On Expansions of Monadic Second-Order Logic with Dynamical Predicates

Joris Nieuwveld
Max Planck Institute for Software Systems
Saarland Informatics Campus
Saarbrücken, Germany
jnieuwve@mpi-sws.org

Joël Ouaknine
Max Planck Institute for Software Systems
Saarland Informatics Campus
Saarbrücken, Germany
joel@mpi-sws.org

***Abstract*—Expansions of the monadic second-order (MSO) theory of the structure $\langle \mathbb{N}; < \rangle$ have been a fertile and active topic 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. Such predicates are so named in view of their close kinship with discrete-time linear dynamical systems. In turn, our results enable decision procedures for a range of new properties over a wide class of linear dynamical systems.**

***Index Terms*—Monadic second-order logic, linear recurrence sequences, decidability**

I. 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 [5], who in the early 1960s established decidability of this theory through a profound connection between logic and automata theory.

Shortly thereafter, in yet another seminal piece of work [8], 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 Fac of factorial numbers, or the set $2^{\mathbb{N}}$ of powers of 2, or the set Sq of perfect squares, and so on.

Much progress followed in the ensuing decades, notably due to Semënov [18], who introduced the notion of *effective almost periodicity*, and Carton and Thomas [7], 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 [16], Rabinovich and Thomas [17], and Berthé *et al.* [1].

In the present paper, we significantly extend this line of research by considering a large class of "dynamical" predicates derived from linear recurrence sequences (LRS). 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.[2] 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;[3] see also [1] 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 I.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. I.1 is the sequence $\langle u_n \rangle_{n=0}^{\infty}$ defined by

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

with $u_0 = 2, u_1 = 4$, and $u_2 = 7$. The subsequent values of the LRS are:

$$10, 9, -6, -53, -150, -271, -206, 787, 4690, 15849,$$
$$41994, 92827, 169530, 230369, 106594, -659933, \ldots.$$

One can readily verify that $\langle u_n \rangle_{n=0}^{\infty}$ satisfies the formula

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

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

[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".

[2] These notions are properly defined in Sec. II-C.

[3] LRS having a single positive dominant root are singularly well behaved: they are either constant, or effectively ultimately monotonically increasing (or decreasing), effectively procyclic, and effectively sparse. In the case of a negative dominant root, essentially the same behaviour is observed by restricting to the positive terms.

Let P be as per Thm. I.1. Viewing P as an ordered set, we have:

$$P = \{u_0, u_1, u_2, u_4, u_3, u_{10}, u_{11}, u_{12}, u_{13}, u_{14}, u_{17}, u_{15}, u_{16}, u_{24}, u_{25}, u_{26}, u_{27}, u_{28}, u_{30}, u_{29}, u_{38}, u_{39}, u_{44}, u_{40}, \dots\}.$$

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 in turn is 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 I.2. *Let $\overline{P} = \{u_n : n \in \mathbb{N}\}$ 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 $\langle \mathbb{Z}; 0, <, \overline{P} \rangle$ is decidable.*

This result is straightforwardly obtained from Thm. I.1 via an application of Shelah's celebrated "composition method" in model theory [19]. In the case at hand, one can directly invoke, for example, [20, 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. I.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 subsentences 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. I.1, we therefore rely instead on a new concept, that of *(effective) weak pronormality*, which we introduce shortly. Weak pronormality is itself predicated on the notion of *weak normality*, whose use in model theory was pioneered by Berthé *et al.* [1]. In particular, Berthé *et al.* study the MSO theory of the structure $\langle \mathbb{N}; <, 2^{\mathbb{N}}, \mathsf{Sq} \rangle$, and establish decidability assuming that the binary expansion of $\sqrt{2}$ is weakly normal, i.e., contains every finite bit pattern as a factor infinitely often.

The hypothesis that $\sqrt{2}$ is weakly normal in base 2 is widely expected to be true, but remains a major open 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 [3] showed over a century ago that non-normal real numbers have Lebesgue measure 0, establishing normality (or even weak normality) of everyday irrational numbers has remained fiercely elusive; see [6], [10], [12], [15] 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 *weakly normal 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) weak pronormality:

Definition I.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 $\langle p_m \rangle_{m=0}^{\infty}$:*

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

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

*For **effectiveness**, we require in addition that the sequence $\langle p_m \rangle_{m=0}^{\infty}$ 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 weak pronormality relates to Thm. I.1. Recall from the hypotheses of the theorem the LRS $\langle u_n \rangle_{n=0}^{\infty}$, along with its infinite set P of positive values, and define the sequence $\langle P_m \rangle_{m=0}^{\infty}$ by letting P_{m-1} denote the mth smallest number in P; in other words, $\langle P_m \rangle_{m=0}^{\infty}$ is a strict ordering of the set P. We will establish the following instrumental result:

Theorem I.4. *Let $\langle P_m \rangle_{m=0}^{\infty}$ be as above, i.e., the sequence of ordered positive values of some non-degenerate, simple, integer-valued LRS having two dominant roots. Then $\langle P_m \rangle_{m=0}^{\infty}$ is effectively weakly pronormal.*

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

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

Thus $S_5 = \{0, 2, 4\}$, $N_5 = 0$, and

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

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

We computed the first million terms of this sequence, but did not encounter the factor $\langle 0, 0, 0 \rangle$ once within that initial segment. Nevertheless, according to Thm. I.4, it should appear infinitely often! Indeed, we prove this in Sec. III-B, and moreover are able to derive an upper bound of approximately $7 \cdot 10^{57}$ for the index of the first occurrence of $\langle 0, 0, 0 \rangle$ in $\langle P_m \rangle_{m=0}^{\infty}$.

The above discussion suggests that, whilst the sequence $\langle P_m \rangle_{m=0}^{\infty}$ is provably weakly normal, it is seemingly 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 I.4 is the key technical device underpinning our main result, Thm. I.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.

II. Preliminaries

A. 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 $\langle w_0, w_1, \ldots, w_k\rangle$, and the infinite word $w_0w_1\cdots$ with the infinite sequence $\langle w_0, w_1, \ldots\rangle$, 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 $\langle w_n, \ldots, w_{n+k}\rangle = \langle w'_0, \ldots, w'_k\rangle$.

An infinite word w is *recursive* (or *computable*) if one can compute w_j for every $j \geq 0$, and is *weakly normal* if each $w' \in \Sigma^*$ appears infinitely often as a factor of w.

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 $\delta : Q \times \Sigma \to Q$, 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 whether $\mathcal{A}$ accepts w for any given deterministic Muller automaton $\mathcal{A}$ with alphabet Σ. We denote the acceptance problem by Acc_w.

Berthé *et al.* established the following [1, Thm. 4.16]:

Theorem II.1. *If $w \in \Sigma^\omega$ is recursive and weakly normal, 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 $\delta : Q \times \Sigma_{\text{in}} \to Q \times \Sigma^*_{\text{out}}$. The transducer $\mathcal{B}$ starts in state q_{init}. It reads a word $w \in \Sigma^*_{\text{in}} \cup \Sigma^\omega_{\text{in}}$ 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 $\mathcal{B}(w) \in \Sigma^*_{\text{out}} \cup \Sigma^\omega_{\text{out}}$ to denote the output word thus computed upon reading $w \in \Sigma_{\text{in}}$.

We now recall a Turing-reducibility property between word acceptance problems [1, Lem. 4.5]:

Lemma II.2. *Let $w \in \Sigma^\omega$ and $\mathcal{B}$ be a deterministic finite transducer. Then the problem $\mathrm{Acc}_{\mathcal{B}(w)}$ reduces to Acc_w.*

B. Monadic Second-Order Logic

A *(unary or monadic) predicate* P is a function $P : \mathbb{N} \to \{0, 1\}$, 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 sequence of elements of P in non-repeating, sorted ascending order. In other words, P_{m-1} is the mth 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:

$$w = 0^{P_0}10^{P_1-P_0-1}10^{P_2-P_1-1}10^{P_3-P_2-1}\cdots. \tag{5}$$

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 [2] 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, [21, Thms. 5.4 and 5.9].

Theorem II.3. *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 II.4. *Let $P \subseteq \mathbb{N}$ be an infinite, recursive, and effectively sparse predicate. If, for each $M \geq 2$ and deterministic Muller automaton over alphabet $\{0, \ldots, M-1\}$, one can decide whether the automaton accepts the word*

$$(P_0 \bmod M)(P_1 \bmod M)(P_2 \bmod M)\cdots, \tag{6}$$

then the MSO theory of the structure $\langle\mathbb{N}; <, P\rangle$ is decidable.

Proof. By Thm. II.3, 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 $w_{\text{init}} := 0^{P_0}10^{P_1-P_0-1}1\cdots 0^{P_{K+1}-P_K-1}1$. 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 $\mathrm{Acc}_{\langle P_m \bmod M\rangle_{m=0}^{\infty}}$ is assumed to be decidable. Then $\mathrm{Acc}_{\langle P_m \bmod M\rangle_{m=K+1}^{\infty}}$ is also decidable (by hard-coding the initial segment) and thus $\mathrm{Acc}_{\mathcal{B}(\langle P_m \bmod M\rangle_{m=K+1}^{\infty})}$ is decidable by Thm. II.2. Therefore $\mathrm{Acc}_{w_{\text{init}}\mathcal{B}(\langle P_m \bmod M\rangle_{m=K+1}^{\infty})}$ 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. □

C. 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 $c_1, \ldots, c_d \in R$, with $c_d \neq 0$, having the property that, for all $n \in \mathbb{N}$,

$$u_{n+d} = c_1u_{n+d-1} + \cdots + c_du_n\,.$$

The entire sequence is therefore completely specified by the $2d$ numbers $c_1, \ldots, c_d$ and $u_0, \ldots, u_{d-1}$. 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 $F(X) = X^d - c_1X^{d-1} - \cdots - c_d \in R[X]$. 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 $\lambda_1, \ldots, \lambda_K$ 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 roots, see, e.g., [1, 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 [1, Lem. 2.6].

Example II.5. *Let $\langle u_n\rangle_{n=0}^{\infty}$ be the ($\mathbb{Z}$-)LRS* (1) *from Sec. I. The characteristic polynomial of $\langle u_n\rangle_{n=0}^{\infty}$ is*

$$\begin{aligned} F(X) &= X^3 - 6X^2 + 13X - 10 \\ &= (X-2)(X-(2+i))(X-(2-i))\,. \end{aligned}$$

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 $r_n = 2^n$.*

D. Number Theory

Baker's theorem on linear forms of algebraic numbers is our main number-theoretic tool. 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 minimum 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, put $h(0) = 0$. For all algebraic numbers $\alpha_1, \ldots, \alpha_k$ and $n \in \mathbb{Z}$, we have the following properties:

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

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

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

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

Matveev [13] proved the following:

Theorem II.6. *If $\Lambda \neq 0$, then*

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

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 [22]:

Theorem II.7. *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 II.8. *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 $n_1 \geq C_4$.

III. Proof of the Main Result

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

We begin in Sec. III-A by untangling the definition of an LRS satisfying the above hypotheses and reduce Thm. I.1 to Thm. I.4. We then provide intuition underlying the proof of the latter through an extended example in Sec. III-B, and finally proceed to establish Thm. I.4 in Sec. III-C.

A. Reduction to Weak Pronormality

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

Lemma III.1. *Assume that $\langle u_n\rangle_{n=0}^{\infty}$ is an LRS satisfying the hypotheses of Thm. I.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 $|\lambda_1| > 1$.*

Proof. As the characteristic polynomial of $\langle u_n\rangle_{n=0}^{\infty}$ has integer coefficients, $\overline{\lambda_1}$ and $\overline{\lambda_2}$ are also dominant characteristic roots. Since $\langle u_n\rangle_{n=0}^{\infty}$ has exactly two dominant roots, $\{\lambda_1, \lambda_2\} = \{\overline{\lambda_1}, \overline{\lambda_2}\}$. If $\lambda_1 = \overline{\lambda_1}$, $\lambda_2 = \overline{\lambda_2}$ and so both λ_1 and λ_2 are real. Hence, $\lambda_1/\lambda_2 = \pm 1$, contradicting non-degeneracy. Thus, $\lambda_2 = \overline{\lambda_1}$.

If the argument of λ_1 is a rational multiple of π, $\lambda_1/\overline{\lambda_1}$ also has argument a rational multiple of π. Having modulus 1, $\lambda_1/\overline{\lambda_1}$ would then be a root of unity, contradicting non-degeneracy.

Assume $|\lambda_1| \leq 1$. By the Vieta formulas, the product of the absolute values of the characteristic roots is at most 1 and also equals $|c_d| \in \mathbb{Z}_{>0}$, where c_d is the constant coefficient of the minimum polynomial of $\langle u_n\rangle_{n=0}^{\infty}$. Hence, $|\lambda_1| = 1$ and there are no non-dominant characteristic roots. Whence, by an old result of Kronecker [11], we conclude that both λ_1 and λ_2 are roots of unity, and thus so is their quotient, contradicting once again non-degeneracy. Hence $|\lambda_1| > 1$ as claimed. □

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 $\langle r_n\rangle_{n=0}^{\infty}$:

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

Here, α and λ are algebraic numbers with $\alpha \neq 0$ (as otherwise λ and $\overline{\lambda}$ 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.

Recall that $P = \{u_n : n \in \mathbb{N}\} \cap \mathbb{N}$ and $\langle P_m\rangle_{m=0}^{\infty}$ is a sequence in which P_{m-1} is the mth smallest element in P. To apply Prop. II.4, we need the following lemma, whose proof relies heavily on the results of Mignotte, Shorey, and Tijdeman from Sec. II-C.

Lemma III.2. *Let $P \subseteq \mathbb{N}$ be as per Thm. I.1. Then P is infinite, recursive, and effectively sparse.*

Proof. First, as discussed in Sec. II-C, compute $r > 0$ and $0 < R < |\lambda|$ such that $rR^n > r_n$ for all $n \in \mathbb{N}$.

To show that $\langle P_m\rangle_{m=0}^{\infty}$ is recursive, it is sufficient to find, for a given $k \in \mathbb{N}$, a number N such that $|u_n| > k$ for all $n \geq N$ as then $k \in P$ if and only if $k \in \{u_0, \ldots, u_{N-1}\}$. Using Thm. II.7, we have that when $n \geq C_2$ and $u_n = k$,

$$n \log|\lambda| - C_1 \log^2(n) \leq \log|u_n| < \log(k+1)\,.$$

Hence n is bounded and the desired N can be obtained.

To show that P is infinite, we invoke Lem. 4 from [4]: for infinitely many n, $\alpha\lambda^n + \overline{\alpha}\overline{\lambda}^n > c|\lambda|^n$ for some real $c > 0$. As $c|\lambda|^n > rR^n$ for all but finitely many n, there is $c' > 0$ such that $u_n \geq c'|\lambda|^n$ for infinitely many n. Hence P is indeed infinite.

It remains to show that $\langle P_m\rangle_{m=0}^{\infty}$ is effectively sparse. Assume $k, n_1, n_2 \in \mathbb{N}$, $n_1 > n_2$, and $|u_{n_1} - u_{n_2}| \leq k$. Then Thm. II.8 asserts that whenever $n_1 \geq C_4$,

$$\begin{aligned}\log(k+1) &\geq \log|u_{n_1} - u_{n_2}| \\ &\geq |\lambda|^{n_1} - C_3 \log(n_1)^2 \log(n_2+2) \\ &\geq |\lambda|^{n_1} - C_3 \log(n_1+1)^3\,.\end{aligned}$$

Thus $|u_{n_1} - u_{n_2}| \leq k$ implies that $n_1 \leq N'$ for some computable constant N'. Hence we can write out the set $P \cap \{0, \ldots, k+1+\max_{0\leq n\leq N'}\{u_n\}\}$ and find the two largest elements in this set having difference at most k. □

By Prop. II.4, it now suffices to prove that for all $M \geq 2$, one can decide $\mathrm{Acc}_{\langle P_m \bmod M\rangle_{m=0}^{\infty}}$ (determine whether a given deterministic Muller automaton $\mathcal{A}$ over alphabet $\{0, \ldots, M-1\}$ accepts $\langle P_m \bmod M\rangle_{m=0}^{\infty}$). The next lemma shows how the effective weak pronormality of $\langle P_m\rangle_{m=0}^{\infty}$ asserted by Thm. I.4 enables us to do this.

Lemma III.3. *Theorem I.4 implies Thm. I.1.*

Proof. By Lem. III.2, P is infinite, recursive, and effectively sparse, and so in order to apply Prop. II.4, we only need to verify that $\mathrm{Acc}_{\langle P_m \bmod M\rangle_{m=0}^{\infty}}$ is decidable for all $M \geq 2$.

Let $M \geq 2$ and recall the definition (3) of S_M. As stated in Sec. II-C, $\langle u_n \bmod M\rangle_{n=0}^{\infty}$ is ultimately periodic modulo M, and both its period and preperiod can be effectively computed. Therefore, we can compute S_M together with a number N' such that for all $n \geq N'$, $u_n \equiv s \pmod M$ for some $s \in S_M$. Next, compute N_M large enough such that $P_{N_M} \geq u_n$ for all $0 \leq n < N'$. Then, by construction, for all $m \geq N_M$, $P_m \equiv s \pmod M$ for some $s \in S_M$.

Let $\mathcal{A}$ be a deterministic Muller automaton over alphabet $\{0, \ldots, M-1\}$. After $\mathcal{A}$ has read $(P_0 \bmod M), \ldots, (P_{N_M-1} \bmod M)$, only elements from S_M will be read. Hence we can build a second deterministic Muller automaton $\mathcal{A}'$ over alphabet S_M which accepts $\langle P_m \bmod M\rangle_{m=N_M}^{\infty}$ if and only if $\mathcal{A}$ accepts $\langle P_m \bmod M\rangle_{m=0}^{\infty}$ by hard-coding the initial segment and restricting the original alphabet $\{0, \ldots, M-1\}$ to S_M. By Thm. I.4, $\langle P_m \bmod M\rangle_{m=N_M}^{\infty} \in {S_M}^{\omega}$ is weakly normal, and thus by Thm. II.1 we can determine whether $\mathcal{A}'$ accepts $\langle P_m \bmod M\rangle_{m=N_M}^{\infty}$. Hence, combined with Lem. III.2, the conditions of Prop. II.4 are met, yielding the desired result. □

Theorem I.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 weakly normal. Let us unpack this definition. $\langle P_m \bmod M\rangle_{m=N_M}^{\infty} \in {S_M}^{\omega}$ is weakly normal if for any $\ell \geq 1$, every pattern $\langle s_1, \ldots, s_\ell\rangle \in {S_M}^{\ell}$ 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 $s_1, \ldots, s_\ell \in S_M$, there are $n_1, \ldots, n_\ell \in \mathbb{N}$ such that

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

As the dominant part $\langle v_n\rangle_{n=0}^{\infty}$ only relies on two algebraic numbers, α and λ, it is easier to work with $\langle v_n\rangle_{n=0}^{\infty}$ than $\langle u_n\rangle_{n=0}^{\infty}$. We have:

Lemma III.4. *Theorem I.4 is implied by the following statement: For given numbers $\ell, N \in \mathbb{N}$, $T \geq 2$, and $t_1, \ldots, t_\ell \in \{0, \ldots, T-1\}$, there are $n_1, \ldots, n_\ell \in \mathbb{N}$ such that*

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

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. II.8 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 $s_1, \ldots, s_\ell \in S$ and $1 \leq j \leq \ell$, there exists a $t_j \in \{0, \ldots, T-1\}$ such that $u_{nT+t_j} \equiv s_j \pmod M$ whenever n is large enough. Therefore, if $n_1, \ldots, n_\ell \in \mathbb{N}$ are at least $\max\{N, N'\}$ and satisfy the hypotheses of the lemma, it follows that $0 \leq u_{n_1} < \cdots < u_{n_\ell}$ and for all $m \in \mathbb{N}$ such that $u_{n_1} < u_m < u_{n_\ell}$, $m \in \{n_1, \ldots, n_\ell\}$. 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. III.4 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 $1/|\alpha|$. That is, we can assume that $|\alpha| = 1$. Write $\alpha = e^{i\phi}$ and $\lambda = |\lambda|e^{i\theta}$.

B. An Extended Example

Let us consider an example. Let $\langle u_n\rangle_{n=0}^{\infty}$ be the sequence (1) from Sec. I and assume $M = 5$. We are interested in the behaviour of 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 $T = 4$, since for $n \geq 1$, the value of u_n modulo 5 only depends on the value of n modulo 4. Thus for all $m \geq 0$, $(P_m \bmod 5) \in \{0, 2, 4\}$. Then Thm. I.4 states that every $\langle s_1, \ldots, s_\ell\rangle \in {S_5}^*$ 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. As $s_1 = 0$, we have to find a $t_1 \in \{0, 1, 2, 3\}$ such that for all large enough n, $u_{4n+t_1} \equiv 0 \pmod 5$. Thanks to (4), we are forced to take $t_1 = 3$. Similarly, $t_2 = t_3 = 3$. Thus, we want to find $n_1, n_2, n_3 \geq 1$ 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 $u_m \in \{u_{n_1}, u_{n_2}, u_{n_3}\}$.

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. III.4, we can work with $v_n = \alpha\lambda^n + \overline{\alpha}\overline{\lambda}^n = \cos(n\theta+\phi)|\lambda|^n$ instead of u_n for large enough n. Here, we have that $\lambda = e^{i\theta}|\lambda| = 2+i$ and $\alpha = 1 = e^{i\phi}$ (as we have scaled α by $|\alpha|^{-1}$ to get $|\alpha| = 1$). Thus, in our example, $\phi = 0$.

Hence, for a given $N \in \mathbb{N}$ 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 for all m with $\cos(n_1\theta) < \cos(m\theta)|\lambda|^{m-n_1} < \cos(n_3\theta)|\lambda|^{n_3-n_1}$, $m \in \{n_1, n_2, n_3\}$ (and hence $m = n_2$ by the strict inequalities). This is the statement of Lem. III.4. For simplicity, let us fix $N = 0$.

We reached this far in the previous section. Next, we aim to find $b_2, b_3 \in \mathbb{N}$ such that $n_1 = n$, $n_2 = n+b_2$, and $n_3 = n+b_3$ for some $n \geq N$ congruent to 3 modulo 4 that satisfies our hypotheses. In particular, $b_2 \equiv b_3 \equiv 3-3 \equiv 0 \pmod 4$. That is, for $j \in \{2, 3\}$, we have that $b_j \equiv t_j - t_1 \equiv 0 \pmod 4$.

In order to solve this discrete problem (find a natural number n meeting these constraints), we first want to solve a

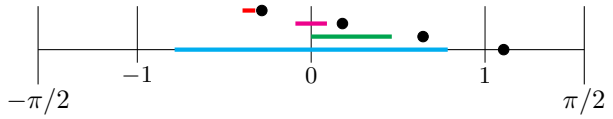

Fig. 1. Let $\lambda = 1+2i$. Then for $d = 1, 2, 3, 4$, $\mathcal{J}_d(1,3)$ are drawn in cyan, green, magenta, and red, respectively, and $|\mathcal{J}_d(1,3)|$ are $\pi/2$, 0.464, 0.182, 0.073, respectively. As some of the intervals overlap, we have stacked them vertically for visual purposes. The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

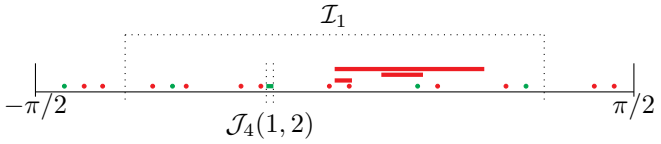

Fig. 2. We drew the intersection of $\mathcal{I}_1$ and $\mathcal{J}_d(1,2)$ for $d = 1, \ldots, 20$ in red when $d \not\equiv 0 \pmod 4$ and in green when $d \equiv 0 \pmod 4$. For ease of visibility, $\mathcal{J}_d(1,2)$ is positioned higher for $d = 1, 2, 3$, and for intervals $\mathcal{J}_d(1,2)$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

continuous variant of this problem: find an *interval* $\mathcal{I}$ in which 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 $x \in \mathcal{I}$,

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

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 numbers of the form $x = n\theta$, where $n \equiv 3 \pmod 4$.

Our approach relies heavily on the following definition.

Definition III.5. *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*

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

Clearly, $\mathcal{J}_d(\gamma, \delta)$ is a union of open intervals. When identifying $\mathbb{R}/(2\pi\mathbb{Z})$ with $(-\pi, \pi]$, $\cos(x) > 0$ if and only if $x \in (-\pi/2, \pi/2)$. Hence, as $\gamma > 0$, $\mathcal{J}_d(\gamma, \delta) \subset (-\pi/2, \pi/2)$. Using the fact that $\cos(x) = \frac{1}{2}(e^{ix} + e^{-ix})$, we can show that for $\eta \in \{\gamma, \delta\}$, $\eta\cos(x) = \cos(x + d\theta)|\lambda|^d$ for at most one $x \in (-\pi/2, \pi/2)$. Hence $\mathcal{J}_d(\gamma, \delta)$ is empty or consists of a single open interval. Furthermore, we will show that when δ is small enough, $|\mathcal{J}_d(\gamma, \delta))| = O((\delta - \gamma)|\lambda|^{-d})$. These intervals $\mathcal{J}_d(\gamma, \delta)$ shrink rapidly with d and it can be shown that every point in them is at most $O(\delta|\lambda|^{-d})$ away from $-d\theta \pm \pi/2$ in $\mathbb{R}/(2\pi\mathbb{Z})$. All of this is proved in Lem. III.7 and illustrated in Fig. 1.

We will construct $\mathcal{I}$ inductively. First, let $\mathcal{I}_1 = (-1.1, 1.1)$. We have chosen this initial interval because $\cos(x) > |\lambda|^{-1}$ for all $x \in \mathcal{I}_1$, and so $\mathcal{I}_1 \cap \mathcal{J}_d(1,2)$ is empty for all $d < 0$. Moreover, $0 < \cos(x) < 2\cos(x)$ for all $x \in \mathcal{I}_1$. The choice of 2 is made because

$$\Big|\bigcup_{d=1}^{\infty} \mathcal{J}_d(1,2)\Big| \leq \sum_{d=1}^{\infty} |\mathcal{J}_d(1,2)| < |\mathcal{I}_1|.$$

Thus, the intervals $\mathcal{J}_d(1, 2)$ with $d \neq 0$ do not cover $\mathcal{I}_1$.

For $\mathcal{I}_2$, we will take an interval $\mathcal{J}_{b_2}(1, \delta) \subset \mathcal{I}_1$, where $b_2 \equiv 0 \pmod 4$ and $1 < \delta < 2$. Arbitrarily, we choose $\delta = 1.95$. As shown in Fig. 2, when picking $b_2 = 4$, $\mathcal{I}_2 \cap \mathcal{J}_d(1, 2)$ is empty for all integers $d < 20$ not equal to either 0 or 4. 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 $d \notin \{0, 4\}$.

For b_3, we find that $\mathcal{J}_d(1,2) \cap \mathcal{I}_2 \neq \emptyset$ for $d = 0, 4, 38, 99, 160, 309, 370, \ldots$. The smallest such d that is not equal to 0 or 4 (which are already in use) and congruent to $0 \equiv n_3 - n_1 \pmod 4$ is 160, for which

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

Then set $\mathcal{I} = \mathcal{I}_3 := \mathcal{J}_{160}(1.95, 2)$, which is tiny: it has length approximately $9 \cdot 10^{-59}$. However, $\mathcal{I} \cap \bigcup_{d=-\infty, d\notin\{0,4,160\}}^{\infty} \mathcal{J}_d(1,2)$ is an even smaller subset of $\mathcal{I}$. Thus we have found an interval $\mathcal{I}$ such that, for all $x \in \mathcal{I}$,

$$\begin{aligned} 0 < \cos(x) < \cos(x + 4\theta)|\lambda|^4 < 1.95\cos(x) \\ < \cos(x + 160\theta)|\lambda|^{160} < 2\cos(x). \end{aligned} \tag{7}$$

This solves the continuous version of our problem.

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

For a real number x, let $|x|_{2\pi}$ denote the distance from x to the nearest integer multiple of 2π. Assume that for n as above Condition (3) is not satisfied. Then $n\theta \in \mathcal{J}_d(1, 2)$ for some integer $d \notin \{0, 4, 160\}$. Hence, combining the information from Lem. III.7 to the effect that $\mathcal{J}_d(1, 2)$ is close to $-d\theta \pm \pi/2$ modulo 2π, we have:

$$|d + n|^{-c_1} < |n\theta - (-d\theta \pm \pi/2)|_{2\pi} < c_2|\lambda|^{-d} \tag{8}$$

for two constants $c_1, c_2 > 0$. In the above, the first inequality follows from Baker's theorem, whereas the second inequality is derived from the exponential rate of shrinkage of the intervals.

As there are many $n\theta$ in $\mathcal{I}$ that are fairly "evenly" distributed, we are able to prove that (8) 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 $m = n + 4$. Translating back to u_n gives us the required result. In particular, we can calculate that when taking

$$n = 14194141717537542957857939524499342238484942328418141212296,$$

we have that $n\theta \in \mathcal{I}$, $n \equiv 0 \pmod 4$, and $u_n < u_m < u_{n+160}$ implies that $m = 4$. Thus, the pattern $\langle 0, 0, 0\rangle$ does indeed appear in $\langle P_m \bmod 5\rangle_{m=0}^{\infty}$.

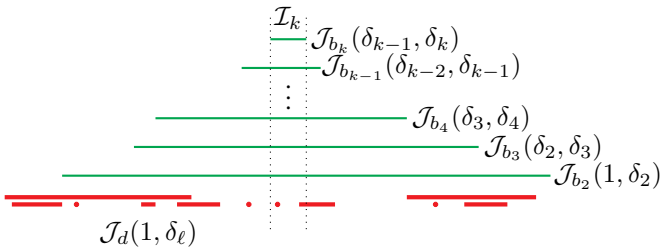

Fig. 3. The inductive construction for $\mathcal{I}$. In green, we see that at each step, $\mathcal{I}_k$ is taken to be $\mathcal{J}_{b_k}(\delta_{k-1},\delta_k)$. This gives (9) and by construction, $\mathcal{I}_{k+1}\subset\mathcal{I}_k$. The red intervals are dense in $\mathcal{I}_k$, but by being careful, do not cover $\mathcal{I}_k$ at any step. The picture is not to scale as both the red and green intervals decrease in size exponentially fast.

C. Proof of Weak Pronormality

We start by presenting a continuous version of weak normality. We then state and prove a number of technical facts on our way to establishing the continuous version and the resulting proof of Thms. I.4 and I.1.

Lemma III.6. *Let $\ell, T\geq 2$ and $t_1,\dots,t_\ell\in\{0,\dots,T-1\}$. Then there are an interval $\mathcal{I}\subset\mathbb{R}/(2\pi\mathbb{Z})$, $b_2,\dots,b_\ell\geq 1$, $1<\delta_2<\cdots<\delta_\ell<\sqrt{|\lambda|}$, and $D\in\mathbb{N}$ such that*

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

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

3) *for all integers $d<D$ not in the set $\{0,b_2,\dots,b_\ell\}$, $\mathcal{I}\cap\mathcal{J}_d(1,\delta_\ell)=\emptyset$;*
4) *$\sum_{d=D}^{\infty}|\mathcal{J}_d(1,\delta_\ell)|<|\mathcal{I}|$.*

Although $\delta_2,\dots,\delta_{\ell-1}$ are not strictly required for our purposes, we include them in the statement of the theorem to simplify our induction approach.

The iterative process (not to scale) is depicted in Fig. 3.

Lemma III.7. *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 $x\in\mathcal{J}_d(\gamma,\delta)$.

Proof. Identify $\mathbb{R}/(2\pi\mathbb{Z})$ with $(-\pi,\pi]$. As $2\cos(x)=e^{ix}+e^{-ix}$ and $e^{id\theta}|\lambda|^d=\lambda^d$, for $\gamma\leq\eta\leq\delta$,

$$\cos(x+d\theta)|\lambda|^d=\eta\cos(x)\iff\left(e^{ix}\right)^2=-\frac{\overline{\lambda}^d-\eta}{\lambda^d-\eta}.\tag{10}$$

Hence, there is a unique $x\in(-\pi/2,\pi/2]$ such that $\cos(x+d\theta)|\lambda|^d=\eta\cos(x)$. If $x=\pi/2$ and $\cos(x+d\theta)=\eta\cos(x)$, then $\cos(x)=0$ and θ/π is rational, which we excluded in Lem. III.1. We conclude that $\mathcal{J}_d(\gamma,\delta)$ is a single interval within $(-\pi/2,\pi/2)$.

Let us now tackle the size of $\mathcal{J}_d(\gamma,\delta)$. As $\mathcal{J}_d(\gamma,\delta)$ consists of a single interval, $|\mathcal{J}_d(\gamma,\delta)|=|x_1-x_2|_{2\pi}$, where x_1 and x_2 are solutions in $(-\pi/2,\pi/2)$ to (10) with $\eta=\gamma$ and $\eta=\delta$, respectively. Using the triangle inequality on the unit circle,

$$|e^{ix_1}-e^{ix_2}|\leq|x_1-x_2|_{2\pi}\leq\frac{\pi}{2}|e^{ix_1}-e^{ix_2}|.$$

If $\gamma=\delta$, $x_1=x_2$, and so by continuity, when $\delta-\gamma$ is small enough, $|e^{ix_1}-e^{ix_2}|<\sqrt{2}$.

On this boundary, $|e^{ix_1}-e^{ix_2}|=\sqrt{2}$, and so $e^{ix_1}=\pm ie^{ix_2}$. It follows that $e^{2ix_1}=-e^{2ix_2}$, and so

$$\begin{aligned}-1&=e^{2ix_1}e^{-2ix_2}\\&=\frac{\overline{\lambda}^d-\gamma}{\lambda^d-\gamma}\cdot\frac{\lambda^d-\delta}{\overline{\lambda}^d-\delta}\\&=\frac{\lambda^d\overline{\lambda}^d-\gamma\lambda^d-\delta\overline{\lambda}^d+\gamma\delta}{\lambda^d\overline{\lambda}^d-\delta\lambda^d-\gamma\overline{\lambda}^d+\gamma\delta}.\end{aligned}$$

Therefore $2\lambda^d\overline{\lambda}^d-(\delta-\gamma)\lambda^d+(\delta-\gamma)\overline{\lambda}^d+2\gamma\delta=0$. Then $|\lambda|^{2d}\leq(\delta-\gamma)|\lambda|^d+\gamma\delta$, and so $(|\lambda|^d+\gamma)(|\lambda|^d-\delta)\leq 0$. This leads to a contradiction as $0<\gamma<\delta<\sqrt{|\lambda|}$ and $d\geq 1$. Thus $|e^{ix_1}-e^{ix_2}|<\sqrt{2}$.

By using the geometry of the unit circle, we see that $|e^{ix_1}-e^{ix_2}|<\sqrt{2}$ implies that $\sqrt{2}\leq|e^{ix_1}+e^{ix_2}|\leq 2$. Then, using the fact that $|e^{2ix_1}-e^{2ix_2}|=|e^{ix_1}-e^{ix_2}||e^{ix_1}+e^{ix_2}|$, we obtain

$$\frac{1}{2}|e^{i2x_1}-e^{i2x_2}|\leq|x_1-x_2|_{2\pi}\leq\frac{\pi}{2\sqrt{2}}|e^{i2x_1}-e^{i2x_2}|.$$

We can rewrite $|e^{i2x_1}-e^{i2x_2}|$ as follows:

$$\begin{aligned}&|e^{2ix_1}-e^{2ix_2}|\\&=\left|\frac{\overline{\lambda}^d-\gamma}{\lambda^d-\gamma}-\frac{\overline{\lambda}^d-\delta}{\lambda^d-\delta}\right|\\&=\frac{\left|\left(\overline{\lambda}^d-\gamma\right)\left(\lambda^d-\delta\right)-\left(\overline{\lambda}^d-\delta\right)\left(\lambda^d-\gamma\right)\right|}{|\lambda^d-\gamma||\lambda^d-\delta|}\\&=\frac{1}{|\lambda^d-\gamma||\lambda^d-\delta|}\left|(\delta-\gamma)\lambda^d-(\delta-\gamma)\overline{\lambda}^d\right|\\&=\frac{(\delta-\gamma)|\lambda|^d}{|\lambda^d-\gamma||\lambda^d-\delta|}\left|e^{i2d\theta}-1\right|.\end{aligned}$$

As $\gamma,\delta<\sqrt{|\lambda|}$, there is a constant $c_1>0$ such that $|\lambda^d-\eta|\geq c_1|\lambda|^d$ for $\eta\in\{\gamma,\delta\}$ and $d\geq 1$. Thus

$$|\mathcal{J}_d(\gamma,\delta)|\leq\frac{\pi}{2\sqrt{2}}|e^{2ix_1}-e^{2ix_2}|<C_5\frac{\delta-\gamma}{|\lambda|^d}\tag{11}$$

for $C_5=\frac{\pi}{2\sqrt{2}c_1^2}$. Similarly,

$$|\mathcal{J}_d(\gamma,\delta)|\geq\frac{1}{2}|e^{ix_1}-e^{ix_2}|=\frac{(\delta-\gamma)|\lambda|^d}{2|\lambda^d-\gamma||\lambda^d-\delta|}|e^{i2d\theta}-1|$$

and then there is a constant $c_2>0$ such that $|\lambda^d-\eta|<c_2|\lambda|^d$ for $\eta\in\{\gamma,\delta\}$ and $d\geq 1$. Thus,

$$|\mathcal{J}_d(\gamma,\delta)|>C_6\frac{|e^{i2d\theta}-1|(\delta-\gamma)}{|\lambda|^d}$$

for a constant C_6. Applying Thm. II.6 on the latter, we obtain a constant C_7 such that $|e^{i2d\theta} - 1| > d^{-C_7}$, and the result follows.

For the last claim, we estimate $|\mathcal{J}_d(0, \sqrt{|\lambda|})|$ with (11). □

For the next 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 d and n congruent to the correct number (t_1 or $t_j - t_1$) modulo T.

Lemma III.8. *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 $n_1, n_2 \equiv t \pmod T$.*

Proof. By the pigeonhole principle, there are distinct $d_1, d_2 \in \mathbb{N}$ such that $0 \leq d_1, d_2 \leq \lceil 2\pi|\mathcal{I}|^{-1} \rceil$ and

$$\left|T(d_1 - d_2)\theta\right|_{2\pi} < |\mathcal{I}|.$$

As the argument of λ is not a rational multiple of π, Baker's theorem (Thm. II.6) implies there is a computable number c_1 such that

$$\left|T(d_1 - d_2)\theta\right|_{2\pi} \geq \left|e^{iT(d_1-d_2)\theta} - 1\right| \geq \left\lceil 2\pi|\mathcal{I}|^{-1} \right\rceil^{-c_1}.$$

Thus, for all $N \in \mathbb{Z}$ and $x \in \mathbb{R}/(2\pi\mathbb{Z})$, $x + nT(d_1 - d_2)\theta \in \mathcal{I}$ for some $N \leq n \leq 2\pi\lceil 2\pi|\mathcal{I}|^{-1}\rceil^{c_1} + N$. Taking C_9 slightly bigger than c_1, $2\pi T\lceil 2\pi|\mathcal{I}|^{-1}\rceil^{c_1} < |\mathcal{I}|^{-C_9}$ when $\mathcal{I}$ is small enough. Hence, for all $N \in \mathbb{Z}$ and $x \in \mathbb{R}/(2\pi\mathbb{Z})$, there is some $n \equiv t \pmod T$ such that $N \leq n \leq |\mathcal{I}|^{-C_9} + N$ and $x + n\theta$ is in $\mathcal{I}$. For n_1, let $x = \phi$ and $N = |\mathcal{I}|^{-C_9}$.

Let $\mathcal{I}'$ be the middle half of $\mathcal{I}$. As before, there is an n_2 congruent to $-t$ modulo T with $-2|\mathcal{I}'|^{-C_9} \leq -n_2 \leq -|\mathcal{I}'|^{-C_9}$ and such that $-n_2\theta \pm \pi/2 \in \mathcal{I}'$. If $\mathcal{J}_{n_2}(0, \sqrt{|\lambda|})$ were not contained in $\mathcal{I}$, then by Lem. III.7,

$$\frac{1}{4}|\mathcal{I}| \leq C_8|\lambda|^{-n_2} \leq C_8|\lambda|^{-|\mathcal{I}'|^{-C_9}} = C_8|\lambda|^{-(|\mathcal{I}|/2)^{-C_9}}.$$

After taking logarithms, we have that

$$\log(|\mathcal{I}|) \leq \log(4C_8) - (|\mathcal{I}|/2)^{-C_9}\log|\lambda|,$$

which cannot hold when $\mathcal{I}$ is small enough. Hence $\mathcal{J}_{n_2}(1, \sqrt{|\lambda|}) \subset \mathcal{I}$. The lemma follows. □

For the fourth condition of Thm. III.6, we would like D to be large. That is, the smallest d such that $\mathcal{J}_d(1, \delta_\ell)$ has a non-empty intersection with $\mathcal{I}$ has to be quite large. We show that this is possible in the following lemma.

Lemma III.9. *Assume $\mathcal{I} \subset \mathbb{R}/(2\pi\mathbb{Z})$, $b_2, \dots, b_\ell \in \mathbb{N}$ and $1 < \delta_2 < \cdots < \delta_\ell < \sqrt{|\lambda|}$ satisfy the hypotheses of Lem. III.6. Then there is a constant $C_{10} > 0$ such that for every small enough $\varepsilon > 0$ there is a subinterval $\mathcal{I}'$ of $\mathcal{I}$ of length ε for which the hypotheses of Lem. III.6 hold for these $b_2, \dots, b_\ell$ and $\delta_1, \dots, \delta_\ell$ and $D > \varepsilon^{-C_{10}}$.*

Proof. For an interval $\mathcal{I}'$, let $D(\mathcal{I}')$ denote the smallest natural number $d \geq 1$ such that $d \neq b_2, \dots, b_\ell$ and $\mathcal{J}_d(1, \delta_\ell) \cap \mathcal{I}'$ is non-empty. By assumption, the intervals $\mathcal{J}_d(1, \delta_\ell)$ with $d \geq 1$ and $d \neq b_2, \dots, b_\ell$ do not cover $\mathcal{I}$. Let

$$c_1 = |\mathcal{I}| - \sum_{d=D(\mathcal{I})}^{\infty} |\mathcal{J}_d(1, \delta_\ell)|.$$

By construction, $c_1 > 0$. Then we have the following construction, depicted in Fig. 4. For $k \geq 1$, let d_k be the kth smallest number $d \geq 1$ not equal to $b_2, \dots, b_\ell$ such that $\mathcal{J}_{d_k}(1, \delta_\ell) \cap \mathcal{I}$ is non-empty. Furthermore, for $k \geq 1$, let $\mathcal{I}_k \subset \mathcal{I} \setminus \bigcup_{j=1}^{k} \mathcal{J}_{d_j}(1, \delta_\ell)$ be an interval of length $\frac{c_1}{k+1}$, which exists by the pigeonhole principle.

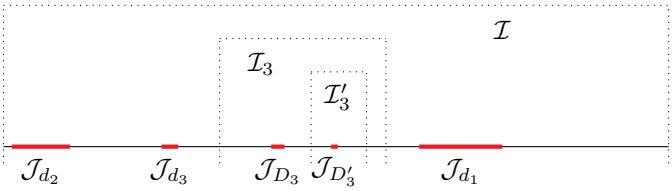

Fig. 4. The construction of $\mathcal{I}'_k$ as per Lem. III.9 for $k = 3$. For simplicity, $\mathcal{J}_d$ is used as short-hand for $\mathcal{J}_d(1, \delta_\ell)$. First, we let $\mathcal{I}_3$ be an interval of length $(|\mathcal{I}| - c_1)/4$ that does not intersect $\mathcal{J}_{d_1}$, $\mathcal{J}_{d_2}$, and $\mathcal{J}_{d_3}$. The smallest two numbers d such that $\mathcal{J}_d \cap \mathcal{I}_3 \neq \emptyset$ are $D_3 < D'_3$. We take $\mathcal{I}'_3$ to be an interval of length $|\mathcal{I}_3|/3$ that does not intersect $\mathcal{J}_{D_3}$ (but could potentially intersect $\mathcal{J}_{D'_3}$). The picture is not to scale as the red intervals decrease in size exponentially fast.

Let $D_k < D'_k$ be the two smallest $d \geq 1$ not equal to $b_2, \dots, b_\ell$ such that $\mathcal{J}_d(1, \delta_\ell) \cap \mathcal{I}_k \neq \emptyset$. We have $D_k > k$. For large enough k, Lem. III.7 entails that

$$|\mathcal{I}_k| = \frac{c_1}{k+1} > C_5\frac{\delta_\ell - 1}{3|\lambda|^k} > C_5\frac{\delta_\ell - 1}{3|\lambda|^{D_k}} \geq \frac{1}{3}|\mathcal{J}_{D_k}(1, \delta_\ell)|.$$

Hence we let $\mathcal{I}'_k \subset \mathcal{I}_k \setminus \mathcal{J}_{D_k}(1, \delta_\ell)$ of length $\frac{1}{3}|\mathcal{I}| = \frac{c_1}{k+1}$. It follows that $D(\mathcal{I}'_k) \geq D'_k$. Lem. III.7 gives that any point in $\mathcal{J}_{d_k}(1, \delta_\ell)$ is at most $C_8|\lambda|^{-D_k}$ from $-D_k\theta \pm \pi/2$, and the same holds for D'_k. Hence, for large enough k,

$$\begin{aligned}
&|e^{i(-D_k\theta \pm \pi/2)}) - e^{i(-D'_k\theta \pm \pi/2)}| \\
&\leq |(-D_k\theta - \pm\pi) - (-D_{k+1}\theta \pm \pi)|_{2\pi} \\
&\leq |\mathcal{I}_k| + C_8|\lambda|^{-D_k} + C_8|\lambda|^{-D'_k} \\
&\leq \frac{c_1}{k+1} + 2C_8|\lambda|^{-k} \\
&\leq \frac{2c_1}{k+1}.
\end{aligned}$$

Meanwhile, Baker's theorem (Thm. II.6) implies that

$$|e^{i(-D_k\theta \pm \pi/2)}) - e^{i(-D'_k\theta \pm \pi/2)}| > (D'_k - D_k)^{-c_2}$$

for a constant $c_2 > 0$. Therefore

$$D(\mathcal{I}'_k) \geq D'_k > D'_k - D_k > \left(\frac{2c_1}{k+1}\right)^{\frac{-1}{c_2}} \geq (6|\mathcal{I}'_k|)^{\frac{-1}{c_2}}.$$

The lemma follows by taking C_{10} slightly smaller than $1/c_2$. □

Now we can prove Lem. III.6.

Proof of Lem. III.6. We apply induction on k and require that the conditions hold for $1,\dots,k-1$ for an interval $\mathcal{I}_{k-1}$, and construct an interval $\mathcal{I}_k$ that satisfies the theorem when the first three conditions are restricted to $1,\dots,k$. Then we take $\mathcal{I}=\mathcal{I}_\ell$.

For the base case, let $\mathcal{I}_1=\{x\in\mathbb{R}/(2\pi\mathbb{Z}):\cos(x)>|\lambda|^{-1}\}$, $D=1$, and $\delta_\ell>1$ small enough. By Lem. III.7,

$$\sum_{d=D}^{\infty}|\mathcal{J}_d(1,\delta_\ell)|\le\sum_{d=1}^{\infty}C_5\frac{\delta_\ell-1}{|\lambda|^d}\le C_5\frac{\delta_\ell-1}{|\lambda|-1}<|\mathcal{I}_1|\,.$$

Hence Condition 4 holds, and the first three conditions follow by construction. The base case follows.

For the other cases, choose $\delta_2,\dots,\delta_{\ell-1}$ such that $1<\delta_2<\cdots<\delta_{\ell-1}<\delta_\ell$. Furthermore, for simplicity, set $\delta_1=1$.

Now assume $k\ge 1$ and let $\varepsilon>0$. For ε small enough, applying Lem. III.9 on $\mathcal{I}_{k-1}$ gives intervals $\mathcal{I}_\varepsilon\subset\mathcal{I}_{k-1}$ of length ε where the smallest d such that $\mathcal{J}_d(1,\delta_\ell)\cap\mathcal{I}_\varepsilon\neq\emptyset$ is at least $\varepsilon^{-C_{10}}$. Furthermore, let $\mathcal{I}'_\varepsilon$ be the middle half of $\mathcal{I}_\varepsilon$. Then $|\mathcal{I}'_\varepsilon|=\varepsilon/2$.

Lemma III.8 implies that when ε is again small enough, there is a $(\varepsilon/2)^{-C_9}<b_k<2(\varepsilon/2)^{-C_9}$ such that $b_k\equiv t_k-t_1 \pmod T$ and $-b_k\theta\pm\pi/2$ is in $\mathcal{I}'_\varepsilon$. We claim that for small enough ε, $\mathcal{J}_{b_k}(\delta_{k-1},\delta_k)\subset\mathcal{I}_\varepsilon$. Using Lem. III.7, this certainly holds when $C_8|\lambda|^{-b_k}<\varepsilon/4$. For a contradiction, assume $C_8|\lambda|^{-b_k}\ge\varepsilon/4$. Then, $4C_8/\varepsilon\ge|\lambda|^{b_k}$ and taking logarithms gives

$$\log(4C_8)-\log(\varepsilon)\ge b_k\log|\lambda|>(\varepsilon/2)^{-C_9}\log|\lambda|\,,$$

which is impossible for sufficiently small $\varepsilon>0$. This proves our claim.

If $d\neq 0,b_2,\dots,b_k$ and $\mathcal{J}_{b_k}(\delta_{k-1},\delta_k)\cap\mathcal{J}_d(1,\delta_\ell)\neq\emptyset$, then $d>\varepsilon^{-C_{10}}$. From Lemma III.7, we have:

$$|(b_k-d)\theta\pm_1\pi/2\pm_2\pi/2|_{2\pi}\le\frac{C_8}{|\lambda|^{b_k}}+\frac{C_8}{|\lambda|^d}\le\frac{2C_8}{|\lambda|^{\min\{b_k,d\}}}\,.$$

We put $j\pi=\pm_1\pi/2\pm_2\pi/2$ for $j\in\mathbb{Z}$.[4] Then by Baker's theorem (Thm. II.6), there is a constant $c_1>0$,

$$\begin{aligned}|b_k-d|^{-c_1}&<|e^{i((b_k-d)\theta+j\pi)}-1|\\&\le|(b_k-d)\theta+j\pi|_{2\pi}\\&\le\frac{2C_8}{|\lambda|^{\min\{b_k,d\}}}\,.\end{aligned}$$

Taking logarithms, we have:

$$\min\{b_k,d\}\log|\lambda|<\log(2C_8)+c_1\log|b_k-d|\,.\qquad(12)$$

Hence, if $d<b_k$, $|b_k-d|<b_k$ (as $d>0$) and

$$d\log|\lambda|<\log(2C_8)+c_1\log(b_k)\,.$$

Using that $d>\varepsilon^{-C_{10}}$ and $b_k\le 2(\varepsilon/2)^{-C_9}$, we obtain

$$\varepsilon^{-C_{10}}\log|\lambda|<\log(2C_8)+c_1\log(2)-c_1C_9\log(\varepsilon/2)\,.$$

This is impossible for sufficiently small ε. We can therefore assume that $d>b_k$. We take $\mathcal{I}_k:=\mathcal{J}_{b_k}(\delta_{k-1},\delta_k)$ such that Conditions (1) and (2) are satisfied. Now assume $d>b_k$ and let $D=d$ (and so Condition (3) automatically holds). For a contradiction, assume Condition (4) is violated. Lemma III.7 gives that for some fixed number $c_2>0$,

$$\frac{C_6(\delta_k-\delta_{k-1})}{|\lambda|^{b_k}b_k^{C_7}}\le|\mathcal{I}_k|\le\sum_{d'=D}^{\infty}|\mathcal{J}_d(1,\delta_\ell)|<c_2|\lambda|^{-d}\,.$$

Hence, setting $c_3=\log(\frac{c_2}{C_6(\delta_k-\delta_{k-1})})$ and taking logarithms,

$$(d-b_k)\log|\lambda|\le c_3+C_7\log(b_k)\,.\qquad(13)$$

Inserting the latter in (12) gives

$$b_k\log|\lambda|\le\log(2C_8)+c_1\log\left(\frac{c_3+C_7\log b_k}{\log|\lambda|}\right)\,,$$

which bounds b_k (independently of ε). As taking ε small gives arbitrarily large b_k, the result follows for k. Induction completes the proof. □

Now that we have solved the continuous version of our problem, we solve the discrete version and conclude the proofs of Thms. I.1 and I.4.

Proof of Thms. I.1 and I.4. As Thm. I.4 implies Thm. I.1 thanks to Lem. III.3, it is sufficient to prove Thm. I.4. In turn, Lem. III.4 states that Thm. I.4 is implied by the following statement: for all $N\in\mathbb{N}$, $T\ge 2$ 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) $n_1,\dots,n_\ell\ge N$;
2) $n_j\equiv t_j \pmod T$ for $1\le j\le\ell$;
3) $0<v_{n_1}<\cdots<v_{n_\ell}$;
4) for all $m\in\mathbb{N}$ such that $v_{n_1}\le v_m\le v_{n_\ell}$, $m\in\{n_1,\dots,n_\ell\}$.

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

Lem. III.6 gives numbers $b_2,\dots,b_\ell\in\mathbb{N}$ and $1<\delta_\ell<\sqrt{|\lambda|}$ and an interval $\mathcal{I}$. We take $n_1=n$ and for $2\le j\le\ell$, $n_j=n+b_j$ and claim that $n\ge N$, $n\equiv t_1 \pmod T$ and $n\theta+\phi\in\mathcal{I}$, imply the first three conditions. Indeed, $n_1\ge N$ and $n_1\equiv t_1 \pmod T$. For $2\le j\le\ell$, $n_j=n+b_j\ge N$ and

$$n_j\equiv n+b_j\equiv n+(t_j-t_1)\equiv t_j \pmod T\,.$$

For the third condition, we have that as $n\theta+\phi\in\mathcal{I}$,

$$\begin{aligned}0<\cos(n\theta+\phi)&<\cos((n+b_2)\theta+\phi)|\lambda|^{b_2}\\&<\cdots<\cos((n+b_\ell)\theta+\phi)|\lambda|^{b_\ell}\end{aligned}$$

and multiplying the last inequalities by $2|\lambda|^n$ and noting that $2\cos(m\theta+\phi)|\lambda|^m=v_m$ for all $m\in\mathbb{N}$, we obtain our claim.

Let $0<\varepsilon<|\mathcal{I}|$ be small enough. Lemma III.9 implies that there is an interval $\mathcal{I}_\varepsilon\subset\mathcal{I}$ of length ε such that for all $d<\varepsilon^{-C_{10}}$, $\mathcal{I}_\varepsilon\cap\mathcal{J}_d(1,\delta_\ell)=\emptyset$. By Lem. III.8, there is an n such that $\varepsilon^{-C_9}<n<2\varepsilon^{-C_9}$, $n\theta+\phi\in\mathcal{I}_\varepsilon$, and $n\equiv t_1 \pmod T$. Thus, for small enough ε, we also have that $n\ge N$.

Now assume that $m\notin\{n_1,\dots,n_\ell\}$ and $v_{n_1}<v_m<v_{n_\ell}$. Then, setting $d=n-m$, we have that $d\notin\{0,b_2,\dots,b_\ell\}$ and

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

[4] We have adorned the $\pm$ operator with subscripts (1 and 2) to indicate how the particular choice of signs should be preserved.

As $\cos((n+b_\ell)\theta+\phi)|\lambda|^{b_\ell} < \delta_\ell \cos(n\theta+\phi)$ because $n\theta+\phi \in \mathcal{I}$, $n\theta+\phi$ is in $\mathcal{J}_d(1,\delta_\ell)$. Thus, $d \geq \varepsilon^{-C_{10}}$. By Lem. III.7, $n\theta+\phi \in \mathcal{J}_d(1,\delta_\ell)$ and $-d\theta \pm \pi/2$ are at most $C_8|\lambda|^{-d}$ apart. Thus, for a constant c_1 derived from Thm. II.6,

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

Taking logarithms,

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

As $d \geq \varepsilon^{-C_{10}}$ and $n \geq \varepsilon^{-C_9}$, $n, d \geq 2$ for small enough ε. In that case, $n+d \leq dn$ and so

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

Hence, either

$$2\log(C_8) + 2c_1 \log(d) > d \log|\lambda|$$

or

$$2c_1 \log(n) > d \log|\lambda| .$$

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

$$2c_1 \log(2\varepsilon^{-C_9}) > \log|\lambda| \varepsilon^{-C_{10}} ,$$

which again is impossible for small enough ε. Hence the fourth condition also follows. □

IV. Concluding Remarks

Our main result, Thm. I.1, significantly expands the decidability landscape of the MSO theory of the structure $\langle \mathbb{N}; <, P\rangle$, by considering predicates P obtained as sets of non-degenerate simple LRS having two dominant roots. A natural question is whether any of these constraints can be relaxed any further. 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 [9] 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 [14]. 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. Finally, one might envisage expanding the present setup by adjoining further predicates. However even in the simplest of cases, one envisions quite formidable difficulties in attempting to follow that research direction; see [1].

References

[1] 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.

[2] Achim Blumensath. Monadic Second-Order Model Theory. http://www.fi.muni.cz/~blumens/, 2024. [Online; accessed on 24 January 2025].

[3] Émile M. Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo (1884-1940)*, 27(1):247–271, 1909.

[4] Mark Braverman. Termination of integer linear programs. In *CAV*, volume 4144 of *Lecture Notes in Computer Science*, pages 372–385. Springer, 2006.

[5] 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.

[6] Yann Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193. Cambridge University Press, 2012.

[7] Olivier Carton and Wolfgang Thomas. The monadic theory of morphic infinite words and generalizations. *Information and Computation*, 176(1):51–65, 2002.

[8] 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.

[9] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence Sequences*. Mathematical Surveys and Monographs. American Mathematical Society, 2003.

[10] Glyn Harman. One hundred years of normal numbers. In *Surveys in Number Theory*, pages 57–74. AK Peters/CRC Press, 2002.

[11] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:173–175, 1857.

[12] Lauwerens Kuipers and Harald Niederreiter. *Uniform distribution of sequences*. Courier Corporation, 2012.

[13] 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.

[14] Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *SODA*, pages 366–379. SIAM, 2014.

[15] Martine Queffélec. Old and new results on normality. *Lecture Notes-Monograph Series*, pages 225–236, 2006.

[16] Alexander Rabinovich. On decidability of monadic logic of order over the naturals extended by monadic predicates. *Information and Computation*, 205(6):870–889, 2007.

[17] 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.

[18] Aleksei Lvovich Semenov. Logical theories of one-place functions on the set of natural numbers. *Mathematics of the USSR-Izvestiya*, 22(3):587, 1984.

[19] S. Shelah. The monadic theory of order. *Ann. Math.*, 102:379–419, 1975.

[20] 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.

[21] Wolfgang Thomas. Languages, automata, and logic. In *Handbook of Formal Languages: Volume 3 Beyond Words*, pages 389–455. Springer, 1997.

[22] 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.