On the Decidability of Monadic Theories of Arithmetic Predicates

VALÉRIE BERTHÉ, Université Paris Cité, IRIF, CNRS, France

TOGHRUL KARIMOV, JORIS NIEUWVELD, JOËL OUAKNINE, and MIHIR VAHANWALA, Max Planck Institute for Software Systems, Germany

JAMES WORRELL, University of Oxford, Department of Computer Science, United Kingdom

We investigate the decidability of the monadic second-order (MSO) theory of the structure $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$, for various unary predicates $P_1, \ldots, P_d \subseteq \mathbb{N}$. We focus in particular on 'arithmetic' predicates arising in the study of linear recurrence sequences, such as fixed-base powers $k^{\mathbf{N}} = \{k^n : n \in \mathbb{N}\}$, kth powers $\mathbf{N}^k = \{n^k : n \in \mathbb{N}\}$, and the set of terms of the Fibonacci sequence $\mathsf{Fib} = \{0, 1, 2, 3, 5, 8, 13, \ldots\}$ (and similarly for other linear recurrence sequences having a single, non-repeated, dominant characteristic root). We obtain several new unconditional and conditional decidability results, a select sample of which are the following:

- The MSO theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, \mathsf{Fib} \rangle$ is decidable;
- The MSO theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, 3^{\mathbf{N}}, 6^{\mathbf{N}} \rangle$ is decidable;
- The MSO theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, 3^{\mathbf{N}}, 5^{\mathbf{N}} \rangle$ is decidable assuming Schanuel's conjecture;
- The MSO theory of $\langle \mathbb{N}; <, 4^{\mathbf{N}}, \mathbf{N}^2 \rangle$ is decidable;
- The MSO theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, \mathbf{N}^2 \rangle$ is Turing-equivalent to the MSO theory of $\langle \mathbb{N}; <, \gamma \rangle$, where $\gamma \colon \mathbb{N} \to \{0, 1\}$ is the binary expansion of $\sqrt{2} - 1$. The widely believed conjecture that $\sqrt{2}$ is *normal* implies decidability of both MSO theories.

These results are obtained by exploiting and combining techniques from dynamical systems, number theory, and automata theory. This paper is the journal version of [9].

Additional Key Words and Phrases: Monadic second-order logic, linear recurrence sequences, toric words, cutting sequences, decidability

ACM Reference Format:
Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. 2025. On the Decidability of Monadic Theories of Arithmetic Predicates. 1, 1 (November 2025), 31 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Büchi's seminal 1962 paper [12] established the decidability of the monadic second-order (MSO) theory of the structure $\langle \mathbb{N}; < \rangle$, and in so doing brought to light the profound connections between mathematical logic and automata theory. Over the ensuing decades, considerable work has been devoted to the question of which expansions of $\langle \mathbb{N}; < \rangle$ retain MSO decidability. In other words, for which unary predicates $P_1, \ldots, P_k$ is the MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_k \rangle$ decidable?[1] Here by unary predicate we mean a fixed set of non-negative integers $P \subseteq \mathbb{N}$. Taking, for example, P to be the set of

[1]The restricted focus on *unary* (or *monadic*) predicates is justified by the fact that most natural non-unary predicates immediately lead to undecidability; see, e.g., [46, Thm. 3].

Authors' addresses: Valérie Berthé, berthe@irif.fr, Université Paris Cité, IRIF, CNRS, , Paris, France, 75013; Toghrul Karimov, toghs@mpi-sws.org; Joris Nieuwveld, jnieuwve@mpi-sws.org; Joël Ouaknine, joel@mpi-sws.org; Mihir Vahanwala, mvahanwa@mpi-sws.org, Max Planck Institute for Software Systems, Saarland Informatics Campus, Saarbrücken, Germany, 66123; James Worrell, jbw@cs.ox.ac.uk, University of Oxford, Department of Computer Science, , Oxford, United Kingdom, OX1 3QD.

prime numbers, Büchi and Landweber [13] observed in 1969 that a proof of decidability of the MSO theory of $\langle \mathbb{N}; <, P\rangle$ would "seem very difficult", as it would *inter alia* enable one (at least in principle) to settle the twin prime conjecture. (Decidability was subsequently established assuming the linear case of Schinzel's hypothesis H [7], also known as Dickson's conjecture.)

The set of prime numbers is, of course, highly intricate. In 1966, Elgot and Rabin [21] considered a large class of simpler predicates of 'arithmetic' origin, such as, for any fixed k, the set $k^{\mathbf{N}} = \{k^n : n \in \mathbb{N}\}$ of powers of k, and the set $\mathbf{N}^k = \{n^k : n \in \mathbb{N}\}$ of kth powers. For any such predicate P, they systematically established decidability of the MSO theory of $\langle \mathbb{N}; <, P\rangle$ by using the so-called *contraction method*. Many years later, their automata-theoretic results were substantially developed and extended by, among others, Carton and Thomas [17], Rabinovich [39], and Rabinovich and Thomas [40], using the framework of *effectively profinite ultimate periodicity*. A related concept that plays a crucial role in this paper is that of *effective almost-periodicity*, introduced in the 1980s by Semënov [45], and recently brought to bear in the MSO model checking of linear dynamical systems [28].

It is notable that whilst Elgot and Rabin established separately the decidability of the MSO theories, for example, of $\langle \mathbb{N}; <, 2^{\mathbf{N}}\rangle$ and $\langle \mathbb{N}; <, 3^{\mathbf{N}}\rangle$, they remained resolutely silent on the obvious joint expansion $\langle \mathbb{N}; <, 2^{\mathbf{N}}, 3^{\mathbf{N}}\rangle$. This in hindsight is wholly unsurprising: there are various statements that one can express in the above theory whose truth values are highly non-trivial to determine. For example, for given fixed a, b, the assertion that there exist infinitely many powers of 3 whose distance to the next power of 2 is congruent to a modulo b. An immediate corollary of our first main result (Thm. 4.4) is that the MSO theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, 3^{\mathbf{N}}\rangle$ is indeed decidable. Although this is new, we should mention that decidability of the *first-order* theory of $\langle \mathbb{N}; <, 2^{\mathbf{N}}, 3^{\mathbf{N}}\rangle$ was proven (using quantifier elimination) over forty years ago by Semënov [44].

Looking over the last several decades' worth of research work on monadic second-order expansions of the structure $\langle \mathbb{N}; <\rangle$, it is fair to say that the bulk of the attention has focused on the addition of a *single* predicate P. The obvious reason is that whilst, in general, the decidability of single-predicate expansions of $\langle \mathbb{N}; <\rangle$ can usually be handled with automata-theoretic techniques alone, by reasoning about individual patterns in isolation, this is not the case when multiple predicates are at play simultaneously. Such collections of predicates can exhibit highly complex interaction patterns, which existing approaches are ill-equipped to handle. In this paper, we overcome these difficulties by showing that key aspects of such interactions can be modelled in the theory of *dynamical systems*.

Our approach to analysing decidability of the MSO theory of a structure $\mathbb{M} \coloneqq \langle \mathbb{N}; <, P_1, \ldots, P_d\rangle$ with $d \geq 1$ predicates is as follows. Firstly, using Büchi's original construction [12], given an MSO formula φ we can construct an automaton (over infinite words) such that φ holds in $\mathbb{M}$ if and only if $\mathcal{A}$ accepts the *characteristic word* α of $\mathbb{M}$, which records, for each P_i, the positions $n \in \mathbb{N}$ such that $n \in P_i$. That is, the decision problem of the MSO theory of $\mathbb{M}$ is Turing-equivalent to the *automaton acceptance problem* for α, denoted Acc_α. Next, we use arithmetic properties of specific $P_1, \ldots, P_d$ to argue that Acc_α is Turing-equivalent to Acc_β, which is the automaton acceptance problem for the so-called *order word* β of $\mathbb{M}$. The order word is a compressed version of the characteristic word that keeps track of only the order in which the elements of $P_1, \ldots, P_d$ occur. In the final step, we give dynamical systems that generate the order word β, and use their various properties to show decidability of Acc_β and hence the MSO theory of $\mathbb{M}$.

In this paper, we study two kinds of structures. Firstly, we study the case of $P_i = \{u_n^{(i)} \geq 0\}$, where $\langle u_n^{(i)}\rangle_{n=0}^\infty$ is a *linear recurrence sequence* with a single, non-repeated dominant root. These include geometric progressions $\langle a\rho^n\rangle_{n=0}^\infty$ for integers $a, \rho \geq 1$, as well as the Fibonacci numbers. In this case, the relevant dynamical systems are *translations on the d-dimensional torus* $\mathbb{T}^d \coloneqq [0, 1)^d$, given by $x \mapsto x + t$ for some $t \in \mathbb{T}^d$ where addition operates coordinatewise and modulo 1. These are fundamental compact dynamical systems that have been extensively studied from the perspectives of symbolic dynamics, ergodic theory, and number theory [14, 23]. Below we state specialised versions of our main results for MSO theories of value sets of LRS with a single, non-repeated dominant root.

Theorem (Weakened version of Thm. 4.4)**.** *Suppose we are given an MSO formula φ and positive integers $a_1, \rho_1, \ldots, a_d, \rho_d$ such that $\frac{1}{\log(\rho_1)}, \ldots, \frac{1}{\log(\rho_d)}$ are linearly independent over $\mathbb{Q}$, and for every $i \neq j$, $a_i\rho_i^n = a_j\rho_j^m$ has only finitely many solutions $(n, m) \in \mathbb{N}^2$. Then it is decidable whether φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d\rangle$, where $P_i = \{a_i\rho_i^n : n \in \mathbb{N}\}$.*

The linear independence condition holds, for example, when $d \leq 2$, or the set $\{\rho_1, \ldots, \rho_d\}$ contains at most two *multiplicatively independent* elements; See Lem. 2.11 for the precise formulation. This captures, for example, the case of $\rho_1 = 2$, $\rho_2 = 3$, and $\rho_3 = 6$. The role of the linear independence condition is to ensure that a certain *hypercubic billiard* dynamical system, which captures the order in which the elements of $P_1, \ldots, P_d$ occur, is non-degenerate; see Sec. 4.3. That $P_i \cap P_j$ should be finite for every $i \neq j$ is similarly a non-degeneracy condition.

Now suppose we have $a_1 = a_2 = a_3$, $\rho_1 = 2$, $\rho_2 = 3$, and ρ_3. It is widely believed that $1/\log(2), 1/\log(3), 1/\log(5)$ are linearly independent over $\mathbb{Q}$. However, no proof is known, and hence the theorem above does not apply. Nevertheless, we can conditionally deduce the required linear independence by invoking, for example, *Schanuel's conjecture* in transcendental number theory [48, Chap. 1.4]. Schanuel's conjecture is a unifying conjecture that, among others, completely describes all *polynomial* relations between logarithms of algebraic numbers, which in turn captures all *linear* relations between the inverses thereof. As another example, it implies that for any non-zero polynomial $p(x, y)$ with rational coefficients, $p(e, \pi) \neq 0$, i.e., the constants e and π are algebraically independent. It turns out that, for power predicates, assuming Schanuel's conjecture we can in fact prove the most general decidability result possible, handling in particular the cases where $1/\log(\rho_1), \ldots, 1/\log(\rho_d)$ are linearly dependent; see Thm. 4.6.

Theorem. *Suppose we are given an MSO formula φ and integers $a_1, \rho_1, \ldots, a_d, \rho_d \geq 1$. Assuming Schanuel's conjecture, it is decidable whether φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d\rangle$, where $P_i = \{a_i\rho_i^n : n \in \mathbb{N}\}$.*

We mention that throughout this paper, all conditional decision procedures that we give rely on Schanuel's conjecture only for termination and not correctness: whenever they terminate, the output assertion as to whether φ holds is unconditionally guaranteed to correct.

Having stated the theorems above, it is natural to ask: what if we fix the structure and allow only the formula φ to be given as the input? That is, for which $P_1, \ldots, P_d$ is the MSO theory decidable? We obtain the following, somewhat surprising result; see Thm. 4.9.

Theorem. *For any integers $a_1, \rho_1, \ldots, a_d, \rho_d \geq 1$, there exists an algorithm that, given an MSO formula φ, decides whether φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d\rangle$, where $P_i = \{a_i\rho_i^n : n \in \mathbb{N}\}$.*

The caveat is that the attendant decision procedure is *non-uniform* in a_i, ρ_i, $1 \leq i \leq d$, in that it "knows" the ideal of all polynomial relations between $\log(a_1), \log(\rho_1), \ldots, \log(a_d), \log(\rho_d)$.

When studying the ordering in which powers of integers occur (i.e., the order word corresponding to the predicates $P_1, \ldots, P_d$ above), we discover interesting connections to word combinatorics and the problem of determining the *factor complexity* (i.e., the number of distinct subwords of a given length n) for certain classes of infinite words. In Sec. 4.3, we discuss how it is possible to replace roughly half of the number theory we make use of with arguments from word combinatorics and automata theory, to establish weakened versions of our main theorems.

The second setting we consider is that of $\langle \mathbb{N}; <, P_1, P_2 \rangle$, where $P_1 = \{qn^d : n \in \mathbb{N}\}$ and $P_2 = \{pb^n : n \in \mathbb{N}\}$ for integers q, b, d, b. In this case, the underlying dynamical systems are given by maps $T_b : [0,1) \to [0,1)$, $T_b(x) = \{b \cdot x\}$ where $b \geq 2$ is an integer and $\{y\}$ denotes the fractional part of $y \in \mathbb{R}$. Iteratively applying T_b starting from $x \in [0,1)$ generates the expansion of x in base b. These are also fundamental dynamical systems that go as far back as the work of Rényi on β-expansions [41]. For the predicates P_1, P_2 above, we give a complete result that links their MSO theory to that of base-b expansions of certain algebraic numbers.[2]

Theorem (See Thm. 5.1)**.** *Let $b, d \geq 2$ and $p, q \geq 1$ be integers, $P_1 = \{qn^d : n \in \mathbb{N}\}$, and $P_2 = \{pb^n : n \in \mathbb{N}\}$. Write $\eta = \sqrt[d]{p/q}$, $\zeta = \sqrt[d]{1/b}$, and let $\gamma_0, \ldots, \gamma_{d-1} \in \{0, \ldots, b-1\}^\omega$ be the base-b expansions of $\{\eta\}, \{\eta\zeta\}, \ldots, \{\eta\zeta^{d-1}\}$, respectively. Then the MSO theories of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ and $\langle \mathbb{N}; <, \gamma_0, \ldots, \gamma_{d-1} \rangle$ are Turing-equivalent.*

Various interesting MSO decidability results follow readily from the above; see Sec. 5 for a detailed discussion.

(A) Taking $p = q = 1$ and $b = d = 2$, we obtain that the MSO theory of $\langle \mathbb{N}; <, \mathbf{N}^2, 2^{\mathbf{N}} \rangle$ is Turing-equivalent to that of $\langle \mathbb{N}; <, \gamma \rangle$, where γ is the binary expansion of $\sqrt{2} - 1$ viewed as function of type $\mathbb{N} \to \{0, 1\}$.

(B) The MSO theory of $\langle \mathbb{N}; <, b^{\mathbf{N}}, \mathbf{N}^d \rangle$ is decidable for any integers $k, d \geq 2$, where $b = k^d$. In this case, $\eta = 1$, $\zeta = 1/k$, and hence $\{\eta\}, \{\eta\zeta\}, \ldots, \{\eta\zeta^{d-1}\} \in \mathbb{Q}$. Recall that expansions of rational numbers in any integer base are ultimately periodic, and hence their representations as functions of type $\mathbb{N} \to \{0, \ldots, b-1\}$ are MSO-definable in $\langle \mathbb{N}; < \rangle$, which itself has a decidable MSO theory.

But what do we know about the expansion of an irrational algebraic number in an integer base b? For such an expansion α, it is known, for example, that $\liminf_{n \to \infty} \frac{\pi_\alpha(n)}{n} = +\infty$ where $\pi_\alpha(n)$ denotes the number of distinct finite words of length w that appear in α (Thm. 2.17). On the other hand, many simple results that would be subsumed by decidability of the MSO theory of an expansion in base b remain elusive: for example, at the time of writing no algorithm is known that decides whether a given finite word occurs in a given expansion. Nevertheless, expansions of irrational algebraic numbers in integer bases are widely conjectured to be *normal*, and *a fortiori disjunctive*: every finite pattern of digits should occur infinitely often. As the MSO theory of any disjunctive word is decidable (Thm. 3.5), the MSO theory of $\langle \mathbb{N}; <, \mathbf{N}^2, 2^{\mathbf{N}} \rangle$ is decidable assuming the binary expansion of $\{\sqrt{2}\} = \sqrt{2} - 1$ is disjunctive.

We recall necessary preliminaries from logic, automata theory, number theory, and word combinatorics in Sec. 2. In Sec. 3, we develop a range of automata-theoretic tools that allow us to reduce between the (decision problems of) MSO theories of various structures. In Sec. 4, we apply our toolbox to show how to decide MSO theories of multiple linear recurrence sequences with a single, non-repeated dominant root. Sec. 5 is dedicated to studying the MSO theories of structures $\langle \mathbb{N}; <, \{qn^d : n \in \mathbb{N}\}, \{qn^d : n \in \mathbb{N}\} \rangle$ through the lens of base-b expansions and normal numbers. Finally, Sec. 6 contains a brief discussion of our results and open problems concerning decidability of MSO theories.

2 PRELIMINARIES

We denote by $\mathbf{0}$ the tuple $(0, \ldots, 0)$ whose dimensions will be clear from the context. We write $\mathbb{T}$ for $[0,1)$, viewed as an additive group where addition operates modulo 1. For $x \in \mathbb{R}$, we write $\{x\}$ for the fractional part $x - \lfloor x \rfloor$ of x.

2.1 Words and automata

By an alphabet Σ we mean a finite non-empty set of letters. The sets of finite, finite non-empty, and infinite words over Σ are denoted Σ^*, Σ^+, and Σ^ω, respectively. For a finite or infinite word α and $n \in \mathbb{N}$, we write $\alpha(n)$ for the nth letter of α.

[2] We view the base-b expansion of $x \in [0,1)$ as an infinite word over $\{0, \ldots, b-1\}$, or equivalently, as a function of type $\mathbb{N} \to \{0, \ldots, b-1\}$.

Thus $\alpha = \alpha(0)\alpha(1)\cdots$. We define $\alpha[n,m) \coloneqq \alpha(n)\cdots\alpha(m-1)$, and assuming α is infinite, $\alpha[n,\infty) \coloneqq \alpha(n)\alpha(n+1)\cdots$. We denote the length of a finite word w by $|w|$. A finite word $w \in \Sigma^*$ *occurs* at a position n in α if $\alpha[n, n+|w|) = w$. Such w is called a *factor* of α. We denote by $\pi_\alpha(n)$ the number of distinct factors of length n of α. The function π_α is called the *factor complexity* of α.

A *deterministic finite Muller automaton* (simply called an *automaton* throughout the paper) $\mathcal{A}$ over an alphabet Σ is given by a tuple $(Q, q_{\text{init}}, \delta, \mathcal{F})$, where Q is the (finite) set of states, q_{init} is the initial state, $\delta\colon Q \times \Sigma \to Q$ is the transition function, and $\mathcal{F}$ is the acceptance condition consisting of subsets of Q. For $q \in Q$ and $u \in \Sigma^*$, we denote by $\delta(q,u)$ the state obtained when the automaton reads u, starting at the state q. We denote by $\mathcal{A}(\alpha)$ the sequence of states visited when $\mathcal{A}$ reads α. A word $\alpha \in \Sigma^\omega$ *is accepted* by $\mathcal{A}$ if the set S of states appearing infinitely often in $\mathcal{A}(\alpha)$ is present in $\mathcal{F}$. We write $\alpha \in L(\mathcal{A})$ to mean that $\mathcal{A}$ accepts α.

A *deterministic finite transducer* (simply called a *transducer* throughout the paper) $\mathcal{B}$ over an input alphabet Σ and an output alphabet Γ is given by $(R, r_{\text{init}}, \sigma)$, where R is the (finite) set of states, r_{init} is the initial state, and $\sigma\colon R\times\Sigma \to R\times\Gamma^*$ is the transition function. At every step, $\mathcal{B}$ reads a letter from the input alphabet Σ, transitions to the next state, and outputs a finite word over the output alphabet Γ. We denote by $\mathcal{B}(\alpha)$ the (possibly finite) word over Γ output by $\mathcal{B}$ upon reading $\alpha \in \Sigma^\omega$.

Let $\mathcal{A}$ be an automaton as above. By a *journey* on $\mathcal{A}$ we mean an element of $J \coloneqq Q \times Q \times 2^Q$. A path $q_0q_1q_2\cdots q_n \in Q^{n+1}$ *makes* the journey (q_0, q_n, V) where V is the set of states occurring in the proper suffix $q_1q_2\cdots q_n$. If $n \geq 1$, then $q_n \in V$ necessarily, but q_0 may not belong to V. The unique journey a word $w \in \Sigma^*$ makes starting in $q_0 \in Q$, denoted by $\operatorname{jour}(w, q_0)$, is the journey made by the path $q_0\cdots q_{|w|}$, where $q_{i+1} = \delta(q_i, w(i))$ for $1 \leq i < |w|$. The empty word makes journeys of the form $(q, q, \emptyset)$. If v makes the journey (q_1, q_3, V_1) and w makes the journey (q_3, q_2, V_2), then vw makes the journey $(q_1, q_2, V_1 \cup V_2)$.

Next, we define the equivalence relation $\sim_{\mathcal{A}}$ as follows. Two words $v, w \in \Sigma^*$ are equivalent, denoted $v \sim_{\mathcal{A}} w$ if the sets of journeys they can undertake (starting from various states) are identical. The equivalence is moreover a congruence: if $v \sim_{\mathcal{A}} w$ and $x \sim_{\mathcal{A}} y$, then $vx \sim_{\mathcal{A}} wy$. Observe that $\sim_{\mathcal{A}}$ is not the classical congruence associated with the automaton $\mathcal{A}$. Our choice, however, will be more convenient for technical reasons.

Since there are only finitely many equivalence classes of $\sim_{\mathcal{A}}$, the quotient of Σ^* by $\sim_{\mathcal{A}}$ is a finite monoid M, called the *journey monoid*. We use h to denote the natural morphism from Σ^* into M. The morphism h maps each letter to its equivalence class modulo $\sim_{\mathcal{A}}$. We also extend the function jour to take inputs from $M \times Q$: For an equivalence class $m = [w]$ and state q, we define $\operatorname{jour}(m, q) = \operatorname{jour}(w, q)$. Finally, we will need the following lemma, whose proof is immediate.

Lemma 2.1. *Let $\mathcal{A}$ be an automaton as above and $\alpha = u_0u_1\cdots \in \Sigma^\omega$, where $u_n \in \Sigma^*$ for all n. Then run of $\mathcal{A}$ on α can be decomposed as the concatenation of journeys*

$$(q_0, q_1, V_0)(q_1, q_2, V_1)(q_2, q_3, V_2)\cdots$$

where $q_0 = q_{\text{init}}$ and $\operatorname{jour}(u_n, q_n) = (q_n, q_{n+1}, V_n)$ for all n. Moreover, every $q \in Q$ appears infinitely often in $\mathcal{A}(\alpha)$ if and only if $q \in V_n$ for infinitely many $n \in \mathbb{N}$.

2.2 Monadic second-order logic

Monadic second-order logic (MSO) is an extension of first-order logic that allows quantification over subsets of the universe. Such subsets can be viewed as unary (that is, monadic) predicates. We will only be interpreting MSO formulas over expansions of the structure $\langle \mathbb{N}; < \rangle$. For a general perspective on MSO, see [11].

Let $\mathbb{S} \coloneqq \langle \mathbb{N}; <, P_1, \ldots, P_m \rangle$ be a structure where each $P_i \subseteq \mathbb{N}$ is a unary predicate. We associate a language $\mathcal{L}_\mathbb{S}$ of terms and formulas with $\mathbb{S}$ as follows. The terms of $\mathcal{L}_\mathbb{S}$ are the countably many constant symbols $\{0, 1, 2, \ldots\}$, lowercase variables that stand for elements of $\mathbb{N}$, and uppercase variables that denote subsets of $\mathbb{N}$. The formulas of $\mathcal{L}_\mathbb{S}$ are the well-formed statements constructed from the built-in equality (=) and membership ($\in$) symbols, logical connectives, quantification over elements of $\mathbb{N}$ (written Qx for a quantifier Q), and quantification over subsets (written QX for a quantifier Q). The MSO theory of the structure $\mathbb{S}$ is the set of all sentences belonging to $\mathcal{L}_\mathbb{S}$ that are true in $\mathbb{S}$. We write $\mathbb{S} \models \varphi$ to mean that the formula φ holds in the structure $\mathbb{S}$. The MSO theory of $\mathbb{S}$ is *decidable* if there exists an algorithm that, given a sentence $\varphi \in \mathcal{L}_\mathbb{S}$, decides whether $\mathbb{S} \models \varphi$.

As an example, consider $\mathbb{S} = \langle \mathbb{N}; <, P \rangle$ where P is the set of all primes. Let $s(\cdot)$ be the successor function defined by $s(x) = y$ if and only if

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

That is, $s(x) = x + 1$. Further let

$$\varphi(X) \coloneqq 1 \in X \ \wedge \ 0, 2 \notin X \ \wedge \ \forall x \colon x \in X \Leftrightarrow s(s(s(x))) \in X$$

$$\psi \coloneqq \exists X \colon \varphi(X) \ \wedge \ \forall y \, \exists z > y \colon z \in X \ \wedge \ P(z).$$

The formula φ defines the subset $\{n \colon n \equiv 1 \pmod 3\}$ of $\mathbb{N}$, and ψ is the sentence "there are infinitely many primes congruent to 1 modulo 3", which is the case. At the time of writing, it is not known whether the MSO theory of the structure $\mathbb{S}$ above is decidable.

The *Acceptance Problem* for an infinite word α, denoted Acc_α, is to determine, given an automaton $\mathcal{A}$, whether $\alpha \in L(\mathcal{A})$. Let $P_1, \ldots, P_d \subseteq \mathbb{N}$ be predicates and $\Sigma = \{0, 1\}^d$.

Definition 2.2. The *characteristic word* of $(P_1, \ldots, P_d)$, written $\alpha \coloneqq \mathrm{Char}(P_1, \ldots, P_d) \in \Sigma^\omega$, is defined by $\alpha(n) = (b_{n,1}, \ldots, b_{n,d})$ where $b_{n,i} = 1$ if $n \in P_i$ and $b_{n,i} = 0$ otherwise.

The following is a reformulation of the seminal result of Büchi through which he showed decidability of the MSO theory of $\langle \mathbb{N}; < \rangle$, which will also be used to prove all of our MSO decidability results. We state it for deterministic Muller automata, which are equivalent to non-deterministic Büchi automata [47]; the latter were used in the original proof of Büchi.

Theorem 2.3 ([47, Thms. 5.4 and 5.9]). *Given an MSO formula φ over predicates $P_1, \ldots, P_d$, we can construct an automaton $\mathcal{A}$ over $\Sigma \coloneqq \{0, 1\}^d$ such that for any structure $\mathbb{S} \coloneqq \langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$ with the characteristic word α,*

$$\mathbb{S} \models \varphi \Leftrightarrow \alpha \in L(\mathcal{A}).$$

In particular, the decision problem of the MSO theory of $\mathbb{S}$ is Turing-equivalent to the decision problem Acc_α.

2.3 Algebraic Numbers

A complex number λ is algebraic if there exists a non-zero polynomial $p \in \mathbb{Q}[x]$ such that $p(\lambda) = 0$. The set of algebraic numbers is denoted by $\overline{\mathbb{Q}}$. The unique irreducible monic polynomial $p \in \mathbb{Q}[x]$ that has λ as a root is called the *minimal* *polynomial* of λ. A *canonical representation* of an algebraic number λ consists of its minimal polynomial p and sufficiently accurate rational approximations of the real and imaginary parts of λ to distinguish it from the other roots of p. All arithmetic operations can be performed effectively on canonical representations of algebraic numbers; see, for example, [18, Sec. 4.2] and [26, Sec. 1.5.4].

Let $z_1, \dots, z_d \in \mathbb{C}^*$. The free abelian group

$$G_M(z_1, \dots, z_d) \coloneqq \{(k_1, \dots, k_d) : z_1^{k_1} \cdots z_d^{k_d} = 1\}$$

is called the *group of multiplicative relations* of $z_1, \dots, z_d$. We say that $z_1, \dots, z_d \in \mathbb{C}^*$ are *multiplicatively independent* if $G_M(z_1, \dots, z_d)$ is the trivial group. The *rank* of $G \coloneqq G_M(z_1, \dots, z_d)$ is the size of any of its *bases*: If $\operatorname{rank}(G) = m$, then G has a basis $B = \{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subseteq \mathbb{Z}^d$ that is linearly independent over $\mathbb{Q}$ with the property that every $\mathbf{z} \in G$ can be uniquely written as an integer linear combination of $\mathbf{v}_1, \dots, \mathbf{v}_m$. For non-zero algebraic $\lambda_1, \dots, \lambda_d$, we can compute a basis of G using a deep result of Masser [33], or the more recent polynomial-time algorithm of Combot [19].

2.4 Linear recurrence sequences

A sequence $\langle u_n \rangle_{n=0}^{\infty}$ over a ring R is a *linear recurrence sequence* (LRS) over R if there exist $c_1, \dots, c_d \in R$ such that

$$u_{n+d} = c_1 u_{n+d-1} + \cdots + c_d u_n \tag{1}$$

for all $n \in \mathbb{N}$. The smallest such d is called the *order* of $\langle u_n \rangle_{n=0}^{\infty}$. We will mostly work with LRS over $\mathbb{Z}$, which we also call *integer LRS*. For example, the Fibonacci sequence satisfies $u_{n+2} = u_{n+1} + u_n$ for all $n \in \mathbb{N}$, and is an integer LRS of order two. We refer the reader to the book [22] for a detailed account of LRS.

The *characteristic polynomial* of $\langle u_n \rangle_{n=0}^{\infty}$ is $p(x) \coloneqq x^d - \sum_{i=1}^{d} c_i x^{d-i}$. Suppose p has the (distinct) roots $\lambda_1, \dots, \lambda_m \in \overline{\mathbb{Q}}$, called the *characteristic roots* of $\langle u_n \rangle_{n=0}^{\infty}$. Then there exist unique polynomials $q_1, \dots, q_m \in \overline{\mathbb{Q}}[x]$ such that

$$u_n = q_1(n)\lambda_1^n + \cdots + q_m(n)\lambda_m^n \tag{2}$$

for all $n \in \mathbb{N}$. Equation (2) is known as the *exponential-polynomial form* of $\langle u_n \rangle_{n=0}^{\infty}$. A characteristic root λ_i is called *non-repeated* if q_i is constant and *dominant* when $|\lambda_i| \geq |\lambda_j|$ for all $1 \leq j \leq m$. Let $I \subseteq \{1, \dots, m\}$ contain the indices of all dominant roots, i.e., $i \in I$ if and only if $|\lambda_i| \geq |\lambda_j|$ for all $1 \leq j \leq m$. The sequence $\langle v_n \rangle_{n=0}^{\infty}$ given by $v_n = \sum_{i \in I} q_i(n)\lambda_i^n$ is called the *dominant part* of $\langle u_n \rangle_{n=0}^{\infty}$ and is an LRS over $\overline{\mathbb{Q}}$ but not necessarily over $\mathbb{Z}$. The sequence $\langle u_n \rangle_{n=0}^{\infty}$ is called *diagonalisable* (alternatively, *simple*) if q_i is constant for all $1 \leq i \leq m$.

Decision problems for linear recurrence sequences, despite being of central interest in algebraic number theory, largely remain open. The most famous problem is the *Skolem Problem*, which asks to decide whether a given LRS $\langle u_n \rangle_{n=0}^{\infty}$ contains zero. It is known to be decidable for sequences of order $d \leq 4$, and is open at order 5 and above [34]. Similarly, the *Positivity Problem* asks to decide whether a given LRS $\langle u_n \rangle_{n=0}^{\infty}$ satisfies $u_n \geq 0$ for all n. Decidability (or, for that matter, undecidability) of the Positivity Problem would imply substantial new results in Diophantine approximation that are currently believed to be out of reach [36]. For this reason, any decision problem to which the Positivity Problem can be reduced is referred to as *Positivity-hard.* Finally, the *Ultimate Positivity Problem* asks to decide whether a given LRS $\langle u_n \rangle_{n=0}^{\infty}$ satisfies $u_n \geq 0$ for all sufficiently large n. This problem is known to be decidable for LRS of order at most 5 as well as LRS (of any order) whose characteristic roots are all non-repeated [36, 37]. At order 6, decidability is again linked to certain open problems in Diophantine approximation [36].

We give two straightforward lemmas about linear recurrence sequences. First, the exponential-polynomial form (2) immediately implies an exponential upper bound on $|u_n|$, formalised below.

Lemma 2.4. *Let $\langle u_n \rangle_{n=0}^{\infty}$ be an LRS, $r, R \in \mathbb{R}_{>0} \cap \overline{\mathbb{Q}}$, and suppose $R > |\lambda_i|$ for any characteristic root λ_i of $\langle u_n \rangle_{n=0}^{\infty}$. We can compute $N \in \mathbb{N}$ such that $|u_n| \leq rR^n$ for all $n \geq N$.*

From (1) it readily follows that an integer LRS is ultimately periodic modulo any $m \in \mathbb{N}_{\geq 1}$. This is known as being *procyclic.*

Lemma 2.5. *Let $\langle u_n \rangle_{n=0}^{\infty}$ be an integer LRS, m be a positive integer, and define the sequence $\langle v_n \rangle_{n=0}^{\infty}$ as $v_n = u_n \bmod m$. We can compute $N \geq 0$ and $p > 0$ such that $v_{n+p} = v_n$ for all $n \geq N$.*

2.5 Schanuel's conjecture

A set $X = \{\alpha_1, \dots, \alpha_d\}$ of complex numbers is said to be *algebraically independent* over $\mathbb{Q}$ if $p(\alpha_1, \dots, \alpha_d) \neq 0$ for any non-zero polynomial $p \in \mathbb{Q}[x_1, \dots, x_d]$. The *transcendence degree* of X is the size of a largest subset of X that is algebraically independent over $\mathbb{Q}$. Below we state Schanuel's conjecture, a classical conjecture in transcendental number theory with far-reaching implications [30].

Conjecture 2.6 (Schanuel's conjecture). *If $\alpha_1, \dots, \alpha_d \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then the transcendence degree of $\{\alpha_1, \dots, \alpha_d, e^{\alpha_1}, \dots, e^{\alpha_d}\}$ is at least d.*

In particular, Schanuel's conjecture implies that $\log(\lambda_1), \dots, \log(\lambda_d)$ are algebraically independent over $\mathbb{Q}$ for multiplicatively independent $\lambda_1, \dots, \lambda_d \in \overline{\mathbb{Q}}^*$. We will use Schanuel's conjecture in the following way. Consider the structure $\mathbb{R}_{\exp} \coloneqq \langle \mathbb{R}; <, +, -, \cdot, \exp(\cdot), 0, 1 \rangle$ of real numbers equipped with arithmetic and (real) exponentiation. By the first-order theory of $\mathbb{R}_{\exp}$ we mean the set of all well-formed first-order sentences that are true in $\mathbb{R}_{\exp}$. In [32], Macintyre and Wilkie show that the first-order theory of the structure $\mathbb{R}_{\exp}$ is decidable assuming Schanuel's conjecture.

Theorem 2.7. *Assuming Schanuel's conjecture, given a sentence $\varphi \in \mathcal{L}_{\exp}$, we can decide whether $\mathbb{R}_{\exp} \models \varphi$. Moreover, Schanuel's conjecture is only required for termination and not correctness.*

The second statement in the theorem above means that the algorithm of Macintyre and Wilkie always terminates assuming Schanuel's conjecture, and whenever it does, it is unconditionally guaranteed to correctly decide whether $\mathbb{R}_{\exp} \models \varphi$.

2.6 Baker's theorem

By an *R-affine form*, where R is a ring, we mean $h(x_1, \dots, x_d) = a_0 + \sum_{i=1}^{d} a_i x_i$, where $a_i \in R$ for all $0 \leq i \leq d$. The following is a (rather weak) version of Baker's celebrated theorem on $\mathbb{Z}$-affine forms of logarithms [5].

Theorem 2.8. *Let $\rho_1, \dots, \rho_d \in \mathbb{R}_{>0} \cap \overline{\mathbb{Q}}$. There exists a computable constant $C > 0$ such that for all $b_1, \dots, b_d \in \mathbb{Z}$ with $B \coloneqq \max\{|b_1| + 2, \dots, |b_d| + 2\}$ and $\Lambda \coloneqq b_1 \log(\rho_1) + \cdots + b_d \log(\rho_d)$,*

$$\Lambda \neq 0 \Rightarrow |\Lambda| > B^{-C}.$$

From Baker's theorem, we derive the following consequence.

Theorem 2.9. *Let $\rho_1, \rho_2 > \mathbb{R}_{>1} \cap \overline{\mathbb{Q}}$ and $c_1, c_2 \in \mathbb{R} \cap \overline{\mathbb{Q}}$. There exists a computable constant C with the following property. Write $E(n_1, n_2) \coloneqq c_1 \rho_1^{n_1} + c_2 \rho_2^{n_2}$ for $n_1, n_2 \in \mathbb{N}$. Then*

$$E(n_1, n_2) \neq 0 \Rightarrow |E(n_1, n_2)| > \frac{\rho_1^{n_1}}{(n_1 + 2)^C}, \frac{\rho_2^{n_2}}{(n_2 + 2)^C}$$

for all $n_1, n_2 \in \mathbb{N}$.

Proof. We can assume that $c_1c_2 < 0$; otherwise the result is trivial. Suppose $E(n_1, n_2) \neq 0$. Then, for $(i, j) = (1, 2)$ or $(2, 1)$,

$$|E(n_1, n_2)| = |c_j| \cdot \rho_j^{n_j} \cdot \left| \frac{c_i}{c_j} \rho_i^{n_i} \rho_j^{-n_j} - 1 \right| > |c_j| \cdot \rho_j^{n_j} \cdot |\log(c_i/c_j) + n_i \log(\rho_i) - n_j \log(\rho_j)|$$

where we have used the fact that $e^x - 1 > x$ for all $x > 0$. Therefore,

$$|E(n_1, n_2)| > |c_j| \cdot \rho_j^{n_j} \cdot |\Lambda(n_1, n_2)|,$$

where $\Lambda(n_1, n_2) = |\log(c_1/c_2) + n_1 \log(\rho_1) - n_2 \log(\rho_2)| = |\log(c_2/c_1) + n_2 \log(\rho_2) - n_1 \log(\rho_1)|$. Therefore, we need construct $C > 0$ such that

$$|\Lambda(n_1, n_2)| > \frac{1}{|c_1|(n_1+2)^C}, \frac{1}{|c_2|(n_2+2)^C}.$$

Compute $\kappa > 1$ such that for all $n_1, n_2 \in \mathbb{N}_{\geq 1}$,

- $n_1 > \kappa n_2 \Rightarrow \log(c_1/c_2) + n_2 \log(\rho_2) < \frac{1}{2} n_1 \log(\rho_1)$, which, in turn, implies that $|\Lambda(n_1, n_2)| > \frac{1}{2} n_1 \log(\rho_1)$ as well as $|\Lambda(n_1, n_2)| > \frac{1}{2} n_2 \log(\rho_2)$, and
- $n_2 > \kappa n_1 \Rightarrow \log(c_1/c_2) + n_1 \log(\rho_1) < \frac{1}{2} n_2 \log(\rho_2)$, which implies that $|\Lambda(n_1, n_2)| > \frac{1}{2} n_2 \log(\rho_2), \frac{1}{2} n_1 \log(\rho_1)$.

It remains to consider the case where $\frac{n_2}{\kappa} \leq n_1 \leq \kappa n_2$ or $n_1 n_2 = 0$. In the former case, by Baker's theorem, there exists a computable constant $D > 0$ such that

$$|\Lambda(n_1, n_2)| > (\max\{2 + n_1, 2 + n_2\})^{-D} \geq (2 + \kappa n_i)^{-D}$$

for $i = 1, 2$. In the latter case, compute $M_1 := \min_{n \in \mathbb{N}} \{|\Lambda(0, n)| : \Lambda(0, n) \neq 0\}$ and $M_2 := \min_{n \in \mathbb{N}} \{|\Lambda(n, 0)| : \Lambda(n, 0) \neq 0\}$, which one can do as $\Lambda(0, n)$ and $\Lambda(n, 0)$ are linear in one variable and we can find the n for which they are zero. It remains to choose C sufficiently large such that

$$\frac{1}{(2 + \kappa n)^D}, \frac{1}{2} n \log(\rho_i), M_1, M_2 > \frac{1}{|c_i|(n+2)^C}$$

for all $n \in \mathbb{N}$ and $i = 1, 2$. □

Baker also proved the following, which is a very special case of Schanuel's conjecture. We will use it to prove the following two lemmas.

Theorem 2.10 (Thm. 1.6 in [48]). *Let $\rho_1, \ldots, \rho_d \in \mathbb{R}_{>0} \cap \overline{\mathbb{Q}}$ be multiplicatively independent, i.e., $\log(\rho_1), \ldots, \log(\rho_d)$ are linearly independent over $\mathbb{Q}$. Then $1, \log(\lambda_1), \ldots, \log(\lambda_d)$ are linearly independent over $\overline{\mathbb{Q}}$.*

Lemma 2.11. *Let $d \geq 2$, $\lambda_1, \ldots, \lambda_d \in \mathbb{R}_{>1} \cap \overline{\mathbb{Q}}$ be pairwise multiplicatively independent, and suppose*

$$\operatorname{rank}(G_M(\lambda_1, \ldots, \lambda_d)) \geq d - 2.$$

Then $1/\log(\lambda_1), \ldots, 1/\log(\lambda_d)$ are linearly independent over $\mathbb{Q}$.

Note that the condition $\operatorname{rank}(G_M(\rho_1, \ldots, \rho_d)) \geq d - 2$ is exactly the same as "each triple of distinct ρ_i, ρ_j, ρ_k is multiplicatively dependent", as well as "each triple of distinct $\log(\rho_i), \log(\rho_j), \log(\rho_k)$ is linearly dependent over $\mathbb{Q}$". This holds trivially when $d = 2$.

Proof of Lem. 2.11. By the two assumptions, for any distinct i, j, k there exist $b_i, b_j, b_k \in \mathbb{Z}_{\neq 0}$ such that $\lambda_i^{b_i} \lambda_j^{b_j} \lambda_k^{b_k} = 1$. Equivalently, $b_i \log(\lambda_i) + b_j \log(\lambda_j) + b_k \log(\lambda_k) = 0$. For $1 \leq j \leq d$, let $b_{1,j}, b_{2,j} \in \mathbb{Q}$ be such that $\log(\lambda_j) = b_{1,j} \log(\lambda_1) + b_{2,j} \log(\lambda_2)$. Then $b_{1,1} = b_{2,2} = 0$ and all other $b_{i,j}$ are non-zero.

Let $c_1, \ldots, c_d \in \mathbb{Q}$ be rational numbers such that $\sum_{j=1}^{d} c_j/\log(\lambda_j) = 0$. We will argue that $c_j = 0$ for all j. Multiplying by (the non-zero number) $\prod_{j=1}^{d} \log(\lambda_j)$ gives

$$\sum_{j=1}^{d} c_j \prod_{1 \le i \ne j \le d} \left(b_{1,j} \log(\lambda_1) + b_{2,j} \log(\lambda_2)\right) = 0,$$

which simplifies to

$$\sum_{i=0}^{d-1} e_i \log(\lambda_1)^i \log(\lambda_2)^{d-i} = 0$$

for some $e_i \in \mathbb{Q}$. Assume not all e_i are zero. Then dividing by $\log(\lambda_2)^{d-1}$ shows that $\log(\lambda_1)/\log(\lambda_2)$ is the root of the non-zero polynomial $\sum_{i=0}^{d-1} e_i x^i \in \mathbb{Q}[x]$. That is, $\log(\lambda_1)/\log(\lambda_2)$ is an algebraic number, say α, and hence $\log(\lambda_1) - \alpha \log(\lambda_2) = 0$, contradicting Thm. 2.10 λ_1 and λ_2 are multiplicatively independent. Therefore, all e_i have to be zero. It follows that the rational function

$$f(x, y) \coloneqq \sum_{j=1}^{d} \frac{c_i}{b_{1,j}x + b_{2,j}y} = 0$$

must be zero everywhere it is defined.

Suppose $c_i \ne 0$ for some i. By the multiplicative independence assumption, the following holds. For every $\lambda \in \mathbb{Q}$ and $j \ne i$, it is not the case that for all $x, y \in \mathbb{R}$, $b_{1,i}x + b_{2,i}y = \lambda(b_{1,j}x + b_{2,j}y)$. (Since $b_{1,j}, b_{2,j} \in \mathbb{Q}$ for all j, the same holds for all $\lambda \in \mathbb{R}$ and $i \ne j$.) Therefore, we can find $\widetilde{x}, \widetilde{y} \in \mathbb{Q}$ such that $b_{1,i}\widetilde{x} + b_{2,i}\widetilde{y} = 0$ and $b_{1,j}\widetilde{x} + b_{2,j}\widetilde{y} \ne 0$ for all $j \ne i$. Now consider what happens as $(x, y) \to (\widetilde{x}, \widetilde{y})$. We have that for all $j \ne i$, $b_{1,j}\widetilde{x} + b_{2,j}\widetilde{y} \to z_j$ for some non-zero $z_j \in \mathbb{Q}$, but $b_{1,i}\widetilde{x} + b_{2,i}\widetilde{y} \to 0$, which implies that $|f(x, y)|$ must diverge. This contradicts the fact that $f(x, y)$ is constant everywhere it is defined, which implies that $c_i = 0$. □

Lemma 2.12. *Given $\lambda_1, \ldots, \lambda_d \in \overline{\mathbb{Q}}$ and $a_0, \ldots, a_d \in \mathbb{Q}$, we can effectively determine the sign of $a_0 + \sum_{i=1}^{d} a_i \log(\lambda_i)$.*

Proof. By computing a basis of $G_M(\lambda_1, \ldots, \lambda_d)$ (see Sec. 2.3), we can rewrite this expression as $a_0 + \sum_{i=1}^{e} b_i \log(\mu_i)$, where for all $1 \le i \le e$, $b_i \ne 0$, $\mu_i = \lambda_j$ for some j, and $\mu_1, \ldots, \mu_e$ are multiplicatively independent. By Thm. 2.10, this expression is zero if and only if $a_0 = b_1 = \cdots = b_e = 0$. If it is non-zero, we can compute its sign by approximating its value from above and below to arbitrary precision. □

2.7 Kronecker's theorem and translations on a torus

Recall that $\mathbb{T}$ denotes $[0, 1)$, viewed as a group with addition modulo 1. In our analysis of MSO theories of powers of integers, we will frequently encounter compact dynamical systems of the form

$$(\mathbb{T}^d, g_\delta\colon \mathbb{T}^d \to \mathbb{T}^d), \qquad g_\delta((x_1, \ldots, x_d)) = (\{x_1 + \delta_1\}, \ldots, \{x_d + \delta_d\})$$

for some $\delta = (\delta_1, \ldots, \delta_d) \in \mathbb{T}^d$. These dynamical systems are well-understood thanks to Kronecker's theorem on Diophantine approximation. Let $\delta = (\delta_1, \ldots, \delta_d) \in \mathbb{T}^d$, and define the groups of affine linear relations and linear relations, respectively, as

$$G_A(\delta_1, \ldots, \delta_d) = \{(k_0, \ldots, k_d) \in \mathbb{Z}^{d+1} : k_1\delta_1 + \cdots + k_d\delta_d = k_0\} \quad \text{and}$$
$$G_L(\delta_1, \ldots, \delta_d) = \{(k_1, \ldots, k_d) \in \mathbb{Z}^{d} : k_1\delta_1 + \cdots + k_d\delta_d = 0\}.$$

Further, let

$$X_\delta = \{(x_1, \dots, x_d \in \mathbb{T}^d) : G_A(x_1, \dots, x_d) \subseteq G_L(\delta_1, \dots, \delta_d)\}.$$

The following is a rephrasing of Kronecker's theorem in Diophantine approximation [24].

Theorem 2.13. *The orbit of* $\mathbf{0} \in \mathbb{T}^d$ *under the map* g_δ *is dense in* X_δ.

That is, every open subset of X_δ is visited infinitely often by the orbit of $\mathbf{0}$ and X_δ is a closed set. For $s \in \mathbb{T}^d$, define $X_{\delta,s} = \{s + x : x \in X_\delta\}$. The following is an immediate consequence of Kronecker's theorem.

Theorem 2.14. *The orbit of* $s \in \mathbb{T}^d$ *under the map* g_δ *is dense in* $X_{\delta,s}$.

Corollary 2.15. *Let* $Z \subseteq \mathbb{T}^d$ *be open. For any* $s \in \mathbb{T}^d$*, the set* $T \coloneqq \{n \in \mathbb{N} : g_\delta^{(n)}(s) \in Z\}$ *is either empty, or has uniformly bounded gaps.*

Proof. If $\widetilde{Z} \coloneqq Z \cap X_{\delta,s} = \emptyset$, then T is empty. Now suppose $\widetilde{Z} \neq \emptyset$. Let $\widetilde{Z}_k = g_\delta^{(-k)}(\widetilde{Z})$ for $k \geq 0$. By Thm. 2.14, these sets form an open cover of $\widetilde{Z}$. Because $X_{\delta,s}$ is compact (being closed and bounded), there exists K such that $\widetilde{Z}_0, \dots, \widetilde{Z}_{-K}$ covers $X_{\delta,s}$ and thus $\widetilde{Z} \subset X_{\delta,s}$. It follows that any $g_\delta^{(n)}(s)$ "falls into" $\widetilde{Z}$ within at most K steps. Therefore, for any $n \geq K$, $n \in T$, there exist $n_1, n_2 \in T$ such that $n - K \leq n_1 < n < n_2 \leq n + K$. □

2.8 Normal numbers

Call a number $a \in \mathbb{R}$ is *disjunctive in base b* if its base-b expansion α is a disjunctive word, i.e. α contains infinitely many occurrences of every $w \in \{0, \dots, b-1\}^*$. Disjunctivity is a weaker property than the more well-known property of being a *normal number*: in the latter case, the *frequency* of occurrences of every finite word $w \in \{0, \dots, b-1\}$ has to be equal to $b^{-|w|}$. For a detailed discussion of disjunctivity, see the book [15] and of normal numbers, see surveys [25, 38] and the book [14]. In particular, [25] states the following conjecture.

Conjecture 2.16. *A real irrational algebraic number* α *is normal in any integer base* $b \geq 2$.

Thus, in particular, this conjecture implies that every real irrational algebraic number is disjunctive in any integer base. The strongest result towards this conjecture is due to Adamczewski and Bugeaud [1].

Theorem 2.17. *If* $b \geq 2$*,* α *is the base-*b *expansion of a real irrational algebraic number, and* π_α *denotes the factor complexity of* α*, then*

$$\liminf_{n \to \infty} \frac{\pi_\alpha(n)}{n} = +\infty.$$

2.9 Fourier-Motzkin elimination

Fourier-Motzkin elimination is a method for solving systems of linear equalities and inequalities over the reals. Suppose we are given the system

$$\Phi(x_1, \dots, x_m) \coloneqq \bigwedge_{i \in I} a_{i,1}x_1 + \cdots + a_{i,m}x_m \sim_i b_i \ \wedge \ \bigwedge_{j \in j} a_{j,1}x_1 + \cdots + a_{j,m}x_m \sim_j b_j$$

where $a_{i,k}, b_i \in \mathbb{R}$ are some constants, $a_{i,k}, a_{j,k} > 0$, $\sim_i \in \{>, \geq\}$, and $\sim_j \in \{<, \leq\}$ for all i, j, k. Then $\Phi(x_1, \dots, x_m)$ can be written as

$$\bigwedge_{i \in I} x_1 \sim_i \frac{a_{i,2}}{a_{i,1}}x_2 + \cdots + \frac{a_{i,m}}{a_{i,1}}x_m + b_i \ \wedge \ \bigwedge_{j \in J} x_1 \sim_j \frac{a_{j,2}}{a_{j,1}}x_2 + \cdots + \frac{a_{j,m}}{a_{j,1}}x_m + b_j$$

and hence the formula $\exists x_1 : \Phi(x_1, \ldots, x_m)$ is equivalent to

$$\bigwedge_{i \in I, j \in J} \frac{a_{i,2}}{a_{i,1}} x_2 + \cdots + \frac{a_{i,m}}{a_{i,1}} x_m + b_i \sim_{i,j} \frac{a_{j,2}}{a_{j,1}} x_2 + \cdots + \frac{a_{j,m}}{a_{j,1}} x_m + b_j$$

where $\sim_{i,j}$ is $\leq$ if both $\sim_i$ and $\sim_j$ are non-strict, and $\sim_{i,j}$ is $<$ otherwise. Hence we can eliminate the variable x_1.

Let A be the set of all numbers that appear as the coefficient of some x_i in Φ (i.e., the set of all $a_{i,k}, a_{j,k}$), and B be the set of all other constants (i.e., the set of all b_i, b_j). By repeating the process described above, we can construct a Boolean combination Ψ of linear inequalities (without any free variables) in the elements of B with coefficients that are polynomial in the elements of A such that Ψ is true if and only if $\exists x_1, \ldots, x_m : \Phi(x_1, \ldots, x_m)$ is true.

3 A TOOLBOX FOR PROVING MSO DECIDABILITY

We recall classical results in Sec. 3.1 and 3.2. Thereafter we give our main new results concerning MSO decidability.

3.1 Uniformly recurrent words

A word $\alpha \in \Sigma^\omega$ is

- *recurrent* if every factor $u \in \Sigma^*$ of α occurs infinitely often in α, and
- *uniformly recurrent* if it is recurrent and for every factor u, the gaps between consecutive occurrences of u in α are bounded. In this case, we define $R_\alpha(n)$ to be the smallest integer R such that every factor u of α with $|u| = n$ appears in $\alpha[k, k+R)$ for all k. The function R_α is called the *recurrence function* of α.

Prominent examples of uniformly recurrent words include the Thue-Morse word [2, Chap. 1] and all Sturmian words [31, Chap. 2]. The following is due to Semënov [45], and a modernized version of this proof is given in [26, Section 3.1].[3]

Theorem 3.1. *Suppose we are given an automaton $\mathcal{A}$ and a uniformly recurrent word α, represented by (i) an oracle to compute $\alpha(n)$ given n, and (ii) an oracle to compute $R_\alpha(n)$ given n. Then we can decide whether $\mathcal{A}$ accepts α.*

Corollary 3.2. *Suppose we are given an automaton $\mathcal{A}$ and a uniformly recurrent word α represented by the oracle (i) above and either*

(iii) *an oracle to decide whether a given finite word u occurs in α, or*
(iv) *an oracle to compute the factor complexity $\pi_\alpha(n)$ given n.*

Then we can decide whether $\mathcal{A}$ accepts α.

Proof. Suppose we can decide whether a given u occurs in α. Then for any k, we can compute the set $L(k)$ of all factors of α of length k. Thus we can compute $R_\alpha(n)$ by computing $L(k)$ for increasing values of $k \geq n$ until we arrive at a set of finite words all of which contain all of $L(n)$ as factors.

Now suppose we can compute $\pi_\alpha(n)$ given n. Then we can decide whether u occurs in α by first computing $\pi_\alpha(|u|)$, and then computing increasingly larger prefixes of α until we have seen $\pi_\alpha(|u|)$ different factors of length $|u|$. At that point we can decide whether u occurs in α. ◻

3.2 Profinitely ultimately periodic words

Carton and Thomas [17] introduced the class of profinitely ultimately periodic words as a framework to generalise the *contraction method* of Elgot and Rabin [21]. Let Σ be an alphabet.

[3] In fact, Semënov's result works for the more general class of *effectively almost-periodic* words, in which every factor occurs either finitely many times, or with bounded gaps.

(a) A sequence of finite words $\langle u_n \rangle_{n\in\mathbb{N}}$ is *effectively profinitely ultimately periodic* [17] if for any morphism $h\colon \Sigma^* \to M$ into a finite monoid M, we can compute integers N, m with $m \geq 1$ such that for all $n \geq N$, $h(u_n) = h(u_{n+m})$.

(b) An infinite word α is *effectively profinitely ultimately periodic* if it can be effectively factorised (by, e.g., a Turing machine that is given α as input) as an infinite concatenation $u_0 u_1 \cdots$ of finite non-empty words forming an effectively profinitely ultimately periodic sequence [39].

(c) We say that a strictly increasing function $f\colon \mathbb{N} \to \mathbb{N}$ is *effectively contractive* if for any morphism $h\colon \mathbb{N} \to M$ into a finite monoid, the sequence $\langle h(f(n+1) - f(n) - 1)\rangle_{n=0}^{\infty}$ is ultimately periodic with computable period and pre-period.

We have the following results about MSO decidability.

Theorem 3.3. *Let $\alpha \in \Sigma^\omega$, and suppose we can compute $\alpha(n)$ given n. The problem* Acc_α *is decidable if and only if α is effectively profinitely ultimately periodic.*

The "if" direction of Thm. 3.3 is due to Carton and Thomas [17], and the converse is due to Rabinovich [39]. Every infinite word is profinitely ultimately periodic, as a close inspection of the use of Ramsey's theorem in Rabinovich's proof reveals. The effectiveness distinguishes words whose automaton acceptance problem is decidable. A comprehensive class of predicates whose characteristic words ($\alpha \in \{0, 1\}^\omega$) are effectively profinitely ultimately periodic is identified by [17, Thm. 5.2]. This class includes fixed base powers $k^{\mathbf{N}}$ as well as kth powers $\mathbf{N}^k$ (see the Introduction).

Effectively contractible words, where f itself is computable, are more restrictive than effectively profinitely ultimately periodic words: in the latter case, we are free to choose the factorisation, but in the former case, the factorisation has to be the natural one. It turns out, however, that effectively contractible words have better compositional properties (Sec. 3.6). For now, we record the following corollary of Thm. 3.3.

Corollary 3.4. *The MSO theory of $\langle \mathbb{N}; <, P\rangle$, where $P = \{f(n) : n \in \mathbb{N}\}$ for a computable and effectively contractive function f, is decidable.*

Proof. The characteristic word α of P is effectively profinitely ultimately periodic, with the required factorisation of α being $0^{f(0)}10^{f(1)-f(0)-1}10^{f(2)-f(1)-1}1\ldots$. □

3.3 Disjunctive words

Recall that a word $\alpha \in \Sigma^\omega$ is *disjunctive* if every $u \in \Sigma^*$ appears infinitely often in α. Disjunctivity is usually considered when $\Sigma = \{0, \ldots, b-1\}$ is the alphabet of digits and α is the base-b expansion of a real number $x \in [0, 1]$. Thus, when $x = \sqrt{2} - 1 = 0.41421356\cdots$ and $b = 10$, $\alpha = 41421356\cdots$. We have the following result about such words.

Theorem 3.5. *If α is disjunctive, then* Acc_α *is decidable.*

Intuitively, the proof uses the abundance of all factors in α to deduce that the set of states visited infinitely often is an entire bottom strongly connected component in the graph induced by the automaton.

Proof. Consider an automaton $\mathcal{A}$ as a directed graph allowing multiple edges. We partition the graph into its strongly connected components (SCCs) and call an SCC without outgoing edges a bottom SCC. We will show that the set of states visited infinitely often by the run of $\mathcal{A}$ on α is precisely a bottom SCC. Hence, we decide Acc_α by simulating this run until a bottom SCC is inevitably reached. Then α is accepted if and only if this bottom SCC is in the (Muller) acceptance condition.

We need to show that (a) if an SCC is not a bottom SCC, then the run eventually exits it; and (b) if the run enters a bottom SCC, it visits all its states infinitely often. To prove (a), let S be a non-bottom SCC. Order the states of S as $q_1, \ldots, q_n$. Inductively construct a sequence of words $u_1, \ldots, u_n \in \Sigma^+$, starting with $k = 1$, such that for all $1 \leq k \leq n$, $\delta(q_k, u_1 \cdots u_k) \notin S$. Here, u_{k+1} can be chosen to be any word such that takes the automaton from the state $\delta(q_{k+1}, u_1 \cdots u_k)$ to state outside S. Then the word $u = u_1 \cdots u_n$ is such that for any $q \in S$, $\delta(q, u) \notin S$. By disjunctivity, u occurs in α. It follows that when reading α from any $q \in S$ the run will exit S.

We prove (b) similarly. Let S be a bottom SCC consisting of the states $q_1, \ldots, q_n$, and $q \in S$. Inductively construct $u_1, \ldots, u_n \in \Sigma^+$ such that $\delta(q_k, u_1 \cdots u_k) = q$ for all k. Here, u_{k+1} can be chosen to be any word that takes the automaton from the state $\delta(q_{k+1}, u_1 \cdots u_k)$ to the state q. It follows that whenever the word $u = u_1 \cdots u_n$ is read, regardless of from which state in S, the state q will be visited. By disjunctivity we have that every $q \in S$ is visited infinitely often. □

3.4 Closure under transductions

In this section, when we say a word $\alpha \in \Sigma^\omega$ is given, we mean that an oracle is given that computes $\alpha(n)$ on input n. Our first result is that automaton acceptance for an infinite word $\alpha = \mathcal{T}(\beta)$, where $\mathcal{T}$ is a transducer, can be reduced to automaton acceptance for β.

Lemma 3.6. *Suppose we are given $\alpha \in \Sigma_1^\omega$, $\beta \in \Sigma_2^\omega$, an automaton $\mathcal{A}$, and a transducer $\mathcal{T}$ such that $\alpha = \mathcal{T}(\beta)$. We can compute an automaton $\mathcal{B}$ such that $\alpha \in L(\mathcal{A}) \Leftrightarrow \beta \in L(\mathcal{B})$.*

Proof. Write $\mathcal{A} = (Q, q_{\text{init}}, \delta, \mathcal{F})$ and $\mathcal{T} = (R, r_{\text{init}}, \sigma)$. The automaton $\mathcal{B}$ simulates what $\mathcal{T}$ would do upon reading α, and furthermore, what $\mathcal{A}$ would do upon reading each output block of $\mathcal{T}(\alpha)$.

The set of states of $\mathcal{B}$ is $Q' = J \times R$, where J is the set of journeys in $\mathcal{A}$. Each state keeps track of the last journey made in $\mathcal{A}$ and the current state in $\mathcal{T}$. We further define $q'_{\text{init}} = ((q_{\text{init}}, q_{\text{init}}, \emptyset), r_{\text{init}})$ and

$$\delta'(((p, q, V), r), b) = (\text{jour}(q, u), r')$$

where $\sigma(r, b) = (r', u)$. By Lem. 2.1, a state s appears infinitely often in $\mathcal{A}(\alpha)$ if and only if a state $((p, q, V), r)$ with $s \in V$ appears infinitely often in $\mathcal{B}(\beta)$. We therefore define $\mathcal{F}'$ by

$$F' \in \mathcal{F}' \iff \left(\bigcup_{((p,q,V),r) \in F'} V \right) \in \mathcal{F}$$

and $\mathcal{B} = (Q', q'_{\text{init}}, \delta', \mathcal{F}')$. □

Corollary 3.7. *Let $\alpha \in \Sigma_1^\omega$, $\beta \in \Sigma_2^\omega$, and suppose that $\alpha = \mathcal{T}(\beta)$ for a transducer $\mathcal{T}$. Then Acc_α reduces to Acc_β.*

We next give a generalisation of Lem. 3.6 that we will be crucial throughout the paper. Here we transduce from β not into α but rather a "compressed" version thereof, where the compression is performed by a morphism into a finite monoid. Given an automaton $\mathcal{A}$, we can choose the monoid to be the journey monoid, and show that to the automaton $\mathcal{A}$, α is indistinguishable from its relevant "compressed" version.

Theorem 3.8. *Suppose we are given $\alpha \in \Sigma_1^\omega$, $\beta \in \Sigma_2^\omega$, an automaton $\mathcal{A}$, and an oracle that, given a morphism $h \colon \Sigma_1^* \to M$ into a finite monoid M, computes a transducer $\mathcal{T}$ (with input alphabet Σ_2 and output alphabet M) with the following property: There exists a factorisation $\alpha = \prod_{n=0}^\infty w_n$ such that $\prod_{n=0}^\infty h(w_n)$ is a factorisation of $\mathcal{T}(\beta)$. Then we can compute an automaton $\mathcal{B}$ such that $\alpha \in L(\mathcal{A}) \Leftrightarrow \beta \in L(\mathcal{B})$.*

Proof. Let J be the set of all journeys in $\mathcal{A}$, M be the journey monoid of $\mathcal{A}$, $h\colon \Sigma_1^* \to M$ be the morphism mapping each finite word to the equivalence class of its set of journeys in $\mathcal{A}$, $\mathcal{T}$ be the corresponding transducer, and $\alpha = \prod_{n=0}^{\infty} w_n$ be the corresponding factorisation. Write $\mathcal{A} = (Q, q_{\text{init}}, \delta, \mathcal{F})$ and $\mathcal{T} = (R, r_{\text{init}}, \sigma)$. We construct an automaton $\mathcal{M} = (J, (q_{\text{init}}, q_{\text{init}}, \varnothing), \delta', \mathcal{F}')$ over the alphabet M as follows. The states simply record the last journey taken. For $(p, q, V) \in J$ and $x \in M$, we define $\delta'((p, q, V), x) = \text{jour}(q, x)$. Finally, we define the acceptance condition by

$$F' \in \mathcal{F}' \iff \left(\bigcup_{(q,r,V) \in F'} V \right) \in \mathcal{F}.$$

Then $\mathcal{M}(\mathcal{T}(\beta))$ is factorisation of the run of $\mathcal{A}$ on α into journeys as in Lem. 2.1, and $\alpha \in L(\mathcal{A}) \Leftrightarrow \mathcal{T}(\beta) \in L(\mathcal{M})$. Applying Lem. 3.6, we construct an automaton $\mathcal{B}$ such that $\mathcal{T}(\beta) \in L(\mathcal{M}) \Leftrightarrow \beta \in L(\mathcal{B})$. □

3.5 Sparse procyclic predicates

We now discuss the main automata-theoretic tool that will be used Sec. 4. The idea is that we reduce from the characteristic word to its compressed version, called the *order word*. Let $P_1, \ldots, P_d$ be infinite predicates with the characteristic word $\alpha \in (\{0,1\}^d)^\omega$. Order the elements of P_i as $\langle p_n^{(i)} \rangle_{n=0}^{\infty}$.

Definition 3.9 (Order Word). The order word of $P_1, \ldots, P_d$, written $\text{Ord}(P_1, \ldots, P_d)$, is the infinite word obtained by deleting all occurrences of $\mathbf{0}$ from α.

In compressing the characteristic word α to the order word β, one only retains partial information, i.e. a particular aspect of the interaction between predicates. Not surprisingly, by an immediate application of Lem. 3.6, given an automaton $\mathcal{B}$ we can construct an automaton $\mathcal{A}$ such that $\alpha \in L(\mathcal{A}) \Leftrightarrow \beta \in L(\mathcal{B})$ for any characteristic word α. In particular, Acc_β reduces to Acc_α. Remarkably however, under certain circumstances, the order word captures all the information we need to decide automaton acceptance, and we can perform the reverse reduction. To see this, write

$$\alpha = \mathbf{0}^{k_0} \beta(0) \cdots \mathbf{0}^{k_n} \beta(n) \cdots$$

and suppose we want to decide whether $\alpha \in L(\mathcal{A})$. The automaton $\mathcal{A}$ is finite, and consequently one can compute $L, p > 0$ such that for all $n \geq L$, it cannot distinguish $\mathbf{0}^n$ from $\mathbf{0}^{n+p}$. Provided that k_n is persistently larger than L, it suffices to only keep track of k_n modulo p. That is, we can construct an automaton $\mathcal{A}'$ such that $\alpha \in L(\mathcal{A}) \Leftrightarrow \alpha' \in L(\mathcal{A}')$ where $\alpha' = \mathbf{0}^{m_0} \beta(0) \cdots \mathbf{0}^{m_n} \beta(n) \cdots$ and each m_n is small but indistinguishable from k_n by $\mathcal{A}$. We can then hope to insert the sequence $\langle \mathbf{0}^{m_n} \rangle_{n=0}^{\infty}$ into β: that is, construct a transducer C such that $\alpha' = C(\beta)$. Then by Lem. 3.6, deciding whether $\alpha' \in L(\mathcal{A}')$ reduces to deciding whether $\beta \in L(\mathcal{B})$ for an automaton $\mathcal{B}$ computed from $\mathcal{A}'$ and C. We next formalise this argument. We say that a sequence $\langle u_n \rangle_{n=0}^{\infty}$ (over any countable set Σ) is *effectively procyclic* if, given $m \geq 1$, we can compute N, p such that $u_{n+p} \bmod m = u_n \bmod p$ for all $n \geq N$.

Definition 3.10 (Effectively Procyclic Predicates). The predicates $P_1, \ldots, P_d$ are effectively procyclic if each $\langle p_n^{(i)} \rangle_{n=0}^{\infty}$ is effectively procyclic.

Note that the predicates $(P_1, \ldots, P_d)$ being (effectively) procyclic is equivalent to the characteristic word α, viewed as an infinite sequence, being (effectively) procyclic. We briefly argue that for a single predicate P, the notions of being effectively procyclic and having an effectively profinitely ultimately periodic characteristic word are incomparable. Firstly, let $\alpha \in \{0,1\}^\omega$ be such that $\alpha(n)$ can be computed given n, but Acc_α is undecidable. For example,[4] writing t_m

[4] This example is due to Edon Kelmendi.

for the mth prime number, we can take

$$\alpha(n) = 1 \Leftrightarrow n = t_m^k \text{ for some } m, k \text{ and the } m\text{th Turing Machine halts (on empty input) in at most } k \text{ steps.}$$

Then the mth Turing machine does not halt on empty input if and only if there exist infinitely many $n \equiv 0 \pmod{t_m}$ such that $\alpha(n) = 1$. Note that by undecidability of Acc_α, both 0 and 1 must occur infinitely often in α. Construct β by replacing in α each 0 by 10 and the kth occurrence of 1 by $10^{k!+1}$. Let $P = \{n : \beta(n) = 1\}$, which is effectively procyclic by construction. However, since $\alpha = \mathcal{B}(\beta)$ for a transducer, by Lem. 3.6, Acc_β and hence the MSO theory of $\langle \mathbb{N}; <, P\rangle$ must be undecidable. Hence β cannot be effectively profinitely ultimately periodic by Thm. 3.3.

Now suppose $\alpha \in \{0,1\}^\omega$ is a non-periodic word such that Acc_α is decidable, e.g., the Thue-Morse word. Let $\beta = 0^{\alpha(0)}10^{\alpha(1)}1\cdots$, $P = \{n \in \mathbb{N} : \beta(n) = 1\}$, and $\langle p_n\rangle_{n=0}^\infty$ be the ordering of P. Observe that $p_{n+1} - p_n \in \{1,2\}$. By construction, for all $m \geq 2$, $\langle p_n \bmod m\rangle_{n=0}^\infty$ is not ultimately periodic, which implies that P is not procyclic. However, by a transduction argument, Acc_α is Turing-equivalent to Acc_β. Therefore, Acc_β is decidable and hence β is effectively profinitely ultimately periodic.

Definition 3.11 (Effectively Sparse Predicates). The predicates $P_1, \ldots, P_d$ are effectively sparse if for every i, j and K, $0 < |p_n^{(i)} - p_m^{(j)}| < K$ has only finitely many solutions that can be effectively determined.

This is equivalent to effective divergence of k_n to $+\infty$: for every K, we can compute N such that for all $n \geq N$, $k_n \geq K$. We are ready to state our reduction from characteristic words to order words. We assume that effectively procyclic and effectively sparse predicates $P_1, \ldots, P_d$ are given by oracles to check whether $n \in P_i$ for all $n \in \mathbb{N}$ and $1 \leq i \leq d$, as well as the oracles described in the definitions above.

Theorem 3.12. *There exists an algorithm that takes an automaton $\mathcal{A}$ and effectively procyclic and effectively sparse predicates $P_1, \ldots, P_d$, and outputs an automaton $\mathcal{B}$ such that $\alpha \in L(\mathcal{A}) \Leftrightarrow \beta \in L(\mathcal{B})$, where α is the characteristic word of $(P_1, \ldots, P_d)$ and β is the corresponding order word.*

Proof. We factorise $\alpha = \prod_{n=0}^\infty w_n$, where $w_n = \mathbf{0}^{k_n}\beta(n)$. By Thm. 3.8 it suffices to show how to construct, given a morphism $h : (\{0,1\}^d)^* \to M$, a transducer $\mathcal{T}$ such that $\mathcal{T}(\beta) = \prod_{n=0}^\infty h(w_n)$. By the classical lasso argument, from M we can construct $L, m \geq 1$ such that for any $x \in M$ and $k \geq L + m$, $x^n = x^{L + (k-L) \bmod m}$. From effective sparsity, we can compute N such that for all $n \geq N$, $k_n > L$.

Define, for all $n \geq 0$ and $1 \leq i \leq d$,

- $t_n = \sum_{i=0}^n (k_i + 1)$, which is equal to $|w_0| + \cdots + |w_n|$,
- $l_n^{(i)} = \max\{t_k \leq t_n : \beta(k) = (b_1, \ldots, b_d), b_i = 1\} - 1$, i.e. the largest $j \leq t_n$ such that $j \in P_i$, and
- $s_n^{(i)} = \min\{t_k > t_n : \beta(k) = (b_1, \ldots, b_d), b_i = 1\} - 1$, i.e. the smallest $j > t_n$ such that $j \in P_i$.

Since $(P_1, \ldots, P_d)$ are effectively procyclic, $(s_n^{(i)} - l_n^{(i)})$ is periodic modulo every m with computable period and pre-period.

The transducer $\mathcal{T}$ has the values of $h(w_0), \ldots, h(w_N)$ hard-coded into it. Before reading $\beta(n+1)$ for $n \geq N$, it has in memory $t_n \bmod m$ for each $1 \leq i \leq d$, as well as the values of $l_n^{(i)} \bmod m$ and $\left(s_n^{(i)} - l_n^{(i)}\right) \bmod m$, the latter via effective procyclicity. Upon reading $\beta(n+1) = (b_1, \ldots, b_d)$, it first determines some i such that $b_i = 1$. At this point we have that $s_n^{(i)} = t_{n+1} - 1$ and hence $t_{n+1} = l_n^{(i)} + (s_n^{(i)} - l_n^{(i)}) + 1$. Therefore, the transducer can compute $t_{n+1} \bmod m$ using the values it has in memory. To compute $k_{n+1} \bmod m$, it remains to observe that $k_{n+1} = t_{n+1} - t_n - 1$. Since $k_{n+1} \geq L + m$, we have that

$$h(w_n) = (h(\mathbf{0}))^{L + (k_{n+1} - L) \bmod m} \cdot h(\beta(n))$$

which can now be computed and output by $\mathcal{T}$. Finally, the transducer computes the values of $l_{n+1}^{(i)} \bmod m$ as well as $s_{n+1}^{(i)} - l_{n+1}^{(i)} \bmod m$ for all i, by checking whether $b_i = 1$ or $b_i = 0$ and using the value of $k_{n+1} \bmod m$. □

Corollary 3.13. *Let $(P_1, \ldots, P_d)$ be effectively procyclic and effectively sparse predicates with the characteristic word α and the order word β. The problems Acc_α and Acc_β are Turing-equivalent.*

Proof. That Acc_α reduces to Acc_β follows from Thm. 3.12, and that Acc_β reduces to Acc_α is true for any predicates $P_1, \ldots, P_d$ as discussed earlier. □

3.6 Closure under compositions

We now study predicates linked by function composition.

Theorem 3.14. *Let $g_1, \ldots, g_d \colon \mathbb{N} \to \mathbb{N}$ be effectively contractible functions and $f_i = g_1 \circ \cdots \circ g_i$ for $1 \le i \le d$. The MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$, where $P_i = \{f_i(n) \colon n \in \mathbb{N}\}$, is decidable.*

Proof. Observe that $f_1(n) = g_1(n)$, $f_2(n) = g_1(g_2(n))$, $f_3(n) = g_1(g_2(g_3(n)))$, and so on. Hence $P_d \subseteq \cdots \subseteq P_1$.

We proceed by induction. If $d = 1$, then decidability follows from Cor. 3.4. Next, consider $g_1, \ldots, g_d$ for some $d > 1$. Let $\Sigma = (\{0,1\})^d$, $\alpha \in \Sigma^\omega$ be the characteristic word of $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$, and $\beta \in \Sigma^\omega$ be the order word. Further let $h_i = g_2 \circ \cdots \circ g_i$ for $2 \le i \le d$, $Q_i = \{h_i(n) \colon n \in \mathbb{N}\}$, and σ be the characteristic word of $\langle \mathbb{N}; <, Q_2, \ldots, Q_d \rangle$. By the induction hypothesis, Acc_σ is decidable. We will show how to transduce from σ into (any compressed version, as appropriate, of) α. The decidability then follows from Thm. 3.8.

Let $h \colon \Sigma^* \to M$ be a morphism into a finite monoid M. For $n \in \mathbb{N}$, write $\beta(n) = (b_{n,1}, \ldots, b_{n,d})$ and $\sigma_n = (s_{n,2}, \ldots, s_{n,d})$. Observe that $b_{n,k} = s_{n,k}$ for all $2 \le k \le d$. We factorise $\alpha = \prod_{n=0}^\infty w_n$ where $w_n = \mathbf{0}^{k_n}\beta(n)$, $k_0 = g_1(0)$, and $k_n = g(n) - g(n-1) - 1$ for all $n \ge 1$. By the assumption on $g_1 = f_1$, $\langle k_n \rangle_{n=0}^\infty$ is effectively profinitely ultimately periodic. In particular, a transducer can compute $\langle h(0^{k_n}) \rangle_{n=0}^\infty$ at the nth step. Therefore, our transducer $\mathcal{T}$, upon reading $\sigma(n)$, outputs $h(\mathbf{0}^{k_n})h((1, s_{n,2}, \ldots, s_{n,d}))$. Then $\mathcal{T}(\sigma) = h(w_0)h(w_1)\cdots$. □

We will not use Thm. 3.14 to prove any of our main theorems. However, we believe that it is of independent interest, as it gives us other new decidability results: for example, if we take $g_1(n) = n_2$, $g_2(n) = 2^n$, and $g_3(n) = 3^n$, we obtain that the MSO theory of $\langle \mathbb{N}; <, \mathbf{N}^2, 4^{\mathbf{N}}, \{2^{2\cdot 3^n} \colon n \in \mathbb{N}\} \rangle$ is decidable. By a similar argument, we obtain that the MSO theory of $\langle \mathbb{N}; <, \{(k^d)^n \colon n \in \mathbb{N}\}, \mathbf{N}^d \rangle$ is decidable for any integers $k, d \ge 2$, which also follows from our second main result (see Cor. 5.4).

4 LINEAR RECURRENCE SEQUENCES WITH A SINGLE NON-REPEATED DOMINANT ROOT

4.1 Overview

In this section, we consider integer linear recurrence sequences $\langle u_n^{(i)} \rangle_{n=0}^\infty$ with respective value sets $P_i \subseteq \mathbb{N}$ for $1 \le i \le d$ that satisfy the following condition.

(A) Each $\langle u_n^{(i)} \rangle_{n=0}^\infty$ has the exponential polynomial representation

$$u_n^{(i)} = c_i \rho_i^n + \sum_{j=1}^{k_i} p_{i,j}(n) \rho_{i,j}^n$$

and the dominant part $\langle c_i \rho_i^n \rangle_{n=0}^\infty$, where $c_i > 0$ and $\rho_i > 1$. That is, $\langle u_n^{(i)} \rangle_{n=0}^\infty$ is non-constant, has the single non-repeated dominant root ρ_i, and P_i is infinite.

Note that if $\rho_i = 1$, because $\langle u_n^{(i)} \rangle_{n=0}^{\infty}$ takes integer values, P_i must be finite. The same conclusion holds if $c_i < 0$. Such P_i can be defined in the structure $\langle \mathbb{N}; < \rangle$, and are not of interest to us. Our main decision problem is the following.

Problem 1. *Given $\langle u_n^{(1)} \rangle_{n=0}^{\infty}, \ldots, \langle u_n^{(d)} \rangle_{n=0}^{\infty}$ and an MSO formula φ, decide whether $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle \models \varphi$.*

When $d = 1$, decidability of Problem 1 can be shown using the contraction method of Elgot and Rabin. (The decidability also follows from the main results in this section.) On the other hand, it is easily shown that Problem 1, even in case of $d = 2$, subsumes many major open decision problems about integer LRS.

Lemma 4.1. *Let $\mathcal{A}$ be an automaton over $\Sigma \coloneqq \{-, 0, +\}$ and $\langle v_n \rangle_{n=0}^{\infty}$ an integer LRS with sign pattern $\sigma \in \Sigma^{\omega}$, where $\sigma(n)$ is defined by the sign of v_n. We can construct integer LRS $\langle u_n^{(1)} \rangle_{n=0}^{\infty}, \langle u_n^{(2)} \rangle_{n=0}^{\infty}$ satisfying (A) with respective value sets P_1, P_2, and an automaton C such that $\sigma \in L(\mathcal{A}) \Leftrightarrow \tau \in L(C)$, where τ is the characteristic word of (P_1, P_2).*

Proof. Let $\varepsilon \in (0, 1)$ be such that $\frac{1}{\rho}(1 + \varepsilon) < (1 - \varepsilon) < (1 + \varepsilon) < \rho$ and let $C \in \mathbb{N}_{>0}$ and $\rho \in \mathbb{N}_{>1}$ be such that $|v_n| < \varepsilon \cdot C\rho^n$ for all n. Define $u_n^{(1)} = C\rho^n$ and $u_n^{(2)} = C\rho^n + v_n$. We give a transducer Γ such that $\Gamma(\tau) = \sigma$, and then invoke Lem. 3.6.

By construction of C, ρ and ε, for all $n \geq 0$, $u_n^{(2)}$ is the unique term in the sequence $\langle u_n^{(2)} \rangle_{n=0}^{\infty}$ belonging to the interval $((1 - \varepsilon) \cdot u_n^{(1)}, (1 + \varepsilon) \cdot u_n^{(1)})$. Moreover, by construction of ε these intervals are disjoint and ordered according to n. Hence the order word β of (P_1, P_2) can be uniquely factorised as $\beta = w_0 w_1 w_2 \cdots$ where each w_n is either $(1, 1)$ (when $v_n = 0$), or $(0, 1)(1, 0)$ (when $v_n > 0$), or $(1, 0)(0, 1)$ (when $v_n < 0$). The transducer Γ simply discards all occurrences of $\mathbf{0}$ from τ, performs the factorisation above, and outputs $-$, 0 or + for each factor w_n. ◻

By the MSO theory of the sign pattern of an LRS $\langle v_n \rangle_{n=0}^{\infty}$ we mean the MSO theory of the structure $\langle \mathbb{N}; <, P_-, P_0, P_+ \rangle$ where the unique predicate $P \in \{P_-, P_0, P_+\}$ containing n is determined by the sign of v_n (i.e., $n \in P_-$ if and only if $v_n < 0$). Observe that in this structure we can ask whether $v_n = 0$ for some n (i.e., the Skolem Problem), whether $v_n \geq 0$ for all (sufficiently large) n (i.e., whether the LRS is ultimately positive), etc. The two corollaries of Lem. 4.1 below follow immediately from Büchi's theorem (Thm. 2.3) and the definitions of Skolem and other problems of LRS (Sec. 2.4).

Corollary 4.2. *Given an integer LRS $\langle v_n \rangle_{n=0}^{\infty}$ and an MSO formula φ, we can construct integer LRS $\langle u_n^{(1)} \rangle_{n=0}^{\infty}, \langle u_n^{(2)} \rangle_{n=0}^{\infty}$ and a formula ψ such that $\langle \mathbb{N}; <, P_-, P_0, P_+ \rangle \models \varphi \Leftrightarrow \langle \mathbb{N}; <, P_1, P_2 \rangle \models \psi$.*

Corollary 4.3. *The Skolem Problem, the Positivity Problem, and the Ultimate Positivity Problem reduce to Problem 1.*

Surprisingly, the problem of deciding, given an MSO formula φ and a *diagonalisable* integer LRS $\langle v_n \rangle_{n=0}^{\infty}$, whether $\langle \mathbb{N}; <, P_-, P_0, P_+ \rangle \models \varphi$ is Turing-equivalent to the Positivity Problem for diagonalisable integer LRS; see [27, Thm. 12] and [26, Lem. 7.0.2]. For non-diagonalisable LRS, no such equivalence is known.

Examining the construction of Lem. 4.1, it is not difficult to see that all three problems, in fact, reduce to the restriction of Problem 1 to first-order formulas φ. By a similar argument, the problem of deciding, given two integer LRS $\langle v_n \rangle_{n=0}^{\infty}$ and $\langle w_n \rangle_{n=0}^{\infty}$, whether $v_n = w_m$ for some n, m also reduces to Problem 1 with first-order φ and $d = 2$. The intersection problem is another problem about LRS that is wide-open at the moment.

Given the hardness of Problem 1, we will further restrict the linear recurrence sequences that we consider. We will be interested in the following conditions in addition to (A).

(B) For any $i \neq j$, $c_i \rho_i^n = c_j \rho_j^m$ holds for finitely many $(n, m) \in \mathbb{N}^2$. Equivalently, for every $i \neq j$, the equation $c_i \rho_i^n = c_j \rho_j^m$ has at most one solution (n, m) in $\mathbb{N}^2$.

(C) The numbers $1/\log(\rho_1), \ldots, 1/\log(\rho_d)$ are linearly independent over $\mathbb{Q}$.

Observe that (C) implies that ρ_i, ρ_j are multiplicatively independent for every $i \neq j$, which implies (B). Our main result is the following.

Theorem 4.4. *Problem 1 is decidable for $\langle u_n^{(1)} \rangle_{n=0}^\infty, \ldots, \langle u_n^{(d)} \rangle_{n=0}^\infty$ that satisfy the conditions (A) and (C).*

To see how (C) can be applied in practice, recall from Lem. 2.11 that if $\mathrm{rank}(G_M(\rho_1, \ldots, \rho_d)) \geq d-2$ (in particular, if $d \leq 2$) and $\rho_1, \ldots, \rho_d$ are pairwise multiplicatively independent, then (C) is satisfied. Our next main result is that if we assume Schanuel's conjecture, then we can drop the condition (C).

Theorem 4.5. *Assuming Schanuel's conjecture, Problem 1 is decidable for integer LRS satisfying conditions (A) and (B). Moreover, the decision procedure relies on Schanuel's conjecture only for termination.*

The second part of the statement of Thm. 4.5 means that termination of the decision procedure is guaranteed by Schanuel's conjecture, and whenever the procedure terminates, its output is unconditionally guaranteed to be correct. As a corollary of Thm. 4.5, we obtain the following theorem from the Introduction.

Theorem 4.6. *Suppose we are given an MSO formula φ and integers $a_1, \rho_1, \ldots, a_d, \rho_d \geq 1$. Assuming Schanuel's conjecture, it is decidable whether φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$, where $P_i = \{a_i \rho_i^n : n \in \mathbb{N}\}$.*

Proof. Observe that if $a_i \rho_i^n = a_j \rho_j^m$ has more that one solution in n, m, then $\rho_i^b = \rho_j^c$ for some positive integers b, c. Therefore, from $\rho_1, \ldots, \rho_d$ we can compute $k \geq 1$ such that, writing $b_i = a_i \rho_i^r$, $\mu_i = \rho_i^k$, and $Q_{i,r} = \{a_i \rho_i^{kn+r} : n \in \mathbb{N}\} = \{b_i \mu_i^n : n \in \mathbb{N}\}$ for $1 \leq i \leq d$ and $0 \leq r < k$, we have that for all i, i', r, r', either $Q_{i,r} = Q_{i',r'}$ or $Q_{i,r} \cap Q_{i',r'}$ is finite. Let $\widetilde{Q}_1, \ldots, \widetilde{Q}_m$ be all the distinct predicates from $\{Q_{i,r} : 1 \leq i \leq d,\ 0 \leq r < k\}$. Then $\widetilde{Q}_i \cap \widetilde{Q}_j$ is finite for all $i \neq j$. Since $P_i = Q_{i,0} \cup \cdots \cup Q_{i,k-1}$, we can construct an MSO formula ψ that holds in $\langle \mathbb{N}; <, \widetilde{Q}_1, \ldots, \widetilde{Q}_m \rangle$ if and only if φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$. It remains to invoke Thm. 4.5. □

What about decidability of the individual MSO theories $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$? That is, what happens if we fix the sequences $\langle u_n^{(1)} \rangle_{n=0}^\infty, \ldots, \langle u_n^{(d)} \rangle_{n=0}^\infty$, but allow the MSO formula φ to be given as input? What information about the specific LRS do we need to decide the MSO theory? The answer is given in Cor. 4.8, which is based on the following theorem. In short, in this setting too we can replace (C) with the weaker condition (B).

Theorem 4.7. *Given integer LRS $\langle u_n^{(1)} \rangle_{n=0}^\infty, \ldots, \langle u_n^{(d)} \rangle_{n=0}^\infty$ satisfying conditions (A) and (B), the ideal of all polynomial relations between $\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d)$, a basis of $G_L(1/\log(\rho_1), \ldots, 1/\log(\rho_d))$, and an MSO formula φ, we can decide whether $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle \models \varphi$.*

We note that a basis for $G_L(1/\log(\rho_1), \ldots, 1/\log(\rho_d))$ can be extracted from the aforementioned ideal by using, for example, Gröbner bases and modifying the algorithm for deciding whether a given polynomial occurs in an ideal [20]: observe that for all $k_1, \ldots, k_d \in \mathbb{Z}$, $\sum_{i=1}^d \frac{k_i}{\log(\rho_i)} = 0$ if and only if $\sum_{i=1}^d k_i \prod_{j \neq i} z_j = 0$. In our formulation, we emphasise that there are two distinct sources of non-uniformity in the following results.

Corollary 4.8. *Let $\langle u_n^{(1)} \rangle_{n=0}^\infty, \ldots, \langle u_n^{(d)} \rangle_{n=0}^\infty$ be integer LRS satisfying conditions (A) and (B). The MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$ is decidable.*

Proof. The Turing machine for deciding the MSO theory of $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$ simply has the ideal of all polynomial relations between $\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d)$, which has a finite representation thanks to Hilbert basis theorem, hard-coded into it. This representation can be effectively operated on using, for example, Gröbner bases. □

From Thm. 4.7 we also obtain the following result stated in the Introduction.

THEOREM 4.9. *For any integers $a_1, \rho_1, \ldots, a_d, \rho_d \geq 1$, there exists an algorithm that, given an MSO formula φ, decides whether φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$, where $P_i = \{a_i \rho_i^n : n \in \mathbb{N}\}$.*

PROOF. Construct $k \geq 1$ and $\widetilde{Q}_1, \ldots, \widetilde{Q}_m$ as in the proof of Thm. 4.6. By Cor. 4.8, the MSO theory of $\langle \mathbb{N}; <, \widetilde{Q}_1, \ldots, \widetilde{Q}_m \rangle$ is decidable. Given φ, construct ψ as in the proof of Thm. 4.6. We have that φ holds in $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle$ if and only if ψ holds in $\langle \mathbb{N}; <, \widetilde{Q}_1, \ldots, \widetilde{Q}_m \rangle$. It remains to check whether the latter is the case. □

We mention that the first part of the statement of Thm. 4.5 immediately follows from Thm. 4.7: Schanuel's conjecture tells us that all polynomial relations between $\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d)$ come from rational multiplicative relations between $c_1, \rho_1, \ldots, c_d, \rho_d$. Making sure that Schanuel's conjecture is only needed for termination and not for correctness is non-trivial. (This issue is explored in some detail in [29].) However, no unconditional method is known for computing all polynomial relations between logarithms of algebraic numbers. Hence, for example, the MSO theory of $\langle \mathbb{N}; <, {a_1}^{\mathbb{N}}, \ldots, {a_d}^{\mathbb{N}} \rangle$ is decidable for any positive integers $a_1, \ldots, a_d$, but with a caveat: we know that a decision procedure exists, but to write it down we need solve a difficult problem about polynomial relations between logarithms of algebraic numbers.

Can we drop condition (B) in the statement of Cor. 4.8? If we could, then applying Lem. 4.1 we would obtain that the MSO theory of the sign pattern of any LRS $\langle v_n \rangle_{n=0}^{\infty}$ is decidable. For diagonalisable LRS, this is indeed the case, but with a caveat: the sign pattern of a diagonalisable LRS has a toric suffix [3, Sec. 3], and hence a decidable MSO theory [10]. However, no method is known for determining this suffix efficiently. Nevertheless, a decision procedure for the MSO theory is allowed to have the position where this suffix begins hard-coded into it. For non-diagonalisable LRS, essentially nothing is known about the decidability of the MSO theory of its sign pattern.

We will prove our main theorems (Thm. 4.4, Thm. 4.5, Thm. 4.7) together. In the remainder of Sec. 4, we denote by $P_1, \ldots, P_d$ the respective value sets of integer linear recurrence sequences $\langle u_n^{(1)} \rangle_{n=0}^{\infty}, \ldots, \langle u_n^{(d)} \rangle_{n=0}^{\infty}$ satisfying (A-B), by φ an MSO formula and by $\mathcal{A}$ the corresponding automaton, by α the characteristic word of $(P_1, \ldots, P_d)$, and by β the order word of $(P_1, \ldots, P_d)$. Recall that deciding whether $\langle \mathbb{N}; <, P_1, \ldots, P_d \rangle \models \varphi$ is equivalent to deciding whether $\alpha \in L(\mathcal{A})$.

4.2 From characteristic words to order words

In this section, fix LRS $\langle u_n^{(1)} \rangle_{n=0}^{\infty}, \ldots, \langle u_n^{(d)} \rangle_{n=0}^{\infty}$ satisfying (A-B) and use the notation above. Thus, let P_i be the value set of $\langle u_n^{(i)} \rangle_{n=0}^{\infty}$ and α be the characteristic word of $(P_1, \ldots, P_d)$. Our approach to deciding whether an automaton $\mathcal{A}$ accepts α is to first reduce this to the problem of checking whether an automaton $\mathcal{B}$ accepts its order word β. We will do this by showing that the predicates $(P_1, \ldots, P_d)$ are effectively procyclic and effectively sparse, and then invoking Thm. 3.12. Thereafter, we will reduce from the order word to a uniformly recurrent word obtained by ordering the dominant parts of our recurrence sequences. We will need order words obtained from sequences that do not necessarily take integer values.

Definition 4.10. Let $f_1(n), \ldots, f_d(n) \colon \mathbb{N} \to \mathbb{R}$ be strictly increasing functions such that $f_i(n) \to +\infty$ as $n \to \infty$ for all i. Write $T = \bigcup_{i=1}^{d} \{f_i(n) : n \in \mathbb{N}\}$, and order the terms of T as $\langle t_n \rangle_{n=0}^{\infty}$. The nth letter $(b_1, \ldots, b_d)$ of the order word

$$\gamma \coloneqq \mathrm{Ord}(f_1(n), \ldots, f_d(n)) \in (\{0,1\}^d)^{\omega}$$

is defined by $b_i = 1 \Leftrightarrow t_n = f_i(m)$ for some m.

The following two lemmas contains the main number-theoretic arguments that we will need.

Lemma 4.11. *We can compute $N \geq 0$ with the following properties. For $1 \leq i \leq d$, let m_i be the smallest integer with the property that $u^{(i)}_{m_i} \geq N$.*

(a) *For all i, $\langle u^{(i)}_{m_i+n}\rangle_{n=0}^{\infty}$ is strictly increasing.*
(b) *For all $i \neq j$ and n_i, n_j such that $n_i \geq m_i$, we have that $c_i\rho_i^{n_i} \neq c_j\rho_j^{n_j}$, $u^{(i)}_{n_i} \neq u^{(j)}_{n_j}$, and $c_i\rho_i^{n_i} > c_j\rho_j^{n_j} \Leftrightarrow u^{(i)}_{n_i} > u^{(j)}_{n_j}$.*
(c) *For all $i \neq j$ and $n_i \geq m_i$, there exists $n_j \geq m_j$ such that $c_i\rho_i^{n_i} \leq c_j\rho_j^{n_j} < \rho_j \cdot c_i\rho_i^{n_i}$.*

Proof. Denote by $\langle v^{(i)}_n\rangle_{n=0}^{\infty}$ the non-dominant part of $\langle u^{(i)}_n\rangle_{n=0}^{\infty}$, and recall that $|v^{(i)}_n| = o((\rho_i^{1-\varepsilon})^n)$ for all sufficiently small $\varepsilon > 0$ (where the implied constant is effective due to Lem. 2.4). For all i, we have that

$$u^{(i)}_{n+1} - u^{(i)}_n = c_i(\rho_i - 1)\rho_i^n + v^{(i)}_{n+1} - v^{(i)}_n. \tag{3}$$

Hence we can compute N_i such that for all m with $u^{(i)}_m \geq N_i$, the sequence $\langle u^{(i)}_{m+n}\rangle_{n=0}^{\infty}$ is strictly increasing. We then take $\widetilde{N}_1 = \max_i N_i$. We next move on to (b).

Next, we compute for every pair $i \neq j$, an integer $N_{i,j}$ such that $c_i\rho_i^n \neq c_j\rho_j^m$ for all n, m satisfying $u^{(i)}_n \geq N_{i,j}$. To do this, we first compute a basis X of $G_M(\rho_i, \rho_j, c_i/c_j)$ (see Sec. 2.3). If $X = \{(0, 0, 0)\}$, then $c_i\rho_i^n = c_j\rho_j^m$ has no non-trivial solution in $n, m \in \mathbb{Z}$, and we can take $N_{i,j} = 1$. Otherwise, by assumption (B), we will have $X = \{(k_1, k_2, k_3)\}$ with $k_3 \neq 0$. If $|k_3| = 1$, then $c_i\rho_i^n = c_j\rho_j^m$ has a unique solution in $n, m \in \mathbb{Z}$, and we can compute $N_{i,j}$ accordingly. Otherwise, there are no solutions and we can take $N_{i,j} = 1$. We then define $\widetilde{N}_2 = \max\{\widetilde{N}_1, \max_{i,j} N_{i,j}\}$.

Next, applying Thm. 2.9, we have that for all $i \neq j$ and $n, m \in \mathbb{N}$ with $\rho_i > \rho_j$ and $u^{(i)}_n \geq \widetilde{N}_2$,

$$|c_i\rho_i^n - c_j\rho_j^m| = |c_j\rho_j^m - c_i\rho_i^n| > \frac{\rho_i^n}{(n+2)^C} \tag{4}$$

for a computable constant C. Since

$$u^{(i)}_n - u^{(j)}_m = c_i\rho_i^n - c_j\rho_j^m + v^{(i)}_n - v^{(j)}_m \tag{5}$$

we can compute $M_{i,j} \geq \widetilde{N}_2$ such that, assuming $u^{(i)}_n \geq M_{i,j}$, $u^{(i)}_n - u^{(j)}_m$ is non-zero and has the same sign as $c_i\rho_i^n - c_j\rho_j^m$. Let $\widetilde{N}_3 = \max_{i,j} M_{i,j}$.

Finally, we choose $N > \widetilde{N}_3$ such that for all $1 \leq i \leq d$, there exists n satisfying $N_3 \leq u^{(i)}_n < N$. Then (a-b) are satisfied since $N \geq \widetilde{N}_3, \widetilde{N}_2$. To see that (c) is satisfied, consider $i \neq j$ and $n_i \geq m_i$. Let n_j be the unique *integer* with the property that $c_j\rho^{n_j} \in [c_i\rho_i^{n_i}, \rho_j \cdot c_i\rho_i^{n_i})$. We have to argue that $n_j \in \mathbb{N}$. By construction of N, there exists k_j such that $N_3 \leq u^{(j)}_{k_j} \leq N$. Because $u^{(j)}_{k_j} \geq \widetilde{N}_3$, we have that $u^{(j)}_{k_j} - u^{(j)}_{n_j}$ has the same sign as $c_j\rho_j^{k_j} - c_j\rho_j^{n_j}$, and the latter is non-zero. Since $u^{(j)}_{n_j} > u^{(j)}_{k_j}$, it follows that $n_j > k_j$ and hence $n_j \in \mathbb{N}$. □

Lemma 4.12. *Given $1 \leq i, j \leq d$ and $K \geq 0$, we can compute L such that for all $u^{(i)}_n, u^{(j)}_m \geq L$,*

$$u^{(i)}_n \neq u^{(j)}_m \Rightarrow |u^{(i)}_n - u^{(j)}_m| > K.$$

Proof. If $i = j$, we use (3) and the fact that $|v^{(i)}_n| = o((\rho_i^{1-\varepsilon})^n)$ for all sufficiently small $\varepsilon > 0$ for an effective implied constant. Suppose $i \neq j$ and that, without loss of generality, $\rho_i \geq \rho_j$. Let $N, m_1, \ldots, m_d$ be as in the previous lemma. We will enumerate all solutions (of which there are finitely many, as argued below) of $|u^{(i)}_n - u^{(j)}_m| \leq K$ with $u^{(i)}_n, u^{(j)}_m < N$.

By (4) and (5), for $u_n^{(i)}, u_m^{(j)} \geq N$ we have that

$$|u_n^{(i)} - u_m^{(j)}| = \frac{\rho_i^n}{(n+2)^C} + o(\rho_i^{n(1-\varepsilon)})$$

for all sufficiently small $\varepsilon > 0$ (where the implied constant is effective). It remains to compute ν such that the right-hand side is greater than K for all $n \geq \nu$, and then $L \geq N$ such that $u_n^{(i)} \geq L \Rightarrow n \geq \nu$. □

Corollary 4.13. *The predicates $P_1, \ldots, P_d$ are effectively procyclic and effectively sparse.*

Proof. Enumerate the elements of P_i as $\langle p_n^{(i)} \rangle_{n=0}^{\infty}$, and let $N, m_1, \ldots, m_d$ be as in the statement of Lem. 4.11. By Lem. 4.11 (a-b), we have that a suffix of $\langle p_n^{(i)} \rangle_{n=0}^{\infty}$ (which can be effectively determined) is equal to $\langle u_{m_i+n}^{(i)} \rangle_{n=0}^{\infty}$, which is effectively procyclic (Lem. 2.5). Hence P_i is effectively procyclic, which implies that $(P_1, \ldots, P_d)$ are effectively procyclic. That $(P_1, \ldots, P_d)$ are effectively sparse follows immediately from the preceding lemma. □

Recall that α and β denote the characteristic and order words of $(P_1, \ldots, P_d)$, respectively.

Corollary 4.14. *Given an automaton $\mathcal{A}$, we can compute*

- *an automaton $\mathcal{B}$ such that*

$$\alpha \in L(\mathcal{A}) \Leftrightarrow \beta \in L(\mathcal{B}),$$

- *and an automaton C such that*

$$\alpha \in L(\mathcal{A}) \Leftrightarrow \mathrm{Ord}(r_1\rho_1^n, \ldots, r_d\rho_d^n) \in L(C)$$

where $r_i = c_i \rho_i^{m_i}$.

Proof. The first claim follows from Cor. 3.13. Let γ be the word obtained by deleting all occurrences of $\mathbf{0}$ from $\alpha[N, \infty)$. Then $\gamma = \beta[\widetilde{N}, \infty)$ for some $\widetilde{N}$. Moreover, by Lem. 4.11 (a-b),

$$\gamma = \mathrm{Ord}(r_1\rho_1^n, \ldots, r_d\rho_d^n).$$

Therefore, C can be constructed from $\mathcal{B}$ by changing the initial state to the one obtained after $\mathcal{B}$ reads $\beta[0, \widetilde{N})$. □

Henceforth, when the context is clear, we denote by N the smallest integer satisfying the statement of Lem. 4.11, and define $m_1, \ldots, m_d$ as in the statement of Lem. 4.11. We further write $r_i = c_i \rho_i^{m_i}$, $\gamma = \mathrm{Ord}(\langle r_1\rho_1^n \rangle_{n=0}^{\infty}, \ldots, \langle r_d\rho_d^n \rangle_{n=0}^{\infty})$, and denote by C the automaton given in Cor. 4.14. Note that by Lem. 4.11, each letter in γ is of the form $(b_1, \ldots, b_d)$, where exactly one $b_i = 1$ and $b_j = 0$ for all $i \neq j$. We replace every such letter with i in both γ and C to construct $\widetilde{\gamma} \in \{1, \ldots, d\}^{\omega}$ and $\widetilde{C}$ such that $\gamma \in L(C) \Leftrightarrow \widetilde{\gamma} \in L(\widetilde{C})$.

4.3 Interlude: applying the theory of cutting sequences

It turns out that the word γ belongs to the class of *cutting sequences* (also known as *billiard words*), which have been studied in word combinatorics [4, 6, 8]. We illustrate this connection through an example.

Example 4.15. Consider $c_1 = 3, \rho_1 = 2, c_2 = 10, \rho_2 = 3$, $u_n^{(1)} = 3 \cdot 2^n$ and $u_n^{(2)} = 10 \cdot 3^n$. Because these two sequences are disjoint and do not have non-dominant parts,

$$\beta = \mathrm{Ord}(3 \cdot 2^n, 10 \cdot 3^n) = 112112122 \cdots$$

where the second equality is up to the renaming $(1, 0) \to 1$, $(0, 1) \to 2$. The smallest N satisfying Lem. 4.11 (particularly note the property (c)) yields $m_1 = 1$, $m_2 = 0$, and $\gamma = \beta[1, \infty)$. Let $a_n = \log(c_1\rho_1^n) = \log(3) + n\log(2)$ and $b_n =$

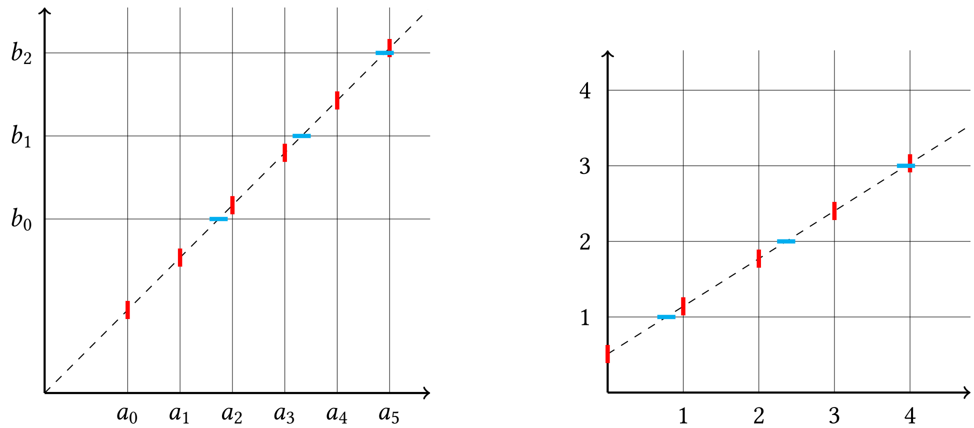

Fig. 1. Generating the word β (left) and its suffix γ, which is a cutting sequence (right).

$\log(c_2\rho_2^n) = \log(7) + n\log(3)$. Figure 1 (left) illustrates a way to generate β. We start at the point $(0, 0)$ and follow the line $y = x$. Every time a vertical line $x = a_n$ for some n is hit, we write 1. When we hit a horizontal line $y = b_n$ for some n, we write 2. If we discard the first letter of β, we obtain a cutting sequence, illustrated in Fig. 1 (right). The figure on the right is obtained from the one on the left by a translation and a scaling. In the former, we start at a point $(0, y)$, where $0 < y < 1$, and follow the dashed line, which has the slope $\log(2)/\log(3)$. When we hit a line $x = n$ for $n \in \mathbb{N}$, we write 1; When we hit $y = n$, we write 2.

Formally, the cutting sequence over $\Sigma = \{1, \ldots, d\}$ with slopes $\lambda_1, \ldots, \lambda_d$ and intercepts $s_1, \ldots, s_d$ is the infinite word obtained by considering intersections of the line $\{(\xi_1 + \lambda_1 t, \ldots, \xi_d + \lambda_d t) : t \geq 0\}$ with the grid lines $x_i = c$ (where $c \in \mathbb{N}$ and $x_1, \ldots, x_d$ denote the d standard coordinates in $\mathbb{R}^d$) as $t \longrightarrow \infty$ starting from $t = 0$, assuming no two grid lines are intersected simultaneously. Cutting sequences are uniformly recurrent, and under some mild assumptions on the slope, there is an explicit formula for the factor complexity, which allows us to apply Cor. 3.2.

(i) If $d = 2$ and $\log(\rho_1)/\log(\rho_2)$ is irrational (which is the case in Fig. 1), then γ is a *Sturmian word* and therefore $\pi_\gamma(n) = n + 1$. See, e.g. [2, Sec. 10.5] and [31, Chap. 2].
(ii) By [4], if $d = 3$, and $1/\log(\rho_1), 1/\log(\rho_2), 1/\log(\rho_3)$ as well as $\log(\rho_1), \log(\rho_2), \log(\rho_3)$ are linearly independent over $\mathbb{Q}$, then $\pi_\gamma(n) = n^2 + n + 1$.
(iii) For arbitrary $d > 0$, Bédaride [8] gives an exact formula for $\pi_\gamma(n)$ assuming $1/\log(\rho_1), \ldots, 1/\log(\rho_d)$ as well as every triple $\log(\rho_i), \log(\rho_j), \log(\rho_k)$ for pairwise distinct i, j, k are linearly independent over $\mathbb{Q}$. This generalises the well-known result [6] of Baryshnikov, which gives an exact formula for the factor complexity assuming both the logarithms and their inverses are linearly independent over $\mathbb{Q}$.

Note that the exact value of the intercept does not matter in (i-iii) above: the only requirement is that no two grid hyperplanes be simultaneously reachable We will not be using cutting sequences to prove our main results. However, we could prove weaker results using the theory of cutting sequences: it is not difficult to prove that γ is the cutting sequence generated by the line $\{(\chi_1 + t/\log(\rho_1), \ldots, \chi_d + t/\log(\rho_d)) : t \geq 0\}$, where $\chi_i \in [0, 1)$ for all i. The following is an immediate consequence of Cor. 3.2 and the aforementioned result of Bédaride.

Proposition 4.16. *Problem 1 is decidable for integer LRS* $\langle u_n^{(1)}\rangle_{n=0}^{\infty},\dots,\langle u_n^{(d)}\rangle_{n=0}^{\infty}$ *satisfying conditions (A), (C), and that every triple* $\log(\rho_i),\log(\rho_j),\log(\rho_k)$ *for pairwise distinct* i,j,k *are linearly independent over* $\mathbb{Q}$.

Note that, however, this is strictly weaker than Thm. 4.4. Consider, for example, $\rho_1 = 2$, $\rho_2 = 3$ and $\rho_3 = 6$. By Lem. 2.11, $1/\log(\rho_1), 1/\log(\rho_2), 1/\log(\rho_3)$ are linearly independent over $\mathbb{Q}$, but $\log(\rho_1),\log(\rho_2),\log(\rho_3)$ are not.

4.4 Deciding whether $\widetilde{\gamma} \in L(\widetilde{C})$

So far, we have only used the assumptions (A-B) to reduce the problem of deciding whether $\alpha \in L(\mathcal{A})$ to whether $\widetilde{\gamma} \in L(\widetilde{C})$. We will show that (i) $\widetilde{\gamma}$ is uniformly recurrent and (ii) apply Cor. 3.2 to decide whether C accepts γ. Let $\Sigma = \{1,\dots,d\}$, and recall that $\widetilde{\gamma} \in \Sigma^\omega$ and $\widetilde{\gamma} = \mathrm{Ord}(\langle r_1\rho_1^n\rangle_{n=0}^{\infty},\dots,\langle r_d\rho_d^n\rangle_{n=0}^{\infty})$ up to the renaming of letters that maps the letter $(b_1,\dots,b_d)$ with $b_i = 1$ and $b_j = 0$ for $j \neq i$ to the letter i. For $b \in \Sigma$ and $w \in \Sigma^*$, we denote by $|w|_b$ the number of occurrences of b in w.

Let $w = b_0b_1\cdots b_m \in \Sigma^*$ and $b = b_0$. Define $f(n,i)$ to be the smallest term $r_i\rho_i^m$ such that $m \geq 0$, $r_i\rho_i^m \geq r_b\rho_b^n$, and $f(n,i,k) = \rho_i^{k-1}f(n,i)$. Thus, $f(n,i,k)$ is the kth largest term of the form $r_i\rho_i^m$, such that $m \geq 0$ and $r_i\rho_i^m > r_b\rho_b^n$, counting from one. Further write $v_i(n) = f(n,b_i,|w[0,i+1)|_{b_i})$ and $\tau_i(n) = f(n,b_i,|w|_{b_i}+1)$. Then the word w occurs in $\widetilde{\gamma}$ at the position corresponding to $r_b\rho_b^n$ if and only if

$$v_0(n) < \cdots < v_m(n) < \tau_1(n),\tau_2(n),\dots,\tau_d(n) \tag{6}$$

which is equivalent to

$$\frac{r_b\rho_b^n}{v_0(n)} > \cdots > \frac{r_b\rho_b^n}{v_m(n)} > \frac{r_b\rho_b^n}{\tau_1(n)},\frac{r_b\rho_b^n}{\tau_2(n)},\dots,\frac{r_b\rho_b^n}{\tau_d(n)}. \tag{7}$$

Next, observe that by definition and Lem. 4.11 (c),

$$\frac{1}{\rho_i} \leq \frac{r_b\rho_b^n}{f(n,i)} < 1$$

for all i, which implies that

$$\frac{1}{\rho_i^{k+1}} \leq \frac{r_b\rho_b^n}{f(n,i,k)} < \frac{1}{\rho_i^k} \tag{8}$$

for all i,k.

Write $f(n,i,k) = r_i\rho_i^l$. Taking logarithms, (8) is equivalent to

$$-(k+1)\log(\rho_i) \leq \log\left(\frac{r_b\rho_b^n}{f(n,i,k)}\right) = \log\left(\frac{r_b}{r_i}\right) + n\log(\rho_b) - l\log(\rho_i) < -k\log(\rho_i) \tag{9}$$

which is equivalent to

$$0 \leq \log\left(\frac{r_b}{r_i}\right) + n\log(\rho_b) + (k+1-l)\log(\rho_i) < \log(\rho_i). \tag{10}$$

Dividing by $\log(\rho_i)$, we obtain that

$$0 \leq \frac{\log(r_b)-\log(r_1)}{\log(\rho_i)} + n\frac{\log(\rho_b)}{\log(\rho_i)} + (k+1-l) < 1. \tag{11}$$

Define $s_i = \frac{\log r_b - \log r_i}{\log(\rho_i)}$, $\delta_i = \frac{\log \rho_b}{\log \rho_i}$, $s = (s_1,\dots,s_d)$, and $\delta = (\delta_1,\dots,\delta_d)$. Then from (11) we conclude that

$$\{\gamma_i + n\delta_i\} = \frac{\log(r_b)-\log(r_1)}{\log(\rho_i)} + n\frac{\log(\rho_b)}{\log(\rho_i)} + (k+1-l).$$

From (9) it then follows that

$$\frac{r_b \rho_b^n}{f(n,i,k)} = \exp\big(-(k+1)\log(\rho_i) + \log(\rho_i)\{\gamma_i + n\delta_i\}\big).$$

Hence, taking logarithms, we can write (7) as

$$k_1 \log(\rho_{b_0}) + \log(\rho_{b_0})\big\{\gamma_{b_0} + n\delta_{b_0}\big\} > \cdots > k_m \log(\rho_{b_m}) + \log(\rho_{b_m})\big\{\gamma_{b_m} + n\delta_{b_m}\big\} > \\ l_1 \log(\rho_1) + \log(\rho_1)\big\{\gamma_1 + n\delta_1\big\}, \ldots, l_d \log(\rho_d) + \log(\rho_d)\big\{\gamma_d + n\delta_d\big\} \quad (12)$$

where k_i, l_i are integers.

So, what did we achieve? Let O_w be the open subset of $\mathbb{T}^d$ consisting of all $x = (x_1, \ldots, x_d)$ such that

$$k_1 \log(\rho_{b_0}) + \log(\rho_{b_0})x_{b_0} > \cdots > k_m \log(\rho_{b_m}) + \log(\rho_{b_m})x_{b_m} > \\ l_1 \log(\rho_1) + \log(\rho_1)x_1, \ldots, l_d \log(\rho_d) + \log(\rho_d)x_d. \quad (13)$$

We have the toric dynamical system (see Sec. 2.7) given by $x \mapsto x + \delta$, and whether the pattern w occurs at a position corresponding to $r_b \rho_b^n$ is characterised by whether $s + n\delta \in O_w$, i.e. whether the orbit of s falls into the open set O_w at the step n. By uniform recurrence (Cor. 2.15), the set $\{n \in \mathbb{N} : s + n\delta \in O_w\}$ is either empty or is infinite and has bounded gaps. Because the letter b_0 occurs infinitely often in $\widetilde{\gamma}$ and with bounded gaps, it follows that either w does not occur in $\widetilde{\gamma}[K, \infty)$ at all, or does so with bounded gaps. **Therefore, $\widetilde{\gamma}$ is uniformly recurrent.**

We now move on to the question of how to effectively check whether w occurs in $\widetilde{\gamma}$, which is all we need by Cor. 3.2 to decide whether $\widetilde{\gamma} \in L(\widetilde{C})$. Let X_δ be the closure of $\langle\{n\delta\}\rangle_{n=0}^\infty$, which is a subset of $\mathbb{T}^d$ defined by $\mathbb{Q}$-affine inequalities. Further let $X_{\delta,s} = s + X_\delta$; this is the closure of $\langle\{n\delta + s\}\rangle_{n=0}^\infty$. We have that the word w occurs (infinitely often) in $\widetilde{\gamma}$ if and only if $X_{\delta,s}$ intersects O_w.

Proof of Thm. 4.4. Suppose $\frac{1}{\log(\rho_1)}, \ldots, \frac{1}{\log(\rho_d)}$ are linearly independent. Consider the equation

$$z_1\delta_1 + \cdots + z_d\delta_d = z_0$$

where $z_i \in \mathbb{Z}$. Because $\delta_b = 1$, it is equivalent to

$$\sum_{i \neq b} \frac{z_i}{\log(\rho_i)} = \frac{a_0 - z_b}{\log(\rho_b)}.$$

By the linear independence assumption, the solutions are

$$z_1 = \cdots = z_{b-1} = z_{b+1} = \cdots = z_d = z_0 - z_b = 0.$$

From Kronecker's theorem (Sec. 2.7) it follows that the orbit of $\mathbf{0}$ under $x \mapsto x + \delta$ is dense in

$$X = \{(x_1, \ldots, x_d) \in \mathbb{T}^d : x_b = 0\}.$$

Since $s_b = 0$, the orbit of s dense in $X_{\delta,s} \coloneqq \{y : y = x + s \text{ for some } x \in X\} = X$. Hence w occurs (infinitely often) in $\widetilde{\gamma}$ if and only if $O_w \cap X$ is non-empty. To check this condition, we perform a change of variables $y_i = \log(\rho_i)x_i$ on the system of equations defining O_w to obtain

$$
\begin{aligned}
&0 \le y_i < \log(\rho_i) \text{ for } 1 \le i \le d, \quad i \ne b \\
&y_b = 0 \\
&k_1 \log(\rho_{b_0}) + y_{b_0} > \cdots > k_m \log(\rho_{b_m}) + y_{b_m} > l_i \log(\rho_i) \text{ for } i = 1, \ldots, d.
\end{aligned}
$$

Note that the coefficients of all $y_1, \ldots, y_d$ are 1. Eliminating $y_1, \ldots, y_d$ using the Fourier-Motzkin algorithm (Sec. 2.9), we transform the system above into a Boolean combination of linear inequalities in $\log(\rho_1), \ldots, \log(\rho_d)$, which we then solve using Lem. 2.12. □

Proof of Thm. 4.7. As discussed above, for all $z_0, \ldots, z_d \in \mathbb{Z}$,

$$\sum_{i=1} z_i \delta_i = z_0 \Leftrightarrow \sum_{i \ne b} \frac{z_i}{\log(\rho_i)} = \frac{z_0 - z_b}{\log(\rho_b)}.$$

Therefore, from a basis of $G_L(1/\log(\rho_1), \ldots, 1/\log(\rho_d))$ we can compute a basis of $G_A(\delta_1, \ldots, \delta_d)$ and hence the closure $X_\delta \subseteq \mathbb{T}^d$ of the orbit of $\mathbf{0}$ under $x \mapsto x + \delta$ (see Sec. 2.7). Hence whether $X_{\delta,s} = s + X_\delta$ intersects O_w (which is equivalent to w appearing $\widetilde{\gamma}$) can be written as the system consisting of (13), the equation $0 \le x_1, \ldots, x_d < 1$, and $\mathbb{Q}$-affine equations stating that $(x_1, \ldots, x_d) \in X_{\delta,s}$ obtained from the basis of $G_A(\delta_1, \ldots, \delta_d)$. Recall that r_i, which appears in the definition of s_i, is equal to $c_i \rho_i^{m_i}$. We thus have a system of polynomial equalities and inequalities in $\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d)$ that holds if and only if $X_{\delta,s}$ intersects O_w. To solve the system, we first check which $p(\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d))$, where p is a polynomial appearing in the system, are equal to zero using the ideal of all polynomial relations (i.e., solving the ideal membership problem using, e.g., Gröbner bases [20]). Thereafter, we can determine the signs of non-zero $p(\log(c_1), \log(\rho_1), \ldots, \log(c_d), \log(\rho_d))$ by computing sufficiently close over- and under-approximations. □

Proof of Thm. 4.5. It suffices to give an algorithm for deciding whether w occurs in γ that relies on Schanuel's conjecture only for termination. We run two semi-algorithms in parallel. On one hand, we generate larger and larger prefixes of γ, and halt if we detect an occurrence of the finite word w. On the other hand, we enumerate all finite subsets V of $\mathbb{Q}^{d+1}$. For each such V, using the decision procedure for the first-order theory of $\mathbb{R}_{\exp}$, we check whether for all $v \coloneqq (v_0, \ldots, v_d) \in V$, $v_0 = \sum_{i=1}^{d} \frac{v_i}{\log(\rho_i)}$. That is, we check whether V is a set of affine relations satisfied by $\frac{1}{\log(\rho_1)}, \ldots, \frac{1}{\log(\rho_d)}$. If no, we generate the next V. If yes, we compute

$$X_V = \{(x_1, \ldots, x_d) \in \mathbb{T}^d : v_0 = x_1 v_1 + \cdots + x_d v_d\}$$

which satisfies $X_V \supseteq X_\delta$. We then check, again using the decision procedure for $\mathbb{R}_{\exp}$, whether $s + X_V$ (which contains $X_{\delta,s}$) intersects O_w. If yes, we move on to the next value of V. If no, we have found a certificate that $X_{\delta,s}$ does not intersect O_w, i.e. the word w does not occur in $\widetilde{\gamma}$. Note that this algorithm always terminates (assuming Schanuel's conjecture) since in case w does not occur, eventually we will generate V such that $X_V = X_\delta$. □

5 MSO DECIDABILITY VIA EXPANSIONS IN INTEGER BASES

In this section, we discuss MSO theories of structures of the form $\langle \mathbb{N}; <, P_1, P_2 \rangle$ where $P_1 = \{qn^d : n \in \mathbb{N}\}$ and $P_2 = \{pb^n : n \in \mathbb{N}\}$ for some positive integers q, p, b, d. Note that both $\langle qn^d \rangle_{n=0}^{\infty}$ and $\langle pb^n \rangle_{n=0}^{\infty}$ are linear recurrence sequences with a single dominant root (1 and b, respectively), but in the former case the dominant root is repeated (in particular, it has multiplicity $d+1$), which does not fall into the scope of the previous section. If $d = 1$ or $b = 1$, then at least one of P_1, P_2 can be defined in $\langle \mathbb{N}; < \rangle$, and hence the MSO theory of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ is decidable by the result of Carton and Thomas [17]. Our approach is again to use automata-theoretic tools to reduce the MSO decision problem to a problem about dynamical systems. However, in this case the relevant dynamical system is given by $x \mapsto \{b \cdot x\}$ (in contrast to $x \mapsto x + t \bmod 1$), which generates the greedy expansion $\tau \in \{0, \ldots, b-1\}^\omega$ of $x \in (0, 1)$ in base b. Our main result is that the MSO theories of our structures are intimately connected to MSO theories of base-b expansions of certain numbers. Recall that for any $\Sigma \subseteq \mathbb{N}$, we can view a word $\tau \in \Sigma^\omega$ as a function of type $\mathbb{N} \to \mathbb{N}$.

Theorem 5.1. *Let $b, d \geq 2$ and $p, q \geq 1$ be integers, $P_1 = \{qn^d : n \in \mathbb{N}\}$, and $P_2 = \{pb^n : n \in \mathbb{N}\}$. Write $\eta = \sqrt[d]{p/q}$, $\zeta = \sqrt[d]{1/b}$, and let $\gamma_0, \ldots, \gamma_{d-1} \in \{0, \ldots, b-1\}^\omega$ be the base-b expansions of $\{\eta\}, \{\eta\zeta\}, \ldots, \{\eta\zeta^{d-1}\}$, respectively. Then the MSO theories of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ and $\langle \mathbb{N}; <, \gamma_0, \ldots, \gamma_{d-1} \rangle$ are Turing-equivalent.*

For example, if $P_1 = \{27n^3 : n \in \mathbb{N}\}$ and $P_2 = 8^{\mathbf{N}}$, then $d = 3$, $\eta = 1/27$, $\zeta = 1/8$, and the base-8 expansions of $1/3$, $1/6$, and $1/12$ underlie the pair of predicates P_1, P_2. Recall that the expansion of a rational number in any base is ultimately periodic with a computable period and pre-period (see, e.g., [42, Thm. 12.4]), and hence definable in $\langle \mathbb{N}; < \rangle$. In our example, because $\eta, \zeta \in \mathbb{Q}$, all three relevant expansions are periodic and the attendant MSO theory is decidable. Let us formalise a few similar corollaries before proving our main result.

Corollary 5.2. *Assuming Conj. 2.16, the MSO theory of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ is decidable whenever $d = 2$ and at least one of $\eta, \eta\zeta$ is rational.*

Proof. Suppose $\eta \in \mathbb{Q}$ or $\eta\zeta \in \mathbb{Q}$. Note that η, ζ are both algebraic. If $\eta, \zeta \in \mathbb{Q}$, then γ_0, γ_1 are periodic and decidability is immediate. Otherwise, for some $i \in \{0, 1\}$, γ_i is periodic and γ_{1-i} is disjunctive by Conj. 2.16. Decidability then follows from Thm. 3.5. □

Corollary 5.3. *The MSO theory of $\langle \mathbb{N}; <, \mathbf{N}^2, 2^{\mathbf{N}} \rangle$ is Turing-equivalent to that of $\langle \mathbb{N}; <, \gamma \rangle$, where γ is the binary expansion of $\sqrt{2} - 1$. .*

Proof. By Thm. 5.1, the MSO theory of $\langle \mathbb{N}; <, \mathbf{N}^2, 2^{\mathbf{N}} \rangle$ is Turing-equivalent to that of $\langle \mathbb{N}; <, \gamma_0, \gamma_1 \rangle$ where $\gamma_0 = 0^\omega$ and γ_1 is the binary expansion of $\sqrt{\frac{1}{2}} = \frac{1}{2} \cdot \sqrt{2}$, which is simply the shifted version of the binary expansion of $\sqrt{2} - 1$. □

Corollary 5.4. *Let $b, d, p, q, P_1, P_2, \eta, \zeta$ be as above. Suppose $1/\zeta = \ell$ for an integer ℓ. Then the (decision problem of the) MSO theory of $\langle \mathbb{N}; <, P_1, P_2 \rangle$ is Turing equivalent to Acc_β, where β is the base-ℓ expansion of η. In particular, the MSO theory of $\langle \mathbb{N}; <, \{(k^d)^n : n \in \mathbb{N}\}, \mathbf{N}^d \rangle$ is decidable for any integers $k, d \geq 2$.*

Proof. We have that $b = \ell^d$. Let $\gamma = \gamma_0 \times \cdots \times \gamma_{d-1}$. Applying Thm. 5.1, it suffices to show that Acc_γ is Turing-equivalent to Acc_σ.

If $x \in (0, 1)$ has the base-b expansion $\sigma \in \{0, \ldots, b-1\}^\omega$, then its base-$\ell$ expansion can be obtained by simply replacing each letter $\sigma(n)$ with its base-ℓ expansion, padded with leading zeros to make the total length equal to d. Hence we can map the base-b expansion of a number to its base-ℓ expansion using a transducer, and vice versa.

Let $\widetilde{\gamma}_i$ be the base-ℓ expansion of $\{\eta\zeta^i\} = \{\eta\ell^i\}$, which is just a shift of the base-ℓ expansion of $\{\eta\}$. Combining this with the earlier argument, we obtain that the base-b expansion γ_i of $\{\eta\zeta^i\}$ can be obtained from the base-ℓ expansion β of $\{\eta\}$ via a transduction, and vice versa. The same conclusion then also holds for γ and β. It remains to apply Cor. 3.7.

To prove the second statement, note that in that case we have $b = k^d$, $1/\zeta = k \in \mathbb{Z}$, $\eta = 1$, and $\beta = 0^\omega$. □

Proof of Thm. 5.1. Henceforth let P_1, P_2 and η, ζ be as above and $\widetilde{\alpha} \in (\{0, 1\}^2)^\omega$ be the characteristic word of $\langle \mathbb{N}; <, P_1, P_2 \rangle$. For $0 \leq i < d$, let $Q_i = \{pb^{dn+i} : n \in \mathbb{N}\}$, and let $\alpha \in (\{0, 1\}^{d+1})^\omega$ be the characteristic word of

$\langle \mathbb{N}; <, P_1, Q_0, \ldots, Q_{d-1} \rangle$. We can construct transducers $\mathcal{B}, C$ such that $\alpha = \mathcal{B}(\widetilde{\alpha})$ and $\widetilde{\alpha} = C(\alpha)$. By Lem. 3.6, $\mathrm{Acc}_{\widetilde{\alpha}}$ and Acc_α are Turing-equivalent. Therefore, our goal is to show that Acc_α is Turing-equivalent to Acc_γ, where $\gamma = \gamma_0 \times \cdots \times \gamma_{d-1} \in (\{0, \ldots, b-1\}^d)^\omega$.

Let $\beta \in (\{0,1\}^{d+1})^\omega$ be the order word of $(P_1, Q_0, \ldots, Q_{d-1})$. We first show that $(P_1, Q_0, \ldots, Q_{d-1})$ are effectively procyclic and effectively sparse, and hence Acc_α is Turing-equivalent to Acc_β. Each predicate is the value set of a strictly increasing integer linear recurrence sequence, and hence is effectively procyclic (Lem. 2.5). It remains to argue that they are collectively effectively sparse. This follows immediately from the facts that

- $|pb^{dn_1+r_1} - pb^{dn_2+r_2}| \geq pb^{\min\{dn_1+r_1, n_2+r_2\}} \cdot \left(1 - \frac{1}{b}\right)$ for all n_1, n_2, r_1, r_2 such that $pb^{dn_1+r_1} - pb^{dn_2+r_2} \neq 0$,
- $\lim_{n\to\infty} q(n+1)^d - qn^d = \infty$,

and the following classical result of Schinzel and Tijdeman [43].

Theorem 5.5. *For every $N \geq 1$, the equation $|qn^d - pb^m| = N$ has finitely many solutions $(n, m) \in \mathbb{N}^2$ that can be effectively enumerated.*

We next prove that Acc_β is Turing-equivalent to Acc_γ. Note that $Q_i \cap Q_j = \varnothing$ for all $i \neq j$, and

$$\mathrm{Ord}(Q_0, \ldots, Q_{d-1}) = ((1,0,\ldots,0)\ (0,1,0,\ldots,0)\ \cdots\ (0,\ldots,0,1))^\omega.$$

This is because, when constructing $Q_0, \ldots, Q_{d-1}$, we simply took the d alternating subsequences from the strictly increasing sequence $\langle pb^n \rangle_{n=0}^\infty$. By Definition 4.10, we have that

$$\beta = \mathrm{Ord}(qn^d, pb^{nd}, pb^{nd+1}, \ldots, pb^{nd+(d-1)}).$$

Dividing by q and taking dth roots,

$$\beta = \mathrm{Ord}(n, v_n^{(0)}, \ldots, v_n^{(d-1)})$$

where

$$v_n^{(i)} = \sqrt[d]{\frac{p}{qb^{d-i}}} \cdot b^{n+1} = \eta\zeta^{d-i} \cdot b^{n+1}. \tag{14}$$

To see the connection to expansions in base b, recall that for any $x > 0$, the nth digit in the base-b expansion of $\{x\}$ is given by $\lfloor x \cdot b^{n+1} \rfloor \bmod b$. Hence

$$\gamma_i(n) = \lfloor v_n^{(i)} \rfloor \bmod d \tag{15}$$

for all i, n. Next, observe that $v_n^{(i)} < v_n^{(j)}$ for all n and $i < j$, and $v_n^{(i)} < v_m^{(j)}$ for all i, j and $n < m$. We can therefore write

$$\beta = \prod_{n=0}^{\infty} w_n, \qquad w_n = (1,0,\ldots,0)^{k_n^{(1)}} z_1 \cdots (1,0,\ldots,0)^{k_n^{(d)}} z_d$$

where $k_n^{(i)} \geq 0$ and

$$z_i = (y_i, \underbrace{0, \ldots, 0}_{i-1 \text{ times}}, 1, 0, \ldots, 0)$$

with $y_i \in \{0,1\}$ for all i and n. The term $v_n^{(i)}$ corresponds to the letter z_i in the factor w_n. By simple counting,

$$\lfloor v_n^{(i)} \rfloor = |\{l \in \mathbb{N} : l \leq v_n^{(i)}\}| = \sum_{m=0}^{n-1} \sum_{j=0}^{d-1} (k_m^{(j)} + y_j) + \sum_{j=0}^{i} (k_m^{(j)} + y_j) \tag{16}$$

for all n, i. Write $v_{n+1}^{(-1)} = v_n^{(d-1)}$ for all n, i. We then have that

$$\lfloor v_n^{(i)} \rfloor = \lfloor v_n^{(i-1)} \rfloor + k_n^{(i)} + y_i. \tag{17}$$

or all $n \geq 1$ and i. Note that

$$\frac{v_n^{(i)}}{v_n^{(i-1)}} = b^{\frac{1}{d}} > 1$$

for all $n \geq 1$ and i, and hence

$$\lim_{n\to\infty} k_n^{(i)} = \infty \tag{18}$$

for all i. On the other hand, $v_{n+1}^{(i)} = b \cdot v_n^{(i)}$ for all n, i, and from (15) it therefore follows that

$$\lfloor v_{n+1}^{(i)} \rfloor = b \cdot \lfloor v_n^{(i)} \rfloor + \gamma_i(n). \tag{19}$$

We can now prove that Acc_β and Acc_γ are Turing-equivalent.

Acc_γ **reduces to** Acc_β**.** We give a transducer $\mathcal{B}$ such that $\gamma = \mathcal{B}(\beta)$, and apply Lem. 3.6. The transducer reads β in chunks $\langle w_n \rangle_{n=0}^\infty$, and outputs $\gamma(n)$ after reading w_n. Before reading w_n for $n \geq 1$, the transducer has in memory only the value of $v_{n-1}^{(1)}$ mod b. As it reads w_n, for all i it records $k_n^{(i)}$ mod b using b states, from which it computes $\lfloor v_n^{(i)} \rfloor$ using (17) and $\gamma_i(n)$ using (15).

Acc_β **reduces to** Acc_γ**.** We will apply Thm. 3.8. The factorisation of β is given by $\beta = \prod_{n=0}^\infty w_n$ as above. Let $\Sigma_1 = \{0, \ldots, b-1\}^d$, $\Sigma_2 = \{0,1\}^{d+1}$, and $h\colon \Sigma_2^* \to M$ be a morphism into a finite monoid. We have to give a transducer $\mathcal{B}$ such that $\mathcal{B}(\gamma) = \prod_{n=0}^\infty h(w_n)$. By the classical lasso argument, from M we can construct L, m with $m \geq 1$ such that for any $x \in M$ and $n \geq L$, $x^n = x^{L+((n-L) \bmod m)}$.

Using (18) and (14), compute N such that $k_n^{(i)} > L$ and $\lfloor v_n^{(i)} \rfloor > L$ for all i and $n \geq N$. The transducer $\mathcal{B}$ has the values of $h(w_n)$ hard-coded into it for all $n \leq N$. Before reading $\gamma(n)$ for $n > N$, it has in its memory the value of $r_{n-1}^{(i)} \coloneqq (\lfloor v_{n-1}^{(i)} \rfloor - L) \bmod m$ for all i. After reading $\gamma(n)$, it first computes $r_n^{(i)} \coloneqq (\lfloor v_n^{(i)} \rfloor - L) \bmod m$ for all i using (19). Then it computes $x^{k_n^{(i)}}$ for all i, where $x = h((1, 0, \ldots, 0))$, using the fact that

$$x^{k_n^{(i)}} = x^{\lfloor v_n^{(i)} \rfloor - \lfloor v_{n-1}^{(i)} \rfloor - y_i} = x^{L + \left(\left(r_n^{(i)} - r_{n-1}^{(i)} - 1\right) \bmod m\right)}$$

which follows from our construction of N. Finally, it outputs $h(w_n) = x^{k_n^{(1)}} h(z_1) \cdots x^{k_n^{(d)}} h(z_d)$. □

6 DISCUSSION

The results of Sec. 4 tell us everything that can be said about decidability of the MSO theories of linear recurrence sequences with one dominant root, barring major advances in the open decision problems of LRS including the Skolem Problem, the Positivity Problem, etc. However, they do not really tell us anything new about the decidability of the MSO theory of $\langle \mathbb{N}; <, \{u_n \geq 0 \colon n \in \mathbb{N}\}\rangle$, where $\langle u_n \rangle_{n=0}^\infty$ is an arbitrary integer LRS: our focus in this paper was rather on how to combine multiple predicates of arithmetic origin. For an LRS $\langle u_n \rangle_{n=0}^\infty$ with a single dominant root (which must be real), decidability of the MSO theory of $\langle \mathbb{N}; <, \{u_n \geq 0 \colon n \in \mathbb{N}\}\rangle$ can be shown using the approach of Carton and Thomas, or even Elgot and Rabin. Recently, it was shown that for non-degenerate $\langle u_n \rangle_{n=0}^\infty$ with exactly two non-repeated non-real dominant roots, the MSO theory of $\langle \mathbb{N}; <, \{u_n \geq 0 \colon n \in \mathbb{N}\}\rangle$ is decidable [35]. The proof is based on a novel idea: such $\langle u_n \rangle_{n=0}^\infty$ are *pro-disjunctive*, defined as follows. Order $\{u_n \geq 0 \colon n \in \mathbb{N}\}$ (which is guaranteed to be infinite due to the assumption on $\langle u_n \rangle_{n=0}^\infty$) as $\langle p_n \rangle_{n=0}^\infty$. Then for any $m \geq 1$ and $w \in \Sigma^*$, where $\Sigma = \{0 \leq r < m \colon r$ occurs infinitely often in $\langle p_n \bmod m \rangle_{n=0}^\infty\}$, the word w occurs infinitely often in $\langle p_n \bmod m \rangle_{n=0}^\infty$.

That is, rather than showing that $\langle p_n \bmod m\rangle_{n=0}^{\infty}$ is very structured for any $m \geq 1$, it is shown that $\langle p_n \bmod m\rangle_{n=0}^{\infty}$ is as random as possible for any $m \geq 1$. However, for LRS with more than two dominant roots (as well as LRS with two repeated non-real dominant roots) decidability of the corresponding MSO theory remains open.

For predicates P_1 and P_2 of arithmetic origin, the following elementary property can be expressed in the monadic second-order (or even first-order) language that is nevertheless of great interest. There exist (infinitely many) pairs n, m such that $n \in P_1$, $m \in P_2$, and $n - m = c$, where c is a fixed integer. For example, the famously open Brocard-Ramanujan problem is to determine whether $n! + 1 = m^2$ has any solution $(n, m) \in \mathbb{N}^2$ with $n \notin \{4, 5, 7\}$. Therefore, showing decidability of the MSO theory of $\langle \mathbb{N}; <, \{n!\colon n \in \mathbb{N}\}, \{n^2\colon n \in \mathbb{N}\}\rangle$ would entail major mathematical breakthroughs. Similarly, for any constant $k \geq 2$, the solutions (n, m) of $|F_n - m^k| = 1$, where F_n denotes the nth Fibonacci number, can be effectively enumerated [16]. However, this is already highly non-trivial, and at the time of writing, no algorithm is known for enumerating all solutions (n, m) of $F_n - m^k = c$ for given constants $k \geq 2$, $c \in \mathbb{Z}$. There are many other examples of arithmetic predicates whose MSO theories are connected to unsolved problems in number theory: in the cases we considered, the number-theoretic obstacles were all overcome using Baker's theorem.

ACKNOWLEDGMENTS

Toghrul Karimov, Joël Ouaknine, and Mihir Vahanwala are supported by DFG grant 389792660 as part of `TRR 248`. Joël Ouaknine is also supported by ERC grant DynAMiCs (101167561), and has a secondary affiliation with Keble College, Oxford as `emmy.network` Fellow. Valérie Berthé is supported by ERC grant DynAMiCs (101167561) and the Agence Nationale de la Recherche through the project "SymDynAr" (ANR-23-CE40-0024-01). James Worrell is supported by EPSRC Fellowship EP/X033813/1.

The Max Planck Institute for Software Systems is part of the Saarland Informatics Campus. This work partly arose through exchanges held at the workshop *Algorithmic Aspects of Dynamical Systems*, which took place in April and May 2023 at McGill University's Bellairs Research Institute in Barbados.

REFERENCES

[1] Boris Adamczewski and Yann Bugeaud. 2007. On the complexity of algebraic numbers. *Annals of Mathematics* 165, 2 (2007), 547–565.

[2] Jean-Paul Allouche and Jeffrey Shallit. 2003. *Automatic sequences: theory, applications, generalizations.* Cambridge University Press.

[3] Shaull Almagor, Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. 2021. Deciding ω-regular properties on linear recurrence sequences. *Proceedings of the ACM on Programming Languages (POPL)* 5 (2021), 1–24.

[4] Pierre Arnoux, Christian Mauduit, Iekata Shiokawa, and Jun-ichi Tamura. 1994. Complexity of sequences defined by billiard in the cube. *Bulletin de la Société Mathématique de France* 122, 1 (1994), 1–12.

[5] A. Baker and G. Wüstholz. 1993. Logarithmic forms and group varieties. *Journal für die reine und angewandte Mathematik* 442 (1993), 19–62.

[6] Yu. Baryshnikov. 1995. Complexity of trajectories in rectangular billiards. *Communications in Mathematical Physics* 174 (1995), 43–56.

[7] Paul T. Bateman, Carl G. Jockusch, and Alan R. Woods. 1993. Decidability and undecidability of theories with a predicate for the primes. *The Journal of Symbolic Logic* 58, 2 (1993), 672–687.

[8] Nicolas Bedaride. 2009. Directional complexity of the hypercubic billiard. *Discrete Mathematics* 309, 8 (2009), 2053–2066.

[9] Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. 2024. On the decidability of monadic second-order logic with arithmetic predicates. In *Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science*. 1–14.

[10] Valérie Berthé, Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. 2025. The monadic theory of toric words. *Theoretical Computer Science* 1025 (2025), 114959.

[11] Achim Blumensath. 2023. Monadic second-order model theory. Pre-print of a book, https://www.fi.muni.cz/~blumens/MSO.pdf.

[12] J. R. Büchi. 1990. On a decision method in restricted second order arithmetic. In *The Collected Works of J. Richard Büchi*. Springer New York, 425–435.

[13] J. R. Büchi and L. H. Landweber. 1969. Definability in the monadic second-order theory of successor. *The Journal of Symbolic Logic* 34, 2 (1969), 166–170.

[14] Yann Bugeaud. 2012. *Distribution modulo one and Diophantine approximation*. Cambridge Tracts in Mathematics, Vol. 193.

[15] Yann Bugeaud. 2012. *Distribution modulo one and Diophantine approximation*. Vol. 193. Cambridge University Press.

[16] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek. 2008. Fibonacci numbers at most one away from a perfect power. *Elemente der Mathematik* 63, 2 (2008), 65–75.
[17] Olivier Carton and Wolfgang Thomas. 2002. The monadic theory of morphic infinite words and generalizations. *Information and Computation* 176, 1 (2002), 51–65.
[18] Henri Cohen. 2013. *A course in computational algebraic number theory*. Vol. 138.
[19] Thierry Combot. 2025. Computing linear relations between polynomial roots. *Mathematics of Computation* (2025).
[20] David A. Cox, John Little, and Donal O'Shea. 2025. Gröbner bases. In *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer, 49–119.
[21] Calvin C. Elgot and Michael O. Rabin. 1966. Decidability and undecidability of extensions of second (first) order theory of (generalized) successor. *The Journal of Symbolic Logic* 31, 02 (1966), 169–181.
[22] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. 2003. *Recurrence sequences*. American Mathematical Society.
[23] N. Pytheas Fogg, Valéré Berthé, Sébastien Ferenczi, Christian Mauduit, and Anne Siegel. 2002. *Substitutions in dynamics, arithmetics and combinatorics*. Springer.
[24] Steven M. Gonek and Hugh L. Montgomery. 2016. Kronecker's approximation theorem. *Indagationes Mathematicae* 27, 2 (2016), 506–523. In Memoriam J.G. Van der Corput (1890–1975) Part 2.
[25] Glyn Harman. 2002. One hundred years of normal numbers. In *Surveys in Number Theory*. AK Peters/CRC Press, 57–74.
[26] Toghrul Karimov. 2023. *Algorithmic Verification of Linear Dynamical Systems*. Ph. D. Dissertation. University of Saarland.
[27] Toghrul Karimov, Edon Kelmendi, Joris Nieuwveld, Joël Ouaknine, and James Worrell. 2023. The power of Positivity. In *2023 38th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*. IEEE, 1–11.
[28] Toghrul Karimov, Engel Lefaucheux, Joël Ouaknine, David Purser, Anton Varonka, Markus A. Whiteland, and James Worrell. 2022. What's decidable about linear loops? *Proceedings of the ACM on Programming Languages (POPL)* 6 (2022), 1–25.
[29] Toghrul Karimov, Joris Nieuwveld, Joël Ouaknine, Mihir Vahanwala, and James Worrell. 2025. Algorithmic applications of Schanuel's conjecture. In *Principles of Formal Quantitative Analysis: Essays Dedicated to Christel Baier on the Occasion of Her 60th Birthday*. Springer, 118–138.
[30] Serge Lang. 1966. *Introduction to transcendental numbers*. Addison-Wesley.
[31] M. Lothaire. 2002. *Algebraic combinatorics on words*. Vol. 90. Cambridge University Press.
[32] A. Macintyre and A. J. Wilkie. 1996. On the decidability of the real exponential field. In *Kreiseliana. About and Around Georg Kreisel*, Piergiorgio Odifreddi (Ed.). AK Peters, 441–467.
[33] David W. Masser. 1988. Linear relations on algebraic groups. *New Advances in Transcendence Theory* (1988), 248–262.
[34] M. Mignotte, T. N. Shorey, and R. Tijdeman. 1984. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik* 349 (1984).
[35] Joris Nieuwveld and Joël Ouaknine. 2025. On Expansions of Monadic Second-Order Logic with Dynamical Predicates. In *50th International Symposium on Mathematical Foundations of Computer Science (MFCS 2025) (LIPIcs, Vol. 345)*, Paweł Gawrychowski, Filip Mazowiecki, and Michał Skrzypczak (Eds.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 80:1–80:17. https://doi.org/10.4230/LIPIcs.MFCS.2025.80
[36] Joël Ouaknine and James Worrell. 2014. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the twenty-fifth annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM, 366–379.
[37] Joël Ouaknine and James Worrell. 2014. Ultimate positivity is decidable for simple linear recurrence sequences. In *International Colloquium on Automata, Languages, and Programming*. Springer, 330–341.
[38] Martine Queffélec. 2006. Old and new results on normality. *Dynamics & Stochastics: Festschrift in Honour of MS Keane* 48 (2006), 225.
[39] Alexander Rabinovich. 2007. On decidability of monadic logic of order over the naturals extended by monadic predicates. *Information and Computation* 205, 6 (2007), 870–889.
[40] Alexander Rabinovich and Wolfgang Thomas. 2006. Decidable theories of the ordering of natural numbers with unary predicates. In *International Workshop on Computer Science Logic*. Springer, 562–574.
[41] Alfréd Rényi. 1957. Representations for real numbers and their ergodic properties. *Acta Mathematica Academiae Scientiarum Hungaricae* 8, 3-4 (1957), 477–493.
[42] Kenneth H. Rosen. 2011. *Elementary number theory*. Pearson Education London.
[43] Andrzej Schinzel and Robert Tijdeman. 1976. On the equation $y^m = P(x)$. *Acta Arithmetica* 31 (1976), 199–204.
[44] A. L. Semënov. 1980. On certain extensions of the arithmetic of addition of natural numbers. *Mathematics of The USSR-Izvestiya* 15, 2 (1980), 401–418.
[45] A. L. Semënov. 1984. Logical theories of one-place functions on the set of natural numbers. *Mathematics of the USSR-Izvestiya* 22, 3 (1984), 587–618.
[46] Wolfgang Thomas. 1975. A note on undecidable extensions of monadic second order successor arithmetic. *Archiv für mathematische Logik und Grundlagenforschung* 17, 1 (1975), 43–44.
[47] Wolfgang Thomas. 1997. Languages, automata, and logic. In *Handbook of formal languages, volume 3*. Springer, 389–455.
[48] Michel Waldschmidt. 2000. *Diophantine approximation on linear algebraic groups: transcendence properties of the exponential function in several variables*. Springer Berlin Heidelberg, Berlin, Heidelberg.