \in \{0, 2, 4\}^*$ does not necessarily appear with frequency $3^{-|w|}$. This is however unsurprising in view of (4): the residue class 4 should statistically appear approximately twice as often as either of the other two residue classes, and indeed it is possible to prove that this is asymptotically the case.

Theorem 4 is the key technical device underpinning our main result, Thm. 1. One of the critical mathematical ingredients entering its proof is Baker’s theorem on linear forms in logarithms of algebraic numbers. We also make use of various automata-theoretic, topological, and combinatorial constructions and tools.

Let us now briefly comment on the motivation and scope of Thm. 1. As noted earlier, linear recurrence sequences and linear dynamical systems are intimately related; in particular, decision procedures for the former often underpin verification algorithms for the latter. Write $P_{\mathbf{u}}$ to denote the set of positive values of a given integer LRS $\mathbf{u}$. We already pointed out that Elgot and Rabin’s contraction method enables one to establish decidability of the MSO theory of $\langle \mathbb{N}; <, P_{\mathbf{u}} \rangle$ provided that $\mathbf{u}$ has a single dominant root, and that [3, Thm. 5.1] provides general conditions under which the MSO theory of $\langle \mathbb{N}; <, P_{\mathbf{u}^{(1)}}, \dots, P_{\mathbf{u}^{(d)}} \rangle$ is decidable, once again under the assumption that each LRS $\mathbf{u}^{(i)}$ possesses a single dominant root. On the other hand, the situation concerning predicates derived from LRS having more than one dominant root is entirely uncharted. The present paper can thus be seen as taking the first significant step (in some six decades!) in this direction.

Nevertheless, the hypotheses of Thm. 1 (the LRS must be non-degenerate, simple, and have exactly two dominant roots) may at first glance appear quite restrictive. It is worth noting, however, that if one were to pick LRS “at random”, then under most “reasonable” probability distributions, with probability tending to 1 such LRS would have either a single dominant root, or be non-degenerate, simple, and have exactly two dominant roots. In other words, the vast majority of LRS are of one of these two types, and thus fall under the scope of the Elgot-Rabin contraction method or our own Thm. 1. (This folklore result follows from the fact that a random polynomial with real coefficients will almost surely have either a single dominant real root, or two dominant complex conjugate roots; and that non-degeneracy and simplicity are null-measure conditions. For a more in-depth discussion of these matters, see the work of Dubickas and Sha [10] and citations therein.) In any event, we briefly return in Sec. 4 to the question of whether the hypotheses of Thm. 1 could be weakened in any way.

2 Preliminaries

2.1 Automata Theory

An *alphabet* Σ is a finite, non-empty set of letters. Σ^* and Σ^ω denote respectively the sets of finite and infinite words over Σ . As words can be viewed as sequences, we freely identify the finite word $w_0w_1 \cdots w_k$ with the finite sequence $\langle w_0, w_1, \dots, w_k \rangle$, and the infinite word $w_0w_1 \cdots$ with the infinite sequence $\langle w_0, w_1, \dots \rangle$, and conversely. A finite word $w' = w'_0w'_1 \cdots w'_k$ is a *factor* of an (in)finite word w if there is an index n such that $\langle w_n, \dots, w_{n+k} \rangle = \langle w'_0, \dots, w'_k \rangle$. We let $|w|$ denote the length of a finite word w .

An infinite word w is *recursive* (or *computable*) if one can compute w_j for every $j \geq 0$, and is *disjunctive* if each $w' \in \Sigma^*$ appears infinitely often as a factor of w . Other authors occasionally use the terminology *weakly normal* or *rich* instead of disjunctive. An infinite word w is *periodic* if $w = v^\omega$ for some $v \in \Sigma^+$ and *ultimately periodic* if $w = uv^\omega$ for some $u, v \in \Sigma^*$. Here, for the smallest possible such u and v , $|u|$ and $|v|$ are referred to as the *preperiod* and *period*, respectively.

A *deterministic Muller automaton* $\mathcal{A} = (\Sigma, Q, q_{\text{init}}, \delta, \mathcal{F})$ consists of an alphabet Σ , a finite set of states Q , an initial state $q_{\text{init}} \in Q$, a transition function $\delta: Q \times \Sigma \rightarrow Q$, and an accepting family of sets $\mathcal{F} \subseteq 2^Q$. The *run* of $w \in \Sigma^* \cup \Sigma^\omega$ on $\mathcal{A}$ is the sequence of states visited while reading w starting in q_{init} and repeatedly updating the state using the transition function. We say that $\mathcal{A}$ *accepts* $w \in \Sigma^\omega$ if the set of states visited infinitely often upon reading w belongs to $\mathcal{F}$. The *acceptance problem* of a recursive word $w \in \Sigma^\omega$ is the question of determining, given a deterministic Muller automaton $\mathcal{A}$ with alphabet Σ , whether $\mathcal{A}$ accepts w . We denote the acceptance problem by Acc_w .

Berthé et al. established the following [3, Thm. 4.16]:

► **Theorem 5.** *If $w \in \Sigma^\omega$ is recursive and disjunctive, then Acc_w is decidable.*

A *deterministic finite transducer* $\mathcal{B} = (\Sigma_{\text{in}}, \Sigma_{\text{out}}, Q, q_{\text{init}}, \delta)$ is given by an input alphabet Σ_{in} , output alphabet Σ_{out} , set of states Q , initial state $q_{\text{init}} \in Q$, and transition function $\delta: Q \times \Sigma_{\text{in}} \rightarrow Q \times \Sigma_{\text{out}}^*$. The transducer $\mathcal{B}$ starts in state q_{init} . It reads a word $w \in \Sigma_{\text{in}}^* \cup \Sigma_{\text{in}}^\omega$ and upon reading letter a whilst in state q , it computes $(q', w') = \delta(q, a)$, moves to state q' , and concatenates w' to the output string. Write $\mathcal{B}(w) \in \Sigma_{\text{out}}^* \cup \Sigma_{\text{out}}^\omega$ to denote the output word thus computed upon reading $w \in \Sigma_{\text{in}}^* \cup \Sigma_{\text{in}}^\omega$.

We now recall a Turing-reducibility property between word acceptance problems [3, Lem. 4.5]:

► **Lemma 6.** *Let $w \in \Sigma^\omega$ and $\mathcal{B}$ be a deterministic finite transducer. Then the problem $\text{Acc}_{\mathcal{B}(w)}$ reduces to Acc_w .*

2.2 Monadic Second-Order Logic

A (*unary or monadic*) *predicate* P is a function $P: \mathbb{N} \rightarrow \{0, 1\}$, which equivalently we can interpret as a subset $P \subseteq \mathbb{N}$. For $P \subseteq \mathbb{N}$ an infinite predicate, let us write $\langle p_m \rangle_{m=0}^\infty$ to denote the enumeration of P in increasing order, i.e., such that p_{m-1} is the m th smallest element of P . The *characteristic word* $w \in \{0, 1\}^\omega$ of P is obtained by setting $w_n = P(n)$. We then have:

$$w = 0^{p_0} 10^{p_1-p_0-1} 10^{p_2-p_1-1} 10^{p_3-p_2-1} \dots \quad (5)$$

A predicate P is *sparse* if for every $N \geq 0$, there is $M \geq 0$ such that $p_{m+1} - p_m \geq N$ for all $m \geq M$. The predicate is *effectively sparse* if M can always be computed from N .

Monadic second-order logic (MSO) is an extension of first-order logic over signature $\{=, <, \in\}$ that allows quantification over subsets of the universe $\mathbb{N}$. We also consider expansions of MSO by various fixed unary predicates $P \subseteq \mathbb{N}$; in other words (abusing notation), the signature is expanded by a predicate symbol P , with interpretation the given subset $P \subseteq \mathbb{N}$. We refer the reader to [4] for a thorough contemporary overview of MSO.

The deep connection between MSO and automata theory was brought to light in the seminal work of Büchi; see, for example, [27, Thms. 5.4 and 5.9].

► **Theorem 7.** *The decidability of the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is Turing equivalent to Acc_w , where w is the characteristic word of P .*

As noted earlier, Elgot and Rabin devised the *contraction method* to establish decidability of the MSO theory of $\langle \mathbb{N}; <, P \rangle$, for various “arithmetic” predicates P . The following proposition is a variation on their method:

► **Proposition 8.** *Let $P \subseteq \mathbb{N}$ be an infinite, recursive, and effectively sparse predicate with enumeration $\langle p_m \rangle_{m=0}^\infty$. If, for each $M \geq 2$, $\text{Acc}_{\langle p_m \bmod M \rangle_{m=0}^\infty}$ is decidable, the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is decidable.*

Proof. By Thm. 7, it is sufficient to be able to decide whether a deterministic Muller automaton $\mathcal{A} = (\{0, 1\}, Q, q_{\text{init}}, \delta, \mathcal{F})$ accepts the characteristic word (5). Let us restrict $\mathcal{A}$ to a directed graph G with nodes Q and 0-transitions as arrows.

By construction, every node in G has outdegree 1 and so each state is in at most one cycle in G . We can therefore compute the least common multiple of the cycle lengths in G (call this number M) and the longest path to a cycle (call this number N). Then, for all states q and numbers $n \geq M + N$ and $d \geq 1$, reading 0^n and 0^{n+dM} leads to journeying through the exact same set of states and ending up in the same state.

Let K be such that $p_{m+1} - p_m \geq M + N + 1$ for all $m \geq K$ (which can be computed as P is effectively sparse). We construct a deterministic finite transducer $\mathcal{B}$ that hard-codes the initial segment $w_{\text{init}} := 0^{p_0} 10^{p_1 - p_0 - 1} 1 \dots 0^{p_{K+1} - p_K - 1} 1$. For $m \geq K$, after reading $(p_m \bmod M)$ and $(p_{m+1} \bmod M)$, $\mathcal{B}$ outputs $0^{k_m} 1$, where $M + N < k_m \leq 2M + N$ is congruent to $p_{m+1} - p_m - 1$ modulo M . Then, by construction, a state q is visited infinitely often upon reading the characteristic word of P if and only if q is visited infinitely often when $\mathcal{A}$ reads $w_{\text{init}} \mathcal{B}(\langle p_m \bmod M \rangle_{m=K+1}^\infty)$.

Recall that $\text{Acc}_{\langle p_m \bmod M \rangle_{m=0}^\infty}$ is assumed to be decidable. Then $\text{Acc}_{\langle p_m \bmod M \rangle_{m=K+1}^\infty}$ is also decidable (by hard-coding the initial segment) and thus $\text{Acc}_{\mathcal{B}(\langle p_m \bmod M \rangle_{m=K+1}^\infty)}$ is decidable by Thm. 6. Therefore $\text{Acc}_{w_{\text{init}} \mathcal{B}(\langle p_m \bmod M \rangle_{m=K+1}^\infty)}$ is decidable (by again hard-coding the initial segment), and by construction, $\mathcal{A}$ accepts the characteristic word of P if and only if $\mathcal{A}$ accepts $w_{\text{init}} \mathcal{B}(\langle p_m \bmod M \rangle_{m=K+1}^\infty)$. Hence Acc_w is decidable, as required. ◀

2.3 Linear Recurrence Sequences

A number $\alpha \in \mathbb{C}$ is *algebraic* if $F(\alpha) = 0$ for some non-zero polynomial $F \in \mathbb{Z}[X]$. The unique such polynomial (up to multiplication by a constant) of least degree is the *minimal polynomial* of α . We write $\overline{\mathbb{Q}}$ to denote the field of algebraic numbers.

A *linear recurrence sequence* over a ring R (an *R-LRS*) is a sequence $\langle u_n \rangle_{n=0}^\infty \in R^\omega$ such that there are numbers $c_1, \dots, c_d \in R$, with $c_d \neq 0$, having the property that, for all $n \in \mathbb{N}$,

$$u_{n+d} = c_1 u_{n+d-1} + \dots + c_d u_n.$$

The entire sequence is therefore completely specified by the $2d$ numbers $c_1, \dots, c_d$ and $u_0, \dots, u_{d-1}$. Although there may be several such recurrence relations, we shall assume that

we are always dealing with the (unique) one for which d is minimal. In the remainder of the paper, whenever R is not specified, we are working over the ring of integers $\mathbb{Z}$. The *characteristic polynomial* of the LRS is given by $F(X) = X^d - c_1 X^{d-1} - \dots - c_d \in R[X]$. The *characteristic roots* of the LRS are the roots of its characteristic polynomial, and the *multiplicity* of a characteristic root λ is its multiplicity as a root of $F(X)$. Every $\overline{\mathbb{Q}}$ -LRS $\langle u_n \rangle_{n=0}^\infty$ with characteristic roots $\lambda_1, \dots, \lambda_K$ admits a unique *exponential-polynomial* representation given by

$$u_n = \sum_{k=1}^K Q_k(n) \lambda_k^n,$$

where $Q_k \in \overline{\mathbb{Q}}[X]$ has degree the multiplicity of λ_k minus 1. A $\overline{\mathbb{Q}}$ -LRS is *simple* if all its characteristic roots have multiplicity 1, and is *non-degenerate* if no quotient of two distinct characteristic roots is a root of unity.

A characteristic root λ is *dominant* if $|\lambda| \geq |\mu|$ for all characteristic roots μ . We define the *dominant part* $\langle v_n \rangle_{n=0}^\infty$ of $\langle u_n \rangle_{n=0}^\infty$ by writing

$$v_n = \sum_{\lambda_j \text{ dominant}} Q_j(n) \lambda_j^n,$$

with the *non-dominant part* $\langle r_n \rangle_{n=0}^\infty$ given by $\langle u_n - v_n \rangle_{n=0}^\infty$. One can compute positive real numbers r and R such that $rR^n > |r_n|$ for all $n \in \mathbb{N}$ and $R < |\lambda|$ for λ a dominant characteristic root, see, e.g., [3, Lem. 2.5].

For every $M \geq 2$ and $\mathbb{Z}$ -LRS $\langle u_n \rangle_{n=0}^\infty$, the sequence $\langle u_n \bmod M \rangle_{n=0}^\infty$ is ultimately periodic and one can effectively compute its period and preperiod [3, Lem. 2.6].

► **Example 9.** Let $\langle u_n \rangle_{n=0}^\infty$ be the $(\mathbb{Z})$ -LRS (1) from Sec. 1. The characteristic polynomial of $\langle u_n \rangle_{n=0}^\infty$ is

$$F(X) = X^3 - 6X^2 + 13X - 10 = (X - 2)(X - (2 + i))(X - (2 - i)).$$

The characteristic roots of $\langle u_n \rangle_{n=0}^\infty$ are 2, $2 + i$, and $2 - i$. Using linear algebra, one easily recovers the exponential-polynomial representation (2). The LRS $\langle u_n \rangle_{n=0}^\infty$ is simple and non-degenerate. Its dominant part is the sequence defined by $v_n = \frac{1}{2}(2 + i)^n + \frac{1}{2}(2 - i)^n$, while its non-dominant part is given by $r_n = 2^n$.

2.4 Number Theory

Our main number-theoretic tool is Baker's theorem on linear forms in logarithms. Specifically, we make use of a flexible version due to Matveev along with some off-the-shelf applications due to Mignotte, Shorey, and Tijdeman.

Let $\alpha \neq 0$ be an algebraic number of degree d with minimal polynomial $F(X) = a_0 \prod_{i=1}^d (X - \alpha_i)$. The *logarithmic Weil height* of α is defined as

$$h(\alpha) = \frac{1}{d} \left(\log |a_0| + \sum_{i=1}^d \log \max\{|\alpha_i|, 1\} \right).$$

Furthermore, set $h(0) = 0$. For all algebraic numbers $\alpha_1, \dots, \alpha_k$ and $n \in \mathbb{Z}$, we have the following properties:

$$\begin{aligned} h(\alpha_1 + \dots + \alpha_k) &\leq \log k + h(\alpha_1) + \dots + h(\alpha_k), \\ h(\alpha_1 \alpha_2) &\leq h(\alpha_1) + h(\alpha_2), \quad \text{and} \\ h(\alpha_1^n) &\leq |n| h(\alpha_1). \end{aligned}$$

A *number field* L is a field extension of $\mathbb{Q}$ such that the degree of $L/\mathbb{Q}$ is finite. If $\alpha_1, \dots, \alpha_d \in \overline{\mathbb{Q}}$, $L = \mathbb{Q}(\alpha_1, \dots, \alpha_d)$ is a number field whose degree can be effectively computed.

Let L be a number field of degree D , $M \geq 1$, $\alpha_1, \dots, \alpha_M \in L^*$, and $b_1, \dots, b_M \in \mathbb{Z}$. Then set $B = \max\{|b_1|, \dots, |b_M|\}$,

$$\Lambda = \prod_{j=1}^M \alpha_j^{b_j} - 1, \quad \text{and} \quad h'(\alpha_j) = \max\{Dh(\alpha_j), |\log \alpha_j|, 0.16\}.$$

Matveev [19] proved the following:

► **Theorem 10.** *If $\Lambda \neq 0$, then*

$$\log |\Lambda| > -3 \cdot 30^{M+4} (M+1)^{5.5} D^2 (1 + \log D) \cdot (1 + \log(MB)) \prod_{j=1}^d h'(\alpha_j).$$

In particular, there is a computable constant c such that when $\Lambda \neq 0$, $|\Lambda| > B^{-c}$.

We will also need the following results from Mignotte, Shorey, and Tijdeman [28]:

► **Theorem 11.** *Let $\langle u_n \rangle_{n=0}^\infty$ be a non-degenerate LRS with two dominant roots of magnitude $|\lambda|$. Then there are computable positive constants C_1 and C_2 such that*

$$|u_n| \geq |\lambda|^n \cdot n^{-C_1 \log(n)}$$

whenever $n \geq C_2$.

► **Theorem 12.** *Let $\langle u_n \rangle_{n=0}^\infty$ be a non-degenerate LRS with two dominant roots of magnitude $|\lambda|$. Then there are computable positive constants C_3 and C_4 such that*

$$|u_{n_1} - u_{n_2}| \geq |\lambda|^{n_1} \cdot n_1^{-C_3 \log(n_1) \log(n_2+2)}$$

whenever $n_1 > n_2$ and $n_1 \geq C_4$.

3 Proof of the Main Result

In this section, we prove Thm. 1: the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is decidable whenever P is a predicate comprising the set of positive terms of some non-degenerate, simple, integer-valued LRS having two dominant characteristic roots.

We begin in Sec. 3.1 by untangling the definition of an LRS satisfying the above hypotheses and reduce Thm. 1 to Thm. 4. We then provide intuition underlying the proof of the latter through an extended example in Sec. 3.2, and consider a continuous version of our problem in Sec. 3.3. Finally, in the same section, we establish Thm. 4.

3.1 Reduction to Prodisjunctivity

Let $\langle u_n \rangle_{n=0}^\infty$ be an LRS satisfying the hypotheses of Thm. 1. We first record some elementary observations whose proof is in the full version.

► **Lemma 13.** *Assume that $\langle u_n \rangle_{n=0}^\infty$ is an LRS satisfying the hypotheses of Thm. 1 and whose two dominant roots are λ_1 and λ_2 . Then $\lambda_2 = \overline{\lambda_1}$, the argument of λ_1 is not a rational multiple of π , and $|\lambda_1| > 1$.*

When writing $\langle u_n \rangle_{n=0}^\infty$ in its exponential-polynomial form, we split it into its dominant part $\langle v_n \rangle_{n=0}^\infty$ and non-dominant part $\langle r_n \rangle_{n=0}^\infty$:

$$u_n = v_n + r_n = \alpha \lambda^n + \overline{\alpha} \overline{\lambda}^n + r_n. \tag{6}$$

Here, α and λ are algebraic numbers with $\alpha \neq 0$ (as otherwise λ and $\bar{\lambda}$ would not be characteristic roots, i.e., roots of the polynomial corresponding to the *minimal* recurrence relation that $\langle u_n \rangle_{n=0}^\infty$ obeys), $|\lambda| > 1$, and the argument of λ is not a rational multiple of π . We keep λ , α , and $\langle r_n \rangle_{n=0}^\infty$ fixed for the remainder of the paper.

Recall that $P = \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$ and $\langle p_m \rangle_{m=0}^\infty$ is an enumeration of P in increasing order. To apply Prop. 8, we need the following lemma, whose proof relies heavily on the results of Mignotte, Shorey, and Tijdeman from Sec. 2.3 and can be found in the full version.

► **Lemma 14.** *Let $P \subseteq \mathbb{N}$ be as per Thm. 1. Then P is infinite, recursive, and effectively sparse.*

By Prop. 8, it now suffices to prove that for all $M \geq 2$, one can decide $\text{Acc}_{\langle p_m \bmod M \rangle_{m=0}^\infty}$ (determine whether a given deterministic Muller automaton $\mathcal{A}$ over alphabet $\{0, \dots, M-1\}$ accepts $\langle p_m \bmod M \rangle_{m=0}^\infty$). The next lemma shows how the effective prodisjunctivity of $\langle p_m \rangle_{m=0}^\infty$ asserted by Thm. 4 enables us to do this. Its proof can be found in the full version.

► **Lemma 15.** *Theorem 4 implies Thm. 1, i.e., if $\langle u_n \rangle_{n=0}^\infty$ is an LRS satisfying the conditions of Thm. 1, $P := \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$, and the enumeration of P is prodisjunctive, then the MSO theory of the structure $\langle \mathbb{N}; <, P \rangle$ is decidable.*

Theorem 4 asserts that, for any $M \geq 2$, the sequence $\langle p_m \bmod M \rangle_{m=N_M}^\infty \in S_M^\omega$ is disjunctive. Let us unpack this definition. We have that $\langle p_m \bmod M \rangle_{m=N_M}^\infty \in S_M^\omega$ is disjunctive if for any $\ell \geq 1$, every pattern $\langle s_1, \dots, s_\ell \rangle \in S_M^\ell$ appears infinitely often in $\langle p_m \bmod M \rangle_{m=N_M}^\infty$. That is, for all $\ell, N \in \mathbb{N}$ with $N \geq N_M$ and $s_1, \dots, s_\ell \in S_M$, there are $n_1, \dots, n_\ell \in \mathbb{N}$ such that

1. $n_1, \dots, n_\ell \geq N$;
2. for all $1 \leq i \leq \ell$, $u_{n_i} \equiv s_i \pmod{M}$;
3. $0 \leq u_{n_1} < \dots < u_{n_\ell}$;
4. for all $m \geq 0$ such that $u_{n_1} \leq u_m \leq u_{n_\ell}$, $u_m \in \{u_{n_1}, \dots, u_{n_\ell}\}$.

As the dominant part $\langle v_n \rangle_{n=0}^\infty$ (where $v_n = \alpha\lambda^n + \bar{\alpha}\bar{\lambda}^n$, see (6)) only relies on two algebraic numbers, α and λ , it is easier to work with $\langle v_n \rangle_{n=0}^\infty$ than $\langle u_n \rangle_{n=0}^\infty$. In the following lemma, we prove that we can actually effect this change.

► **Lemma 16.** *Assume that for all natural numbers $\ell, N, T \geq 2$, and $t_1, \dots, t_\ell \in \{0, \dots, T-1\}$, there are $n_1, \dots, n_\ell \in \mathbb{N}$ such that*

1. $n_1, \dots, n_\ell \geq N$;
2. for all $1 \leq j \leq \ell$, $n_j \equiv t_j \pmod{T}$;
3. $0 < v_{n_1} < \dots < v_{n_\ell}$;
4. for all $m \geq 0$ such that $v_{n_1} < v_m < v_{n_\ell}$, $m \in \{n_2, \dots, n_{\ell-1}\}$.

Then the enumeration $\langle p_m \rangle_{m=0}^\infty$ of $P := \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$ is effectively prodisjunctive.

Proof. We claim that for some computable number N' , $u_{m_1} < u_{m_2}$ if and only if $v_{m_1} < v_{m_2}$ whenever $m_1, m_2 \geq N'$. Suppose not. Then, without loss of generality, $m_1 > m_2$ and $|v_{m_1} - v_{m_2}| < |r_{m_1}| + |r_{m_2}| < 2rR^{m_1}$. But Thm. 12 implies that for $m_1 \geq C_4$,

$$\begin{aligned} \log(2r) + m_1 \log R &> \log |v_{m_1} - v_{m_2}| \\ &> m_1 \log |\lambda| - C_3 \log(m_1)^2 \log(m_2 + 2) \\ &> m_1 \log |\lambda| - C_3 \log(m_1 + 1)^3, \end{aligned}$$

which cannot hold for $m_1 \geq N'$ for some computable $N' \in \mathbb{N}$ as $\log |\lambda| > \log |R|$. Our claim therefore follows.

Assume that $\langle u_n \bmod M \rangle_{n=0}^\infty$ has period T (which can be effectively computed). If $s_1, \dots, s_\ell \in S$ and $1 \leq j \leq \ell$, there exists a $t_j \in \{0, \dots, T-1\}$ such that $u_{nT+t_j} \equiv s_j \pmod{M}$ whenever n is large enough. Therefore, if $n_1, \dots, n_\ell \in \mathbb{N}$ are at least $\max\{N, N'\}$ and satisfy the hypotheses of the lemma, it follows that $0 \leq u_{n_1} < \dots < u_{n_\ell}$ and for all $m \in \mathbb{N}$ such that $u_{n_1} < u_m < u_{n_\ell}$, $m \in \{n_2, \dots, n_{\ell-1}\}$. In other words, if $p_m = u_{n_1}$, then for $2 \leq j \leq \ell$, $p_{m+j-1} = u_{n_j}$ and $p_{m+j-1} = u_{n'T+t_j} \equiv s_j \pmod{M}$ for some $n' \in \mathbb{N}$. ◀

As $|\alpha| \neq 0$ and Lem. 16 is only concerned with inequalities $v_{n_1} < v_{n_2}$ and $v_{n_1} > 0$ for natural numbers n_1 and n_2 , we can scale v_n by $1/|2\alpha|$. That is, we can assume that $|\alpha| = 1/2$. Write $\alpha = \frac{1}{2}e^{i\phi}$ and $\lambda = |\lambda|e^{i\theta}$. Thus, $v_n = \cos(\theta n + \phi)|\lambda|^n$.

Let us now sketch the method we will use to establish the hypothesis of Lem. 16 whose proof relies heavily on the following notation.

► **Definition 17.** For integers $d \neq 0$ and real numbers $0 < \gamma < \delta$, define $\mathcal{J}_d(\gamma, \delta) \subset \mathbb{R}/(2\pi\mathbb{Z})$ as

$$\mathcal{J}_d(\gamma, \delta) = \left\{ x \in \mathbb{R}/(2\pi\mathbb{Z}) : 0 < \gamma \cos(x) < \cos(x + d\theta)|\lambda|^d < \delta \cos(x) \right\}.$$

Moreover, we define $J_d(0, \delta)$ to stand for the limit of $\mathcal{J}_d(\gamma, \delta)$ as γ tends to 0.

In Lem. 18, we can quantify the size of these intervals. For a real number x , let $|x|_{2\pi}$ denote the distance of x to the nearest integer multiple of 2π . The proof of Lem. 18 can be found in the full version.

► **Lemma 18.** One can compute constants C_5, C_6, C_7 , and C_8 such that for all $0 < \gamma < \delta < \sqrt{|\lambda|}$ and all $d \geq 1$, $\mathcal{J}_d(\gamma, \delta)$ consists of a single interval,

$$C_6 \frac{\delta - \gamma}{|\lambda|^d d^{C_7}} < |\mathcal{J}_d(\gamma, \delta)| < C_5 \frac{\delta - \gamma}{|\lambda|^d},$$

and $|x - (-d\theta \pm \pi/2)|_{2\pi} < C_8 |\lambda|^{-d}$ for any $x \in \mathcal{J}_d(\gamma, \delta)$.

We now continue with the most technical step in the proof of Thm. 1: establishing a continuous version of the hypothesis of Lem. 16. Items 3 and 4 of Lem. 16 involve terms of the form v_n , and we can divide them by $|\lambda|^{n_1}$. Further, for $2 \leq j \leq \ell$, we set $b_j := n_j - n_1$ and $x = n\theta + \phi$. Then, item 3 turns into

$$0 < \cos(x) < \cos(x + b_2\theta)|\lambda|^{b_2} < \dots < \cos(x + b_\ell\theta)|\lambda|^{b_\ell} \quad (7)$$

and item 4 turns into

$$\forall d \in \mathbb{Z}: \cos(x) < \cos(x + d\theta)|\lambda|^d < \cos(b_\ell\theta)|\lambda|^{b_\ell} \implies d \in \{b_2, \dots, b_{\ell-1}\}. \quad (8)$$

We want to find an interval $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$ and numbers b_j such that $b_j \equiv t_j - t_1 \pmod{T}$ (for item 2), (7) holds for all $x \in \mathcal{I}$, and (8) hold for “most” $x \in \mathcal{I}$. This leads us to the following:

► **Lemma 19.** Let $\ell, T \geq 2$ and $t_1, \dots, t_\ell \in \{0, \dots, T-1\}$. Then there are an interval $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$, natural numbers $D, b_2, \dots, b_\ell \geq 1$, and real numbers $1 < \delta_2 < \dots < \delta_\ell < \sqrt{|\lambda|}$ such that

- (a) for all $2 \leq j \leq \ell$, $b_j \equiv t_j - t_1 \pmod{T}$;
- (b) for all $x \in \mathcal{I}$,

$$\begin{aligned} 0 &< \cos(x) < \cos(x + b_2\theta)|\lambda|^{b_2} < \delta_2 \cos(x) \\ &< \cos(x + b_3\theta)|\lambda|^{b_3} < \delta_3 \cos(x) \\ &\vdots \\ &< \cos(x + b_\ell\theta)|\lambda|^{b_\ell} < \delta_\ell \cos(x); \end{aligned} \quad (9)$$

- (c) for all integers $d < D$ not in the set $\{b_2, \dots, b_{\ell-1}\}$, $\mathcal{I} \cap \mathcal{J}_d(1, \delta_\ell) = \emptyset$;
 (d) $\sum_{d=D}^{\infty} |\mathcal{J}_d(1, \delta_\ell)| < |\mathcal{I}|$.

Translating (b) in the notation of intervals $\mathcal{J}$, we have that

$$\mathcal{I} \subseteq (-\pi/2, \pi/2) \cap \mathcal{J}_{b_2}(1, \delta_2) \cap \mathcal{J}_{b_3}(\delta_2, \delta_3) \cap \dots \cap \mathcal{J}_{b_\ell}(\delta_{\ell-1}, \delta_\ell).$$

The proof of Lem. 19 is in the full version. The remaining tools we need for this proof are listed in Sec. 3.3. Finally, we derive Thm. 1 from Lem. 19. But first, in the upcoming section we go through an example to recap the construction.

3.2 An Extended Example

Let $\langle u_n \rangle_{n=0}^\infty$ be the sequence (1) from Sec. 1 and assume $M = 5$. Let us study the sequence $u_n = \frac{1}{2}(2+i)^n + \frac{1}{2}(2-i)^n + 2^n$ modulo 5.

From (4), we conclude that $S_5 = \{0, 2, 4\}$ and $T = 4$ (that is, $\langle u_n \bmod 5 \rangle_{n=0}^\infty$ is ultimately periodic with period $T = 4$, and $\{0, 2, 4\}$ are exactly the congruence classes that appear infinitely often in $\langle u_n \bmod 5 \rangle_{n=0}^\infty$). Thus for all $m \geq 0$, $p_m \bmod 5 \in \{0, 2, 4\}$, where $\langle p_m \rangle_{m=0}^\infty$ is the enumeration of $P := \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$. Then Thm. 4 asserts that every $\langle s_1, \dots, s_\ell \rangle \in S_5^*$ appears in $\langle p_m \bmod 5 \rangle_{m=0}^\infty$ infinitely often as a factor. We will show that this indeed holds when $\ell = 3$ and $\langle s_1, s_2, s_3 \rangle = \langle 0, 0, 0 \rangle$.

Let us compute t_1 , t_2 , and t_3 (the conjugacy classes modulo $T = 4$ such that for large enough n , $u_{Tn+t_i} \equiv s_i \bmod 5$). In view of (4), we are forced to take $t_i = 3$ for $i = 1, 2, 3$ as $s_i = 0$. Thus, to find $\langle 0, 0, 0 \rangle$ in $\langle p_m \rangle_{m=0}^\infty$, we want to find $n_1, n_2, n_3 \in \mathbb{N}$ congruent to 3 modulo 4 such that $0 < u_{n_1} < u_{n_2} < u_{n_3}$, and if $u_{n_1} < u_m < u_{n_3}$ for some $m \geq 0$, then $m \in \{n_2\}$ (i.e., $m = n_2$).

By (2), the dominant part $\langle v_n \rangle_{n=0}^\infty$ of $\langle u_n \rangle_{n=0}^\infty$ is given by $v_n = \frac{1}{2}(2+i)^n + \frac{1}{2}(2-i)^n$ and the non-dominant part $\langle r_n \rangle_{n=0}^\infty$ by $r_n = 2^n$. As shown in Lem. 16, we can work with $v_n = \alpha\lambda^n + \bar{\alpha}\bar{\lambda}^n = \cos(n\theta + \phi)|\lambda|^n$ instead of u_n for large enough n . Here, we have that $\lambda = e^{i\theta}|\lambda| = 2+i$ and $\alpha = \frac{1}{2}e^{i\phi} = \frac{1}{2}$. Thus, in this example, $\phi = 0$.

Hence, for a given $N \in \mathbb{N}$ (for simplicity, let us take $N = 0$) we wish to find $n_1, n_2, n_3 \geq N$ that are congruent to 3 modulo 4, satisfy

$$0 < \cos(n_1\theta) < \cos(n_2\theta)|\lambda|^{n_2-n_1} < \cos(n_3\theta)|\lambda|^{n_3-n_1},$$

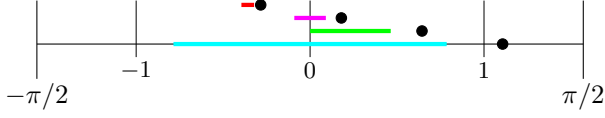
and such that $m = n_2$ for any $m \in \mathbb{N}$ satisfying the inequality $\cos(n_1\theta) < \cos(m\theta)|\lambda|^{m-n_1} < \cos(n_3\theta)|\lambda|^{n_3-n_1}$. This is the statement of Lem. 16.

Next, we aim to find $b_2, b_3 \in \mathbb{N}$ such that $n_1 = n$, $b_2 = n_2 - n$, and $b_3 = n_3 - n$ for some $n \geq N$ congruent to 3 modulo 4 that satisfies our hypotheses. To ensure that for $j \in \{2, 3\}$, $n_j \equiv t_j \equiv 3 \pmod{4}$, we have to require that $b_j \equiv 0 \pmod{4}$.

In order to solve this discrete problem (find natural numbers n_1, n_2, n_3 meeting these constraints), we first want to solve a continuous variant of this problem: find b_2 and b_3 and an interval $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$ such that for $x \in \mathcal{I}$, these properties hold “often”. We will construct an open, non-empty interval $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$ such that for all $x \in \mathcal{I}$,

$$0 < \cos(x) < \cos(x + b_2\theta)|\lambda|^{b_2} < \cos(x + b_3\theta)|\lambda|^{b_3}. \quad (10)$$

We cannot ensure that for all $x \in \mathcal{I}$ and $m \in \mathbb{Z}$, $\cos(x) < \cos(x + m\theta)|\lambda|^m < \cos(x + b_3\theta)|\lambda|^{b_3}$ implies that $m = b_2$. However, we can ensure that it happens for “many” $x \in \mathcal{I}$, including for infinitely many numbers of the form $x = n\theta$, where $n \equiv 3 \pmod{4}$.



■ **Figure 1** Let $\lambda = 1 + 2i$. Then for $d = 1, 2, 3, 4$, $\mathcal{J}_d(1, 3)$ are drawn in cyan, green, magenta, and red, respectively, and $|\mathcal{J}_d(1, 3)|$ are $\pi/2, 0.464, 0.182, 0.073$, respectively. As some of the intervals overlap, we have stacked them vertically for visual purposes. The points in black mark out $-d\theta \pm \pi/2$ for the corresponding value of d .

We can translate the last part into the notation of the intervals $\mathcal{J}_d(\gamma, \delta)$. Then, arbitrarily setting $\delta_2 = 1.95$ and $\delta_3 = 2$, we strengthen (10) in the form of item (b) in Lem. 19: we want that for all $x \in \mathcal{I}$,

$$0 < \cos(x) < \cos(x + b_2\theta)|\lambda|^{b_2} < 1.95 \cos(x) < \cos(x + b_3\theta)|\lambda|^{b_3} < 2 \cos(x).$$

Thus, $I \subseteq (-\pi/2, \pi/2)$ (as $\cos(x) > 0$ and $x \in \mathcal{I}$), $I \subseteq \mathcal{J}_{b_2}(1, 1.95)$ (as $1 \cdot \cos(x) < \cos(x + b_2\theta)|\lambda|^{b_2} < 1.95 \cos(x)$), and similarly, $I \subseteq \mathcal{J}_{b_3}(1.95, 2)$.

Dealing with items (c) and (d) of Lem. 19 is harder. In Lem. 18, we have proven many useful results on the structure of the sets $\mathcal{J}_d(\gamma, \delta)$. For $d \in \mathbb{Z}$ and small enough δ , if $\mathcal{J}_d(\gamma, \delta)$ is non-empty, it is a single interval and $|\mathcal{J}_d(\gamma, \delta)| = O((\delta - \gamma)|\lambda|^{-d})$. Hence, item (d) of Lem. 19 can easily be estimated using a geometric series:

$$\sum_{d=D}^{\infty} |\mathcal{J}_d(1, \delta_\ell)| \leq O(\delta_\ell |\lambda|^{-D}).$$

Moreover, every point in $\mathcal{J}_d(\gamma, \delta)$ is at most $O(\delta|\lambda|^{-d})$ away from $-d\theta \pm \pi/2$ in $\mathbb{R}/(2\pi\mathbb{Z})$. We illustrate this in Fig. 1.

As we have guessed $\delta_2 = 1.95$ and $\delta_3 = 2$, we will construct $\mathcal{I}$ inductively as

$$\mathcal{I} := \mathcal{I}_3 := \mathcal{J}_{b_3}(1.95, 2) \subseteq \mathcal{I}_2 := \mathcal{J}_{b_2}(1, 1.95) \subseteq \mathcal{I}_1.$$

At each step $i = 1, 2, 3$, the items (a) and (b) hold for $j \leq i$ while items (c) and (d) also hold for the interval $\mathcal{I}_i$.

First, for $i = 1$, we take $\mathcal{I}_1 := (-1.1, 1.1) \subset (-\pi/2, \pi/2)$. Then, for an integer $d < 0$ and $x \in \mathcal{I}_1$, we have that $\cos(x + \theta d)|\lambda|^d < \cos(x)$. So in item (c), we can take $D = 1$. As $\delta_3 = 2$, we can prove that item (d) is satisfied:

$$\left| \bigcup_{d=1}^{\infty} \mathcal{J}_d(1, \delta_3) \right| \leq \sum_{d=1}^{\infty} |\mathcal{J}_d(1, \delta_3)| < |\mathcal{I}_1|. \quad (11)$$

For $i = 2$, recall that $\delta_2 = 1.95$ and that b_2 has to satisfy $\mathcal{J}_{b_2}(1, 1.95) \subset \mathcal{I}_1$ and $b_2 \equiv 0 \pmod{4}$. We pick $b_2 = 4$, being the smallest possible choice for b_2 . As shown in Fig. 2, we have that $\mathcal{I}_2$ is indeed in $\mathcal{I}_1$. For all integers $d \leq 20$ not equal to either 0 or 4, $\mathcal{I}_2 \cap \mathcal{J}_d(1, 2)$ is empty. As $\sum_{d=21}^{\infty} |\mathcal{J}_d(1, 2)| < |\mathcal{J}_4(1, 1.95)|$, $\mathcal{I}_2 := \mathcal{J}_4(1, 1.95)$ is not covered by the intervals $\mathcal{J}_d(1, 2)$ with $d \notin \{0, 4\}$. Hence, $D = 21$ is valid choice in this step of our inductive procedure.

For b_3 , recall that $b_3 \equiv 0 \pmod{4}$. We find that $\mathcal{J}_b(1.95, 2) \cap \mathcal{I}_2$ is non-empty for $b = 0, 4, 38, 99, 160, 309, 370, \dots$. The smallest such b that is not equal to 0 or 4 (which are already in use) and congruent to 0 modulo 4 is 160. Then,

$$\sum_{d=1, d \notin \{4, 160\}}^{\infty} |\mathcal{J}_d(1, 2) \cap \mathcal{J}_{160}(1.95, 2)| < |\mathcal{J}_{160}(1.95, 2)|$$

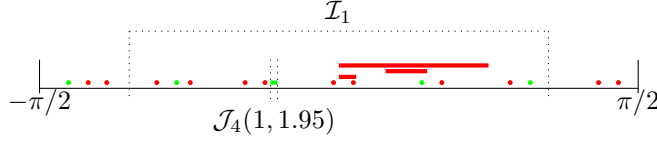


Figure 2 We drew the intersection of $\mathcal{I}_1$ and $\mathcal{J}_d(1, 1.95)$ for $d = 1, \dots, 20$ in red when $d \not\equiv 0 \pmod{4}$ and in green when $d \equiv 0 \pmod{4}$. For ease of visibility, $\mathcal{J}_d(1, 2)$ is positioned higher for $d = 1, 2, 3$, and for intervals $\mathcal{J}_d(1, 2)$ that are too small to draw, their position is marked out with a dot.

allows us to take $D = 160$ and $\mathcal{I} := \mathcal{J}_{160}(1.95, 2)$. This interval $\mathcal{I}$ is tiny: it has length approximately $5.7 \cdot 10^{-58}$. However, it satisfies the constraints in Lem. 19.

Now we must show that there is some $x = n\theta \in \mathcal{I}$ such that $n \equiv 3 \pmod{4}$ and item 4 of Lem. 16 holds, as the three other conditions are already satisfied.

Recall that for a real number x , $|x|_{2\pi}$ denotes the distance from x to the nearest integer multiple of 2π . If $x = n\theta$ and $n \geq N$, then items 1, 2 and 3 of Lem. 16 are satisfied. Assume that for n as above item 4 in Lem. 16 is not satisfied. Then $n\theta \in \mathcal{J}_d(1, 2)$ for some $d \in \mathbb{Z} \setminus \{0, 4, 160\}$. Hence, combining the information from Lem. 18 to the effect that $\mathcal{J}_d(1, 2)$ is close to $-d\theta \pm \pi/2$ modulo 2π , we have:

$$c_1 |\lambda|^{-d} > |n\theta - (-d\theta \pm \pi/2)|_{2\pi} > |d + n|^{-c_2} \quad (12)$$

for two constants c_1 (derived from Lem. 18) and $c_2 > 0$ (derived from Thm. 10).

As there are many $n\theta$ in $\mathcal{I}$ that are fairly “evenly” distributed, we are able to prove that (12) cannot hold for all n . In other words, there must be some n for which

$$0 < v_n < v_{n+4} < v_{n+160}$$

and $v_n < v_m < v_{n+160}$ implies that $m = n + 4$. Then, using the strategy of Lemma 16, we translate this back to the sequence $\langle u_n \rangle_{n=0}^\infty$ to give the required result when n is large enough. In particular, we can calculate that when taking

$$n = 218085867698737188268427463501308698889728969450963229999559,$$

we have that $n\theta \in \mathcal{I}$, $n \equiv 3 \pmod{4}$, and $u_n < u_m < u_{n+160}$ implies that $m = 4$. Thus, for some value $m \in \mathbb{N}$, $\langle p_m, p_{m+1}, p_{m+2} \rangle = \langle u_n, u_{n+4}, u_{n+160} \rangle$ where all three terms are divisible by 5. Thus, the pattern $\langle 0, 0, 0 \rangle$ does indeed appear in $\langle p_m \bmod 5 \rangle_{m=0}^\infty$.

However, this construction is far from optimal. Although our choices of $b_2 = 4$ and $b_3 = 160$ were as small as possible with our choice of δ_2 and δ_3 , δ_2 and δ_3 were not optimal choices. Still, that would give just a minor improvement as one has to be more careful with inequalities like (11). Then one can find that choosing $b_2 = 8$, $b_3 = 28$, and $n = 16958443$, we indeed get that there is no $m \in \mathbb{N} \setminus \{0, 8, 28\}$ such that u_m is between u_n , u_{n+b_2} and u_{n+b_3} . Meanwhile, $\cos(n\theta) \approx 0.404$, $\cos((n + b_2)\theta) \approx 94.5$ and $\cos((n + b_3)\theta) \approx 751$, and so one should have had chosen much larger δ_2 and δ_3 for which the general bounds in Lem. 18 fail.

3.3 Proof of the Main Theorems

In this section, we establish Thms. 4 and 1. We first prove two technical lemmas. These two lemmas will both serve to prove these theorems but also to prove Lem. 19, the continuous version of disjointivity.

For the first lemma, we want that to show that each interval in $\mathbb{R}/(2\pi\mathbb{Z})$ contains intervals $\mathcal{J}_d(0, \sqrt{|\lambda|})$ and numbers $n\theta + \phi$ for relatively small numbers d and n in a certain congruent class. The proof of this lemma is in the full version.

► **Lemma 20.** *Let $T \geq 2$. There is a number $C_9 > 0$ such that for every $t \in \{0, \dots, T-1\}$ and small enough interval $\mathcal{I} \subset (-\pi/2, \pi/2) \subset \mathbb{R}/(2\pi\mathbb{Z})$, there are $|\mathcal{I}|^{-C_9} \leq n_1, n_2 \leq 2|\mathcal{I}|^{-C_9}$ such that $n_1\theta + \phi \in \mathcal{I}$, $\mathcal{J}_{n_2}(0, \sqrt{|\lambda|}) \subset \mathcal{I}$ and $n_1, n_2 \equiv t \pmod{T}$.*

For the fourth condition of Lem. 19, we would like D to be large. That is, the smallest d such that $\mathcal{J}_d(1, \delta_\ell) \cap \mathcal{I} \neq \emptyset$ has to be quite large. This is hard to guarantee, and our solution is to show that we can find a subinterval $\mathcal{I}' \subset \mathcal{I}$ for which this number D is large. We show this in the following lemma whose proof is in the full version.

► **Lemma 21.** *Assume $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$, $b_2, \dots, b_\ell \in \mathbb{N}$, $1 < \delta_2 < \dots < \delta_\ell < \sqrt{|\lambda|}$ and $D > 0$ satisfy the assertions of Lem. 19. Then for every small enough $\varepsilon > 0$ there is a subinterval $\mathcal{I}'$ of $\mathcal{I}$ of length ε for which the assertions of Lem. 19 hold for these $b_2, \dots, b_\ell$ and $\delta_1, \dots, \delta_\ell$ and some $D' > \varepsilon^{-1/2}$.*

With these last two lemmas, we have gathered all the tool needed to prove Lem. 19, which is also done in the full version. The idea of this proof is as described in Sec. 3.2: we inductively construct the numbers $b_2, \dots, b_\ell$ and intervals

$$(-\pi/2, \pi/2) \supset \mathcal{I}_1 \supset \mathcal{I}_2 := \mathcal{I}_{b_2}(1, \delta_2) \supset \mathcal{I}_3 := \mathcal{I}_{b_3}(\delta_2, \delta_3) \supset \dots \supset \mathcal{I}_{b_\ell}(\delta_{\ell-1}, \delta_\ell)$$

such that on step i , we show that some b_i exists for which the lemma holds for $b_2, \dots, b_i$ and $\mathcal{I}_i$.

Having established the continuous version of our result in Lem. 19, we can solve the discrete version Thm. 4 and conclude Thm. 1: the MSO theory of the structure $\langle \mathbb{N}; <, \{u_n : n \in \mathbb{N}\} \cap \mathbb{N} \rangle$ is decidable. The proof shares some of the main ideas of the proof of Lem. 19.

Proof of Thms. 1 and 4. As Thm. 4 implies Thm. 1 thanks to Lem. 15, it is sufficient to prove Thm. 4. In turn, Lem. 16 states that Thm. 4 is implied by the following statement: for all $N \in \mathbb{N}$, $T \geq 2$ and $t_1, \dots, t_\ell \in \{0, \dots, T-1\}$, we can find $n_1, \dots, n_\ell \in \mathbb{N}$ such that

1. $n_1, \dots, n_\ell \geq N$;
2. $n_j \equiv t_j \pmod{T}$ for $1 \leq j \leq \ell$;
3. $0 < v_{n_1} < \dots < v_{n_\ell}$;
4. for all $m \in \mathbb{N}$ such that $v_{n_1} < v_m < v_{n_\ell}$, $m \in \{n_2, \dots, n_{\ell-1}\}$.

We will prove this statement for given N, T, ℓ , and $t_1, \dots, t_\ell$.

Lem. 19 gives numbers $b_2, \dots, b_\ell \in \mathbb{N}$, $1 < \delta_\ell < \sqrt{|\lambda|}$ and an interval $\mathcal{I}$. We take $n_1 = n$ and $n_j = n + b_j$ for $2 \leq j \leq \ell$.

When $n \geq N$, $n \equiv t_1 \pmod{T}$ and $n\theta + \phi \in \mathcal{I}$, imply items 1, 2, and 3. Indeed, items 2 and 3 hold for $n_1 = n$, and for $2 \leq j \leq \ell$, $n_j = n + b_j > n \geq N$ and

$$n_j \equiv n_1 + b_j \equiv n_1 + (t_j - t_1) \equiv t_j \pmod{T}.$$

For item 3, we have that as $n\theta + \phi \in \mathcal{I}$,

$$0 < \cos(n\theta + \phi) < \cos((n + b_2)\theta + \phi)|\lambda|^{b_2} < \dots < \cos((n + b_\ell)\theta + \phi)|\lambda|^{b_\ell}.$$

Multiplying these inequalities by $|\lambda|^n$ and noting that $\cos(m\theta + \phi)|\lambda|^m = v_m$ entails item 3.

Let $0 < \varepsilon < |\mathcal{I}|$ be small enough. Lemma 21 implies that there is an interval $\mathcal{I}_\varepsilon \subset \mathcal{I}$ of length ε such that $\mathcal{I}_\varepsilon \cap \mathcal{J}_d(1, \delta_\ell) = \emptyset$ for all $d < \varepsilon^{-1/2}$. By Lem. 20, there is a $\varepsilon^{-C_9} < n < 2\varepsilon^{-C_9}$ such that $n\theta + \phi \in \mathcal{I}_\varepsilon$ and $n \equiv t_1 \pmod{T}$. Thus, $n \geq N$ for small enough ε and items 1, 2, and 3 are satisfied.

Now assume that $m \notin \{n_2, \dots, n_{\ell-1}\}$ and $v_{n_1} < v_m < v_{n_\ell}$. Then, setting $d = m - n$, we have that $d \notin \{b_2, \dots, b_{\ell-1}\}$ and

$$0 < \cos(n\theta + \phi)|\lambda|^n < \cos((n+d)\theta + \phi)|\lambda|^{n+d} < \cos((n+b_\ell)\theta + \phi)|\lambda|^{n+b_\ell}.$$

As $n\theta + \phi \in \mathcal{I}_\varepsilon \subset \mathcal{I}$, $\cos((n+b_\ell)\theta + \phi)|\lambda|^{b_\ell} < \delta_\ell \cos(n\theta + \phi)$. Thus, $n\theta + \phi$ is in $\mathcal{J}_d(1, \delta_\ell)$ and so $d \geq \varepsilon^{-1/2}$ (which comes from Lem. 21).

By Lem. 18, $n\theta + \phi \in \mathcal{J}_d(1, \delta_\ell)$ and $-d\theta \pm \pi/2$ are at most $C_8|\lambda|^{-d}$ apart. Thus, for a constant c_1 derived from Thm. 10,

$$\begin{aligned} C_8|\lambda|^{-d} &\geq |(n\theta + \phi) - (-d\theta \pm \pi/2)|_{\pi/2} \\ &\geq |e^{i(n\theta + \phi) - (-d\theta \pm \pi/2)}| \\ &> \frac{\pi}{2}|n + d|^{-c_1}. \end{aligned}$$

Taking logarithms,

$$\log(C_8) + c_1 \log(n + d) > d \log |\lambda|.$$

As $d \geq \varepsilon^{-1/2}$ and $n \geq \varepsilon^{-C_9}$, we have that $n, d \geq 2$ for small enough ε . Then, $dn \geq n + d$ and so

$$\log(C_8) + c_1 \log(n) + c_1 \log(d) > d \log |\lambda|.$$

Hence, either

$$2 \log(C_8) + 2c_1 \log(d) > d \log |\lambda| \quad \text{or} \quad 2c_1 \log(n) > d \log |\lambda|.$$

The former is impossible for large enough d (and thus small enough ε) while for the latter, the upper and lower bounds for n and d give that

$$2c_1 \log(2\varepsilon^{-C_9}) > 2c_1 \log(n) > d \log |\lambda| > \log |\lambda| \varepsilon^{-1/2},$$

which again is impossible for small enough ε . Hence item 4 also follows. $\blacktriangleleft$

4 Concluding Remarks

Our main result, Thm. 1, significantly expands the decidability landscape of MSO theories of structures of the form $\langle \mathbb{N}; <, P \rangle$, by considering predicates P obtained as sets of positive terms of non-degenerate simple LRS having two dominant roots. A natural question is whether any of these constraints can be relaxed. It is conceivable that investigating simple LRS with three dominant roots might yield positive decidability results, although the present development would have to be significantly altered at various junctures. We also note that open instances of the Skolem Problem [12] can easily be reduced from in the presence of simple LRS having four or more dominant roots. Likewise, considering non-simple LRS having three dominant roots or more exposes one to Positivity-hardness [20]. Let us remark that non-degeneracy is essential, as lifting this restriction has the effect of voiding the constraint on the number of dominant roots.⁵ Finally, one might envisage expanding the present setup by adjoining further predicates. However, even in the simplest of cases, one expects quite formidable difficulties in attempting to follow that research direction; see [3].

⁵ More precisely, one can construct a degenerate LRS for which the two dominant roots “cancel” each other out at every odd index, and the sub-LRS that remains over odd indices (involving the non-dominant roots) can be arbitrarily complex.

References

- 1 Rajab Aghamov, Christel Baier, Toghrul Karimov, Joël Ouaknine, and Jakob Piribauer. Linear dynamical systems with continuous weight functions. In *HSCC*, pages 22:1–22:11. ACM, 2024. doi:10.1145/3641513.3650173.
- 2 Christel Baier, Florian Funke, Simon Jantsch, Toghrul Karimov, Engel Lefauchaux, Florian Luca, Joël Ouaknine, David Purser, Markus A. Whiteland, and James Worrell. The orbit problem for parametric linear dynamical systems. In *CONCUR*, volume 203 of *LIPICs*, pages 28:1–28:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPICS.CONCUR.2021.28.
- 3 Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. On the decidability of monadic second-order logic with arithmetic predicates. In *LICS*, pages 11:1–11:14. ACM, 2024. doi:10.1145/3661814.3662119.
- 4 Achim Blumensath. Monadic Second-Order Model Theory. <http://www.fi.muni.cz/~blumens/>, 2024. [Online; accessed on 24 January 2025].
- 5 Émile M. Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 27(1):247–271, 1909.
- 6 J. Richard Büchi. Symposium on decision problems: On a decision method in restricted second order arithmetic. In *Studies in Logic and the Foundations of Mathematics*, volume 44, pages 1–11. Elsevier, 1966.
- 7 Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193. Cambridge University Press, 2012.
- 8 Olivier Carton and Wolfgang Thomas. The monadic theory of morphic infinite words and generalizations. *Information and Computation*, 176(1):51–65, 2002. doi:10.1006/INCO.2001.3139.
- 9 Julian D’Costa, Toghrul Karimov, Rupak Majumdar, Joël Ouaknine, Mahmoud Salamaty, and James Worrell. The pseudo-reachability problem for diagonalisable linear dynamical systems. In *MFCS*, volume 241 of *LIPICs*, pages 40:1–40:13. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. doi:10.4230/LIPICS.MFCS.2022.40.
- 10 Artūras Dubickas and Min Sha. Positive density of integer polynomials with some prescribed properties. *Journal of Number Theory*, 159:27–44, 2016.
- 11 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(2):169–181, 1966. doi:10.2307/2269808.
- 12 Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*. Mathematical Surveys and Monographs. American Mathematical Society, 2003.
- 13 Glyn Harman. One hundred years of normal numbers. In *Surveys in Number Theory*, pages 57–74. AK Peters/CRC Press, 2002.
- 14 Toghrul Karimov, Edon Kelmendi, Joris Nieuwveld, Joël Ouaknine, and James Worrell. The power of positivity. In *LICS*, pages 1–11. IEEE, 2023. doi:10.1109/LICS56636.2023.10175758.
- 15 Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. What’s decidable about discrete linear dynamical systems? In *Principles of Systems Design*, volume 13660 of *Lecture Notes in Computer Science*, pages 21–38. Springer, 2022. doi:10.1007/978-3-031-22337-2_2.
- 16 Toghrul Karimov, Engel Lefauchaux, Joël Ouaknine, David Purser, Anton Varonka, Markus A. Whiteland, and James Worrell. What’s decidable about linear loops? *Proc. ACM Program. Lang.*, 6(POPL):1–25, 2022. doi:10.1145/3498727.
- 17 Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Courier Corporation, 2012.
- 18 Florian Luca, Joël Ouaknine, and James Worrell. Algebraic model checking for discrete linear dynamical systems. In *FORMATS*, volume 13465 of *Lecture Notes in Computer Science*, pages 3–15. Springer, 2022. doi:10.1007/978-3-031-15839-1_1.

- 19 Eugene M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II. *Izvestiya: Mathematics*, 64(6):1217, 2000.
- 20 Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *SODA*, pages 366–379. SIAM, 2014. doi:10.1137/1.9781611973402.27.
- 21 Martine Queffélec. Old and new results on normality. *Lecture Notes-Monograph Series*, pages 225–236, 2006.
- 22 Alexander Rabinovich. On decidability of monadic logic of order over the naturals extended by monadic predicates. *Information and Computation*, 205(6):870–889, 2007. doi:10.1016/J.IC.2006.12.004.
- 23 Alexander Rabinovich and Wolfgang Thomas. Decidable theories of the ordering of natural numbers with unary predicates. In *International Workshop on Computer Science Logic*, pages 562–574. Springer, 2006.
- 24 Aleksei Lvovich Semenov. Logical theories of one-place functions on the set of natural numbers. *Mathematics of the USSR-Izvestiya*, 22(3):587, 1984.
- 25 S. Shelah. The monadic theory of order. *Ann. Math.*, 102:379–419, 1975.
- 26 Wolfgang Thomas. Ehrenfeucht games, the composition method, and the monadic theory of ordinal words. In *Structures in Logic and Computer Science*, volume 1261 of *Lecture Notes in Computer Science*, pages 118–143. Springer, 1997. doi:10.1007/3-540-63246-8_8.
- 27 Wolfgang Thomas. Languages, automata, and logic. In *Handbook of Formal Languages: Volume 3 Beyond Words*, pages 389–455. Springer, 1997. doi:10.1007/978-3-642-59126-6_7.
- 28 R. Tijdeman, M. Mignotte, and T. N. Shorey. The distance between terms of an algebraic recurrence sequence. *J. Reine Angew. Math.*, 346:63–76, 1984.