

Computing the Density of the Positivity Set for Linear Recurrence Sequences

Edon Kelmendi

Abstract

The set of indices that correspond to the positive entries of a sequence of numbers is called its positivity set. In this paper, we study the density of the positivity set of a given linear recurrence sequence, that is the question of how much more frequent are the positive entries compared to the non-positive ones. We show that one can compute this density to arbitrary precision, as well as decide whether it is equal to zero (or one). If the sequence is diagonalisable, we prove that its positivity set is finite if and only if its density is zero. Lastly, arithmetic properties of densities are treated, in particular we prove that it is decidable whether the density is a rational number, given that the recurrence sequence has at most one pair of dominant complex roots.

Contents

1	Introduction	2
2	Sequences and Densities	7
3	Strongly Non-Degenerate Subsequences	9
3.1	Period P_1	10
3.2	Period P_2	10
3.3	Properties of the Subsequences	12
4	The Density 1 Problem	14
4.1	The Case of Diagonalisable Sequences	17
5	Computing the Density	19
6	When is the Density a Rational Number?	22
6.1	Density as a Period	22
6.2	One Pair of Dominant Complex Roots	24

1 Introduction

Linear recurrence sequences (LRS) are infinite sequences of rational numbers $\langle u_n \rangle_{n \in \mathbb{N}}$, whose every entry is a linear combination of the k preceding entries. That is, a sequence that satisfies a recurrence relation:

$$u_n = a_1 u_{n-1} + \cdots + a_k u_{n-k}, \quad (1)$$

for all $n > k$, where a_1, \dots, a_k are rationals and $a_k \neq 0$. The constants a_1, \dots, a_k , and u_1, \dots, u_k uniquely identify the sequence.

Firmly grounded as one of the fundamental families of finitely represented number sequences, they are ubiquitous in mathematics and computer science; their importance is evident. A basic object of study in modern number theory, they appear in the investigation of pseudo-random number generators, in cellular automata, as solutions of some Diophantine equations, as the number of zeros of varieties over finite fields, to name just a few examples. Furthermore, they are intrinsically related to linear dynamical systems, and the field of dynamical systems as a whole.

From another point of view, a linear recurrence sequence can be seen as a kind of restricted Turing machine, namely one that has a single loop inside which the variables are updated by a linear function. As such programs permeate any larger piece of software, verifying their correctness has become increasingly important in recent years. This motivation has driven further interest in algorithmic questions regarding these sequences.

This field has been a rather active area of research in the past few decades — a considerable body of work has amassed. The wide-scoped monograph [EVDPS⁺03] by Everest, van der Poorten, Shparlinski, and Ward is a place where one can find central results, their applications, as well as a taste of techniques that have proven useful. Here we recount only a brief summary of the theorems that are directly relevant to the present work.

We start with a basic question: What does the zero set of a linear recurrence sequence $\{n : u_n = 0\}$ look like? The wonderfully simple answer, provided in 1934 by Thoralf Skolem [Sko34] using p -adic analysis, is that the zero set of a linear recurrence sequence is a finite union of arithmetic progressions and a finite set. In other words, the zero set is ultimately periodic. This theorem was soon after generalised to sequences of algebraic numbers by Mahler [Mah35], and then later on by Lech, to sequences of members of any ring of characteristic zero [Lec53]. An elementary proof of Skolem's theorem can be found in [Han85], see also the discussion in Chapter 2.1 of [EVDPS⁺03]. Unfortunately, even though we know the form of zero sets, we do not know how to decide if it is empty. Every known proof of this result uses, in some way or other, p -adic analysis, resulting in a non-constructive argument. The question of whether one can decide if there exists some n , such that $u_n = 0$, known as Skolem's problem, remains to this day, the central open problem for LRS.

However, there are some partial results for sequences of low order¹: With the help of Baker's theorem for linear forms in logarithms of algebraic numbers, Mignotte, Shorey,

¹The order of the sequence is the smallest k for which the sequence satisfies a recurrence like (1).

and Tijdeman [TMS84, Theorem 2], and in parallel Vereshchagin [Ver85, Theorem 4], proved that for sequences of order at most four, one can decide whether their zero set is empty. In the direction of hardness, Skolem’s problem is known to be NP-hard [BP02].

One can raise the same questions about the positivity set $\{n : u_n > 0\}$. This set, however, unlike the zero set, does not admit a clean description. In fact the positivity problem (is there some n such that $u_n > 0$) is more general than the Skolem’s problem. That is, there is a polynomial reduction from Skolem’s problem to the positivity problem (with a quadratic increase in the order). The positivity problem is known to be decidable for LRS of order at most five [OW13], where Baker’s theorem plays a crucial role again. In the direction of hardness, a decision procedure for the positivity problem for LRS of order six would allow one to compute the homogeneous Diophantine approximation type of a large class of transcendental numbers [OW13, Theorem 5.2]. Which suggests that such a procedure must come hand-in-hand with a deeper understanding — than hitherto exists — of Diophantine approximations of transcendental numbers.

Questions of asymptotic nature seem to be slightly more approachable. For example, one can decide if a sequence has infinitely many zeros [BM76, Theorem 2]. The corresponding problem for the positivity set, *i.e.* are there infinitely many n , for which $u_n > 0$ is not known to be decidable, however. This problem is called the ultimate positivity problem². In fact, as for positivity, a similar link to Diophantine approximations exists [OW13, Theorem 5.1]. Nevertheless, there is an important positive result: namely that the ultimate positivity problem is decidable for *diagonalisable* LRS [OW14]. A sequence is diagonalisable if its characteristic polynomial, which for a sequence that satisfies (1) is

$$x^k - a_1 x^{k-1} - \dots - a_{k-1} x - a_k, \quad (2)$$

has no repeated roots. In fact, it is possible to go much further for diagonalisable sequences [AKK⁺21]: One can decide any asymptotic ω -regular property, even when the property itself is part of the input.

For the general case not much progress has been made however, it remains a long standing, difficult, open problem to decide anything about the positivity set of a general LRS, in particular whether this set is empty, or whether it is finite. In the present paper, we prove that it is possible to decide some things about another notion of size of a subset of naturals: its *density*.

Recall that the density of a set $S \subseteq \mathbb{N}$ is

$$\lim_{n \rightarrow \infty} \frac{|\{1, 2, \dots, n\} \cap S|}{n},$$

where the vertical bars denote cardinality (note that the limit need not exist). The density is a notion used to measures how *large* an infinite subset of natural numbers is.

Example 1.1. Here is a trivial LRS: $u_1 = 1$ and $u_n = -u_{n-1}$. Clearly its positivity set are the odd numbers, and its density is equal to $1/2$.

²Ultimate positivity is the question: “is it true that after some point every entry of the sequence is positive?” Which is false if and only if the negativity set is infinite, or the positivity set of $\langle -u_n \rangle_{n \in \mathbb{N}}$ is infinite.

Example 1.2. It is possible to construct linear recurrence sequences that are equal to $\cos(n\theta)$, $n \in \mathbb{N}$. If θ is a rational multiple of π , the positivity set of these sequences will have some rational density, if however θ is not a rational multiple of π then, we will later see, that the density is equal to $1/2$.

The density of the positivity set of any linear recurrence sequence always exists. This fact was proved by Bell and Gerhold [BG07, Theorem 1], and is our principal starting point. With the exception of the paper above, to the best of my knowledge there is no other work that deals with the density of the positivity set. The paper [BM76] can however be interpreted as providing an algorithm to compute the density of the zero set.

We now describe the results of this paper. The first one is of a qualitative nature:

Theorem 1.3. *There is a procedure that inputs a LRS and decides whether the density of its positivity set is equal to 1.*

The same procedure can be used to decide whether the density is equal to 0, after a trivial pre-processing step.

Bell and Gerhold have observed, by using a uniformity theorem in Cassel’s book [Cas59], that the density is equal to the Lebesgue measure of a certain set. We proceed along the same path and go further by constructing this set, for which it is necessary to explicitly describe the multiplicative relations among the roots of the polynomial (2). Afterwards, the problem is reduced to checking the emptiness of a semialgebraic set, which can be done using the decidability of the theory of real closed fields, *i.e.* Tarski’s algorithm. These tools have been successfully employed by Ouaknine, Worrell, and others on a number of related problems, it is not surprising that they prove useful to bear on the problems of this paper as well.

The procedure in Theorem 1.3 runs in PSPACE, but when the order of the sequence is fixed, the complexity drops to PTIME.

Although we do not yet know how to decide whether the sequence has infinitely many positive entries, we can decide whether there are *many* of them, in the sense of having non-zero density, using Theorem 1.3. Another point of view is that the question “is the density 0?” over-approximates the question “is the positivity set finite?”, because a positive answer to the latter implies the same for the former. However, for the family of diagonalisable sequences, the implication becomes an equivalence — the two questions are the same:

Theorem 1.4. *In a diagonalisable sequence the positivity set is finite if and only if its density is zero.*

Theorem 1.3 and Theorem 1.4 together imply the main theorem of [OW14], that ultimate positivity is decidable for diagonalisable LRS. However the proof has the same ingredients, in particular a result on the growth of LRS by Evertse, van der Poorten and Schlickewei, which is based on a lower bound for sums of S -units, itself based on the deep “subspace theorem” of Schmidt.

The main theorem of this paper says that we can compute densities to arbitrary precision:

Theorem 1.5. *There is a procedure that inputs a LRS $\langle u_n \rangle_{n \in \mathbb{N}}$ and a rational number $\epsilon \in \mathbb{Q}$, and computes some δ' , such that $|\delta - \delta'| < \epsilon$, where δ is the density of the positivity set of $\langle u_n \rangle_{n \in \mathbb{N}}$.*

The complexity is the same as for the density 1 problem, the problem is in PSPACE in the input and $\lceil \epsilon^{-1} \rceil$, but it drops to polynomial time when the order of the sequence is fixed.

The idea of the proof of Theorem 1.5 is straightforward. We have to approximate the Lebesgue measure of a certain subset of the d -dimensional unit cube. To this end, we draw a grid of N^d points and count how many of these points fall in the set. It then remains to prove that we can decide whether a given rational point is a member of the set, and to upper bound the error term. For the latter we use a result of Koiran [Koi95]. We note that it is possible, instead of testing for every point whether it belongs to the set, to test it for fewer points that are picked randomly, resulting in a faster Monte-Carlo type algorithm.

Let us give a simple example that illustrates some of the ideas behind the theorems above.

Example 1.6. Consider the following simple program:

```
x=0; y=6; z=4;
while true do
  x=4x+3y;
  y=4y-3x;
  z=5z;
  if y+z>0 then
    | Region A
  else
    | Region B
  end
end
```

It is not immediately evident from looking at this program that, for example, Region A is entered infinitely often. The algorithm from Theorem 1.5 can be used to conclude not only Region A is entered infinitely often, but that it is entered with frequency:

$$0.732279 \dots = \frac{\cos^{-1}(-2/3)}{\pi}.$$

At first sight, it might seem strange to see notions related to circles and triangles such as π and \cos appearing in the answer of a simple question about a simple program, but the reality is that only through them can we understand the program above. Let us explain the answer in more detail. The value of $y + z$ in the n -th iteration of the loop is clearly equal to

$$\begin{pmatrix} 0 & 6 & 4 \end{pmatrix} \cdot \begin{pmatrix} 4 & -3 & 0 \\ 3 & 4 & 0 \\ 0 & 0 & 5 \end{pmatrix}^n \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Multiplying this quantity with 5^{-n} will not change its sign and we see that after the multiplication, the update matrix is a rotation in the first two coordinates:

$$\begin{pmatrix} 4/5 & -3/5 & 0 \\ 3/5 & 4/5 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} \cos n\phi & -\sin n\phi & 0 \\ \sin n\phi & \cos n\phi & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where the angle ϕ is $\cos^{-1}(4/5)$. Multiplying this matrix with the row vector and the column vector above, we see that the variable $y + z$ in the n -th iteration of the loop has the same sign as $6 \cos(n\phi) + 4$. So now the question: with what frequency does the loop enter Region A? has been reduced to the question: for how many n is $\cos(n\phi) > -2/3$? When the angle ϕ is not a rational multiple of π (which is the case here), it is a theorem that $n\phi$ is uniformly recurrent modulo π , meaning that for any interval I in $[0, \pi]$, the frequency with which $n\phi \bmod \pi$ enters I is proportional to the size of I (that is length of the interval divided by π). As a consequence, since $\cos(n\phi) > -2/3$ if and only if $n\phi \bmod \pi$ belongs to the interval $[0, \cos^{-1}(-2/3)]$, the answer follows.

Example 1.6 and Example 1.2 show that density can be both a rational and an irrational quantity. Therefore, the algorithm in Theorem 1.5 cannot *a priori* be used to decide quantitative questions, such as whether the density is larger than some given rational. We give a partial result in this direction but leave the general case open:

Theorem 1.7. *There is a procedure that inputs a LRS that has at most one pair of dominant complex roots, and decides whether the density of its positivity set is rational, and if it is, computes it exactly.*

We also prove that when there are no (non-trivial) multiplicative relations among the dominant roots, the density is a *period*, as defined by Kontsevich and Zagier [KZ01]. We note that conjectures by Kontsevich and Zagier, and of Grothendieck predict the transcendence degree of sets of intervals, but we do not pursue this conjectural direction further.

The rest of this paper is organised as follows. Section 2 contains the principal definitions and generalities. Section 3 is a technical section where we define a strong non-degeneracy condition and split the sequence into subsequences that satisfy it, as a pre-processing step for the algorithms that follow. Section 4 deals with the density 1 problem, as well as the analysis for diagonalisable sequences. In the section that follows we give the procedure to compute the density. In the end, in Section 6, we give the proof of Theorem 1.7, deciding when the density is a rational number.

2 Sequences and Densities

A sequence $\langle u_n \rangle_{n \in \mathbb{N}}$ that satisfies a recurrence relation (1) for all $n > k$, but does not satisfy any linear recurrence with fewer terms, is called a LRS of **order** k . The **characteristic polynomial** of such sequence is the polynomial (2), whose roots are, say

$$\Lambda_1, \Lambda_2, \dots, \Lambda_l,$$

assumed to be distinct, with respective multiplicities $m_1 \dots, m_l$, where $1 \leq l \leq k$. The sequence $\langle u_n \rangle_{n \in \mathbb{N}}$ can be written as a **generalised power sum** (see [EVDPS⁺03, Section 1.1.6]):

$$u_n = \sum_{i=1}^l f_i(n) \Lambda_i^n, \quad (3)$$

where the polynomials f_i have algebraic coefficients, $f_i \in \overline{\mathbb{Q}}[x]$, and the degree of f_i is $m_i - 1$. The converse also holds, any sequence $\langle u_n \rangle_{n \in \mathbb{N}}$ that can be written in the form (3) is a LRS over algebraic numbers. The sequences whose roots all have multiplicity 1, *i.e.* there are no repeated roots, are called **diagonalisable** (or simple) sequences.

A LRS is given by the numbers a_1, \dots, a_k and u_1, \dots, u_k . From which, it is possible to compute descriptions of the constants in (3) in polynomial time in the bitlength of the input. By a **description** of an algebraic number we mean³ a first-order formula that defines it, typically this is the number's minimal polynomial together with intervals specifying where its real and imaginary parts lie. To compute the descriptions of the roots, one runs a root isolation algorithm on the characteristic polynomial (to compute the approximating intervals), see for example [YS11] and [BPR06]. Afterwards, for the computation of polynomials f_i , one solves a system of linear equations of polynomial size in the input. All this can be done in polynomial time. As a consequence, we assume that we have computed the descriptions every constant in (3), and that the roots are ordered by their modulus, *i.e.*

$$|\Lambda_i| \geq |\Lambda_{i+1}|.$$

Density (also referred to as natural density, or asymptotic density in the literature) is a notion that measures how large a subset $S \subseteq \mathbb{N}$ of natural numbers is. It is defined as:

$$D(S) \stackrel{\text{def}}{=} \lim_{n \rightarrow \infty} \frac{|\{1, 2, \dots, n\} \cap S|}{n}, \quad (4)$$

where by the vertical bars we denote the cardinality of the set. Not every set has a density; the limit might not exist. However they do have lower and upper density, which are defined by replacing limit with \liminf and \limsup respectively.

³There are other encodings of an algebraic number α . Mostly one uses the fact that a number field $\mathbb{Q}(\alpha)$ is a vector space of finite dimension. For our purposes however, it is more convenient to define algebraic numbers by first-order formulas over the reals (defined below).

Example 2.1. Here is the density of some simple subsets of natural numbers.

1. An (infinite) arithmetic progression, with common differences d , has density $1/d$. If the set $S \subseteq \mathbb{N}$ is such that the difference between consecutive elements of S is at most d , then the lower density of S is larger than $1/d$.
2. The squares $\{n^2 : n \in \mathbb{N}\}$ have density zero. To prove this, observe that from $n = c^2$ to $n = (c + 1)^2$, the ratio in the definition (4) decreases.
3. The primes have density zero due to the prime number theorem.

The principal object of study in this paper is the density of the **positivity set**:

$$D(\{n : u_n > 0\})$$

of a given LRS $\langle u_n \rangle_{n \in \mathbb{N}}$. Bell and Gerhold proved that it always exists:

Theorem 2.2 ([BG07, Theorem 1]). *The positivity set of any linear recurrence sequence has a density.*

The negativity set is just the positivity set of the sequence $\langle -u_n \rangle_{n \in \mathbb{N}}$ (which is plain, from (3) and the discussion above, that it can be computed). Therefore in the rest of this paper, we only deal with the density of the positivity set, which is simply referred to as the **density of the sequence**.

We will make ample use of procedures for deciding the first-order **theory of real closed fields**, proved by Tarski [Tar51]. In this logic the atomic formulas are

$$f(x_1, \dots, x_n) \geq 0,$$

where $f \in \mathbb{Z}[x_1, \dots, x_n]$ is a polynomial with integer coefficients. The atomic formulas can be connected with Boolean connectives, and one is allowed to quantify over real numbers. Subsets of \mathbb{R}^n defined by such formulas are called **semialgebraic** sets. In the paper cited above, Tarski proved that there exists a procedure that inputs a first-order formula and decides whether it is true when interpreted over the reals.

We can also interpret such formulas over the complex numbers instead of the reals, using the embedding of \mathbb{C}^n to \mathbb{R}^{2n} , handling the real and imaginary parts individually.

Note that our definition of descriptions of algebraic numbers is a simple formula in Tarski's logic. Other formulas that we will construct will be equally simple in the following sense: they will belong to the existential fragment, *i.e.* formulas of the type

$$\exists x_1 \exists x_2 \cdots \exists x_n \quad \Phi(x_1, \dots, x_n),$$

where Φ is quantifier-free. The complexity of this fragment is relatively low:

Theorem 2.3 ([Can88, Theorem 3.3] and [Ren92, Theorem 1.1], respectively). *The existential theory of reals is decidable in PSPACE. When the number of variables is fixed, the complexity drops to PTIME⁴.*

The theorems above expect the polynomials in the input to be written as a sequence of coefficients, each encoded in binary. Note that the exponents cannot be encoded in binary.

⁴The PTIME upper bound holds for the full logic, when the number of variables is fixed.

3 Strongly Non-Degenerate Subsequences

Let $P \in \mathbb{N}$, and consider subsequences of the form:

$$\{\langle u_{nP+\ell} \rangle_{n \in \mathbb{N}} : 0 \leq \ell < P\}. \quad (5)$$

Each one is itself a LRS ([EVDPS⁺03, Theorem 1.3]). One can easily observe this fact from the equality (3): the roots of the subsequence are Λ_i^P and the polynomials $f_i(nP + \ell)$ are multiplied by the constant Λ_i^ℓ .

The purpose of this section is a crucial preprocessing step that splits the sequence into subsequences (5), for a particular $P \in \mathbb{N}$, which we will compute. The subsequences have a number of properties (enumerated in a lemma at the end of the section) that make them more amenable. Effectively dividing the initial problem into easier sub-problems, we can recombine answers of the sub-problems to get answers for the initial problem. For example, if we know the densities of the P subsequences, then the density of the original sequence is equal to their sum divided by P . Or for the density 1 problem: the original sequence has density 1 if and only if all the subsequences have density 1.

In our case the period P is a product:

$$P \stackrel{\text{def}}{=} P_1 \cdot P_2,$$

where P_1 comes from degeneracy, and P_2 from multiplicative relations among the roots. Let N be the bitlength of the input and k the order of the sequence, later in this section we will prove that P will have the upper bound:

$$P \in 2^{\mathcal{O}(k^5 \log \log N)}. \quad (6)$$

Before we give the definitions of the periods P_1 and P_2 , let us first discuss the description of the roots Λ_i^P , as this is important for the complexity upper bounds when P is large. Let $r \in \mathbb{N}$, and let $z \in \overline{\mathbb{Q}}$ be an algebraic number with description $\phi(x)$ (i.e. the formula $\phi(x)$ holds if and only if $x = z$). There are two ways to describe the number z^r :

1. The *trivial way*: saying that there exists some x such that $\phi(x)$ and

$$y = \underbrace{x \cdot x \cdots x}_{r \text{ times}}.$$

Resulting in a constant increase on the number of variables, and a linear increase in r on the size of the formula.

2. The *repeated squaring way*: saying that there exist a roughly $s := \log r$ number of variables x_1, \dots, x_s such that

$$\phi(x_1) \text{ and } y = x_s \text{ and } x_{i+1} = x_i \cdot x_i, \ 1 \leq i \leq s.$$

Resulting in a $\log r$ increase in both the number of variables and the size of the formula.

We will use both methods, depending on which complexity bound we want to derive.

Proposition 3.1. *For a given constant P , bounded by (6), the description of any Λ_i^P can be computed in polynomial time. Furthermore, such a description grows both in the number of variables and in size by a term in $\mathcal{O}(k^5 \log \log N)$.*

When the order of the sequence is fixed, the size of the description grows by a term in $\mathcal{O}(\log N)$ while the number of variables by a constant.

Proof. Using the repeated squaring method results in a formula that grows both in size and in the number of variables by a $\log P$ term, hence the first statement of the proposition.

When k , the order of the sequence is fixed however, it makes more sense to use the trivial way of constructing the formula, because this will result in a constant increase in the number of variables, and a linear in P increase in the size of the formula. Since for fixed k , P is in $\mathcal{O}(\log N)$ the second statement of the proposition follows. \square

Now we define P_1 and P_2 , as well as show how to compute them. In the end of this section we summarise the properties that every subsequence $\langle u_{nP+\ell} \rangle_{n \in \mathbb{N}}$ has.

3.1 Period P_1

We begin with the standard notion of degeneracy. A LRS is said to be **degenerate** if it has two distinct roots Λ_i and Λ_j , whose ratio Λ_i/Λ_j is a root of unity. One can test in PTIME whether a given sequence is degenerate by checking whether any of its ratios of distinct roots satisfies a cyclotomic polynomial of appropriate degree. Consult Section 3 in [YLN95]. If the sequence is degenerate, taking the least common multiple of all the orders of roots of unity that can occur in this way, we get a quantity P_1 , such that all the subsequences with period P_1 are either identically zero, or non-degenerate. The quantity P_1 is upper bounded only by the order of the sequence:

Theorem 3.2 ([EVDPS⁺03, Theorem 1.2]). *Let $\langle u_n \rangle_{n \in \mathbb{N}}$ be a LRS of order k . Then there is a constant*

$$M_k \in 2^{\mathcal{O}(k \sqrt{\log k})},$$

such that for some $P_1 \leq M_k$, each subsequence

$$\langle u_{nP_1+\ell} \rangle_{n \in \mathbb{N}},$$

$0 \leq \ell < P_1$ is either identically zero, or is non-degenerate.

3.2 Period P_2

The definition of P_2 requires a little bit more work. We have assumed that the roots are ordered by their modulus: $|\Lambda_i| \geq |\Lambda_{i+1}|$, suppose that the first j ones are dominant, i.e.,

$$|\Lambda_1| = \dots = |\Lambda_j| > |\Lambda_{j+1}|.$$

Let d be the maximal degree of the polynomials f_1, \dots, f_j from (3), and suppose, without loss of generality, that it is exactly the polynomials f_1, \dots, f_m that are of degree d , for some $m \leq j$. Define the normalised roots:

$$\lambda_i \stackrel{\text{def}}{=} \frac{\Lambda_i^{P_1}}{|\Lambda_i^{P_1}|} \quad 1 \leq i \leq m.$$

We are interested in the multiplicative relations:

$$\mathcal{M}(\lambda_1, \dots, \lambda_m) \stackrel{\text{def}}{=} \{\vec{r} \in \mathbb{Z}^m : \lambda_1^{r_1} \lambda_2^{r_2} \dots \lambda_m^{r_m} = 1\}.$$

This set with addition forms a subgroup of \mathbb{Z}^m . Since the latter is a free abelian group with a basis of m elements, by [Lan02, Theorem 7.3, Chapter I] the subgroup \mathcal{M} is a free abelian group with some basis

$$\vec{b}_1, \dots, \vec{b}_v \in \mathbb{Z}^m, \quad (7)$$

where $v \leq m$. Define

$$P_2 \stackrel{\text{def}}{=} 2 \prod_{\substack{1 \leq s \leq v \\ 1 \leq t \leq m}} |b_{s,t}|. \quad (8)$$

Lemma 3.3. *The integer P_2 is effective. It can be computed in PSPACE. When the order of the sequence is fixed, the computation can be performed in PTIME.*

Proof. We argue that we can compute the basis (7) and hence also P_2 .

It follows from [vdPL77, Theorem 1], that there is an effective upper bound on the absolute value of the coordinates of the basis (7) of size:

$$2^{\mathcal{O}(k^2)} \prod_{i=2}^m \log H(\lambda_i),$$

where H is the Mahler measure, defined as follows. For an algebraic number $z \in \overline{\mathbb{Q}}$, with minimal polynomial

$$a_0 x^d + a_1 x^{d-1} + \dots + a_d = a_0 (x - z_1) \dots (x - z_d),$$

we say that its Mahler measure is:

$$H(z) \stackrel{\text{def}}{=} |a_0| \prod_{i=1}^d \max\{1, |z_i|\} \leq \sqrt{d} \max_{0 \leq i \leq d} |a_i|,$$

where the upper bound comes from [vdPL77, Lemma 1]. Using the fact that for any algebraic number $z \in \overline{\mathbb{Q}}$ and $r \in \mathbb{N}$, $H(z^r) = H(z)^r$, whose proof can be found in [Wal00, Chapter 3], via a straightforward computation, we can derive the following upper bound:

$$\max_{\substack{1 \leq s \leq v \\ 1 \leq t \leq m}} |b_{s,t}| \in 2^{\mathcal{O}(k^3 \log \log N)}, \quad (9)$$

where k is the order of the sequence and N is the bitlength of the input. For any $\vec{b} \in \mathbb{Z}^m$ with the same upper bound, the assertion

$$\vec{b} \in \mathcal{M}(\lambda_1, \dots, \lambda_m),$$

is an existential first-order formula of polynomial size in N , due to Proposition 3.1. Which means that by brute force, we can compute a basis (7) in PSPACE by using the algorithm from Theorem 2.3. When the order k is fixed, the number of variables is constant. As a consequence of the second statement of Theorem 2.3, in this scenario, the basis can be computed in PTIME. \square

From the definition of P_2 , (8), the estimate (9) and Theorem 3.2 one can derive the upper bound (6).

3.3 Properties of the Subsequences

Let $0 \leq \ell < P$, we list a number of properties of the subsequence

$$\langle u_{nP+\ell} \rangle_{n \in \mathbb{N}}, \quad (10)$$

which we assume is not identically zero. We start by replacing the dependent roots as follows.

The only case when the group $\mathcal{M}(\lambda_1, \dots, \lambda_m)$ is trivial is when $m = 1$, which implies that $\lambda_1 = 1$, because complex roots come as conjugate pairs (of the same multiplicity), and being a conjugate pair is a multiplicative relation. In this case, every problem that we treat becomes trivial. Therefore suppose that $m > 1$. Then there exists some member of the basis (7) — say \vec{b}_1 without loss of generality — that has at least two non-zero coordinates. By definition,

$$\lambda_1^{b_{1,1}} \dots \lambda_m^{b_{1,m}} = 1.$$

Suppose that $b_{1,m} \neq 0$. By using Euler's formula we see that we can write:

$$\lambda_m = \varrho \lambda_1^{-b_{1,1}/b_{1,m}} \dots \lambda_{m-1}^{-b_{1,m-1}/b_{1,m}}, \quad (11)$$

where ϱ is a $b_{1,m}$ -th root of unity (and hence also a P_2 -th root of unity, by definition of P_2), and at least one of the exponents $b_{1,1}, \dots, b_{1,m-1}$ is nonzero. Replacing λ_m in the other equations, and continuing in this manner, making at most v replacements, one for every member of the basis, we conclude that the set of indices $\{1, \dots, m\}$ can be partitioned into the indices corresponding to the independent roots and depended roots of the form (11), more precisely it can be partitioned into subsets:

- I - a non-empty subset, with independent λ_i , i.e. that do not have multiplicative relations among themselves,

- D - a subset with dependent λ_i , i.e. those that can be written in the form (11), where in the right hand side only members of I appear, and there is a factor ϱ which is a P_2 -th root of unity (perhaps not primitive)⁵, and
- U - an empty set or a singleton containing some i for which $\lambda_i = 1$.

The reason why U has cardinality at most 1 is as follows. By the process described above, we cannot obtain more than one equation of the type $\lambda_i^r = 1$, because among $\lambda_1, \dots, \lambda_m$, the only root of unity that can appear is the number 1. Indeed, if there were some complex λ_i that is r -th root of unity, then its complex conjugate $\bar{\lambda}_i$ will also appear among the dominant roots $\lambda_1, \dots, \lambda_m$ (with the same multiplicity), and $(\lambda_i/\bar{\lambda}_i)^r = \lambda_i^{2r} = 1$, meaning that the sequences $\langle u_{nP_1+\ell} \rangle_{n \in \mathbb{N}}$ are degenerate, a contradiction of Theorem 3.2.

Rearrange the the roots λ_i such that for some η

$$I = \{1, \dots, \eta\}, \quad D = \{\eta + 1, \dots, m - 1\}, \quad U = \{m\}.$$

The case when D or U is empty is omitted, as it can be treated in essentially the same way. It is convenient to define for all i , $1 \leq i \leq m$:

$$\alpha_i \stackrel{\text{def}}{=} \lambda_i^{P_2} = \frac{\Lambda_i^P}{|\Lambda_i^P|},$$

and the rationals $q_{i,j} \in \mathbb{Q}$, $i \in D, j \in I$, such that:

$$\alpha_i = \prod_{j \in I} \alpha_j^{q_{i,j}}.$$

The generalised power sum form of the sequence (10) is:

$$u_{nP+\ell} = \sum_{i=1}^l \Lambda_i^\ell f_i(nP + \ell) (\Lambda_i^P)^n.$$

Dividing by $n^d |\Lambda_1^P|^n$ does not change the sign, where d is the largest degree of polynomials multiplying the dominant roots. We get the sequence:

$$\begin{aligned} v_n &\stackrel{\text{def}}{=} \sum_{i=1}^m c_i \alpha_i^n + R(n) \\ &= \sum_{i \in I} c_i \alpha_i^n + \sum_{i \in D} c_i \prod_{j \in I} \alpha_j^{q_{i,j}} + c_m + R(n), \end{aligned} \tag{12}$$

where $c_i \in \overline{\mathbb{Q}}$, and $R(n)$ is some residue that tends to zero exponentially, i.e.

$$|R(n)| \in \mathcal{O}(\xi^n), \text{ for some } 0 < \xi < 1. \tag{13}$$

⁵Here we see the reason behind the definition of P_2 : In subsequences with the period P_2 we can directly write the dependent roots as a function of the independent ones; the factor ϱ disappears because it is a P_2 -th root of unity.

Furthermore there are no multiplicative relations among the roots α_i , for $i \in I$, that is:

$$\mathcal{M}(\alpha_1, \dots, \alpha_\eta) = \{\vec{0}\}. \quad (14)$$

A non-degenerate LRS whose signs are the same as some sequence that can be written like v_n above is what we call **strongly non-degenerate**. We summarise the the properties of subsequences $\langle u_{nP+\ell} \rangle_{n \in \mathbb{N}}$.

Lemma 3.4. *For any ℓ , $0 \leq \ell < P$, the following statements are true for the sequence $\langle u_{nP+\ell} \rangle_{n \in \mathbb{N}}$ that is not identically zero:*

1. *is non-degenerate,*
2. *has finitely many zeros,*
3. *its entries have the same sign as the entries of $\langle v_n \rangle_{n \in \mathbb{N}}$ defined in (12),*
4. *the description of the algebraic numbers c_i , α_i , and $q_{i,j}$ are of polynomial size, have polynomial many variables, and can be computed in PSPACE,*
5. *when the order of the sequence is fixed, the descriptions of the numbers above are of polynomial size, with a constant number of variables, and can be computed in PTIME.*

Proof. Property 1 comes from the fact that P_1 divides P and Theorem 3.2. Any non-degenerate sequence that is not identically zero has finitely many zeros [EVDPS⁺03, Section 2.1], hence Property 2. The third property holds because we have obtained the sequence $\langle v_n \rangle_{n \in \mathbb{N}}$ by dividing with positive numbers.

To see that Property 4 holds for the roots α_i , first observe that P can be computed in PSPACE, as a consequence of Lemma 3.3, and the discussion in Section 3.1. Then applying Proposition 3.1 gives the wanted conclusion. A similar argument holds for the constants c_i . As for the rationals $q_{i,j}$, a combination of two facts is used. First, note that in the proof of Lemma 3.3 the basis (7) is being computed in PSPACE. Second, in the procedure that computes these rationals, described above, we do at most v^2 many replacements where $v \leq m$ is the size of the basis. Each such replacement can be done in PTIME.

One can do a similar analysis for the case where the order of the sequence is fixed, resulting in Property 5. \square

4 The Density 1 Problem

In this section we prove that it is decidable whether the density of a given sequence is equal to 0. The procedure expects a strongly non-degenerate sequence as input, *i.e.* a sequence of the form in (12) with the properties that are listed in Lemma 3.4. Suppose that we are given such a sequence and let δ be its density.

Note that the density of the *negativity* set of the sequence (which is the same as the density of $\langle -v_n \rangle_{n \in \mathbb{N}}$) is equal to $1 - \delta$, because the zeros $\langle v_n \rangle_{n \in \mathbb{N}}$ do not affect the density, being finitely many; a consequence of Property 2 in Lemma 3.4. Hence the density of the sequence $\langle v_n \rangle_{n \in \mathbb{N}}$ is 0 if and only if the density of $\langle -v_n \rangle_{n \in \mathbb{N}}$ is 1. Thus the two problems, “is the density 1?” and “is the density 0?” are inter-reducible.

The argument for decidability of the density 0 problem is as follows. We define two open and measurable sets \mathcal{P} and \mathcal{Q} such that

$$\mathcal{P} = \emptyset \quad \Longleftrightarrow \quad \mathcal{Q} = \emptyset, \quad (15)$$

and furthermore

$$\mathcal{Q} \text{ is semialgebraic} \quad \text{and} \quad \delta = \mu(\mathcal{P}), \quad (16)$$

where μ denotes the Lebesgue measure. Being open sets, it follows that $\delta > 0$ if and only if the semialgebraic set \mathcal{Q} is nonempty, which can be decided, in particular because of Theorem 2.3. In this way decidability of the density 1 problem, *i.e.* Theorem 1.3, will follow from (15) and (16), as well as the reduction from the density 1 to the density 0 problem.

We proceed with the definitions of the sets \mathcal{P} and \mathcal{Q} . Let \mathbb{T} be the unit circle, *i.e.* the set of complex numbers $z \in \mathbb{C}$, for which $|z| = 1$. Define the auxiliary functions F and G which are $v_n - R(n)$ but the roots α_i are replaced by variables; more precisely F is a map from $[0, 1]^\eta$ to the reals, and G a map from \mathbb{T}^η to the reals, defined as:

$$\begin{aligned} F(\vec{\varphi}) &\stackrel{\text{def}}{=} \sum_{i=1}^{\eta} c_i \exp(2\pi i \varphi_i) + \sum_{i=\eta+1}^{m-1} c_i \exp\left(2\pi i \sum_{j=1}^{\eta} q_{i,j} \varphi_j\right) + c_m, \\ G(\vec{z}) &\stackrel{\text{def}}{=} \sum_{i=1}^{\eta} c_i z_i + \sum_{i=\eta+1}^{m-1} c_i \prod_{j=1}^{\eta} z_i^{q_{i,j}} + c_m. \end{aligned}$$

Now the sets \mathcal{P} and \mathcal{Q} are defined as:

$$\begin{aligned} \mathcal{P} &\stackrel{\text{def}}{=} \{\vec{\varphi} \in [0, 1]^\eta : F(\vec{\varphi}) > 0\}, \\ \mathcal{Q} &\stackrel{\text{def}}{=} \{\vec{z} \in \mathbb{T}^\eta : G(\vec{z}) > 0\}. \end{aligned}$$

As one can obtain \mathcal{P} by applying $\log z/2\pi i$ component-wise to elements of \mathcal{Q} , it is plain that \mathcal{P} is non-empty if and only if \mathcal{Q} is non-empty. Since \mathcal{P} is open, it has non-zero measure if and only if it is non-empty. Furthermore, \mathcal{Q} is semialgebraic, thus it only remains to show that $\delta = \mu(\mathcal{P})$.

The proof follows closely the proof of the main theorem of [BG07], and is crucially based on the following theorem of Cassels.

Theorem 4.1 ([Cas59, Theorem 1, page 64]). *Let $\theta_1, \dots, \theta_k, 1 \in \mathbb{R}$ be linearly independent over \mathbb{Q} , and $S \subseteq [0, 1]^k$ a measurable set, then*

$$D(\{n : (n\theta_1 \bmod 1, \dots, n\theta_k \bmod 1) \in S\}) = \mu(S).$$

It says that the fractional parts of $n\vec{\theta}$ fall in the set S with frequency that is equal to the measure of the set S , in other words they are uniformly distributed in the k -dimensional cube.

For $i \in \{1, \dots, \eta\}$, define the arguments of the roots:

$$\theta_i \stackrel{\text{def}}{=} \frac{\log \alpha_i}{2\pi i} \in [0, 1].$$

Since there are no multiplicative relations among the $\alpha_1, \dots, \alpha_\eta$, from (14), we have that $\theta_1, \dots, \theta_\eta, 1$ are linearly independent over \mathbb{Q} . To see this, write $\alpha_i = \exp(2\pi i \theta_i)$ and observe that there are no multiplicative relations among the α_i if and only if there is no linear combination over \mathbb{Q} of θ_i that is equal to an integer. As a consequence, we note that Theorem 4.1 is applicable to the tuple $\theta_1, \dots, \theta_\eta$.

The proof of $\delta = \mu(\mathcal{P})$ is preceded by two lemmas. The first one says that the set of points that F maps to 0 has measure 0.

Lemma 4.2. $\mu(\{\vec{\varphi} : F(\vec{\varphi}) = 0\}) = 0$.

Proof. Since any generalised power sum is a LRS over $\overline{\mathbb{Q}}$ [EVDPS⁺03, Section 1.1.6], the sequence

$$\langle F(n\vec{\theta}) \rangle_{n \in \mathbb{N}} = \langle v_n - R(n) \rangle_{n \in \mathbb{N}}$$

is a non-degenerate LRS. As a corollary of the Skolem-Mahler-Lech theorem [EVDPS⁺03, Section 2.1], this sequence has finitely many zeros, so

$$\mathcal{D}(\{n : F(n\vec{\theta}) = 0\}) = 0.$$

As noted above, we can apply Theorem 4.1 to $\vec{\theta}$, which implies

$$\mathcal{D}(\{n : F(n\vec{\theta}) = 0\}) = \mu(\{\vec{\varphi} : F(\vec{\varphi}) = 0\}),$$

where the set on the right hand side is clearly measurable. Combining these two equations yields the statement of the lemma. \square

The second lemma says that the indices in which the residue $R(n)$ is larger in absolute value than the dominating terms of the sequence, have upper density 0. This means that it is only the dominant part that plays any role on the density δ . Denote by $\hat{\mathcal{D}}$ the upper density (same as density except that the limit is replaced by \limsup): for all $S \subset \mathbb{N}$,

$$\hat{\mathcal{D}}(S) \stackrel{\text{def}}{=} \limsup_{n \rightarrow \infty} \frac{|\{1, 2, \dots, n\} \cap S|}{n}.$$

Lemma 4.3. $\hat{D}(\{n : |F(n\vec{\theta})| < |R(n)|\}) = 0$.

Proof. For $\epsilon > 0$, define:

$$\begin{aligned}\mathcal{P}_\epsilon &\stackrel{\text{def}}{=} \{\vec{\varphi} \in [0, 1]^\eta : |F(\vec{\varphi})| \leq \epsilon\}, \\ \mathcal{R}_\epsilon &\stackrel{\text{def}}{=} \{n \in \mathbb{N} : |F(n\vec{\theta})| \leq \epsilon\}.\end{aligned}$$

The residue $|R(n)|$ tends to zero as n gets larger (13), hence for all $\epsilon > 0$,

$$\hat{D}(\{n : |F(n\vec{\theta})| < |R(n)|\}) \leq D(\mathcal{R}_\epsilon). \quad (17)$$

The set \mathcal{R}_ϵ has density as a consequence of Theorem 4.1, also

$$D(\mathcal{R}_\epsilon) = \mu(\mathcal{P}_\epsilon) = \int_{[0,1]^\eta} \mathbb{1}_{\mathcal{P}_\epsilon} d\mu,$$

where by $\mathbb{1}_{\mathcal{P}_\epsilon}$ we have denoted the indicator function of the set \mathcal{P}_ϵ . Almost everywhere the function $\mathbb{1}_{\mathcal{P}_\epsilon}$ tends to $\mathbb{1}_{\mathcal{P}_0}$ as $\epsilon \rightarrow 0$, hence by Lebesgue's dominated convergence theorem [Bil08, Theorem 16.4] we have

$$\int_{[0,1]^\eta} \mathbb{1}_{\mathcal{P}_\epsilon} d\mu \rightarrow \int_{[0,1]^\eta} \mathbb{1}_{\mathcal{P}_0} d\mu = 0,$$

where the equality to zero comes from Lemma 4.2. Since (17) holds for all $\epsilon > 0$, the statement of the lemma follows. \square

A consequence of Lemma 4.3 is that,

$$\delta = D(\{n : v_n > 0\}) = D(\{n : F(n\vec{\theta}) > 0\}).$$

The density on the right hand side is equal to $\mu(\mathcal{P})$ by again applying Theorem 4.1.

Thus we have proved Theorem 1.3, that it is possible to decide whether the density is equal to 0 (or to 1). The complexity of the procedure is in PSPACE: the formula for non-emptiness of \mathcal{Q} is of polynomial size due to Property 4 of Lemma 3.4, and hence whether it is true can be decided in PSPACE, Theorem 2.3.

The procedure runs in PTIME if the order of the sequence is fixed. This follows from Property 5 of Lemma 3.4 and Theorem 2.3.

4.1 The Case of Diagonalisable Sequences

If the given LRS has only finitely many positive entries then the density of the sequence is 0. The converse, however, does not always hold, as it can be seen from the following example:

Example 4.4. One can construct an LRS $\langle w_n \rangle_{n \in \mathbb{N}}$ that is equal to

$$w_n \stackrel{\text{def}}{=} \frac{n}{2} \lambda^n + \frac{n}{2} \bar{\lambda}^n + (1 - n),$$

where $\lambda \in \mathbb{T}$ is some algebraic number in the unit circle, that is not a root of unity. Let $\theta = \log \lambda / 2\pi i$. Then, by writing $\lambda^n = \cos(2\pi n\theta) + i \sin(2\pi n\theta)$, we see that

$$w_n > 0 \quad \Longleftrightarrow \quad \cos(2\pi n\theta) > 1 - \frac{1}{n}.$$

The sequence $\langle w_n \rangle_{n \in \mathbb{N}}$ has infinitely many positive entries [AKK⁺21, Proposition 4.1], however it has density 0. Indeed if it had density $\delta > 0$, then we could have chosen some n large enough such that the interval of φ for which $\cos(2\pi i \varphi) > 1 - 1/n$, is smaller than δ , at which point, by applying Theorem 4.1 one can derive a contradiction. The Cassels' theorem is applicable because λ is not a root of unity, which means that θ is irrational, by definition.

The direction “density 0” implies “positivity set is finite”, does however hold for an important class of LRS, namely the diagonalisable sequences. These are sequences $\langle t_n \rangle_{n \in \mathbb{N}}$ whose characteristic polynomial has no repeated roots, as a consequence of which, its generalised power sum is of the following form:

$$t_n \stackrel{\text{def}}{=} \sum_{i=1}^k a_i \Lambda_i^n,$$

where a_i are some algebraic constants and Λ_i are the roots.

Theorem 1.4. *In a diagonalisable sequence the positivity set is finite if and only if its density is zero.*

Proof. We prove the contrapositive, i.e. we show that if $\langle t_n \rangle_{n \in \mathbb{N}}$ has infinitely many positive entries then it also has positive density. Assume that the roots are ordered by modulus, i.e. $|\Lambda_i| \geq |\Lambda_{i+1}|$, and assume that the first j roots have maximal modulus. Write

$$t_n = \underbrace{\sum_{i=1}^j a_i \Lambda_i^n}_{D(n)} + \underbrace{\sum_{i=j+1}^k a_i \Lambda_i^n}_{r(n)}.$$

Suppose that $|\Lambda_1| > 1$, indeed if it is not, we can always multiply the sequence with $\langle K^n \rangle_{n \in \mathbb{N}}$ for $K \in \mathbb{N}$ large enough, without changing the sign.

The proof hinges on a lower bound on the growth of LRS that was proved Evertse, and in parallel by van der Poorten and Schlickewei, using the subspace theorem. See the discussion in [EVDPS⁺03, Section 2.4] as well as the appendix of [FH20]. Applying this theorem to our case, we have that for all $\epsilon > 0$ there exists some threshold $n_0 \in \mathbb{N}$ such that:

$$|D(n)| \geq |\Lambda_1|^{(1-\epsilon)n} \text{ for all } n \geq n_0.$$

Since $|r(n)|$ can be upper bounded by some $c|\Lambda|^n$, with $c \in \mathbb{R}$ a constant, and $|\Lambda| < |\Lambda_1|$, it follows that we can pick some $\epsilon > 0$ for which we know that there exists some $n_0 \in \mathbb{N}$ such that:

$$|D(n)| > |r(n)| \text{ for all } n \geq n_0.$$

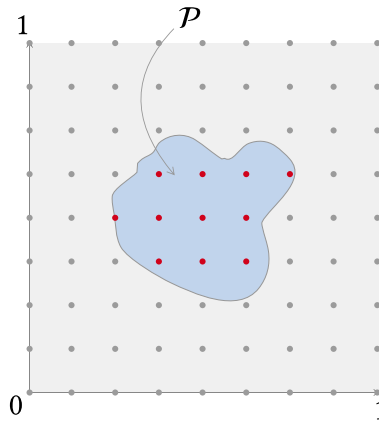
This is a stronger version of Lemma 4.3, signifying that asymptotically the sign depends only on that of the dominant terms⁶. As a consequence of the inequality above, since the sequence $\langle t_n \rangle_{n \in \mathbb{N}}$ has infinitely many positive terms, so does the sequence $\langle D(n) \rangle_{n \in \mathbb{N}}$.

We sketch the rest of the proof. As in Section 3 we can define the multiplicative relations among $\Lambda_1, \dots, \Lambda_j$, and define a set \mathcal{P}' analogous to the set \mathcal{P} , defined in the previous page. One can then prove that the set \mathcal{P}' is open and furthermore it is non-empty as a consequence of the fact that $\langle D(n) \rangle_{n \in \mathbb{N}}$ has infinitely many positive entries. Non-emptiness implies that \mathcal{P}' has non-zero measure, and finally, by applying Theorem 4.1, one concludes that the density of the sequence is positive. \square

The algorithm that we have presented in this section is not the same, but it is quite similar to the algorithm of [OW14] for deciding ultimate positivity for diagonalisable sequences. We have shown that this algorithm can be used for deciding a different problem, namely whether the density of the sequence is zero, and that when the sequence is diagonalisable, the density 0 question is equivalent to the question of whether the sequence has only finitely many positive entries. The complexity lower bound of [OW14, Section 5] applies to our case as well.

5 Computing the Density

One method of approximating the density δ , which is the same as approximating the volume $\mu(\mathcal{P})$ of the set \mathcal{P} is conceptually simple: draw a grid and count the points that belong to \mathcal{P} . We summarise this in the picture below.



⁶This inequality holds for general LRS. The difference is that for diagonalisable LRS, the dominant part $D(n)$ is easier to analyse.

From the grid of M^η points (in the example 9^2 points), we count how many are in \mathcal{P} , and denote this number by $C(M)$ (in the example this is equal to 11 red points). Since \mathcal{P} is a measurable subset of the unit cube,

$$\frac{C(M)}{M^\eta} \rightarrow \mu(\mathcal{P}),$$

as M tends to infinity.

For this scheme to work, we need to be able to do two things. First, for any rational $\vec{q} \in [0, 1]^\eta$, to be able to decide whether $\vec{q} \in \mathcal{P}$. And second, to upper bound

$$\left| \frac{C(M)}{M^\eta} - \mu(\mathcal{P}) \right|, \quad (18)$$

by a function in M . We prove that both are feasible.

Lemma 5.1. *Given any rational $\vec{q} \in [0, 1]^\eta$, it is decidable whether $\vec{q} \in \mathcal{P}$.*

Proof. Let $0 \leq k/n \leq 1$ be a rational number. The complex number $\exp(2\pi i/n)$ is a primitive n -th root of unity, which we can isolate as a root of $x^n - 1$. It follows that $\exp(2\pi i k/n) = \exp(2\pi i/n)^k$ is an algebraic number that we can easily define. Consequently the assertion $\vec{q} \in \mathcal{P}$, which is equivalent to $F(\vec{q}) > 0$, is a first-order formula whose truthiness can be decided by Tarski's algorithm, Theorem 2.3. \square

For an upper bound on the error (18), we use the work of Koiran [Koi95, Theorem 3]. To introduce his theorem we need to define the parameter $\kappa(\mathcal{P})$ first, and estimate it.

Let $S \subseteq [0, 1]^\eta$ be a measurable set, define $\kappa(S)$ to be the maximal number of connected components of the intersection $L \cap S$ where L is an axis-parallel line. In other words, draw a line parallel to any one of the axes, and count how many times it goes in and out of the set. To estimate $\kappa(\mathcal{P})$, in our case, this translates to fixing all but one parameter of function F and counting how many times it will change its sign. More precisely, consider the function that we get by fixing all but one parameter of F , it will be of the form:

$$H(\varphi) \stackrel{\text{def}}{=} z_0 \exp(2\pi i \varphi) + \sum_{i=1}^{\ell} z_i \exp(2\pi i r_i \varphi) + c,$$

defined for $\varphi \in [0, 1]$, where $\ell \leq m$, c, z_i are some algebraic numbers, and r_i are taken among the $q_{i,j}$, $\eta < i < m$, $1 \leq j \leq \eta$. The nature of the constants is such that H is a real-valued function. How many times does H change its sign in its domain $[0, 1]$? By continuity, the answer is upper bounded by the number of zeros of H , which we will estimate. To this end, let $r_i = a_i/b_i$, and define

$$b \stackrel{\text{def}}{=} \text{lcm}\{b_1, \dots, b_\ell\}.$$

Set $a'_i \in \mathbb{N}$ to be such that $r_i = a'_i/b$.

Lemma 5.2. *The function H has at most*

$$\hat{q} \stackrel{\text{def}}{=} \max\{b, a'_1, \dots, a'_\ell\}$$

zeros in the unit interval $[0, 1]$.

Proof. We can write H as

$$z_0 (\exp(2\pi i \varphi/b))^b + \sum_{i=1}^{\ell} z_i (\exp(2\pi i \varphi/b))^{a'_i} + c,$$

which is a polynomial of degree at most \hat{q} , and hence can have at most that many zeros. \square

Having estimated thus the parameter $\kappa(\mathcal{P})$, we have the following upper bound on the error:

Theorem 5.3 ([Koi95, Theorem 3]). *For all $M \in \mathbb{N}$,*

$$\left| \frac{C(M)}{M^\eta} - \mu(\mathcal{P}) \right| \leq \frac{\eta \kappa(\mathcal{P})}{M} \leq \frac{\eta \hat{q}}{M}.$$

Now Theorem 1.5 follows from Lemma 5.1 and Theorem 5.3. Indeed if we want to compute the density δ up to precision ϵ , it suffices to choose $M \geq \eta \hat{q}/\epsilon$, then for every member of

$$\left\{ \left(\frac{k_1}{M}, \dots, \frac{k_\eta}{M} \right) : 0 \leq k_i \leq M, 1 \leq i \leq \eta \right\}, \quad (19)$$

test whether it is in \mathcal{P} , and in this way compute the quantity $C(M)/M^\eta$ which by the proposition above is guaranteed to differ from the density by no more than ϵ .

Even though M is exponential in the input, by using the repeated squaring way of expressing the exponents in the formulas, as in Section 3, it is possible to construct formulas of polynomial size for testing whether points of the grid (19) belong to \mathcal{P} . In particular to define $\exp(2\pi i/M)$, the formula says that it is a root of $x^M - 1$ (which is of polynomial size), and that both the real and imaginary parts are positive and minimal. It follows that the algorithm for approximating the density is making exponentially many calls to a PSPACE algorithm (due to Theorem 2.3), each of which is used to decide whether to increment a counter that is upper bounded by M^η . Hence this algorithm is running in PSPACE on $\lceil \epsilon^{-1} \rceil$ and N , the bitlength of the description of the sequence. A similar analysis yields a PTIME upper bound in N and $\lceil \epsilon^{-1} \rceil$ when the order of the sequence is fixed.

Instead of testing whether *every* point in the grid belongs to \mathcal{P} , intuitively, we could test it for a smaller number $M' < M$, but choose the points uniformly at random. This is the Monte-Carlo integration method [Koi95]. It results in a number of points in the set $C'(M')$ for which it is known that for all $\epsilon > 0$,

$$\frac{1}{M^\eta} |C'(M') - C(M)| \leq \epsilon$$

holds with probability at least $1 - 2e^{-2M'\epsilon^2}$. This can be demonstrated using Hoeffding's inequality.

6 When is the Density a Rational Number?

We have proved that it is possible to decide whether the density of a given sequence is equal to 0, or to 1. Can we also decide whether the density is larger than some $q \in \mathbb{Q}$? The approximating scheme of the previous section is *a priori* of no help: since it might be the case that it outputs the estimates $\delta_1, \delta_2, \dots$, for error bounds $\epsilon_1 > \epsilon_2 > \dots$ such that q belongs to all intervals $(\delta_i - \epsilon_i, \delta_i + \epsilon_i)$. A natural approach to tackling this difficulty is to ask whether the density itself is an irrational number. If the density is irrational then it has some ϵ -neighbourhood which does not contain q , which means that for a sufficiently small ϵ_i , q does not belong in the interval $(\delta_i - \epsilon_i, \delta_i + \epsilon_i)$.

In this section we report some progress of this direction. We begin by showing that when there are no non-trivial multiplicative relations among the roots, density is a *period* as defined by Kontsevich and Zagier [KZ01], *i.e.* an integral of an algebraic function over a semialgebraic set. Afterwards, we prove that when there is at most one pair of dominant complex roots, it is decidable whether the density is rational, in which case we can compute it exactly.

6.1 Density as a Period

The complex roots of a sequence $u_n = \sum f_i(n) \Lambda_i^n$ come in conjugate pairs. Furthermore if $\Lambda_j = \overline{\Lambda_i}$ then also $f_j(n) = \overline{f_i(n)}$. See [HHHK05, Proposition 2.13] for a proof. The multiplicative relations due to complex conjugacy, *i.e.* $\lambda_j \lambda_i = 1$, where $\lambda_i = \Lambda_i / |\Lambda_i|$ is the normalised root, we call **trivial relations**. Here we study sequences that do not have any non-trivial multiplicative relations among the roots. Under this restriction, the function F , defined in Section 4, has the following form:

$$F(\vec{\varphi}) = \sum_{i=1}^{\eta} c_i \exp(2\pi i \varphi_i) + \sum_{i=1}^{\eta} \overline{c_i} \exp(-2\pi i \varphi_i) + c_m,$$

since the only dependent roots are the complex conjugates of the independent ones. Using Euler's formula, and a trigonometric identity, we see that this function can also be written as:

$$F(\vec{\varphi}) = c + \sum_{i=1}^{\eta} r_i \cos(2\pi(\varphi_i + \tau_i)),$$

where $c = c_m \in \mathbb{R}$, $r_i = |c_i|$, and τ_i is the argument of c_i .

We proceed by getting rid of the translation by τ_i . Define:

$$F'(\vec{\varphi}) \stackrel{\text{def}}{=} F(\vec{\varphi} - \vec{\tau}).$$

Recall that \mathcal{P} was defined as the set of $\vec{\varphi}$ for which $F(\vec{\varphi}) > 0$, and observe that

$$\mathcal{P}' \stackrel{\text{def}}{=} \{ \vec{\varphi} : F'(\vec{\varphi}) > 0 \} = \mathcal{P} + \vec{\tau}.$$

Since \mathcal{P}' is obtained from \mathcal{P} by a translation, they have the same measure. Furthermore, as a consequence of symmetry of cosine we have:

$$\mu(\mathcal{P}') = 2^\eta \mu(\underbrace{\mathcal{P}' \cap [0, 1/2]^\eta}_{\hat{\mathcal{P}}}).$$

So the density of the sequence can be derived from the volume of $\hat{\mathcal{P}}$. We write the latter as a certain integral. To this end, define the set \mathcal{L} as,

$$\mathcal{L} \stackrel{\text{def}}{=} \left\{ \vec{x} \in [-1, 1]^\eta : c + \sum_{i=1}^{\eta} r_i x_i > 0 \right\}.$$

Observe that the function $\cos^{-1}(\vec{x})/2\pi$, denoted $g(\vec{x})$, is a continuously differentiable bijection from $[-1, 1]^\eta$ to $[0, 1/2]^\eta$, and that furthermore:

$$g(\mathcal{L}) = \hat{\mathcal{P}}.$$

Denote by g' the Jacobian of g , then a variable change (see [Spi18, Theorem 3-13]) leads to:

$$\mu(\hat{\mathcal{P}}) = \int_{g(\mathcal{L})} d\vec{\varphi} = \int_{\mathcal{L}} |\det g'| d\vec{x} = \frac{1}{(2\pi)^\eta} \int_{\mathcal{L}} \prod_{i=1}^{\eta} \frac{1}{\sqrt{1-x_i^2}} d\vec{x}.$$

From here it follows that $\mu(\mathcal{P})$ is rational if and only if

$$\int_{\mathcal{L}} \prod_{i=1}^{\eta} \frac{1}{\sqrt{1-x_i^2}} d\vec{x} \in \mathbb{Q} \pi^\eta. \quad (20)$$

The class of numbers that can be expressed as integrals of algebraic functions over semialgebraic sets are known as **periods** [KZ01]. They contain all algebraic numbers, as well as their logarithms, and some transcendental numbers like π ; they are exceedingly commonplace however not well understood.

We do not know how to decide (20), but we point out to some work that might prove to be helpful. One is Conjecture 1 in [KZ01], that says that if one period has two different representations as integrals, one can obtain one from the other through three simple operations: additivity, change of variables and Stoke's formula. It is not clear however, even if the conjecture were to be true, how one can calculate a sequence of such operations. A more direct conjecture is one made by Grothendieck that predicts the transcendence degree of a finite set of periods. See [Ayo14] for definitions and a discussion about these two conjectures. More seems to be known about the special case of curves [HW18], but in this case, for our purposes, we can give a more satisfactory answer by simpler means.

6.2 One Pair of Dominant Complex Roots

When there is at most one pair of dominant complex roots, we have $\eta = 1$ and the function F can be written as:

$$F(\varphi) = c + r \cos(2\pi(\varphi + \tau)).$$

Clearly when $|c| \geq |r|$ the density is either 1 or 0 depending on the sign of c , so assume that $|c| < |r|$. As we explained above, we can do away with the translation by τ when solely interested in density, and furthermore we can restrict φ to the interval $[0, 1/2]$.

Since the sequence is non-degenerate, the ratio $\lambda/\bar{\lambda}$ is not a root of unity, which implies that φ is not a rational number. In this case Cassel's theorem (Theorem 4.1) is applicable. As a consequence of that theorem, to calculate the density, it suffices to calculate the length of the interval in $[0, 1/2]$ which includes all φ for which:

$$\cos(2\pi\varphi) > \frac{-c}{r}.$$

Depending on the sign of $-c/r$, the length of this interval is

$$\text{either } \frac{\cos^{-1}(-c/r)}{2\pi} \quad \text{or} \quad 1 - \frac{\cos^{-1}(-c/r)}{2\pi},$$

in both cases it is rational if and only if $\cos^{-1}(-c/r)$ is a rational multiple of π . In the remainder of this section we prove that we can decide whether the inverse cosine of a real algebraic number is a rational multiple of π .

Proposition 6.1. *Given a real algebraic number $\alpha \in [-1, 1]$ of degree d , it is decidable whether*

$$\cos^{-1}(\alpha) \in \mathbb{Q}\pi.$$

Proof. Clearly $\cos^{-1}(\alpha)$ is a rational multiple of π if and only if there is a rational $a/b \in \mathbb{Q}$, $b > 0$, such that $a \cos^{-1}(\alpha) = b\pi$. Which, in turn, holds if and only if there exists $a/b \in \mathbb{Q}$ (possibly different), $b > 0$, such that:

$$\cos(a \cos^{-1}(\alpha)) = (-1)^b.$$

To proceed we need the definition of the **Chebyshev polynomials of the first kind** of order n . These are univariate polynomials T_n , for $n \in \mathbb{N}$ that are characterised by the equation:

$$T_n(\cos \theta) \stackrel{\text{def}}{=} \cos(n\theta).$$

One can also define them via a recurrence relation. We see that:

$$T_a(\alpha) = T_a(\cos \cos^{-1}(\alpha)) = \cos(n \cos^{-1}(\alpha)) = (-1)^b.$$

As a consequence $\cos^{-1}(\alpha)$ is a rational multiple of π if and only if there is some $n \in \mathbb{N}$, such that α is a root of

$$T_n(x) - 1 \quad \text{or} \quad T_n(x) + 1.$$

The roots of these polynomials are straightforward to describe:

Observation 6.1. Let $n \in \mathbb{N}$. All the roots of $T_n(x) + 1$ and of $T_n(x) - 1$ come from the set

$$\left\{ \pm \cos(k\pi/n) : 0 \leq k \leq n \right\}.$$

The proof of this observation follows plainly from the fact that for all $x \in \mathbb{R}$ such that $|x| \leq 1$, we have

$$T_n(x) = T_n(\cos \cos^{-1} x) = \cos(n \cos^{-1} x)$$

and the fact that we can write $-\cos(k\pi/n)$ as $\cos(k\pi/n + \pi)$.

From Observation 6.1 and the discussion preceding it we conclude that $\cos^{-1}(\alpha)$ is a rational multiple of π if and only if it is equal to $\pm \cos(k\pi/n)$ for some $k, n \in \mathbb{N}$, $k \leq n$. The numbers $\pm \cos(k\pi/n)$ are algebraic, indeed they satisfy the Chebyshev polynomial of order n , furthermore if $\gcd(k, n) = 1$ then $\cos(2k\pi/n)$ is an algebraic integer of degree $\Phi(n)/2$ [Leh33, Theorem 1], where Φ is the Euler's totient function.

Now, since α has degree d , we take some $N \in \mathbb{N}$ such that $\Phi(N) \geq 2d$. By testing (with the algorithms from Theorem 2.3 say) whether α is a root of any $T_n(x) \pm 1$, for $n \leq N$ we can decide whether $\cos^{-1}(\alpha)$ is a rational multiple of π . \square

Acknowledgement

I am grateful to James Worrell for the many helpful discussions.

References

- [AKK⁺21] Shaull Almagor, Toghrul Karimov, Edon Kelmendi, Joël Ouaknine, and James Worrell. Deciding ω -regular properties on linear recurrence sequences. *Proceedings of the ACM on Programming Languages*, 5(POPL):1–24, 2021.
- [Ayo14] Joseph Ayoub. Periods and the conjectures of grothendieck and kontsevich-zagier. *European Mathematical Society. Newsletter*, (91):12–18, 2014.
- [BG07] Jason P Bell and Stefan Gerhold. On the positivity set of a linear recurrence sequence. *Israel Journal of Mathematics*, 157(1):333–345, 2007.
- [Bil08] Patrick Billingsley. *Probability and measure*. John Wiley & Sons, 2008.
- [BM76] Jean Berstel and Maurice Mignotte. Deux propriétés décidables des suites récurrentes linéaires. *Bulletin de la Societe mathematique de France*, 79:175–184, 1976.
- [BP02] Vincent D. Blondel and Natacha Portier. The presence of a zero in an integer linear recurrent sequence is np-hard to decide. *Linear Algebra and its Applications*, 351-352:91–98, 2002.

- [BPR06] Saugata Basu, Richard Pollack, and Marie-Francois Roy. *Real Roots*, pages 351–401. Algorithms in Real Algebraic Geometry. Springer Berlin Heidelberg, 2006.
- [Can88] John Canny. Some algebraic and geometric computations in pspace. *Proceedings of the twentieth annual ACM symposium on Theory of computing - STOC '88*, 1988.
- [Cas59] J. W. S. Cassels. *An Introduction To Diophantine Approximation*. Cambridge University Press, 1959.
- [EVDPS⁺03] Graham Everest, Alfred Jacobus Van Der Poorten, Igor Shparlinski, Thomas Ward, et al. *Recurrence sequences*, volume 104. American Mathematical Society Providence, RI, 2003.
- [FH20] Clemens Fuchs and Sebastian Heintze. On the growth of linear recurrences in function fields. *CoRR*, 2020.
- [Han85] Georges Hansel. A simple proof of the skolem-mahler-lech theorem. In *International Colloquium on Automata, Languages, and Programming*, pages 244–249. Springer, 1985.
- [HHHK05] Vesa Halava, Tero Harju, Mika Hirvensalo, and Juhani Karhumäki. Skolem’s problem—on the border between decidability and undecidability. Technical report, Citeseer, 2005.
- [HW18] Annette Huber and Gisbert Wüstholz. Transcendence and linear relations of 1-periods. *arXiv preprint arXiv:1805.10104*, 2018.
- [Koi95] Pascal Koiran. Approximating the volume of definable sets. In *Proceedings of IEEE 36th Annual Foundations of Computer Science*, pages 134–141. IEEE, 1995.
- [KZ01] Maxim Kontsevich and Don Zagier. *Periods*, pages 771–808. Mathematics Unlimited - 2001 and Beyond. Springer Berlin Heidelberg, 2001.
- [Lan02] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2002.
- [Lec53] Christer Lech. A note on recurring series. *Arkiv för Matematik*, 2(5):417–421, 1953.
- [Leh33] Derrick H Lehmer. A note on trigonometric algebraic numbers. *Amer. Math. Monthly*, 40(3):165–166, 1933.
- [Mah35] Kurt Mahler. *Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen*. Noord-Hollandsche Uitgevers Mij, 1935.
- [OW13] Joël Ouaknine and James Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, 12 2013.
- [OW14] Joël Ouaknine and James Worrell. *Ultimate Positivity is Decidable for Simple Linear Recurrence Sequences*, pages 330–341. Automata, Languages, and Programming. Springer Science + Business Media, 2014.

- [Ren92] James Renegar. On the computational complexity and geometry of the first-order theory of the reals. part i: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of symbolic computation*, 13(3):255–299, 1992.
- [Sko34] Thoralf Skolem. Ein verfahren zur behandlung gewisser exponentialer gleichungen und diophantischer gleichungen. *C. r.*, 8:163–188, 1934.
- [Spi18] Michael Spivak. *Calculus On Manifolds*. CRC Press, 2018.
- [Tar51] Alfred Tarski. *A decision method for elementary algebra and geometry*. University of California Press, 1951.
- [TMS84] R. Tijdeman, M. Mignotte, and T.N. Shorey. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1984(349):63–76, 1984.
- [vdPL77] A.J. van der Poorten and J.H. Loxton. Multiplicative relations in number fields. *Bulletin of the Australian Mathematical Society*, 16(1):83–98, 1977.
- [Ver85] N. K. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical notes of the Academy of Sciences of the USSR*, 38(2):609–615, 1985.
- [Wal00] Michel Waldschmidt. *Diophantine Approximation on Linear Algebraic Groups*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2000.
- [YLN95] Kazuhiro Yokoyama, Ziming Li, and István Nemes. Finding roots of unity among quotients of the roots of an integral polynomial. In *Proceedings of the 1995 international symposium on Symbolic and algebraic computation - ISSAC '95*, - 1995.
- [YS11] Chee K. Yap and Michael Sagraloff. A simple but exact and efficient algorithm for complex root isolation. In *Proceedings of the 36th international symposium on Symbolic and algebraic computation - ISSAC '11*, - 2011.