H A B I L I T A T I O N S S C H R I F T

Subsequences of digitally defined functions

Teilfolgen ziffernbasierter Funktionen

ausgeführt zum Zwecke der Erlangung der *venia docendi* für das Fach Mathematik

eingereicht an der Technischen Universität Wien,
Fakultät für Mathematik und Geoinformation

von

Lukas SPIEGELHOFER

Abstract

The present postdoctoral thesis deals with *digitally defined functions*. Such a function is defined via some *digital expansion*, such as the ubiquitous base-ten expansion, or more general, the base-q expansion. Our goal is to better understand functions of this kind, from a combinatorial, number theoretic, as well as from an analytical point of view.

The so-called *sum-of-digits function* s_q in base $q \geq 2$ will be our primary source of difficult problems. The number $\mathsf{s}_q(n)$, for a natural number n, is just the sum of all base-q *digits* of n (which are integers and can be summed up). This quantity is also the minimal number of powers of q needed to represent n as their sum:

$$\mathsf{s}_q(n) = \min\bigl\{k \geq 0 : \text{there exist } d_0, \dots, d_{k-1} \in \mathbb{N} \text{ such that } n = q^{d_0} + \cdots + q^{d_{k-1}}\bigr\}.$$

Heuristically, the sum-of-digits function captures much of the complexity connected to digital expansions, and there are numerous elementary questions that can be asked. The difficulty of these questions ranges from trivial to intractable, and we are well advised to choose our research problems from the "middle section".

Contrary to the first impression that problems of this kind might give, there are questions concerning digital expansions that are (a) easy to formulate but (b) non-trivial to answer, (c) non-artificial, and (d) connected to other areas of pure mathematics, such as (harmonic) analysis, Diophantine approximation, multiplicative number theory, the theory of dynamical systems, or multiplicative number theory.

Examples that, in our opinion, satisfy all of these *very vague* criteria, include:

- How is the base-q expansion of a sum $n + t$ of natural numbers related to the base-q expansions of the summands n and t?
- How often does s_q along a finite arithmetic progression attain a given value?
- At which positions n do we have $(-1)^{\mathsf{s}_q(n)} \neq (-1)^{\mathsf{s}_q(n+r)}$? In particular ($q = 2$), we are interested in the *Thue–Morse sequence* $\mathbf{t}(n) \coloneqq \mathsf{s}_2(n) \bmod 2$. Where do the "sign changes" in $\mathbf{t}$, corresponding to $r = 1$, take place?
- Do we have $\mathsf{s}_2(n) = \mathsf{s}_3(n)$ infinitely often?

The four papers we are going to present in this thesis are concerned with these four items, respectively. They give answers, or partial answers, to each of these four questions. Moreover, they embed the research topic "digital expansions" into a broader picture by using methods from various mathematical methods and highlighting further connections such as in (d) above.

Contents

Chapter 1

Introduction

> "Für die Entwicklung der logischen Wissenschaften wird es, ohne Rücksicht auf etwaige Anwendungen, von Bedeutung sein, ausgedehnte Felder für Spekulation über schwierige Probleme zu finden. Wir werden hier in dieser Abhandlung einige Untersuchungen aus einer Theorie über Zeichenreihen, die gewisse Berührungspunkte mit der Zahlentheorie darbietet, mitteilen."
>
> Axel Thue, 1912 [158]

Thue would perhaps have been interested in observing that "Zeichenreihen" — strings of digits — would be of fundamental importance later in the 20^{th} century.

1.1 Included articles

We selected four of our relatively recent articles, three of which are single-authored, and one is joint work with Michael Wallner (TU Wien). The contribution of each of the two authors to that latter article can be estimated to be 50%.

All four papers are published or accepted for publication:

1. "The binary digits of $n + t$", with Michael Wallner,
   Ann. Sc. Norm. Super. Pisa Cl. Sci., to appear;
2. "The level of distribution of the Thue–Morse sequence,
   Compos. Math. 156 (2020), no. 12, 2560–2587;
3. "Gaps in the Thue–Morse word",
   J. Aust. Math. Soc., published online, to appear ;
4. "Collisions of digit sums in bases 2 and 3",
   Israel J. Math., accepted for publication (2022).

The full texts of these articles can be found in Chapters 2–5 below, and are also available on arXiv.

Remark 1. For reasons of brevity, we did not include the manuscript "Primes as sums of Fibonacci numbers" (135 pages), written jointly with M. Drmota and C. Müllner, and recently accepted (2022) for publication in Mem. Amer. Math. Soc.
`https://www.ams.org/cgi-bin/mstrack/accepted_papers/memo`
This preprint is available on arXiv.

Notation. For real x, we write

$$\mathrm{e}(x) \coloneqq \exp(2\pi i x), \qquad \|x\| \coloneqq \min\big\{|x-n| : n \in \mathbb{Z}\big\},$$
$$\lfloor x \rfloor \coloneqq \max\{n \in \mathbb{Z} : n \le x\}, \quad \{x\} \coloneqq x - \lfloor x \rfloor.$$

In our papers, $\mathbb{N}$ denotes the set of nonnegative integers.

1.2 Digital expansions

Digital expansions owe their name to the Latin word *digitus*, meaning finger. Indeed, it is certainly not a coincidence that using the *decimal system* — a positional system of numeration, employing the number ten as base — is quite popular.

More generally, assume that $q \ge 2$ is an integer. Every integer $n \ge 0$ has a unique expansion

$$n = \sum_{j=0}^{\ell-1} \delta_j q^j, \tag{1.2.1}$$

where $\ell \ge 0$ is an integer and $\big(\delta_0, \dots, \delta_{\ell-1}\big) \in \{0, \dots, q-1\}^\ell$, and either $\ell = 0$ or $\delta_{\ell-1} \ne 0$. Due to this uniqueness, we may write $\delta_j(n)$ for the base-q digit of n at index j, and $\ell(n)$ for the quantity ℓ appearing in (1.2.1) — the *length* of the base-q expansion. We also set $\delta_j(n) = 0$ for $j \ge \ell(n)$. Note that the base-q expansion of 0 is the empty string. This expansion has length 0.

The tuple $\big(\delta_0(n), \dots, \delta_{\ell(n)-1}(n)\big) \in \{0, \dots, q-1\}^\ell$ is called the *base-q expansion* of n, and we use the notation

$$n = \big(\delta_{\ell(n)-1}(n) \cdots \delta_0(n)\big)_q.$$

For example, in the aforementioned decimal system, the base q is the number ten, and the set of digits is $\{0,1,2,3,4,5,6,7,8,9\}$.

Based on the base-q expansion, we define the *sum-of-digits function* in base q. Since the digits of a natural number n in base q are natural numbers, we may form their sum, and define

$$\mathsf{s}_q(n) \coloneqq \sum_{j \ge 0} \delta_j(n).$$

In order to encounter the type of problems that we deal with in our papers, we do not need to consider "large bases" such as ten. The case $q = 2$, and problems appearing when combining this case with the next higher base $q = 3$, already provides plenty of research opportunities, and intractable problems, too.

1.3 The binary digits of $n + t$

The first paper we want to discuss is joint work with M. Wallner, and will appear in **Ann. Sc. Norm. Super. Pisa Cl. Sci.** [153]. The accepted version of this paper can be found in **Chapter 2**.

The binary sum-of-digits function s_2 has a somewhat fractal appearance. For example, the $2^{\lambda+1}$-tuple $T_{\lambda+1}$, where $T_\mu \coloneqq \big(\mathsf{s}_2(0), \dots, \mathsf{s}_2\big(2^\mu - 1\big)\big)$, results from concatenating the 2^λ-tuples T_λ and $T_\lambda + 1$, where each value in the latter tuple is obtained from the corresponding entry in the first tuple, by adding 1. The connection to fractal structures becomes even more apparent when studying *divisibility in Pascal's triangle* (see Figure 1.1 below). Assume that p is a prime number. *Legendre's formula* implies that

$$\nu_p(n!) = \frac{n - \mathsf{s}_p(n)}{p-1}, \tag{1.3.1}$$

which relates the p-valuation of $n!$ to the sum-of-digits function in base p. Here of course $\nu_p(m) = \max\{k \geq 0 : p^k \mid m\}$ for integers $m \geq 1$. Using (2.1.2) thrice, we can express the relation $p^j \mid \binom{n+t}{t}$ in the form of the identity

$$(p-1)\,\nu_p\left(\binom{n+t}{t}\right) = \mathsf{s}_p(n) + \mathsf{s}_p(t) - \mathsf{s}_p(n+t). \tag{1.3.2}$$

In particular, we see that $\binom{n+t}{t}$ is odd if and only if

$$\mathsf{s}_2(n+t) = \mathsf{s}_2(n) + \mathsf{s}_2(t). \tag{1.3.3}$$

This property can also be understood using *Lucas' congruence* [98]. This well-known congruence asserts that for $t \leq n$ and $\mu \geq \max\big(\ell(n), \ell(t)\big)$, we have

$$\binom{n}{t} \equiv \binom{\delta_{\mu-1}(n)}{\delta_{\mu-1}(t)} \cdots \binom{\delta_0(n)}{\delta_0(t)} \bmod p.$$

Since p is a prime number, we have $p \nmid \binom{n}{t}$ if and only if none of the factors is divisible by p. This, in turn, is equivalent to

$$\delta_j(t) \leq \delta_j(n) \text{ for all } i < \mu,$$

which we denote by $t \preceq n$ for a moment.

For simplicity, we assume in the following that $p = 2$. In this case, we have $t \preceq n + t$ if and only if the supports of the sequences of digits of n and t are disjoint:

$$\begin{gathered} t \preceq n + t \quad \text{if and only if} \\ \text{for all } j \geq 0 : \big(\delta_j(n), \delta_j(t)\big) \neq \big(1, 1\big). \end{gathered} \tag{1.3.4}$$

The proof of this statement is direct and very easy, and does not involve carries.

It is well-known that marking the positions of odd entries in Pascal's triangle generates, in a certain sense, the Sierpiński triangle. Therefore, we see that this fractal can be understood either by means of the sum-of-digits function in base 2 (1.3.3), or by checking "disjointness of the digits" of n and t (1.3.4). This can also be formulated in terms of *carries* [91]. Let $c(n,t)$ be the number of carries arising in the addition $n + t$. By Kummer's paper, we have in particular $c(n,t) = \nu_2\binom{n+t}{n}$. For the "base case" we have the following equivalent statements.

$$\begin{aligned} &2 \nmid \binom{n+t}{t} && \text{if and only if} \\ &\mathsf{s}_2(n+t) = \mathsf{s}_2(n) + \mathsf{s}_2(t) && \text{if and only if} \\ &t \preceq n + t && \text{if and only if} \\ &\text{for all } j \geq 0 : \big(\delta_j(n), \delta_j(t)\big) \neq \big(1, 1\big) && \text{if and only if} \\ &c(n,t) = 0. \end{aligned} \tag{1.3.5}$$

Let us now study higher divisibility and assume that $k \geq 0$. It is known [78] that the sets

$$A_k := \left\{(n,t) : 2^{k+1} \nmid \binom{n}{t}\right\} \tag{1.3.6}$$

of entries in Pascal's triangle not divisible by 2^{k+1} can be constructed by the following simple iterative procedure (omitting precise definitions of the used terms).

$k = 0$: Start with the infinite discrete Sierpiński triangle, which is A_0.

$k \geq 1$: Into each triangular hole of A_{k-1}, insert a maximal discrete Sierpiński triangle, in order to obtain A_k.

The following picture illustrates this procedure for the first 32 rows of Pascal's triangle, and $k \leq 2$.

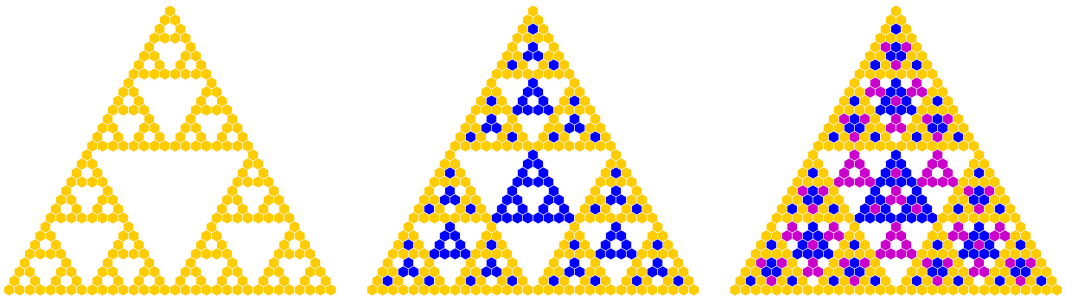


Figure 1.1: Binomial coefficients exactly divisible by 2^0(), 2^1(), or 2^2().

The blue hexagons in this picture correspond to binomial coefficients $\binom{n+t}{t}$ exactly divisible by 2, in other words, $\mathsf{s}_2(n+t)+1 = \mathsf{s}_2(n)+\mathsf{s}_2(t)$ (see (1.3.2)). Purple corresponds to exact divisibility by 4, and the equation $\mathsf{s}_2(n+t)+2 = \mathsf{s}_2(n)+\mathsf{s}_2(t)$.

It looked manageable at first to gain precise understanding of the occurrence of carries when adding n and t, that is, the set

$$\mathcal{C}_{n,t} := \big\{j \in \mathbb{N} : \text{ a carry appears at index } j \text{ in the addition } n+t\big\}. \tag{1.3.7}$$

This definition captures, intuitively, the "complexity" of the addition of integers.

We soon came to realize that the task of understanding the sets $\mathcal{C}_{n,t}$ is an infeasible one. In this context, we would like to first highlight the paper [150] with M. Wallner, where a glimpse of the apparent complexity of divisibility in Pascal's triangle can be taken. In that paper, we give a structural result concerning the quantities

$$\vartheta(j,n) := \#\left\{t \leq n : 2^j \mid \binom{n+t}{t} \text{ and } 2^{j+1} \nmid \binom{n+t}{t}\right\}$$

(the number of terms in row n of Pascal's triangle that are exactly divisible by 2^j). We studied an exact representation of $\vartheta(j,n)$ in terms of *subword-counting functions*

$$|n|_w := \#\big\{j \geq 0 : \text{the word } w \text{ appears at position } j \text{ in the binary expansion of } n\big\}.$$

For example, [150]

$$\vartheta(1,n)2^{-\mathtt{s}_2(n)} = \frac{1}{2}|n|_{\mathtt{10}}, \quad \text{and}$$
$$\vartheta(16,n)2^{-\mathtt{s}_2(n)} = \frac{1}{2^{16}16!}|n|_{\mathtt{10}}^{16} + (872748 \text{ monomials}),$$

where each of the 872748 additional monomials is a product of (at most 15) subword-counting functions $|\cdot|_w$ (see the Online Encyclopedia of Integer Sequences [140, A275012]). It is important to note that such a representation by a polynomial in block-counting functions is unique, as soon as only words $w = \mathtt{1}w'\mathtt{0}$ are admitted [150, Proposition 2.1], moreover there does exist a polynomial representation satisfying this restriction (see Barat–Grabner [12], and Rowland [134]). Note that the first formula expresses the number of blue hexagons in Figure 1.1, while hexagons "of color 16" do not appear before line $2^{16} = 65536$ in Pascal's triangle.

Another, even more striking, illustration of the complexity of this topic is the very close connection to the so-called *Diatomic Sequence* of Stern [154]. This 2-regular sequence (see Allouche–Shallit [3]) is defined by the deceptively simple recurrence

$$a(0) = 0, \quad a(1) = 1, \quad a(2n) = s(n), \quad a(2n+1) = a(n) + a(n+1). \tag{1.3.8}$$

The connection to Pascal's triangle can be seen from the formula

$$a(n+1) = \#\left\{(i,j) \in \mathbb{N}^2 : 2i + j = n, \binom{i+j}{i} \text{ is odd}\right\}. \tag{1.3.9}$$

This identity can be proved using *hyperbinary expansions* of an integer, see Northshield, [125, Theorem 4.1]. In other words, Stern's sequence is given by *diagonal sums* across Pascal's triangle modulo 2 [126]. By the equivalence (1.3.5) and the definition (1.3.7) of $\mathcal{C}_{n,t}$, we have

$$a(n+1) = \#\left\{i \geq 0 : \#\mathcal{C}_{i,n-2i} = 0\right\}. \tag{1.3.10}$$

From this we see that results on the structure of carries occurring in the addition of integers leads to a better understanding of Stern's sequence.

Stern's sequence a, in turn, is closely related to continued fractions (see Stern [154], Lehmer [93], Lind [95], and Graham, Knuth, and Patashnik [77, Exercise 6.50]): if

$$n = \left(\mathtt{1}^{k_0}\mathtt{0}^{k_1}\cdots\mathtt{1}^{k_{r-2}}\mathtt{0}^{k_{r-1}}\mathtt{1}^{k_r}\right)_2,$$

then a_n is the numerator of the rational represented by the continued fraction

$$[k_0; k_1, \ldots, k_r].$$

Therefore, it appears reasonable that "understanding carries occurring in the addition of integers" leads to "understanding the continued fraction expansion of rationals" (and consequently, the Euclidean algorithm, Farey series, ...). From this we derive the following informal guideline.

We cannot expect to gain complete understanding of the set $\mathcal{C}_{n,t}$. (1.3.11)

Due to the apparent difficulties connected to a precise understanding of carries, we have to lower our expectations.

In the first paper [153] of this series, jointly with M. Wallner, we explore this topic by investigating the inequality

$$\mathtt{s}_2(n+t) \geq \mathtt{s}_2(n). \tag{1.3.12}$$

Taking (1.3.11) to heart, we will not strive to fully characterize the set of pairs (n,t) such that (1.3.12) is satisfied. Instead, we will only study the *frequency* of integers n such that this inequality holds. In symbols, we set

$$c_t \coloneqq \lim_{N\to\infty} \frac{1}{N}\#\big\{n < N : \mathsf{s}_2(n+t) \geq \mathsf{s}_2(n)\big\}. \tag{1.3.13}$$

T. W. Cusick conjectured [private communication, 2011, 2015] that for each $t \geq 0$, we have

$$c_t > \frac{1}{2}. \tag{1.3.14}$$

Even though the behaviour of c_t should be more admissible than $\mathcal{C}_{n,t}$, we expect that the exact form of the value c_t will still be very difficult to grasp. We therefore content ourselves with bounds and asymptotic statements [42, 144, 148, 151–153].

Theorem 2.1.1 from **Chapter 2** gives an almost-solution to Cusick's (Hamming weight) conjecture. We prove that $c_t > 1/2$ if the binary expansion of t contains *a sufficient number* of maximal blocks of 1s. That is, we have $c_t > 1/2$ as soon as $|t|_{01} > M$, where M is an absolute, *effective* constant.

The second theorem in that paper identifies a Gaussian behaviour within the family $(\delta(t,j))_{j\in\mathbb{Z}}$ of densities

$$\delta(t,j) \coloneqq \lim_{N\to\infty} \frac{1}{N}\#\big\{n < N : \mathsf{s}_2(n+t) - \mathsf{s}_2(n) = j\big\}.$$

The quality of this normal approximation increases with the number of maximal blocks of `1` in the binary expansion of t.

Remark 2 (Relation to the main topic of this thesis)**.** Cusick's conjecture is firmly rooted in the topic "Subsequences of digitally defined functions". To see this, it suffices to note the following items.

1. In Cusick's conjecture, we may assume that t is odd, for the simple reason that $c_{2t} = c_t$ [42].
2. We have $\mathsf{s}_2(n+t) - \mathsf{s}_2(n) \leq \mathsf{s}(t)$ (see (1.3.2)).
3. The relation $\mathsf{s}_2(n+t) - \mathsf{s}_2(n) = j$ is in fact periodic in n with some period 2^q [17, 163].

Taking these points together, we see that Cusick's conjecture is a question on the subsequence

$$a^{(t)} \coloneqq \big(\mathsf{s}_2(nt)\big)_{n\geq 0}.$$

Namely, for t odd, we have

$$c_t = \lim_{N\to\infty} \frac{1}{N}\#\big\{0 \leq n < N : a^{(t)}(n+1) \geq a^{(t)}(n)\big\}.$$

1.4 The level of distribution of the Thue–Morse sequence

The second paper under discussion is published in **Compos. Math.** [145], and can be found in **Chapter 3**.

Section 2 we saw that Cusick's conjecture can be formulated as a conjecture on arithmetic subsequences of s_2. In Chapter 3, we study arithmetic subsequences again, but with a different

focus. In this chapter, we are interested in *short* arithmetic progressions, while Cusick's conjecture is a question on *long*, in fact, infinite, arithmetic progressions (see Remark 2). Short arithmetic progressions are, heuristically, more difficult to control than long ones. (The meaning of "short" can be found in the formulation of Theorem 3.2.1.)

As a compensation, we simplify the function $\mathtt{s}_2$ by reducing it modulo 2, leading to the *Thue–Morse sequence*

$$\begin{aligned}\mathbf{t}(n) &\coloneqq \mathtt{s}_2(n) \bmod 2\\ &= \big(\mathtt{0110100110010110100101100110100110010110011010010\cdots}\big).\end{aligned} \tag{1.4.1}$$

This sequence is *automatic* [5], as it is generated by feeding the binary expansion of $n \in \mathbb{N}$ into the following automaton.

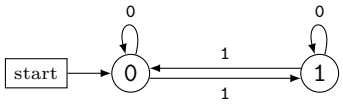


Figure 1.2: An automaton generating $\mathbf{t}$

Each time we encounter the digit 0, we stay at the same node, and each time 1 is read, we change sides. In this way, the number of 1s in binary is counted, modulo 2.

As a second simplification (of our problem to study digital expansions along short arithmetic progressions), we only ask for the number of times each of the values 0 and 1 is attained by $\mathbf{t}$ along our progression. Meanwhile, Cusick's conjecture was concerned with consecutive values of $\mathtt{s}_2$ along an arithmetic progression, more precisely, the difference $\mathtt{s}_2((n+1)t) - \mathtt{s}_2(nt)$.

This setup leads us to the notion of the *level of distribution*, which is a prominent topic in multiplicative number theory [67, 90, 164]. For example, the well-known Bombieri–Vinogradov theorem states that the *von Mangoldt function* Λ has level of distribution (at least) $1/2$. Loosely speaking, this theorem asserts in particular that the number of prime numbers in an arithmetic progression

$$\big(a, a+q, \dots, a+(N-1)q\big),$$

where $a < q$ and $\gcd(a,q) = 1$, is close to $\pi(Nq)/\varphi(q)$, for most moduli $q \asymp N(\log N)^{-A}$. Any improvement of the level of distribution beyond $1/2$ would constitute substantial progress in multiplicative number theory.

Understanding the behaviour of the Thue–Morse sequence is certainly more manageable than understanding prime numbers. In this case, it was already known that the value 0.5924, strictly larger than $1/2$, is an admissible level of distribution for the Thue–Morse sequence [64]. We were able to obtain the (optimal) value 1, which is the content of the main theorem in our second paper. The precise statement of this theorem (Theorem 3.2.1) is presented in Chapter 3 of this thesis.

Roughly, this result states that for most moduli $q \asymp N^R$, all of the numbers

$$\#\big\{n < N : \mathbf{t}(a+nq) = \mathtt{0}\big\},$$

for $a \geq 0$, are close to $N/2$.

The above-cited result [64] by Fouvry and Mauduit — the Thue–Morse sequence has level of distribution $\alpha = 0.5924$ — corresponds to $R \leq \alpha/(1-\alpha) \approx 1.453$. The substantial improvement

contained in our theorem is the fact that R may be chosen arbitrarily large. This explains the term "(very) short arithmetic progression", as the common difference may be astronomical compared to the number of terms.

In **Chapter 3** we prove this theorem, which has the potential for significant impact on the field.

Remark 3. We note that the proof strategy of Theorem 3.2.1 has been extended by M. Drmota, C. Müllner, and the author, in order to handle the *Zeckendorf sum-of-digits function* z. We were able to prove, in particular, the following statement [49, Theorem 1.1]:

> Let k be a sufficiently large integer. There exists a prime number p that is the sum of k pairwise different and non-consecutive Fibonacci numbers.

The paper containing this result is going to be published by Mem. Amer. Math. Soc.

1.5 Gaps in the Thue–Morse word

Chapter 4 is of a slightly different flavour, and concerns the paper [147], which will appear in **J. Aust. Math. Soc.**

Let $\mathfrak{a}$ be a digitally defined sequence over the alphabet A, and w a finite word in A. We start with a property $P_{\mathfrak{a},w}(\ell)$:

$$P_{\mathfrak{a},w}(\ell) \Longleftrightarrow \text{the word } w \text{ appears at position } \ell \text{ in the sequence } \mathfrak{a}.$$

The object of interest in this paper is the increasing sequence $n = (n_j)_{j\geq 0}$ of positions ℓ for which this property holds. (The subsequence $j \mapsto \mathfrak{a}(n_j)$ is constant.) We consider in particular the increasing sequence $n = (n_j)_{j\geq 0}$ of positions in the Thue–Morse word at which the subword $\mathtt{01}$ appears. The main result of this chapter states that the sequence n is not k-*regular*, for every $k \geq 2$, in the sense of J.-P. Allouche and J. Shallit [3]. Thereby we answer a question of Shallit in the affirmative.

In fact, what Shallit asked (private communication, 2019) was to prove that the *gap sequence*

$$\mathbf{B} = \big(n_{j+1} - n_j\big)_{j\geq 0}$$

of occurrences of $\mathtt{01}$ in the Thue–Morse sequence is not automatic. Since the sequence of partial sums of k-automatic sequences is k-regular, differences $j \mapsto f(j+1) - f(j)$ of k-regular sequences are again k-regular, and finite-valued k-regular sequences are k-automatic [3], these two problems are equivalent. As a corollary to our method, we derive the result that the gap sequence corresponding to *any* factor of the Thue–Morse sequence, of length at least two, is not automatic. Here a *factor* of a word is any contiguous finite subsequence of that word.

Our proof of Theorem 4.1.1 is based on a close relation to the well-known *ternary Thue–Morse sequence* $\mathbf{A}$ [2, 20, 84], see the definition by a morphism in (4.2.1). This sequence on the letters $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ is in fact automatic, and we display a corresponding base-2 automaton in Figure 1.3 below.

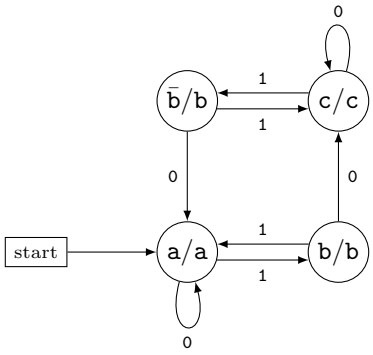


Figure 1.3: An automaton generating **A**

Following the edges according to the binary expansion of an integer, we arrive at one of the four nodes a, b, $\bar{\mathtt{b}}$, or c; applying the projection $\mathtt{a} \mapsto \mathtt{a}$, $\mathtt{b} \mapsto \mathtt{b}$, $\bar{\mathtt{b}} \mapsto \mathtt{b}$, $\mathtt{c} \mapsto \mathtt{c}$, we obtain the sequence **A** on three symbols. (Note that applying the projection $\mathtt{a} \mapsto \mathtt{0}$, $\bar{\mathtt{b}} \mapsto \mathtt{0}$, $\mathtt{b} \mapsto \mathtt{1}$, $\mathtt{c} \mapsto \mathtt{1}$ instead, we obtain the Thue–Morse sequence!) The gap sequence **B** can be recovered from **A**, replacing each occurrence of a by 33, each b by 4, and each c by 2.

$$\mathbf{A} = \mathtt{a\ bca\ cba\ bcba\ ca\ bca\ cba\ ca\ bcba\ bca\ cba\ bcba\ ca\ bcba\ bca\ cb}\cdots$$
$$\mathbf{B} = 33423324334243323342332433233424334233243342433233424334233424334233424334233424\cdots$$

Figure 1.4: **A** is automatic, while **B** is not

The gap sequence **B** is *substitutive*, or *morphic*, as a morphic image of an automatic sequence (Figure 1.4), see [5, Corollary 7.7.5]. Our main theorem, Theorem 4.1.1, states that the gap sequence **B** is not automatic in any base.

The second part of our paper [147] is concerned with the *discrepancy* of the number of occurrences of 01. This quantity is defined by

$$D_N := \#\big\{0 \le n < N : \mathbf{t}_n = \mathtt{0}, \mathbf{t}_{n+1} = \mathtt{1}\big\} - \frac{N}{3}.$$

To this end, we closely investigate the structure of **A**. More precisely, we study certain *rotations* of letters, which transform **A** into the periodic word $(\mathtt{abcabc}\cdots)$. Understanding the nested structure of these rotations is the subject of this part of the paper. In particular, we represent the discrepancy by means of *output sums of a transducer* [83], and derive the corollary that D_N takes every value in $\frac{1}{3}\mathbb{Z}$ infinitely often, see (4.3.22).

1.6 Collisions of digit sums in bases 2 and 3

In **Chapter 5** we solve a long-standing folklore conjecture on the joint digital expansion of natural numbers in bases 2 and 3. The corresponding paper [146] will be published in **Israel J. Math.**

The following form of the conjecture — now a theorem (Theorem 5.1.1) — was formulated at the latest towards the end of the last century.

Conjecture 1. We have $\mathsf{s}_2(n) = \mathsf{s}_3(n)$ infinitely often.

We list some values of the binary and the ternary sum-of-digits functions, where we highlight collisions — integers n such that $\mathsf{s}_2(n) = \mathsf{s}_3(n)$ — using boxes.

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
$\boxed{0}$	0	0
$\boxed{1}$	1	1
2	1	2
3	2	1
4	1	2
5	2	3
$\boxed{6}$	2	2
$\boxed{7}$	3	3
8	1	4
9	2	1

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
$\boxed{10}$	2	2
$\boxed{11}$	3	3
$\boxed{12}$	2	2
$\boxed{13}$	3	3
14	3	4
15	4	3
16	1	4
17	2	5
$\boxed{18}$	2	2
$\boxed{19}$	3	3

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
20	2	4
$\boxed{21}$	3	3
22	3	4
23	4	5
24	2	4
25	3	5
26	3	6
27	4	1
28	3	2
29	4	3

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
30	4	2
31	5	3
32	1	4
33	2	3
34	2	4
35	3	5
$\boxed{36}$	2	2
$\boxed{37}$	3	3
38	3	4
39	4	3

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
40	2	4
41	3	5
42	3	4
43	4	5
44	3	6
45	4	3
$\boxed{46}$	4	4
$\boxed{47}$	5	5
48	2	4
49	3	5

n	$\mathsf{s}_2(n)$	$\mathsf{s}_3(n)$
50	3	6
51	4	5
52	3	6
53	4	7
54	4	2
55	5	3
56	3	4
57	4	3
$\boxed{58}$	4	4
$\boxed{59}$	5	5

The sequence of collisions therefore begins as follows:

$$0, 1, 6, 7, 10, 11, 12, 13, 18, 19, 21, 36, 37, 46, 47, 58, 59, \ldots,$$

which is sequence `A037301` in the OEIS [140].

An obvious question would be to decide whether there exist arbitrarily long sequences of consecutive collisions. It is easy to see, however, that there cannot exist five consecutive collisions. To this end, assume that $\mathsf{s}_2(n) = \mathsf{s}_3(n)$ for $n \in A = \{n_0, \ldots, n_0+4\}$. Then $\{3\ell, 3\ell+1, 3\ell+2\} \subseteq A$ for some ℓ, which implies

$$\mathsf{s}_2(3\ell + 2) = \mathsf{s}_3(3\ell + 2) = \mathsf{s}_3(3\ell) + 2 = \mathsf{s}_2(3\ell) + 2.$$

However, $\mathsf{s}_2(m + 2) \leq \mathsf{s}_2(m) + 1$ by (1.3.2), which is a contradiction.

Note that on the OEIS page for sequence `A037301`, an exhaustive search up to 3^{29} in search of five or more adjacent collisions is mentioned, an effort that would not have been necessary.

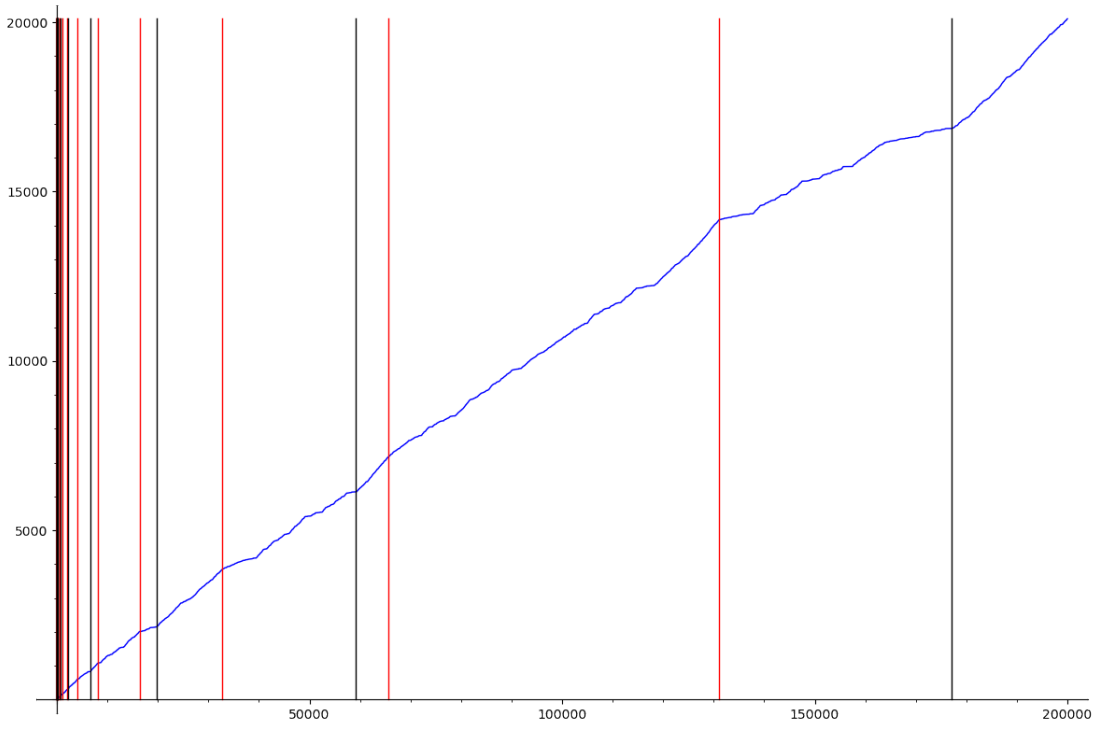


Figure 1.5: blue: number of collisions up to N; red: powers of 2; black: powers of 3

In Figure 1.5 we can clearly see that for N near powers of 2 and 3, there appear to be fluctuations in the observed numbers of collisions up to N. Heuristically, this can be explained as follows. For example, approaching a power of 2 from below, the number of digits 1 in binary is above average. Since the expected sum of digits in base 3 is larger than the expected sum of digits in base 2, this bias shifts the expected values closer to each other, and we expect more collisions.

The main result of Chapter 5 — Theorem 5.1.1 — states that the number of collisions is indeed infinite. More precisely, a lower bound of the form N^η, where $\eta > 0$, for the number of collisions up to N is given: we have

$$\#\big\{n < N : \mathsf{s}_2(n) = \mathsf{s}_3(n)\big\} \geq CN^\eta$$

for some constants $C, \eta > 0$.

We would also like to highlight a connection to the base-12 expansion of $n!$ [35, 36, 39]. By (2.1.2), the integer $n \geq 0$ is a collision if and only if

$$\nu_2(n!) = n - \mathsf{s}_2(n) = 2\,\frac{n - \mathsf{s}_3(n)}{2} = 2\,\nu_3(n!).$$

This is the case if and only if $n!$ is *exactly divisible by* $(2^2 \cdot 3^1)^k = 12^k$ for some k, by which we mean the property

$$12^k \mid n! \quad \text{and} \quad \gcd(12, n!/12^k) = 1.$$

In this case, and in this case only, the last significant base-12 digit of $n!$, in symbols, $\ell_{12}(n!)$, is an element of $\{1, 5, 7, 11\}$. Summarizing, we have the equivalences

$$\begin{aligned} &\mathsf{s}_2(n) = \mathsf{s}_3(n) && \text{if and only if} \\ &\nu_2(n!) = 2\,\nu_3(n!) && \text{if and only if} \\ &12^k \text{ exactly divides } n! \text{ for some } k && \text{if and only if} \\ &\ell_{12}(n!) \in \{1, 5, 7, 11\}. \end{aligned} \tag{1.6.1}$$

Together with J.-M. Deshouillers and M. Drmota (work in progress) we prove that the last significant digit of $n!$ in base 12 attains each of $1, 5, 7$, and 11 infinitely many times, which is a refinement of Conjecture 1.

Remark 4. We note that the proof of Theorem 5.1.1, and thus the solution of Conjecture 1, heavily relies on arithmetic subsequences of s_2 and s_3, and thus fits nicely into the general framework of this thesis. In fact, the problem greatly simplifies when the sequence $n \mapsto \mathsf{s}_2(n) - \mathsf{s}_3(n)$, where $n \in [N, 2N)$, is *rarefied* by a certain power 3^ζ. According to (5.2.44), we will have

$$\zeta \sim \left(1 - \frac{\log 3}{2 \log 2}\right) \frac{\log N}{\log 2}.$$

The simple heuristics behind this rarefaction is the following: along the arithmetic progression $3^\zeta \mathbb{N} \cap [N, 2N)$, the expected values of $\mathsf{s}_2(n)$ and $\mathsf{s}_3(n)$ will be similar (within few standard deviations from each other), while the expected values on the interval $[N, 2N)$, without rarefaction, differ by many standard deviations. The technicalities surrounding this *key argument* are notable, but it should be kept in mind that it is really the essence of the proof. We will not reproduce the details at this point, but postpone them to Chapter 5. Let us only note that we were not able to prove the theorem without such an "expectation-adjusting rarefaction".

Summarizing, passing to a suitable *subsequence of a digitally defined function*, the formerly intractable Conjecture 1 becomes manageable.

Chapter 2

The binary digits of $n + t$

Lukas Spiegelhofer and Michael Wallner
To appear in Ann. Scuola Norm. Sup. Pisa Cl. Sci.
DOI: https://doi.org/10.2422/2036-2145.202105_069

Abstract

The binary sum-of-digits function s counts the number of ones in the binary expansion of a nonnegative integer. For any nonnegative integer t, T. W. Cusick defined the asymptotic density c_t of integers $n \geq 0$ such that

$$s(n + t) \geq s(n).$$

In 2011, he conjectured that $c_t > 1/2$ for all t — the binary sum of digits should, more often than not, weakly increase when a constant is added. In this paper, we prove that there exists an explicit constant M_0 such that indeed $c_t > 1/2$ if the binary expansion of t contains at least M_0 maximal blocks of contiguous ones, leaving open only the "initial cases" — few maximal blocks of ones — of this conjecture. Moreover, we sharpen a result by Emme and Hubert (2019), proving that the difference $s(n + t) - s(n)$ behaves according to a Gaussian distribution, up to an error tending to 0 as the number of maximal blocks of ones in the binary expansion of t grows.

2.1 Introduction and main result

The binary expansion of an integer is a fundamental concept occurring most prominently in number theory and computer science. Its close relative, the decimal expansion, is found throughout everyday life to such an extent that "numbers" are often understood as being the same as a string of decimal digits. However, it is difficult to argue — mathematically — that base ten is special; in our opinion the binary case should be considered first when a problem on digits occurs.

The basic problem we deal with is the (not yet fully understood) addition in base two. Let us consider two simple examples: $\mathtt{10} + \mathtt{1} = \mathtt{11}$ and $\mathtt{11} + \mathtt{1} = \mathtt{100}$. The difference between these two, and what makes the second one more complicated, is the occurrence of *carries* and their

interactions via *carry propagation*. These carries turn the problem of addition into a complicated case-by-case study and a complete characterization is unfortunately out of sight. In order to approach this problem, we consider a parameter associated to the binary expansion — the *binary sum of digits* $s(n)$ of a nonnegative integer n. This is just the number of 1s in the binary expansion of n, and equal to the minimal number of powers of two needed to write n as their sum. While we are only dealing with this parameter instead of the whole expansion, we believe that it already contains the main difficulties caused by carry propagation.

Cusick's conjecture encodes these difficulties by simultaneously studying the sum-of-digits function of n and $n+t$. It states (private communication, 2011, 2015[1]) that for all $t \geq 0$,

$$c_t > 1/2, \tag{2.1.1}$$

where

$$c_t = \lim_{N\to\infty} \frac{1}{N}\big|\big\{0 \leq n < N : s(n+t) \geq s(n)\big\}\big|$$

is the proportion of nonnegative integers n such that $n+t$ contains it its binary representation at least as many 1s as n.

This easy-to-state conjecture seems to be surprisingly hard to prove. Moreover, it has an important connection to divisibility questions in Pascal's triangle: the formula

$$s(n+t) - s(n) = s(t) - \nu_2\left(\binom{n+t}{t}\right) \tag{2.1.2}$$

essentially due to Legendre links our research problem to the 2-valuation ν_2 of binomial coefficients, which is defined by $\nu_2(a) := \max\{e \in \mathbb{Z} : 2^e \mid a\}$. Note also that the last term in (2.1.2) is the number of carries appearing in the addition $n+t$, a result that is due to Kummer [91]. The strong link expressed in (2.1.2), and the combination of simplicity and complexity, has been a major motivation for our research.

In order to better understand the conjecture, we start with some simple examples. For $t = 0$ we directly get $c_0 = 1$. For $t = 1$ it suffices to consider the last two digits of n to obtain $c_1 = 3/4$. Note that in the two binary additions above we have $t = 1$, where the first one satisfies $s(n+1) \geq s(n)$, while the second does not. For more values of c_t we used the recurrence (2.1.5) defined below and we verified $c_t > 1/2$ for all $t \leq 2^{30}$ numerically. In Figure 2.1 we illustrate the first values of c_t.

The full conjecture is still open, yet some partial results have been obtained [42, 54–56, 144, 148]. Among these, we want to stress a central limit-type result by Emme and Hubert [55], a lower bound due to the first author [148], and an almost-all result by Drmota, Kauers, and the first author [42] stating that for all $\varepsilon > 0$, we have

$$|\{t < T : 1/2 < c_t < 1/2 + \varepsilon\}| = T - \mathcal{O}\left(\frac{T}{\log T}\right).$$

(The symbol $\mathcal{O}$ is used for Big O notation throughout this paper.) Moreover, Cusick's conjecture is strongly connected to the *Tu–Deng conjecture* [159, 160] in cryptography, which is also still open, yet with some partial results [29,34,60,61,152,159]. We presented this connection in [152], in which we proved an almost-all result for the Tu–Deng conjecture and where we showed that the full Tu–Deng conjecture implies Cusick's conjecture.

[1]The conjecture was initially termed "Cusick problem" or "Question by Cusick" in the community, but in an e-mail dated 2015 to the first author, Cusick upgraded it to "conjecture".

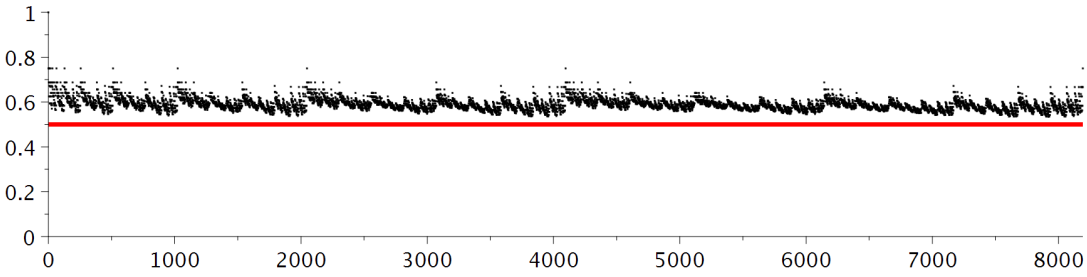


Figure 2.1: Cusick's conjecture states that $c_t > 1/2$ for all $t \geq 0$, which is illustrated in this figure for all $t \leq 2^{13}$, and which we computationally confirmed for all $t \leq 2^{30}$. In this paper we prove that it holds for all t with sufficiently many blocks of 1s, so that only finitely many classes (each class is concerned with those t having a fixed number of maximal blocks of 1s) remain open.

The main theorem of this paper is the following near-solution to Cusick's conjecture, which significantly improves the previous results. Note that it happens repeatedly that difficult conjectures are (more easily) provable for sufficiently large integers and recently even two more important ones have been resolved in this manner: Sendov's conjecture [157] and the Erdős–Faber–Lovász conjecture [86]. Our method will combine several techniques such as recurrence relations, cumulant generating functions, and integral representations.

Theorem 2.1.1. *There exists a constant M_0 with the following property: If the natural number t has at least M_0 maximal blocks of* 1*s in its binary expansion, then $c_t > 1/2$.*

Remark 5. We note the important observation that all constants in this paper could be given numerical values by following our proofs. In order to keep the technicalities at a minimum, we decided not to compute them explicitly. In this paper, we do not rely on arguments making it impossible to extract explicit values for our constants (such as certain proofs by contradiction). We are dealing with *effective* results, without giving a precise definition of this term.

The central objects to tackle the conjecture are the asymptotic densities

$$\delta(j,t) = \lim_{N\to\infty} \frac{1}{N} \#\big\{0 \leq n < N : s(n+t) - s(n) = j\big\},$$

where $j \in \mathbb{Z}$. The limit exists in our case; see Bésineau [18]. These densities lead to the useful decomposition

$$c_t = \sum_{j\geq 0} \delta(j,t). \tag{2.1.3}$$

The sum on the right hand side is in fact finite, since $\delta(j,t) = 0$ for $j > s(t)$, which follows from (2.1.2). Therefore we get equality in (2.1.3) — asymptotic densities are finitely additive.

Distinguishing between even and odd cases, one can show that the values $\delta(k,t)$ satisfy the following recurrence [42, 144, 148]:

$$\delta(j,1) = \begin{cases} 0, & j > 1; \\ 2^{j-2}, & j \leq 1, \end{cases} \tag{2.1.4}$$

and for $t \geq 0$,

$$\begin{aligned} \delta(j,2t) &= \delta(j,t), \\ \delta(j,2t+1) &= \frac{1}{2}\delta(j-1,t) + \frac{1}{2}\delta(j+1,t+1). \end{aligned} \tag{2.1.5}$$

In particular, the recurrence shows that $\delta(\_,t)$ is a probability mass function for each t:

$$\sum_{j\in\mathbb{Z}} \delta(j,t) = 1, \tag{2.1.6}$$

and $\delta(j,t) \geq 0$ by definition. Furthermore, the set

$$\{n \in \mathbb{N} : s(n+t) - s(n) = j\}$$

defining $\delta(j,t)$ is a finite union of arithmetic progressions $a + 2^m\mathbb{N}$, which can be seen along the same lines.

Our second main result gives an asymptotic formula for the densities $\delta(j,t)$ and is obtained in the course of establishing Theorem 2.1.1.

Theorem 2.1.2. *For integers $t \geq 1$, let us define*

$$\kappa_2(1) = 2; \qquad \kappa_2(2t) = \kappa_2(t); \qquad \kappa_2(2t+1) = \frac{\kappa_2(t) + \kappa_2(t+1)}{2} + 1.$$

If the positive integer t has M maximal blocks of `1`*s in its binary expansion, and M is larger than some constant M_0, then we have*

$$\delta(j,t) = \frac{1}{\sqrt{2\pi\kappa_2(t)}} \exp\left(-\frac{j^2}{2\kappa_2(t)}\right) + \mathcal{O}\big(M^{-1}(\log M)^4\big)$$

for all integers j. The multiplicative constant in the error term can be made explicit.

Concerning the effectiveness of the constants, we refer to the remark after Theorem 2.1.1. We will see in Corollary 2.2.3 and in Lemma 2.2.4 that

$$M \leq \kappa_2(t) \leq CM$$

for some constant C. Therefore, the main term dominates the error term for large M if

$$|j| \leq \frac{1}{2}\sqrt{M \log M}.$$

Note that the factor $1/2$ is arbitrary and any value $\rho < 1$ is good enough (for M larger than some bound depending on ρ). Moreover, in the statement of Theorem 2.1.2, the lower bound $M > M_0$ is, in fact, not needed, as it can be taken care of by the constant C in the error term. Simply choose C so large that the error term is greater than 1 (for example, $C = M_0$ is sufficient, since $\delta(j,t) \leq 1$). We decided to keep the theorem as it is, since we feel that increasing a constant only for reasons of brevity is somewhat artificial.

Without giving a full proof we note that, by summation, this theorem can be used for proving a statement comparing $\Delta(j,t) = \sum_{j'\geq j} \delta(j',t)$ and the Gaussian $\Phi\big(-j/\sqrt{\kappa_2(t)}\big)$. This leads to a sharpening of the main result in Emme and Hubert [55]. By summing the asymptotic formula in Theorem 2.1.2 from 0 to $\sqrt{M}\log M$, we also obtain the following corollary.

Corollary 2.1.3. *There exists a constant C such that*

$$c_t \geq 1/2 - CM^{-1/2}\big(\log M\big)^5$$

for all $t \geq 1$, where M is the number of maximal blocks of `1`*s in t.*

The proof is straightforward, and left to the reader. This corollary is weaker than Theorem 2.1.1, but we stated it here since it gives a quantitative version of the main theorem in [148].

Notation. In this paper, $0 \in \mathbb{N}$. We will use Big O notation, employing the symbol $\mathcal{O}$. We let $\mathrm{e}(x)$ denote $e^{2\pi i x}$ for real x. In our calculations, the number π will often appear with a factor 2. Therefore we use the abbreviation $\tau = 2\pi$.

We consider blocks of `0`s or `1`s in the binary expansion of an integer $t \in \mathbb{N}$. Writing "block of `1`s of length ν in t", we always mean a maximal subsequence $\varepsilon_\mu = \varepsilon_{\mu+1} = \cdots = \varepsilon_{\mu+\nu-1} = 1$ (where maximal means that $\varepsilon_{\mu+\nu} = 0$ and either $\mu = 0$ or $\varepsilon_{\mu-1} = 0$). "Blocks of `0`s of length ν in t" are subsequences $\varepsilon_\mu = \cdots = \varepsilon_{\mu+\nu-1} = 0$ such that $\varepsilon_{\mu+\nu} = 1$ and either $\mu = 0$ or $\varepsilon_{\mu-1} = 1$. We call blocks of zeros bordered by `1`s on both sides "inner blocks of `0`s". For example, $2^k n$ and n have the same number of inner blocks of `0`s. The *number of blocks in t* is the sum of the number of blocks of `1`s and the number of blocks of `0`s.

All constants in this paper are absolute and effective. The letter C is often used for constants; occurrences of C at different positions need not necessarily designate the same value.

In the remainder we give the proof of our main result, Theorem 2.1.1, followed by the proof of Theorem 2.1.2.

Acknowledgments.

On one of his first days as a PhD student in 2011, the first author was introduced to Cusick's conjecture by Johannes F. Morgenbesser, whom he wishes to thank at this point. This conjecture has ever since been a source of inspiration and motivation to him. We also wish to thank Michael Drmota, Jordan Emme, Wolfgang Steiner, and Thomas Stoll for fruitful discussions on the topic. Finally, we thank Thomas W. Cusick for constant encouragement and interest in our work.

2.2 Proof of the main theorem

The proof of our main Theorem 2.1.1 is split into several parts. The main idea is to work with the cumulant generating function of the probability distribution given by the densities $\delta(j,t)$, which we define in Section 2.2.1. The crucial observation later on is that it is sufficient to work with an approximation using only the cumulants up to order 5. This approximation is analyzed in Section 2.2.2 and used in Section 2.2.3 inside an explicit integral representation of c_t to prove our main result up to an exceptional set of ts. It remains to prove that these exceptional values, which are defined by the cumulants of order 2 and 3, satisfy an inequality involving the cumulants of order 4 and 5. For this reason, we needed to choose an approximation of the cumulant generating function up to order 5. Thus, in Section 2.2.4 we determine this exceptional set and in Section 2.2.5 we prove bounds on the cumulants of order 4 and 5. Finally, in Section 2.2.6 we combine all ingredients to prove the inequality.

2.2.1 Characteristic function and cumulant generating function

We begin with the definition of the characteristic function of the probability distribution given by the densities $\delta(j,t)$. In particular, we use the following variant, involving a scaling factor $\tau = 2\pi$. For $t \geq 0$ and $\vartheta \in \mathbb{R}$ we define

$$\gamma_t(\vartheta) = \sum_{j\in\mathbb{Z}} \delta(j,t)\,\mathrm{e}(j\vartheta).$$

Since $\delta(\_,t)$ defines a probability distribution and $|\mathrm{e}(x)| \leq 1$ for real x, we may interchange summation and integration by the dominated convergence theorem:

$$\begin{aligned}\delta(j,t) &= \sum_{k\in\mathbb{Z}} \delta(k,t)\cdot \left\{ \begin{array}{ll} 1, & k=j; \\ 0, & k\neq j \end{array} \right\} = \sum_{k\in\mathbb{Z}} \delta(k,t) \int_{-1/2}^{1/2} \mathrm{e}((k-j)\vartheta)\,\mathrm{d}\vartheta \\ &= \int_{-1/2}^{1/2} \mathrm{e}(-j\vartheta) \sum_{k\in\mathbb{Z}} \delta(k,t)\,\mathrm{e}(k\vartheta)\,\mathrm{d}\vartheta = \int_{-1/2}^{1/2} \gamma_t(\vartheta)\,\mathrm{e}(-j\vartheta)\,\mathrm{d}\vartheta.\end{aligned} \tag{2.2.1}$$

The recurrence (2.1.5) directly carries over to the characteristic functions. For all $t \geq 0$, we have

$$\begin{aligned}\gamma_{2t}(\vartheta) &= \gamma_t(\vartheta), \\ \gamma_{2t+1}(\vartheta) &= \frac{\mathrm{e}(\vartheta)}{2}\gamma_t(\vartheta) + \frac{\mathrm{e}(-\vartheta)}{2}\gamma_{t+1}(\vartheta),\end{aligned} \tag{2.2.2}$$

and in particular

$$\gamma_1(\vartheta) = \frac{\mathrm{e}(\vartheta)}{2-\mathrm{e}(-\vartheta)}. \tag{2.2.3}$$

Therefore, for all $t \geq 1$, we have

$$\gamma_t(\vartheta) = \omega_t(\vartheta)\gamma_1(\vartheta),$$

where ω_t is a trigonometric polynomial such that $\omega_t(0) = 1$. These polynomials satisfy the same recurrence relation as γ_t. In particular, noting also that the denominator $2 - \mathrm{e}(-\vartheta)$ is nonzero near $\vartheta = 0$, we have $\operatorname{Re}\gamma_t(\vartheta) > 0$ for ϑ in a certain disk

$$D_t = \{\vartheta \in \mathbb{C} : |\vartheta| < r(t)\},$$

where $r(t) > 0$. It follows that

$$K_t = \log \circ\, \gamma_t \tag{2.2.4}$$

is analytic in D_t and therefore there exist complex numbers $\kappa_j(t)$ for $j \in \mathbb{N}$ such that

$$\gamma_t(\vartheta) = \exp(K_t(\vartheta)) = \exp\left(\sum_{j\geq 0} \frac{\kappa_j(t)}{j!}(i\tau\vartheta)^j\right) \tag{2.2.5}$$

for all $\vartheta \in D_t$. These numbers $\kappa_j(t)$ are the *cumulants* of the probability distribution defined by $\delta(\_,t)$ (up to a scaling by τ); see, e.g., [19]. They are real numbers since characteristic functions are Hermitian: $\gamma_t(\vartheta) = \overline{\gamma_t(-\vartheta)}$. The real-valuedness also follows directly from the fact that cumulants are defined via the logarithm of the moment generating function, which has real coefficients. The cumulant $\kappa_2(t)$ is the variance: we have

$$\kappa_2(t) = \sum_{j\in\mathbb{Z}} j^2\delta(j,t). \tag{2.2.6}$$

For $t = 0$, we have $\kappa_j(t) = 0$ for all $j \geq 0$, as $\delta(k, 0) = 1$ if $k = 0$ and $\delta(k, 0) = 0$ otherwise. The recurrence (2.2.2) shows that

$$\gamma_t(\vartheta) = 1 + \mathcal{O}(\vartheta^2)$$

at 0, which implies $\kappa_0(t) = \kappa_1(t) = 0$. Let us write

$$x_j = \kappa_j(t), \quad y_j = \kappa_j(t+1), \quad \text{and} \quad z_j = \kappa_j(2t+1). \tag{2.2.7}$$

Next, we will express the coefficients z_j as functions of the coefficients x_j and y_j. Therefore we substitute the cumulant representation from (2.2.5) for $\gamma_t(\vartheta)$ into the recurrence (2.2.2) and obtain that these quantities are related via the fundamental identity

$$\begin{aligned} \exp\Big(\frac{z_2}{2}(i\tau\vartheta)^2 + \frac{z_3}{6}(i\tau\vartheta)^3 + \cdots\Big) \\ = \frac{1}{2}\exp\Big(\ \ i\tau\vartheta + \frac{x_2}{2}(i\tau\vartheta)^2 + \frac{x_3}{6}(i\tau\vartheta)^3 + \cdots\Big) \\ + \frac{1}{2}\exp\Big(-i\tau\vartheta + \frac{y_2}{2}(i\tau\vartheta)^2 + \frac{y_3}{6}(i\tau\vartheta)^3 + \cdots\Big), \end{aligned} \tag{2.2.8}$$

valid for $\vartheta \in D = D_t \cap D_{t+1} \cap D_{2t+1}$. From this equation, we derive the following lemma by comparing coefficients of the appearing analytic functions.

Lemma 2.2.1. *Assume that $t \geq 0$ and let x_j, y_j, and z_j be defined by (2.2.7). We have*

$$z_2 = \frac{x_2 + y_2}{2} + 1; \tag{2.2.9}$$

$$z_3 = \frac{x_3 + y_3}{2} + \frac{3}{2}(x_2 - y_2); \tag{2.2.10}$$

$$z_4 = \frac{x_4 + y_4}{2} + 2(x_3 - y_3) + \frac{3}{4}(x_2 - y_2)^2 - 2; \tag{2.2.11}$$

$$z_5 = \frac{x_5 + y_5}{2} + \frac{5}{2}(x_4 - y_4) + \frac{5}{2}(x_2 - y_2)(x_3 - y_3) - 10(x_2 - y_2). \tag{2.2.12}$$

In particular,

$$\kappa_2(1) = 2, \quad \kappa_3(1) = -6, \quad \kappa_4(1) = 26, \quad \kappa_5(1) = -150. \tag{2.2.13}$$

Proof. Extracting the coefficient of ϑ^2 in (2.2.8), we obtain

$$\begin{aligned} z_2 = \frac{1}{(i\tau)^2}[\vartheta^2]\Big(1 + i\,\tau\vartheta + \frac{x_2}{2}(i\tau\vartheta)^2 + \frac{1}{2}\big(i\,\tau\vartheta + \frac{x_2}{2}(i\tau\vartheta)^2\big)^2 \\ + 1 - i\,\tau\vartheta + \frac{y_2}{2}(i\tau\vartheta)^2 + \frac{1}{2}\big(-i\,\tau\vartheta + \frac{y_2}{2}(i\tau\vartheta)^2\big)^2\Big) = \frac{x_2 + y_2}{2} + 1, \end{aligned}$$

where $[x^k]\sum f_k x^k = f_k$ denotes the coefficient extraction operator and this gives (2.2.9).

Similarly, we handle the higher coefficients. We proceed with $[\vartheta^3]K_t(\vartheta)$. From (2.2.8) we obtain by collecting the cubic terms

$$\begin{aligned} z_3 &= \frac{3}{(i\tau)^3}\left(\frac{x_3}{6}(i\tau)^3 + 2\frac{1}{2}\frac{x_2}{2}(i\tau)^3 + \frac{1}{6}(i\tau)^3 + \frac{y_3}{6}(i\tau)^3 - 2\frac{1}{2}\frac{y_2}{2}(i\tau)^3 - \frac{1}{6}(i\tau)^3\right) \\ &= \frac{x_3 + y_3}{2} + \frac{3}{2}(x_2 - y_2), \end{aligned}$$

which is (2.2.10). For the next coefficient $[\vartheta^4]K_t(\vartheta)$, we have to take the quadratic term of the exponential on the left hand side of (2.2.8) into account. This yields, inserting the recurrence for z_2 obtained before,

$$\begin{aligned}\left[\vartheta^4\right]\exp\left(\frac{z_2}{2}(i\tau\vartheta)^2+\frac{z_3}{6}(i\tau\vartheta)^3+\frac{z_4}{24}(i\tau\vartheta)^4\right)&=\tau^4\left(\frac{z_4}{24}+\frac{z_2^2}{8}\right)\\&=\tau^4\left(\frac{z_4}{24}+\frac{1}{8}+\frac{x_2+y_2}{8}+\frac{(x_2+y_2)^2}{32}\right).\end{aligned}$$

The coefficient of ϑ^4 of the right hand side of (2.2.8) gives, collecting the quartic terms,

$$\begin{aligned}&\frac{\tau^4}{2}\left(\frac{x_4}{24}+\frac{1}{2}\left(\frac{x_3}{3}+\frac{x_2^2}{4}\right)+\frac{1}{6}\left(3\frac{x_2}{2}\right)+\frac{1}{24}\right.\\&\qquad\left.+\frac{y_4}{24}+\frac{1}{2}\left(-\frac{y_3}{3}+\frac{y_2^2}{4}\right)+\frac{1}{6}\left(3\frac{y_2}{2}\right)+\frac{1}{24}\right)\\&\qquad=\tau^4\left(\frac{x_4+y_4}{48}+\frac{x_3-y_3}{12}+\frac{x_2^2+y_2^2}{16}+\frac{x_2+y_2}{16}+\frac{1}{24}\right).\end{aligned}$$

Equation (2.2.11) follows. Finally, we need the quintic terms. The left hand side of (2.2.8) yields

$$\begin{aligned}\left[\vartheta^5\right]\exp\left(\frac{z_2}{2}(i\tau\vartheta)^2+\frac{z_3}{6}(i\tau\vartheta)^3+\frac{z_4}{24}(i\tau\vartheta)^4+\frac{z_5}{120}(i\tau\vartheta)^5\right)&=(i\tau)^5\left(\frac{z_5}{120}+\frac{z_2z_3}{12}\right)\\&=(i\tau)^5\left(\frac{z_5}{120}+\frac{1}{12}\left(\frac{x_2+y_2}{2}+1\right)\left(\frac{x_3+y_3}{2}+\frac{3}{2}(x_2-y_2)\right)\right),\end{aligned}$$

while the right hand side of (2.2.8) yields

$$\begin{aligned}&\frac{(i\tau)^5}{2}\left(\frac{x_5}{120}+\frac{1}{2}\left(2\frac{x_2x_3}{12}+2\frac{x_4}{24}\right)+\frac{1}{6}\left(3\frac{x_3}{6}+3\frac{x_2^2}{4}\right)+\frac{1}{24}\left(4\frac{x_2}{2}\right)+\frac{1}{120}\right.\\&\quad\left.+\frac{y_5}{120}+\frac{1}{2}\left(2\frac{y_2y_3}{12}-2\frac{y_4}{24}\right)+\frac{1}{6}\left(3\frac{y_3}{6}-3\frac{y_2^2}{4}\right)-\frac{1}{24}\left(4\frac{y_2}{2}\right)-\frac{1}{120}\right)\\&\quad=(i\tau)^5\left(\frac{x_5+y_5}{240}+\frac{x_4-y_4}{48}+\frac{x_3+y_3}{24}+\frac{x_2x_3+y_2y_3}{24}+\frac{x_2^2-y_2^2}{16}+\frac{x_2-y_2}{24}\right),\end{aligned}$$

which implies (2.2.12) after a short calculation. Finally, we compute the values $\kappa_2(1),\dots,\kappa_5(1)$ by substituting $t=0$ in (2.2.9)–(2.2.12). ⊠

In the following, we are not concerned with the original definition of κ_j, involving a disk D_t with potentially small radius. Instead, we only work with the recurrences (2.2.9)–(2.2.12), which we restate here explicitly as a main result of this section:

$$\begin{aligned}\kappa_j(2t)&=\kappa_j(t)\quad\text{for all } j\ge 0;\\\kappa_2(2t+1)&=\frac{1}{2}\big(\kappa_2(t)+\kappa_2(t+1)\big)+1;\\\kappa_3(2t+1)&=\frac{1}{2}\big(\kappa_3(t)+\kappa_3(t+1)\big)+\frac{3}{2}\big(\kappa_2(t)-\kappa_2(t+1)\big);\\\kappa_4(2t+1)&=\frac{1}{2}\big(\kappa_4(t)+\kappa_4(t+1)\big)+2\big(\kappa_3(t)-\kappa_3(t+1)\big)\end{aligned}\tag{2.2.14}$$

$$
\begin{aligned}
&\quad + \frac{3}{4}\big(\kappa_2(t) - \kappa_2(t+1)\big)^2 - 2;\\
\kappa_5(2t+1) &= \frac{1}{2}\big(\kappa_5(t) + \kappa_5(t+1)\big) + \frac{5}{2}\big(\kappa_4(t) - \kappa_4(t+1)\big)\\
&\quad + \frac{5}{2}\big(\kappa_2(t) - \kappa_2(t+1)\big)\big(\kappa_3(t) - \kappa_3(t+1)\big)\\
&\quad - 10\big(\kappa_2(t) - \kappa_2(t+1)\big),
\end{aligned}
$$

for all integers $t \geq 0$. Note that $\kappa_2(t)$ is obviously nonnegative, since it is a variance; this can also easily be seen from this recurrence.

Remarks. Let us discuss some properties and other appearances of $\kappa_j(t)$.

1. The sequence κ_2 is 2-*regular* [3, 6, 7]. More precisely, we define

$$
B_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1/2 & 1/2 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 1/2 & 1/2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.2.15}
$$

   and

$$
S(n) = \begin{pmatrix} S_1(n) \\ S_2(n) \\ S_3(n) \end{pmatrix} = \begin{pmatrix} \kappa_2(n) \\ \kappa_2(n+1) \\ 1 \end{pmatrix}.
$$

   Then for all $n \geq 0$, the recurrence yields

$$
S(2n) = B_0 S(n), \qquad S(2n+1) = B_1 S(n). \tag{2.2.16}
$$

   Thus κ_2 is 2-regular, compare to [3, Theorem 2.2, item (e)].

   In this manner, we can also prove 2-regularity of $\kappa_3, \kappa_4, \kappa_5$. Considering for example the case κ_5, we introduce a sequence S_ℓ for each term that occurs in one of the recurrence formulas (2.2.14), such as $\kappa_2(n)\kappa_3(n+1)$; we see that it is sufficient to consider two 16×16-matrices.

2. The sequence $d_t = \kappa_2(t)/2$ appears in another context too: it is the *discrepancy of the van der Corput sequence* [43,143], and it satisfies $d_1 = 1$, $d_{2t} = d_t$, $d_{2t+1} = (d_t + d_{t+1} + 1)/2$. We do not know yet if this connection between our problem and discrepancy is a meaningful one. After all, it is no big surprise that one of the simplest 2-regular sequences occurs in two different problems concerning the binary expansion.

3. By the same method of proof (or alternatively, by concatenating the power series for log and $\gamma_t(\vartheta)$) the list in Lemma 2.2.1 can clearly be prolonged indefinitely. For the proof of our main theorem, however, we only need the terms up to κ_5. Without giving a rigorous proof, we note that this also shows that κ_j is 2-regular for all $j \geq 0$. Note the important property that lower cumulants always appear as differences; we believe that this behavior persists for higher cumulants.

4. More explicit values of $\kappa_j(1)$ can be easily computed from the closed form (2.2.3). Note that by (2.1.4) we know that these numbers are the cumulants of a geometric distribution with parameter $p = 1/2$ and given by the OEIS sequence `http://oeis.org/A000629A000629` with many other combinatorial connections.

In the next section we analyze an approximation of the cumulant generating function $\gamma_t(\vartheta)$ anticipating the fact that it captures all important properties for the subsequent proof.

2.2.2 An approximation of the cumulant generating function

Let us define the following approximation of γ_t. Set

$$\gamma_t^*(\vartheta) = \exp\left(\sum_{2\le j\le 5} \frac{\kappa_j(t)}{j!}(i\tau\vartheta)^j\right). \tag{2.2.17}$$

We are going to replace γ_t by γ_t^*, and for this purpose we have to bound the difference

$$\widetilde{\gamma}_t(\vartheta) = \gamma_t(\vartheta) - \gamma_t^*(\vartheta).$$

Clearly, we have $\widetilde{\gamma}_{2t}(\vartheta) = \widetilde{\gamma}_t(\vartheta)$. Moreover,

$$\begin{aligned}\widetilde{\gamma}_{2t+1}(\vartheta) &= \frac{\mathrm{e}(\vartheta)}{2}\big(\widetilde{\gamma}_t(\vartheta)+\gamma_t^*(\vartheta)\big) + \frac{\mathrm{e}(-\vartheta)}{2}\big(\widetilde{\gamma}_{t+1}+\gamma_{t+1}^*(\vartheta)\big) - \gamma_{2t+1}^*(\vartheta)\\ &= \frac{\mathrm{e}(\vartheta)}{2}\widetilde{\gamma}_t(\vartheta) + \frac{\mathrm{e}(-\vartheta)}{2}\widetilde{\gamma}_{t+1}(\vartheta) + \xi_t(\vartheta),\end{aligned} \tag{2.2.18}$$

where

$$\xi_t(\vartheta) = \frac{\mathrm{e}(\vartheta)}{2}\gamma_t^*(\vartheta) + \frac{\mathrm{e}(-\vartheta)}{2}\gamma_{t+1}^*(\vartheta) - \gamma_{2t+1}^*(\vartheta). \tag{2.2.19}$$

We prove the following rough bounds on differences of the cumulants κ_j.

Lemma 2.2.2. *We have*

$$|\kappa_2(t+1)-\kappa_2(t)| \le 2; \tag{2.2.20}$$
$$|\kappa_3(t+1)-\kappa_3(t)| \le 6; \tag{2.2.21}$$
$$|\kappa_4(t+1)-\kappa_4(t)| \le 28; \tag{2.2.22}$$
$$|\kappa_5(t+1)-\kappa_5(t)| \le 240. \tag{2.2.23}$$

Proof. We prove these statements by induction, inserting the recurrences (2.2.14). We have

$$\kappa_2(2t+1)-\kappa_2(2t) = \frac{\kappa_2(t)+\kappa_2(t+1)}{2} + 1 - \kappa_2(t) = \frac{\kappa_2(t+1)-\kappa_2(t)}{2} + 1$$

and

$$\kappa_2(2t+2)-\kappa_2(2t+1) = \kappa_2(t+1) - \frac{\kappa_2(t)+\kappa_2(t+1)}{2} + 1 = \frac{\kappa_2(t+1)-\kappa_2(t)}{2} - 1.$$

Then, by induction, the first statement is an easy consequence. Next, we consider the second inequality. From (2.2.14) we get

$$\begin{aligned}\kappa_3(2t+1)-\kappa_3(2t) &= \frac{\kappa_3(t+1)-\kappa_3(t)}{2} - \frac{3}{2}\big(\kappa_2(t+1)-\kappa_2(t)\big),\\ \kappa_3(2t+2)-\kappa_3(2t+1) &= \frac{\kappa_3(t+1)-\kappa_3(t)}{2} + \frac{3}{2}\big(\kappa_2(t+1)-\kappa_2(t)\big),\end{aligned}$$

and using the first part and induction, the claim follows. Concerning (2.2.22),

$$\begin{aligned}\kappa_4(2t+1)-\kappa_4(2t) = \frac{\kappa_4(t+1)-\kappa_4(t)}{2} &+ 2\big(\kappa_3(t)-\kappa_3(t+1)\big)\\ &+ \frac{3}{4}\big(\kappa_2(t)-\kappa_2(t+1)\big)^2 - 2,\end{aligned}$$

and the last three summands add up to a value bounded by 14 in absolute value, using the first two estimates and the fact that all cumulants are real numbers. An analogous statement for $\kappa_4(2t+2) - \kappa_4(2t+1)$ holds. This implies the third line. Finally,

$$\begin{aligned}\kappa_5(2t+1) - \kappa_5(2t) = \frac{\kappa_5(t+1) - \kappa_5(t)}{2} + \frac{5}{2}\big(\kappa_4(t) - \kappa_4(t+1)\big) \\ + \frac{5}{2}\big(\kappa_2(t) - \kappa_2(t+1)\big)\big(\kappa_3(t) - \kappa_3(t+1)\big) - 10\big(\kappa_2(t) - \kappa_2(t+1)\big),\end{aligned}$$

and the sum of the last three summands is bounded by 120 in absolute value. In complete analogy to the above, this implies (2.2.23). ⛒

Corollary 2.2.3. *There exists a constant C such that for all t having M blocks of $\mathtt{1}$s we have*

$$|\kappa_2(t)| \le CM, \quad |\kappa_3(t)| \le CM, \quad |\kappa_4(t)| \le CM, \quad |\kappa_5(t)| \le CM.$$

Proof. We proceed by induction on the number of blocks of $\mathtt{1}$s in t. Appending $\mathtt{0}^r$ to the binary expansion, there is nothing to show by the identity $\kappa_j(2t) = \kappa_j(t)$. We append a block of $\mathtt{1}$s of length r: Using the following (trivial) identity

$$\kappa_j\big(2^r t + 2^r - 1\big) = \kappa_j(t) + \big(\kappa_j\big(2^r t + 2^r - 1\big) - \kappa_j(t+1)\big) - \big(\kappa_j(t) - \kappa_j(t+1)\big),$$

and since $\kappa_j\big(\big(2^r t + 2^r - 1\big) + 1\big) = \kappa_j(t+1)$ due to $\kappa_j(2t) = \kappa_j(t)$, the result follows by Lemma 2.2.2. ⛒

The following lower bound is [143, Lemma 3.1], and essentially contained in [43]; see also [55].

Lemma 2.2.4. *Let M be the number of blocks of $\mathtt{1}$s in t. Then $\kappa_2(t) \ge M$.*

We prove the following upper bound for $\widetilde{\gamma}_t(\vartheta)$, using the recurrence (2.2.14) as an essential input. This proposition is the central property in our proof of the main theorem, showing the crucial uniformity of our approximation.

Proposition 2.2.5. *There exists a constant C such that for $|\vartheta| \le \min\big(M^{-1/6}, \tau^{-1}\big)$ we have*

$$\begin{aligned}\big|\widetilde{\gamma}_t(\vartheta)\big| &\le CM\vartheta^6, \\ \big|\xi_t(\vartheta)\big| &\le C\vartheta^6,\end{aligned}$$

where M is the number of blocks of $\mathtt{1}$s in t.

Proof. From (2.2.17) and (2.2.18) we see that by construction $\widetilde{\gamma}_t(\vartheta) = \mathcal{O}(\vartheta^6)$ and $\xi_t(\vartheta) = \mathcal{O}(\vartheta^6)$ as the Taylor coefficients at $\vartheta = 0$ of $\gamma_t(\vartheta)$ and $\gamma_t'(\vartheta)$ up to ϑ^5 are the same. It remains to show that the constants are effective and uniform in t. To begin with, there is a constant C such that (2.2.24) holds for $t \in \{0, 1\}$; a numerical value can be extracted from the first few $\widetilde{\gamma}_t(\vartheta)$ and $\xi_t(\vartheta)$, which have explicit expansions.

We proceed by induction on the length L of the binary expansion of t. As induction hypothesis, we choose the following strengthened statement:

$$\begin{aligned}\big|\widetilde{\gamma}_t(\vartheta)\big| &\le 2CM\vartheta^6; \\ \big|\widetilde{\gamma}_{t+1}(\vartheta)\big| &\le 2CM\vartheta^6; \\ \big|\xi_t(\vartheta)\big| &\le C\vartheta^6\end{aligned} \tag{2.2.24}$$

for all t whose binary expansion has a length bounded by L, and for all real ϑ satisfying $|\vartheta| \le 1/\tau$ and $|\vartheta| \le M^{-1/6}$, where M is the number of blocks in t.

Note that in this proof, and in this proof only, we use the total number of blocks instead of the number of blocks of 1s because this works well with the induction statement. The statement of the proposition is not changed by this, since the numbers of blocks of 0s and blocks of 1s differ at most by one.

The statement holds for $t \in \{0,1\}$. We therefore assume that (2.2.24) holds for all t whose binary expansion has a length strictly less than L, where $L \geq 2$. Our strategy is now to first prove the inequalities for $\widetilde{\gamma}_t(\vartheta)$ and $\widetilde{\gamma}_{t+1}(\vartheta)$, and after that the one for $\xi_t(\vartheta)$. In order to make the interplay between the statements in the induction hypothesis explicit, we rewrite (2.2.18) as a matrix recurrence for $t \geq 1$:

$$\begin{pmatrix} \widetilde{\gamma}_{2t}(\vartheta) \\ \widetilde{\gamma}_{2t+1}(\vartheta) \end{pmatrix} = A_0 \begin{pmatrix} \widetilde{\gamma}_t(\vartheta) \\ \widetilde{\gamma}_{t+1}(\vartheta) \end{pmatrix} + \begin{pmatrix} 0 \\ \xi_t(\vartheta) \end{pmatrix} \quad \text{with} \quad A_0 = \begin{pmatrix} 1 & 0 \\ \frac{\mathrm{e}(\vartheta)}{2} & \frac{\mathrm{e}(-\vartheta)}{2} \end{pmatrix};$$

$$\begin{pmatrix} \widetilde{\gamma}_{2t+1}(\vartheta) \\ \widetilde{\gamma}_{2t+2}(\vartheta) \end{pmatrix} = A_1 \begin{pmatrix} \widetilde{\gamma}_t(\vartheta) \\ \widetilde{\gamma}_{t+1}(\vartheta) \end{pmatrix} + \begin{pmatrix} \xi_t(\vartheta) \\ 0 \end{pmatrix} \quad \text{with} \quad A_1 = \begin{pmatrix} \frac{\mathrm{e}(\vartheta)}{2} & \frac{\mathrm{e}(-\vartheta)}{2} \\ 0 & 1 \end{pmatrix}.$$

The idea is now to use these relations to reduce the length of t. For this purpose, we regard the run of 0s or 1s at the very right of the binary expansion of t.

First, if we have a run of 0s, we can write $t = 2^k t'$, where t' is odd. Iterating the first matrix equation above, we accumulate powers of A_0:

$$\begin{aligned} \begin{pmatrix} \widetilde{\gamma}_{2^k t'}(\vartheta) \\ \widetilde{\gamma}_{2^k t'+1}(\vartheta) \end{pmatrix} &= A_0^k \begin{pmatrix} \widetilde{\gamma}_{t'}(\vartheta) \\ \widetilde{\gamma}_{t'+1}(\vartheta) \end{pmatrix} + \sum_{0 \leq j < k} A_0^{k-1-j} \begin{pmatrix} 0 \\ \xi_{2^\ell t'}(\vartheta) \end{pmatrix} \\ &= A_0^k \begin{pmatrix} \widetilde{\gamma}_{t'}(\vartheta) \\ \widetilde{\gamma}_{t'+1}(\vartheta) \end{pmatrix} + \begin{pmatrix} 0 \\ E_0(\vartheta) \end{pmatrix}, \end{aligned}$$

where, due to $\mathrm{e}(\vartheta)^j = \mathrm{e}(j\vartheta)$, we have

$$E_0(\vartheta) = \sum_{0 \leq j < k} \frac{\mathrm{e}(-(k-1-j)\vartheta)}{2^{k-1-j}} \xi_{2^j t'}(\vartheta),$$

which satisfies

$$\big|E_0(\vartheta)\big| \leq 2 \max_{0 \leq j < k} \big|\xi_{2^j t'}(\vartheta)\big|.$$

Now, the binary length of $2^j t'$ is strictly less than the binary length of t, therefore we can use our hypothesis in order to conclude that $|E_0(\vartheta)| \leq 2C\vartheta^6$. Moreover, the number M' of blocks (of 0s or 1s) in t' is the number M of blocks in t decreased by one (since t' is odd). By the hypothesis and the fact that A_0 has row-sum norm equal to 1, we obtain $\big|\widetilde{\gamma}_t(\vartheta)\big| \leq 2CM\vartheta^6$ and $\big|\widetilde{\gamma}_{t+1}(\vartheta)\big| \leq 2CM\vartheta^6$ for $t = 2^k t'$.

Second, appending a block of 1s to an even integer t', we obtain from the second matrix equation

$$\begin{pmatrix} \widetilde{\gamma}_{2^k t'+2^k-1}(\vartheta) \\ \widetilde{\gamma}_{2^k(t'+1)}(\vartheta) \end{pmatrix} = A_1^k \begin{pmatrix} \widetilde{\gamma}_{t'}(\vartheta) \\ \widetilde{\gamma}_{t'+1}(\vartheta) \end{pmatrix} + \begin{pmatrix} E_1(\vartheta) \\ 0 \end{pmatrix},$$

where

$$E_1(\vartheta) = \sum_{0 \leq j < k} \frac{\mathrm{e}(-(k-1-j)\vartheta)}{2^{k-1-j}} \xi_{2^j t'+2^j-1}(\vartheta)$$

satisfies

$$\big|E_1(\vartheta)\big| \le 2 \max_{0\le j<k} \big|\xi_{2^j t'+2^j-1}(\vartheta)\big|.$$

As above, we have by our induction hypothesis $E_1(\vartheta) \le 2C\vartheta^6$. Then, since the integer t' has one block less than t and since A_1 has row-sum norm equal to 1, we can use our induction hypothesis (2.2.24) and get $|\widetilde{\gamma}_t(\vartheta)| \le 2CM\vartheta^6$ and $|\widetilde{\gamma}_{t+1}(\vartheta)| \le 2CM\vartheta^6$ for $t = 2^k t' + 2^k - 1$.

It remains to consider the inequality for $\xi_t(\vartheta)$. We start by dividing Equation (2.2.19) by $\gamma_t^*(\vartheta)$. This gives

$$\begin{aligned}\frac{\xi_t(\vartheta)}{\gamma_t^*(\vartheta)} = \frac{\mathrm{e}(\vartheta)}{2} + \frac{\mathrm{e}(-\vartheta)}{2} \exp\Bigg(\sum_{2\le j\le 5} \frac{\kappa_j(t+1)-\kappa_j(t)}{j!}(i\tau\vartheta)^j\Bigg) \\ - \exp\Bigg(\sum_{2\le j\le 5} \frac{\kappa_j(2t+1)-\kappa_j(t)}{j!}(i\tau\vartheta)^j\Bigg)\end{aligned} \tag{2.2.25}$$

As observed before, we have $\xi_t(\vartheta) = \mathcal{O}(\vartheta^6)$ and consequently, dividing by the power series $\gamma_t^*(\vartheta) = 1 + \mathcal{O}(\vartheta^2)$, we see that the series of the right hand side also belongs to $\mathcal{O}(\vartheta^6)$. Next, we get by the triangle inequality and the induction hypothesis

$$\big|\gamma_t^*(\vartheta)\big| \le \big|\gamma_t(\vartheta)\big| + \big|\widetilde{\gamma}_t(\vartheta)\big| \le 1 + 2CM\vartheta^6$$

and since $\vartheta \le M^{-1/6}$, we obtain

$$\big|\gamma_t^*(\vartheta)\big| = \mathcal{O}(1).$$

Now we turn our attention to the right hand side of (2.2.25), where we will treat each summand separately. The first term $\mathrm{e}(\vartheta)/2$ has $(i\,\tau)^k/(2\cdot k!)$ as coefficients; since $\tau\vartheta \le 1$, the contribution of the coefficients for $k \ge 6$ is bounded by

$$\frac{1}{2}\sum_{k\ge 6}\frac{(\tau\vartheta)^k}{k!} \le \frac{1}{2}(\tau\vartheta)^6(e - 163/60) < \frac{1}{1234}(\tau\vartheta)^6.$$

Next, we want to show that the contribution of the second term (i.e., the product of two exponentials) and the third term are each bounded by $C(\tau\vartheta)^6$. By Lemma 2.2.2, an upper bound for the coefficients of the second term is given by the coefficients of

$$f(\vartheta) = \exp\big(2\big((\tau\vartheta) + \cdots + (\tau\vartheta)^5\big)\big).$$

Clearly, the term ϑ^k in the j-fold product $(\vartheta + \vartheta^2 + \cdots + \vartheta^5)^j$ appears at most 5^j times, but only for $j \ge k/5$. Therefore the coefficient $[\vartheta^k]f(\vartheta)$ is bounded by

$$\tau^k \sum_{k/5\le j\le k} 2^j \frac{5^j}{j!} \le \tau^k \sum_{j\ge k/5} \frac{10^j}{j!}.$$

Consequently, as we only need to consider coefficients of ϑ^k with $k \ge 6$, and since $|\tau\vartheta| \le 1$, we get

$$\sum_{k\ge 6}\vartheta^k\big[\vartheta^k\big]f(\vartheta) \le (\tau\vartheta)^6 \sum_{k\ge 6}\sum_{j\ge k/5}\frac{10^j}{j!} \le 5(\tau\vartheta)^6\sum_{j\ge 1}\frac{10^j j}{j!} \le C'\vartheta^6$$

for some absolute constant C'. The same holds for the third exponential in (2.2.25), as $|\kappa_j(2t+1)-\kappa_j(t)| = |\kappa_j(2t+1)-\kappa_j(2t)| \le 240$. Collecting these results we get an absolute and effective constant C such that $|\xi_t(\vartheta)| \le C\vartheta^6$ as long as $\vartheta \le M^{-1/6}$ and $|\tau\vartheta| \le 1$. ⛒

2.2.3 An integral representation of c_t

We use the following representation of the values c_t.

Proposition 2.2.6 ([148, Proposition 2.1]). *Let $t \geq 0$. We have*

$$c_t = \frac{1}{2} + \frac{\delta(0,t)}{2} + \frac{1}{2}\int_{-1/2}^{1/2} \operatorname{Im}\gamma_t(\vartheta)\cot(\pi\vartheta)\,\mathrm{d}\vartheta, \tag{2.2.26}$$

where the integrand is a bounded, continuous function.

We split the integral at the points $\pm\vartheta_0$, where $\vartheta_0 = M^{-1/2}R$. Here M is the number of blocks of 1s in t and R is a small parameter to be chosen in a moment. For now, we assume that

$$8 \leq R \leq M^{1/3} \quad \text{and} \quad \vartheta_0 \leq 1/\tau \tag{2.2.27}$$

for technical reasons as, among others, we need to apply Proposition 2.2.5. Note that under these hypotheses,

$$\vartheta_0 \leq M^{-1/6},$$

so that the proposition will be applicable. We will choose $R = \log M$; then (2.2.27) will be satisfied for large M. The tails of the above integral will be estimated using the following lemma.

Lemma 2.2.7 ([148, Lemma 2.7]). *Assume that $t \geq 1$ has at least $M = 2M' + 1$ blocks of 1s. Then*

$$|\gamma_t(\vartheta)| \leq \left(1 - \frac{\vartheta^2}{2}\right)^{M'} \leq \exp\left(-\frac{M'\vartheta^2}{2}\right) \leq 2\exp\left(-\frac{M\vartheta^2}{4}\right)$$

for $|\vartheta| \leq 1/2$.

We have $\cot(x) = 1/x + \mathcal{O}(1)$ for $x \leq 1/2$. The contribution of the tail can therefore be bounded by

$$\int_{M^{-1/2}R}^{1/2} \exp\left(-\frac{M\vartheta^2}{4}\right)\cot(\pi\vartheta)\,\mathrm{d}\vartheta \leq \frac{1}{\pi}I + \mathcal{O}\left(J\right),$$

where

$$I = \int_{M^{-1/2}R}^{\infty} \exp\left(-\frac{M\vartheta^2}{4}\right)\frac{\mathrm{d}\vartheta}{\vartheta}$$

and

$$J = \int_{M^{-1/2}R}^{\infty} \exp\left(-\frac{M\vartheta^2}{4}\right)\mathrm{d}\vartheta.$$

The integral J is bounded by

$$\mathcal{O}\left(\exp\bigl(-M(M^{-1/2}R)^2/4\bigr)\right) = \mathcal{O}\left(\exp\bigl(-R^2/4\bigr)\right).$$

In order to estimate I, we write

$$I \leq \sum_{j\geq 0}\int_{2^j\vartheta_0}^{2^{j+1}\vartheta_0} \exp\left(-\frac{M\vartheta^2}{4}\right)\frac{\mathrm{d}\vartheta}{2^j\vartheta_0} \leq \sum_{j\geq 0}\exp\left(-\frac{4^jR^2}{4}\right).$$

Using the hypothesis $R \geq 1$, this is easily shown to be bounded by $\mathcal{O}\left(\exp\bigl(-R^2/4\bigr)\right)$ by a geometric series. For $|\vartheta| \leq \vartheta_0$, we replace $\gamma_t(\vartheta)$ by $\gamma_t^*(\vartheta)$ in the integral in (2.2.26), using

Proposition 2.2.5. Noting the hypotheses (2.2.27), we obtain $|\gamma_t(\vartheta) - \gamma_t^*(\vartheta)| \ll M|\vartheta|^6$, where M is the number of blocks in t. Therefore

$$\begin{aligned}\int_{-1/2}^{1/2} \operatorname{Im}\gamma_t(\vartheta)\cot(\pi\vartheta)\,\mathrm{d}\vartheta &= \int_{-\vartheta_0}^{\vartheta_0} \operatorname{Im}\gamma_t(\vartheta)\cot(\pi\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}\big(\exp\big(-R^2/4\big)\big)\\ &= \int_{-\vartheta_0}^{\vartheta_0} \operatorname{Im}\gamma_t^*(\vartheta)\cot(\pi\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}\left(M\int_0^{\vartheta_0}\vartheta^5\,\mathrm{d}\vartheta\right) + \mathcal{O}\big(\exp\big(-R^2/4\big)\big) \qquad (2.2.28)\\ &= \int_{-\vartheta_0}^{\vartheta_0} \operatorname{Im}\gamma_t^*(\vartheta)\cot(\pi\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}(E),\end{aligned}$$

where, due to $\vartheta_0 = M^{-1/2}R$, we have

$$E = M^{-2}R^6 + \exp\big(-R^2/4\big).$$

Similarly, combining (2.2.1) with the above reasoning, we get

$$\delta(0,t) = \int_{-\vartheta_0}^{\vartheta_0} \operatorname{Re}\gamma_t^*(\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}(E). \qquad (2.2.29)$$

Next we return to the definition of $\gamma_t^*(\vartheta)$ from (2.2.17). By the Taylor expansion of exp, using Corollary 2.2.3, we have for $|\vartheta| \le \vartheta_0$

$$\begin{aligned}\gamma_t^*(\vartheta) = \exp\left(-\kappa_2(t)\frac{(\tau\vartheta)^2}{2}\right) &\times \Big(1 + \frac{\kappa_3(t)}{6}(i\tau\vartheta)^3 + \frac{\kappa_4(t)}{24}(i\tau\vartheta)^4 + \frac{\kappa_5(t)}{120}(i\tau\vartheta)^5\\ &+\frac{1}{72}\kappa_3(t)^2(i\tau\vartheta)^6 + \frac{1}{144}\kappa_3(t)\kappa_4(t)(i\tau\vartheta)^7 + \frac{1}{1296}\kappa_3(t)^3(i\tau\vartheta)^9\Big)\\ &+ \mathcal{O}\big(M^2\vartheta^8 + M^3\vartheta^{10}\big) + i\mathcal{O}\big(M^2\vartheta^9 + M^3\vartheta^{11}\big),\end{aligned}$$

where both error terms are real. We note that $\cot(\pi\vartheta) = 2/(\tau\vartheta) - \tau\vartheta/6 + \mathcal{O}(\vartheta^3)$ for $|\vartheta| \le 1/2$. Splitting into real and imaginary summands, of which there are three and four, respectively, we obtain by (2.2.28) and (2.2.29)

$$\begin{aligned}c_t &= \frac{1}{2} + \frac{1}{2}\int_{-\vartheta_0}^{\vartheta_0} \exp\left(-\kappa_2(t)\frac{(\tau\vartheta)^2}{2}\right)\left(1 + \frac{\kappa_4(t)}{24}(\tau\vartheta)^4 - \frac{1}{72}\kappa_3(t)^2(\tau\vartheta)^6\right.\\ &\quad+\Big(-\frac{1}{6}\kappa_3(t)(\tau\vartheta)^3 + \frac{1}{120}\kappa_5(t)(\tau\vartheta)^5 - \frac{1}{144}\kappa_3(t)\kappa_4(t)(\tau\vartheta)^7\\ &\quad\left.+\frac{1}{1296}\kappa_3(t)^3(\tau\vartheta)^9\Big)\cot(\pi\vartheta)\right)\mathrm{d}\vartheta + \mathcal{O}\big(E + E_2\big)\\ &= \frac{1}{2} + \frac{1}{2}\int_{-\vartheta_0}^{\vartheta_0} \exp\left(-\kappa_2(t)\frac{(\tau\vartheta)^2}{2}\right)\left(1 + \frac{\kappa_4(t)}{24}(\tau\vartheta)^4 - \frac{\kappa_3(t)^2}{72}(\tau\vartheta)^6 - \frac{\kappa_3(t)}{3}(\tau\vartheta)^2\right.\\ &\quad\left.+\frac{\kappa_5(t)}{60}(\tau\vartheta)^4 - \frac{\kappa_3(t)\kappa_4(t)}{72}(\tau\vartheta)^6 + \frac{\kappa_3(t)^3}{648}(\tau\vartheta)^8 + \frac{\kappa_3(t)}{36}(\tau\vartheta)^4\right)\mathrm{d}\vartheta + \mathcal{O}\big(E + E_2\big),\end{aligned}$$

where

$$E_2 = \int_{-\vartheta_0}^{\vartheta_0}\big(M\vartheta^6 + M^2\vartheta^8 + M^3\vartheta^{10}\big)\,\mathrm{d}\vartheta \ll M^{-5/2}R^{11}.$$

We extend the integration limits again, introducing an error

$$E_3 \ll \int_{M^{-1/2}R}^{\infty} \exp\left(-\kappa_2(t)\frac{\vartheta^2}{2}\right)\big(1 + M\vartheta^2 + M\vartheta^4 + M^2\vartheta^6 + M^3\vartheta^8\big).$$

In order to estimate this, we use the following lemma.

Lemma 2.2.8. *For real numbers $a > 0$ and $\delta \geq 0$, and integers $j \geq 0$, we define*

$$I_j = \int_\delta^\infty x^j \exp(-ax^2).$$

Then

$$\begin{aligned}
I_2 &\ll \frac{\delta}{a}\exp\bigl(-a\delta^2\bigr),\\
I_4 &\ll \left(\frac{\delta^3}{a} + \frac{\delta}{a^2}\right)\exp\bigl(-a\delta^2\bigr),\\
I_6 &\ll \left(\frac{\delta^5}{a} + \frac{\delta^3}{a^2} + \frac{\delta}{a^3}\right)\exp\bigl(-a\delta^2\bigr),\\
I_8 &\ll \left(\frac{\delta^7}{a} + \frac{\delta^5}{a^2} + \frac{\delta^3}{a^3} + \frac{\delta}{a^4}\right)\exp\bigl(-a\delta^2\bigr).
\end{aligned}$$

Proof. We have

$$\frac{\partial}{\partial x}x^m\exp\bigl(-ax^2\bigr) = \bigl(mx^{m-1} - 2ax^{m+1}\bigr)\exp\bigl(-ax^2\bigr),$$

therefore

$$I_{m+1} = -\frac{x^m}{2a}\exp(-ax^2)\Big|_\delta^\infty + \frac{m}{2a}I_{m-1}.$$

Noting that $I_0 \ll \exp\bigl(-a\delta^2\bigr)$, we obtain the above estimates by recurrence. ⊠

We insert $a = \kappa_2(t)/2$ and $\delta = \vartheta_0$. By Lemma 2.2.4 we have $a \geq M/2 > 0$, and by our hypothesis (2.2.27) we have $R \leq M^{1/6}$, which implies in particular that $\delta = M^{-1/2}R \leq 1$. By these estimates and Lemma 2.2.8, we obtain

$$\begin{aligned}
E_3 &\ll \Bigl(1 + M^{-1/2}R + M^{-3/2}R^7\Bigr)\exp\Bigl(-\kappa_2(t)(M^{-1/2}R)^2/2\Bigr)\\
&\ll \exp\bigl(-R^2/2\bigr) \ll E.
\end{aligned}$$

Substituting $\tau\vartheta$ by ϑ, we obtain

$$\begin{aligned}
c_t = \frac{1}{2} + \frac{1}{2\tau}\int_{-\infty}^{\infty}\exp\left(-\kappa_2(t)\frac{\vartheta^2}{2}\right)\left(1 - \frac{\kappa_3(t)}{3}\vartheta^2 + \left(\frac{\kappa_3(t)}{36} + \frac{\kappa_4(t)}{24} + \frac{\kappa_5(t)}{60}\right)\vartheta^4\right.\\
\left. + \left(-\frac{\kappa_3(t)}{72} - \frac{\kappa_4(t)}{72}\right)\kappa_3(t)\vartheta^6 + \frac{\kappa_3(t)^3}{648}\vartheta^8\right)\mathrm{d}\vartheta + \mathcal{O}\bigl(E + E_2\bigr).
\end{aligned}$$

Inserting standard Gaussian integrals, it follows that

$$\begin{aligned}
c_t = \frac{1}{2} + \frac{\sqrt{2}}{4\sqrt{\pi}}\Bigg(&\kappa_2(t)^{-1/2} - \frac{\kappa_2(t)^{-3/2}\kappa_3(t)}{3}\\
&+ 3\kappa_2(t)^{-5/2}\left(\frac{\kappa_3(t)}{36} + \frac{\kappa_4(t)}{24} + \frac{\kappa_5(t)}{60}\right)\\
&+ 15\kappa_2(t)^{-7/2}\left(-\frac{\kappa_3(t)}{72} - \frac{\kappa_4(t)}{72}\right)\kappa_3(t) + 105\kappa_2(t)^{-9/2}\frac{\kappa_3(t)^3}{648}\Bigg)\\
&+ \mathcal{O}\left(M^{-2}R^{11} + \exp\bigl(-R^2/4\bigr)\right)
\end{aligned} \tag{2.2.30}$$

under the hypotheses that $8 \le R \le M^{1/6}$ and $M^{-1/2}R \le 1/\tau$, where M is the number of blocks of 1s in t. The multiplicative constant in the error term is absolute, as customary in this paper. In order to simplify the error term, we choose

$$R = \log M. \tag{2.2.31}$$

Using the hypothesis $R \ge 8$, we have $\exp\bigl(-R^2/4\bigr) \le M^{-2}$. Then, since $\kappa_2(t) \ge 0$ for all t, we see that for $c_t > 1/2$ it is sufficient to prove

$$v(t) \ge 0,$$

where

$$\begin{aligned} v(t) = \kappa_2(t)^4 - \kappa_2(t)^3\frac{\kappa_3(t)}{3} + \kappa_2(t)^2\biggl(\frac{\kappa_3(t)}{12} + \frac{\kappa_4(t)}{8} + \frac{\kappa_5(t)}{20}\biggr) \\ + 5\kappa_2(t)\biggl(-\frac{\kappa_3(t)}{24} - \frac{\kappa_4(t)}{24}\biggr)\kappa_3(t) + 35\frac{\kappa_3(t)^3}{216} - C\kappa_2(t)^{5/2}R^{11}. \end{aligned} \tag{2.2.32}$$

and C is large enough such that the error term in (2.2.30) is strictly dominated by $C\kappa_2(t)^{5/2}M^{-2}R^{11}$. Usually the first term is the dominant one; the critical cases occur when the first two terms in (2.2.32) almost cancel. We couple these terms and write

$$D = D(t) = \kappa_2(t) - \frac{\kappa_3(t)}{3}.$$

Let us rewrite the expression for $v(t)$, eliminating $\kappa_3(t)$. Clearly, we have $\kappa_3(t)^2 = 9\kappa_2(t)^2 - 18D\kappa_2(t) + 9D^2$ and $\kappa_3(t)^3 = 27\kappa_3(t)^3 - 81D\kappa_3(t)^2 + 81D^2\kappa_3(t) - 27D^3$. Omitting the argument t of the functions κ_j for brevity, we obtain

$$\begin{aligned} v(t) &= D\kappa_2^3 + \frac{1}{4}\kappa_2^3 - \frac{1}{4}D\kappa_2^2 + \frac{1}{8}\kappa_2^2\kappa_4 + \frac{1}{20}\kappa_2^2\kappa_5 \\ &\quad - \frac{15}{8}\kappa_2^3 + \frac{15}{4}D\kappa_2^2 - \frac{15}{8}D^2\kappa_2 - \frac{5}{8}\kappa_2^2\kappa_4 + \frac{5}{8}D\kappa_2\kappa_4 \\ &\quad + \frac{35}{8}\biggl(\kappa_2^3 - 3D\kappa_2^2 + 3D^2\kappa_2 - D^3\biggr) - C\kappa_2^{5/2}R^{11} \\ &= \biggl(D + \frac{11}{4}\biggr)\kappa_2^3 - \frac{1}{2}\kappa_2^2\kappa_4 + \frac{1}{20}\kappa_2^2\kappa_5 - \frac{77}{8}D\kappa_2^2 \\ &\quad + \frac{5}{8}D\kappa_2\kappa_4 + \frac{45}{4}D^2\kappa_2 - \frac{35}{8}D^3 - C\kappa_2^{5/2}R^{11}. \end{aligned} \tag{2.2.33}$$

We distinguish between small and large values of D. Note that $|\kappa_j| \le CM$, $D \le CM$ for some absolute constant C (expressed in Corollary 2.2.3), moreover $\kappa_2 \ge M$ (Proposition 2.2.4) and $R = \log M$. Thus, we have $|\kappa_j| \le C\kappa_2$ and $D \le C\kappa_2$. Therefore there exists an absolute constant D_0 (which could be made explicit easily) such that

$$v(t) \ge \bigl(D(t) - D_0\bigr)\kappa_2(t)^3 \tag{2.2.34}$$

for all $t \ge 1$. Clearly this implies $v(t) \ge 0$ for all t such that $D(t) \ge D_0$. We have therefore proved the following result.

Lemma 2.2.9. *There exists a constant D_0 such that, if $\kappa_2(t) - \kappa_3(t)/3 \ge D_0$, then $c_t > 1/2$.*

The remainder of the proof of Theorem 2.1.1 is concerned with the case $D(t) < D_0$. As D_0 is an absolute constant, independent of t and M, we see that $D(t)/\kappa_2(t)^\lambda$ with $\lambda > 0$ becomes arbitrarily small when the number of blocks in t increase. Thus, we obtain from (2.2.33) the following statement: for all $\varepsilon > 0$ there is an M_0 such that for $M \geq M_0$ we have

$$v(t) \geq \left(D + \frac{11}{4} - \varepsilon\right)\kappa_2^3 - \frac{1}{2}\kappa_2^2\kappa_4 + \frac{1}{20}\kappa_2^2\kappa_5. \tag{2.2.35}$$

We proceed by taking a closer look at the values $D(t)$. We have

$$D(2t+1) = \frac{\kappa_2(t)+\kappa_2(t+1)}{2} - \frac{\kappa_3(t)+\kappa_3(t+1)}{6} - \frac{\kappa_2(t)-\kappa_2(t+1)}{2} + 1,$$

therefore

$$D(2t) = D(t) \quad \text{and} \quad D(2t+1) = \frac{D(t)+D(t+1)}{2} + \frac{\kappa_2(t+1)-\kappa_2(t)}{2} + 1. \tag{2.2.36}$$

By (2.2.13), we have $D(1) = D(2) = 4$, moreover the term $(\kappa_2(t+1)-\kappa_2(t))/2+1$ is nonnegative by Lemma 2.2.2. This implies

$$D(t) \geq 4. \tag{2.2.37}$$

Choosing $\varepsilon = 1/8$ in (2.2.35), we see that it remains to show that

$$53\kappa_2 - 4\kappa_4 + \frac{2}{5}\kappa_5 > 0 \tag{2.2.38}$$

if t contains many blocks, and $D(t)$ is bounded by some absolute constant D_0.

This is done in two steps: first, we determine the structure of the exceptional set of integers t such that $D(t)$ is bounded. We will see that such an integer has few blocks of `0`s of length ≥ 2, and few blocks of `1`s of bounded length. As a second step, we prove lower bounds for the numbers $-\kappa_4(t)$ and $\kappa_5(t)$, if t is contained in this exceptional set.

2.2.4 Determining the exceptional set

We define the exceptional set

$$\{t : D(t) < D_0\},$$

where D_0 is the constant from Lemma 2.2.9. In this section we will derive some structural properties of its elements.

We begin with investigating the effect of appending a block of the form $\mathtt{01}^k$.

Lemma 2.2.10. *For $t \geq 0$ and $k \geq 0$ we have*

$$\kappa_2(2^{k+1}t + 2^k - 1) = \frac{(2^k+1)\kappa_2(t)}{2^{k+1}} + \frac{(2^k-1)\kappa_2(t+1)}{2^{k+1}} + \frac{3\left(2^k-1\right)}{2^k}, \tag{2.2.39}$$

$$\begin{aligned} D(2^{k+1}t + 2^k - 1) = {} & \frac{2^k+1}{2^{k+1}}D(t) + \frac{2^k-1}{2^{k+1}}D(t+1) \\ & + \left(\frac{1}{2} + \frac{k-1}{2^{k+1}}\right)\big(\kappa_2(t+1)-\kappa_2(t)\big) + 1 + \frac{3k-1}{2^k}. \end{aligned} \tag{2.2.40}$$

Proof. The proof of the first part is easy, using induction and the recurrence (2.2.14).

We continue with the second part. The statement is trivial for $k = 0$ and for $k = 1$ it follows from (2.2.39). We use the abbreviations $\rho_k = 1/2 + (k-1)/2^{k+1}$ and $\sigma_k = 1 + (3k-1)/2^k$. For $k \geq 1$ we have by induction, using (2.2.36) and (2.2.39),

$$\begin{aligned}
D(2^{k+2}t + 2^{k+1} - 1) &= \frac{D(2^{k+1}t + 2^k - 1) + D(2t+1)}{2} \\
&\quad + \frac{\kappa_2(2t+1) - \kappa_2(2^{k+1}t + 2^k - 1)}{2} + 1 \\
&= \frac{2^k+1}{2^{k+2}} D(t) + \frac{2^k-1}{2^{k+2}} D(t+1) + \frac{\rho_k}{2}\big(\kappa_2(t+1) - \kappa_2(t)\big) + \frac{\sigma_k}{2} \\
&\quad + \frac{D(t) + D(t+1)}{4} + \frac{\kappa_2(t+1) - \kappa_2(t)}{4} + \frac{1}{2} + \frac{\kappa_2(t) + \kappa_2(t+1)}{4} + \frac{1}{2} \\
&\quad - \frac{1}{2}\left(\frac{2^k+1}{2^{k+1}}\kappa_2(t) + \frac{2^k-1}{2^{k+1}}\kappa_2(t+1) + 3\frac{2^k-1}{2^k}\right) + 1 \\
&= \frac{2^{k+1}+1}{2^{k+2}} D(t) + \frac{2^{k+1}-1}{2^{k+2}} D(t+1) + \left(\frac{\rho_k}{2} + \frac{1}{4} + \frac{1}{2^{k+2}}\right)\big(\kappa_2(t+1) - \kappa_2(t)\big) \\
&\quad + \frac{\sigma_k}{2} + \frac{1}{2} + \frac{3}{2^{k+1}},
\end{aligned}$$

which implies the statement. ⊠

We obtain the following corollary.

Corollary 2.2.11. *For all $t \geq 0$ and $k \geq 1$ we have*

$$D\big(2^{k+1}t + 2^k - 1\big) \geq \min\big(D(t), D(t+1)\big) + \frac{k}{2^{k-1}}.$$

Proof. Set $\alpha = \big(2^k+1\big)/2^{k+1}$ and $\beta = \big(2^k-1\big)/2^{k+1}$. By the bound $|\kappa_2(t+1) - \kappa_2(t)| \leq 2$ from Lemma 2.2.2, it follows from Equation (2.2.40) that

$$\begin{aligned}
D\big(2^{k+1}t + 2^k - 1\big) &\geq \alpha D(t) + \beta D(t+1) + \frac{1}{2}\big(\kappa_2(t+1) - \kappa_2(t) + 2\big) + \frac{k}{2^{k-1}} \\
&\geq \min\big(D(t), D(t+1)\big) + \frac{k}{2^{k-1}}.
\end{aligned}$$

⊠

We can now extract the contribution to the value of D of a block of the form $\mathtt{01}^k\mathtt{0}$. For this, we use the notation

$$m(t) = \min\big(D(t), D(t+1)\big).$$

This notation is introduced in order to obtain the following *monotonicity property*: by the recurrence (2.2.36) and the nonnegativity of $a(t) = \big(\kappa_2(t+1) - \kappa_2(t)\big)/2 + 1$ we have

$$\begin{aligned}
\min\big(m(2t), m(2t+1)\big) &= \min\left(D(t), \frac{D(t) + D(t+1)}{2} + a(t), D(t+1)\right) \\
&\geq \min\big(D(t), D(t+1)\big) = m(t)
\end{aligned} \tag{2.2.41}$$

Note also $m(t) \geq 4$ by (2.2.37). These properties will be used in an essential way in the important Corollary 2.2.13 below, where an induction along the binary expansion of t is used.

Corollary 2.2.12. *For all $t \geq 0$ and $k \geq 1$ we have*

$$m(2^{k+2}t + 2^{k+1} - 2) \geq m(t) + \frac{k}{2^k}.$$

Proof. We have $D(2^{k+2}t+2^{k+1}-2) = D(2^{k+1}t+2^k-1)$, and by Corollary 2.2.11 this is bounded below by $m(t) + \frac{k}{2^{k-1}}$. Also, $D(2^{k+2}t + 2^{k+1} - 2 + 1) = D(2^{k+2}t + 2^{k+1} - 1) \geq m(t) + \frac{k+1}{2^k}$ and clearly, $\min\bigl(k/2^{k-1}, (k+1)/2^k\bigr) \geq k/2^k$. ⛝

Moreover, we want to find the contribution of a block of `0`s of length ≥ 2. For this, we append `001` and look what happens: note that

$$\begin{aligned}\kappa_2(4t+1) &= \frac{3\kappa_2(t)}{4} + \frac{\kappa_2(t+1)}{4} + \frac{3}{2},\\ D(4t+1) &= \frac{3D(t)}{4} + \frac{D(t+1)}{4} + \frac{\kappa_2(t+1)-\kappa_2(t)}{2} + 2\end{aligned}$$

by (2.2.39) and (2.2.40). Therefore, by the recurrence (2.2.36), we obtain

$$\begin{aligned}D(8t+1) &= \frac{D(t)+D(4t+1)}{2} + \frac{\kappa_2(4t+1)-\kappa_2(t)}{2} + 1\\ &= \frac{7}{8}D(t) + \frac{1}{8}D(t+1) + \frac{3}{8}\bigl(\kappa_2(t+1)-\kappa_2(t)\bigr) + \frac{11}{4}.\end{aligned}$$

These formulas together with $D(8t+2) = D(4t+1)$ and $|\kappa_2(t+1) - \kappa_2(t)| \leq 2$ show that

$$m(8t+1) \geq m(t) + 1. \tag{2.2.42}$$

Corollary 2.2.13. *Assume that $k \geq 2$ and $t \geq 1$ are integers. Let K be the number of inner blocks of `0`s of length at least two in the binary expansion of t, and L be the number of blocks of `1`s of length $\leq k$. Then*

$$m(t) \geq 4 + K + \max\left(0, \left\lfloor \frac{L-2K-1}{2} \right\rfloor\right) \frac{k}{2^k}.$$

In particular, for all integers $D_0 \geq 2$ and $k \geq 2$, there exists a bound $B = B(D_0, k)$ with the following property: for all integers $t \geq 1$ such that $D(t) \leq D_0$, the number of inner blocks of `0`s of length ≥ 2 in t and the number of blocks of `1`s of length $\leq k$ in t are bounded by B.

Proof. We are going to apply (2.2.42) K times and Corollary 2.2.12 $\lfloor (L-2K-1)/2 \rfloor$ times, using the monotonicity of m expressed in (2.2.41) in an essential way. We proceed by induction along the binary expansion of t, beginning at the most significant digit. The constant 4 is explained by the starting value $m(1) = \min(D(1), D(2)) = 4$. Each inner block of `0`s of length ≥ 2 (bordered by `1`s on both sides) corresponds to a factor `001` in the binary expansion: we simply choose the block of length three starting at the second zero from the right. Therefore (2.2.42) explains the contribution K. For the application of Corollary 2.2.12 we need a block of the form $\texttt{01}^r\texttt{0}$ with $r \geq 1$, but we cannot guarantee that the adjacent blocks of `0`s have not already been used for (2.2.42). Therefore each of the K inner blocks of `0`s of length ≥ 2 renders the two adjacent blocks of `1`s unusable for the application of Corollary 2.2.12. Out of the remaining blocks of `1`s of length $\leq k$, we can only use each second block, and the first and the last blocks of `1`s are excluded also. That is, if $L - 2K \in \{3, 4\}$, we can apply Corollary 2.2.12 once, for $L - 2K \in \{5, 6\}$ twice, and so on. Finally, we note that $k/2^k$ is nonincreasing. This explains the last summand. ⛝

In the following, we will only use the "in particular"-statement of Corollary 2.2.13.

2.2.5 Bounds for κ_4 and κ_5

Lemma 2.2.14. *Assume that t contains M blocks of $\mathtt{1}$s. Then*

$$\kappa_4(t) \le 26(M+1).$$

Proof. Recall that $\kappa_4(1) = 26$ by (2.2.13). Using (2.2.14) and the estimates from Lemma 2.2.2 we get

$$\kappa_4(2t+1) \le \frac{\kappa_4(t) + \kappa_4(t+1)}{2} + 13.$$

Using the geometric series, this implies

$$\kappa_4\big(2^k t + 2^k - 1\big) \le \frac{\kappa_4(t)}{2^k} + \frac{\big(2^k-1\big)\kappa_4(t+1)}{2^k} + 26. \tag{2.2.43}$$

The statement for $M = 1$ easily follows. We also study $t' = 2^k t + 1$: In this case, we have

$$\kappa_4\big(2^k t + 1\big) \ge \frac{\big(2^k-1\big)\kappa_4(t)}{2^k} + \frac{\kappa_4(t+1)}{2^k} + 13 \tag{2.2.44}$$

by induction. We consider the values $n(t) = \min(\kappa_4(t), \kappa_4(t+1))$ and prove the stronger statement that $n(t) \ge 26(M+1)$ by induction. We append a block $\mathtt{1}^k$ to t and obtain $t' = 2^k t + 2^k - 1$. Then

$$\kappa_4(t') \le \frac{\kappa_4(t)}{2^k} + \frac{\big(2^k-1\big)\kappa_4(t+1)}{2^k} + 26 \le \min(\kappa_4(t), \kappa_4(t+1)) + 26 = n(t) + 26,$$

and $\kappa_4(t'+1) = \kappa_4(t+1)$. Analogously, we append $\mathtt{0}^k$ to t and obtain $t' = 2^k t$. Clearly, $\kappa_4(t') = \kappa_4(t)$, and

$$\kappa_4(t'+1) \le \frac{\big(2^k-1\big)\kappa_4(t)}{2^k} + \frac{\kappa_4(t+1)}{2^k} + 26 \ge n(t) + 26.$$

This implies the statement. ⛒

We want to find a lower bound for $\kappa_5(t)$. In the following, we consider the behavior of the differences $\kappa_j(t) - \kappa_j(t+1)$ when a block of $\mathtt{1}$s is appended to t. We do so step by step, starting with $\kappa_2(t)$. Assume that $k \ge 1$ is an integer and set $t^{(k)} = 2^k t + 2^k - 1$. Note that by (2.2.14) we have $\kappa_j(t^{(k)} + 1) = \kappa_j(t+1)$. By the recurrence (2.2.9) we obtain

$$\begin{aligned}\kappa_2\big(t^{(k)}\big) - \kappa_2\big(t^{(k)} + 1\big) &= \frac{\kappa_2\big(t^{(k-1)}\big) + \kappa_2(t+1)}{2} + 1 - \kappa_2(t+1) \\ &= \frac{\kappa_2\big(t^{(k-1)}\big) - \kappa_2(t+1)}{2} + 1,\end{aligned}$$

which gives by induction

$$\begin{aligned}\kappa_2\big(t^{(k)}\big) - \kappa_2\big(t^{(k)} + 1\big) &= \frac{\kappa_2(t) - \kappa_2(t+1)}{2^k} + \frac{2^k - 1}{2^{k-1}} \\ &= 2 + \mathcal{O}\big(2^{-k}\big).\end{aligned} \tag{2.2.45}$$

We proceed to $\kappa_3(t)$. For $k \ge 1$, we have

$$\kappa_3\big(t^{(k)}\big) - \kappa_3\big(t^{(k)} + 1\big) = \frac{\kappa_3\big(t^{(k-1)}\big) - \kappa_3(t+1)}{2} + 3 + \mathcal{O}\big(2^{-k}\big)$$

by (2.2.10) and (2.2.45). By induction and the geometric series we obtain

$$\begin{aligned}\kappa_3\big(t^{(k)}\big)-\kappa_3\big(t^{(k)}+1\big)&=\frac{\kappa_3(t)-\kappa_3(t+1)}{2^k}+6+\mathcal{O}\big(k2^{-k}\big)\\&=6+\mathcal{O}\big(k2^{-k}\big).\end{aligned}\tag{2.2.46}$$

Concerning $\kappa_4(t)$, we have by (2.2.11), (2.2.45), and (2.2.46)

$$\begin{aligned}\kappa_4\big(t^{(k)}\big)-\kappa_4\big(t^{(k)}+1\big)&=\frac{\kappa_4\big(t^{(k-1)}\big)-\kappa_4(t+1)}{2}+2\big(\kappa_3\big(t^{(k-1)}\big)-\kappa_3(t^{(k-1)}+1)\big)\\&\quad+\frac{3}{4}\Big(\kappa_2\big(t^{(k-1)}\big)-\kappa_2(t^{(k-1)}+1)\Big)^2-2\\&=\frac{\kappa_4\big(t^{(k-1)}\big)+\kappa_4(t+1)}{2}+12+\mathcal{O}(k2^{-k})+\frac{3}{4}\big(2+\mathcal{O}(2^{-k})\big)^2-2\\&=\frac{\kappa_4\big(t^{(k-1)}\big)-\kappa_4(t+1)}{2}+13+\mathcal{O}(k2^{-k})\end{aligned}$$

and by induction we obtain

$$\kappa_4\big(t^{(k)}\big)-\kappa_4\big(t^{(k)}+1\big)=26+\mathcal{O}\big(k^2 2^{-k}\big).\tag{2.2.47}$$

Finally, we have by (2.2.12), (2.2.45), (2.2.46), and (2.2.47)

$$\begin{aligned}\kappa_5\big(t^{(k)}\big)-\kappa_5\big(t^{(k)}+1\big)&=\frac{\kappa_5\big(t^{(k-1)}\big)-\kappa_5(t+1)}{2}+\frac{5}{2}\Big(\kappa_4\big(t^{(k-1)}\big)-\kappa_4(t^{(k-1)}+1)\Big)\\&\quad+\frac{5}{2}\Big(\kappa_2\big(t^{(k-1)}\big)-\kappa_2(t^{(k-1)}+1)\Big)\Big(\kappa_3\big(t^{(k-1)}\big)-\kappa_3(t^{(k-1)}+1)\Big)\\&\quad-10\Big(\kappa_2\big(t^{(k-1)}\big)-\kappa_2(t^{(k-1)}+1)\Big)=\frac{\kappa_5\big(t^{(k-1)}\big)-\kappa_5(t+1)}{2}+65+\mathcal{O}\big(k^2 2^{-k}\big)\\&\quad+\frac{5}{2}\big(2+\mathcal{O}\big(2^{-k}\big)\big)\big(6+\mathcal{O}\big(k2^{-k}\big)\big)-20+\mathcal{O}\big(2^{-k}\big)\\&=\frac{\kappa_5\big(t^{(k-1)}\big)-\kappa_5(t+1)}{2}+75+\mathcal{O}\big(k2^{-k}\big).\end{aligned}$$

and therefore by induction

$$\kappa_5\big(t^{(k)}\big)-\kappa_5\big(t^{(k)}+1\big)=150+\mathcal{O}\big(k^3 2^{-k}\big).\tag{2.2.48}$$

Proposition 2.2.15. *Let $k\geq 1$ be an integer. Assume that the integer $t\geq 1$ has N_0 inner blocks of zeros of length ≥ 2, and N_1 blocks of* `1`*s of length $\leq k$. Define $N=N_0+N_1$. If N_2 is the number of blocks of* `1`*s of length $>k$, we have*

$$\kappa_5(t)\geq 150N_2-C\big(N+N_2k^3 2^{-k}\big)$$

with an absolute constant C.

Proof. We proceed by induction on the number of blocks of `1`s in t. The statement obviously holds for $t=0$. Clearly, by the identity $\kappa_5(2t)=\kappa_5(t)$ we may append `0`s, preserving the truth of the statement (note that N and N_2 are unchanged, since we only count *inner* blocks of `0`s). We therefore consider, for $r\geq 1$, appending a block of the form $\texttt{01}^r$ to t, obtaining $t'=2^{r+1}t+2^r-1$. Define the integers N' and N_2' according to this new value t'. If t is even, an

additional block of zeros of length ≥ 2 appears, therefore $N' \geq N+1$, moreover $N_2' \leq N_2+1$. By the bound $|\kappa_5(m+1)-\kappa_5(m)| \leq 240$ from (2.2.23), $\kappa_5(2n)=\kappa_5(n)$, and the induction hypothesis we have

$$\begin{aligned}\kappa_5\big(t'\big) &= \big(\kappa_5(t')-\kappa_5(2t+1)\big)+\big(\kappa_5(2t+1)-\kappa_5(t)\big)+\kappa_5(t)\\ &\geq \kappa_5(t)-480 \geq 150N_2 - C\big(N+N_2k^3 2^{-k}\big)+480\\ &\geq 150N_2 - C\big(N'+N_2'k^3 2^{-k}\big)\end{aligned} \tag{2.2.49}$$

if C is chosen large enough. The case of odd t remains. The integer t ends with a block of 1s of length $s \geq 1$. We distinguish between three cases. First, let $r \leq k$. In this case, $N'=N+1$ and $N_2'=N_2$, and reusing the calculation (2.2.49) yields the claim.

In the case $r>k$, we have $N'=N$ and $N_2'=N_2+1$. This case splits into two subcases. Assume first that $s \neq k$. We first consider the integer $t''=2t+1$. The quantities N'' and N_2'' corresponding to the integer t'' satisfy $N''=N$ and $N_2''=N_2$ due to the restriction $s\neq k$, and by hypothesis — recall that the induction is on the number of blocks of 1s in t — we have

$$\kappa_5(2t+1) \geq 150N_2 - C\big(N+N_2k^3 2^{-k}\big). \tag{2.2.50}$$

In this case, we need to extract the necessary gain of 150 from (2.2.48): this formula yields together with (2.2.50)

$$\begin{aligned}\kappa_5(t') &= \kappa_5(2t+1)+150+\mathcal{O}\big(k^3 2^{-k}\big)\\ &\geq 150N_2' - C\big(N'+N_2'k^3 2^{-k}\big)\end{aligned}$$

if C is chosen appropriately. Finally, we consider the subcase $s=k$, and again we set $t''=2t+1$ and choose N'' and N_2'' accordingly. Here we have $N''=N-1=N'-1$ and $N_2''=N_2+1=N_2'$, and therefore by hypothesis

$$\kappa_5(2t+1) \geq 150N_2 - C\big((N-1)+(N_2+1)k^3 2^{-k}\big).$$

By the bound (2.2.23) we have

$$\kappa_5(t') \geq \kappa_5(2t+1)-240 \geq 150N_2' - C\big(N'+N_2'k^3 2^{-k}\big).$$

This finishes the proof of Proposition 2.2.15. ⊠

2.2.6 Finishing the proof of the main theorem

By Lemma 2.2.9 there is a constant D_0 such that $c_t > 1/2$ if $D(t) \geq D_0$. Assume that C is the constant from Proposition 2.2.15 and choose k large enough such that $Ck^3 2^{-k} \leq 20$. Choose $B=B(D_0,k)$ as in Corollary 2.2.13 and assume that $D(t) \leq D_0$. The number N_0 of inner blocks of 0s of length ≥ 2 in t and the number N_1 of blocks of 1s of length $\leq k$ in t are bounded by B by this corollary. Furthermore, recall that $M=N_1+N_2$, where N_2 is the number of blocks of 1s of length $>k$. Therefore by Proposition 2.2.15,

$$\kappa_5(t) \geq 130M - CB.$$

If t contains sufficiently many blocks of 1s, we therefore have by Lemmas 2.2.4 and 2.2.14

$$53\kappa_2(t) - 4\kappa_4(t) + \frac{2}{5}\kappa_5(t) \geq 53M - 104(M+1) + 52M - \frac{4}{5}CB$$

$$= M - \frac{4}{5}CB - 104.$$

For large M this is positive, and by (2.2.38) it follows that $c_t > 1/2$ for sufficiently many (greater than some absolute bound) blocks of `1`s. The proof is complete.

2.3 Normal distribution of $\delta(j,t)$

In this section we prove Theorem 2.1.2. By (2.2.1) we have

$$\delta(j,t) = \int_{-1/2}^{1/2} \gamma_t(\vartheta)\,\mathrm{e}(-j\vartheta)\,\mathrm{d}\vartheta.$$

As above, we truncate the integral at $\pm\vartheta_0$, where

$$\vartheta_0 = M^{-1/2}R,$$

$M = 2M' + 1$ is the number of blocks of `1`s in t, and R is chosen later. In analogy to the reasoning above, we assume that

$$8 \le R \le M^{1/6} \quad \text{and} \quad \vartheta_0 \le \frac{1}{\tau}.$$

Again, by our choice of $R = \log M$ below, this will be satisfied for a sufficiently large number M of blocks. We define a coarser approximation of $\gamma_t(\vartheta)$ than used for the proof of our main theorem, as it is sufficient to derive the normal distribution-statement. Let

$$\gamma_t^{(2)}(\vartheta) = \exp\left(-\kappa_2(t)\frac{(\tau\vartheta)^2}{2}\right),$$
$$\widetilde{\gamma}_t^{(2)}(\vartheta) = \gamma_t(\vartheta) - \gamma_t^{(2)}(\vartheta).$$

The proof of the following estimate essentially only requires to change some numbers in the proof of Proposition 2.2.5 and we leave it to the interested reader.

Proposition 2.3.1. *There exists an absolute constant C such that we have*

$$\bigl|\widetilde{\gamma}_t^{(2)}(\vartheta)\bigr| \le CM\vartheta^3$$

for $|\vartheta| \le \min\bigl(M^{-1/3}, \tau^{-1}\bigr)$, where M is the number of blocks of `1`s in t.

Noting that $\vartheta_0 \le M^{-1/3}$ and $\vartheta_0 \le 1/\tau$ for large M, we obtain from Lemma 2.2.7 and Proposition 2.3.1

$$\begin{aligned}\delta(j,t) &= \int_{-\vartheta_0}^{\vartheta_0} \gamma_t(\vartheta)\,\mathrm{e}(-jt)\,\mathrm{d}\vartheta + \mathcal{O}\left(\exp(-R^2/4)\right)\\ &= \int_{-\vartheta_0}^{\vartheta_0} \gamma_t^{(2)}(\vartheta)\,\mathrm{e}(-j\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}\left(M^{-1}R^4\right) + \mathcal{O}\left(\exp(-R^2/4)\right)\end{aligned}$$

if only M is large enough and $R \le M^{1/6}$. We extend the integral to $\mathbb{R}$, introducing an error

$$\int_{\tau\vartheta_0}^{\infty} \exp\bigl(-\kappa_2(t)\vartheta^2/2\bigr)\,\mathrm{d}\vartheta \ll \exp\bigl(-\kappa_2(t)R^2/(2M)\bigr) \le \exp\bigl(-R^2/2\bigr)$$

since $\kappa_2(t) \geq M$ by Lemma 2.2.4. We obtain the representation

$$\begin{aligned}\delta(j,t) &= \int_{-\infty}^{\infty} \exp\bigl(-\kappa_2(t)(\tau\vartheta)^2/2\bigr)\,\mathrm{e}(-j\vartheta)\,\mathrm{d}\vartheta + \mathcal{O}(E)\\ &= \frac{1}{\tau}\int_{-\infty}^{\infty} \exp\bigl(-\kappa_2(t)\vartheta^2/2 - ij\vartheta\bigr)\,\mathrm{d}\vartheta + \mathcal{O}(E)\end{aligned}$$

for large enough M and $R \leq M^{1/6}$, where

$$E = M^{-1}R^4 + \exp\bigl(-R^2/4\bigr).$$

Now, we choose $R = \log M$. Our hypothesis $R \geq 8$ implies $\exp\bigl(-R^2/4\bigr) \leq M^{-1}$ and therefore

$$E \ll M^{-1}\bigl(\log M\bigr)^4.$$

The appearing integral can be evaluated by completing to a square and evaluating a complete Gauss integral:

$$-\kappa_2(t)\vartheta^2/2 - ij\vartheta = -\left((\kappa_2(t)/2)^{1/2}\vartheta + \frac{ij}{\sqrt{2}\kappa_2(t)^{1/2}}\right)^2 - \frac{j^2}{2\kappa_2(t)}.$$

The imaginary shift is irrelevant due to the residue theorem, and after inserting the Gauss integral and slight rewriting we obtain the theorem.

Data availability statement

The datasets generated and analysed during the current study are available from the corresponding author on reasonable request.

Chapter 3

The level of distribution of the Thue–Morse sequence

Lukas Spiegelhofer
Compos. Math. 156 (2020), no. 12, 2560–2587
DOI: https://doi.org/10.1112/S0010437X20007563

Abstract

The level of distribution of a complex valued sequence b measures the quality of distribution of b along sparse arithmetic progressions $nd + a$. We prove that the Thue–Morse sequence has level of distribution 1, which is essentially best possible. More precisely, this sequence gives one of the first nontrivial examples of a sequence satisfying a Bombieri–Vinogradov type theorem for each exponent $\theta < 1$. This result improves on the level of distribution 2/3 obtained by Müllner and the author.

As an application of our method, we show that the subsequence of the Thue–Morse sequence indexed by $\lfloor n^c \rfloor$, where $1 < c < 2$, is *simply normal*. This result improves on the range $1 < c < 3/2$ obtained by Müllner and the author and closes the gap that appeared when Mauduit and Rivat proved (in particular) that the Thue–Morse sequence along the squares is simply normal.

3.1 Introduction

The Thue–Morse sequence $\mathbf{t}$ is one of the most easily defined automatic sequences. Like any automatic sequence, it can be defined using a *uniform morphism* over a finite alphabet: $\mathbf{t}$ is the unique fixed point of the substitution $0 \mapsto 01$, $1 \mapsto 10$ that starts with 0. Therefore $\mathbf{t} = (0110100110010110\ldots)$. Alternatively, this sequence can be defined using the *binary sum-of-digits function* s, which counts the number of 1s in the binary expansion of a nonnegative integer n: we have $\mathbf{t}(n) = 0$ if and only if $s(n) \equiv 0 \bmod 2$. The equivalence of these two definitions can be proved via a third description: start with the one-element sequence $\mathbf{t}^{(0)} := (0)$ and define $\mathbf{t}^{(n+1)}$ by concatenating $\mathbf{t}^{(n)}$ and the Boolean complement $\neg\mathbf{t}^{(n)}$. Then $\mathbf{t}$ is the (pointwise) limit of this sequence of finite words. In this work, we will adopt the second viewpoint. In fact, in the

proofs we will work with the sequence $(-1)^{s(n)}$ instead of $\mathbf{t}$, and we also call this sequence the Thue–Morse sequence by slight abuse of notation. When working with exponential sums, we will always use the "multiplicative version" $(-1)^{s(n)}$. For an overview on the Thue–Morse sequence, we refer the reader to the article by Allouche and Shallit [4], which points out occurrences of this sequence in different fields of mathematics and offers a good bibliography. We also wish to mention the survey paper [104] by Mauduit on the Thue–Morse sequence. For a comprehensive treatment of automatic and morphic sequences, see the book [6] by Allouche and Shallit.

The main topic of this article is the study of $\mathbf{t}$ along arithmetic progressions and, more generally, along Beatty sequences $\lfloor n\alpha + \beta \rfloor$, where α and β are real numbers and $\alpha \geq 0$. This topic can be traced back at least to Gel'fond [72], who proved the following theorem on the base-q sum-of-digits function s_q defined by $s_q(\varepsilon_\nu q^\nu + \cdots + \varepsilon_0 q^0) = \varepsilon_\nu + \cdots + \varepsilon_0$ for $\varepsilon_i \in \{0, \dots, q-1\}$.

Theorem A (Gel'fond)**.** *Let q, m, d, b, a be integers and $q, m, d \geq 2$. Suppose that* $\gcd(m, q-1) = 1$*. Then*

$$\bigl|\{1 \leq n \leq x : n \equiv a \bmod d, s_q(n) \equiv b \bmod m\}\bigr| = \frac{x}{dm} + \mathcal{O}\bigl(x^\lambda\bigr)$$

for some $\lambda < 1$ independent of $x, d, a,$ and b.

We are particularly interested in the error term for *sparse* arithmetic progressions, having large common difference d. This leads us directly to the other main concept of this paper, the notion of *level of distribution*. (We use this term in the same way as Goldston–Pintz–Yıldırım [74]; the term is also used for a very similar concept by other authors. Moreover, the term *exponent of distribution* is also common.) Very roughly speaking, the level of distribution is a measure of how well a given sequence behaves on arithmetic progressions. A formal definition can be found in the article [63] by Fouvry and Mauduit. We adapt this definition.

Definition 1. Let $c = (c_n)_{n\geq 0}$ be a sequence of complex numbers, and for each integer $d \geq 1$ let $\mathcal{Q}(d)$ and $\mathcal{R}(d) \neq \emptyset$ be subsets of $\mathbb{Z}/d\mathbb{Z}$ such that $\mathcal{Q}(d) \subseteq \mathcal{R}(d)$. The sequence c has *level of distribution θ* with respect to $\mathcal{Q}$ and $\mathcal{R}$ if for all $\varepsilon > 0$ and $A > 0$ we have for all $x \geq 1$

$$\sum_{1\leq d\leq D} \max_{0\leq y\leq x} \max_{\substack{0\leq a<d \\ a+d\mathbb{Z}\in\mathcal{Q}(d)}} \left| \sum_{\substack{0\leq n<y \\ n\equiv a \bmod d}} c_n - \frac{1}{|\mathcal{R}(d)|} \sum_{\substack{0\leq n<y \\ n+d\mathbb{Z}\in\mathcal{R}(d)}} c_n \right| \ll (\log 2x)^{-A} \sum_{0\leq n<x} |c_n|,$$

where $D = x^{\theta-\varepsilon}$. The implied constant may depend on A and ε. In this definition, the maximum over the empty index set is defined to be 0.

The most well-known cases are $\mathcal{R}(d) = \mathbb{Z}/d\mathbb{Z}$ or $\mathcal{R}(d) = \bigl(\mathbb{Z}/d\mathbb{Z}\bigr)^*$; the treatment of the main term

$$\frac{1}{|\mathcal{R}(d)|} \sum_{\substack{0\leq n<y \\ n+d\mathbb{Z}\in\mathcal{R}(d)}} c_n$$

is usually the easy part of an estimate as in the definition. In the case of the Bombieri–Vinogradov theorem, we use $\mathcal{R}(d) = \bigl(\mathbb{Z}/d\mathbb{Z}\bigr)^*$, since the prime numbers are distributed evenly in the residue classes relatively prime to d. The summands in Definition 1 measure the maximal deviation of a sum over an arithmetic progression from the expected value, where the maximum is taken over a set $\mathcal{Q}(d)$ of residue classes, and the length of the progression may also vary.

The level of distribution is an important concept in sieve theory. As a striking application, a variant of this concept was used in the paper by Zhang [164] on bounded gaps between primes.

For more information on this subject, we refer the reader to the survey by Kontorovich [90]. Moreover, we wish to draw the attention of the reader to the book [67] on sieve theory by Friedlander and Iwaniec, in particular Chapter 22 on the level of distribution.

We are ready to present our main result. Note that we use $\mathcal{O}_\varepsilon$ to indicate that the implied constant may depend on ε.

Theorem 3.1.1. *The Thue–Morse sequence has level of distribution* 1 *with respect to* $\mathcal{Q}$ *and* $\mathcal{R}$ *given by* $\mathcal{Q}(d) = \mathcal{R}(d) = \mathbb{Z}/d\mathbb{Z}$. *More precisely, for all* $\varepsilon > 0$ *we have*

$$\sum_{1\le d\le D} \max_{\substack{y,z\ge 0\\ z-y\le x}} \max_{0\le a<d} \left| \sum_{\substack{y\le n<z\\ n\equiv a \bmod d}} (-1)^{s(n)} \right| = \mathcal{O}_\varepsilon(x^{1-\eta})$$

for some $\eta > 0$ *depending on* ε, *where* $D = x^{1-\varepsilon}$.

Before presenting some history, we wish to say a word about the proof: we are going to reduce the problem to the estimation of a certain *Gowers uniformity norm* of the Thue–Morse sequence. These expressions appear by repeated application of Van der Corput's inequality and have the form

$$\sum_{\substack{0\le n<2^\rho\\ 0\le r_1,\dots,r_k<2^\rho}} \prod_{\varepsilon\in\{0,1\}^k} (-1)^{s_\rho(n+\varepsilon\cdot r)},$$

where $\varepsilon \cdot r = \sum_{1\le i\le k} \varepsilon_i r_i$ and s_ρ is the truncated sum-of-digits function in base 2 defined by $s_\rho(n) = s(n \bmod 2^\rho)$. Note that, strictly speaking, this is not the Gowers norm of the Thue–Morse sequence, but the Gowers norm of order k of the projection of $(-1)^{s(n)}$ to $\mathbb{Z}/2^\rho\mathbb{Z}$. The proof of a very similar statement was given recently by Konieczny [89], and we use the proof from that paper to prove our estimate.

Gowers norms are certain averaged multiple correlations and were introduced by Gowers [75, 76], who used them to give a new proof of Szemerédi's theorem. These norms are a central tool in *higher order Fourier analysis* [156]; this theory can be used to study questions in additive combinatorics, such as the behaviour of an arithmetic function f on arithmetic progressions $n, n+d, n+2d, \dots, n+(\ell-1)d$. In the groundbreaking paper [80] by Green and Tao, Gowers norms were used to prove the existence of arbitrarily long arithmetic progressions in the primes. Our result is a statement on arithmetic progressions too; although it is different in nature, Gowers norms are applicable here.

In order to put Theorem 3.1.1 into context, we present some related theorems. The well-known Bombieri–Vinogradov theorem concerns the level of distribution of the von Mangoldt function Λ, which is defined by $\Lambda(n) = \log p$ if $n = p^\ell$ for some prime p and some $\ell \ge 1$ and $\Lambda(n) = 0$ otherwise. This theorem states that Λ has level of distribution $1/2$ with respect to $\mathcal{Q}$ and $\mathcal{R}$ given by $\mathcal{Q}(d) = \mathcal{R}(d) = (\mathbb{Z}/d\mathbb{Z})^*$.

Theorem B (Bombieri–Vinogradov)**.** *Let* $d \ge 1$ *and* a *be integers and define*

$$\psi(x; d, a) = \sum_{\substack{1\le n\le x\\ n\equiv a \bmod d}} \Lambda(n).$$

For all real numbers $A > 0$ *there exist* $B > 0$ *and a constant* C *such that setting* $D = x^{1/2}(\log x)^{-B}$ *we have for all* $x \ge 2$

$$\sum_{1\le d\le D} \max_{1\le y\le x} \max_{\substack{0\le a<d\\ \gcd(a,d)=1}} \left| \psi(y; d, a) - \frac{y}{\varphi(d)} \right| \le Cx(\log x)^{-A}.$$

Here φ denotes Euler's totient function.

No improvement on the level of distribution $1/2$ in this theorem is currently known. Meanwhile the Elliott–Halberstam conjecture [53] states that we can choose $D = x^{1-\varepsilon}$ for any $\varepsilon > 0$. That is, it is conjectured that the primes have level of distribution 1. Improvements on the exponent $1/2$ exist for certain sequences of integers; we refer to the articles [65, 66] by Fouvry, by Fouvry and Iwaniec [62] and by Friedlander and Iwaniec [68]. Moreover, we mention the series [21–23] by Bombieri, Friedlander and Iwaniec concerning this topic. In this context, we also note the result of Goldston, Pintz, and Yıldırım [74], who showed in particular the following conditional result: if the primes have level of distribution θ for some $\theta > 1/2$, then there exists a constant C such that $p_{n+1} - p_n < C$ infinitely often, where p_n is the n-th prime. In a groundbreaking paper we mentioned before, Zhang [164] used the Goldston–Pintz–Yıldırım method and a variant of the Bombieri–Vinogradov theorem to prove the above result unconditionally. Maynard [115] later proved the bounded gaps result using only the classical Bombieri–Vinogradov theorem.

Improvements on the level $1/2$ are also known for the sum-of-digits function modulo m. Fouvry and Mauduit [64] established 0.5924 as a level of distribution of the Thue–Morse sequence, with respect to $\mathcal{Q}$ and $\mathcal{R}$, where $\mathcal{Q}(d) = \mathcal{R}(d) = \mathbb{Z}/d\mathbb{Z}$.

Theorem C (Fouvry–Mauduit)**.** *Set*

$$A(x; d, a) = \big|\big\{0 \le n < x : \mathbf{t}(n) = \mathtt{0}, n \equiv a \bmod d\big\}\big|.$$

Then

$$\sum_{1\le d\le D} \max_{1\le y\le x} \max_{0\le a<d} \Big|A(y; d, a) - \frac{y}{2d}\Big| \le Cx(\log 2x)^{-A} \tag{3.1.1}$$

for all real A and $D = x^{0.5924}$, where C may depend on A.

More generally, for $m \ge 2$ they also study the sum-of-digits function in base 2 modulo m, obtaining the weaker level of distribution 0.55711. Using sieve theory, they apply this result to the study of the sum of digits modulo m of numbers having at most two prime factors. Later, Mauduit and Rivat [110], in an important paper, managed to treat the sum of digits modulo m of prime numbers, thereby answering one of the questions posed by Gel'fond [72].

Müllner and the author [124] improved the exponent 0.5924 to $2/3 - \varepsilon$, thereby establishing $2/3$ as an admissible level of distribution of the Thue–Morse sequence.

Fouvry and Mauduit [63] also considered, more generally, the sum-of-digits function s_q in base q modulo an integer m such that $\gcd(m, q-1) = 1$. They obtain the result that the level of distribution approaches 1 as the base q gets larger.

Theorem D (Fouvry–Mauduit)**.** *Let $q \ge 2$, $m \ge 1$ and b be integers such that $\gcd(m, q-1) = 1$. There exists $\theta_q > 0$ such that for all A and $\varepsilon > 0$ we have for all $x \ge 1$*

$$\sum_{1\le d\le D} \max_{0\le y\le x} \max_{0\le a<d} \Bigg| \sum_{\substack{n<y, s_q(n)\equiv b \bmod m \\ n\equiv a \bmod d}} 1 - \frac{1}{d} \sum_{n<y, s_q(n)\equiv b \bmod m} 1 \Bigg| = \mathcal{O}_{m,q,A,\varepsilon}(x(\log 2x)^{-A}),$$

where $D = x^{\theta_q - \varepsilon}$. The implied constant depends at most on m, q, A and ε. As $q \to \infty$, the value of θ_q tends to 1.

As an application of this theorem, they consider the sum of digits in base q of integers having at most two prime factors; moreover, they study the sum $\sum_{n<x, s_q(n)\equiv b \bmod m} \Lambda_\ell(n)$, where Λ_ℓ is the generalized von Mangoldt function of order $\ell \geq 2$ ([63, Corollaire 2]).

Theorem D motivates us to look for sequences having level of distribution equal to 1. In the paper by Fouvry and Mauduit [63] cited above, for example, a list of sequences having this property is given. Also, we note [67, Chapter 22.3], which studies the level of distribution for additive convolutions, giving further examples. However, in these examples, other than the trivial example $c_n = 1$ for all n, the maximum over a does not play a rôle: the set $\mathcal{Q}(d)$ consists of at most one element.

We are interested in sequences c having level of distribution 1 and such that the set $\mathcal{Q}(d)$ contains "many" residue classes. In other words, we want to find analogues of the Elliott–Halberstam conjecture. Requiring monotonicity of c, examples can be constructed easily: $c(n) = n$ is such an example, and more generally, increasing sequences c satisfying certain growth conditions have this property. Apart from such "trivial" sequences, no other examples seem to be known. Our Theorem 3.1.1, giving such an example, might therefore be of interest.

We believe that our method can be adapted to $s_q(n)$ mod m for all $m \geq 1$ and general bases $q \geq 2$, which would yield $\theta_q = 1$ for all $q \geq 2$ in Theorem D.

The second focus of this paper concerns *Piatetski-Shapiro sequences*, which are sequences of the form $(\lfloor n^c \rfloor)_{n\geq 0}$ for some $c \geq 1$. In order to state the second main theorem, we do not need additional preparation.

Theorem 3.1.2. *Let $1 < c < 2$. The Thue–Morse sequence along $\lfloor n^c \rfloor$ is simply normal. That is, each of the letters* 0 *and* 1 *appears with asymptotic frequency $1/2$ in $n \mapsto \mathtt{t}(\lfloor n^c \rfloor)$.*

A in our earlier paper [124] with Müllner, this theorem is proved via a Beatty sequence variant of Theorem 3.1.1. That theorem in turn is proved by arguments analogous to the arguments in the proof of Theorem 3.1.1, and reduces to the same estimate of the Gowers uniformity norm of Thue–Morse. Theorem 3.1.2 is therefore an application of the method of proof of Theorem 3.1.1.

Again, we present some historical background. Studying Piatetski–Shapiro subsequences of a given sequence can be seen as a step towards proving theorems on polynomial subsequences. For example, it is unknown whether there are infinitely many primes of the form $n^2 + 1$; therefore it is of interest to consider primes of the form $\lfloor n^c \rfloor$ for $1 < c < 2$ and prove an asymptotic formula for the number of such primes. Piatetski-Shapiro [129] proved such a formula for $1 < c < 12/11$, and the currently best known bound is $1 < c < 2817/2426$ due to Rivat and Sargos [133]. In a similar way, the study of the sum-of-digits function along $\lfloor n^c \rfloor$ can be justified. It is another problem posed by Gel'fond [72] to study the distribution of the sum of digits of polynomial sequences in residue classes. Since this problem could not be solved at first, Mauduit and Rivat [106, 107] considered q-multiplicative functions along $\lfloor n^c \rfloor$ (where a q-multiplicative function $f : \mathbb{N} \to \{z \in \mathbb{C} : |z| = 1\}$ satisfies $f(aq^m + b) = f(aq^m)f(b)$ for nonnegative integers a, b, m such that $b < q^m$) and they obtained an asymptotic formula for $c < 7/5$.

Theorem E (Mauduit–Rivat)**.** *Let $1 < c < 7/5$ and set $\gamma = 1/c$. For all $\delta \in (0, (7-5c)/9)$ there exists a constant $C > 0$ such that for all q-multiplicative functions $f : \mathbb{N} \to \{z \in \mathbb{C} : |z| = 1\}$ and all $x \geq 1$ we have*

$$\left| \sum_{1\leq n\leq x} f\left(\lfloor n^c \rfloor\right) - \sum_{1\leq m\leq x^c} \gamma m^{\gamma-1} f(m) \right| \leq C x^{1-\delta}.$$

Since the Thue–Morse sequence is 2-multiplicative, it follows in particular that the subsequence indexed by $\lfloor n^c \rfloor$ assumes each of the two values $\mathtt{0}$, $\mathtt{1}$ with asymptotic frequency $1/2$, as long as $1 < c < 7/5$. This means that this subsequence is simply normal. In the paper [37] by Deshouillers, Drmota, and Morgenbesser, a statement as in Theorem E for arbitrary automatic sequences and $1 < c < 7/5$ is proved. Moreover, we wish to note the paper [118] by Morgenbesser, who proved uniform distribution of $s_q(\lfloor n^c \rfloor)$ in residue classes for *all* non-integer $c > 0$, as long as the base q is large enough (depending on c).

Some progress on Gel'fond's question on polynomials was made by Drmota and Rivat [50] and by Dartyge and Tenenbaum [30]; finally, Mauduit and Rivat [108] managed to answer Gel'fond's question for the polynomial n^2. This latter paper was generalized by Drmota, Mauduit and Rivat [45], who showed that in fact $\mathbf{t}(n^2)$ defines a *normal sequence*, by which we understand an infinite sequence on $\{\mathtt{0}, \mathtt{1}\}$ such that every finite sequence of length L occurs as a factor (contiguous finite subsequence) with asymptotic frequency 2^{-L}. This result also generalizes a paper by Moshe [121] who showed that every finite word on $\{\mathtt{0}, \mathtt{1}\}$ occurs as a factor of $n \mapsto \mathbf{t}(n^2)$ at least once.

However, the distribution of the sum of digits of $\lfloor n^c \rfloor$ in residue classes, for $c \in [7/5, 2)$, remained an open problem. Progress in this direction was made by the author [141], who improved the bound on c to $1 < c \leq 1.42$ for the Thue–Morse sequence. The key idea in that paper is to approximate $\lfloor n^c \rfloor$ by a Beatty sequence $\lfloor n\alpha + \beta \rfloor$ and thus reduce the problem to a linear one. Müllner and the author [124], using the same linearization argument and a Bombieri–Vinogradov type theorem for the Thue–Morse sequence on Beatty sequences, were able to extend this range to $1 < c < 3/2$. In that paper, we also handled occurrences of factors in Piatetski-Shapiro subsequences of $\mathbf{t}$, thus showing that $\mathbf{t}\left(\lfloor n^c \rfloor\right)$ defines a normal sequence for $1 < c < 3/2$.

Theorem F (Müllner–Spiegelhofer)**.** *Let $1 < c < 3/2$. Then the sequence $\mathbf{u} = \left(\mathbf{t}\left(\lfloor n^c \rfloor\right)\right)_{n \geq 0}$ is normal. More precisely, for any $L \geq 1$ there exists an exponent $\eta > 0$ and a constant C such that*

$$\left| \left| \left\{ n < N : \mathbf{u}(n+i) = \omega_i \text{ for } 0 \leq i < L \right\} \right| - N/2^L \right| \leq C N^{1-\eta}$$

for all $(\omega_0, \ldots, \omega_{L-1}) \in \{\mathtt{0}, \mathtt{1}\}^L$.

This theorem also improved on an earlier result by the author [142], who obtained normality for $1 < c < 4/3$, using an estimate for Fourier coefficients related to the Thue–Morse sequence provided by Drmota, Mauduit and Rivat [45].

Our Theorem 3.1.2 finally closes the gap in the set of exponents c such that we have an asymptotic formula for Thue–Morse on $\lfloor n^c \rfloor$. This gap appeared with the Mauduit–Rivat result on squares [108]; at that time, the gap was $[7/5, 2)$, now, after our paper with Müllner [124], it was only left to close the smaller gap $[3/2, 2)$.

However, the case $c > 2$ remains open for now, for $c \in \mathbb{Z}$ (which is contained in Gel'fond's problem on polynomial subsequences) as well as for Piatetski-Shapiro sequences. For example, it is a notorious open question to prove that $\mathtt{0}$ occurs with frequency $1/2$ in $n \mapsto \mathbf{t}(n^3)$.

Mauduit [104, Conjecture 1] conjectures that

$$\lim_{N \to \infty} \frac{1}{N} \left\{ 1 \leq n \leq N : s_q(\lfloor n^c \rfloor) \equiv b \bmod m \right\} = \frac{1}{m}$$

for almost all $c > 1$ with respect to Lebesgue measure, where $q \geq 2$, $m \geq 1$ and b are integers. While this almost-all result is known for $1 < c < 2$, as he notes just before this conjecture,

we believe (as we noted before) that our method can be adapted to generalize our results to general sequences $s_q(n) \bmod m$ and thus to prove the asymptotic identity for all $c \in (1,2)$. However, while we are confident that the asymptotic identity in Mauduit's conjecture holds for *all* non-integer $c > 1$, the case $c > 2$ cannot yet be handled by our methods.

We note that it would definitely be interesting to generalize the normality result from Theorem F to all exponents $1 < c < 2$.

Notation. For a real number x, we write $\mathrm{e}(x) = \exp(2\pi i x)$, $\{x\} = x - \lfloor x \rfloor$, $\|x\| = \min_{n\in\mathbb{Z}} |x-n|$ and $\langle \cdot \rangle = \lfloor x + 1/2 \rfloor$ (the "nearest integer" to x). For a prime number p let $\nu_p(n)$ be the exponent of p in the prime factorization of n. We define the *truncated binary sum-of-digits function*

$$s_\lambda(n) \coloneqq s(n'),$$

where $0 \le n' < 2^\lambda$ and $n' \equiv n \bmod 2^\lambda$, which is the 2^λ-periodic extension of the restriction of s to $\{0, \dots, 2^\lambda - 1\}$. For $\mu \le \lambda$ we define the *two-fold restricted binary sum-of-digits function*

$$s_{\mu,\lambda}(n) = s_\lambda(n) - s_\mu(n).$$

For a real number $x \ge 0$, we set

$$\log^+ x = \max\{1, \log x\}.$$

The symbol $\mathbb{N}$ denotes the set of nonnegative integers.

Constants implied by the symbols $\ll$ and $\mathcal{O}$ may depend on the variable k (which describes the number of times that we apply Van der Corput's inequality), but are otherwise absolute. Exceptions to this rule will be indicated in the text.

3.2 Results

In order to (re)state our main theorem, we introduce some notation. Let α, β, y and z be nonnegative real numbers such that $\alpha \ge 1$. We define

$$A(y,z;\alpha,\beta) = \big|\{y \le m < z : \mathbf{t}(m) = \mathtt{0} \text{ and } \exists n \in \mathbb{Z} \text{ such that } m = \lfloor n\alpha + \beta \rfloor\}\big|.$$

For integers $d = \alpha$ and $a = \beta$, we clearly have

$$A(y,z;d,a) = \big|\{y \le m < z : \mathbf{t}(m) = \mathtt{0} \text{ and } m \equiv a \bmod d\}\big|.$$

Our main theorem is the following result.

Theorem 3.2.1. *Let $\varepsilon > 0$. There exist $\eta > 0$ and C such that*

$$\sum_{1\le d\le D} \max_{\substack{y,z\ge 0\\ z-y\le x}} \max_{0\le a<d} \left| A(y,z;d,a) - \frac{z-y}{2d} \right| \le C x^{1-\eta}$$

for all $x \ge 1$ and $D = x^{1-\varepsilon}$.

Note that this theorem allows intervals $[y,z)$ for arbitrary $y \ge 0$, which is more general than our definition of a level of distribution. Noting that $1 - 2\mathbf{t}(n) = (-1)^{s(n)}$, we obtain the form of this theorem given in the introduction.

As a corollary we obtain an estimate for the least element m in an arithmetic progression such that $\mathbf{t}(m) = \mathtt{1}$. For most common differences d, we do not have to search for a long time until we encounter the first $\mathtt{1}$.

Corollary 3.2.2. *For $d \geq 1$ and $a \geq 0$ we define*

$$m(d,a) = \min\{n \in \mathbb{N} : \mathtt{t}(nd+a) = \mathtt{1}\}.$$

For each $\varepsilon > 0$ we have, as $D \to \infty$,

$$\big|\{d < D : \max_{a \geq 0} m(d,a) \geq d^{\varepsilon}\}\big| = o(D).$$

We note that Dartyge and Tenenbaum considered (among many other things) the homogeneous problem concerning $a = 0$: they proved in particular [30, Théorème 2.5] that for *any* function $\xi(d)$ tending to ∞, we have $m(d,0) \leq \xi(d)$ for almost all d in the sense of asymptotic density. The added value of our corollary lies in the fact that the maximum is taken over all arithmetic progressions having a given common difference and a given number of terms. We also wish to note that Morgenbesser, Shallit, and Stoll [119] proved in particular that $m(d,0) \leq d+4$ for *all* nonnegative integers d.

Our second result concerns Piatetski-Shapiro subsequences of the Thue–Morse sequence.

Theorem 3.2.3. *Let $1 < c < 2$. Then the sequence $n \mapsto \mathtt{t}(\lfloor n^c \rfloor)$ is simply normal. More precisely, there exists an exponent $\eta > 0$ and a constant C such that*

$$\left|\frac{1}{N}\big|\big\{0 \leq n < N : \mathtt{t}(\lfloor n^c \rfloor) = \mathtt{0}\big\}\big| - \frac{1}{2}\right| \leq CN^{-\eta}.$$

In order to prove this theorem, we use the general argument presented in Section 4.2 of [124]. This argument uses linear approximation of $\lfloor n^c \rfloor$ by $\lfloor n\alpha + \beta \rfloor$ and thus reduces the problem to Beatty sequences. Therefore Theorem 3.2.3 is a corollary of the following Beatty sequence version of a statement on the level of distribution.

Theorem 3.2.4. *Let $0 < \theta_1 \leq \theta_2 < 1$. There exist $\eta > 0$ and C such that*

$$\int_D^{2D} \max_{\substack{y,z \geq 0 \\ z-y \leq x}} \max_{\beta \geq 0} \left| A(y,z;\alpha,\beta) - \frac{z-y}{2\alpha} \right| \mathrm{d}\alpha \leq Cx^{1-\eta}$$

for all x and D such that $x \geq 1$ and $x^{\theta_1} \leq D \leq x^{\theta_2}$.

In order to derive Theorem 3.2.3 from this result, it is essential that we have the maximum over β inside the integral over α, since we need to approximate $\lfloor n^c \rfloor$ by inhomogeneous (shifted) Beatty sequences $\lfloor n\alpha + \beta \rfloor$.

Concerning Theorem 3.2.1, we can obtain a weakened version of this result, without the maximum over a, using Martin, Mauduit and Rivat [99].

Remark 6. Martin, Mauduit and Rivat [99, Proposition 3] proved an estimate of a sum of type II containing the following special case: let a_m and b_n be complex numbers satisfying $|a_m| \leq 1$ and $|b_n| \leq 1$. Assume that $x \geq 2$, $0 < \varepsilon \leq 1/2$, $x^{\varepsilon} \leq M, N \leq x$ and $MN \leq x$. Then

$$S_0 = \sum_{M < m \leq 2M} \sum_{\substack{N < n \leq 2N \\ mn \leq x}} a_m b_n (-1)^{s(mn)} \leq Cx^{1-\eta}$$

for an absolute constant C and some $\eta > 0$ only depending on ε. By dyadic decomposition and using the trivial estimate for $n < x^{\varepsilon}$, we obtain

$$\sum_{M < m \leq 2M} \left| \sum_{\substack{0 \leq n \leq 2N \\ mn \leq x}} (-1)^{s(mn)} \right| \ll_{\varepsilon} x^{1-\eta} \log N + Mx^{\varepsilon}$$

for M and N satisfying the same restrictions, and with an implied constant that may depend on ε. Let x be given and assume that $x^\varepsilon \le M \le x^\theta$ for some $\theta \in (1/2, 1)$. Set $\varepsilon = 1 - \theta \le 1/2$ and $N = x/M$. Then $N \ge x^\varepsilon$ and the condition $mn \le x$ implies $n \le 2N$. Using dyadic decomposition again, this time in the variable m, we obtain

$$\sum_{x^\varepsilon < m \le D} \left| \sum_{\substack{0 \le u \le x \\ u \equiv 0 \bmod m}} (-1)^{s(u)} \right| \ll_\varepsilon x^{1-\eta} \log^2 x + M x^\varepsilon \log x$$

for $D = x^\theta$. Finally, we use Fouvry and Mauduit [64] in order to handle residue classes having small modulus m, that is, $m \le x^\varepsilon$. We note (as we did in [124]) that the error term in their estimate [64, equation (1.6)] is in fact $x^{1-\eta}$ for some $\eta > 0$; this follows from Théorème 2 in the same paper [64]. We obtain

$$\sum_{1 \le d \le D} \left| \sum_{\substack{0 \le u \le x \\ n \equiv 0 \bmod d}} (-1)^{s(u)} \right| \le C x^{1-\eta}$$

for $D = x^\theta$ and some $\eta > 0$ and C depending on θ. This is a weak version of a statement of the type "the Thue–Morse sequence has level of distribution 1", where $\mathcal{Q}(d)$ has only one element. We note that we could also handle the maximum over $y \le x$, using the factor $\mathrm{e}(\beta mn)$ that appears in [99, Proposition 3]. The added value of our paper (compare also to the remark after Corollary 3.2.2) lies in the maximum over the residue classes modulo d.

Finally, we note the following open questions concerning Theorems 3.2.1 and 3.2.3:

1. In Theorem 3.2.1, can we choose $D = x(\log x)^{-B}$ for some $B > 0$, using $x(\log x)^{-A}$ as error term?

2. Does Theorem 3.2.3 hold for $\lfloor x^2 (\log x)^{-C} \rfloor$ (and similar sequences, possibly with a worse error term) in place of $\lfloor x^c \rfloor$?

Plan of the paper. In Section 4.2.1 we state two results (Propositions 3.3.1 and 3.3.2) from which Theorems 3.2.1 and 3.2.4 follow; moreover, we prove an important Gowers uniformity norm estimate for the Thue–Morse sequence in Proposition 3.3.3. We also give an idea of the proof of Proposition 3.3.1. Using Proposition 3.3.1, the proof of Corollary 3.2.2 is very short, and we present it in that section. In Section 3.4 we state lemmas needed for proving the results from Section 4.2.1. Section 3.5 is devoted to proving Propositions 3.3.1 and 3.3.2. Finally, in sections 3.5.1 and 3.5.2, we prove Proposition 3.3.3 and a technical lemma appearing in the proof of Propositions 3.3.1 and 3.3.2.

3.3 Auxiliary results

It will be sufficient to prove the following two propositions in order to obtain our main theorems. To see this, we follow our earlier paper with Müllner [124, Section 4.1], and Fouvry and Mauduit [64] for handling small d. In fact, as we noted before, their Théorème 2 holds with an improved error term. Moreover, the proof of this result also reveals that the result holds for arbitrarily shifted intervals $[y, z)$.

Proposition 3.3.1. *For real numbers $N, D \geq 1$ and ξ set*

$$S_0 = S_0(N, D, \xi) = \sum_{D \leq d < 2D} \max_{a \geq 0} \left| \sum_{0 \leq n < N} \mathrm{e}\left(\frac{1}{2} s(nd + a)\right) \mathrm{e}(n\xi) \right|. \tag{3.3.1}$$

Let $\rho_2 \geq \rho_1 > 0$. There exists an $\eta > 0$ and a constant C such that

$$\frac{S_0}{ND} \leq CN^{-\eta} \tag{3.3.2}$$

holds for all $\xi \in \mathbb{R}$ and all real numbers $N, D \geq 1$ satisfying $N^{\rho_1} \leq D \leq N^{\rho_2}$.

With the help of this proposition, it is not difficult to prove Corollary 3.2.2: we have $|\{d \in [D, 2D) : \max_{a \geq 0} m(d, a) \geq N\}| \leq CDN^{-\eta}$ for all N, D such that $N^{\rho_1} \leq D \leq N^{\rho_2}$, and some $C > 0$, $\eta > 0$. This is the case since we cannot have more than $CDN^{-\eta}$ many trivial sums in the expression S_0; this means that for each nontrivial summand we encounter at least one $\mathtt{1}$ for each a. It follows that $|\{d \in [D, 2D) : \max_{a \geq 0} m(d, a) \geq D^{\varepsilon}\}| \leq CD^{1-\eta'}$ for all $\varepsilon > 0$. By dyadic decomposition the statement of the corollary follows.

Proposition 3.3.2. *For real numbers $D, N \geq 1$ and ξ set*

$$S_0 = S_0(N, D, \xi) = \int_D^{2D} \max_{\beta \geq 0} \left| \sum_{0 \leq n < N} \mathrm{e}\left(\frac{1}{2} s\big(\lfloor n\alpha + \beta \rfloor\big)\right) \mathrm{e}(n\xi) \right| \mathrm{d}\alpha. \tag{3.3.3}$$

Let $\rho_2 \geq \rho_1 > 0$. There exist $\eta > 0$ and a constant C such that

$$\frac{S_0}{ND} \leq CN^{-\eta} \tag{3.3.4}$$

holds for all real numbers $D, N \geq 1$ satisfying $N^{\rho_1} \leq D \leq N^{\rho_2}$ and for all $\xi \in \mathbb{R}$.

In the proof of these results, we will use the following essential estimate of a *Gowers uniformity norm* of the Thue–Morse sequence (see Konieczny [89]).

Proposition 3.3.3. *Let $k \geq 2$ be an integer. There exists some $\eta > 0$ and some C such that*

$$\frac{1}{2^{(k+1)\rho}} \sum_{\substack{0 \leq n < 2^{\rho} \\ 0 \leq r_1, \dots, r_k < 2^{\rho}}} \mathrm{e}\left(\frac{1}{2} \sum_{\varepsilon \in \{0,1\}^k} s_{\rho}(n + \varepsilon \cdot r)\right) \leq C 2^{-\rho\eta}$$

for all $\rho \geq 0$, where $\varepsilon \cdot r = \sum_{1 \leq i \leq k} \varepsilon_i r_i$.

Remark 7. Since the paper [89] by Konieczny also handles the Rudin–Shapiro sequence, it is certainly possible to prove analogous theorems for this sequence instead of the Thue–Morse sequence.

We wish to give a rough idea of the proof of Proposition 3.3.1 (Proposition 3.3.2 being proved essentially in the same way.)

Idea of the proof of Proposition 3.3.1. The key idea is to reduce the number of digits that have to be taken into account, and thus to replace the sum-of-digits function s by its truncated version s_{ρ}. Here 2^{ρ} will be significantly smaller than N, so that (we simplify things a bit to convey the idea) we may replace the sum over $s(nd+a)$ by a full sum over the periodic function

$s_\rho(n)$. This reducing of the digits is achieved by a refinement of the method used by Müllner and the author [124], which in turn builds on the ideas from the papers [108, 110] by Mauduit and Rivat.

First, we apply Van der Corput's inequality and use a "carry propagation lemma" in order to replace s by s_λ. In general, 2^λ will be much larger than N, so that we have to reduce λ further. The next step is to apply the generalized Van der Corput inequality repeatedly. With each application, we remove μ many digits. This is achieved by appealing to the Dirichlet approximation theorem, by which we can find a multiple of $\alpha = d/2^{j\mu}$ that is close to a multiple of 2^μ. This property can be used to discard the μ lowest digits.

By this repeated application the estimate is reduced to an estimate of a Gowers uniformity norm of the Thue–Morse sequence, and we use the method of proof of Konieczny [89] in order to obtain this estimate. The application of Van der Corput's inequality in the context of digital problems is well-established, beginning with the work of Mauduit and Rivat [108, 110]. The combination with Gowers norms however is novel, and we think that this connection is a fruitful one: iterated application of Van der Corput's inequality leads to multiple correlations, which in a natural way lead to Gowers norms.

3.4 Lemmas

We have the following series of lemmas that can also be found in our earlier paper with Müllner [124]. The first lemma can be proved by elementary considerations.

Lemma 3.4.1. *Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$.*

$$\text{If } \|a\| < \varepsilon \text{ and } \|b\| \geq \varepsilon, \text{ then } \lfloor a+b \rfloor = \langle a \rangle + \lfloor b \rfloor. \tag{3.4.1}$$

$$\|na\| \leq n\|a\|. \tag{3.4.2}$$

$$\text{If } \|a\| < \varepsilon \text{ and } 2n\varepsilon < 1, \text{ then } \langle na \rangle = n\langle a \rangle. \tag{3.4.3}$$

As an essential tool, we will use repeatedly the following generalized Van der Corput inequality [108, Lemme 17].

Lemma 3.4.2. *Let I be a finite interval in $\mathbb{Z}$ containing N integers and let z_n be a complex number for $n \in I$. For all integers $K \geq 1$ and $R \geq 1$ we have*

$$\left| \sum_{n \in I} z_n \right|^2 \leq \frac{N + K(R-1)}{R} \sum_{0 \leq |r| < R} \left(1 - \frac{|r|}{R}\right) \sum_{\substack{n \in I \\ n + Kr \in I}} z_{n+Kr} \overline{z_n}. \tag{3.4.4}$$

Assume that α is a real number and N is a nonnegative integer. We define the *discrepancy* of the sequence $n\alpha$ modulo 1:

$$D_N(\alpha) = \sup_{\substack{0 \leq x \leq 1 \\ y \in \mathbb{R}}} \left| \frac{1}{N} \sum_{n < N} 1_{[0,x)+y+\mathbb{Z}}(n\alpha) - x \right|.$$

Applying this definition, using $x = 1/(KT)$, $y = t/(KT)$, and α/K instead of α, we obtain the following lemma.

Lemma 3.4.3. *Let J be an interval in $\mathbb{R}$ containing N integers and let α and β be real numbers. Assume that t, T, ℓ and L are integers such that $0 \le t < T$ and $0 \le \ell < L$. Then*

$$\left|\left\{n \in J : \frac{t}{T} \le \{n\alpha+\beta\} < \frac{t+1}{T}, \lfloor n\alpha+\beta\rfloor \equiv \ell \bmod L\right\}\right| = \frac{N}{LT} + \mathcal{O}\left(ND_N\left(\frac{\alpha}{L}\right)\right)$$

with an absolute implied constant.

In the estimation of our error terms, we will use the following mean discrepancy results (Lemma 3.4 in [124]).

Lemma 3.4.4. *For integers $\mu \ge 0$ and $N \ge 1$ we have*

$$\sum_{0\le d<2^\mu} D_N\left(\frac{d}{2^\mu}\right) \le C_1 \frac{N+2^\mu}{N}(\log^+ N)^2.$$

Also, the estimate

$$\int_0^1 D_N(\alpha)\,\mathrm{d}\alpha \le C_2 \frac{(\log^+ N)^2}{N}$$

holds. The constants C_1 and C_2 in these estimates are absolute.

The following "carry propagation lemma" will allow us to replace the sum-of-digits function s by its truncated version s_λ. Statements of this type were used by Mauduit and Rivat in their papers on the sum of digits of primes and squares [108, 110].

Lemma 3.4.5. *Let r, N, λ be nonnegative integers and $\alpha > 0, \beta \ge 0$ real numbers. Assume that I is an interval containing N integers. Then*

$$\begin{aligned}\big|\big\{n \in I : s\big(\lfloor(n+r)\alpha+\beta\rfloor\big) - s\big(\lfloor n\alpha+\beta\rfloor\big) \ne s_\lambda\big(\lfloor(n+r)\alpha+\beta\rfloor\big) - s_\lambda\big(\lfloor n\alpha+\beta\rfloor\big)\big\}\big| \\ \le r(N\alpha/2^\lambda + 2).\end{aligned}$$

Let $\mathcal{F}_n$ the set of rational numbers p/q such that $1 \le q \le n$, the *Farey series of order n*. Each $a \in \mathcal{F}_n$ has two *neighbours* $a_L, a_R \in \mathcal{F}_n$, satisfying $a_L < a < a_R$ and $(a_L, a)\cap\mathcal{F}_n = (a, a_R)\cap\mathcal{F}_n = \emptyset$. We have the following elementary lemma concerning this set (see [82, Chapter 3]).

Lemma 3.4.6. *Assume that a/b, c/d are reduced fractions such that $b, d > 0$ and $a/b < c/d$. Then $a/b < (a+c)/(b+d) < c/d$. If a/b and c/d are neighbours in the Farey series $\mathcal{F}_n$, then $bc - ad = 1$ and $b + d > n$, moreover*

$$(a+c)/(b+d) - a/b < \frac{1}{bn} \quad \text{and} \quad c/d - (a+c)/(b+d) < \frac{1}{dn}.$$

Let $\alpha \in \mathbb{R}$ and Q a positive integer. We assign a fraction $p_Q(\alpha)/q_Q(\alpha)$ to α according to the Farey dissection of the reals: consider reduced fractions $a/b < c/d$ that are neighbours in the Farey series $\mathcal{F}_Q$, such that $a/b \le \alpha < c/d$. If $\alpha < (a+c)/(b+d)$, then set $p_Q(\alpha) = a$ and $q_Q(\alpha) = b$, otherwise set $p_Q(\alpha) = c$ and $q_Q(\alpha) = d$. Lemma 3.4.6 implies

$$\big|q_Q(\alpha)\alpha - p_Q(\alpha)\big| < Q^{-1}. \tag{3.4.5}$$

We will call an interval of the form $\{\alpha \in \mathbb{R} : p_Q(\alpha) = p, q_Q(\alpha) = q\}$ a *Farey interval* around p/q.

3.5 Proof of Propositions 3.3.1 and 3.3.2

As in the proof of Proposition 2.5 in [124], for (3.3.2) and (3.3.4) to hold it is sufficient to prove that there exists $\eta > 0$ and a constant C such that

$$\frac{S_0(N, 2^\nu, \xi)}{N 2^\nu} \le C N^{-\eta}$$

for all real numbers ξ and for all positive integers N and ν such that there exists a real number $D \ge 1$ satisfying $N^{\rho_1} \le D \le N^{\rho_2}$ and $D < 2^\nu \le 2D$, where S_0 is defined according to (5.2.50) or (3.3.3).

In order to treat the two propositions to some extent in parallel, we will work with two measures $\boldsymbol{\mu}$: for Proposition 3.3.1 we take the measure defined by $\boldsymbol{\mu}(A) = |A \cap \mathbb{Z}|$, counting the number of integers inside a set, while for Proposition 3.3.2, $\boldsymbol{\mu}$ is the Lebesgue measure. We note that in this proof, implied constants in estimates depend only on the variable k, whose meaning will become clear later.

By Cauchy–Schwarz, followed by Van der Corput's inequality (3.4.4) (R_0 will be specified later), we obtain

$$\begin{aligned}\big|S_0(N, 2^\nu, \xi)\big|^2 \le 2^\nu \frac{N + R_0}{R_0} \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta \ge 0} \sum_{0 \le |r_0| < R_0} \Big(1 - \frac{|r_0|}{R_0}\Big) \mathrm{e}\big(r_0 \xi\big) \\ \times \sum_{\substack{0 \le n < N \\ 0 \le n + r_0 < N}} \mathrm{e}\bigg(\frac{1}{2} s\big(\lfloor (n + r_0)\alpha + \beta \rfloor\big) - \frac{1}{2} s\big(\lfloor n\alpha + \beta \rfloor\big)\bigg) \mathrm{d}\boldsymbol{\mu}(\alpha)\end{aligned}$$

We apply the carry propagation lemma (Lemma 3.4.5), treat the summand $r_0 = 0$ separately, and omit the condition $0 \le n + r_0 < N$. Moreover, we consider r_0 and $-r_0$ synchronously. In this way we obtain for all $\lambda \ge 0$

$$\begin{aligned}\big|S_0(N, 2^\nu, \xi)\big|^2 \ll \big(2^\nu N\big)^2 E_0 + \frac{2^\nu N}{R_0} \sum_{1 \le r_0 < R_0} \\ \times \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta \ge 0} \bigg| \sum_{0 \le n < N} \mathrm{e}\bigg(\frac{1}{2} s_\lambda\big(\lfloor (n + r_0)\alpha + \beta \rfloor\big) - \frac{1}{2} s_\lambda\big(\lfloor n\alpha + \beta \rfloor\big)\bigg)\bigg| \mathrm{d}\boldsymbol{\mu}(\alpha),\end{aligned}$$

where

$$E_0 = \frac{1}{R_0} + \frac{R_0\, 2^\nu}{2^\lambda} + \frac{R_0}{N}.$$

We apply Cauchy–Schwarz on the sum over r_0 and the integral over α in order to prepare our expression for another application of Van der Corput's inequality. It follows that

$$\big|S_0(N, 2^\nu, \xi)\big|^4 \ll \frac{2^{3\nu} N^2}{R_0} \sum_{1 \le r_0 < R_0} \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta \ge 0} \big|S_1\big|^2 \mathrm{d}\boldsymbol{\mu}(\alpha) + \big(2^\nu N\big)^4 E_0$$

where

$$S_1 = \sum_{0 \le n < N} \mathrm{e}\bigg(\frac{1}{2} s_\lambda\big(\lfloor (n + r_0)\alpha + \beta \rfloor\big) - \frac{1}{2} s_\lambda\big(\lfloor n\alpha + \beta \rfloor\big)\bigg).$$

(Note that the error term is also squared, but if it is larger or equal to 1, the estimate is trivial anyway. We will use this argument again in a moment.) We apply Van der Corput's inequality (3.4.4) with $R = R_1$ and $K = K_1$ to be chosen later:

$$\big|S_1\big|^2 \le \frac{N + K_1(R_1-1)}{R_1} \sum_{0\le|r_1|<R_1} \Big(1 - \frac{|r_1|}{R_1}\Big) \times \sum_{\substack{0\le n<N\\ 0\le n+r_1K_1<N}} \mathrm{e}\bigg(\frac{1}{2} \sum_{\varepsilon_0,\varepsilon_1\in\{0,1\}} s_\lambda\big(\lfloor(n+\varepsilon_0r_0+\varepsilon_1r_1K_1)\alpha+\beta\rfloor\big)\bigg),$$

therefore, combining the summands for r_1 and $-r_1$ and omitting the condition $0 \le n+r_1K_1 < N$,

$$\big|S_0(N,2^\nu,\xi)\big|^4 \ll \frac{2^{3\nu}N^3}{R_0\,R_1} \sum_{\substack{1\le r_0<R_0\\ 0\le r_1<R_1}} \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta\ge0}\big|S_2\big|\,\mathrm{d}\boldsymbol{\mu}(\alpha) + \big(2^\nu N\big)^4\big(E_0+E_1\big),$$

where

$$S_2 = \sum_{0\le n<N} \mathrm{e}\bigg(\frac{1}{2} \sum_{\varepsilon_0,\varepsilon_1\in\{0,1\}} s_\lambda\big(\lfloor(n+\varepsilon_0r_0+\varepsilon_1r_1K_1)\alpha+\beta\rfloor\big)\bigg)$$

and

$$E_1 = \frac{R_1K_1}{N}.$$

Cauchy–Schwarz over r_0, r_1 and α yields

$$\big|S_0(N,\nu,\xi)\big|^8 \ll \frac{2^{7\nu}N^6}{R_0R_1} \sum_{\substack{1\le r_0<R_0\\ 0\le r_1<R_1}} \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta\ge0}|S_2|^2\,\mathrm{d}\boldsymbol{\mu}(\alpha) + \big(2^\nu N\big)^8\big(E_0+E_1\big).$$

We apply Van der Corput's inequality with $R = R_2$ and $K = K_2$ to be chosen later:

$$\frac{\big|S_0(N,2^\nu,\xi)\big|^8}{\big(2^\nu N\big)^8} \ll \big(E_0+E_1+E_2\big) + \frac{1}{R_0R_1R_2 2^\nu N} \sum_{\substack{1\le r_0<R_0\\ 0\le r_1<R_1\\ 0\le r_2<R_2}} \int_{2^\nu}^{2^{\nu+1}} \sup_{\beta\ge0}\big|S_3\big|\,\mathrm{d}\boldsymbol{\mu}(\alpha)$$

where

$$S_3 = \sum_{0\le n<N} \mathrm{e}\bigg(\frac{1}{2} \sum_{\varepsilon_0,\varepsilon_1,\varepsilon_2\in\{0,1\}} s_\lambda\big(\lfloor n\alpha+\beta+\varepsilon_0r_0\alpha+\varepsilon_1r_1K_1\alpha+\varepsilon_2r_2K_2\alpha\rfloor\big)\bigg)$$

and $E_2 = R_2K_2/N$. Continuing in this manner and replacing the range of integration (we note that we are going to choose $\lambda > \nu$ later), we obtain

$$\bigg|\frac{S_0(N,2^\nu,\xi)}{2^\nu N}\bigg|^{2^{k+1}} \ll \big(E_0+E_1+\cdots+E_k\big) + \frac{1}{R_0R_1\cdots R_k 2^\nu N} \sum_{\substack{1\le r_0<R_0\\ 0\le r_i<R_i,\,1\le i\le k}} \int_0^{2^\lambda} \sup_{\beta\ge0}\big|S_4\big|\,\mathrm{d}\boldsymbol{\mu}(\alpha), \quad (3.5.1)$$

where

$$S_4 \;=\; \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_\lambda\big(\lfloor n\alpha \,+\, \beta \,+\, \varepsilon_0 r_0\alpha \,+\, \varepsilon_1 r_1 K_1\alpha \,+\, \cdots \,+\, \varepsilon_k r_k K_k\alpha\rfloor\big)\right)$$

and

$$E_0 = \frac{1}{R_0} + \frac{R_0\, 2^\nu}{2^\lambda} + \frac{R_0}{N},$$
$$E_i = \frac{R_i\, K_i}{N} \quad \text{for } 1\le i\le k.$$

Now we choose the multiples $K_1,\dots,K_k$ in such a way that the number of digits to be taken into account is reduced from λ to $\rho := \lambda-(k+1)\mu$, where μ is chosen later. For this we use Farey series, see (3.4.5). Let

$$K_1 = q_{2^{2\mu+2\sigma}}\left(\frac{\alpha}{2^{2\mu}}\right) q_{2^\sigma}\left(\frac{p_{2^{2\mu+2\sigma}}\left(\alpha/2^{2\mu}\right)}{2^{(k-1)\mu}}\right);$$
$$K_i = q_{2^{\mu+2\sigma}}\left(\frac{\alpha}{2^{(i+1)\mu}}\right) q_{2^\sigma}\left(\frac{p_{2^{\mu+2\sigma}}\left(\alpha/2^{(i+1)\mu}\right)}{2^{(k-i)\mu}}\right) \quad \text{for } 2\le i<k;$$
$$K_k = q_{2^{\mu+\sigma}}\left(\frac{\alpha}{2^{(k+1)\mu}}\right),$$

where σ is chosen later. Moreover, we set

$$M_1 = p_{2^{2\mu+2\sigma}}\left(\frac{\alpha}{2^{2\mu}}\right) q_{2^\sigma}\left(\frac{p_{2^{2\mu+2\sigma}}\left(\alpha/2^{2\mu}\right)}{2^{(m-1)\mu}}\right);$$
$$M_i = p_{2^{\mu+2\sigma}}\left(\frac{\alpha}{2^{(i+1)\mu}}\right) q_{2^\sigma}\left(\frac{p_{2^{\mu+2\sigma}}\left(\alpha/2^{(i+1)\mu}\right)}{2^{(k-i)\mu}}\right) \quad \text{for } 2\le i<k;$$
$$M_k = p_{2^{\mu+\sigma}}\left(\frac{\alpha}{2^{(k+1)\mu}}\right).$$

By Lemma 3.4.6, estimating the second factor in the definition of K_i and M_i by 2^σ, we have

$$\begin{aligned} \left|K_1\alpha - 2^{2\mu}M_1\right| &< 2^{-\sigma};\\ \left|\frac{K_i\alpha}{2^{i\mu}} - 2^\mu M_i\right| &< 2^{-\sigma} \quad \text{for } 2\le i<k;\\ \left|\frac{K_k\alpha}{2^{k\mu}} - 2^\mu M_k\right| &< 2^{-\sigma}. \end{aligned} \tag{3.5.2}$$

We are going to use these inequalities in order to replace $r_iK_i\alpha$ in the sum S_4, starting with $r_1K_1\alpha$. We treat the case when α is an integer first: in this case, $K_1\alpha = 2^{2\mu}M_1$, and by the fact that the arguments of s_λ corresponding to $\varepsilon_1 = 0,1$ differ by a multiple of $2^{2\mu}$ we may shift the argument by 2μ digits and thus reduce the number of digits to be taken into account from λ to $\lambda-2\mu$.

$$S_4 = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_{2\mu,\lambda}\left(\lfloor n\alpha+\beta\right.\right.$$

$$+\varepsilon_0 r_0\alpha+\varepsilon_1 r_1 M_1 2^{2\mu}+\varepsilon_2 r_2 K_2\alpha+\cdots+\varepsilon_k r_k K_k\alpha\big\rfloor\big)\Big)$$

$$=\sum_{0\le n<N}\mathrm{e}\Big(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}}s_{\lambda-2\mu}\Big(\Big\lfloor\frac{n\alpha+\beta}{2^{2\mu}}+\frac{\varepsilon_0 r_0\alpha}{2^{2\mu}}+\varepsilon_1 r_1 M_1+\frac{\varepsilon_2 r_2 K_2\alpha}{2^{2\mu}}+\cdots+\frac{\varepsilon_k r_k K_k\alpha}{2^{2\mu}}\Big\rfloor\Big)\Big).$$

In the case $\alpha\notin\mathbb{Z}$, we use the inequalities (3.5.2) and the argument that $n\alpha$-sequences are usually not close to an integer. This can be made precise as follows. Assume that

$$\|n\alpha+\beta'\|\ge R_1/2^\sigma, \tag{3.5.3}$$

where $\beta'=\beta+\varepsilon_0 r_0\alpha+\varepsilon_2 r_2 K_2\alpha+\cdots+\varepsilon_k r_k K_k\alpha$, and that $2R_1<2^\sigma$. Using the inequality (3.4.3) in Lemma 3.4.1 with $\varepsilon=1/2^\sigma$, where $\sigma\ge1$ is chosen later, and (3.4.5), we obtain

$$\big\langle r_1 K_1\alpha\big\rangle=r_1\big\langle K_1\alpha\big\rangle=r_1 2^{2\mu}M_1.$$

Applying (3.4.1), setting $\varepsilon=R_1/2^\sigma$, we see that (3.5.3) together with (3.5.2) implies

$$\lfloor n\alpha+r_1K_1\alpha+\beta'\rfloor=\lfloor n\alpha+r_1 2^{2\mu}M_1+\beta'\rfloor.$$

The number of n where hypothesis (3.5.3) fails for some $\varepsilon_0,\varepsilon_2,\dots,\varepsilon_k$ can be estimated by discrepancy estimates for $\{n\alpha\}$-sequences: for all positive integers N and $2R_1<2^\sigma$ we have

$$\begin{aligned}&\big|\big\{n\in[0,N-1]:\|n\alpha+\beta'\|\le R_1/2^\sigma\big\}\big|\\&\quad=\big|\big\{n\in[0,N-1]:n\alpha+\beta'\in[-R_1/2^\sigma,R_1/2^\sigma]+\mathbb{Z}\big\}\big|\\&\quad=\big|\big\{n\in[0,N-1]:n\alpha\in[0,2R_1/2^\sigma]-\beta'-R_1/2^\sigma+\mathbb{Z}\big\}\big|\\&\quad\le ND_N(\alpha)+2R_1N/2^\sigma.\end{aligned}$$

Therefore, the number of $n\in[0,N-1]$ such that there exist $\varepsilon_0,\varepsilon_2,\dots,\varepsilon_k\in\{0,1\}$ with $\|n\alpha+\beta'\|\le R_1/2^\sigma$ is bounded by $2^kN\big(D_N(\alpha)+2R_1/2^\sigma\big)$, which is $\ll N\big(D_N(\alpha)+2R_1/2^\sigma\big)$ by our convention that implied constants may depend on k.

We replace $K_1\alpha$ by $2^{2\mu}M_1$ and subsequently shift the digits by 2μ and obtain

$$S_4=\sum_{0\le n<N}\mathrm{e}\Big(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}}s_{\lambda-2\mu}\Big(\Big\lfloor\frac{n\alpha+\beta}{2^{2\mu}}+\frac{\varepsilon_0 r_0\alpha}{2^{2\mu}}+\varepsilon_1 r_1 M_1+\frac{\varepsilon_2 r_2 K_2\alpha}{2^{2\mu}}+\cdots+\frac{\varepsilon_k r_k K_k\alpha}{2^{2\mu}}\Big\rfloor\Big)\Big)+\mathcal{O}\big(ND_N(\alpha)+NR_1/2^\sigma\big)$$

Repeating this argument for all $i\in\{2,\dots,k\}$, we obtain

$$\begin{aligned}S_4=N\mathcal{O}\Big(\widetilde{D}_N(\alpha)+D_N\Big(\frac{\alpha}{2^{2\mu}}\Big)+\cdots+D_N\Big(\frac{\alpha}{2^{k\mu}}\Big)+\frac{R_1+\cdots+R_k}{2^\sigma}\Big)\\+\sum_{0\le n<N}\mathrm{e}\Big(\frac{1}{2}\sum_{\varepsilon_1,\dots,\varepsilon_k\in\{0,1\}}s_{\lambda-(k+1)\mu}\Big(\Big\lfloor\frac{n\alpha+\beta}{2^{(k+1)\mu}}+\frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}+\sum_{1\le i\le k}\frac{\varepsilon_i r_i M_i}{2^{(k-i)\mu}}\Big\rfloor\Big)\Big),\end{aligned}$$

where $\widetilde{D}_N(\alpha)=D_N(\alpha)$ if $\alpha\notin\mathbb{Z}$ and $\widetilde{D}_N(\alpha)=0$ otherwise.

Now the second factor in the definition of K_i comes into play. We use the definition of M_i together with the approximation property (3.4.5), and apply the discrepancy estimate for $\{n\alpha\}$-sequences again to obtain

$$S_4 = N\mathcal{O}\left(\widetilde{D}_N(\alpha) + D_N\left(\frac{\alpha}{2^{2\mu}}\right) + \cdots + D_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right) + \frac{R_1 + \cdots + R_k}{2^\sigma}\right) + S_5, \tag{3.5.4}$$

where

$$S_5 = \sum_{0\le n<N} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_{\lambda-(k+1)\mu}\left(\left\lfloor \frac{n\alpha+\beta}{2^{(k+1)\mu}} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor + \sum_{1\le i\le k}\varepsilon_i r_i \mathfrak{p}_i\right)\right),$$

and

$$\begin{aligned}
\mathfrak{p}_1 &= p_{2^\sigma}\left(\frac{p_{2^{2\mu+2\sigma}}\left(\alpha/2^{2\mu}\right)}{2^{(k-1)\mu}}\right);\\
\mathfrak{p}_i &= p_{2^\sigma}\left(\frac{p_{2^{\mu+2\sigma}}\left(\alpha/2^{(i+1)\mu}\right)}{2^{(k-i)\mu}}\right) \quad \text{for } 2\le i<k;\\
\mathfrak{p}_k &= p_{2^{\mu+\sigma}}\left(\frac{\alpha}{2^{(k+1)\mu}}\right).
\end{aligned} \tag{3.5.5}$$

Our next goal is to remove the Beatty sequence occurring in S_5, and also to remove the integers $\mathfrak{p}_i$. The resulting expression can be handled by the Gowers norm estimate given in Proposition 3.3.3, which will finish the proof.

We start by splitting the Beatty sequence into two summands. Let t, T be integers such that $0 \le t < T$ and define

$$S_6 = \sum_{\substack{0\le n<N\\ \frac{t}{T}\le\left\{\frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\}<\frac{t+1}{T}}} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_{\lambda-(k+1)\mu}\left(\left\lfloor \frac{n\alpha+\beta+\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor + \sum_{1\le i\le k}\varepsilon_i r_i\mathfrak{p}_i\right)\right).$$

We define

$$G = \left\{1\le t<T : \left[\frac{t}{T} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}, \frac{t+1}{T} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right)\cap\mathbb{Z} = \emptyset\right\}.$$

Clearly we have $|G| \ge T-2$, since we have to exclude at most one t. For $t\in\{0,\dots,T-1\}\setminus G$ we estimate S_6 trivially, using Lemma 3.4.3: we obtain

$$S_6 \ll \frac{N}{T} + ND_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right). \tag{3.5.6}$$

Assume that $t\in G$ and that $t/T \le \{(n\alpha+\beta)/2^{(k+1)\mu}\} < (t+1)/T$. Then

$$\left\lfloor \frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\rfloor + \frac{t}{T} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}} \le \frac{n\alpha+\beta+\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}} < \left\lfloor \frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\rfloor + \frac{t+1}{T} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}$$

and the assumption $t\in G$ gives

$$\left\lfloor \frac{n\alpha+\beta+\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor = \left\lfloor \frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\rfloor + \left\lfloor \frac{t}{T} + \frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor$$

for $\varepsilon_0 \in \{0,1\}$. From these observations we obtain for $t \in G$:

$$S_6 = \sum_{0\le m<2^\rho} \sum_{\substack{0\le n<N \\ \frac{t}{T}\le\left\{\frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\}<\frac{t+1}{T} \\ \left\lfloor\frac{n\alpha+\beta}{2^{(k+1)\mu}}\right\rfloor\equiv m \bmod 2^\rho}} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_\rho\left(m+\left\lfloor\frac{t}{T}+\frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor+\sum_{1\le i\le k}\varepsilon_i r_i\mathfrak{p}_i\right)\right).$$

Note that the Beatty sequence $\lfloor(n\alpha+\beta)/2^{(k+1)\mu}\rfloor$ does not occur in the summand any more. We may therefore remove the second summation by estimating the number of times the three conditions under the summation sign are satisfied. At this point we want to stress the fact that N is going to be significantly larger than $2^\rho = 2^{\lambda-(k+1)\mu}$. Using Lemma 3.4.3 and the usually very small discrepancy of $n\alpha$-sequences, this fact will enable us to remove the summation over n, while introducing only a negligible error term for most α. This is the point in the proof where the successive "cutting away" of binary digits with the help of Farey series pays off.

By Lemma 3.4.3, applied with $L = 2^\rho$, and noting that $\lambda = (k+1)\mu+\rho$, we obtain for $t \in G$

$$S_6 = \frac{N}{2^\rho T}\,S_7 + \mathcal{O}\left(2^\rho N D_N\left(\frac{\alpha}{2^\lambda}\right)\right), \tag{3.5.7}$$

where

$$S_7 = \sum_{0\le m<2^\rho} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}} s_\rho\left(m+\left\lfloor\frac{t}{T}+\frac{\varepsilon_0 r_0\alpha}{2^{(k+1)\mu}}\right\rfloor+\sum_{1\le i\le k}\varepsilon_i r_i\mathfrak{p}_i\right)\right).$$

We note the important fact that this expression is independent of β. This will allow us to remove the maximum over β inside the integral over α, and thus prove the strong statement on the level of distribution.

We wish to simplify this expression in such a way that Proposition 3.3.3 is applicable. To this end, we use the summation over r_i and the integral over α. We define

$$S_8 = \int_0^{2^\lambda} \sum_{0\le r_1,\dots,r_k<2^\rho} \left|S_7\right| \mathrm{d}\boldsymbol{\mu}(\alpha),$$

which is an expression that will appear when we expand the original sum S_0.

We are going to apply the argument that for most $\alpha < 2^\lambda$ (with respect to $\boldsymbol{\mu}$) the 2-adic valuation of $\mathfrak{p}_1,\dots,\mathfrak{p}_k$ is small. For these α, the term $r_i\mathfrak{p}_i \bmod 2^\rho$ attains each $m \in \{0,\dots,2^\rho-1\}$ not too often, as r_i varies. We may therefore replace $r_i\mathfrak{p}_1$ by r_i and thus obtain full sums over r_i — at this point, we set

$$R_i = 2^\rho \quad \text{for} \quad 1 \le i \le k.$$

In order to make this argument work, we are going to utilize the following technical result, the proof of which we give in section 3.5.2.

Lemma 3.5.1. *Let $\mu,\lambda,\sigma,\gamma,k$ be nonnegative integers such that $k \ge 2$ and*

$$\begin{aligned} \lambda \ge (k+1)\mu, \quad \gamma \le \lambda-(k+1)\mu, \\ \mu \ge 4\sigma, \quad \sigma \ge \gamma \ge 1. \end{aligned} \tag{3.5.8}$$

Let $\mathfrak{p}_1,\dots,\mathfrak{p}_k$ be defined by (3.5.5) *and set*

$$A = \{\alpha \in \{0,\dots,2^\lambda-1\} : 2^{3\gamma} \mid \mathfrak{p}_i \text{ for some } i = 1,\dots,k\}.$$

Then

$$|A| = \mathcal{O}\big(2^{\lambda-\gamma}\big).$$

Analogously, if

$$A = \{\alpha \in [0, 2^\lambda] : 2^{3\gamma} \mid \mathfrak{p}_i \text{ for some } i = 1, \dots, k\}.$$

Then

$$\boldsymbol{\lambda}(A) = \mathcal{O}\big(2^{\lambda-\gamma}\big),$$

where $\boldsymbol{\lambda}$ is the Lebesgue measure. The implied constants only depend on m (and are independent of μ, λ, σ, and γ).

Let A be defined as in this lemma. We choose $R_i = 2^\rho$ for $1 \le i \le k$.

Assume that $\alpha \notin A$. Then by an elementary argument, $r_i\mathfrak{p}_i \bmod 2^\rho$ attains each value not more than $2^{3\gamma}$ times, as r_i runs through $\{0, \dots, 2^\rho - 1\}$. The contribution for $\alpha \in A$ will be estimated trivially by the lemma. We obtain

$$S_8 \le 2^{3\gamma k} \int_0^{2^\lambda} \sum_{0 \le r_1, \dots, r_k < 2^\rho} |S_9| \, \mathrm{d}\boldsymbol{\mu}(\alpha) + \mathcal{O}\left(2^{\lambda+(k+1)\rho-\gamma}\right),$$

where

$$S_9 = \sum_{0 \le n < 2^\rho} \mathrm{e}\left(\frac{1}{2} \sum_{\varepsilon_0, \dots, \varepsilon_k \in \{0,1\}} s_\rho\left(n + \left\lfloor \frac{t}{T} + \frac{\varepsilon_0 r_0 \alpha}{2^{(k+1)\mu}} \right\rfloor + \sum_{1 \le i \le k} \varepsilon_i r_i\right)\right).$$

The next step is removing the remaining floor function, using the integral over α. In the continuous case, the expression $\lfloor t/T + r_0 K_0 \alpha / 2^{(k+1)\mu} \rfloor \bmod 2^\rho$ runs through $\{0, \dots, 2^\rho - 1\}$ in a completely uniform manner. That is, for $r_0 \neq 0$ and $0 \le m < 2^\rho$ we have

$$\boldsymbol{\lambda}\left(\left\{\alpha \in [0, 2^\lambda] : \left\lfloor t/T + r_0 \alpha / 2^{(k+1)\mu} \right\rfloor \equiv m \bmod 2^\rho\right\}\right) = 2^{\lambda-\rho},$$

where $\boldsymbol{\lambda}$ is the Lebesgue measure. We consider the discrete case. Assume that $r_0 \le 2^{(k+1)\mu}$ (we will choose R_0 very small at the end of the proof, so that this will be satisfied). Then the set of $\alpha \in \{0, \dots, 2^\lambda - 1\}$ such that $\lfloor t/T + r_0\alpha/2^{(k+1)\mu} \rfloor \equiv m \bmod 2^\rho$ decomposes into at most $r_0 + 1$ intervals (note that $\lambda = (k+1)\mu + \rho$), each having $\le 2^{(k+1)\mu}/r_0 + 1$ elements. In total we have $\ll 2^{\lambda-\rho}$ elements, where the implied constant is absolute. It follows that

$$S_8 \ll 2^{\lambda+(k+1)\rho-\gamma} + 2^{\lambda-\rho+3\gamma k} \sum_{0 \le r_0, \dots, r_k < 2^\rho} |S_{10}(r_0, \dots, r_k)|,$$

where

$$S_{10}(r_0, \dots, r_k) = \sum_{0 \le n < 2^\rho} \mathrm{e}\left(\frac{1}{2} \sum_{\varepsilon_0, \dots, \varepsilon_k \in \{0,1\}} s_\rho\left(n + \sum_{0 \le i \le k} \varepsilon_i r_i\right)\right).$$

As a final step in the procedure of reducing the main theorems to Proposition 3.3.3, we are going to to remove the absolute value around S_{10}. For brevity, we set

$$g(n) = \sum_{\varepsilon_0, \dots, \varepsilon_k \in \{0,1\}} s_\rho\left(n + \sum_{0 \le i \le k} \varepsilon_i r_i\right)$$

By the 2^ρ-periodicity of g we have

$$\begin{aligned}\sum_{0\le r_0,\dots,r_k<2^\rho}|S_{10}(r_0,\dots,r_k)|^2 &= \sum_{0\le r_0,\dots,r_k<2^\rho}\sum_{0\le n_1,n_2<2^\rho}\mathrm{e}\left(\frac{1}{2}g(n_1)+\frac{1}{2}g(n_2)\right)\\ &= \sum_{0\le r_0,\dots,r_k<2^\rho}\sum_{0\le n_1<2^\rho}\sum_{0\le r_{k+1}<2^\rho}\mathrm{e}\left(\frac{1}{2}g(n_1)+\frac{1}{2}g(n_1+r_{k+1})\right)\\ &= \sum_{0\le r_0,\dots,r_{k+1}<2^\rho}\sum_{0\le n_1<2^\rho}\mathrm{e}\left(\frac{1}{2}g(n_1)+\frac{1}{2}g(n_1+r_{k+1})\right)\\ &= \sum_{0\le r_0,\dots,r_{k+1}<2^\rho}\sum_{0\le n_1<2^\rho}\mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon_0,\dots,\varepsilon_k\in\{0,1\}}\sum_{\varepsilon_{k+1}\in\{0,1\}}s_\rho(n_1+\varepsilon\cdot r+\varepsilon_{k+1}r_{k+1})\right)\\ &= \sum_{0\le r_0,\dots,r_{k+1}<2^\rho}S_{10}(r_0,\dots,r_{k+1}).\end{aligned}$$

We have therefore removed the absolute value around S_{10} for the price an additional variable r_{k+1}; see also [81, Section 4] for this type of argument. This means that we have reduced our main theorems to Proposition 3.3.3.

By this proposition and Cauchy-Schwarz we obtain

$$S_8 \ll 2^{\lambda+(k+1)\rho}\left(2^{-\gamma}+2^{3\gamma k-\eta\rho}\right) \tag{3.5.9}$$

for some $\eta>0$.

It remains to collect the error terms and to choose values for the free variables. Using (3.5.7) and (3.5.6), we obtain

$$\begin{aligned}S_5 &\ll \sum_{t\notin G}\left(\frac{N}{T}+ND_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right)\right)+\sum_{t\in G}\left(\frac{N}{2^\rho T}S_7+2^\rho ND_N\left(\frac{\alpha}{2^\lambda}\right)\right)\\ &\ll \frac{N}{2^\rho T}\sum_{t\in G}S_7+\frac{N}{T}+ND_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right)+2^\rho NTD_N\left(\frac{\alpha}{2^\lambda}\right)\end{aligned}$$

and by (3.5.4) and (3.5.1) we obtain

$$\begin{aligned}\left|\frac{S_0(N,\nu,\xi)}{2^\nu N}\right|^{2^{k+1}} &\ll \mathcal{O}\left(\frac{1}{R_0}+\frac{R_0\,2^\nu}{2^\lambda}+\frac{R_0}{N}+\frac{R_1K_1}{N}\cdots+\frac{R_kK_k}{N}\right)\\ &+\frac{1}{2^\nu N}\int_0^{2^\lambda}N\mathcal{O}\left(\widetilde{D}_N(\alpha)+D_N\left(\frac{\alpha}{2^{2\mu}}\right)+\cdots+D_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right)+\frac{R_1+\cdots+R_k}{2^\sigma}\right)\mathrm{d}\boldsymbol{\mu}(\alpha),\\ &+\frac{1}{2^\nu N}\int_0^{2^\lambda}\mathcal{O}\left(\frac{N}{T}+ND_N\left(\frac{\alpha}{2^{(k+1)\mu}}\right)+2^\rho TND_N\left(\frac{\alpha}{2^\lambda}\right)\right)\mathrm{d}\boldsymbol{\mu}(\alpha),\\ &+\frac{1}{R_0\cdots R_k2^\nu N}\frac{N}{2^\rho T}\sum_{t\in G}\sum_{1\le r_0<R_0}\int_0^{2^\lambda}\sum_{0\le r_1,\dots,r_k<2^\rho}\left|S_7\right|\mathrm{d}\boldsymbol{\mu}(\alpha).\end{aligned} \tag{3.5.10}$$

We employ the mean discrepancy estimates from Lemma 3.4.4. Assume that $\delta\le\lambda$. In the continuous case we have

$$\frac{1}{2^\nu}\int_0^{2^\lambda}D_N\left(\frac{\alpha}{2^\delta}\right)\mathrm{d}\alpha \ll 2^{\lambda-\nu-\delta}\int_0^{2^\delta}D_N\left(\frac{\alpha}{2^\delta}\right)\mathrm{d}\alpha \ll 2^{\lambda-\nu}\frac{(\log^+N)^2}{N},$$

while the discrete case gives

$$\frac{1}{2^\nu}\sum_{0\le d<2^\lambda} D_N\left(\frac{d}{2^\delta}\right) \ll 2^{\lambda-\delta-\nu}\frac{N+2^\delta}{N}(\log^+ N)^2 = 2^{\lambda-\nu}(\log^+ N)^2\left(\frac{1}{N}+\frac{1}{2^\delta}\right)$$

In total, noting that $\lambda \ge (k+1)\mu$, the discrepancy terms can be estimated by

$$\ll 2^{\lambda-\nu}(\log^+ N)^2 2^\rho T\left(\frac{1}{N}+\frac{1}{2^{2\mu}}\right).$$

By (3.5.9), the last summand in (3.5.10) can be estimated by

$$\ll 2^{\lambda-\nu}\left(2^{-\gamma}+2^{3\gamma k-\eta\rho}\right).$$

Moreover, using the facts $R_1=\cdots=R_k=2^\rho$ and $K_i \le 2^{2\mu+3\sigma}$ for $1\le i\le k$, we obtain

$$\begin{aligned}\left|\frac{S_0(N,\nu,\xi)}{2^\nu N}\right|^{2^{k+1}} \ll{}& \frac{1}{R_0}+\frac{R_0\,2^\nu}{2^\lambda}+\frac{R_0}{N}+\frac{2^{\rho+2\mu+3\sigma}}{N}+\\ &2^{\lambda-\nu}(\log^+ N)^2 2^\rho T\left(\frac{1}{N}+\frac{1}{2^{2\mu}}\right)+2^{\rho-\sigma+\lambda-\nu}+\frac{1}{T}+2^{\lambda-\nu}\left(2^{-\gamma}+2^{3\gamma k-\eta\rho}\right)\end{aligned} \tag{3.5.11}$$

with some implied constant only depending on k. Collecting also the requirements on the variables we assumed in the course of our calculation, we see that this estimate is valid as long as

$$\begin{aligned}&R_0, T\ge 1, k\ge 2, \gamma,\nu,\lambda,\rho,\mu\ge 0, && R_1=\cdots=R_k=2^\rho,\\ &\lambda>\nu, && \rho=\lambda-(k+1)\mu,\\ &\gamma\le\rho<\sigma-1, && \mu\ge 4\sigma,\\ &R_0\le 2^{(k+1)\mu}. &&\end{aligned} \tag{3.5.12}$$

It remains to choose the variables within these constraints. Choose the integer $j\ge 1$ in such a way that $N^{j-1}\le 2^\nu < N^j$ and set $k=3j-1$. Clearly, $k\ge 2$. We define

$$\mu=\left\lfloor\frac{\nu}{k+1+1/8}\right\rfloor,\quad \sigma=\lfloor\mu/4\rfloor,\quad \widetilde{\rho}=\nu-(k+1)\mu.$$

We obtain the inequalities $N\ge 2^{3\mu}$, $\mu\ge 4\sigma$, $\widetilde{\rho}\ge 0$. Moreover, for large ν we obtain $\widetilde{\rho}\sim\mu/8$.

Choose $\gamma=\lfloor\widetilde{\rho}\eta/(6k)\rfloor$ and $R_0=\lfloor 2^{\gamma/4}\rfloor$. Then the last summand in (3.5.11) is $\ll 2^{\lambda-\nu}\big(2^{-\gamma}+2^{-\widetilde{\rho}\eta/2}\big)\ll 2^{\lambda-\nu-\gamma}$. Finally, set $\lambda=\nu+\lfloor\gamma/2\rfloor$, $T=2^\gamma$ and $\rho=\lambda-(k+1)\mu$. It follows that $\rho=\widetilde{\rho}+\lfloor\gamma/2\rfloor\sim\frac{\mu}{8}(1+\eta/(12k))\le\mu/8+\mu/192$. Using these definitions, it is not hard to see that, for large N and ν, the requirements (3.5.12) are met.

Using the statements $N^{\rho_1}\le D\le N^{\rho_2}$ and $D<2^\nu\le 2D$ we can easily estimate (3.5.11) term by term and conclude that $S_0(N,\nu,\xi)/(2^\nu N)\le CN^{-\eta'}$ for some $\eta'>0$ and some constant C. This finishes the proof of Propositions 3.3.1 and 3.3.2 and therefore of our main theorems. It remains to prove our auxiliary results.

3.5.1 Proof of Proposition 3.3.3

We utilize ideas from the paper [89] by Konieczny. In that paper, he uses the Gowers norm on intervals in $\mathbb{Z}$, while we are concerned with the cyclic group $\mathbb{Z}/2^\rho\mathbb{Z}$. The proof of Proposition 3.3.3 is analogous to Konieczny's proof. In fact, it is possible to relate the two notions

of Gowers norms to each other and therefore avoid going into the details of the proof in [89] (Konieczny, private communication; we also thank the anonymous referee for pointing out this possibility). In this paper however, we chose to follow the proof from [89], as the argument is interesting and not unreasonably long.

Set

$$A_\rho(\mathbf{a}) = \frac{1}{2^{(k+1)\rho}} \sum_{\substack{0\le n<2^\rho \\ 0\le r_1,\dots,r_k<2^\rho}} \mathrm{e}\left(\frac{1}{2}\sum_{\varepsilon\in\{0,1\}^k} s_\rho(n+\varepsilon\cdot r+\mathbf{a}_\varepsilon)\right).$$

Then in analogy to equation (16) of [89], we get after a similar calculation (using $k\ge 2$)

$$A_{\rho+1}(\mathbf{a}) = \frac{(-1)^{|\mathbf{a}|}}{2^{k+1}} \sum_{e_0,\dots,e_k\in\{0,1\}} A_\rho(\delta(\mathbf{a},e)), \tag{3.5.13}$$

where $|\mathbf{a}| = \sum_{\varepsilon\in\{0,1\}^k}\mathbf{a}_\varepsilon$ and

$$\delta(\mathbf{a},e)_\varepsilon = \left\lfloor \frac{\mathbf{a}_\varepsilon + e_0 + \sum_{1\le i\le k}\varepsilon_i e_i}{2}\right\rfloor.$$

We define a directed graph with weighted edges according to (3.5.13). The set of vertices is given by the set of families $\mathbf{a}\in\mathbb{Z}^{\{0,1\}^k}$. There is an edge from $\mathbf{a}$ to $\mathbf{b}$ if and only if there is an $e=(e_0,\dots,e_k)\in\{0,1\}^{k+1}$ such that $\delta(\mathbf{a},e)=\mathbf{b}$ and this edge has the weight

$$w(\mathbf{a},\mathbf{b}) = \frac{(-1)^{|\mathbf{a}|}}{2^{k+1}}\left|\left\{e\in\{0,1\}^{k+1} : \delta(\mathbf{a},e)=\mathbf{b}\right\}\right|.$$

Note that

$$\sum_{\mathbf{b}\in\mathbb{Z}^{\{0,1\}^k}} |w(\mathbf{a},\mathbf{b})| = 1, \tag{3.5.14}$$

which we will need later. We are interested in the subgraph (V,E,w) induced by the set of vertices reachable from $\mathbf{0}$. This graph is finite: we have

$$\max_{\varepsilon\in\{0,1\}^k}|\delta(\mathbf{a},e)_\varepsilon| \le \frac{1}{2}\left(\max_{\varepsilon\in\{0,1\}^k}|\mathbf{a}_\varepsilon| + k + 1\right)$$

and by induction, it follows that $\max_{\varepsilon\in\{0,1\}^k}|\mathbf{a}_\varepsilon| < k+1$ for all $\mathbf{a}\in V$, which implies the finiteness of V.

This subgraph is strongly connected. We prove this by showing that $\mathbf{0}$ is reachable from each $\mathbf{a}\in V$. This follows immediately by considering the path given by the edges $(\mathbf{a}^{(0)},\mathbf{a}^{(1)})$, $(\mathbf{a}^{(1)},\mathbf{a}^{(2)}),\dots,(\mathbf{a}^{(j)},\mathbf{a}^{(j+1)})$ defined by $\mathbf{a}^{(0)}=\mathbf{a}$ and $\mathbf{a}^{(i+1)}=\delta(\mathbf{a}^{(i)},(0,\dots,0))$. It is clear from the definition of δ that such a path reaches $\mathbf{0}$ if j is large enough.

We wish to apply (3.5.13) recursively. We therefore define, for two vertices $\mathbf{a},\mathbf{b}\in V$ and a positive integer j, the weight $w_j(\mathbf{a},\mathbf{b})$ as the sum of all weights of paths of length j from $\mathbf{a}$ to $\mathbf{b}$. (Here the weight of a path is the product of the weights of the edges.)

In order to prove Proposition 3.3.3, it is sufficient to prove that there is a j such that

$$\sum_{\mathbf{b}\in V}|w_j(\mathbf{a},\mathbf{b})| < 1$$

for all $\mathbf{a}\in V$. In order to prove this, it is sufficient, by the strong connectedness of the graph and (3.5.14), to prove that there are two paths of the same length from $\mathbf{0}$ to $\mathbf{0}$ such

that their respective weights have different sign. One of this paths is the trivial one, choosing $e_0 = \cdots = e_j = 0$ in each step. This path has positive weight.

For the second path, we follow Konieczny [89, proof of Proposition 2.3]. As in that paper, we define $\mathbf{a}^{(0)} = \mathbf{a}^{(j+1)} = \mathbf{0}$ and for $1 \le i \le j$,

$$\mathbf{a}_\varepsilon^{(i)} = \begin{cases} 1, & \text{if } \varepsilon_1 = \cdots = \varepsilon_i = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Assuming for a moment that there is an edge from $\mathbf{a}^{(i)}$ to $\mathbf{a}^{(i+1)}$ for all $i \in \{0, \dots, j\}$, it is easy to see that each edge $(\mathbf{a}^{(i)}, \mathbf{a}^{(i+1)})$ has positive weight for $0 \le i < j$, while $(\mathbf{a}^{(j)}, \mathbf{a}^{(j+1)})$ has negative weight. Proving that these vertices indeed define a path is contained completely in the argument given in [89]. This finishes the proof of Lemma 3.3.3.

3.5.2 Proof of Lemma 3.5.1

We choose an integer $\gamma > 0$ and bound the size of the set of $\alpha < 2^\lambda$ such that $2^{3\gamma} \mid \mathfrak{p}_i$ for some $i \in \{1, \dots, k\}$. We will need the following two lemmas.

Lemma 3.5.2. *Let $\boldsymbol{\lambda}$ be the Lebesgue measure. Assume that $K \ge 1$ and $\gamma \ge 0$ are integers. Then*

$$\boldsymbol{\lambda}\big(\{x \in [0,1] : 2^\gamma \mid q_K(x)\}\big) \ll \frac{1}{2^\gamma} + \frac{1}{K}.$$

The constant in this estimate is absolute.

Proof. We have to sum up the lengths of the Farey intervals around p/q such that $2^\gamma \mid q$. By Lemma 3.4.6, each such fraction contributes at most $2/(Kq)$. By summing over $p \in \{1, \dots, q\}$, this gives a contribution $2/K$ for each multiple q of 2^γ, and we obtain a total contribution

$$\ll \sum_{\substack{1 \le q \le K \\ 2^\gamma \mid q}} \frac{1}{K} \le \frac{1}{2^\gamma} + \frac{1}{K}.$$

⛋

Lemma 3.5.3. *Let $x_0, \dots, x_{M-1} \in [0,1]$ and $\delta > 0$. Assume that $\|x_i - x_j\| \ge \delta$ for $i \ne j$. Then*

$$\big|\{n \in \{0, \dots, M-1\} : 2^\gamma \mid q_K(x_i)\}\big| \ll \frac{K^2}{2^\gamma} + \frac{1}{\delta}\left(\frac{1}{2^\gamma} + \frac{1}{K}\right).$$

The implied constant is absolute.

Proof. In each Farey interval around p/q such that q is divisible by 2^γ there are at most $2/(Kq\delta) + 1$ many points x_i. By summing over p and q, we can bound the number of points in such intervals by

$$\begin{aligned} \ll \sum_{\substack{1 \le q \le K \\ 2^\gamma \mid q}} \sum_{1 \le p \le q} \left(\frac{1}{qK\delta} + 1\right) &= \sum_{\substack{1 \le q \le K \\ 2^\gamma \mid q}} \left(\frac{1}{K\delta} + q\right) = \left(K2^{-\gamma} + 1\right)\frac{1}{K\delta} + \sum_{\substack{1 \le q \le K \\ 2^\gamma \mid q}} q \\ &\le \frac{1}{2^\gamma\delta} + \frac{1}{K\delta} + 2^\gamma \sum_{1 \le q' \le \lfloor K2^{-\gamma} \rfloor} q' \ll \frac{K^2}{2^\gamma} + \frac{1}{2^\gamma\delta} + \frac{1}{K\delta}. \end{aligned}$$

⛋

We proceed to the proof of Lemma 3.5.1. Consider $\mathfrak{p}_1$ and the case "α discrete". In this case, we have $p_{2^{2\mu+2\sigma}}(\alpha/2^{2\mu}) = \alpha$. Assume therefore that $\alpha = \alpha_0 + 2^{(k-1)\mu}\alpha_1$, where $\alpha_0 \in \{0, \dots, 2^{(k-1)\mu} - 1\}$ and $\alpha_1 \in \{0, \dots, 2^{\lambda-(k-1)\mu} - 1\}$.

Then

$$\mathfrak{p}_1 = p_{2^\sigma}\big(\alpha/2^{(k-1)\mu}\big) = p_{2^\sigma}\big(\alpha_0/2^{(k-1)\mu}\big) + q_{2^\sigma}\big(\alpha_0/2^{(k-1)\mu}\big)\alpha_1.$$

By Lemma 3.5.3, using also (3.5.8), it follows that the number of $\alpha_0 \in \{0, \dots, 2^{(k-1)\mu} - 1\}$ such that $2^\gamma \nmid q_{2^\sigma}\big(\alpha_0/2^{(k-1)\mu}\big)$ is $2^{(k-1)\mu}\,(1 - \mathcal{O}(2^{-\gamma}))$. For each such α_0, we let α_1 run through $\{0, \dots, 2^{\lambda-(k-1)\mu} - 1\}$. Then two occurrences α_1, α_1' such that $2^{2\gamma} \mid \mathfrak{p}_1$ are separated by at least 2^γ steps; it follows that the number of such α_1 is bounded by $2^{\lambda-(k-1)\mu-\gamma}$. Putting these errors together, we see that the number of $\alpha \in \{0, \dots, 2^\lambda - 1\}$ such that $2^{2\gamma} \nmid \mathfrak{p}_1$ is given by $2^{(k-1)\mu}\,(1 - \mathcal{O}(2^{-\gamma}))\,2^{\lambda-(k-1)\mu}\,(1 - \mathcal{O}(2^{-\gamma})) = 2^\lambda\,(1 - \mathcal{O}(2^{-\gamma}))$.

Next, we consider the continuous case. We write $\alpha = \alpha_0 + 2^{2\mu}\alpha_1 + 2^{(k+1)\mu}\alpha_2$, where $\alpha_0 \in [0, 2^{2\mu})$ is real and $\alpha_1 < 2^{(k-1)\mu}$ and $\alpha_2 < 2^{\lambda-(k+1)\mu}$ are nonnegative integers. Set $p = p_{2^{2\mu+2\sigma}}\big(\alpha_0/2^{2\mu}\big)$ and $q = q_{2^{2\mu+2\sigma}}\big(\alpha_0/2^{2\mu}\big)$. Then

$$\frac{p_{2^{2\mu+2\sigma}}\big(\alpha/2^{2\mu}\big)}{2^{(k-1)\mu}} = \frac{p + \big(\alpha_1 + 2^{(k-1)\mu}\alpha_2\big)q}{2^{(k-1)\mu}} = \frac{p + \alpha_1 q}{2^{(k-1)\mu}} + \alpha_2 q.$$

By the approximation property (3.4.5) (note that $\sigma \geq 1$) we have

$$\begin{aligned}\mathfrak{p}_1 &= \left\langle \left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}} + \alpha_2 q\right) q_{2^\sigma}\left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}}\right)\right\rangle \\ &= \left\langle \frac{p + \alpha_1 q}{2^{(k-1)\mu}} q_{2^\sigma}\left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}}\right)\right\rangle + \alpha_2 q\, q_{2^\sigma}\left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}}\right)\end{aligned}$$

and we note that the first summand does not depend on α_2.

As α_0 runs through $[0, 2^{2\mu}]$, we have by Lemma 3.5.2 $2^\gamma \nmid q$ in a set of measure $2^{2\mu}(1 - \mathcal{O}(2^{-\gamma} + 2^{-2\mu-2\sigma}))$. By (3.5.8), this is $2^{2\mu}\big(1 - \mathcal{O}\big(2^{-\gamma}\big)\big)$. Assume that α_0 is such that $2^\gamma \nmid q$ and set $\gamma' = \nu_2(q) < \gamma$. Next, we let α_1 run. We choose $x_j = \big\{(p + jq)/2^{(k-1)\mu}\big\}$ for $0 \leq j < 2^{(k-1)\mu-\gamma'}$ and we note that these points satisfy $\|x_i - x_j\| \geq 1/2^{(k-1)\mu-\gamma'}$ for $i \neq j$. By Lemma 3.5.3 it follows that

$$\left\{\alpha_1 \in \{0, \dots, 2^{(k-1)\mu-\gamma'} - 1\} : 2^\gamma \mid q_{2^\sigma}\left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}}\right)\right\} \ll \frac{2^{2\sigma}}{2^\gamma} + 2^{(k-1)\mu-\gamma'}\left(\frac{1}{2^\gamma} + \frac{1}{2^\sigma}\right).$$

By (3.5.8), this is $\ll 2^{(k-1)\mu-\gamma'-\gamma}$. Performing this also for the other intervals of length $2^{(k-1)\mu-\gamma'}$, we obtain

$$\left\{\alpha_1 \in \{0, \dots, 2^{(k-1)\mu} - 1\} : 2^\gamma \mid q_{2^\sigma}\left(\frac{p + \alpha_1 q}{2^{(k-1)\mu}}\right)\right\} \ll 2^{(k-1)\mu-\gamma}.$$

Finally, α_2 runs through $\{0, \dots, 2^{\lambda-(k+1)\mu} - 1\}$ and we consider $\mathfrak{p}_1$. For given good α_1 and α_0 (such that $2^\gamma \nmid q$ and $2^\gamma \nmid q_{2^\sigma}((p + \alpha_1 q)/2^{(k-1)\mu})$), $\mathfrak{p}_1$ is an arithmetic progression in α_2 whose common difference is not divisible by $2^{2\gamma}$. Similarly to the discrete case, it follows that $\mathfrak{p}_1$ is divisible by $2^{3\gamma}$ for at most $2^{\lambda-(k+1)\mu-\gamma}$ many α_2. It follows that there is a set of measure

$$2^{2\mu}\big(1 - \mathcal{O}(2^{-\gamma})\big)2^{(k-1)\mu}\big(1 - \mathcal{O}(2^{-\gamma})\big)2^{\lambda-(k+1)\mu}\big(1 - \mathcal{O}(2^{-\gamma})\big) = 2^\lambda\big(1 - \mathcal{O}(2^{-\gamma})\big)$$

of $\alpha < 2^\lambda$ such that $2^{3\gamma} \nmid \mathfrak{p}_1$.

The cases $2 \le i \le k$ do not require any new ideas; we only give a sketch of a proof. Let $2 \le i < k$. We treat the discrete and continuous cases in parallel. We write $\alpha = \alpha_0 + 2^{(i+1)\mu}\alpha_1 + 2^{(k+1)\mu}\alpha_2$, where $\alpha_0 < 2^{(i+1)\mu}$, and $\alpha_1 < 2^{(k-i)\mu}$ and $\alpha_2 < 2^{\lambda-(k+1)\mu}$ are nonnegative integers. Set $p = p_{2^{\mu+2\sigma}}\big(\alpha_0/2^{(i+1)\mu}\big)$ and $q = q_{2^{\mu+2\sigma}}\big(\alpha_0/2^{(i+1)\mu}\big)$. Then

$$\mathfrak{p}_i = \left\langle \frac{p+\alpha_1 q}{2^{(k-i)\mu}} q_{2^\sigma}\left(\frac{p+\alpha_1 q}{2^{(k-i)\mu}}\right)\right\rangle + \alpha_2 q\, q_{2^\sigma}\left(\frac{p+\alpha_1 q}{2^{(k-i)\mu}}\right),$$

as before. By Lemmas 3.5.2 and 3.5.3 we have $2^\gamma \nmid q$ for α_0 in a set of measure $2^{(i+1)\mu}(1 - \mathcal{O}(2^{-\gamma}))$, where we used $2\mu+4\sigma \le (i+1)\mu$ in the discrete case. (We note that this last inequality is the reason for defining $\mathfrak{p}_1$ separately, using $2^{2\mu}$ instead of 2^μ.) The remaining steps are as before, and this case is finished.

Finally, in the case $i = k$ we write $\alpha = \alpha_0 + 2^{(k+1)\mu}\alpha_1$, where $\alpha_0 < (k+1)\mu$ and $\alpha_1 \in \{0, \dots, 2^{\lambda-(k+1)\mu} - 1\}$. Then

$$\mathfrak{p}_k = p_{2^{\mu+\sigma}}\big(\alpha_0/2^{(k+1)\mu}\big) + q_{2^{\mu+\sigma}}\big(\alpha_0/2^{(k+1)\mu}\big)\alpha_1.$$

By Lemmas 3.5.2 and 3.5.3 and (3.5.8) we have $2^\gamma \mid q_{2^{\mu+\sigma}}\big(\alpha_0/2^{(k+1)\mu}\big)$ for α_0 in a set of measure $\mathcal{O}(2^{(k+1)\mu-\gamma})$ and the statement follows as before.

In total, we have a set of measure $2^\lambda\big(1 - \mathcal{O}(2^{-\gamma})\big)$ of $\alpha < 2^\lambda$ such that $2^{3\gamma} \nmid \mathfrak{p}_i$ for all i.

Acknowledgements

The author wishes to thank Thomas Stoll for helpful discussions during his stay in Nancy, France, where the work on this project began. Moreover, the author wishes to thank Michael Drmota and Clemens Müllner for several fruitful discussions on the topic, and the anonymous referees for numerous suggestions. Finally, the author is indebted to Etienne Fouvry, Jakub Konieczny, Christian Mauduit, and Gwendal Collet for valuable advice.

Chapter 4

Gaps in the Thue–Morse word

Lukas Spiegelhofer
To appear in **Journal of the Australian Mathematical Society**
Published online by Cambridge University Press: 25 January 2022, pp. 1-35
DOI: https://doi.org/10.1017/S1446788721000380

Abstract

The Thue–Morse sequence is a prototypical automatic sequence found in diverse areas of mathematics, and in computer science. We study occurrences of factors w within this sequence, more precisely, the sequence of gaps between consecutive occurrences. This gap sequence is morphic; we prove that it is not automatic as soon as the length of w is at least 2, thereby answering a question by J. Shallit in the affirmative. We give an explicit method to compute the *discrepancy* of the number of occurrences of the block 01 in the Thue–Morse sequence. We prove that the sequence of discrepancies is the sequence of output sums of a certain base-2 transducer.

4.1 Introduction and main result

Automatic sequences can be defined via deterministic finite automata with output (DFAO): feeding the base-q expansion (where $q \geq 2$ is an integer) of $0, 1, 2, \ldots$ into such an automaton, we obtain an automatic sequence as its output, and each automatic sequence is obtained in this way. One of the simplest automatic sequences — in terms of the size of the defining substitution — is the Thue–Morse sequence $\mathbf{t}$. It is the fixed point of the substitution τ given by

$$\tau : \mathtt{0} \mapsto \mathtt{01}, \quad \mathtt{1} \mapsto \mathtt{10}, \tag{4.1.1}$$

starting with 0:

$$\mathbf{t} = \tau^\omega(\mathtt{0}) = \mathtt{0110100110010110100101100110100 1} \cdots . \tag{4.1.2}$$

(Here $\tau^\omega(\mathtt{0})$ denotes the point-wise limit of the iterations $\tau^k(\mathtt{0})$, in symbols $\tau^\omega(\mathtt{0})\big|_j = \lim_{k\to\infty} \tau^k(\mathtt{0})\big|_j$. We use analogous notation in other places too.) Occurrences of this sequence in different areas of mathematics can be found in the paper [4] by Allouche and Shallit, which also offers a good bibliography. Another survey paper on the Thue–Morse sequence was written by Mauduit [104].

Much more information concerning automatic and general morphic sequences is presented in the book [5] by Allouche and Shallit.

Terms 1 through 12 of the Thue–Morse sequence (the 0th term is omitted) make a peculiar appearance in *The Simpsons Movie* [26]:

> Russ Cargill: '[...] I want 10,000 tough guys, and I want 10,000 soft guys to make the tough guys look tougher! And here's how I want them arranged:
> tough, tough, soft, tough, soft, soft, tough, tough, soft, soft, tough, soft.'

This could, of course, be a coincidence. A different, more sensible explanation of this appearance is along the lines of Brams and Taylor [24, 36–44]. They rediscover the Thue–Morse sequence while seeking *balanced alternation* between two parties 'Ann' and 'Ben'. However, Brams and Taylor do not attribute the resulting sequence to Thue and Morse (and neither to Prouhet).

We are interested in counting the number of times that a word occurs as a *factor* — a contiguous finite subsequence — of another word; a related concept is the *binomial coefficient of two words*, which counts the corresponding number concerning general subsequences. We wish to note the related paper by Rigo and Salimov [132], defining *m-binomial equivalence* of two words, and the later paper by Lejeune, Leroy, and Rigo [94], where the Thue–Morse sequence is investigated with regard to this new concept.

It is well known that the sequence $\mathbf{t}$ is *uniformly recurrent* [96, Section 1.5.2]. That is, for each factor w of $\mathbf{t}$ there is a length n with the following property: every contiguous subsequence of $\mathbf{t}$ of length n contains w as a factor. The factor 01 therefore appears in $\mathbf{t}$ with bounded distances. We are interested in the infinite word $\mathbf{B}$ (over a finite alphabet) describing these differences. We mark the occurrences of 01 in the first 64 letters of $\mathbf{t}$:

$$\overset{\downarrow\ \downarrow\ \downarrow\quad \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\quad \downarrow\ \downarrow\ \downarrow\quad \downarrow\ \downarrow\quad \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\ \downarrow\quad \downarrow\ \downarrow\ \downarrow}{0110100110010110100101100110100110010110011010010110100110010110}, \tag{4.1.3}$$

from which we see that

$$\mathbf{B} = 334233243342433233423\cdots.$$

The blocks 000 and 111 do not appear as factors in $\mathbf{t}$, since $\mathbf{t}$ is a concatenation of the blocks 01 and 10. Therefore the gaps between consecutive occurrences of 01 in $\mathbf{t}$ are in fact bounded by 4, and clearly they are bounded below by 2 (since different occurrences of 01 cannot overlap). It follows that we only need three letters, 2, 3, and 4, in order to capture the gap sequence.

The set of *return words* [52, 85] of a factor w of $\mathbf{t}$ is the set of words x of the form $x = w\tilde{x}$, where w is not a factor of $\tilde{x}$, and $w\tilde{x}w$ is a factor of $\mathbf{t}$. The gap sequence is the sequence of lengths of words in the decomposition $\mathbf{t} = x_0x_1\cdots$ of the Thue–Morse sequence into return words of 01, which are 011, 010, 0110, and 01 in order of appearance.

An appearance of the factor 01 marks the beginning of a block of 1s in $\mathbf{t}$. Moreover, no other block of 1s can appear before the next appearance of 01: between two blocks of 1s we can find a block of one or more 0s, and the last 0 in this block is followed by 1. The assumption that we see a block of 1s before the next appearance of 01 therefore leads to a contradiction. This argument is clearly visible in (4.1.3). The sequence $\mathbf{B}$ therefore gives the distances of consecutive blocks of 1s. We will see in Lemma 4.2.3 that the sequence $\mathbf{B}$ is *morphic*, or *substitutive*. That is, it can be described as the coding of a fixed point of a substitution over a finite alphabet. Jeffrey Shallit (private communication, July 2019) proposed to prove the non-automaticity of $\mathbf{B}$ to the author.

In the present paper, we investigate the sequence **B** and the closely related, very well-known automatic sequence **A** defined in Section 4.2.1. In particular, we prove the following theorem.

Theorem 4.1.1. *Let w be a factor of the Thue–Morse word of length at least 2, and C the sequence of gaps between consecutive occurrences of w in $\mathbf{t}$. Then C is morphic, but not automatic.*

Note that the set of positions where a given factor w appears in $\mathbf{t}$ *is* 2-automatic — that is, its characteristic sequence is automatic. This follows from the following theorem by Brown, Rampersad, Shallit, and Vasiga [27, Theorem 2.1].

Theorem A. *Let $\mathbf{a} = a_0a_1a_2\cdots$ be a k-automatic sequence over the alphabet Δ, and let $w \in \Delta^*$. Then the set of of positions p such that w occurs beginning at position p is k-automatic.*

Concerning factors of length 1, the corresponding gap sequence is automatic too; this follows from [20].

The second part of our paper is concerned with the *discrepancy* of occurrences of `01`-blocks in $\mathbf{t}$. More precisely, assume that N is a nonnegative integer. We count the number of times the factor `01` occurs in the first N terms of the Thue–Morse sequence, and compare it to $N/3$:

$$D_N \coloneqq \#\big\{0 \le n < N : \mathbf{t}_n = \mathtt{0}, \mathbf{t}_{n+1} = \mathtt{1}\big\} - \frac{N}{3}. \tag{4.1.4}$$

From Theorem A we can immediately derive that the sequence $(D_N)_{N\ge0}$ is 2-*regular* [3, 7] as the sequence of partial sums of a 2-automatic sequence: the sequence having

$$\begin{cases} 2/3 & \text{if } \mathbf{t}_n\mathbf{t}_{n+1} = \mathtt{01}; \\ -1/3 & \text{otherwise} \end{cases}$$

as its nth term is automatic as the sum of four 2-automatic sequences, and D_N is the sum of the first N terms of this sequence [3, Theorem 3.1]. Our second theorem shows, more specifically, that D_N can be obtained as the output sum of a base-2 transducer (see Heuberger, Kropf, and Prodinger [83], in particular Remark 3.10 in that paper).

Theorem 4.1.2. *The sequence $(D_N)_{N\ge0}$ is the sequence of output sums of a base-2 transducer. In particular, $D_N \le C\log N$ for some absolute implied constant C. Moreover,*

$$\{D_N : N \ge 0\} = \frac{1}{3}\mathbb{Z}. \tag{4.1.5}$$

Note that the unboundedness of D_N follows from Corollary 4.10 in the paper [16] by Berthé and Bernales on balancedness in words.

Plan of the paper. In Section 4.2 we prove that the gap sequence for a factor w of $\mathbf{t}$ is not automatic. The central step of this proof is the case $w = \mathtt{01}$, which will be handled in the first three sub-sections. Section 4.2.4 reduces the general case to this special case. In Section 4.3 we study the automatic sequence **A** on the three symbols $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, closely related to the gap sequences. In particular, we lift this sequence to the seven-letter alphabet $K = \{\mathtt{a}, \underline{\mathtt{b}}, \overline{\mathtt{b}}, \mathtt{b}_{\lrcorner}, \mathtt{b}_{\llcorner}, \underline{\mathtt{c}}, \overline{\mathtt{c}}\}$. From this new sequence we can in particular read off the discrepancy D_N easily, which leads to a proof of Theorem 4.1.2.

4.2 Proving the non-automaticity of gap sequences

The main part of the proof of Theorem 4.1.1 concerns non-automaticity of the gaps between occurrences of 01. As a second step in our proof, the general case will be reduced to this one.

4.2.1 An auxiliary automatic sequence

We start by defining a substitution φ on three letters:

$$\varphi: \quad \mathtt{a} \mapsto \mathtt{abc}, \quad \mathtt{b} \mapsto \mathtt{ac}, \quad \mathtt{c} \mapsto \mathtt{b}. \tag{4.2.1}$$

The morphism φ can be extended to $\{\mathtt{a},\mathtt{b},\mathtt{c}\}^{\mathbb{N}}$ by concatenation, and we denote this extension by φ again. The unique fixed point (of length > 0) of φ is

$$\mathbf{A} = \mathtt{abcacbabcbacabcacbacabcbabcacbabcbacabcbabcacbac}\cdots .$$

This fixed point is a *morphic*, or *substitutive*, sequence [5, Chapter 7]. As a fixed point of φ — without having to apply a coding of the fixed point — it is even *pure morphic*. The sequence $\mathbf{A}$ is in fact 2-automatic, which follows from Berstel [13, Corollaire 4]. It is a 'hidden automatic sequence' as treated very recently by Allouche, Dekking, and Queffélec [2]. In fact, every automatic sequence can also be written as a coding of a fixed point of a non-uniform morphism [8] and this sense is a 'hidden' automatic sequence. We will re-state a corresponding 2-uniform substitution found by Berstel further down. The sequence $\mathbf{A}$, called *ternary Thue–Morse sequence* (for example, in the OEIS [140, A036577]), *Istrail squarefree sequence* [2, 84], or vtm [20], is well-known. Citing Dekking [32], we note that it appears in fact twelve times on the OEIS [140], featuring all renamings of the letters corresponding to permutations of the sets $\{0,1,2\}$ and $\{1,2,3\}$. These twelve entries are A005679, A007413, and A036577–A036586. The sequence $\mathbf{A}$ encodes the gaps between consecutive 1s in $\mathbf{t}$ [20]. Thue [158] showed that $\mathbf{A}$ is squarefree, while Rao, Rigo, and Salimov [130] later proved the stronger statement that $\mathbf{A}$ even avoids 2-*binomial squares* [132], thus settling in particular the question whether 2-abelian squares are avoidable over a 3-letter alphabet. We will use the squarefreeness property in our proof of Theorem 4.1.1.

Lemma 4.2.1 (Thue)**.** *The sequence* $\mathbf{A}$ *is squarefree. That is, no factor of the form* CC*, where* C *is a finite word over* $\{\mathtt{a},\mathtt{b},\mathtt{c}\}$ *of length at least* 1*, appears in* $\mathbf{A}$*.*

We have the following important relation between $\mathbf{A}$ and our problem.

Lemma 4.2.2. *The Thue–Morse sequence* $\mathbf{t}$ *can be recovered from* $\mathbf{A}$ *via the substitution*

$$f: \mathtt{a} \mapsto \mathtt{011010}, \quad \mathtt{b} \mapsto \mathtt{0110}, \quad \mathtt{c} \mapsto \mathtt{01}, \tag{4.2.2}$$

by concatenation: we have

$$\mathbf{t} = f(\mathbf{A}_0)f(\mathbf{A}_1)\cdots . \tag{4.2.3}$$

We will prove this in a moment. From this observation, noting also that each of the three words $f(\mathtt{a})$, $f(\mathtt{b})$, and $f(\mathtt{c})$ begins with 01, we see that we can extract from $\mathbf{A}$ the sequence of gaps between occurrences of the factor 01 in $\mathbf{t}$: each a yields two consecutive gaps of size 3, each b yields a gap of size 4, and each c a gap of size 2.

Proof of Lemma 4.2.2. We prove that for $k \geq 1$,

$$\mathbf{t}_{[0,6\cdot 2^k]} = f(\mathbf{A}_0)f(\mathbf{A}_1)\cdots f\big(\mathbf{A}_{L_k}\big), \tag{4.2.4}$$

where $L_k = 3\cdot 2^{k-1}-1$, by induction. The case $k=1$ is just the trivial identity $\mathtt{011010011001} = f(\mathtt{a})f(\mathtt{b})f(\mathtt{c})$.

Note that $\tau(f(\mathtt{a})) = f(\mathtt{a})f(\mathtt{b})f(\mathtt{c})$, $\tau(f(\mathtt{b})) = f(\mathtt{a})f(\mathtt{c})$, and $\tau(f(\mathtt{c})) = f(\mathtt{b})$. Extending f by concatenation, for convenience of notation, to words over $\{\mathtt{a},\mathtt{b},\mathtt{c}\}$, we obtain $\tau(f(x)) = f(\varphi(x))$ for each $x \in \{\mathtt{a},\mathtt{b},\mathtt{c}\}$. An application of the morphism τ to both sides of (4.2.4) yields

$$\begin{aligned}\mathbf{t}_{[0,6\cdot 2^{k+1})} &= \tau\big(f(\mathbf{A}_0)\big)\cdots\tau\big(f\big(\mathbf{A}_{L_k}\big)\big) = f(\varphi(\mathbf{A}_0))\cdots f\big(\varphi\big(\mathbf{A}_{L_k}\big)\big)\\ &= f\big(\varphi\big(\mathbf{A}_0\cdots\mathbf{A}_{L_k}\big)\big) = f\big(\mathbf{A}_1\cdots\mathbf{A}_{L_{k+1}}\big) = f(\mathbf{A}_0)\cdots f\big(\mathbf{A}_{L_{k+1}}\big).\end{aligned}$$

Note that we see by induction that $\varphi^k(\mathtt{abc})$ contains each of the three letters 2^k times, hence the numbers L_k. This proves the lemma. ⛝

Since each of the words $f(\mathtt{a})$, $f(\mathtt{b})$, and $f(\mathtt{c})$ starts with $\mathtt{01}$, the differences $a_j = k_{j+1} - k_j$ between successive occurrences of $\mathtt{01}$ in $\mathbf{t}$ are easily obtained from $\mathbf{A}$ by the substitution

$$r : \mathtt{a} \mapsto 33, \quad \mathtt{b} \mapsto 4, \quad \mathtt{c} \mapsto 2. \tag{4.2.5}$$

Here each $\mathtt{a}$ yields two blocks $\mathtt{01}$, and each of $\mathtt{b}$ and $\mathtt{c}$ one block.

Let $\mathbf{B}$ be the sequence of gaps between consecutive occurrences of $\mathtt{01}$ in the Thue–Morse sequence, and $\check{\mathbf{B}}$ the corresponding sequence for $\mathtt{10}$.

Lemma 4.2.3. *The sequence $\mathbf{B}$ is a morphic sequence, given by the substitution ψ on the four letters $\mathtt{a},\bar{\mathtt{a}},\mathtt{b},\mathtt{c}$, together with the coding p,*

$$\begin{array}{lllll}\psi: & \mathtt{a}\mapsto \mathtt{a}\bar{\mathtt{a}}, & \bar{\mathtt{a}}\mapsto \mathtt{bc}, & \mathtt{b}\mapsto \mathtt{a}\bar{\mathtt{a}}\mathtt{c}, & \mathtt{c}\mapsto \mathtt{b},\\ p: & \mathtt{a}\mapsto 3, & \bar{\mathtt{a}}\mapsto 3, & \mathtt{b}\mapsto 4, & \mathtt{c}\mapsto 2.\end{array} \tag{4.2.6}$$

Let $\bar{\mathbf{B}}$ denote the fixed point of ψ starting with $\mathtt{a}$.

The sequence $\check{\mathbf{B}}$ is morphic. More precisely, it is the image of $\bar{\mathbf{B}}$ under the morphism

$$\check{p} : \mathtt{a}\mapsto 24, \quad \bar{\mathtt{a}}\mapsto 33, \quad \mathtt{b}\mapsto 233, \quad \mathtt{c}\mapsto 4. \tag{4.2.7}$$

Note that $\bar{\mathbf{B}}$ is the pointwise limit of the finite words $\psi^k(\mathtt{a})$, and begins as follows:

$$\bar{\mathbf{B}} = \mathtt{a}\bar{\mathtt{a}}\mathtt{bca}\bar{\mathtt{a}}\mathtt{cba}\bar{\mathtt{a}}\mathtt{bcba}\bar{\mathtt{a}}\mathtt{cba}\bar{\mathtt{a}}\mathtt{bca}\bar{\mathtt{a}}\mathtt{cba}\bar{\mathtt{a}}\mathtt{bcba}\bar{\mathtt{a}}\mathtt{cba}\bar{\mathtt{a}}\mathtt{bca}\bar{\mathtt{a}}\mathtt{cba}\bar{\mathtt{a}}\mathtt{bcba}\bar{\mathtt{a}}\mathtt{c}\cdots .$$

Proof. Let q be the morphism that replaces $\mathtt{a}$ by $\mathtt{a}\bar{\mathtt{a}}$ and leaves $\mathtt{b}$ and $\mathtt{c}$ unchanged. We show by induction on the length of a word C over $\mathtt{abc}$ that

$$q\big(\varphi(C)\big) = \psi(q(C)). \tag{4.2.8}$$

This is clear for words of length 1, since $q(\varphi(\mathtt{a})) = \mathtt{a}\bar{\mathtt{a}}\mathtt{bc} = \psi(q(\mathtt{a}))$, $q(\varphi(\mathtt{b})) = \mathtt{a}\bar{\mathtt{a}}\mathtt{c} = \psi(q(\mathtt{b}))$, and $q(\varphi(\mathtt{c})) = \mathtt{b} = \psi(q(\mathtt{c}))$. Appending a letter $x \in \{\mathtt{a},\mathtt{b},\mathtt{c}\}$ to a word C for which the identity (4.2.8) already holds, we obtain

$$\begin{aligned}q\big(\varphi(Cx)\big) &= q\big(\varphi(C)\varphi(x)\big) = q\big(\varphi(C)\big)q(\varphi(x))\\ &= \psi(q(C))\psi(q(x)) = \psi(q(C)q(x)) = \psi(q(Cx))\end{aligned}$$

and therefore (4.2.8) for C replaced by Cx. Next, we prove by induction, using (4.2.8), that

$$q(\varphi^k(\mathtt{a})) = \psi^k(q(\mathtt{a})).$$

Clearly, this holds for $k = 1$. For $k \geq 2$, we obtain

$$q\big(\varphi^k(\mathtt{a})\big) = q\big(\varphi(\varphi^{k-1}(\mathtt{a}))\big) = \psi\big(q\big(\varphi^{k-1}(\mathtt{a})\big)\big) = \psi\big(\psi^{k-1}(q(\mathtt{a}))\big) = \psi^k(q(\mathtt{a})).$$

Noting that $q(\mathtt{a}) = \psi(\mathtt{a})$ and $p \circ q = r$, the proof of the first part of Lemma 4.2.3 is complete.

We proceed to the second part, concerning $\check{\mathbf{B}}$. Note that by Corollary 7.7.5 in [5] we only have to prove that $\check{\mathbf{B}} = \check{p}(\bar{\mathbf{B}})$.

Let

$$\check{f} : \mathtt{a} \mapsto \mathtt{011010}, \quad \bar{\mathtt{a}} \mapsto \mathtt{011001}, \quad \mathtt{b} \mapsto \mathtt{01101001}, \quad \mathtt{c} \mapsto \mathtt{0110}, \tag{4.2.9}$$

and extend this function to words (finite or infinite) over $\{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$ by concatenation.

Applying τ, we see by direct computation that

$$\tau\big(\check{f}(\mathtt{a})\big) = \mathtt{011010011001} = \check{f}(\mathtt{a})\check{f}(\bar{\mathtt{a}}) = \check{f}\big(\psi(\mathtt{a})\big),$$

and analogously, we get $\tau\big(\check{f}(x)\big) = \check{f}\big(\psi(x)\big)$ for each letter $x \in \{\bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$. Applying this letter by letter, we obtain

$$\tau\big(\check{f}(w)\big) = \check{f}\big(\psi(w)\big) \tag{4.2.10}$$

for every finite word over $\{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$. By induction, we obtain

$$\tau^k\big(\check{f}(\mathtt{a})\big) = \check{f}\big(\psi^k(\mathtt{a})\big),$$

using the step

$$\tau^{k+1}\big(\check{f}(\mathtt{a})\big) = \tau\big(\tau^k\big(\check{f}(\mathtt{a})\big)\big) = \tau\big(\check{f}\big(\psi^k(\mathtt{a})\big)\big) = \check{f}\big(\psi^{k+1}(\mathtt{a})\big).$$

Noting that $\check{f}(\mathtt{a})$ begins with $\mathtt{0}$, we obtain $\mathbf{t} = \check{f}(\bar{\mathbf{B}})$. In other words, the sequence $\bar{\mathbf{B}}$ yields the decomposition $\mathbf{t} = x_0 x_1 \cdots$ of the Thue–Morse sequence into return words of $\mathtt{0110}$, where $x_j = \check{f}\big(\bar{\mathbf{B}}_j\big)$. From this decomposition we can easily read off the sequence of gaps between occurrences of $\mathtt{10}$, since this word appears in each of the four return words, and the first occurrence always takes place at the same position, which is 2. In this way, we obtain the gaps 2 and 3 from the return word $\check{f}(\mathtt{a})$ each time $\mathtt{a}$ appears in $\bar{\mathbf{B}}$. Analogously, $\bar{\mathtt{a}}$ yields the gaps 3 and 3, the letter $\mathtt{b}$ the gaps 2, 3, and 3, and finally $\mathtt{c}$ yields the gap 4. This proves the second part of Lemma 4.2.3. ⛝

Remark 8. A hint how to come up with the definition of ψ can be found by combining the substitutions φ and r, given in (4.2.1) and (4.2.5) respectively, and considering the first few words $w_k = r(\varphi^k(\mathtt{a}))$: we have $w_1 = \mathtt{3342}$, $w_2 = \mathtt{33423324}$, $w_3 = \mathtt{3342332433424332}$. We see that a first guess for a definition of ψ, choosing $\mathtt{3} \mapsto \mathtt{3342}$, leads to the incorrect result $\mathtt{33423342}\cdots$ after the next iteration; we are led to distinguishing between 'the first letter "3"' and 'the second letter "3"' in each occurrence of $\mathtt{33}$, which is exactly what our definition of ψ does. On the other hand, we directly obtain (4.2.6) by inspecting the decomposition of $\mathbf{t}$ into return words of $\mathtt{01}$. (Equivalently, we can study return words of $\mathtt{0110}$, as we did in the second part of the proof of Lemma 4.2.3.) We can write the image under τ of each return word as a concatenation of return words, which yields the desired morphism.

4.2.2 Factors of B appearing at positions in a residue class

The main step in our proof of Theorem 4.1.1 is given by the following proposition. For completeness, we let ψ^0 denote the identity, such that $\psi^0(w) = w$ for all words w over $\{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$.

Proposition 4.2.4. *Let $\mu \geq 0$ be an integer. The sequence of indices where $\psi^{4\mu}(\mathtt{a})$ appears as a factor in $\bar{\mathbf{B}}$ has nonempty intersection with every residue class $a + m\mathbb{Z}$, where $m \geq 1$ and a are integers.*

In the remainder of this section, we prove this proposition. We work with the fourth iteration $\sigma = \psi^4$ of the substitution ψ: we have

$$\begin{aligned} \sigma(\mathtt{a}) &= \mathtt{a\bar{a}bcaacbaa\bar{a}bcbaa\bar{a}c}, & \sigma(\bar{\mathtt{a}}) &= \mathtt{a\bar{a}bcaa\bar{a}cbaa\bar{a}caa\bar{a}bcb}, \\ \sigma(\mathtt{b}) &= \mathtt{a\bar{a}bcaa\bar{a}cbaa\bar{a}bcbaa\bar{a}caa\bar{a}bcb}, & \sigma(\mathtt{c}) &= \mathtt{a\bar{a}bcaa\bar{a}cbaa\bar{a}c}. \end{aligned} \tag{4.2.11}$$

We have the following explicit formulas for the lengths of $\sigma^k(x)$, where $x \in \{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$:

$$\begin{aligned} a_k &\coloneqq \left|\sigma^k(\mathtt{a})\right| = \left|\sigma^k(\bar{\mathtt{a}})\right| = 16^k, \\ b_k &\coloneqq \left|\sigma^k(\mathtt{b})\right| = \frac{4 \cdot 16^k - 1}{3}, \\ c_k &\coloneqq \left|\sigma^k(\mathtt{c})\right| = \frac{2 \cdot 16^k + 1}{3}. \end{aligned} \tag{4.2.12}$$

The proof of this identity is based on the formula

$$\begin{pmatrix} 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \\ 5 & 5 & 6 & 5 \\ 3 & 3 & 2 & 3 \end{pmatrix}^k = \begin{pmatrix} 16^k/4 & 16^k/4 & 16^k/4 & 16^k/4 \\ 16^k/4 & 16^k/4 & 16^k/4 & 16^k/4 \\ (16^k-1)/3 & (16^k-1)/3 & (16^k+2)/3 & (16^k-1)/3 \\ (16^k+2)/6 & (16^k+2)/6 & (16^k-4)/6 & (16^k+2)/6 \end{pmatrix},$$

valid for $k \geq 1$, which takes care of the numbers of the letters $\mathtt{a}$, $\bar{\mathtt{a}}$, $\mathtt{b}$, and $\mathtt{c}$ in $\sigma^k(\mathtt{a})$, $\sigma^k(\bar{\mathtt{a}})$, $\sigma^k(\mathtt{b})$, and $\sigma^k(\mathtt{c})$. This formula can be proved easily by induction. Moreover, (4.2.12) also holds for $k = 0$.

By applying σ^k on the first line of (4.2.11), we see that each letter in $\{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$ is replaced by a word having the respective lengths a_k, a_k, b_k, c_k. For each $\nu \geq 0$, it follows that the factor $\sigma^\nu(\mathtt{a})$, of length $a_\nu = 16^\nu$, can be found at the following positions in $\sigma^{\nu+1}(\mathtt{a})$:

$$\begin{aligned} A^{(\nu,0)} &\coloneqq 0, & A^{(\nu,1)} &\coloneqq 4 \cdot 16^\nu, \\ A^{(\nu,2)} &\coloneqq 8 \cdot 16^\nu, & A^{(\nu,3)} &\coloneqq 12 \cdot 16^\nu + \frac{4 \cdot 16^\nu - 1}{3}. \end{aligned} \tag{4.2.13}$$

We may repeat this for $\nu - 1, \nu - 2, \ldots, \mu$, where $\mu \leq \nu$ is a given natural number, from which we obtain the following statement. For all integers $0 \leq \mu \leq \nu$ and all $\boldsymbol{\varepsilon} = (\varepsilon_\mu, \varepsilon_{\mu+1}, \ldots, \varepsilon_\nu) \in \{0,1,2,3\}^{\nu-\mu+1}$, the factor $\sigma^\mu(\mathtt{a})$ of length 16^μ can be found at the position

$$N_{\boldsymbol{\varepsilon}} \coloneqq A^{(\mu,\varepsilon_\mu)} + A^{(\mu+1,\varepsilon_{\mu+1})} + \cdots + A^{(\nu,\varepsilon_\nu)} \tag{4.2.14}$$

in $\bar{\mathbf{B}}$. There are other positions where the factor $\sigma^\mu(\mathtt{a})$ appears, but for our proof it is sufficient to consider these special positions. We will show that we can find one among these indices $N_{\boldsymbol{\varepsilon}}$ in a given residue class $a + m\mathbb{Z}$.

Let us sketch the remainder of the proof. The case that m is even causes mild difficulties. We therefore write $m = 2^k d$, where d is odd, and proceed in two steps. As a first step, we will

find integers μ, ν, and $\varepsilon_\mu, \varepsilon_{\mu+1}, \dots, \varepsilon_{\lambda-1} \in \{0,1,2,3\}$, such that $N_{\varepsilon_\mu,\varepsilon_{\mu+1},\dots,\varepsilon_{\lambda-1}}$ lies in any given residue class modulo 2^k. The second step will consist in refining the description by appending a sequence $(\varepsilon_\lambda, \dots, \varepsilon_{\nu-1}) \in \{0,1,2\}^{\nu-\lambda}$. Since we exclude the digit $\varepsilon_i = 3$, and we will take care that $16^\mu \geq 2^k$, we have

$$N_{\varepsilon_\mu,\dots,\varepsilon_{\nu-1}} \equiv N_{\varepsilon_\mu,\dots,\varepsilon_{\lambda-1}} \bmod 2^k.$$

We will choose the integers ε_j for $\lambda \leq j < \mu$ in such a way that any given residue class modulo d (note that d is odd), is hit. Due to the excluded digit 3, this is a *missing digit* problem, and a short argument including exponential sums will finish this step. Combining these two steps, we will see that every residue class modulo $2^k d$ is reached. We will now go into the details.

The first step: hitting a residue class modulo 2^k

We are interested in appearances of the initial segment $\sigma^\mu(\mathtt{a})$ in $\bar{\mathbf{B}}$ at positions lying in the residue class $a + 2^k\mathbb{Z}$. Let us assume in the following that

$$16^\mu \geq 2^k. \tag{4.2.15}$$

This lower bound on μ will not cause any problem.

We will choose $\lambda > \mu$ in a moment, and we set $\varepsilon_\mu = \cdots = \varepsilon_{\lambda-1} = 3$. Let us consider the integers $\alpha_0 \coloneqq 0$, and for $1 \leq \ell \leq \lambda - \mu$,

$$\alpha_\ell \coloneqq N_{\varepsilon_\mu,\dots,\varepsilon_{\mu+\ell-1}}.$$

Assume that $0 \leq \ell < \lambda - \mu$. By (4.2.14), (4.2.15), we have

$$\begin{aligned}\alpha_{\ell+1} - \alpha_\ell &= 12 \cdot 16^{\mu+\ell} + \frac{4 \cdot 16^{\mu+\ell} - 1}{3} \equiv \frac{4 \cdot 16^{\mu+\ell} - 1}{3} \bmod 2^\ell \\ &\equiv \sum_{0 \leq j \leq 2\mu+2\ell} 4^j \bmod 2^\ell \equiv \sum_{0 \leq j < 2\mu} 4^j \bmod 2^\ell.\end{aligned}$$

The latter sum is an odd integer, and independent of ℓ. It follows that $(\alpha_\ell)_{0 \leq \ell \leq \lambda-\mu}$ is an arithmetic progression modulo 2^k, where the common difference is odd; choosing $\lambda \geq \mu + 2^k$, we see that $(\alpha_\ell)_{0 \leq \ell < \lambda-\mu}$ hits every residue class modulo 2^k. We summarise the first step in the following lemma.

Lemma 4.2.5. *Let $k \geq 0$ and $\mu \geq k/4$, and choose $\varepsilon_{\mu+\ell} = 3$ for $\ell \geq 0$. The integers $N_{\varepsilon_\mu,\dots,\varepsilon_{\lambda-1}}$ hit every residue class modulo 2^k, as λ runs through the integers $\geq \mu$.*

A discrete Cantor set — missing digits

We follow the paper [59] by Erdős, Mauduit, and Sárközy, who studied integers with missing digits in residue classes. Let $\mathcal{W}_\lambda$ be the set of nonnegative multiples of 16^λ having only the digits $0, 4$, and 8 in their base-16 expansion. Set

$$U(\alpha) = \frac{1}{3} \sum_{0 \leq k \leq 2} \mathrm{e}(4k\alpha) \quad \text{and} \quad G(\alpha, \lambda, \nu) = \frac{1}{3^{\nu-\lambda}} \sum_{\substack{0 \leq j < 16^\nu \\ j \in \mathcal{W}}} \mathrm{e}(j\alpha),$$

where $\mathrm{e}(x) = \exp(2\pi i x)$. Note that elements $j \in \mathcal{W}_\lambda$ have the form $j = \sum_{\lambda \leq k < \eta} 4\,\varepsilon_k 16^k$, where $\eta \geq 0$ and $\varepsilon_k \in \{0,1,2\}$ for $\lambda \leq k < \eta$. In particular, $\mathcal{W}_\lambda \cap [0, 16^\eta)$ has $3^{\eta-\lambda}$ elements for $\eta \geq \lambda$.

We obtain

$$\begin{aligned} G(\alpha,\lambda,\nu) &= \frac{1}{3^{\nu-\lambda}} \sum_{(\varepsilon_\lambda,\dots,\varepsilon_{\nu-1})\in\{1,2,3\}^{\nu-\lambda}} \mathrm{e}\big(4\,\varepsilon_\lambda 16^\lambda\alpha + \cdots + 4\,\varepsilon_{\nu-1}16^{\nu-1}\alpha\big) \\ &= \prod_{\lambda\le r<\nu} \frac{1}{3}\big(\mathrm{e}\big(0\cdot 16^r\alpha\big) + \mathrm{e}\big(4\cdot 16^r\alpha\big) + \mathrm{e}\big(8\cdot 16^r\alpha\big)\big) \\ &= \prod_{\lambda\le r<\nu} U\left(16^r\alpha\right). \end{aligned} \tag{4.2.16}$$

The purpose of this section is to prove the following lemma.

Lemma 4.2.6. *Let $\lambda \ge 0$ be an integer, and a, d integers such that $d \ge 1$ is odd. Then $\mathcal{W}_\lambda \cap \big(a + d\,\mathbb{Z}\big)$ contains infinitely many elements.*

In order to prove this, we first show that it is sufficient to prove the following auxiliary result (compare [59, (4.3)]).

Lemma 4.2.7. *Assume that $d \ge 1$ is an odd integer, and $\ell \in \{1,\dots,d-1\}$. Let $\lambda \ge 0$ be an integer. Then*

$$\lim_{\nu\to\infty} G\left(\frac{\ell}{d},\lambda,\nu\right) = 0.$$

In fact, by the orthogonality relation

$$\frac{1}{d}\sum_{0\le n<d} \mathrm{e}(nk/d) = \begin{cases} 1, & \text{if } d \mid k; \\ 0, & \text{otherwise,} \end{cases}$$

we have

$$\begin{aligned} &\frac{1}{3^{\nu-\lambda}}\#\big\{0\le j<16^\nu : j\in\mathcal{W}, j\equiv a \bmod d\big\} - \frac{1}{d} \\ &\quad= \frac{1}{d}\frac{1}{3^{\nu-\lambda}} \sum_{0\le\ell<d}\sum_{\substack{0\le j<16^\nu \\ j\in\mathcal{W}}} \mathrm{e}\big(\ell(j-a)/d\big) - \frac{1}{d} \\ &\quad= \frac{1}{d}\sum_{1\le\ell<d} \mathrm{e}\big(-\ell a/d\big)\frac{1}{3^{\nu-\lambda}} \sum_{\substack{0\le j<16^\nu \\ j\in\mathcal{W}}} \mathrm{e}\big(j\ell/d\big) \le \sum_{1\le\ell<d}\left|G\left(\frac{\ell}{d},\lambda,\nu\right)\right|. \end{aligned} \tag{4.2.17}$$

If $G\big(\ell/d,\lambda,\nu\big)$ converges to zero as $\nu\to\infty$, for all $\ell\in\{1,\dots,d-1\}$, the last sum in (4.2.17) is eventually smaller than $1/d$. This implies that the cardinalities $\#\big\{0\le j<16^\nu : j\in\mathcal{W}_\lambda, j\equiv a \bmod d\big\}$ diverge to ∞, and therefore $\mathcal{W}_\lambda\cap(a+d\mathbb{Z})$ is infinite.

Proof of Lemma 4.2.7. By (4.2.17), we have to show that the product

$$\prod_{\lambda\le r<\nu} U(16^r\ell/d) = \prod_{\lambda\le r<\nu}\big(1+\mathrm{e}\big(4\cdot 16^r\ell/d\big)+\mathrm{e}\big(8\cdot 16^r\ell/d\big)\big) \tag{4.2.18}$$

converges to zero as $\nu\to\infty$. To this end, we use the following lemma [33] by Delange.

Lemma 4.2.8 (Delange)**.** *Assume that $q\ge 2$ is an integer and $z_1,\dots,z_{q-1}$ are complex numbers such that $|z_j|\le 1$ for $1\le j<q$. Then*

$$\left|\frac{1}{q}\big(1+z_1+\cdots+z_{q-1}\big)\right| \le 1 - \frac{1}{2q}\max_{1\le j<q}\big(1-\operatorname{Re} z_j\big).$$

Since d is odd and $1 \le \ell < d$, the integer $4k16^r\ell$ is not a multiple of d for $k \in \{1,2\}$. It follows that $\operatorname{Re}\mathrm{e}\big(4k16^r\ell/d\big) \le 1-\tilde{\varepsilon}$ for some $\tilde{\varepsilon} > 0$ only depending on d.

Therefore each factor in (4.2.16) is smaller than $1-\varepsilon$, where $\varepsilon > 0$ does not depend on r. Consequently, by Lemma 4.2.8 the product (4.2.18) converges to zero. Lemma 4.2.7, and therefore Lemma 4.2.6, is proved. ⛒

Now we combine the two steps, corresponding to the cases (i) 2^k and (ii) d odd.
Let $k \ge 0$ and $d \ge 1$ be integers, and d odd. We are interested in a residue class $a + 2^k d\,\mathbb{Z}$, where $a \in \mathbb{Z}$. Choose

$$a^{(1)} \coloneqq a \bmod 2^k \in \{0, \dots, 2^k - 1\}.$$

Choose μ large enough such that $16^\mu \ge 2^k$. By Lemma 4.2.5 there exists $\lambda \ge \mu$ in such a way that

$$\kappa^{(1)} \equiv a^{(1)} \bmod 2^k,$$

where $\kappa^{(1)} \coloneqq N_{\varepsilon_\mu,\dots,\varepsilon_{\lambda-1}}$ and $\varepsilon_\ell = 3$ for $\mu \le \ell < \lambda$. Next, choose

$$a^{(2)} \coloneqq \big(a - \kappa^{(1)}\big) \bmod d.$$

By Lemma 4.2.6, the set $\mathcal{W}_\lambda \cap \big(a^{(2)} + d\,\mathbb{Z}\big)$ is not empty. Let $\sum_{\lambda \le \ell < \nu} 4\,\varepsilon_\ell 16^\ell$ be an element, where $\varepsilon_\ell \in \{0,1,2\}$ for $\lambda \le \ell < \nu$. By (4.2.14) we have

$$\kappa \coloneqq N_{\varepsilon_\mu,\dots,\varepsilon_{\lambda-1},\varepsilon_\lambda,\dots,\varepsilon_{\nu-1}} = \kappa^{(1)} + \kappa^{(2)},$$

where

$$\kappa^{(2)} \coloneqq N_{\varepsilon_\lambda,\dots,\varepsilon_{\nu-1}}.$$

The integer $\kappa^{(1)}$ lies in the residue class $a^{(1)} + 2^k\mathbb{Z}$ by construction, while $\kappa^{(2)}$ is divisible by 2^k, as no digit among $\varepsilon_\lambda, \dots, \varepsilon_{\nu-1}$ equals 3. It follows that $\kappa \in a^{(1)} + 2^k\mathbb{Z} = a + 2^k\mathbb{Z}$. Moreover, by (4.2.13),

$$\kappa^{(2)} = \sum_{\lambda \le \ell < \nu} 4\,\varepsilon_\ell 16^\ell \in a^{(2)} + d\,\mathbb{Z},$$

hence $\kappa = \kappa^{(1)} + \kappa^{(2)} \equiv \kappa^{(1)} + \big(a - \kappa^{(1)}\big) \equiv a \bmod d$.

Summarising, we have $\kappa \in \big(a + 2^k\mathbb{Z}\big) \cap \big(a + d\,\mathbb{Z}\big)$. Since 2^k and d are coprime, which implies $2^k\mathbb{Z} \cap d\,\mathbb{Z} = 2^k d\,\mathbb{Z}$, we have $\big(a + 2^k\mathbb{Z}\big) \cap \big(a + d\,\mathbb{Z}\big) = a + 2^k d\,\mathbb{Z}$ (applying a shift by a) and therefore $\kappa \in a + 2^k d\,\mathbb{Z}$. This finishes the proof of Proposition 4.2.4. ⛒

4.2.3 Non-automaticity of B

In order to prove that $\mathbf{B}$ is not automatic, we use the characterization by the k-kernel: a sequence $(a_n)_{n\ge0}$ is k-automatic if and only if the set

$$\big\{\big(a_{\ell+k^j n}\big)_{n\ge0} : j \ge 0, 0 \le \ell < k^j\big\} \tag{4.2.19}$$

is finite.

We are now in the position to prove that *any* two arithmetic subsequences of $\mathbf{B}$ with the same modulus m and different shifts ℓ_1, ℓ_2 are different: the sequences $\big(\mathbf{B}(\ell_1 + nm)\big)_{n\ge0}$ and $\big(\mathbf{B}(\ell_2 + nm)\big)_{n\ge0}$ cannot be equal. This will prove in particular that the k-kernel is infinite and thus non-automaticity of the gap sequence for `01`.

Let us assume, in order to obtain a contradiction, that the sequence $\mathbf{B}$ contains two identical arithmetic subsequences with common differences equal to m, indexed by $n \mapsto \ell_1 + nm$ and $n \mapsto \ell_2 + nm$ respectively, where $\ell_1 < \ell_2$. Let $r = \ell_2 - \ell_1$, and choose μ large enough such that $16^\mu \geq 2r$. By Proposition 4.2.4, the block $\sigma^\mu(\mathtt{a})$ appears in $\bar{\mathbf{B}}$ at positions that hit each residue class. In particular, for each $s \in \{0, \ldots, r-1\}$ we choose the residue class $\ell_1 - s + m\mathbb{Z}$, and we can find an index n such that $\sigma^\mu(\mathtt{a})$ appears at position $\ell_1 - s + nm$ in $\bar{\mathbf{B}}$. Since $16^m \geq 2r > s$, this means that $\ell_1 + mn$ hits the sth letter in $\sigma^\mu(\mathtt{a})$, in symbols,

$$\bar{\mathbf{B}}_{\ell_1+nm} = \sigma^\mu(\mathtt{a})\big|_s.$$

Since $s + r$ is still in the range $[0, 16^\mu)$, we also have

$$\bar{\mathbf{B}}_{\ell_2+nm} = \sigma^\mu(\mathtt{a})\big|_{s+r}$$

for the same index n. Applying the coding p defined in (4.2.6), and our equality assumption, we see that

$$\mathbf{B}_s = p\big(\sigma^\mu(\mathtt{a})\big|_s\big) = \mathbf{B}_{\ell_1+nm} = \mathbf{B}_{\ell_2+nm} = p\big(\sigma^\mu(\mathtt{a})\big|_{s+r}\big) = \mathbf{B}_{s+r}.$$

Carrying this out for all $s \in \{0, \ldots, r-1\}$, we see that the first $2r$ terms of $\mathbf{B}$ form a square. Now there are two cases to consider.

The case $r = 1$. Assume that $\mathbf{B}_{\ell_1+nm} = \mathbf{B}_{\ell_1+1+nm}$ for all $n \geq 0$. By Proposition 4.2.4, the positions where the prefix $\mathtt{3342} = \mathbf{B}_0\mathbf{B}_1\mathbf{B}_2\mathbf{B}_3$ appears as a factor in $\mathbf{B}$ hit every residue class. In particular, there is an index n such that the block $\mathtt{3342}$ can be found at position $\ell_1 - 1 + nm$ in $\mathbf{B}$. This implies $\mathtt{3} = \mathbf{B}_1 = \mathbf{B}_{\ell_1+nm} = \mathbf{B}_{\ell_1+1+nm} = \mathbf{B}_2 = \mathtt{4}$, a contradiction.

The case $r \geq 2$. In this case we will resort to the fact, proved below, that $\mathbf{B}$ does not contain squares of length > 2. Therefore we get a contradiction also in this case. In order to complete the proof that $\mathbf{B}$ is not automatic, it remains to prove (the second part of) the following result.

Lemma 4.2.9. *The infinite word $\bar{\mathbf{B}}$ is squarefree. The word $\mathbf{B}$ does not contain squares of length > 2.*

Proof. We begin with the first statement. Note first that, by the morphism (4.2.5), letters '$\mathtt{3}$' in $\mathbf{B}$ appear in pairs; moreover, the squarefreeness of $\mathbf{A}$ implies that there are no runs of three or more $\mathtt{3}$s. This implies that the morphism r defined in (4.2.5) can be 'reversed' in the sense that $\mathbf{A}$ can be restored from $\mathbf{B}$ by the (unambiguous) rule $\tilde{r} : \mathtt{33} \mapsto \mathtt{a}$, $\mathtt{4} \mapsto \mathtt{b}$, $\mathtt{2} \mapsto \mathtt{c}$. Also, $\bar{\mathbf{B}}$ can be restored from $\mathbf{B}$ by the (unambiguous) rule $\mathtt{33} \mapsto \mathtt{a}\bar{\mathtt{a}}$, $\mathtt{4} \mapsto \mathtt{b}$, $\mathtt{2} \mapsto \mathtt{c}$, thus reversing the effect on $\bar{\mathbf{B}}$ of the morphism p defined in (4.2.6). In particular, since $\mathbf{A}$ is squarefree, each occurrence of the factor $\mathtt{a}\bar{\mathtt{a}}$ in $\bar{\mathbf{B}}$ is bordered by symbols $\in \{\mathtt{b}, \mathtt{c}\}$ (where of course the first occurrence at 0 is not bordered on the left by another symbol).

Assume, in order to obtain a contradiction, that the square CC is a factor of $\bar{\mathbf{B}}$. We distinguish between two cases.

The case $|C| = 1$. Let C consist of a single symbol $x \in \{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$. The squarefreeness of $\mathbf{A}$ forbids $x \in \{\mathtt{b}, \mathtt{c}\}$; moreover, we saw a moment ago that $\mathtt{a}$ and $\bar{\mathtt{a}}$ may only appear together, bordered by symbols $\in \{\mathtt{b}, \mathtt{c}\}$. This excludes the possibility $x \in \{\mathtt{a}, \bar{\mathtt{a}}\}$, therefore this case leads to a contradiction.

The case $|C| \geq 2$. There are two cases to consider. (i) Assume that C begins with $\bar{\mathtt{a}}$. In this case, C has to end with $\mathtt{a}$: the concatenation CC has to be a factor of $\bar{\mathbf{B}}$, and therefore the symbol $\bar{\mathtt{a}}$ at the start of the second 'C' has to be preceded by a symbol $\mathtt{a}$. Analogously, each occurrence of the word CC is immediately preceded by $\mathtt{a}$, and followed by $\bar{\mathtt{a}}$. That is, $\mathtt{a}CC\bar{\mathtt{a}}$ appears as a factor of $\bar{\mathbf{B}}$. Writing $C = \bar{\mathtt{a}}y\mathtt{a}$ for a finite (possibly empty) word y over $\{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$,

we see that $\mathtt{a}\bar{\mathtt{a}}y\mathtt{a}\bar{\mathtt{a}}y\mathtt{a}\bar{\mathtt{a}}$ is a factor of $\bar{\mathbf{B}}$. Applying the coding p, it follows that $T = \mathtt{aa}y\mathtt{aa}y\mathtt{aa}$ appears in $\mathbf{B}$, and it is a concatenation of the words 33, 4, and 2. Consequently, it makes sense to apply the 'inverse morphism' $\tilde{r} : 33 \mapsto \mathtt{a}$, $4 \mapsto \mathtt{b}$, $2 \mapsto \mathtt{c}$. Therefore $\tilde{r}(T) = \mathtt{a}z\mathtt{a}z\mathtt{a}$, for some finite word z over $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$, appears in $\mathbf{A}$. This contradicts Lemma 4.2.1. (ii) Assume that C starts with a letter $\in \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. In this case, C ends with a letter $\in \{\bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$: otherwise, the concatenation CC, and therefore $\bar{\mathbf{B}}$, would contain $\mathtt{aa}$, which we have already ruled out. We apply p, and in this case $p(C)$ is a concatenation of the words 33, 4, and 2. Therefore we can form $\tilde{r}(p(C))$, revealing that the square $\tilde{r}(p(C))\tilde{r}(p(C))$ is a factor of $\mathbf{A}$. This is a contradiction.

We have to prove the second statement. Assume that CC is a factor of $\mathbf{B}$, where $|C| \geq 2$. This proof is analogous to the corresponding case for $\bar{\mathbf{B}}$, and we skip some of the details that we have already seen there. (i) Assume that C begins with exactly one $\mathtt{a}$. In this case, C has to end with exactly one $\mathtt{a}$, and therefore $C = \mathtt{a}y\mathtt{a}$ for a finite word y over $\{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$. It follows that $\mathtt{aa}y\mathtt{aa}y\mathtt{aa}$ is a factor of $\mathbf{B}$. Applying $\tilde{r}$, we obtain a contradiction to Lemma 4.2.1.

(ii) Assume that C starts with $\mathtt{aa}$, $\mathtt{b}$, or $\mathtt{c}$. In this case, C ends with $\mathtt{aa}$, $\mathtt{b}$, or $\mathtt{c}$, otherwise CC, and therefore $\bar{\mathbf{B}}$, would contain a block of $\mathtt{a}$s of length $\neq 2$. We apply p on the word CC, followed by $\tilde{r}$, which yields the square $\tilde{r}(p(C))\tilde{r}(p(C))$. Again, this contradicts Lemma 4.2.1. ⛝

Summarising, arithmetic subsequences of $\mathbf{B}$ with common difference m are distinct as soon as their offsets differ. In particular, for each integer $k \geq 2$ the k-kernel of $\mathbf{B}$ is infinite. Therefore $\mathbf{B}$ is not automatic, which proves the case $w = \mathtt{01}$ of Theorem 4.1.1.

4.2.4 Occurrences of general factors in t

We begin with the case $w = \mathtt{10}$. We will work with the Thue–Morse morphism $\tau : \mathtt{0} \mapsto \mathtt{01}$, $\mathtt{1} \mapsto \mathtt{10}$, defined in (4.1.1). First of all, we recall the well-known fact that $a_{k+1} = \tau^{k+1}(\mathtt{0})$ can be constructed from $a_k = \tau^k(\mathtt{0})$ by concatenating a_k and its Boolean complement $\overline{a_k}$ (which replaces each $\mathtt{0}$ by $\mathtt{1}$ and each $\mathtt{1}$ by $\mathtt{0}$). The proof of this little fact is by an easy induction. For $k = 0$ we have $a_1 = \mathtt{01} = \mathtt{0}\overline{\mathtt{0}}$. The case $k \geq 1$ makes use of the identity $\tau(\overline{w}) = \overline{\tau(w)}$, valid for each word w over $\{\mathtt{0}, \mathtt{1}\}$, which follows from the special structure of the morphism τ. Applying this identity and the induction hypothesis, we obtain

$$\begin{aligned} a_{k+1} &= \tau\big(\tau^k(\mathtt{0})\big) = \tau\big(a_{k-1}\overline{a_{k-1}}\big) \\ &= \tau\big(a_{k-1}\big)\tau\big(\overline{a_{k-1}}\big) = \tau\big(a_{k-1}\big)\overline{\tau\big(a_{k-1}\big)} = a_k\overline{a_k}. \end{aligned}$$

Using this, we show that for even $k \geq 0$, the word $\tau^k(\mathtt{0})$ is a palindrome. The case $k = 0$ is trivial. If $a_k = \tau^k(\mathtt{0})$ is a palindrome, then $a_{k+2} = \tau(\tau(a_k)) = \tau(a_k\overline{a_k}) = a_k\overline{a_k}\overline{a_k}a_k$ is clearly a palindrome too, and the statement follows by induction. In particular, we see from the above that

$$\tau^k(\mathtt{0}) = \tau^{k-1}(\mathtt{0})\tau^{k-1}(\mathtt{1}), \quad \tau^k(\mathtt{1}) = \tau^{k-1}(\mathtt{1})\tau^{k-1}(\mathtt{0}) \quad \text{for all } k \geq 0. \tag{4.2.20}$$

Note that, by applying τ^k on $\mathbf{t}$, every $\mathtt{0}$ gets replaced by $\tau^k(\mathtt{0})$ and every $\mathtt{1}$ by $\tau^k(\mathtt{1})$, and the result is again $\mathbf{t}$ since it is a fixed point of τ. It follows that

$$\begin{aligned} &\text{for all } k \geq 0, \quad \text{we have } \mathbf{t} = A_{\mathbf{t}_0}A_{\mathbf{t}_1}A_{\mathbf{t}_2}\cdots, \\ &\qquad\qquad\quad \text{where } A_x = \tau^k(x) \text{ for } x \in \{\mathtt{0}, \mathtt{1}\}. \end{aligned} \tag{4.2.21}$$

Let $(r_j)_{j\geq 0}$ be the increasing sequence of indices where $\mathtt{10}$ occurs in $\mathbf{t}$. For k even, let $J = J(k)$ be the number of occurrences of $\mathtt{10}$ with indices $\leq 2^k - 2$. Note that $r_{J-1} = 2^k - 2$. We read

the (palindromic) sequence a_k, of length 2^k, backwards; it follows that $(2^k-1-r_{J-1-j})_{0\le j<J}$ is the increasing sequence of indices pointing to the letter $\mathtt{1}$ in an occurrence of $\mathtt{01}$ in a_k. Therefore

$$\big(2^k-2-r_{J-1-j}\big)_{0\le j<J}$$

is the increasing sequence of indices where $\mathtt{01}$ occurs in a_k. Consequently, by the definition of $\mathbf{B}$ as the differences of these indices, we obtain $\mathbf{B}_j=-r_{J-1-(j+1)}+r_{J-1-j}$ for $0\le j<J-1$ and thus

$$r_{j+1}-r_j=\mathbf{B}_{J-2-j}\quad\text{for } 0\le j\le J-2. \tag{4.2.22}$$

We have to prove that the sequence

$$\check{\mathbf{B}}=(r_{j+1}-r_j)_{j\ge0} \tag{4.2.23}$$

is not automatic. More generally, we prove that any two arithmetic subsequences

$$L^{(1)}=\big(\check{\mathbf{B}}(\ell_1+nd)\big)_{n\ge0},\quad L^{(2)}=\big(\check{\mathbf{B}}(\ell_2+nd)\big)_{n\ge0},$$

where $d\ge1$ and $\ell_1\ne\ell_2$, are different. In order to obtain a contradiction, let us assume that $L^{(1)}=L^{(2)}$, and let $k\ge0$ be even. By (4.2.22), we get arithmetic subsequences M_1, M_2 of $\mathbf{B}$ with common difference d, different offsets $m_1(k),m_2(k)\in\{0,\dots,d-1\}$, and length equal to $J(k)-1$, such that

$$\mathbf{B}_{m_1(k)+nd}=M_j^{(1)}=M_j^{(2)}=\mathbf{B}_{m_2(k)+nd}\quad\text{for } 0\le n\le J(k)-2.$$

Note the important fact that the offsets $m_j(k)$ are bounded by d. Since there are only $d(d-1)/2$ pairs $(a,b)\in\{0,\dots,d-1\}^2$ with $a\ne b$, it follows that there are two different offsets $0\le\overline{m_1},\overline{m_2}<d$ with the following property: there are arbitrarily long arithmetic subsequences of $\mathbf{B}$ with indices of the form $\overline{m_1}+nd$ and $\overline{m_2}+nd$ respectively, taking the same values. This is just the statement that the *infinite* sequences $\big(\mathbf{B}_{\overline{m_1}+nd}\big)_{n\ge0}$ and $\big(\mathbf{B}_{\overline{m_2}+nd}\big)_{n\ge0}$ are equal. In the course of proving that $\mathbf{B}$ is not automatic (which is the case $w=\mathtt{01}$ of Theorem 4.1.1) we proved that this is impossible, and we obtain a contradiction. The sequence $\check{\mathbf{B}}$ is therefore not automatic either, which finishes the case $w=\mathtt{10}$.

We proceed to the case $w=\mathtt{00}$. Let $(a_i)_{i\ge0}$ be the increasing sequence of indices j such that $\mathbf{t}_j\mathbf{t}_{j+1}=\mathtt{00}$. Assume that $i\ge0$, and set $j\coloneqq a_i$. We have $j\equiv1 \bmod 2$, since $\mathbf{t}_{2j'}=\overline{\mathbf{t}_{2j'+1}}$ for all $j'\ge0$ (where the overline denotes the Boolean complement, $\mathtt{0}\mapsto\mathtt{1}$, $\mathtt{1}\mapsto\mathtt{0}$). Equality $\mathbf{t}_j=\mathbf{t}_{j+1}$ (as needed) can therefore only occur at odd indices j, and we choose $j'\ge0$ such that $j=2j'+1$. Necessarily, $\mathbf{t}_{j'}=\mathtt{1}$ and $\mathbf{t}_{j'+1}=\mathtt{0}$, since the identities $\mathbf{t}_{2j'+1}=\overline{\mathbf{t}_{j'}}$ and $\mathbf{t}_{2j'+2}=\mathbf{t}_{j'+1}$ would produce an output $\mathbf{t}_{2j'+1}\mathbf{t}_{2j'+2}\ne\mathtt{00}$ in the other case. On the other hand, $\mathbf{t}_{j'}\mathbf{t}_{j'+1}=\mathtt{10}$ indeed implies $\mathbf{t}_{2j'+1}\mathbf{t}_{2j'+2}=\mathtt{00}$. Each occurrence of $\mathtt{00}$ in $\mathbf{t}$, at position j, therefore corresponds in a bijective manner to an occurrence of $\mathtt{10}$, at position $(j-1)/2$ (which is an integer). It follows that the corresponding gap sequence equals $2\check{\mathbf{B}}$, which is not automatic by the already proved case $w=\mathtt{10}$.

In a completely analogous manner, we can reduce the case $w=\mathtt{11}$ to the case $\mathtt{01}$, and the gap sequence equals $2\mathbf{B}$, which is not automatic either.

We will now reduce the case of general factors w of $\mathbf{t}$ of length ≥3 to these four cases.

Lemma 4.2.10. *For $x,y\in\{\mathtt{0},\mathtt{1}\}$, let $(a_k^{xy})_{k\ge0}$ be the increasing sequence of indices j such that $\mathbf{t}_j\mathbf{t}_{j+1}=xy$. We have*

$$\begin{aligned}&a_0^{\mathtt{01}}<a_0^{\mathtt{10}}<a_1^{\mathtt{01}}<a_1^{\mathtt{10}}<a_2^{\mathtt{01}}<a_2^{\mathtt{10}}<\cdots\quad\textit{and}\\&a_0^{\mathtt{11}}<a_0^{\mathtt{00}}<a_1^{\mathtt{11}}<a_1^{\mathtt{00}}<a_2^{\mathtt{11}}<a_2^{\mathtt{00}}<\cdots.\end{aligned} \tag{4.2.24}$$

Proof. First of all, $\mathbf{t}$ begins with $\mathtt{011}$, whence the first items of the two displayed chains of inequalities. The first chain is almost trivial since after each block of consecutive $\mathtt{0}$s, a letter $\mathtt{1}$ follows, and vice versa.

Let us prove the second series of inequalities by induction. Assume that $a_0^{(\mathtt{11})} < a_0^{(\mathtt{00})} < \cdots < a_{i-1}^{(\mathtt{00})} < a_i^{(\mathtt{11})} = j$. Then $\mathbf{t}_j\mathbf{t}_{j+1} = \mathtt{11}$, and it follows that $\mathbf{t}_{j+2} = \mathtt{0}$, since $\mathtt{111}$ is not a factor of $\mathbf{t}$. Two cases can occur. (i) If $\mathbf{t}_{j+3} = \mathtt{0}$, then clearly $a_i^{(\mathtt{11})} < a_i^{(\mathtt{00})} = j+2$ by our hypothesis. (ii) Otherwise, we have $\mathbf{t}_j\mathbf{t}_{j+1}\mathbf{t}_{j+2}\mathbf{t}_{j+3} = \mathtt{1101}$. Necessarily, j is odd: if $j = 2j'$, it would follow that $\mathbf{t}_j\mathbf{t}_{j+1} \in \{\mathtt{01}, \mathtt{10}\}$, but we need $\mathtt{11}$. Moreover, $j \equiv 3 \bmod 4$ is also not possible: Let $j+1 = 4j'$. Then $\mathbf{t}_{j+1}\mathbf{t}_{j+2}\mathbf{t}_{j+3} \in \{\mathtt{011}, \mathtt{100}\}$, but we need $\mathtt{101}$. It follows that $j \equiv 1 \bmod 4$, and therefore $\mathbf{t}_{j+4}\mathbf{t}_{j+5} = \mathtt{00}$, which implies $a_i^{(\mathtt{00})} = j+4$. By a completely analogous argument (reversing the roles of $\mathtt{1}$ and $\mathtt{0}$), we may finish the proof of Lemma 4.2.10 by induction. ⛒

Let w be a factor of $\mathbf{t}$, of length ≥ 3. Choose $k \geq 0$ minimal such that w is a factor of some $a_k^{xy} = \tau^k(x)\tau^k(y)$, where $x, y \in \{\mathtt{0}, \mathtt{1}\}$. By minimality, w is not a factor of $\tau^k(\mathtt{0})$ or $\tau^k(\mathtt{1})$, using (4.2.20). Consequently, w appears at most once in each a_k^{xy}. Next, we need the fact that $\mathbf{t}$ is *overlap-free* [14,27,158], meaning that is does not contain a factor of the form $axaxa$, where $a \in \{\mathtt{0}, \mathtt{1}\}$ and $x \in \{\mathtt{0}, \mathtt{1}\}^*$. We derive from this property that w cannot occur simultaneously in both members of either of the pairs

$$(a_k^{\mathtt{00}}, a_k^{\mathtt{01}}), \quad (a_k^{\mathtt{00}}, a_k^{\mathtt{10}}), \quad (a_k^{\mathtt{11}}, a_k^{\mathtt{01}}), \quad (a_k^{\mathtt{11}}, a_k^{\mathtt{10}}). \tag{4.2.25}$$

For example, assume that w is a factor of both $a_k^{\mathtt{00}}$ and $a_k^{\mathtt{01}}$. By minimality, as we had before,

$$\tau^k(\mathtt{0})\tau^k(\mathtt{0}) = AwB, \quad \tau^k(\mathtt{0})\tau^k(\mathtt{1}) = A'wB',$$

where A and A' are initial segments of $\tau^k(\mathtt{0})$, and B resp. B' are final segments of $\tau^k(\mathtt{0})$ resp. $\tau^k(\mathtt{1})$, and all of these segments are proper subwords of the respective words. We have $A \neq A'$, since otherwise $\tau^k(\mathtt{0}) = \tilde{w}B = \tilde{w}B' = \tau^k(\mathtt{1})$ for some $\tilde{w}$ that is not the empty word. This contradicts the fact that $\tau^k(\mathtt{0}) = \overline{\tau^k(\mathtt{1})}$. Let us, without loss of generality, assume that $|A| < |A'|$. The first 2^k letters of Aw and $A'w$ are equal, in symbols,

$$(Aw)\big|_{[0,2^k)} = (A'w)\big|_{[0,2^k)}. \tag{4.2.26}$$

We can therefore choose $a \in \{\mathtt{0}, \mathtt{1}\}$ and $w_1, w_2 \in \{\mathtt{0}, \mathtt{1}\}^*$ in such a way that $aw_1w_2 = w$ and $Aaw_1 = A'$. Then trivially $Aw = Aaw_1w_2 = A'w_2$, and since $|A| < 2^k$, $|A'| < 2^k$, it follows from (4.2.26) that $w_2 = aw_3$ for some $w_3 \in \{\mathtt{0}, \mathtt{1}\}^*$. Finally, the factor $A'w$ of $\mathbf{t}$ can be written as $A'w = Aaw_1w = Aaw_1aw_1w_2 = Aaw_1aw_1aw_3$, which contradicts the overlap-freeness of $\mathbf{t}$. The other three cases, corresponding to the second through fourth pairs in (4.2.25), are analogous. We have therefore shown that the set of $A \in \{a_k^{\mathtt{00}}, a_k^{\mathtt{01}}, a_k^{\mathtt{10}}, a_k^{\mathtt{11}}\}$ such that w is a factor of A is a subset of either $\{a_k^{\mathtt{01}}, a_k^{\mathtt{10}}\}$ or $\{a_k^{\mathtt{00}}, a_k^{\mathtt{11}}\}$.

First case. Let w be a factor of $a_k^{\mathtt{01}}$, or of $a_k^{\mathtt{10}}$. Assume first that w is a factor of $a_k^{\mathtt{01}}$, but not of $a_k^{\mathtt{10}}$. In this case, we show that the gap sequence for w is given by the gap sequence for $a_k^{\mathtt{01}}$: (i) each occurrence of $a_k^{\mathtt{01}}$ yields exactly one occurrence of w (involving a constant shift); (ii) by (4.2.21), every occurrence of w takes place within a block of the form a_k^{xy}; (iii) only the block $a_k^{\mathtt{01}}$ is eligible. We prove that $a_k^{\mathtt{01}}$ appears exactly at positions 2^kj in $\mathbf{t}$, where $\mathbf{t}_j\mathbf{t}_{j+1} = \mathtt{01}$. The easy direction follows from (4.2.21): each occurrence of $\mathtt{01}$ yields an occurrence of $a_k^{\mathtt{01}}$, where the index has to be multiplied by 2^k. On the other hand, it is sufficient to show that $a_k^{\mathtt{01}}$ can only appear on positions 2^kj. Given this, there is no admissible choice for $(\mathbf{t}_j, \mathbf{t}_{j+1})$

different from $(\mathtt{0},\mathtt{1})$, by (4.2.21). Suppose that we already know this for some $k \geq 0$ (the case $k = 0$ being trivial). Assume that

$$a_{k+1}^{\mathtt{01}} = \tau^k(\mathtt{0})\tau^k(\mathtt{1})\tau^k(\mathtt{1})\tau^k(\mathtt{0}) \text{ appears on some position } \ell. \tag{4.2.27}$$

Since $\tau^k(\mathtt{0})\tau^k(\mathtt{1}) = a_k^{\mathtt{01}}$, we know by hypothesis that $\ell \equiv 0 \bmod 2^k$. Assume that the case $\ell \equiv 2^k \bmod 2^{k+1}$ occurs. We set $\ell = (2j+1)2^k$ for some $j \geq 0$. Our assumption (4.2.27) implies $\tau^k(\mathtt{1}) = \tau^k(\mathbf{t}_{2j+2}) = \tau^k(\mathbf{t}_{j+1})$ and therefore $\mathbf{t}_{j+1} = \mathtt{1}$, which implies that $\tau^{k+1}(\mathbf{t}_{j+1}) = \tau^k(\mathtt{1})\tau^k(\mathtt{0})$ appears on position $\ell + 2^k = (2j+2)2^k$ in $\mathbf{t}$. This is incompatible with (4.2.27). In particular, the gap sequence for w, which is identical to the gap sequence for $a_k^{\mathtt{01}}$, is given by $2^k\mathbf{B}$, and therefore not automatic. Switching the roles of $\mathtt{0}$ and $\mathtt{1}$ in this proof, we also obtain non-automaticity for the case that w is a factor of $a_k^{\mathtt{10}}$, but not of $a_k^{\mathtt{01}}$ — with the sequence $2^k\check{\mathbf{B}}$ as the corresponding gap sequence.

Let w be a factor of both $a_k^{\mathtt{01}}$ and $a_k^{\mathtt{10}}$. In this case, each occurrence of w in $\mathbf{t}$ takes place within a subblock of $\mathbf{t}$ of one of these two forms. By Lemma 4.2.10, combined with the above argument that occurrences of $a_k^{\mathtt{01}}$ resp. $a_k^{\mathtt{10}}$ in $\mathbf{t}$ take place at indices obtained from occurrences of $\mathtt{01}$ resp. $\mathtt{10}$, multiplied by 2^k, these blocks occur alternatingly. Assuming, in order to obtain a contradiction, that the gap sequence $(g_j)_{j\geq 0}$ for w is automatic, we obtain a new automatic sequence $(g_{2j} + g_{2j+1})_{j\geq 0}$ as the sum of two automatic sequences (note that the characterisation involving the 2-kernel (4.2.19) immediately implies that $(g_{2j+\varepsilon})_{j\geq 0}$, for $\varepsilon \in \{0,1\}$, is automatic). By the alternating property, this is the gap sequence for $a_k^{\mathtt{01}}$, which is not automatic, as we have just seen. A contradiction!

Second case. Let w be a factor of $a_k^{\mathtt{00}}$ or of $a_k^{\mathtt{11}}$. This case is largely analogous. We assume that w be a factor of $a_k^{\mathtt{00}}$, but not of $a_k^{\mathtt{11}}$. As in the case $a_k^{\mathtt{01}}$, the gap sequence for w in this case is identical to the gap sequence for $a_k^{\mathtt{00}}$, and we only have to show that this sequence is not automatic. We know already that the gap sequence for $\mathtt{00}$ is not automatic. Therefore it suffices to prove that $\tau^k(\mathtt{0})\tau^k(\mathtt{0})$ can only appear at positions in $\mathbf{t}$ divisible by 2^k. Suppose that we already know this for some $k \geq 0$ (the case $k = 0$ being again trivial). Assume that

$$a_{k+1}^{\mathtt{00}} = \tau^k(\mathtt{0})\tau^k(\mathtt{1})\tau^k(\mathtt{0})\tau^k(\mathtt{1}) \text{ appears on some position } \ell. \tag{4.2.28}$$

Since $\tau^k(\mathtt{0})\tau^k(\mathtt{1}) = a_k^{\mathtt{01}}$, we know by hypothesis that $\ell \equiv 0 \bmod 2^k$. Assume that the case $\ell \equiv 2^k \bmod 2^{k+1}$ occurs. We set $\ell = (2j+1)2^k$ for some $j \geq 0$. Our assumption (4.2.28) implies $\tau^k(\mathtt{1}) = \tau^k(\mathbf{t}_{2j+4}) = \tau^k(\mathbf{t}_{j+2})$ and therefore $\mathbf{t}_{j+2} = \mathtt{1}$, which implies that $\tau^{k+1}(\mathbf{t}_{j+2}) = \tau^k(\mathtt{1})\tau^k(\mathtt{0})$ appears on position $\ell + 3\cdot 2^k = (2j+4)2^k$ in $\mathbf{t}$. On position ℓ, we therefore see the factor

$$\tau^k(\mathtt{0})\tau^k(\mathtt{1})\tau^k(\mathtt{0})\tau^k(\mathtt{1})\tau^k(\mathtt{0}),$$

which contradicts the overlap-freeness of $\mathbf{t}$.

Again, the case that w is a factor of $a_k^{\mathtt{11}}$, but not of $a_k^{\mathtt{00}}$, is analogous; the case that it is a factor of both words can be handled as in the case $\{a_k^{\mathtt{01}}, a_k^{\mathtt{10}}\}$, this time with the help of the second chain of inequalities in (4.2.24).

Summarising, we have shown the non-automaticity for all gap sequences for factors w of $\mathbf{t}$ of length ≥ 2.

In order to finish the proof of Theorem 4.1.1, we still have to prove that the gap sequence is morphic for the 'mixed cases'. That is, assume that w is a factor of two words of the form a_k^{xy}, where $x, y \in \{\mathtt{0},\mathtt{1}\}$, and where k is chosen minimal such that w is a factor of at least one of $a_k^{\mathtt{00}}, a_k^{\mathtt{01}}, a_k^{\mathtt{10}}, a_k^{\mathtt{11}}$. Let us begin with the case $\{a_k^{\mathtt{01}}, a_k^{\mathtt{10}}\}$. The positions where w appears in $\mathbf{t}$

are given by $2^k j + \sigma_0$, where $\mathtt{b}_j\mathtt{b}_{j+1} = \mathtt{01}$, and $2^k j + \sigma_1$, where $\mathtt{b}_j\mathtt{b}_{j+1} = \mathtt{10}$. Here σ_0, σ_1 are the positions where the word w appears in $a_k^{\mathtt{01}}$ and $a_k^{\mathtt{10}}$ respectively. As before, this follows since $\mathbf{t}_j\mathbf{t}_{j+1} = \mathtt{01}$ is equivalent to $(\mathbf{t}_\ell, \dots, \mathbf{t}_{\ell+2^{k+1}-1}) = a_k^{\mathtt{01}}$, and the corresponding statement for $\mathtt{10}$. We see that it is sufficient to write $\mathbf{t}$ as a concatenation of the words

$$w_{\mathtt{a}} \coloneqq \mathtt{011}, \quad w_{\bar{\mathtt{a}}} \coloneqq \mathtt{010}, \quad w_{\mathtt{b}} \coloneqq \mathtt{0110}, \quad \text{and} \quad w_{\mathtt{c}} = \mathtt{01}, \tag{4.2.29}$$

since each word w_x takes care of one $\mathtt{01}$-block, followed by one $\mathtt{10}$-block, and the gap sequence for w is obtained by replacing each w_x by a succession of two gaps. Applying the morphism τ, we obtain $\tau(w_{\mathtt{a}}) = w_{\mathtt{a}}w_{\bar{\mathtt{a}}}$, $\tau(w_{\bar{\mathtt{a}}}) = w_{\mathtt{b}}w_{\mathtt{c}}$, $\tau(w_{\mathtt{b}}) = w_{\mathtt{a}}w_{\bar{\mathtt{a}}}w_{\mathtt{c}}$, $\tau(w_{\mathtt{c}}) = w_{\mathtt{b}}$. This mimics the morphism ψ; proceeding as in the proof of Lemma 4.2.2 (alternatively, as in the proof of Lemma 4.2.3), we obtain

$$\mathbf{t} = w_{\bar{\mathbf{B}}_0}w_{\bar{\mathbf{B}}_1}w_{\bar{\mathbf{B}}_2}\cdots. \tag{4.2.30}$$

Since $\bar{\mathbf{B}}$ is morphic, the succession of gaps with which w occurs in $\mathbf{t}$ is morphic by [5, Corollary 7.7.5] (that is, 'morphic images of morphic sequences are morphic').

The case $\{a_k^{\mathtt{00}}, a_k^{\mathtt{11}}\}$ is similar. Defining

$$\tilde{w}_{\mathtt{a}} \coloneqq \mathtt{011010}, \quad \tilde{w}_{\bar{\mathtt{a}}} \coloneqq \mathtt{011001}, \quad \tilde{w}_{\mathtt{b}} \coloneqq \mathtt{01101001}, \quad \text{and} \quad \tilde{w}_{\mathtt{c}} \coloneqq \mathtt{0110},$$

it is straightforward to verify that $\tau(\tilde{w}_{\mathtt{a}}) = \tilde{w}_{\mathtt{a}}\tilde{w}_{\bar{\mathtt{a}}}$, $\tau(\tilde{w}_{\bar{\mathtt{a}}}) = \tilde{w}_{\mathtt{b}}\tilde{w}_{\mathtt{c}}$, $\tau(\tilde{w}_{\mathtt{b}}) = \tilde{w}_{\mathtt{a}}\tilde{w}_{\bar{\mathtt{a}}}\tilde{w}_{\mathtt{c}}$, and $\tau(\tilde{w}_{\mathtt{c}}) = \tilde{w}_{\mathtt{b}}$. Again, we can spot the morphism ψ, and we obtain

$$\mathbf{t} = \tilde{w}_{\bar{\mathbf{B}}_0}\tilde{w}_{\bar{\mathbf{B}}_1}\tilde{w}_{\bar{\mathbf{B}}_2}\cdots \tag{4.2.31}$$

in exactly the same way as before. Each of the words w_x in this representation yields a block $\mathtt{11}$ in $\mathbf{t}$, followed by a block $\mathtt{00}$. Therefore, also in this case, the gap sequence for w is a morphic image of a morphic sequence. This finishes the proof of Theorem 4.1.1. ⛝

Remark 9. Let us have a closer look at the gaps in the 'mixed case' $\{a_k^{\mathtt{01}}, a_k^{\mathtt{10}}\}$. Let σ_0 be the index at which w appears in $a_k^{\mathtt{01}}$, and σ_1 the index at which w appears in $a_k^{\mathtt{10}}$. By (4.2.30) and the choice (4.2.29), each letter $x \in \{\mathtt{a}, \bar{\mathtt{a}}, \mathtt{b}, \mathtt{c}\}$ in $\bar{\mathbf{B}}$ corresponds to two gaps, as follows.

Letter in $\bar{\mathbf{B}}$	Gap 1	Gap 2
$\mathtt{a}$	$\sigma_1 - \sigma_0 + 2^{k+1}$	$\sigma_0 - \sigma_1 + 2^k$
$\bar{\mathtt{a}}$	$\sigma_1 - \sigma_0 + 2^k$	$\sigma_0 - \sigma_1 + 2^{k+1}$
$\mathtt{b}$	$\sigma_1 - \sigma_0 + 2^{k+1}$	$\sigma_0 - \sigma_1 + 2^{k+1}$
$\mathtt{c}$	$\sigma_1 - \sigma_0 + 2^k$	$\sigma_0 - \sigma_1 + 2^k$

(4.2.32)

It follows that there are at most four gaps that can occur in this case. For example, consider the gap sequence for the factor $w = \mathtt{010}$. In this case, $k = 2$, and we have $a_2^{\mathtt{01}} = \mathtt{011}\underline{\mathtt{01}}\mathtt{001}$ and $a_2^{\mathtt{10}} = \mathtt{10}\underline{\mathtt{010}}\mathtt{110}$, where the occurrences of w are underlined. We have $\sigma_0 = 3$ and $\sigma_1 = 2$. This yields the gaps 3, 5, 7, and 9, occurring only in the combinations $(7, 5)$, $(3, 9)$, $(7, 9)$, and $(3, 5)$. Noting also the first occurrence $\mathbf{t}_3\mathbf{t}_4\mathbf{t}_5 = \mathtt{010}$, the first few occurrences of $\mathtt{010}$ in $\mathbf{t}$ are at positions 3, 10, 15, 18, and 27, compare (4.1.2). In particular, the gap sequence is not of the form $2^\ell\mathbf{B}$ or $2^\ell\check{\mathbf{B}}$ for some $\ell \geq 0$, each of which has only three different values.

Similar considerations hold for the case $\{a_k^{\mathtt{00}}, a_k^{\mathtt{11}}\}$. More precisely, let σ_0 be the index at which w appears in $a_k^{\mathtt{11}}$ and σ_1 the index at which w appears in $a_k^{\mathtt{00}}$. Each letter occurring in $\bar{\mathbf{B}}$

corresponds to two gaps for w, as follows.

Letter in $\bar{\mathbf{B}}$	Gap 1	Gap 2
$\mathtt{a}$	$\sigma_1 - \sigma_0 + 4 \cdot 2^k$	$\sigma_0 - \sigma_1 + 2 \cdot 2^k$
$\bar{\mathtt{a}}$	$\sigma_1 - \sigma_0 + 2 \cdot 2^k$	$\sigma_0 - \sigma_1 + 4 \cdot 2^k$
$\mathtt{b}$	$\sigma_1 - \sigma_0 + 4 \cdot 2^k$	$\sigma_0 - \sigma_1 + 4 \cdot 2^k$
$\mathtt{c}$	$\sigma_1 - \sigma_0 + 2 \cdot 2^k$	$\sigma_0 - \sigma_1 + 2 \cdot 2^k$.

(4.2.33)

An example for this case is given by the word $\mathtt{00110}$, which is a factor of $a_2^{\mathtt{00}} = \mathtt{01100110}$ and of $a_2^{\mathtt{11}} = \mathtt{10011001}$. We have $\sigma_0 = 1$ and $\sigma_1 = 3$, and therefore the gaps 6, 10, 14, and 18, which appear as pairs $(18, 6)$, $(10, 14)$, $(18, 14)$, and $(10, 6)$.

4.3 The structure of the sequence A

In this section, we investigate the infinite word **A**, in particular by extending it to a word over a 7-letter alphabet. This extension allows us to better understand the structure of **A**, and gives us a tool to handle the discrepancy D_N. In particular, we prove Theorem 4.1.2.

4.3.1 A is automatic

It has been known since Berstel [13] that **A** is 2-automatic. In this section, we re-prove this statement using slightly different notation. Note that we had similar proofs (of Lemmas 4.2.2 and 4.2.3) in the first part of this paper. First of all, we recapture Berstel's 2-uniform morphism. Introducing an auxiliary letter $\bar{\mathtt{b}}$, we have the morphism $\overline{\varphi}$ as well as the coding π:

$$\begin{array}{llllll} \overline{\varphi}: & \mathtt{a} \mapsto \mathtt{ab}, & \mathtt{b} \mapsto \mathtt{ca}, & \bar{\mathtt{b}} \mapsto \mathtt{ac}, & \mathtt{c} \mapsto \mathtt{c}\bar{\mathtt{b}}, \\ \pi: & \mathtt{a} \mapsto \mathtt{a}, & \mathtt{b} \mapsto \mathtt{b}, & \bar{\mathtt{b}} \mapsto \mathtt{b}, & \mathtt{c} \mapsto \mathtt{c}. \end{array} \tag{4.3.1}$$

We wish to prove that

$$\pi(\overline{\mathbf{A}}) = \mathbf{A}, \tag{4.3.2}$$

where $\overline{\mathbf{A}}$ is the fixed point of $\overline{\varphi}$ starting with $\mathtt{a}$. For this, we will show, by induction on $k \geq 0$, that the initial segment

$$s_k := \overline{\varphi}^k(\mathtt{abc})$$

of $\overline{\mathbf{A}}$, of length $3 \cdot 2^k$, is a concatenation of the three words $w_0 = \mathtt{abc}$, $w_1 = \mathtt{ac}$, and $w_2 = \bar{\mathtt{b}}$. We also call the words w_j 'base words' in this context, and the latter statement 'concatenation property'. Having proved this property, we use (recall the morphism φ defined in (4.2.1))

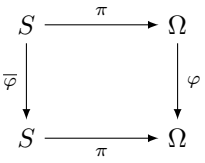
$$\begin{array}{lll} \pi\big(\overline{\varphi}(w_1)\big) & = \mathtt{abcacb} & = \varphi(\pi(w_1)); \\ \pi\big(\overline{\varphi}(w_2)\big) & = \mathtt{abcb} & = \varphi(\pi(w_1)); \\ \pi\big(\overline{\varphi}(w_3)\big) & = \mathtt{ac} & = \varphi(\pi(w_3)), \end{array} \tag{4.3.3}$$

in order to obtain

$$\varphi\big(\pi(s_k)\big) = \pi\big(\overline{\varphi}(s_k)\big) \tag{4.3.4}$$

for all $k \geq 0$, by concatenation. In other words, φ and $\overline{\varphi}$ act in the same way on an initial segment of $\overline{\mathbf{A}}$ of length $3 \cdot 2^k$.

We may also display the relation (4.3.4) graphically. Define $S = \{s_k : k \geq 0\} \subseteq \{\mathtt{a}, \mathtt{b}, \bar{\mathtt{b}}, \mathtt{c}\}^{\mathbb{N}}$ and $\Omega = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}^{\mathbb{N}}$. Then the following diagram is commutative.



Gluing together copies of this diagram, we obtain, for all $\ell \geq 1$,

$$\begin{aligned}\varphi^\ell\big(s_0\big) &= \varphi^\ell\big(\pi(s_0)\big) = \varphi^{\ell-1}\big(\pi(\overline{\varphi}(s_0))\big)\\ &= \varphi^{\ell-2}\big(\varphi(\pi(\overline{\varphi}(s_0)))\big) = \varphi^{\ell-2}\big(\pi(\overline{\varphi}^2(s_0))\big) = \cdots = \pi\big(\overline{\varphi}^\ell(s_0)\big).\end{aligned}$$

For each index $j \geq 0$, choose ℓ so large that $3 \cdot 2^\ell \geq j$. Then

$$\mathbf{A}_i = \varphi^\ell(s_0)\big|_i = \pi\big(\overline{\varphi}^\ell(s_0)\big)\big|_i = \pi\big(\overline{\varphi}^\ell(s_0)\big|_i\big) = \pi(\overline{\mathbf{A}}_i)$$

for $0 \leq i < j$. Therefore the infinite word $\mathbf{A}$ is 2-automatic, being the coding under π of the 2-automatic sequence $\overline{\mathbf{A}}$, and thus we have derived (4.3.2) from the concatenation property.

We still have to prove that s_k is a concatenation of the base words. Clearly, this holds for $s_0 = \mathtt{abc} = w_0$. Assume that we have already established that $s_k = w_{\varepsilon_0} w_{\varepsilon_1} \cdots$ for some $\varepsilon_j \in \{0, 1, 2\}$. We have

$$\begin{aligned}\overline{\varphi}(w_1) &= \mathtt{abcac\bar{b}} = w_0 w_1 w_2,\\ \overline{\varphi}(w_2) &= \mathtt{abc\bar{b}} = w_0 w_2,\\ \overline{\varphi}(w_3) &= \mathtt{ac} = w_1,\end{aligned}$$

and thus

$$s_{k+1} = \overline{\varphi}(s_k) = \overline{\varphi}(w_{\varepsilon_0})\overline{\varphi}(w_{\varepsilon_1}) \cdots$$

is a concatenation of the w_j too. This proves (4.3.2).

Complementing this result, we note that Berstel [13, Corollaire 7] also proved that $\mathbf{A}$ itself is not a fixed point of (the extension of) a uniform morphism.

4.3.2 Transforming A

We will identify *circular shifts*, or *rotations*, of factors of length $L \geq 2$ appearing in the sequence $\mathbf{A}$. Such a rotation of a word $(a_i)_{i\geq 0}$ replaces the subword $a_j\, a_{j+1} \cdots a_{j+L-2}\, a_{j+L-1}$ by $a_{j+1} \cdots a_{j+L-2}\, a_{j+L-1}\, a_j$ (rotation to the left), or $a_{j+L-1}\, a_j\, a_{j+1} \cdots a_{j+L-2}$ (rotation to the right), respectively.

Carrying out a certain number of such rotations, we will see that the sequence $\mathbf{A}$ is reduced to the periodic word $(\mathtt{abc})^\omega$. Of course, this is possible for any word containing an infinite number of each of `a`, `b`, and `c`, and it can be achieved in uncountably many ways. In our case however, an admissible sequence of rotations can be made very explicit, by defining a new morphism φ^+. This morphism has the fixed point $\overline{\mathbf{A}}$, which maps to $\mathbf{A}$ under a coding. From this augmented sequence, we will see very clearly the 'nested structure' of the above-mentioned rotations. In particular, we can find a certain *non-crossing matching*, defined in (4.3.13), describing the intervals that we perform rotations on, and the direction of each rotation. Moreover, in the process we learn something about the discrepancy of `01`-blocks in $\mathbf{t}$, which was defined in (4.1.4). Let us consider the iteration $\overline{\varphi}^2$ of Berstel's morphism:

$$\overline{\varphi}^2 : \quad \mathtt{a} \mapsto \mathtt{abca}, \quad \mathtt{b} \mapsto \mathtt{c\bar{b}ab}, \quad \mathtt{\bar{b}} \mapsto \mathtt{abc\bar{b}}, \quad \mathtt{c} \mapsto \mathtt{c\bar{b}ac}. \tag{4.3.5}$$

We introduce certain decorations— *connectors* — of the letters. Their meaning will become clear in a moment. Based on the morphism $\overline{\varphi}^2$, we define the following decorated version, which is a morphism on the 7-letter alphabet

$$K = \{\mathtt{a}, \bar{\mathtt{b}}, \bar{\mathtt{b}}, \mathtt{b}, \mathtt{b}, \mathtt{c}, \mathtt{c}\}. \tag{4.3.6}$$

$$\varphi^+ : \begin{array}{llll} \mathtt{a} \mapsto \mathtt{abca}, & \bar{\mathtt{b}} \mapsto \mathtt{abc}\bar{\mathtt{b}}, & \bar{\mathtt{b}} \mapsto \mathtt{ab}\bar{\mathtt{c}}\mathtt{b}, & \\ \mathtt{b} \mapsto \mathtt{c}\bar{\mathtt{b}}\mathtt{ab}, & \mathtt{b} \mapsto \mathtt{c}\bar{\mathtt{b}}\mathtt{ab}, & \mathtt{c} \mapsto \mathtt{c}\bar{\mathtt{b}}\mathtt{ac}, & \mathtt{c} \mapsto \mathtt{c}\bar{\mathtt{b}}\mathtt{ac}. \end{array} \tag{4.3.7}$$

This morphism has a unique fixed point $\mathbf{A}^+$ starting with $\mathtt{a}$. The image of $\mathbf{A}^+$ under the obvious coding γ given by

$$\gamma : \begin{array}{llll} \mathtt{a} \mapsto \mathtt{a}, & & & \\ \mathtt{b} \mapsto \mathtt{b}, & \mathtt{b} \mapsto \mathtt{b}, & \bar{\mathtt{b}} \mapsto \mathtt{b}, & \bar{\mathtt{b}} \mapsto \mathtt{b}, \\ \mathtt{c} \mapsto \mathtt{c}, & \mathtt{c} \mapsto \mathtt{c} & & \end{array} \tag{4.3.8}$$

yields the sequence **A**. Based on this, we will speak of *letters of types* $\mathtt{a}$, $\mathtt{b}$, and $\mathtt{c}$, thus referring to letters from $\{\mathtt{a}\}$, $\{\bar{\mathtt{b}}, \bar{\mathtt{b}}, \mathtt{b}, \mathtt{b}\}$, and $\{\mathtt{c}, \mathtt{c}\}$, respectively.

From the substitution (4.3.7), we can immediately derive the following lemma.

Lemma 4.3.1. *Let $j \geq 1$, and $(x, y, z) = (\mathbf{A}^+_{j-1}, \mathbf{A}^+_j, \mathbf{A}^+_{j+1})$. Then*

$$\begin{array}{llll} y = \bar{\mathtt{b}} & \Rightarrow & xyz = \mathtt{c}\bar{\mathtt{b}}\mathtt{a}; & \qquad y = \bar{\mathtt{b}} \quad \Rightarrow \quad xyz = \mathtt{c}\bar{\mathtt{b}}\mathtt{a}; \\ y = \mathtt{b} & \Rightarrow & xyz = \mathtt{abc}; & \qquad y = \mathtt{b} \quad \Rightarrow \quad xyz = \mathtt{abc}. \end{array} \tag{4.3.9}$$

We wish to connect the 'loose ends' of the connectors — we say that two connectors at indices $i < j$ *match* if the connector at i points to the right and the connector at j points to the left. The very simple algorithm `FindMatching` joins matching connectors, beginning with shortest connections. Only pairs of *free* connectors are connected, that is, each letter may be the starting point of only one link.

```
procedure FindMatching(w):
  M←{};
  SelectedIndices←{};
  n←1;
  while n < w.length:
    for all i such that there are matching connectors at i and i+n:
      if i ∉ SelectedIndices and i+n ∉ SelectedIndices:
        Add the pair (i,i+n) to the set M;
        Add i and i+n to the set SelectedIndices;
    n←n+1;
  return M;
end.
```

Algorithm `FindMatching`. Link free connectors

Note that we have to pay attention that previously selected indices are not chosen again, whence the introduction of `SelectedIndices`. A connection between the two letters at indices

i and j is just a different name for the pair (i, j). For any finite word w over the alphabet K this procedure yields a (possibly empty) set $M(w)$ of pairs (i, j) of indices.

We wish to prove that the algorithm is *monotone*.

Lemma 4.3.2. *Let w and w' be finite words over the alphabet K, and assume that w is an initial segment of w'. Let $M(w)$ resp. $M(w')$ be the sets of pairs found by the algorithm* `FindMatching`*. Then*

$$M(w) \subseteq M(w'). \tag{4.3.10}$$

Proof. We show this by induction on the length j of w. Clearly this holds for $j = 0$. Let us append a symbol $x \in K$ to w (at position j). Define $M_\ell(w)$ as the set of connections (a, b) for w of length strictly smaller than ℓ, found by the algorithm. Define $M_\ell(wx)$ analogously. We prove by induction on ℓ that $M_\ell(w) \subseteq M_\ell(wx)$, and that, if the inclusion is strict, we have $M_\ell(wx) = M_\ell(w) \cup \{(i, j)\}$ for some $i < j$. Suppose that this is true for some ℓ (clearly it holds for $\ell = 0$). We distinguish between two cases. (i) If $(i, j) \notin M_\ell(wx)$ for all i, we have $M_\ell(w) = M_\ell(wx)$ by hypothesis; we add each pair (a, b) with $b < j$ having matching connectors and such that $b - a = \ell$ to the sets $M_\ell(w)$ and $M_\ell(wx)$, and possibly one more pair (i, j), for some $i < j$, to $M_\ell(wx)$. (ii) If $(i, j) \in M_\ell(wx)$ for some i, we have $\ell > j - i$ by the definition of $M_\ell(wx)$; we add the pairs (a, b), with $b < j$, having matching connectors and such that $a \neq i$ and $b - a = \ell$ to both sets $M_\ell(w)$ and $M_\ell(wx)$. There are clearly no more pairs added to $M_\ell(wx)$, since i and j are already taken; moreover, the condition that $\ell > j - i$ renders impossible the chance of another connection (i, b), where $b < j$, to be added to $M_\ell(w)$. ⛝

We extend M to a function on all (finite or infinite) words w over K, in the following obvious way: for each ℓ, form the set $\tilde{M}_\ell(w)$ of all pairs (a, b) satisfying $b - a = \ell$, having matching connectors, such that neither a nor b is a component of any $\tilde{M}_{\ell'}(w)$, where $\ell' < \ell$. Set $\tilde{M}(w) = \bigcup_{\ell \geq 1} \tilde{M}_\ell(w)$. The following lemma gives us a method to compute a matching for an infinite word by only looking at finite segments.

Lemma 4.3.3. *Let w be an infinite word over K. Then*

$$\bigcup_{j \geq 0} M\big(w|_{[0,j)}\big) = \tilde{M}(w). \tag{4.3.11}$$

Proof. Let $M_\ell(w)$ be the set of connections added in step ℓ of the algorithm `FindMatching`. We prove, more generally, that

$$\bigcup_{j \geq 0} M_\ell\big(w|_{[0,j)}\big) = \tilde{M}_\ell(w). \tag{4.3.12}$$

We prove this by induction on ℓ, and we start at connections of length $\ell = 1$. Let $(i, i+1) \in M_\ell\big(w|_{[0,j)}\big)$. Then there is a pair of matching connectors at indices i and $i+1$ (where $i+1 < j$), and therefore this pair is also contained in $\tilde{M}_1(w)$. This proves the inclusion "$\subseteq$". On the other hand, if $(i, i+1)$ is a link connecting matching connectors in w, this link is also to be found in the sequence $w|_{[0,i+2)}$, hence the inclusion "$\supseteq$". Assume that (4.3.12) holds for some $\ell \geq 1$. If the algorithm finds a pair $(i, i+\ell)$ of matching connectors in $w|_{[0,j)}$, where $(i, i+\ell) \notin M_\ell\big(w|_{[0,j)}\big)$, this pair trivially also matches in the (unrestricted) word w. By hypothesis, the connectors at i and $i+\ell$ are not used by $\tilde{M}_\ell(w)$, hence the inclusion "$\subseteq$". On the other hand, a link $(i, i+\ell)$ of matching connectors in w that is still free in step ℓ is also free in $w|_{[0,i+\ell+1)}$ by hypothesis, which proves (4.3.12) and hence the lemma. ⛝

Our algorithm avoids crossing connections: if $i < j < k < \ell$ were indices such that $(i,k) \in M(w)$ and $(j,\ell) \in M(w)$, then the connector at index j is pointing to the right, and the one at k to the left, so the shorter connection (j,k) would have been chosen earlier. This contradicts the construction rule that indices may only be chosen once.

More generally, a *non-crossing matching* for a word w over K (finite or infinite) is a set M of pairs (i,j) such that

$$\begin{aligned}
&i < j && \text{for all } (i,j) \in M,\\
&w_i w_j \in \{\mathtt{b}\mathtt{c}, \bar{\mathtt{b}}\mathtt{c}, \mathtt{c}\mathtt{b}, \mathtt{c}\bar{\mathtt{b}}\} && \text{for all } (i,j) \in M,\\
&w_i = a && \text{for all } i \notin \bigcup M, \qquad (4.3.13)\\
&\left.\begin{array}{ll}(i,j) = (k,\ell) & \text{or}\\ i < k < \ell < j & \text{or}\\ k < i < j < \ell & \end{array}\right\} && \text{for all } (i,j) \in M,\ (k,\ell) \in M.
\end{aligned}$$

Here $\bigcup M = \{i : (i,j) \in M \text{ for some } j \text{ or } (j,i) \in M \text{ for some } j\}$.

We call a word w *closed* if there exists a non-crossing matching for w.

Lemma 4.3.4. *Let w be a word over K. There is at most one non-crossing matching for w. If there exists one,* `FindMatching` *generates it by virtue of* (4.3.11).

Proof. Let m be a non-crossing matching of w. Since all connectors have to connect to something and the connecting lines must not cross, we see that all pairs $(i,i+1)$ of indices where matching connectors appear have to be contained in m. It follows that $M_1\big(w\big|_{[0,j)}\big) \subseteq m$ for all j, and therefore $\tilde{M}_1(w) \subseteq m$ by (4.3.12). On the other hand, the definition of a non-crossing matching only allows matching connectors, therefore each connection $(i,i+1)$ in m is found by `FindMatching`, for $j = i+2$.

Similar reasoning applies for longer connections too. Let us assume that the set of connections of length $< \ell$ coming from `FindMatching` is the same as the set of connections of length $< \ell$ contained in m. Assume that i is an index such that the connectors at indices i and $i+\ell$ match, and neither i nor $i+\ell$ appears in a connection of length $< \ell$ in m. Since m is a matching, the connector at index i has to be linked to a connector at an index $j > i$. Indices $j \in \{i+1, \dots, i+\ell-1\}$ are excluded by our hypothesis, indices $j > i+\ell$ are impossible by the non-crossing property, therefore $(i,i+\ell) \in m$. Again, other connections of length ℓ cannot appear in m, therefore `FindMatching` finds all pairs $(i,i+\ell)$ contained in m. This completes our argument by induction. Therefore $m = \tilde{M}(w)$, and both statements of Lemma 4.3.4 follow. ⛝

Lemma 4.3.5. *The sequence $\mathbf{A}^+$ is closed.*

Proof. First of all we note that it is sufficient to prove that φ^+ maps closed words w to closed words. If this is established, we obtain, by induction, that the initial segments $(\varphi^+)^k(\mathtt{a})$ of $\mathbf{A}^+$ are closed. Since non-crossing matchings are unique, the corresponding sequence $(m_k)_{k\ge0}$ of non-crossing matchings satisfies $m_k \subseteq m_{k+1}$, and $\bigcup_{k\ge0} m_k$ is easily seen to be the desired matching for $\mathbf{A}^+$.

We prove by induction on the length n of a closed word w that $\varphi^+(w)$ is closed. This is obvious for the closed words of length $n \le 2$: the word $\varphi^+(\mathtt{a}) = \mathtt{a}\mathtt{b}\mathtt{c}\mathtt{a}$ is closed, and the cases $\mathtt{b}\mathtt{c}$, $\bar{\mathtt{b}}\mathtt{c}$, $\mathtt{c}\mathtt{b}$, and $\mathtt{c}\bar{\mathtt{b}}$ are also easy. Moreover, a concatenation of two closed words is also closed: one of the matchings has to be shifted (both components of each entry have to be shifted), and we only have to form the union of the matchings.

If w is of the form $\bar{\mathtt{b}}\,C\,\mathtt{c}$ for some nonempty word C over K, we obtain a non-crossing matching for C by stripping the pair $(1, n)$ from a corresponding matching for w. Therefore C is closed. Applying φ^+, we see that

$$\varphi^+(w) = \mathtt{a}\,\mathtt{b}\,\mathtt{c}\,\bar{\mathtt{b}}\,\varphi^+(C)\,\mathtt{c}\,\bar{\mathtt{b}}\,\mathtt{a}\,\mathtt{c}\,. \tag{4.3.14}$$

This is closed by our hypothesis, since C is shorter than w. The other case $\mathtt{c}\,C\,\bar{\mathtt{b}}$ is analogous (note that there are no more cases by (4.3.9)), and the proof is complete. ⛝

Remark 10. We note that this proof can also be used to show that the substitution φ^+ *respects* non-crossing matchings, in the following sense. If m is a non-crossing matching for w, then there exists a (unique) non-crossing matching m' for $\varphi^+(w)$; the matching m can be recovered from m' by omitting certain links, and applying a renaming $(i, j) \mapsto (\mu(i), \mu(j))$ to the remaining links, where $\mu : \mathbb{N} \to \mathbb{N}$ is nonincreasing. The proof is not difficult: if this procedure works for the closed word C, we can also carry this out for $\bar{\mathtt{b}}\,C\,\mathtt{c}$ by (4.3.14); we see that the additional link $\bar{\mathtt{b}} \cdots \mathtt{c}$ is still present in $\varphi^+\big(\bar{\mathtt{b}}\,C\,\mathtt{c}\big)$. Also, the procedure of recovering m' from m is compatible with concatenations of closed words C and D, as a matching for $\varphi^+(CD) = \varphi^+(C)\,\varphi^+(D)$ does not connect letters in $\varphi^+(C)$ and $\varphi^+(D)$.

The construction of the matching in the proof of Lemma 4.3.5 also shows the following result.

Corollary 4.3.6. *Let m be the non-crossing matching for $\mathbf{A}^+$. By virtue of m, each letter of type* `c` *is connected to exactly one letter, which is of type* `b`*, and each letter of type* `b` *is connected to exactly one letter, which is of type* `c`*.*

Our interest in the link structure of $\mathbf{A}^+$ stems from the fact that we may transform the sequence $\mathbf{A}$ into a periodic one, using the following transparent mechanism. Let m be the non-crossing matching for $\mathbf{A}^+$, and let $((i_k, j_k))_{k\geq 0}$ be an enumeration of m such that $(j_k - i_k)_{k\geq 0}$ is nondecreasing. We define a sequence $(A^{(k)})_{k\geq 0}$ as follows.

- Set $A^{(0)} = \mathbf{A}^+$.
- Let $k \geq 0$. If $A^{(k)}_{i_k} = \mathtt{c}$, we *rotate* the letters in $A^{(k)}$ with indices $i_k, i_k + 1, \ldots, j_k$ *to the right* by one place, yielding $A^{(k+1)}$. Otherwise, we necessarily have $A^{(k)}_{j_k} = \mathtt{c}$ and we rotate the letters with indices $i_k, i_k + 1, \ldots, j_k - 1$ *to the left* by one place.

In more colourful language, in each step some letter of type `b` is moved along its connecting link and inserted just before the letter of type `c` it is connected to. Note that due to the monotonicity requirement and the non-crossing property, the kth rotation does not change the indices at which the subsequent rotations are carried out. Therefore the sequence $(A^{(k)})_{k\geq 0}$ is well-defined. Moreover, the result does not depend on the particular nondecreasing enumeration of m for the same reasons. Since the first N indices eventually remain unchanged, the limit

$$\rho(\mathbf{A}^+) \coloneqq \gamma\big(\lim_{k\to\infty} A^{(k)}\big) \tag{4.3.15}$$

exists (note that γ, defined in (4.3.8), replaces each letter of type x by x). The definition of $A^{(k)}$ is summarised in the algorithm `RotateAlongLinks`. As in the case of the algorithm `FindMatching`, we require a finite word w (and a finite set $m \subset \mathbb{N}^2$) as input in order to guarantee finite running time.

```
procedure RotateAlongLinks(w,m)
```

```
  if m is not a non-crossing matching for w:
     exit(Error: a non-crossing matching is required);
  Create a list m' from m, ordered by SecondComponent-FirstComponent
  for p in m':
     i←p.FirstComponent;
     j←p.SecondComponent;
     if w[i]=c:
       #Rotate right
       (w[i],...,w[j-1],w[j])←(w[j],w[i],...,w[j-1]);
     else:
       #In this case, w[j]=c. Rotate left
       (w[i],w[i+1],...,w[j-1])←(w[i+1],...,w[j-1],w[i]);
  return w;
end.
```

Algorithm `RotateAlongLinks`. Transform a closed word according to a non-crossing matching

By the above remarks, the words $\texttt{RotateAlongLinks}\big(w_k, M(w_k)\big)$ converge to $\rho(\mathbf{A}^+)$ as $k \to \infty$, where $w = \big(\varphi^+\big)^k(\mathtt{a})$. We have the following central proposition.

Proposition 4.3.7. *Let m be the non-crossing matching for $\mathbf{A}^+$. Then*

$$\rho\big(\mathbf{A}^+\big) = (\mathtt{abc})^\omega. \tag{4.3.16}$$

Proof. Let us first note that the limit itself can be obtained in a simpler way. For any closed word C over K,

(1) apply γ, (2) remove all occurrences of $\mathtt{b}$, (3) reinsert $\mathtt{b}$ before each $\mathtt{c}$.

The resulting word equals $\rho(C)$. This statement simply follows from the facts that (i) both procedures do not change the order in which the underlying letters $\mathtt{a}$ and $\mathtt{c}$ appear, that (ii) each occurrence of $\mathtt{c}$ in both results is preceded by $\mathtt{b}$, and that (iii) in both results, $\mathtt{b}$ does not appear at other places. We therefore see that Proposition 4.3.7 is equivalent to the following. Let $\mathbf{C}$ be the sequence obtained from $\mathbf{A}^+$ by deleting all decorations, and all occurrences of $\mathtt{b}$ and $\bar{\mathtt{b}}$. Then $\mathbf{C} = (\mathtt{ac})^\omega$. In other words, we only have to show that $\mathtt{a}$ and $\mathtt{c}$ occur alternatingly in $\mathbf{A}$, with the empty word or one occurrence of $\mathtt{b}$ in between. We prove a stronger statement concerning the sequence $\overline{\mathbf{A}}$, which will complete the proof of Proposition 4.3.7.

Lemma 4.3.8. *There are sequences $(\varepsilon_k)_{k\geq 0}$ and $(\varepsilon'_k)_{k\geq 0}$ in $\{0,1\}$ such that*

$$\overline{\mathbf{A}} = \mathtt{a}\big(\mathtt{bc}(\mathtt{ac})^{\varepsilon_0}\bar{\mathtt{b}}\mathtt{a}(\mathtt{ca})^{\varepsilon'_0}\big)\big(\mathtt{bc}(\mathtt{ac})^{\varepsilon_1}\bar{\mathtt{b}}\mathtt{a}(\mathtt{ca})^{\varepsilon'_1}\big)\cdots.$$

In order to prove this, we apply the second iteration $\overline{\varphi}^2$ of Berstel's morphism on one of the expressions in brackets. We use the abbreviation

$$b(\varepsilon,\varepsilon') = \mathtt{bc}(\mathtt{ac})^{\varepsilon}\bar{\mathtt{b}}\mathtt{a}(\mathtt{ca})^{\varepsilon'}.$$

Direct computation yields

$$\begin{aligned}
\overline{\varphi}^2(b(0,0)) &= \mathtt{c\bar{b}abc\bar{b}acabc\bar{b}abca} = \mathtt{c\bar{b}a}\, b(0,1)b(0,0)\mathtt{bca},\\
\overline{\varphi}^2(b(0,1)) &= \mathtt{c\bar{b}abc\bar{b}acabc\bar{b}abcac\bar{b}acabca} = \mathtt{c\bar{b}a}\, b(0,1)b(0,0)b(1,1)\mathtt{bca},\\
\overline{\varphi}^2(b(1,0)) &= \mathtt{c\bar{b}abc\bar{b}acabcac\bar{b}acabc\bar{b}abca} = \mathtt{c\bar{b}a}\, b(0,1)b(1,1)b(0,0)\mathtt{bca},\\
\overline{\varphi}^2(b(1,1)) &= \mathtt{c\bar{b}abc\bar{b}acabcac\bar{b}acabc\bar{b}abcac\bar{b}acabca}\\
&\qquad = \mathtt{c\bar{b}a}\, b(0,1)b(1,1)b(0,0)b(1,1)\mathtt{bca}.
\end{aligned}$$

Arbitrary concatenations of these expressions are again of the form $\mathtt{c\bar{b}a}R\,\mathtt{bca}$, where R is a concatenation of words $b(\varepsilon,\varepsilon')$. Assuming that w is of the form $\mathtt{a}\prod_{j<r} b(\varepsilon_j,\varepsilon'_j)\mathtt{bca}$, we obtain $\overline{\varphi}^2(w) = \mathtt{a}\,b(1,0)R\,\mathtt{bca}$. Since the words $\big(\overline{\varphi}^2\big)^k(\mathtt{a})$ approach a fixed point, and

$$\overline{\varphi}^4(\mathtt{a}) = \mathtt{a}\,b(1,0)b(0,1)\mathtt{bca},$$

it follows by induction that $\overline{\mathbf{A}}$ is indeed of the form stated in the lemma, and we have in particular proved Proposition 4.3.7. ⛝

From this algorithm, we can clearly see that a given letter $\mathtt{a}$ is shifted, one place at a time, for each link that is passing over this letter. The direction in which $\mathtt{a}$ is shifted depends on whether $\underset{\llcorner}{\mathtt{c}}$ or $\underset{\lrcorner}{\mathtt{c}}$ appears in the link we are dealing with. We will use considerations of this kind in the following section, together with Proposition 4.3.7, in order to determine the *discrepancy* of $\mathtt{01}$-occurrences in $\mathbf{t}$.

4.3.3 The discrepancy of 01-blocks

For an integer $j \geq 0$ let us define the *degree* of j as follows. Let m be the non-crossing matching for $\mathbf{A}^+$ and set

$$\begin{aligned}
\deg^+(j) &= \#\big\{(k,\ell) \in m : k < j < \ell \text{ and } \mathbf{A}^+_k = \underset{\llcorner}{\mathtt{c}}\big\},\\
\deg^-(j) &= \#\big\{(k,\ell) \in m : k < j < \ell \text{ and } \mathbf{A}^+_\ell = \underset{\lrcorner}{\mathtt{c}}\big\},\\
\deg(j) &= \deg^+(j) - \deg^-(j).
\end{aligned} \tag{4.3.17}$$

We will also talk about the degree of a letter in $\mathbf{A}^+$, where the position in question will always be clear from the context.

We display the first 192 letters of $\mathbf{A}^+$, obtained by applying the third iteration of φ^+ on the word $\mathbf{A}^+_0\mathbf{A}^+_1\mathbf{A}^+_2 = \underset{\llcorner\lrcorner}{\mathtt{abc}}$, and we connect associated connectors by actual lines for better readability. On position $10 = (22)_4$ in $\mathbf{A}^+$, we have a letter $\mathtt{a}$ of degree -1, and on position $170 = (2222)_4$, a letter $\mathtt{a}$ of degree -2. These positions are marked with an arrow.

$$\begin{array}{l}
\mathtt{a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}\overset{\downarrow}{\underset{\llcorner}{\bar{b}}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}}\\
\mathtt{a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}}\\
\mathtt{a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}}\\
\mathtt{a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}\overset{\downarrow}{\underset{\llcorner}{a}}c\underset{\llcorner}{a}b\underset{\llcorner}{c}\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}a\underset{\llcorner}{b}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{b}c\underset{\llcorner}{a}c\underset{\llcorner}{\bar{b}}a\underset{\llcorner}{c}}
\end{array} \tag{4.3.18}$$

From this initial segment we see that the sequence $(\deg(j))_{j\geq}$ starts with the 48 integers

$$\begin{aligned}
&0,0,0,0,0,0,0,0,0,0,-1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,\\
&-1,0,0,0,0,0,-1,-1,-1,-1,0,0,-1,0,\ldots,
\end{aligned}$$

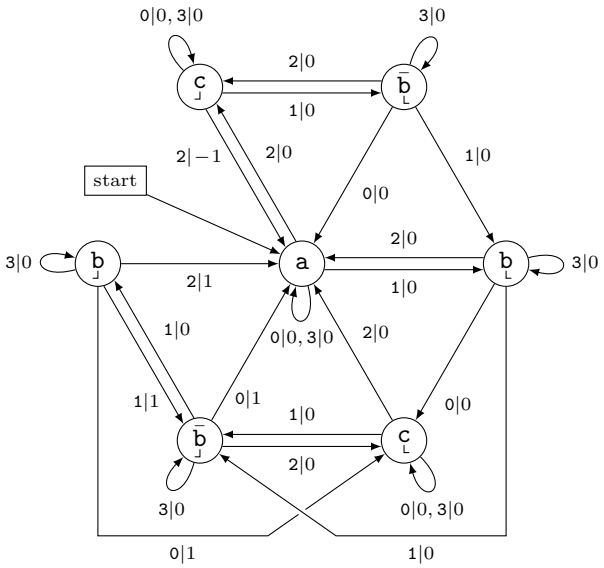


Figure 4.1: A base-4 transducer that generates the degree sequence

corresponding to the first line of (4.3.18). Applying the substitution $(\varphi^+)^2$ on $\bar{\mathtt{b}}\mathtt{a}\mathtt{c}$ appearing on positions 169–171, we obtain the following 48 letters. The marked letter $\mathtt{a}$ has degree -3, and it corresponds to the position $(222222)_4$.

$$\mathtt{a}\mathtt{b}\mathtt{c}\mathtt{a}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{c}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{b}\mathtt{c}\mathtt{a}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{c}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{c}\mathtt{a}\mathtt{b}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{b}\mathtt{c}\mathtt{a}\mathtt{c}\bar{\mathtt{b}}\mathtt{a}\mathtt{c}$$

In general, on position $(2^{2k})_4$, a letter $\mathtt{a}$ of degree $-k$ appears. This can be seen by considering the images of $\mathtt{a}$ and $\underline{\mathtt{c}}$ under φ^+.

By Proposition 4.3.7, $\deg(j)$ has the following meaning in the case that $\mathbf{A}_j^+ = \mathtt{a}$. A number of $\deg^+(j)$ letters $\underline{\mathtt{b}}$ is transferred from the right of the letter $\mathtt{a}$ to the left of it; note that the letter $\mathtt{a}$ is shifted to the right $\deg^+(j)$ places. Analogously, $\deg^-(j)$ letters $\bar{\underline{\mathtt{b}}}$ are transferred from the left of $\mathtt{a}$ to the right, and the letter $\mathtt{a}$ is shifted to the left $\deg^-(j)$ places. In total, the letter $\mathtt{a}$ (among other letters) is shifted by $\deg(j)$ places, and $\mathtt{b}$s or $\bar{\mathtt{b}}$s are moved to account for the generated trailing space. The proposition states that the letters to the left of $\mathtt{a}$'s new position $j+\deg^+(j)$ are balanced — after removing decorations and replacing $\bar{\mathtt{b}}$ by $\mathtt{b}$, the letters $\mathtt{a}$, $\mathtt{b}$, and $\mathtt{c}$ occur the same number of times. If $\mathbf{A}_j^+ \in \{\underline{\mathtt{c}}, \bar{\underline{\mathtt{c}}}\}$, similar considerations hold. The case of letters of degree $\mathtt{b}$ is different, since a single rotation may shift such a letter to a remote place.

The transducer $\mathcal{T}_1$ displayed in Figure 4.1 allows us to compute the degree of an arbitrary position j: starting from the centre node, we traverse the graph, guided by the base-4 expansion $\delta_{\nu-1}\cdots\delta_0$ of j (read from left to right). Along the way, we sum up the numbers k whenever a vertex $\delta_i \mid k$ is taken. The sum over these numbers is the degree of j, multiplied by 3. The transducer $\mathcal{T}_1$ is derived directly from the decorated, 4-uniform morphism φ^+ given in (4.3.7). Note that a change of degree takes place whenever new letters are inserted, by virtue of the morphism φ^+, into the range of already existing links, which happens for $\underline{\mathtt{b}}$ and $\bar{\underline{\mathtt{b}}}$; or, if a new

link together with a letter $\mathtt{a}$ in its range is created, which happens for $\underline{\mathtt{c}}$.

We will now apply Proposition 4.3.7 to the discrepancy D_N of occurrences of $\mathtt{01}$ in $\mathbf{t}$.

Proposition 4.3.9. *Let $j \in \mathbb{N}$ and set $d = \deg(j)$. Then*

$$\begin{aligned}
D_{4j} &= d/3, && \text{if } \mathbf{A}^+_j = \mathtt{a};\\
D_{4j} &= d/3 + 1/3, && \text{if } \mathbf{A}^+_j = \bar{\underline{\mathtt{b}}};\\
D_{4j} &= d/3, && \text{if } \mathbf{A}^+_j = \underline{\mathtt{b}};\\
D_{4j+2} &= d/3 + 1/3, && \text{if } \mathbf{A}^+_j = \underline{\mathtt{b}};\\
D_{4j+2} &= d/3, && \text{if } \mathbf{A}^+_j = \underline{\mathtt{b}};\\
D_{4j+2} &= d/3 - 1/3, && \text{if } \mathbf{A}^+_j = \underline{\mathtt{c}};\\
D_{4j+2} &= d/3, && \text{if } \mathbf{A}^+_j = \underline{\mathtt{c}}.
\end{aligned} \tag{4.3.19}$$

In each of these cases, the subscript of D is the position in $\mathbf{t}$ that corresponds to the jth letter in $\mathbf{A}$ via (4.2.3).

Proof. Choose $\varepsilon \in \{0, 1, 2\}$ and $n \in \mathbb{N}$ such that $j = 3n + \varepsilon$. Let us consider each of the seven cases corresponding to letters from K.

First case. Assume that $\mathbf{A}^+_j = \mathtt{a}$. By Algorithm `RotateAlongLinks` and Proposition 4.3.7, a total of d letters of type $\mathtt{b}$ have to be shifted from the right of our $\mathtt{a}$ in question to the left (if $d > 0$), or the other way round (if $d < 0$). After this procedure, the numbers of letters of types $\mathtt{a}$, $\mathtt{b}$, and $\mathtt{c}$ to the left are equal. It follows that $\varepsilon \equiv -d \bmod 3$; moreover, $m = n + (\varepsilon + d)/3$ is the number of letters $\mathtt{a}$ (and also the number of letters of type $\mathtt{c}$) strictly to the left of j. The number of letters of type $\mathtt{b}$ to the left of j is $m' = n + (\varepsilon - 2d)/3$. Symbols of type $\mathtt{a}$ contribute two blocks $\mathtt{01}$ and correspond to a factor of length six in $\mathbf{t}$, by (4.2.2); letters of type $\mathtt{b}$ contribute one block and correspond to a factor of length four; letters of type $\mathtt{c}$ contribute one block and correspond to a factor of length two. It follows that below position

$$N = (6+2)\left(n + \frac{\varepsilon + d}{3}\right) + 4\left(n + \frac{\varepsilon - 2d}{3}\right) = 12n + 4\,\varepsilon = 4j,$$

we find

$$(2+1)\left(n + \frac{\varepsilon + d}{3}\right) + \left(n + \frac{\varepsilon - 2d}{3}\right) = 4n + 4\,\varepsilon/3 + d/3$$

blocks $\mathtt{01}$. This proves the case $\mathbf{A}^+_j = a$.

Second case. If $\mathbf{A}^+_j = \bar{\underline{\mathtt{b}}}$, we note that necessarily $\mathbf{A}^+_{j+1} = \mathtt{a}$, by Lemma 4.3.1. We apply the first case on position $j+1$, which has degree d. Noting that a letter of type $\mathtt{b}$ in $\mathbf{A}^+$ corresponds to $\mathtt{0110}$ in Thue–Morse, we obtain $D_{4j} = D_{4j+4} + 1/3 = d/3 + 1/3$, where $4j$ resp. $4j+2$ correspond to the jth resp. $(j+1)$th position in $\mathbf{A}^+$.

Third case. Assume that $\mathbf{A}^+_j = \bar{\underline{\mathtt{b}}}$. In this case, the letter at $j+1$ is $\mathtt{a}$ by Lemma 4.3.1 and $j+1$ has degree $d-1$. It follows that $D_{4j} = D_{4j+4} + 1/3 = d/3 - 1/3 + 1/3 = d/3$.

Fourth case. If $\mathbf{A}^+_j = \underline{\mathtt{b}}$, we note that necessarily $\mathbf{A}^+_{j-1} = \mathtt{a}$; we apply the first case on position $j-1$, which has degree $d+1$. since $\mathtt{a}$ corresponds to $\mathtt{011010}$ in Thue–Morse, we have $D_{4j+2} = D_{4j-4} = d/3 + 1/3$, where $4j-4$ resp. $4j+2$ correspond to the $(j-1)$th resp. jth positions in $\mathbf{A}^+$.

Fifth case. Assume that $\mathbf{A}^+_j = \underline{\mathtt{b}}$. Then $\mathbf{A}^+_{j-1} = \mathtt{a}$, and $j-1$ has degree d. Analogously to the fourth case, we obtain $D_{4j+2} = D_{4j-4} = d/3$.

Sixth case. If $\mathbf{A}^+_j = \underline{\mathtt{c}}$, this letter is connected to a letter of type $\mathtt{b}$ to the left, which stays on the left of $\underline{\mathtt{c}}$ after applying the rotations. Therefore the number of letters of type $\mathtt{b}$ to the left

are changed by d, and the numbers of letters of types a or c to the left stay the same. Similarly to the first case, it follows that $\varepsilon \equiv 2 - d \bmod 3$. The numbers of letters, of type a, b, and c respectively, to the left of j, are therefore $m = n + (\varepsilon + d + 1)/3$, $m - d$, and $m - 1$ respectively. It follows that, below position

$$\begin{aligned} N &= 6\left(n + \frac{\varepsilon + d + 1}{3}\right) + 4\left(n + \frac{\varepsilon - 2d + 1}{3}\right) + 2\left(n + \frac{\varepsilon + d - 2}{3}\right) \\ &= 12n + 4\,\varepsilon + 2 = 4j + 2, \end{aligned}$$

there are

$$2\left(n + \frac{\varepsilon + d + 1}{3}\right) + \left(n + \frac{\varepsilon - 2d + 1}{3}\right) + \left(n + \frac{\varepsilon + d - 2}{3}\right) = 4n + \frac{4\,\varepsilon}{3} + \frac{d}{3} + \frac{1}{3}$$

blocks 01.

Seventh case. If $\mathbf{A}_j^+ = \underline{\mathtt{c}}$, a letter of type b is taking its place after one rotation. In this case, we have $\varepsilon \equiv 1 - d \bmod 3$; the numbers of letters to the left of j, of types a, b, and c respectively, are therefore $m = n + (\varepsilon + d + 2)/3$, $m - d - 1$, and $m - 1$ respectively. Therefore, below position

$$\begin{aligned} N &= 6\left(n + \frac{\varepsilon + d + 2}{3}\right) + 4\left(n + \frac{\varepsilon - 2d - 1}{3}\right) + 2\left(n + \frac{\varepsilon + d - 1}{3}\right) \\ &= 12n + 4\,\varepsilon + 2 = 4j + 2, \end{aligned}$$

there are

$$2\left(n + \frac{\varepsilon + d + 2}{3}\right) + \left(n + \frac{\varepsilon - 2d - 1}{3}\right) + \left(n + \frac{\varepsilon + d - 1}{3}\right) = 4n + \frac{4\,\varepsilon}{3} + \frac{d}{3} + \frac{2}{3}$$

blocks 01, which proves the last case. ⛝

Since $\deg(j)$ is easy to obtain, Proposition 4.3.9 gives us a simple method to compute the discrepancy D_N for any given N.

Proposition 4.3.10. *Let $N \geq 0$ be an integer and $j = \lfloor N/4 \rfloor$.*

1. *If $\mathbf{A}_j^+ \in \{\mathtt{a}, \bar{\underline{\mathtt{b}}}, \bar{\underline{\mathtt{b}}}\}$, choose $\delta = D_{4j}/3 = \deg(j)/3 + \varepsilon$, where $\varepsilon \in \{0, 1/3\}$ is given by the first block of* (4.3.19)*. Then*

$$\big(D_{4j}, D_{4j+1}, D_{4j+2}, D_{4j+3}\big) = \big(\delta, \delta + 2/3, \delta + 1/3, \delta\big). \tag{4.3.20}$$

2. *If $\mathbf{A}_j^+ \in \{\underline{\mathtt{b}}, \underline{\mathtt{b}}, \underline{\mathtt{c}}, \underline{\mathtt{c}}\}$, choose $\delta = D_{4j+2}/3 = \deg(j)/3 + \varepsilon$, where $\varepsilon \in \{-1/3, 0, 1/3\}$ is given by the second block of* (4.3.19)*. Then*

$$\big(D_{4j}, D_{4j+1}, D_{4j+2}, D_{4j+3}\big) = \big(\delta + 2/3, \delta + 1/3, \delta, \delta + 2/3\big). \tag{4.3.21}$$

The scaled sequence of discrepancies (multiplied by 3) therefore begins with the 48 integers

$$\begin{array}{llllll} 0,2,1,0, & 2,1,0,2, & 1,0,-1,1, & 0,2,1,0, & 2,1,0,2, & 1,3,2,1, \\ 0,2,1,0, & 2,1,0,2, & 1,0,-1,1, & 0,2,1,0, & -1,1,0,-1, & 1,0,-1,1. \end{array}$$

The partition into segments of length four is for better readability. Each segment corresponds to one symbol in $\mathbf{A}^+$.

Proof of Proposition 4.3.10. For the first sentence of each of the two cases, there is nothing to show, by Proposition 4.3.9. Let us begin with the first case. By the proposition, the position $4j$ in the Thue–Morse sequence corresponds to a letter $\mathtt{a}$ or $\mathtt{b}$ in $\mathbf{A}$ (on position j), and by (4.2.2) we have $(\mathbf{t}_{4j}, \mathbf{t}_{4j+1}, \mathbf{t}_{4j+2}, \mathbf{t}_{4j+3}) = (\mathtt{0110})$. Therefore (4.3.20) follows. Concerning the second case, Proposition 4.3.9 gives us an expression for D_{4j+2} in terms of $\deg(j)$, and the position $4j+2$ corresponds to the index j in $\mathbf{A}$. By (4.2.2), we have $(\mathbf{t}_{4j+2}, \mathbf{t}_{4j+3}) = (\mathtt{0}, \mathtt{1})$. Therefore

$$\big(D_{4j+2}, D_{4j+3}\big) = \big(\delta, \delta + 2/3\big).$$

In order to compute D_{4j} and D_{4j+1} in this case, we note that $\underline{\mathtt{b}}$ and $\underline{\mathtt{b}}$ are always preceded by $\mathtt{a}$ (as we noted in the proof of Proposition 4.3.9), and $\underline{\mathtt{c}}$ and $\underline{\mathtt{c}}$ are always preceded by a letter of type $\mathtt{a}$ or $\mathtt{b}$, since $\mathbf{A}$ is squarefree. It follows that the letter at index $j-1$ is of type $\mathtt{a}$ or $\mathtt{b}$, and therefore $(\mathbf{t}_{4j}, \mathbf{t}_{4j+1}) = (\mathtt{10})$. Consequently, we have

$$\big(D_{4j}, D_{4j+1}\big) = \big(\delta + 2/3, \delta + 1/3\big),$$

and (4.3.21) follows. ⛛

4.3.4 Proof of Theorem 4.1.2

We may now show that the sequence $(D_N)_{N\geq 0}$ of discrepancies is given by a base-2 transducer. The transducer in Figure 4.1 may be described by eight 7×7-matrices $A^{(\ell)}, W^{(\ell)}$, for $0 \leq \ell < 4$, where rows and columns are indexed by the letters of K, in the order $(\mathtt{a}\bar{\underline{\mathtt{b}}}, \bar{\underline{\mathtt{b}}}, \underline{\mathtt{b}}, \underline{\mathtt{b}}, \underline{\mathtt{c}}, \underline{\mathtt{c}})$.

The entry $A^{(\ell)}_{i,j}$ equals 1 if there is an arrow with first component equal to ℓ from the jth node to the ith node in Figure 4.1, and it is zero otherwise. The matrices $A^{(\ell)}$ are permutation matrices. The entry $W^{(\ell)}_{i,j}$ is the second component of the arrow from j to i with first component ℓ, if there is one, and equal to zero otherwise.

The final modification given by (4.3.20) and (4.3.21) is dealt with by four more matrices $Z^{(\ell)}$, where $0 \leq \ell < 4$. The first three columns of these matrices are given by (4.3.20), as follows. Define the quadruple $(q_0, q_1, q_2, q_3) = (0, 2/3, 1/3, 0)$ (containing the shifts in (4.3.20)), and the triple $(r_1, r_2, r_3) = (0, 1/3, 0)$ (taking care of the shifts present in the first block of (4.3.19)). Let $1 \leq j \leq 3$ (corresponding to the letter at which an arrow starts), and $0 \leq \ell < 4$ (a base-4 digit; the first component of the label of the arrow). There is a unique $i \in \{1, \dots, 7\}$ such that $A^{(\ell)}_{i,j} = 1$, and we set $Z^{(\ell)}_{i,j} = q_\ell + r_j$, and $Z^{(\ell)}_{i',j} = 0$ for $i' \neq i$. The remaining four columns are filled with the help of (4.3.21), as follows. Define $(\tilde{q}_0, \tilde{q}_1, \tilde{q}_2, \tilde{q}_3) = (2/3, 1/3, 0, 2/3)$ and $(r_4, r_5, r_6, r_7) = (1/3, 0, -1/3, 0)$. Let $4 \leq j \leq 7$ and $0 \leq \ell < 4$. There is a unique $i \in \{1, \dots, 7\}$ such that $A^{(\ell)}_{i,j} = 1$, and we set $Z^{(\ell)}_{i,j} = \tilde{q}_\ell + r_j$, and $Z^{(\ell)}_{i',j} = 0$ for $i' \neq i$.

In order to generate the discrepancy, we blow up the transducer by a factor 28, in order to keep track of the arrow that led to the current node (that is, we need to save the previously read digit $\ell' \in \{0, 1, 2, 3\}$ and the node in $\mathcal{T}_1$ that was last visited).

In each step, the contribution of $Z^{(\ell')}$ is cancelled out, and the contributions of $A^{(\ell')}$ and $Z^{(\ell)}$ are added (where ℓ is the currently read digit). More precisely, let (i, ℓ', j), for $1 \leq i, j \leq 7$ and $0 \leq \ell' < 4$, be the 196 nodes of our new transducer $\mathcal{T}_2$. There is an arrow from (j, ℓ', k) to (i, ℓ, j') if and only if $j = j'$ and $A^{(\ell)}_{j,i} = 1$ — that is, if there is an arrow from j to i in $\mathcal{T}_1$ whose label has ℓ as its first component. We may now define the weight of an arrow $(j, \ell', k) \to (i, \ell, j)$ as

$$Z^{(\ell)}_{i,j} - Z^{(\ell')}_{j,k} + W^{(\ell')}_{j,k}.$$

The initial node is $(1,0,1)$, which corresponds to the fact that leading zeros do not make a difference. Let us illustrate, by a short but representative example, the easy proof that the transducer $\mathcal{T}_2$ generates the discrepancy sequence. We wish to compute the discrepancy $D_{41} = D_{(221)_4}$. The corresponding path in $\mathcal{T}_2$ is given by

$$(1,0,1) \longrightarrow (5,2,1) \longrightarrow (1,2,5) \longrightarrow (4,1,1).$$

Note that the first and third components correspond to letters in K, that is, to nodes in $\mathcal{T}_1$, via $1 \rightleftharpoons \mathtt{a}$, $4 \rightleftharpoons \mathtt{b}$, and $5 \rightleftharpoons \mathtt{c}$. The sum of the weights simplifies, due to a telescoping sum and $W^{(0)}_{1,1} = Z^{(0)}_{1,1} = 0$, to

$$W^{(2)}_{5,1} + W^{(2)}_{1,5} + Z^{(1)}_{4,1}.$$

The first two summands sum up to $\deg((22)_4) = -1/3$ by the construction of our transducer, while the last summand consists of two parts: the shift in the first line of the first block of (4.3.19) (which is 0), and the shift in the second component of (4.3.20) (which is $2/3$). Summing up, we obtain $D_{41} = 1/3$. It is clear that the proof of the general case is not more complicated this example.

Since the integers 2 and 4 are multiplicatively dependent, in symbols, $2^m = 4^n$ for $(m,n) = (2,1)$, the sequence D is also generated by a base-2 transducer. In order to carry out this reduction to base two, the four arrows starting from a given node in our base-4 transducer have to be replaced by a complete binary tree of depth 2, where two auxiliary nodes have to be inserted. The proposition is proved, and thus the first part of Theorem 4.1.2.

The output sum of a base-q transducer is clearly bounded by a constant times the length of the base-q expansion we feed into the transducer. This immediately yields $D_N \ll \log N$.

We easily see from Figure 4.1 that the integers

$$(2^{2k})_4 = 2\,\frac{16^k - 1}{3} \quad \text{and} \quad ((\mathtt{110})^k)_4 = 20\,\frac{64^k - 1}{63}$$

have degrees $-k$ and k respectively, for $k \geq 1$, and that the letter $\mathtt{a}$ is attained at these positions. Therefore Proposition 4.3.9 implies

$$D_{8(16^k-1)/3} = -k/3 \quad \text{and} \quad D_{80(64^k-1)/63} = k/3 \tag{4.3.22}$$

for $k \geq 1$, and clearly $D_0 = 0$. In particular, $\{D_N : N \geq 0\} = (1/3)\mathbb{Z}$, which finishes the proof of Theorem 4.1.2. ⛒

By considering the path given by $n' = (2^{2k-1})_4$ instead, we end up in the node $\mathtt{c}$, and the position n' has degree $-k+1$. Proposition 4.3.10 implies $D_n = -k/3$, where $n = 4n' + 2 = ((\mathtt{10})^{4k})_2$. This was observed by Jeffrey Shallit (private communication, 2021), but such an unboundedness result does not seem to be stated in the literature.

Acknowledgements.

The author thanks Jeff Shallit for sharing with him the research question treated in this paper, constant interest in his research, and quick and informative answers to e-mails. The question was presented to the author during the workshop 'Numeration and Substitution' at the ESI Vienna (Austria) in July 2019. We express our thanks to the ESI for providing optimal working conditions at the workshop, including offices for participants and blackboards in unconventional places. Finally, we thank Michel Rigo for fruitful discussions on the topic and Clemens Müllner for pointing out that the case of arbitrary factors can be reduced to the case $\mathtt{01}$.

Chapter 5

Collisions of digit sums in bases 2 and 3

Lukas Spiegelhofer
Accepted for publication in Israel J. Math., 2022

Dedicated to Jean-Marc Deshouillers on the occasion of his 75th birthday

Abstract

We prove a folklore conjecture concerning the sum-of-digits functions in bases two and three: there are infinitely many positive integers n such that the sum of the binary digits of n equals the sum of the ternary digits of n.

5.1 Introduction and main result

Representations of the same number x in two or more multiplicatively independent integer bases apparently look very different. This topic is far from being understood, and the relation of the base-q_1 and the base-q_2 expansion to each other is a source of difficult problems.

The base-q expansion is intimately connected to powers of q. In order to understand the relation of different bases q_1 and q_2 to each other better we consider, as a start, the arrangement of powers of 2 and 3. Assume that the set containing all powers of two and three (with nonnegative exponents) is sorted in ascending order:

$$(a_n)_{n\geq 0} = (1, 2, 3, 4, 8, 9, 16, 27, 32, 64, 81, 128, 243, 256, 512, 729, 1024, \ldots)$$

(this is sequence `A006899` in Sloane's OEIS [140]). In what manner are the powers of two and three interleaved? Taking logarithms, we see that the answer to this question is encoded in the Sturmian word

$$w = \big(\lfloor (n+1)\alpha \rfloor - \lfloor n\alpha \rfloor\big)_{n\geq 0},$$

where $\alpha = \log 3/\log 2 = \log_2(3)$, as follows: start with $3^0 = 1$, append the first $w_0 = 1$ powers of two — that is, the integer 2 — append 3^1, then $w_1 = 2$ powers of two, followed by 3^2 and $w_2 = 1$ powers of two, and so on. Our question is therefore equivalent to understanding the

continued fraction expansion of α (consult, for example, Berthé [15] for an explanation of this connection). However, it is not even known whether the sequence of partial quotients of α is bounded, that is, whether α is *badly approximable*; any system in this sequence has yet to be found. The number α is transcendental by the Gelfond–Schneider theorem [70, 71]; by Baker's theorem [9–11] we obtain

$$\left|\frac{\log 3}{\log 2} - \frac{p}{q}\right| \geq \frac{c}{q^\rho}$$

for all integers $q > 0$ and p and some effective positive constants c and ρ. More precisely, a bound for the *irrationality measure* $\mu(\alpha)$ of α, which is the infimum of ρ for which there exists c such that this estimate holds for all p, q, was given by Rhin [131, Equation (8)]: we have $\mu(\alpha) \leq 8.616$. Also, Wu and Wang [162] obtained the bound $\mu(\log 3) \leq 5.1163051$. Note that badly approximable numbers have irrationality measure 2. We would also like to mention the interesting blog entry by Tao[1] on the topic.

In view of the above problem we have to expect major difficulties when we try to mix different bases. In this context, the following unsolved conjecture of Furstenberg [69] is of interest, concerning *multiplicatively independent* integer bases $p, q \geq 2$ (that is, such that $p^k \neq q^\ell$ for all $k, \ell \geq 1$): define

$$O_a(x) \coloneqq \left\{a^k x \bmod 1 : k \in \mathbb{N}\right\}$$

and let $\dim_H(A)$ be the Hausdorff dimension of a set $A \subseteq [0, 1]$. Then

$$\dim_H\left(\overline{O_p(x)}\right) + \dim_H\left(\overline{O_q(x)}\right) \geq 1 \tag{5.1.1}$$

for all irrational $x \in [0, 1]$. Furstenberg's conjecture underlines the idea stated before: different bases should produce very different representations of the same number. We note the papers [139, 161] for recent progress on this conjecture, and the recent preprint [1] by Adamczewski and Faverjon, where related independence results can be found.

The related topic of studying the base-p expansion of powers of q is very difficult and has attracted the attention of many researchers; we note the recent preprint [87] by Kerr, Mérai, and Shparlinski and the references contained therein. Erdős [57] conjectured that the only powers of two having no digit 2 in its ternary expansion are $1, 4$, and 256 (see also Lagarias [92]). This conjecture is open, and Erdős wrote "[...] as far as I can see, there is no method at our disposal to attack this conjecture" [57]. Meanwhile, there is a close connection to to Erdős' *squarefree conjecture* [58], stating that the central binomial coefficient $\binom{2n}{n}$ is never squarefree for $n \geq 5$. The latter conjecture was proved for all large n by Sárközy [135], and solved completely by Granville and Ramaré [79]. The connection between these two conjectures can be understood by considering the identities

$$\nu_2\left(\binom{2n}{n}\right) = s_2(n) \quad \text{and} \quad \nu_3\left(\binom{2n}{n}\right) = s_3(n) - \frac{s_3(2n)}{2},$$

where s_q is the sum-of-digits function in base q, and ν_p is the p-adic valuation of an integer ≥ 1 (with p prime). That is, $\binom{2n}{n}$ is divisible by the square 4 if $n \geq 1$ is not a power of two, and so a stronger form of the (already proved) squarefree conjecture would follow from a proof of the conjecture that

$$s_3(2^k) - s_3(2^{k+1})/2 \geq 2 \quad \text{for } k \geq 9. \tag{5.1.2}$$

In fact, (5.1.2) implies $4 \mid \binom{2n}{n}$ or $9 \mid \binom{2n}{n}$ for each $n \geq 257$, while $\binom{512}{256}$ is divisible by neither 4 nor 3. Equation (5.1.2) in turn would follow if we could prove that the integer 2^k contains at

[1] `https://terrytao.wordpress.com/2011/08/21/hilberts-seventh-problem-and-powers-of-2-and-3/`

least two digits equal to 2 in ternary for $k \geq 9$: in this case at least two carries appear in the addition $2^k + 2^k$ in ternary. We also would like to note the recent preprint [40] by Dimitrov and Howe on this topic.

The main objects in this paper are the sum-of-digits functions s_2 and s_3. For a nonnegative integer n and a base q, the integer $s_q(n)$ is in fact the minimal number of powers of q needed to represent n as their sum (which can be proved using that the q-ary expansion is the lexicographically largest representation of n as a sum of powers of q).

Senge and Straus [138] proved the important theorem that for coprime integers $p, q \geq 2$ and arbitrary $c > 0$, there are only finitely many integers $n \geq 0$ such that

$$s_p(n) \leq c \quad \text{and} \quad s_q(n) \leq c. \tag{5.1.3}$$

This statement is, at least heuristically, close to Furstenberg's conjecture (5.1.1): digital expansions of a number in multiplicatively independent bases usually cannot be simple simultaneously. Extensions of (5.1.3) were proved by Stewart [155], Mignotte [117], Schlickewei [136,137], Pethő–Tichy [128], and Ziegler [165]. See also [25, 28, 97] for related results.

Gelfond [73] proposed to prove that

$$\#\big\{n \leq x : s_{q_1}(n) \equiv \ell_1 \bmod m_1 \text{ and } s_{q_2}(n) \equiv \ell_2 \bmod m_2\big\} = \frac{x}{m_1 m_2} + \mathcal{O}\big(x^\delta\big) \tag{5.1.4}$$

for some $\delta < 1$, where $q_1, q_2 \geq 2$ are coprime bases, m_1, m_2 are integers satisfying $\gcd(m_1, q_1 - 1) = \gcd(m_2, q_2 - 1) = 1$, and $\ell_1, \ell_2 \in \mathbb{Z}$. A weak error term $o(1)$ for this problem was proved by Bésineau [17], while the full statement was obtained by D.-H. Kim [88].

Drmota [41, Theorem 4] proved (among other things) an asymptotic formula for the proportion

$$\frac{1}{x}\#\big\{n < x : s_{q_1}(n) = k_1, s_{q_2}(n) = k_2\big\}, \tag{5.1.5}$$

where $q_1, q_2 \geq 2$ are coprime bases, with an error term $(\log x)^{-1}$. This may be called a *local limit theorem* for the joint sum-of-digits function $n \mapsto (s_p(n), s_q(n))$. Note that Bésineau's result follows as a special case, as the two sum-of-digits functions on $[0, x)$ are mostly found close to their expected values, compare (5.2.48) below.

We also wish to note the recent paper by Drmota, Mauduit, and Rivat [47], who proved a result on the sum of digits of prime numbers in two different bases.

The starting point for the present paper is the article [38] by Deshouillers, Habsieger, Landreau, and Laishram.

> "[...] it seems to be unknown whether there are infinitely many integers n for which $s_2(n) = s_3(n)$ or even for which $|s_2(n) - s_3(n)|$ is significantly small." [38]

They prove the following result.

Theorem. *For sufficiently large N, we have*

$$\#\big\{n \leq N : |s_3(n) - s_2(n)| \leq 0.1457205 \log n\big\} > N^{0.970359}.$$

Note that the difference $s_3(n) - s_2(n)$ is expected to have a value around $C \log n$, where

$$C = \frac{1}{\log 3} - \frac{1}{\log 4} = 0.18889\ldots;$$

by the above theorem there exist indeed many integers n such the difference $|s_2(n) - s_3(n)|$ is "significantly small".

This result was extended by La Bretèche, Stoll, and Tenenbaum [31], who proved in particular that

$$\{s_p(n)/s_q(n) : n \geq 1\} \tag{5.1.6}$$

is dense in $\mathbb{R}^+$ for all multiplicatively independent integer bases p, $q \geq 2$.

We also wish to note the papers [114] by Mauduit and Sárközy, and by Mauduit, Pomerance, and Sárközy [105]. In these papers, integers with a fixed sum of digits and corresponding asymptotic formulas are studied, and possible extensions to several bases are addressed.

Let us call a natural number n such that $s_2(n) = s_3(n)$ a *collision* (of s_2 and s_3). The question on the infinitude of collisions, mentioned in [38], is not a new one. M. Drmota (private communication to the author) received a hand-written letter from A. Hildebrand more than twenty years ago, in which the very same problem was presented.

In the present paper, we give a definite answer to this question.

Theorem 5.1.1. *There exist infinitely many nonnegative integers n such that*

$$s_2(n) = s_3(n). \tag{5.1.7}$$

More precisely, for all $\delta > 0$ we have

$$\#\{n < N : s_2(n) = s_3(n)\} \gg N^{\frac{\log 3}{\log 4} - \delta}, \tag{5.1.8}$$

where the implied constant may depend on δ. Note that $\log 3/\log 4 = 0.792\ldots$.

The difficulty in proving this theorem lies in the separation of the values of $s_2(n)$ and $s_3(n)$. The sum-of-digits functions can be thought of as a sum of independent, identically distributed random variables, and they concentrate (according to Hoeffding's inequality, for example) around the values $\frac{1}{2}\log_2 N$ and $\log_3 N$ respectively, where $0 \leq n < N$. More precisely, the variances are of order $\log N$, and the tails of these distributions decay as least as fast as $\exp(-C(x-\mu)^2/\sigma^2)$, where μ is the expected value, and σ^2 the variance. Since the gap $(1/\log 3 - 1/\log 4)\log N$ comprises $\asymp (\log N)^{1/2}$ standard deviations, we can only expect a number $\ll N^\delta$ of collisions, where $\delta < 1$ is some constant. In the light of this argument, we see that our result cannot be too far from the true number of collisions.

The increasing sequence $\mathfrak{s}_{2,3}$ of nonnegative integers n such that $s_2(n) = s_3(n)$ is listed as entry `A037301` in the OEIS [140]. The question whether this sequence is infinite had to remain open there. The first few collisions are as follows:

n in	binary	0	1	110	111	1010	1011	1100	1101	10010	10011	10101	100100
n in	ternary	0	1	20	21	101	102	110	111	200	201	210	1100
n in	decimal	0	1	6	7	10	11	12	13	18	19	21	36.

Remarks. Note the subsequence $(10, 11, 12, 13)$; contiguous subsequences of $\mathbb{N}$ of length greater than four do not appear in $\mathfrak{s}_{2,3}$, since s_3 on such a subsequence contains two consecutive up-steps, while s_2 decreases or stays constant after one up-step. We expect that it is possible to extend our proof to arbitrary *patterns* in $\mathfrak{s}_{2,3}$: for example, we expect that there are infinitely many n such that

$$s_2(n+v) = s_3(n+v) \quad \text{for} \quad v \in \{0, 1, 2, 3\}, \tag{5.1.9}$$

and infinitely many n (the integer $n = 13$ is an example) such that

$$\big\{v \in \{0, \dots, 23\} : s_2(n+v) = s_3(n+v)\big\} = \{0, 5, 6, 8, 23\}. \tag{5.1.10}$$

More generally, every pattern that appears at all should appear infinitely often in $\mathfrak{s}_{2,3}$. To this end, we will have to study certain residue classes modulo $2^k 3^\ell$ — note that for $n \in (2 + 8\mathbb{Z}) \cap (1 + 9\mathbb{Z})$, for example, we have $s_2(n+v) - s_3(n+v) = c$ for some c and all $v \in \{0, 1, 2, 3\}$. The next step would be to scan these "candidate residue classes" for collisions, using our method. But residue classes of this form are used in our proof anyway, therefore we are optimistic that the main problems have already been overcome. (Note that also a suitable replacement for Proposition 5.2.1 below will have to be found. This proposition takes care of the parity restriction $s_3(n+t) - s_3(n) \equiv s_3(t) \bmod 2$.)

We would like to note that our proof of Theorem 5.1.1 is not a constructive one. We do not give an algorithm that allows us to find integers n such that $s_2(n) = s_3(n)$. We leave it as an open problem to find a construction method for such integers n.

Also, it is a very interesting open problem to prove that $s_2(p) = s_3(p)$ for infinitely many prime numbers p. We believe that this question is difficult. This guess is due to the analogy to *missing digit problems*, where sparse sets $S \subseteq \mathbb{N}$ (that is, $\#(S \cap [1, N]) \ll N^\delta$ for some $\delta < 1$) of a similar kind are studied; Maynard [116], in an important and difficult paper, could prove that infinitely many primes excluding any given decimal digit exist. Our set $S = \{n : s_2(n) = s_3(n)\}$ is even less understood than the set of integers in Maynard's result, hence our scepticism.

Plan of the paper.

The main body of the paper concerns the proof of the auxiliary statement, Proposition 5.2.1 below, which directly leads to the main theorem. This proof is organized into three main steps, represented by Propositions 5.2.2–5.2.4. After the statement of these results, in Section 5.2.1, we prove Proposition 5.2.1 and thus Theorem 5.1.1 from these three propositions. The three sections thereafter, Sections 5.2.2, 5.2.3, and 5.2.4, are dedicated to the proofs of the three main steps. At the end of the paper, we present (mostly difficult) research questions.

Notation. The symbol log denotes the natural logarithm, and $\log_a = \frac{1}{\log a} \log$ is the logarithm in base $a > 1$. We use Landau notation, employing the symbols $\mathcal{O}$, $\ll$, and o. The symbol $f(n) \asymp g(n)$ abbreviates the statement $\big(f(n) \ll g(n)$ and $g(n) \ll f(n)\big)$, while $f(n) \sim g(n)$ means that $f(n)/g(n)$ converges to 1 as $n \to \infty$. We also use the exponential $\mathrm{e}(x) = \exp(2\pi i x)$. For $M \geq 0$, the statement "a is M-close to b" means $|a - b| \leq M$.

5.2 Proofs

Our main theorem follows from the following proposition.

Proposition 5.2.1. *For all $\delta > 0$ the number of $n < N$ such that*

$$s_2(n) - s_3(n) \in \{0, 1\} \tag{5.2.1}$$

is bounded below by $CN^{\frac{\log 3}{\log 4} - \delta}$ (where the constant C may depend on δ).

We call an integer n such that (5.2.1) is satisfied an *almost-collision*.

Let $N \geq 4$ be an integer. We are going to find many collisions in the interval $[N, 2N)$ for all large enough N, which will prove Theorem 5.1.1. Let $\varepsilon > 0$ be arbitrary throughout this proof.

This variable is used as exponent of $\log\log N$, and its value, as long as it is strictly positive, is irrelevant for our proof. For given N, we define λ, η, f, m, and J as follows. Set

$$\begin{aligned} \lambda_0 &\coloneqq \log N, \quad \eta_0 \coloneqq \lambda_0^{3/4}, \qquad f_0 \coloneqq (\log\lambda_0)^{1/2+\varepsilon}, \quad m_0 \coloneqq \lambda_0^{1/2}/f_0, \quad J_0 \coloneqq f_0^2, \\ \lambda &\coloneqq \lfloor\lambda_0\rfloor, \quad \eta \coloneqq 4\lfloor\eta_0/4\rfloor, \quad f \coloneqq \lfloor f_0\rfloor, \qquad m \coloneqq \lfloor m_0\rfloor, \qquad J \coloneqq \lfloor J_0\rfloor. \end{aligned} \tag{5.2.2}$$

We wish to give a rough and very imprecise idea of the meaning of this choice of variables. The length of a binary or ternary expansion of $n \in [N, 2N)$ is of size $\asymp \lambda$, and the standard deviation of a (binary or ternary) sum-of-digits function on $[N, 2N)$ is of order $\asymp (\log N)^{1/2}$. The variable m is smaller than the standard deviation by a factor f (the *fineness*), and taking J steps of length m, we cover sufficiently many standard deviations. That is, the tail (comprising deviations larger than Jm from the expected value) is bounded by λ^{-D} for all $D > 0$ due to the presence of $\varepsilon > 0$. Finally, η is the ternary length of certain integers $\mathfrak{a}$ and $\mathfrak{b}$ that we choose freely. It is large enough to allow for differences of ternary sum-of-digits functions larger than the standard deviation $\asymp \lambda^{1/2}$ by any logarithmic factor $(\log\lambda)^\rho$ (compare to (5.2.32)), and small enough so that a concatenation of $2J+1$ ternary expansions of length η is still much shorter than λ.

After this very informal explanation of our choice of parameters, we give a brief description of the proof. The search for collisions will consist of three main steps.

1. "Preparation": find a residue class A' on which $f(n+t) - f(n)$ takes prescribed, constant differences, where $f(n) = s_2(n) - s_3(n)$;
2. "Rarefaction": concentrate the values of $f(n)$ into the interval $[-Jm, Jm]$ by finding a rarefied and truncated arithmetic progression $A'' \subset A'$, and considering only integers $n \in A''$;
3. "Fair share": select only those $n \in A''$ such that $f(n) \in m\mathbb{Z}$.

Steps 2 and 3 are used to find many values of n from a given given residue class such that $f(n) \in Q \coloneqq \{-Jm, (-J+1)m, \dots, Jm\}$. The purpose of Step 1 is to define *in advance* a larger residue class $A' = L + 2^\nu 3^\beta\mathbb{Z}$ and a set $\mathbf{d} = \{d_{-J}, d_{-J+1}, \dots, d_J\}$ of *shifts* such that $f(n + d_j) - f(n) = jm + \xi_j$ for all $n \in A'$, all $j \in \{-J, \dots, J\}$, and some $\xi_j \in \{0, 1\}$. This procedure yields many n such that $f(n) \in \{0, 1\}$, by choosing for each index n such that $f(n) \in Q$ the appropriate shift $d(n) \in \mathbf{d}$. A short argument involving differences $s_j(n+1) - s_j(n)$ of sum-of-digits functions on residue classes (where $j \in \{2, 3\}$) allows us to get rid of the unpleasant correction term ξ_j.

We will prove the following three propositions, corresponding to our three steps.

Proposition 5.2.2. *Let $\beta = (2J+1)\eta + 1$ and choose the integer $\nu \geq 1$ minimal such that $2^{\nu-1} \geq 3^\beta$. Set*

$$d_j \coloneqq \big(1^{(j+1+J)\eta}0\big)_3 = 3\frac{3^{(j+1+J)\eta} - 1}{2}. \tag{5.2.3}$$

There exists $L \in \{0, \dots, 2^\nu 3^\beta - 1\}$ such that $L \equiv 9 \bmod 12$, and $\xi_j \in \{0, 1\}$ for $-J \leq j \leq J$ such that

$$f(n + d_j) - f(n) = jm + \xi_j \quad \text{for all } j \in \{-J, \dots, J\} \text{ and all } n \in A' \coloneqq L + 2^\nu 3^\beta\mathbb{N}. \tag{5.2.4}$$

Proposition 5.2.3. *For an integer $\zeta \geq 0$, define*

$$A'' \coloneqq \big(L + 2^\nu 3^{\beta+\zeta}\mathbb{N}\big) \cap [N, 2N) \tag{5.2.5}$$

and

$$I \coloneqq \big\{k \in \mathbb{N} : N \le L + 2^\nu 3^{\beta+\zeta} k < 2N\big\}. \tag{5.2.6}$$

Here ν, β, and L are given by Proposition 5.2.2. For all $D > 0$ there exists a constant $C = C(D)$ such that the following statement holds.

$$\begin{aligned}&\text{There exists a sequence } \big(\zeta_N\big)_{N\ge 4} \text{ of nonnegative integers such that}\\ &\zeta_N \sim \log_3(N)\big(1 - \log 3/\log 4\big) \text{ as } N \to \infty, \text{ and for all } N \text{ and all but at most}\\ &C|I|\lambda^{-D} \text{ integers } n \in A'', \text{ the quantity } f(n) \text{ is } Jm\text{-close to } 0.\end{aligned} \tag{5.2.7}$$

Note that I and A'' in this statement depend on $\zeta = \zeta_N$, which in turn depends on N.

Proposition 5.2.4. *Using the set A'' from* (5.2.5)*, we set*

$$P \coloneqq \#\big\{n \in A'' : f(n) \in m\mathbb{Z}\big\}. \tag{5.2.8}$$

As $N \to \infty$, we have

$$P = \frac{|I|}{m}\big(1 + o(1)\big). \tag{5.2.9}$$

That is, the residue class $m\mathbb{Z}$ receives the expected ratio $\lambda^{-1/2}(\log\lambda)^{1/2+\varepsilon}$ of the values of $f(n) = s_2(n) - s_3(n)$ along the finite arithmetic progression A'' defined in (5.2.5)*.*

5.2.1 Deriving Theorem 5.1.1 from Propositions 5.2.2–5.2.4

The expected number P of integers $n \in A''$ such that $f(n) \in m\mathbb{Z}$ is given by Proposition 5.2.4. At the same time, Proposition 5.2.3 states that for all $D > 0$, $f(n)$ lies in the interval $[-Jm, Jm]$ for $|I|(1-\mathcal{O}(\lambda^{-D}))$ many integers $n \in A''$ (where the implied constant depends on D). Note that for $D > 1/2$ this error term is of smaller magnitude than P. Consequently, any choice $D > 1/2$ will yield many integers $n \in A''$ such that $s_2(n) - s_3(n) = jm$ for some $j \in \{-J, \dots, J\}$. By (5.2.4) the integer $n' = n + d_{-j}$ satisfies $s_2(n') - s_3(n') \in \{0, 1\}$. Noting that $\zeta \asymp \log N$ and $J\eta \ll (\log N)^{3/4}(\log\log N)^{1+2\varepsilon}$, we see that the shifts d_j are asymptotically smaller than the common difference $2^\nu 3^{\beta+\zeta}$ of A''. Varying N, we get an almost-collision (as in Proposition 5.2.1) in each large enough interval $[N, 2N)$ and thus the qualitative statement in Theorem 5.1.1.

Considering the asymptotic sizes of ν, β, and ζ, it is easy to see that the interval I defined in (5.2.6) is in fact of size $\gg N^{\log 3/\log 4 - \delta}$ for all $\delta > 0$. Most $k \in I$ yield a value $\tilde{f}(k) = f(L + 2^\nu 3^{\beta+\zeta}k) \in [-Jm, Jm]$ by (5.2.7), and the expected proportion $\sim m^{-1} \gg (\log N)^{-1/2}$ of them satisfy $\tilde{f}(k) \in m\mathbb{Z}$, see (5.2.9). These k yield pairwise different values $k + d_{j(k)}$ as before. Here the integer $j = j(k)$ is chosen suitably from $\{-J, \dots, J\}$ in order to force an almost-collision.

Let $\delta > 0$ be given and set $A = \log 3/\log 4 - \delta$. If the number of $n < N$ such that $s_2(n) - s_3(n) = 0$ and $n \equiv 9 \bmod 12$ is $\gg N^A$, there is nothing to be done. Otherwise, we note that $n \equiv 9 \bmod 12$ is equivalent to $\big(n \equiv 0 \bmod 3 \text{ and } n \equiv 1 \bmod 4\big)$, therefore $s_3(n+1) = s_3(n)+1$ and $s_2(n+1) = s_2(n)$. The existence of a number $\gg N^A$ of solutions of $s_2(n)-s_3(n) = 1$ on $(9 + 12\mathbb{Z}) \cap [N, 2N)$ therefore implies a number $\gg N^A$ of collisions on $(10 + 12\mathbb{Z}) \cap [N, 2N)$. This establishes (5.1.8) and completes the proof. ☒

Remark 11. In the last step towards finding almost-collisions — choosing $j \in \{-J, \dots, J\}$ suitably — the "element of non-constructiveness" in our argument is clearly visible. Currently we do not have any control over the choice of j.

In order to prove Theorem 5.1.1, it is sufficient to establish Propositions 5.2.2–5.2.4.

5.2.2 Constant differences of sum-of-digits functions — proof of Proposition 5.2.2

We will use *blocks* in ternary, whose lengths are given by the integer η. Let us choose nonnegative integers $d_{-J}, d_{-J+1}, \dots, d_J$ by concatenating such blocks of ternary digits. Set

$$\mathfrak{b} \coloneqq \big(1^\eta\big)_3 = \frac{3^\eta - 1}{2},$$

where 1^η denotes η-fold repetition of the digit 1. Define d_j, for $-J \le j \le J$, by $(j+1+J)$-fold concatenation of 1^η, with 0 appended at the right, as in (5.2.3). The emphasis on "blocks of length η" will become clear in the construction of the integers k_j further down (see (5.2.36)). Since the ternary expansion of d_j consists of blocks 1111 and ends with 0, we have $d_j \equiv 0 \bmod 12$ (note that $4 \mid (1111)_3 = 40$). Choose the integer $\nu \ge 1$ minimal so that

$$2^{\nu-1} \ge 3^{(2J+1)\eta+1}. \tag{5.2.10}$$

In particular,

$$d_j < 2^{\nu-1}. \tag{5.2.11}$$

The next important step consists in choosing a certain integer $a \in \{1, \dots, 2^{\nu-1}-1\}$; its meaning will become clear in a moment. The size restrictions imply $d_j + a < 2^\nu$ for all $j \in \{-J, \dots, J\}$. This means in particular that no carry from the $(\nu-1)$th to the νth digit occurs in the addition $d_j + a$, which implies the simple but important identity

$$s_2\big(2^\nu n + a + d_j\big) - s_2\big(2^\nu n + a\big) = s_2^{(\nu)}(a + d_j) - s_2^{(\nu)}(a) \tag{5.2.12}$$

for all $n \ge 0$. The function defined by $s_2^{(\nu)}(n) = s_2(n \bmod 2^\nu)$ is the *truncated binary sum-of-digits function*. Note that the right hand side of (5.2.12) is independent of n; we want to use Chebychev's inequality for choosing a value a such that these values are small for all $j \in \{-J, \dots, J\}$. In order to obtain an estimate for the variance, needed for Chebychev's inequality, we adapt parts from [149]. For integers $t, L \ge 0$ and j, we define a probability mass function $\varphi(\_, t, L)$ by

$$\varphi(j, t, L) \coloneqq \frac{1}{2^L} \#\big\{0 \le n < 2^L : s_2^{(L)}(n+t) - s_2^{(L)}(n) = j\big\}, \tag{5.2.13}$$

and the characteristic function

$$\omega_t(\vartheta, L) \coloneqq \sum_{j \in \mathbb{Z}} \varphi(j, t, L)\, \mathrm{e}(j\vartheta) = \frac{1}{2^L} \sum_{0 \le n < 2^L} \mathrm{e}\big(\vartheta s_2^{(L)}(n+t) - \vartheta s_2^{(L)}(n)\big), \tag{5.2.14}$$

where $\mathrm{e}(x) = \exp(2\pi i x)$. Noting that

$$s_2^{(L+1)}(2n) = s_2^{(L)}(n) \quad \text{and} \quad s_2^{(L+1)}(2n+1) = s_2^{(L)}(n) + 1, \tag{5.2.15}$$

the proof of the following statement is not difficult and left to the reader.

Lemma 5.2.5. *For all $t, L \ge 0$ and $j \in \mathbb{Z}$ we have*

$$\begin{aligned} \varphi(j, 1, L) &= \begin{cases} 2^{j-2}, & -L+2 \le j \le 1; \\ 2^{-L}, & j = -L; \\ 0, & \textit{otherwise,} \end{cases} \\ \varphi(j, 2t, L+1) &= \varphi(j, t, L), \\ \varphi(j, 2t+1, L+1) &= \frac{1}{2}\varphi(j-1, t, L) + \frac{1}{2}\varphi(j+1, t+1, L). \end{aligned} \tag{5.2.16}$$

The characteristic function satisfies

$$\begin{aligned} \big|\omega_t(\vartheta, L)\big| &\le 1, \\ \omega_{2t}(\vartheta, L+1) &= \omega_t(\vartheta, L), \\ \omega_{2t+1}(\vartheta, L+1) &= \frac{\mathrm{e}(\vartheta)}{2}\omega_t(\vartheta, L) + \frac{\mathrm{e}(-\vartheta)}{2}\omega_{t+1}(\vartheta, L) \quad \textit{for } t \ge 1. \end{aligned} \tag{5.2.17}$$

The recurrence (5.2.17) leads to a recurrence for the moments

$$m_k(t, L) \coloneqq \sum_{j\in\mathbb{Z}} \varphi(j, t, L) j^k \tag{5.2.18}$$

of $\varphi(\_, t, L)$. Using the identity

$$\omega_t(\vartheta, L) = \sum_{j\in\mathbb{Z}} \delta(j, t)\,\mathrm{e}(jx) = \sum_{k\ge 0} \frac{m_k(t, L)}{k!}\big(2\pi i\vartheta\big)^k \tag{5.2.19}$$

(all involved series are absolutely convergent), we obtain

$$m_k(t, L) = \frac{k!}{(2\pi i)^k}\big[\vartheta^k\big]\omega_t(\vartheta, L), \tag{5.2.20}$$

from which we can iteratively obtain recurrences for the moments $m_k(t, L)$.

From (5.2.16) we clearly see that $m_0(t, L) = \sum_{j\in\mathbb{Z}} \varphi(j, t, L) = 1$, $m_1(t, L) = \sum_{j\in\mathbb{Z}} j\varphi(j, t, L) = 0$, $\varphi(j, 2t, L{+}1) = \varphi(j, t, L)$, and $m_2(1, L) = 2{-}2^{-L+1}$. Moreover, (5.2.17), (5.2.19), and (5.2.20) imply

$$\begin{aligned} m_2(2t+1, L+1) &= -\frac{1}{4\pi^2}\big[\vartheta^2\big]\Big(\big(1 + 2\pi i\vartheta - 2\pi^2\vartheta^2\big)\big(1 - \big(2\pi^2\big)m_2(t, L)\big) \\ &\qquad + \big(1 - 2\pi i\vartheta - 2\pi^2\vartheta^2\big)\big(1 - \big(2\pi^2\big)m_2(t+1, L)\big)\Big) \\ &= m_2(t, L)/2 + m_2(t+1, L)/2 + 1. \end{aligned}$$

Summarizing, for all $k \ge 0$, $t \ge 1$, and $L \ge 0$, we have

$$\begin{aligned} m_0(t, L) &= 1, \\ m_1(t, L) &= 0, \\ m_2(1, L) &= 2 - 2^{-L+1}, \\ m_k(2t, L+1) &= m_k(t, L), \\ m_2(2t+1, L+1) &= \frac{m_2(t, L) + m_2(t+1, L)}{2} + 1. \end{aligned} \tag{5.2.21}$$

From the recurrence (5.2.17) for the characteristic function we could easily obtain recurrences for the higher moments too (compare [149, (2·11)]), but here we only need the first and second moments. In analogy to Corollary 2.3 in [153] we obtain the following statement.

> There exists a constant C such that for all integers $B, L \ge 1$, and $t \ge 1$ having B blocks of 1s,
>
> $$m_2(t, L) \le CB.$$

However, we only need the following version, which follows directly from (5.2.21): we have

$$m_2(t,\nu) \le 2\nu \quad \text{for all } t,\nu \ge 1 \text{ such that } t < 2^\nu. \tag{5.2.22}$$

In particular, this holds for $t = d_j$ defined in (5.2.3), and for this estimate we do not need to know what d_j looks like in binary. We are interested in the differences on the right hand side of (5.2.12). By Chebychev's inequality and (5.2.22), the number of integers $a \in \{0,\dots,2^\nu-1\}$ such that

$$\left|s_2^{(\nu)}(a+d_j) - s_2^{(\nu)}(a)\right| \le R_2(2\nu)^{1/2} \tag{5.2.23}$$

is bounded below by

$$2^\nu\big(1-1/R_2^2\big).$$

Intersecting $2J+1$ sets, we obtain the set of $a < 2^\nu$ that satisfy (5.2.23) for all $j \in \{-J,\dots,J\}$, having cardinality $\ge 2^\nu(1-(2J+1)/R_2^2)$. We choose $R_2 = \lambda/(2\nu)$, which is $\asymp \lambda^{1/8}/(\log\lambda)^{1/2+\varepsilon}$ as $N\to\infty$. It follows that the set of $a \in \{0,\dots,2^\nu-1\}$ satisfying

$$\left|s_2^{(\nu)}(a+d_j) - s_2^{(\nu)}(a)\right| \le \lambda^{1/2} \quad \text{for all } j \in \{-J,\dots,J\} \tag{5.2.24}$$

has at least

$$2^\nu\big(1-\mathcal{O}\big((\log\lambda)^{2+4\varepsilon}\lambda^{-1/4}\big)\big)$$

elements, by the definitions (5.2.2). Since powers win against logarithms for large N, we obtain some integer a with the properties that

$$\begin{aligned} &a \equiv 1 \bmod 4, \\ &0 \le a < 2^{\nu-1}, \quad \text{and} \\ &|\delta_j| \le \lambda^{1/2} \qquad \text{for all } j \in \{-J,\dots,J\}, \end{aligned} \tag{5.2.25}$$

where

$$\delta_j \coloneqq s_2^{(\nu)}(a+d_j) - s_2^{(\nu)}(a). \tag{5.2.26}$$

Note that the first two restrictions in (5.2.25) will pose no problem since asymptotically almost all $a < 2^\nu$ (as $N\to\infty$) satisfy the third.

By (5.2.12) we have therefore found an arithmetic progression

$$A = a + 2^\nu\mathbb{N} \tag{5.2.27}$$

such that each of the sequences

$$\sigma_j = \big(s_2(m+d_j) - s_2(m)\big)_{m\in A},$$

for $-J \le j \le J$, is constant, and attains a value δ_j bounded by $\lambda^{1/2}$ in absolute value.

In the next step, the ternary sum of digits will come into play, and we rarefy the progression A by a factor 3^β, where

$$\beta = (2J+1)\eta + 1. \tag{5.2.28}$$

Note that $\eta \asymp \lambda^{3/4}$ has been used in the definition (5.2.3) of the values d_j before. The selection of this subsequence has to be carried out with care, so that certain differences $f(n+d_j)-f(n)$, where

$$f(n) = s_2(n) - s_3(n), \tag{5.2.29}$$

are attained on this rarefied progression for $-J \le j \le J$. Sure enough, in order to obtain these differences we will have to "repair" the deviation δ_j from 0 caused by the differences of binary sums of digits. We are going to select a residue class $B = K + 3^\beta\mathbb{N}$, where $K < 3^\beta$, on which certain differences

$$s_3(n + d_j) - s_3(n) \tag{5.2.30}$$

occur for $n \in B$. This process will be executed step by step, thinning out the current residue class by a factor 3^η for each $j \in \{-J, \dots, J\}$. We have found a certain arithmetic progression A in (5.2.27). A sub-progression A' of A having the desired difference properties in bases 2 and 3 — that is, $s_2(n + d_j) - s_2(n) = \delta_j$ and (5.2.39) below — will be obtained by the intersection

$$A \cap B = (a + 2^\nu\mathbb{N}) \cap \big(K + 3^\beta\mathbb{N}\big) = L + 2^\nu 3^\beta\mathbb{N}, \tag{5.2.31}$$

where $0 \le L < 2^\nu 3^\beta$. We need to find K. This number will in fact be divisible by 3 (hence the definition of d_j as a multiple of three) — together with $a \equiv 1 \bmod 4$ this leads to $L \equiv 9 \bmod 12$. The construction is similar to the definition of d_j, where we concatenated ternary expansions of length η, given by $\mathfrak{b} = \big(\mathtt{1}^\eta\big)_3$. We begin with the integer k_{-J}. By our preparation, the quantity $Jm + \delta_{-J}$ (of size $\lambda^{1/2}$ times a logarithmic factor) is considerably smaller than η (of size $\lambda^{3/4}$).

The large number of $\mathtt{1}$s in $\mathfrak{b}$ can be used to find some $\mathfrak{a} \in \{0, \dots, 3^{\eta-1} - 1\}$ and $\xi \in \{0, 1\}$ such that

$$s_3\big(\mathfrak{a} + \mathfrak{b}\big) - s_3(\mathfrak{a}) = Jm + \delta_{-J} - \xi. \tag{5.2.32}$$

In fact, such an integer $\mathfrak{a}$ is found by assembling blocks of length four of ternary digits, where no carry between these blocks occurs, using the following addition patterns in base 3:

$$\begin{array}{r} \mathtt{0112} \\ +\,\mathtt{1111} \\ \hline =\,\mathtt{2000.} \end{array} \qquad \begin{array}{r} \mathtt{0202} \\ +\,\mathtt{1111} \\ \hline =\,\mathtt{2020,} \end{array} \qquad \begin{array}{r} \mathtt{0200} \\ +\,\mathtt{1111} \\ \hline =\,\mathtt{2011.} \end{array}$$

We see that each block of length four can be used to obtain a variation $\in \{-2, 0, 2\}$ of the ternary sum of digits; there are $\eta/4 \gg \lambda^{3/4}$ such blocks, while the needed variation is $\asymp \lambda^{1/2}(\log\lambda)^{1/2+\varepsilon}$ and thus much smaller. Moreover, by construction (5.2.2), the integer η is divisible by four, so there are no phenomena due to trailing digits. Using any $\xi \in \{0, 1\}$ and $\mathfrak{a} < 3^{\eta-1}$ satisfying (5.2.32), we set

$$k_{-J} \coloneqq 3\mathfrak{a} \quad \text{and} \quad \xi_{-J} \coloneqq \xi. \tag{5.2.33}$$

Trivially, we obtain

$$s_3\big(k_{-J} + d_{-J}\big) - s_3\big(k_{-J}\big) = Jm + \delta_{-J} - \xi_{-J}. \tag{5.2.34}$$

Since $\mathfrak{a} < 3^{\eta-1}$, there does not appear a carry to the $\eta + 1$th ternary digit in the addition $k_{-J} + d_{-J}$. Assume that k_{j-1} has already been defined, for some $-J < j \le J$. In analogy to the above, choose $\mathfrak{a} \in \{0, \dots, 3^{\eta-1} - 1\}$ and $\xi \in \{0, 1\}$ in such a way that

$$s_3(\mathfrak{a} + \mathfrak{b}) - s_3(\mathfrak{a}) = -m - \delta_{j-1} + \xi_{j-1} + \delta_j - \xi, \tag{5.2.35}$$

and set

$$k_j = k_{j-1} + 3^{(j+J)\eta+1}\mathfrak{a} \quad \text{and} \quad \xi_j \coloneqq \xi. \tag{5.2.36}$$

Note that the target value satisfies $-m - \delta_{j-1} + \xi_{j-1} + \delta_j - \xi \ll \lambda^{1/2}$, which is again small compared to the number of $\mathtt{1}$s in $\mathfrak{b}$. Since carry propagation between blocks of length η is not

possible by construction (as in the case $j = -J$), we obtain by concatenating blocks of length η and applying a telescoping sum,

$$s_3\big(k_j + d_j\big) - s_3\big(k_j\big) = -jm + \delta_j - \xi_j \quad \text{for all } j \in \{-J, \dots, J\}. \tag{5.2.37}$$

Finally, set $K = k_J$ and note that $\beta = (2J+1)\eta + 1$ according to (5.2.28), so that $K < 3^\beta$. By construction (note that the ternary digits of d_j from $(j+1+J)\eta + 1$ on are zero) we have

$$s_3(K + d_j) - s_3(K) = -jm + \delta_j - \xi_j \quad \text{for all } j \in \{-J, \dots, J\}. \tag{5.2.38}$$

Similar to (5.2.12), noting that there is no carry propagation in base three to the βth digit in the addition $K + d_j$, we have in fact

$$s_3(n + d_j) - s_3(n) = -jm + \delta_j - \xi_j \tag{5.2.39}$$

for all $n \in K + 3^\beta\mathbb{N}$. Define L by (5.2.31). By construction, the residue class $L + 2^\nu 3^\beta\mathbb{Z}$ is a subset of both $3\mathbb{Z}$ and $1 + 4\mathbb{Z}$, therefore $L \equiv 9 \bmod 12$, and we obtain the *difference property* (5.2.4) and thus Proposition 5.2.2. ⛝

5.2.3 Small values of $f(n)$ — proof of Proposition 5.2.3

By our difference property (5.2.4) it is sufficient to prove the existence of (many) elements $n \in A'$ such that

$$f(n) \in Q, \quad \text{where} \quad Q = \{jm : -J \le j \le J\}. \tag{5.2.40}$$

After all, for each n satisfying (5.2.40) we can adjust the value of f, up to a correction term $\in \{0, 1\}$, by any amount $c \in Q$ using a suitably chosen shift $d(n) \in \{d_{-J}, d_{-J+1}, \dots, d_J\}$. Having done so, we arrive at the desired property $f(n + d(n)) \in \{0, 1\}$. Since for each given N the constructed quantities d_j are nonnegative and smaller than the common difference of A' — by (5.2.3) we have $d_j < 2^\nu 3^\beta$ — this will show that there are infinitely many solutions to $s_2(n) - s_3(n) \in \{0, 1\}$, and in fact we will give a quantitative lower bound. Proving that (5.2.40) has many solutions in A' will be the subject of this and the following section, constituting the second ("rarefaction") and third ("fair share") stages of our proof, respectively.

In the present section we are concerned with restricting our residue class A' in order to obtain $f(n) \in [-Jm, Jm]$ for many integers n in the new set A''. The third step will consist in the study of the property $f(n) \in m\mathbb{Z}$, which will be carried out in Section 5.2.4.

Note that for all M, the value $s_2(a+nM)$ will be $C\sqrt{\log N}$-close to $\log_4(N)$ for asymptotically almost all $n < N$ as $N \to \infty$, while $s_3(a + nM)$ will be $C\sqrt{\log N}$-close to $\log_3(N)$ most of the time. Therefore a concentration property of $f(n)$ can only be satisfied for a finite segment of any arithmetic progression. The fact that the values of f can be concentrated around zero by selecting a finite arithmetic subsequence is an essential point. It is based on the consideration that $3^\tau n$ has the same ternary sum of digits as n for all integers $\tau \ge 0$, while the binary sum of digits — usually — increases considerably under multiplication by 3^τ. This small remark is in fact the main idea that started the research on the present paper.

Recall the definition (5.2.5) of A'', for a natural number ζ that will be chosen in due course. Suitable choice of ζ will cause most values of f along A'' to lie in the interval $[-Jm, Jm]$. At this point we only note that 3^ζ will be much larger than 2^ν and 3^β, in orders of magnitude, $\nu \asymp \beta \asymp \lambda^{3/4}(\log\lambda)^{1+2\varepsilon}$, while $\zeta \asymp \lambda$. Trivially, (5.2.4) is satisfied on the subsequence A'' too. We are therefore interested in the expression

$$f\big(L + 2^\nu 3^{\beta+\zeta} k\big) = s_2\big(L + 2^\nu 3^{\beta+\zeta} k\big) - s_3\big(L + 2^\nu 3^{\beta+\zeta} k\big), \tag{5.2.41}$$

where k varies in the interval I defined in (5.2.6). We can decompose (5.2.41) in the form

$$f\big(L + 2^\nu 3^{\beta+\zeta} k\big) = s_2\big(b_2 + 3^{\beta+\zeta} k\big) - s_3\big(b_3 + 2^\nu k\big) + s_2(r_2) - s_3(r_3), \tag{5.2.42}$$

where

$$\begin{aligned} b_2 &= \big\lfloor 2^{-\nu} L \big\rfloor \qquad \text{and} \qquad b_3 = \big\lfloor 3^{-\beta-\zeta} L \big\rfloor, \\ r_2 &= L \bmod 2^\nu \qquad \text{and} \qquad r_3 = L \bmod 3^{\beta+\zeta}. \end{aligned}$$

Let us choose

$$\zeta_0 \coloneqq \log_3(N) \left(1 - \frac{\log 3}{\log 4}\right) + s_3(L) - s_2(r_2) + \frac{\nu}{2} - \beta, \quad \text{and} \quad \zeta \coloneqq \lfloor \zeta_0 \rfloor. \tag{5.2.43}$$

We have $r_2 < 2^\nu$, and $L < 2^\nu 3^\beta$; moreover, it follows from the definitions that $\nu = o(\log N)$ and $\beta = o(\log N)$. Therefore $\zeta \sim C \log_3 N$, where the constant equals

$$C = 1 - \frac{\log 3}{2 \log 2} = 0.207\ldots. \tag{5.2.44}$$

In particular, $3^\zeta \geq 2^\nu$ for all large N. Since $L < 2^\nu 3^\beta$, we have in fact

$$b_3 = 0 \quad \text{and} \quad r_3 = L.$$

That is, r_2 and r_3 do not depend on the particular choice of $\zeta \geq \nu \log_3 2$. In (5.2.43) this freedom is used in order to define the rarefaction parameter ζ suitably. This in turn determines the arithmetic progression A'' defined in (5.2.5). Note that we have already replaced r_3 by L in the definition of ζ_0 in order to avoid a circular definition. This procedure, as we will see, very accurately defines an interval around zero in which $f(n)$, for $n \in A''$, can be found most of the time. That is, (5.2.41) is close to zero for most $k \in I$.

We study the values

$$f_2(k) = s_2\big(b_2 + 3^{\beta+\zeta} k\big) \quad \text{and} \quad f_3(k) = s_3\big(2^\nu k\big) \tag{5.2.45}$$

separately, as k varies in I.

Sure enough, the study of (5.2.45) will be infeasible in general using current techniques. This is the case because we encounter problems arising from powers of 2 and 3, as considered in the introduction. In our application however, the interval I is of the form

$$I = [M, 2M + \mathcal{O}(1)] \tag{5.2.46}$$

for some M considerably larger than 2^ν and $3^{\beta+\zeta}$, which enables us to prove a nontrivial statement on the distributions of $f_2(k)$ and $f_3(k)$.

In the following, we use the abbreviation $\alpha = \beta + \zeta$. Let us partition the binary expansion of $b_2 + 3^\alpha k$ into two parts, using the integer $\kappa_2 = \min\{m : 2^m \geq 3^\alpha\}$. For all integers $k \geq 0$, we have

$$s_2\big(b_2 + 3^\alpha k\big) = s_2\left(\left\lfloor k \frac{3^\alpha}{2^{\kappa_2}} + \sigma \right\rfloor\right) + s_2\big(\big(b_2 + 3^\alpha k\big) \bmod 2^{\kappa_2}\big), \tag{5.2.47}$$

where $\sigma = b_2 2^{-\kappa_2} < 1$, which follows from $b_2 \leq L 2^{-\nu} < 3^\beta < 2^{\kappa_2}$.

The values of $\lfloor k 3^\alpha / 2^{\kappa_2} + \sigma \rfloor$ start at $\tilde{M} + \mathcal{O}(1)$, where $\tilde{M} = \rho M$ and $\rho = 3^\alpha / 2^{\kappa_2} \in (1/2, 1)$, increase step by step as k runs through I, and remain on the same integer for at most two

consecutive values of k. Consequently, the distribution of the first summand for $k \in I$ originates from the distribution of $s_2(k')$ for $k' \in I'$, where

$$I' = [\tilde{M} - 1, 2\tilde{M} + 1],$$

and each number of occurrences is multiplied by a value $\in \{0, 1, 2\}$. Therefore, using the binomial distribution, the first summand in (5.2.47) can be found within a short interval containing $\frac{1}{2}\log_2 M$ most of the time. More precisely, we apply Hoeffding's inequality. Construing the binary sum-of-digits function on $[0, 2^K)$ as a sum of independent random variables with mean $1/2$, we obtain for all integers $T \geq 0$ and real $t \geq 0$

$$\frac{1}{2^T}\big\{0 \leq n < 2^T : \big|s_2(n) - T/2\big| \geq t\big\} \leq 2\exp\left(-2t^2/T\right). \tag{5.2.48}$$

We apply this for $t = Jm/5$ and T minimal such that $2^T \geq 2\tilde{M} + 1$. Note that

$$T \sim \log_2\left(\frac{N}{2^\nu 3^{\beta+\zeta}}\right) \asymp \lambda.$$

Note that we used the definition of ζ for the latter asymptotics. From (5.2.48) we obtain

$$\begin{aligned}\big\{k \in I : \big|s_2\left(\lfloor k3^\alpha/2^{\kappa_2} + \sigma\rfloor\right) - T/2\big| \geq t\big\} &\leq 2\big\{k' \in I' : \big|s_2(k') - T/2\big| \geq t\big\} \\ &\leq 2\big\{0 \leq k' < 2^T : \big|s_2(k') - T/2\big| \geq t\big\} \\ &\ll \exp\big(-2\lambda(\log\lambda)^{1+2\varepsilon}/(25T)\big) \\ &\ll \exp\big(-C(\log\lambda)^{1+2\varepsilon}\big) \\ &\ll \lambda^{-D}\end{aligned} \tag{5.2.49}$$

for all $D > 0$ and some C, as $N \to \infty$. Meanwhile, the second summand in (5.2.47) also follows a binomial distribution, with mean $\kappa_2/2$ and a corresponding concentration property. For this, it is important to note that the sum over k is longer than 2^{κ_2} (for large N): this is due to the observation, given in (5.2.44), that $C < 1/2$. Therefore, multiples of the odd integer 3^α traverse each residue class modulo 2^{κ_2} in a uniform way. After forming an intersection, the value of $f_2(k) = s_2(b_2 + 3^\alpha k)$ is $2Jm/5$-close to the value

$$E_2 = \frac{1}{2}\log_2\left(\frac{N}{2^\nu 3^{\beta+\zeta}}\right) + \frac{1}{2}\log_2 3^{\beta+\zeta} = \frac{1}{2}\log_2(N) - \frac{\nu}{2},$$

for all but $\mathcal{O}\big(|I|\lambda^{-D}\big)$ integers $k \in I$. The contribution of $f_3(k) = s_3(2^\nu k)$ can be handled in an analogous fashion. In this case, the expression $f_3(k)$ is $2Jm/5$-close to the value

$$E_3 = \log_3\left(\frac{N}{2^\nu 3^{\beta+\zeta}}\right) + \log_3(2^\nu) = \log_3(N) - \beta - \zeta$$

for all but $\mathcal{O}\big(|I|\lambda^{-D}\big)$ integers $k \in I$. Again, $D > 0$ is arbitrary. Including the term $s_2(r_2) - s_3(r_3)$ from (5.2.42) leads to the definition of ζ in (5.2.43). Joining the preceding statements and (5.2.42), noting that the allowed deviation Jm is not surpassed when adding two times the error $2Jm/5$ and also considering the rounding error coming from the floor function $\zeta = \lfloor\zeta_0\rfloor$, we obtain Proposition 5.2.3. ⛝

5.2.4 The critical expression modulo m — proof of Proposition 5.2.4

The final piece in the puzzle, which we consider before we proceed to the assembly of these pieces, is the study of the function $f(n) \bmod m = (s_2(n) - s_3(n)) \bmod m$ along arithmetic progressions.

We are going to adapt the Mauduit–Rivat method for digital problems [44, 46, 47, 51, 100–103, 109, 111–113], also applied in the papers [48, 120, 122, 123, 127, 148]. This will be used in order to obtain a statement concerning the number P defined in (5.2.8),

$$\begin{aligned} P &= \#\big\{n \in A'' : f(n) \in m\mathbb{Z}\big\} \\ &= \#\left\{k \in I : s_2\big(b_2 + 3^{\beta+\zeta}k\big) - s_3\big(2^\nu k\big) \equiv t \bmod m\right\}, \end{aligned}$$

where $t = s_3(r_3) - s_2(r_2)$ (see (5.2.42)). In order to handle this quantity, it is sufficient to study

$$S_0 = S_0(\vartheta) = \sum_{k\in I} \mathrm{e}\big(\vartheta s_2\big(b_2 + 3^{\beta+\zeta}k\big) - \vartheta s_3\big(2^\nu k\big)\big), \tag{5.2.50}$$

with $\vartheta = \ell/m$, where $\ell \in \{0, \dots, m-1\}$. By orthogonality relations,

$$P = \frac{|I|}{m} + \frac{1}{m} \sum_{1\le b<m} \mathrm{e}\left(-\frac{bt}{m}\right) S_0\left(\frac{b}{m}\right), \tag{5.2.51}$$

and it is sufficient to find an upper bound for $S_0(\vartheta)$. We apply van der Corput's inequality (for example, [111, Lemme 4]), where $R \ge 1$ is chosen later:

$$\begin{aligned} |S_0|^2 \le \frac{|I|+R-1}{R} &\sum_{-R<r<R} \left(1 - \frac{|r|}{R}\right) \\ &\times \sum_{\substack{k\in I \\ k+r\in I}} \mathrm{e}\Big(\vartheta\big(s_2\big(b_2 + 3^{\beta+\zeta}(k+r)\big) - s_2\big(b_2 + 3^{\beta+\zeta}k\big)\big) - \vartheta\big(s_3\big(2^\nu(k+r)\big) - s_3\big(2^\nu k\big)\big)\Big). \end{aligned}$$

Next, we apply a suitable *carry propagation lemma* in order to "cut off digits", that is, to replace s_2 and s_3 by *truncated sum-of-digits functions*:

$$\begin{aligned} s_2^{(\mu_2)}(n) &= s_2\big(n \bmod 2^{\mu_2}\big), \\ s_3^{(\mu_3)}(n) &= s_3\big(n \bmod 3^{\mu_3}\big), \end{aligned}$$

where $\mu_2, \mu_3 \ge 0$ are chosen later. See [148, Lemma 4.5] for the base-2 version used here; an analogous statement holds for all bases, and we also need the completely analogous base-3 variant (the original statement was given in [111, Lemme 5], compare also [109, Lemme 16]). We discard the condition $n + r \in I$, and join the cases r and $-r$, in order to obtain

$$|S_0|^2 \le |I|^2 \mathcal{O}\left(\frac{R}{|I|} + \frac{3^{\beta+\zeta}R}{2^{\mu_2}} + \frac{2^\nu R}{3^{\mu_3}}\right) + \frac{2\,|I|}{R} \sum_{0\le r<R} \big|S_1\big|, \tag{5.2.52}$$

where

$$\begin{aligned} S_1 = \sum_{k\in I} \mathrm{e}\Big(&\vartheta s_2^{(\mu_2)}\big(3^{\beta+\zeta}k + b_2 + 3^{\beta+\zeta}r\big) - \vartheta s_2^{(\mu_2)}\big(3^{\beta+\zeta}k + b_2\big) \\ &- \vartheta s_3^{(\mu_3)}\big(2^\nu k + 2^\nu r\big) + \vartheta s_3^{(\mu_3)}\big(2^\nu k\big)\Big). \end{aligned} \tag{5.2.53}$$

Note that the lowest μ_2 binary digits of $b_2 + 3^{\beta+\zeta}k$ and the lowest μ_3 ternary digits of $2^\nu k$ are visited *uniformly and independently* — this is just the Chinese remainder theorem.

We obtain

$$S_1 = \frac{|I|}{2^{\mu_2}3^{\mu_3}} \sum_{0\le n_2<2^{\mu_2}} \mathrm{e}\big(\vartheta s_2^{(\mu_2)}\big(n_2 + 3^{\beta+\zeta}r\big) - \vartheta s_2^{(\mu_2)}(n_2)\big) \\ \times \sum_{0\le n_3<3^{\mu_3}} \mathrm{e}\big(\vartheta s_3^{(\mu_3)}\big(n_3 + 2^{\nu}r\big) - \vartheta s_3^{(\mu_3)}(n_3)\big) + \mathcal{O}\big(2^{\mu_2}3^{\mu_3}\big). \tag{5.2.54}$$

For this estimate to be relevant, it is important that the number C defined in (5.2.44) is smaller than $1/2$: the interval I has length $\asymp N/(2^\nu 3^{\beta+\zeta})$, and we need to run through $2^\nu 3^{\beta+\zeta}$ many integers $n \in I$ in order to apply the Chinese remainder theorem. In contrast, comparing the bases 2 and 7, the corresponding constant

$$C_{2,7} \coloneqq 1 - \frac{(2-1)\log 7}{(7-1)\log 2} = 0.532\ldots$$

will already be greater than $1/2$, so new ideas will be needed for bases of "very different size". Meanwhile, adjacent bases b and $b+1$, for example, can certainly be handled by our method; the sequence of constants $C_{b,b+1}$ decreases to zero as $b \to \infty$.

It is sufficient to find a nontrivial estimate for the first factor in (5.2.54), concerning the binary expansion. We are concerned with the correlation (a characteristic function) we had in (5.2.14):

$$\omega_t(\vartheta, L) = \frac{1}{2^L} \sum_{0\le n<2^L} \mathrm{e}\big(\vartheta s_2^{(L)}(n+t) - \vartheta s_2^{(L)}(n)\big).$$

Reusing the argument leading to [149, Lemma 2·7], and Lemma 5.2.5, we obtain the following result.

Lemma 5.2.6. *Assume that integers $B \ge 0$ and $L, t \ge 1$ are given such that t contains at least $2B+1$ blocks of* `1`*s, and $t < 2^L$. Then for all real ϑ,*

$$\big|\omega_t(\vartheta, L)\big| \le \left(1 - \frac{1}{2}\|\vartheta\|^2\right)^B.$$

Our focus therefore lies on the number B of blocks of `1`s in the binary expansion of $3^{\beta+\zeta}r$. The only thing we need to know about powers of three in this context is the fact that they are odd integers — we exploit in an essential way the summation over r instead. The parameter R will be a certain power of N; in this way, the expected size of B is $\gg \lambda$.

Note that counting the number of blocks of `1`s in binary amounts to counting the number of occurrences of `01` (where the `0` corresponds to the more significant digit), up to an error $\mathcal{O}(1)$. For simplicity, we only count such occurrences where the digit `1` in the block `01` occurs at an even index. For example, in the binary expansion `10110110` the corresponding number is 1, whereas there exist three blocks of `1`s. This simplification will, on average, give $1/2$ of the actual expected value, which is sufficient for our purposes. We are therefore concerned with the number $\#\mathtt{1}(n)$ of `1`s occurring in the base-4 expansion of n: the number of integers $0 \le n < 4^K$ such that $\#\mathtt{1}(n) = \ell$ is given by

$$4^K \binom{K}{\ell} (1/4)^\ell (3/4)^{K-\ell}.$$

Suppose that we have $R = 4^K$. Note that

$$r \mapsto r3^{\beta+\zeta} \bmod 4^K$$

is a bijection of the set $\{0, \dots, 4^K-1\}$. We abbreviate $\alpha = 1-\|\vartheta\|^2/2$, and obtain by Lemma 5.2.6

$$\begin{aligned} S_2 &\coloneqq \sum_{0\le r<R} \left| \frac{1}{2^{\mu_2}} \sum_{0\le n_2<2^{\mu_2}} \mathrm{e}\big(\vartheta s_2^{(\mu_2)}\big(n_2+3^{\beta+\zeta}r\big) - \vartheta s_2^{(\mu_2)}(n_2)\big)\right| \\ &\le \sum_{0\le \ell\le K} \sum_{\substack{0\le r<4^K \\ \#1(r)=\ell}} \alpha^{\frac{\ell-2}{2}} \\ &= 4^K\alpha^{-1} \sum_{0\le\ell\le K} \binom{K}{\ell} (1/4)^\ell (3/4)^{K-\ell} \alpha^{\ell/2} \\ &= 4^K\alpha^{-1}\big(\sqrt{\alpha}/4+3/4\big)^K. \end{aligned}$$

Since $\sqrt{1+x} \le 1 + x/2$ for $x \ge -1$, we have

$$\sqrt{\alpha} = \big(1-\|\vartheta\|^2/2\big)^{1/2} \le 1 - \frac{1}{4}\|\vartheta\|^2, \tag{5.2.55}$$

and the inequality $(1+x)^K = \exp\big(K\log(1+x)\big) \le \exp(Kx)$ yields

$$S_2 \ll 4^K \exp\left(-\frac{K}{16}\|\vartheta\|^2\right). \tag{5.2.56}$$

We translate this back to S_0, noting that $\|\vartheta\| \ge 1/m \sim \lambda^{-1/2}(\log\lambda)^{1/2+\varepsilon}$: for some constant $C > 0$ (any value $C \in (0, 1/16)$ is good enough) we obtain

$$|S_0|^2 \ll |I|^2 \left(\frac{R}{|I|} + \frac{3^{\beta+\zeta}R}{2^{\mu_2}} + \frac{2^\nu R}{3^{\mu_3}} + \exp\big(-CK\lambda^{-1}(\log\lambda)^{1+2\varepsilon}\big)\right). \tag{5.2.57}$$

We see that the last term yields a contribution to S_0 that is is smaller than the fair share $|I|m^{-1} \sim |I|\lambda^{-1/2}(\log\lambda)^{1/2+\varepsilon}$ as soon as $K \asymp \lambda$, due to the presence of the power $(\log\lambda)^{1+2\varepsilon}$ in the exponent. For this, we need to choose $R = 4^K$ as large as some positive (fixed) power of N. At the same time we have to take care of the other error terms in (5.2.57). It is obvious that we can choose $R \asymp N^\iota$, where ι is small, and 2^{μ_2} resp. 3^{μ_3} larger than $R\,3^{\beta+\zeta}$ resp. $R\,2^\nu$ (by some small power of N), in such a way that $2^{\mu_2}3^{\mu_3}$ is still smaller than $|I|$ (by another power of N). Such a choice is possible by the fact that $\zeta < 1/2$, and we commented on this after (5.2.54). We therefore obtain (5.2.9) from (5.2.51) and (5.2.57), which completes the proof of Proposition 5.2.4 and thus the proof of Theorem 5.1.1. ⛒

5.3 Open problems

1. Find a construction method for collisions, and for patterns of collisions as in (5.1.9), (5.1.10).

2. Prove that there are infinitely many prime numbers p such that

$$s_2(p) = s_3(p). \tag{5.3.1}$$

3. Prove or disprove the asymptotic formula

$$\#\big\{n < N : s_2(n) = s_3(n)\big\} \sim cN^{\eta} \tag{5.3.2}$$

for some real constants c and η.

4. Prove an asymptotic formula (in k) for the number of solutions of the equation

$$2^{\mu_1} + \cdots + 2^{\mu_k} = 3^{\nu_1} + \cdots + 3^{\nu_k}, \tag{5.3.3}$$

and for the numbers

$$\#\big\{n \in \mathbb{N} : s_2(n) = s_3(n) = k\big\}$$

(finiteness in the second case was proved by Senge and Straus [138]).

5. Generalize Theorem 5.1.1 and Problems 1–4 to any pair (q_1, q_2) of multiplicatively independent bases, and to arbitrary families $(q_1, \ldots, q_K)$ of pairwise coprime bases ≥ 2. It would also be interesting to prove the existence of infinitely many Catalan numbers *exactly divisible* by some power of a, where $a \geq 2$ is an arbitrary integer. This property can be defined by

$$a^k \| n \Leftrightarrow \big(a^k \mid n \ \text{ and } \ \gcd(na^{-k}, a) = 1\big)\,. \tag{5.3.4}$$

6. Study collisions of integer-valued *k-regular sequences* [3, 7] in coprime bases, generalizing the sum-of-digits case.

Acknowledgements.

The author is grateful to Michael Drmota and Joël Rivat, who introduced him to digital expansions as a research topic, and to Thomas Stoll for proposing related research problems to him. Moreover, he thanks Jean-Marc Deshouillers for pointing out the article [38], which was the starting point for the work on the present paper.

Bibliography

[1] Boris Adamczewski and Colin Faverjon, *Mahler's method in several variables and finite automata*, 2020.

[2] Jean-Paul Allouche, Michel Dekking, and Martine Queffélec, *Hidden automatic sequences*, 2021, pp. Paper No. 20, 15. MR 4396225

[3] Jean-Paul Allouche and Jeffrey Shallit, *The ring of k-regular sequences*, Theoret. Comput. Sci. **98** (1992), no. 2, 163–197. MR 1166363 (94c:11021)

[4] ———, *The ubiquitous Prouhet-Thue-Morse sequence*, Sequences and their applications (Singapore, 1998), Springer Ser. Discrete Math. Theor. Comput. Sci., Springer, London, 1999, pp. 1–16. MR 1843077 (2002e:11025)

[5] ———, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003. MR 1997038 (2004k:11028)

[6] ———, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge University Press, Cambridge, 2003. MR 1997038 (2004k:11028)

[7] ———, *The ring of k-regular sequences. II*, Theoret. Comput. Sci. **307** (2003), no. 1, 3–29. MR 2014728 (2004m:68172)

[8] ———, *Automatic sequences are also non-uniformly morphic*, [2020] ©2020, pp. 1–6. MR 4179410

[9] Alan Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), 204–216 (English).

[10] Alan Baker, *Linear forms in the logarithms of algebraic numbers. II*, Mathematika **14** (1967), 102–107 (English).

[11] ———, *Linear forms in the logarithms of algebraic numbers. III*, Mathematika **14** (1967), 220–228 (English).

[12] Guy Barat and Peter J. Grabner, *Distribution of binomial coefficients and digital functions*, J. London Math. Soc. (2) **64** (2001), no. 3, 523–547. MR 1865548 (2002j:11009)

[13] Jean Berstel, *Sur la construction de mots sans carré*, Séminaire de théorie des nombres, 1978–1979, CNRS, Talence, 1979, Exp. No. 18, 15 pages. MR 567880

[14] ———, *Axel Thue's papers on repetitions in words: a translation*, Publications du Laboratoire de Combinatoire et d'Informatique Mathématique, vol. 20, Université du Québec à Montréal, 1995.

[15] Valérie Berthé, *Autour du système de numération d'Ostrowski*, Bull. Belg. Math. Soc. Simon Stevin **8** (2001), no. 2, 209–239, Journées Montoises d'Informatique Théorique (Marne-la-Vallée, 2000). MR 1838931

[16] Valérie Berthé and Paulina Cecchi Bernales, *Balancedness and coboundaries in symbolic systems*, Theor. Comput. Sci. **777** (2019), 93–110 (English).

[17] Jean Bésineau, *Indépendance statistique d'ensembles liés à la fonction "somme des chiffres"*, Acta Arith. **20** (1972), 401–416. MR 0304335 (46 #3470)

[18] Jean Bésineau, *Indépendance statistique d'ensembles liés à la fonction "somme des chiffres"*, Acta Arith. **20** (1972), 401–416. MR 0304335

[19] Patrick Billingsley, *Probability and Measure*, Wiley Series in Probability and Statistics, John Wiley & Sons, Inc., Hoboken, NJ, 2012. MR 2893652

[20] Francine Blanchet-Sadri, James D. Currie, Narad Rampersad, and Nathan Fox, *Abelian complexity of fixed point of morphism* $0 \mapsto 012$, $1 \mapsto 02$, $2 \mapsto 1$, Integers **14** (2014), Paper No. A11, 17 pages. MR 3239592

[21] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), no. 3-4, 203–251. MR 834613

[22] ———, *Primes in arithmetic progressions to large moduli. II*, Math. Ann. **277** (1987), no. 3, 361–393. MR 891581

[23] ———, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc. **2** (1989), no. 2, 215–224. MR 976723

[24] Stephen J. Brams and Alan D. Taylor, *The win-win solution: guaranteeing fair shares to everybody*, W.W. Norton & Company, 1999.

[25] Jhon J. Bravo and Florian Luca, *On the Diophantine equation* $F_n + F_m = 2^a$, Quaest. Math. **39** (2016), no. 3, 391–400 (English).

[26] James L. Brooks, Matt Groening, Al Jean, Mike Scully, Richard Sakai, Ian Maxtone-Graham, George Meyer, et al., *The Simpsons movie*, Beverly Hills, Calif.: 20th Century Fox Home Entertainment, 2007.

[27] Shandy Brown, Narad Rampersad, Jeffrey Shallit, and Troy Vasiga, *Squares and overlaps in the Thue-Morse sequence and some variants*, Theor. Inform. Appl. **40** (2006), no. 3, 473–484. MR 2269205

[28] Yann Bugeaud, Mihai Cipu, and Maurice Mignotte, *On the representation of Fibonacci and Lucas numbers in an integer base*, Ann. Math. Qué. **37** (2013), no. 1, 31–43 (English).

[29] Thomas W. Cusick, Yuan Li, and Pantelimon Stănică, *On a combinatorial conjecture*, Integers **11** (2011), A17, 17. MR 2798642

[30] Cécile Dartyge and Gérald Tenenbaum, *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. **38** (2006), no. 1, 61–69. MR 2201604 (2006k:11039)

[31] Régis de la Bretèche, Thomas Stoll, and Gérald Tenenbaum, *Somme des chiffres et changement de base*, Ann. Inst. Fourier **69** (2019), no. 6, 2507–2518 (French).

[32] F. Michel Dekking, *Morphisms, symbolic sequences, and their standard forms*, J. Integer Seq. **19** (2016), no. 1, Article 16.1.1, 8. MR 3448591

[33] Hubert Delange, *Sur les fonctions q-additives ou q -multiplicatives*, Acta Arith. **21** (1972), 285–298. (errata insert). MR 0309891 (46 #8995)

[34] Guixin Deng and Pingzhi Yuan, *On a combinatorial conjecture of Tu and Deng*, Integers **12** (2012), Paper No. A48, 9. MR 3083421

[35] Jean-Marc Deshouillers, *A footnote to the least non zero digit of n! in base* 12 *[mr2907974]*, Unif. Distrib. Theory **7** (2012), no. 1, 71–73. MR 2943161

[36] ———, *Yet another footnote to the least non zero digit of n*! *in base 12 [MR2907974]*, Unif. Distrib. Theory **11** (2016), no. 2, 163–167. MR 3636294

[37] Jean-Marc Deshouillers, Michael Drmota, and Johannes F. Morgenbesser, *Subsequences of automatic sequences indexed by* $\lfloor n^c \rfloor$ *and correlations*, J. Number Theory **132** (2012), no. 9, 1837–1866. MR 2925851

[38] Jean-Marc Deshouillers, Laurent Habsieger, Shanta Laishram, and Bernard Landreau, *Sums of the digits in bases* 2 *and* 3, Number theory — Diophantine problems, uniform distribution and applications, Springer, 2017, pp. 211–217.

[39] Jean-Marc Deshouillers and Imre Z. Ruzsa, *The least nonzero digit of n*! *in base 12*, Publ. Math. Debrecen **79** (2011), no. 3-4, 395–400. MR 2907974

[40] Vassil S. Dimitrov and Everett W. Howe, *Powers of* 3 *with few nonzero bits and a conjecture of Erdős*, 2021.

[41] Michael Drmota, *The joint distribution of q-additive functions*, Acta Arith. **100** (2001), no. 1, 17–39 (English).

[42] Michael Drmota, Manuel Kauers, and Lukas Spiegelhofer, *On a Conjecture of Cusick Concerning the Sum of Digits of n and* $n + t$, SIAM J. Discrete Math. **30** (2016), no. 2, 621–649, arXiv:1509.08623. MR 3482392

[43] Michael Drmota, Gerhard Larcher, and Friedrich Pillichshammer, *Precise distribution properties of the van der Corput sequence and related sequences*, Manuscripta Math. **118** (2005), no. 1, 11–41. MR 2171290

[44] Michael Drmota, Christian Mauduit, and Joël Rivat, *Primes with an average sum of digits*, Compos. Math. **145** (2009), no. 2, 271–292. MR 2501419

[45] Michael Drmota, Christian Mauduit, and Joël Rivat, *Normality along squares*, J. Eur. Math. Soc **21** (2019), no. 2, 507–548.

[46] Michael Drmota, Christian Mauduit, and Joël Rivat, *Normality along squares*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 2, 507–548. MR 3896209

[47] Michael Drmota, Christian Mauduit, and Joël Rivat, *Prime numbers in two bases*, Duke Math. J. **169** (2020), no. 10, 1809–1876 (English).

[48] Michael Drmota and Johannes F. Morgenbesser, *Generalized Thue-Morse sequences of squares*, Isr. J. Math. **190** (2012), 157–193 (English).

[49] Michael Drmota, Clemens Müllner, and Lukas Spiegelhofer, *Primes as sums of fibonacci numbers*, 2021.

[50] Michael Drmota and Joël Rivat, *The sum-of-digits function of squares*, J. London Math. Soc. (2) **72** (2005), no. 2, 273–292. MR 2156654

[51] Michael Drmota, Joël Rivat, and Thomas Stoll, *The sum of digits of primes in* $\mathbb{Z}[i]$, Monatsh. Math. **155** (2008), no. 3-4, 317–347 (English).

[52] Fabien Durand, *A characterization of substitutive sequences using return words*, Discrete Math. **179** (1998), no. 1-3, 89–101. MR 1489074

[53] P. D. T. A. Elliott and H. Halberstam, *A conjecture in prime number theory*, Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), Academic Press, London, 1970, pp. 59–72. MR 0276195 (43 #1943)

[54] Jordan Emme and Pascal Hubert, *Normal distribution of correlation measures of binary sum-of-digits functions*, 2018, Preprint, http://arxiv.org/abs/1810.11234.

[55] ———, *Central limit theorem for probability measures defined by sum-of-digits function in base 2*, Annali della Scuola Normale Superiore di Pisa **XIX** (2019), no. 2, 757–780.

[56] Jordan Emme and Alexander Prikhod'ko, *On the Asymptotic Behavior of Density of Sets Defined by Sum-of-digits Function in Base 2*, Integers **17** (2017), A58, 28.

[57] Paul Erdős, *Some unconventional problems in number theory*, Math. Mag. **52** (1979), 67–70 (English).

[58] Paul Erdős and Ronald L. Graham, *Old and new problems and results in combinatorial number theory*, vol. 28, L'Enseignement Mathématique, Université de Genève, Genève, 1980 (English).

[59] Paul Erdős, Christian Mauduit, and András Sárközy, *On arithmetic properties of integers with missing digits. I. Distribution in residue classes*, J. Number Theory **70** (1998), no. 2, 99–120. MR 1625049

[60] Jean-Pierre Flori, *Fonctions booléennes, courbes algébriques et multiplication complexe*, Ph.D. thesis, Télécom ParisTech, 2012.

[61] Jean-Pierre Flori, Hugues Randriam, Gérard Cohen, and Sihem Mesnager, *On a conjecture about binary strings distribution*, Sequences and their applications—SETA 2010, Lecture Notes in Comput. Sci., vol. 6338, Springer, Berlin, 2010, pp. 346–358. MR 2830750

[62] E. Fouvry and H. Iwaniec, *On a theorem of Bombieri-Vinogradov type*, Mathematika **27** (1980), no. 2, 135–152 (1981). MR 610700

[63] E. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. **77** (1996), no. 4, 339–351. MR 1414514

[64] ———, *Sommes des chiffres et nombres presque premiers*, Math. Ann. **305** (1996), no. 3, 571–599. MR 1397437 (97k:11029)

[65] Étienne Fouvry, *Répartition des suites dans les progressions arithmétiques*, Acta Arith. **41** (1982), no. 4, 359–382. MR 677549

[66] ———, *Autour du théorème de Bombieri-Vinogradov*, Acta Math. **152** (1984), no. 3-4, 219–244. MR 741055

[67] John Friedlander and Henryk Iwaniec, *Opera de cribro.*, Providence, RI: American Mathematical Society (AMS), 2010 (English).

[68] John B. Friedlander and Henryk Iwaniec, *Incomplete Kloosterman sums and a divisor problem*, Ann. of Math. (2) **121** (1985), no. 2, 319–350, With an appendix by Bryan J. Birch and Enrico Bombieri. MR 786351

[69] H. Furstenberg, *Intersections of Cantor sets and transversality of semi-groups*, Probl. Analysis, Sympos. in Honor of Salomon Bochner, Princeton Univ. 1969, 41-59 (1970)., 1970.

[70] A. Gelfond, *Sur le septième problème de D. Hilbert*, C. R. (Dokl.) Acad. Sci. URSS, n. Ser. **1934** (1934), no. 2, 1–6 (Russian; French).

[71] ———, *Sur le septième Problème de Hilbert*, Bull. Acad. Sci. URSS **1934** (1934), no. 4, 623–634 (English).

[72] A. O. Gel′fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265. MR 0220693 (36 #3745)

[73] A. O. Gel'fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/68), 259–265. MR 220693

[74] Daniel A. Goldston, János Pintz, and Cem Y. Yıldırım, *Primes in tuples. I*, Ann. of Math. (2) **170** (2009), no. 2, 819–862. MR 2552109

[75] W. T. Gowers, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), no. 3, 529–551. MR 1631259

[76] ———, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588. MR 1844079

[77] R. L. Graham, D.E. Knuth, and O. Patashnik, *Concrete Mathematics: a Foundation for Computer Science*, Addison–Wesley, 1989.

[78] Andrew Granville, *Zaphod Beeblebrox's brain and the fifty-ninth row of Pascal's triangle*, Amer. Math. Monthly **99** (1992), no. 4, 318–331. MR 1157222

[79] Andrew Granville and Olivier Ramaré, *Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients*, Mathematika **43** (1996), no. 1, 73–107 (English).

[80] Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547. MR 2415379

[81] ———, *An arithmetic regularity lemma, an associated counting lemma, and applications*, An irregular mind, Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest, 2010, pp. 261–334. MR 2815606

[82] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, at the Clarendon Press, 1954, 3rd ed. MR 0067125 (16,673c)

[83] Clemens Heuberger, Sara Kropf, and Helmut Prodinger, *Output sum of transducers: limiting distribution and periodic fluctuation*, Electron. J. Combin. **22** (2015), no. 2, Paper 2.19, 53. MR 3359922

[84] Sorin Istrail, *On irreductible languages and nonrational numbers*, Bull. Math. Soc. Sci. Math. R. S. Roumanie **21** (1977), no. 69, 301–308.

[85] Jacques Justin and Laurent Vuillon, *Return words in Sturmian and episturmian words*, Theor. Inform. Appl. **34** (2000), no. 5, 343–356. MR 1829231

[86] Dong Yeap Kang, Tom Kelly, Daniela Kühn, Abhishek Methuku, and Deryk Osthus, *A proof of the Erdős-Faber-Lovász conjecture*, 2021, Preprint, available at http://arxiv.org/abs/2101.04698.

[87] Bryce Kerr, László Mérai, and Igor E. Shparlinski, *On digits of mersenne numbers*, 2021.

[88] Dong-Hyun Kim, *On the joint distribution of q-additive functions in residue classes*, J. Number Theory **74** (1999), no. 2, 307–336. MR 1671677 (2000a:11132)

[89] Jakub Konieczny, *Gowers norms for the Thue-Morse and Rudin-Shapiro sequences*, 2017, Preprint, http://arxiv.org/abs/1611.09985.

[90] Alex Kontorovich, *Levels of distribution and the affine sieve*, Ann. Fac. Sci. Toulouse Math. (6) **23** (2014), no. 5, 933–966. MR 3294598

[91] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. **44** (1852), 93–146.

[92] Jeffrey C. Lagarias, *Ternary expansions of powers of* 2, J. Lond. Math. Soc., II. Ser. **79** (2009), no. 3, 562–588 (English).

[93] D. H. Lehmer, *On Stern's Diatomic Series*, Amer. Math. Monthly **36** (1929), no. 2, 59–67. MR 1521653

[94] Marie Lejeune, Julien Leroy, and Michel Rigo, *Computing the* k*-binomial complexity of the Thue–Morse word*, J. Comb. Theory, Ser. A **176** (2020), 105284.

[95] D. A. Lind, *An extension of Stern's diatomic series*, Duke Math. J. **36** (1969), 55–60. MR 0245504

[96] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications, vol. 90, Cambridge University Press, Cambridge, 2002, A collective work by Jean Berstel, Dominique Perrin, Patrice Seebold, Julien Cassaigne, Aldo De Luca, Steffano Varricchio, Alain Lascoux, Bernard Leclerc, Jean-Yves Thibon, Veronique Bruyere, Christiane Frougny, Filippo Mignosi, Antonio Restivo, Christophe Reutenauer, Dominique Foata, Guo-Niu Han, Jacques Desarmenien, Volker Diekert, Tero Harju, Juhani Karhumaki and Wojciech Plandowski, With a preface by Berstel and Perrin. MR 1905123

[97] Florian Luca, *On the Diophantine equation* $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$, Indag. Math., New Ser. **14** (2003), no. 2, 207–222 (English).

[98] E. Lucas, *Sur les congruences des nombres eulériens et les coefficients différentiels des functions trigonométriques suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54. MR 1503769

[99] Bruno Martin, Christian Mauduit, and Joël Rivat, *Théoréme des nombres premiers pour les fonctions digitales*, Acta Arith. **165** (2014), no. 1, 11–45. MR 3263939

[100] Bruno Martin, Christian Mauduit, and Joël Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arith. **165** (2014), no. 1, 11–45 (English).

[101] ———, *Fonctions digitales le long des nombres premiers*, Acta Arith. **170** (2015), no. 2, 175–197 (English).

[102] ———, *Nombres premiers avec contraintes digitales multiples*, Bull. Soc. Math. Fr. **147** (2019), no. 2, 259–287 (French).

[103] ———, *Propriétés locales des chiffres des nombres premiers*, J. Inst. Math. Jussieu **18** (2019), no. 1, 189–224 (French).

[104] Christian Mauduit, *Multiplicative properties of the Thue-Morse sequence*, Period. Math. Hungar. **43** (2001), no. 1-2, 137–153. MR 1830572 (2002i:11081)

[105] Christian Mauduit, Carl Pomerance, and András Sárközy, *On the distribution in residue classes of integers with a fixed sum of digits*, Ramanujan J. **9** (2005), no. 1-2, 45–62 (English).

[106] Christian Mauduit and Joël Rivat, *Répartition des fonctions q-multiplicatives dans la suite* $([n^c])_{n\in\mathbf{N}},\ c > 1$, Acta Arith. **71** (1995), no. 2, 171–179. MR 1339124 (96g:11116)

[107] ———, *Propriétés q-multiplicatives de la suite* $\lfloor n^c \rfloor$, $c > 1$, Acta Arith. **118** (2005), no. 2, 187–203. MR 2141049 (2006e:11151)

[108] ———, *La somme des chiffres des carrés*, Acta Math. **203** (2009), no. 1, 107–148. MR 2545827 (2010j:11119)

[109] Christian Mauduit and Joël Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), no. 1, 107–148. MR 2545827

[110] Christian Mauduit and Joël Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171** (2010), no. 3, 1591–1646. MR 2680394 (2011j:11137)

[111] Christian Mauduit and Joël Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171** (2010), no. 3, 1591–1646. MR 2680394

[112] ———, *Prime numbers along Rudin-Shapiro sequences*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 10, 2595–2642. MR 3420517

[113] Christian Mauduit and Joël Rivat, *Rudin-Shapiro sequences along squares*, Trans. Am. Math. Soc. **370** (2018), no. 11, 7899–7921 (English).

[114] Christian Mauduit and András Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. **81** (1997), no. 2, 145–173. MR 1456239

[115] James Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413. MR 3272929

[116] ———, *Primes with restricted digits*, Invent. Math. **217** (2019), no. 1, 127–218. MR 3958793

[117] M. Mignotte, *Sur les entiers qui s'écrivent simplement en différentes bases. (On integers simply represented in different bases)*, Eur. J. Comb. **9** (1988), no. 4, 307–316 (French).

[118] Johannes F. Morgenbesser, *The sum of digits of $\lfloor n^c \rfloor$*, Acta Arith. **148** (2011), no. 4, 367–393. MR 2800701

[119] Johannes F. Morgenbesser, Jeffrey Shallit, and Thomas Stoll, *Thue-Morse at multiples of an integer*, J. Number Theory **131** (2011), no. 8, 1498–1512. MR 2793891

[120] Johannes F. Morgenbesser and Thomas Stoll, *On a problem of Chen and Liu concerning the prime power factorization of $n!$*, Proc. Am. Math. Soc. **141** (2013), no. 7, 2289–2297 (English).

[121] Yossi Moshe, *On the subword complexity of Thue-Morse polynomial extractions*, Theoret. Comput. Sci. **389** (2007), no. 1-2, 318–329. MR 2363381 (2008j:68064)

[122] Clemens Müllner, *Automatic sequences fulfill the Sarnak conjecture*, Duke Math. J. **166** (2017), no. 17, 3219–3290. MR 3724218

[123] Clemens Müllner, *The Rudin-Shapiro sequence and similar sequences are normal along squares*, Can. J. Math. **70** (2018), no. 5, 1096–1129 (English).

[124] Clemens Müllner and Lukas Spiegelhofer, *Normality of the Thue–Morse sequence along Piatetski-Shapiro sequences, II*, Israel J. Math. **220** (2017), no. 2, 691–738. MR 3666442

[125] S. Northshield, *Stern's diatomic sequence* $0, 1, 1, 2, 1, 3, 2, 3, 1, 4, \ldots$, Amer. Math. Monthly **117** (2010), no. 7, 581–598. MR 2681519 (2011d:11051)

[126] Sam Northshield, *Sums across Pascal's triangle mod 2*, Congr. Numer. **200** (2010), 35–52. MR 2597704

[127] Najib Ouled Azaiez, Mohamed Mkaouar, and Jörg M. Thuswaldner, *Sur les chiffres des nombres premiers translatés*, Funct. Approximatio, Comment. Math. **51** (2014), no. 2, 237–267 (French).

[128] Attila Pethő and Robert F. Tichy, *S-unit equations, linear recurrences and digit expansions*, Publ. Math. **42** (1993), no. 1-2, 145–154 (English).

[129] Ilya I. Piatetski-Shapiro, *On the distribution of prime numbers in sequences of the form $[f(n)]$*, Mat. Sbornik N.S. **33(75)** (1953), 559–566 (Russian). MR 0059302 (15,507e)

[130] Michaël Rao, Michel Rigo, and Pavel Salimov, *Avoiding 2-binomial squares and cubes*, Theoret. Comput. Sci. **572** (2015), 83–91. MR 3314232

[131] Georges Rhin, *Approximants de Padé et mesures effectives d'irrationalité*, Théorie des Nombres, Sémin. Paris 1985/86, Prog. Math. 71, 155-164 (1987)., 1987.

[132] Michel Rigo and Pavel Salimov, *Another generalization of abelian equivalence: binomial complexity of infinite words*, Theor. Comput. Sci. **601** (2015), 47–57.

[133] Joël Rivat and Patrick Sargos, *Nombres premiers de la forme* $\lfloor n^c \rfloor$, Canad. J. Math. **53** (2001), no. 2, 414–433. MR 1820915 (2002a:11107)

[134] Eric Rowland, *The number of nonzero binomial coefficients modulo* p^α, J. Comb. Number Theory **3** (2011), no. 1, 15–25. MR 2908178

[135] A. Sárközy, *On divisors of binomial coefficients. I*, J. Number Theory **20** (1985), 70–80 (English).

[136] Hans Peter Schlickewei, *Linear equations in integers with bounded sum of digits*, J. Number Theory **35** (1990), no. 3, 335–344 (English).

[137] ———, *S-unit equations over number fields*, Invent. Math. **102** (1990), no. 1, 95–107 (English).

[138] H. G. Senge and E. G. Straus, *PV-numbers and sets of multiplicity*, Period. Math. Hung. **3** (1973), 93–100 (English).

[139] Pablo Shmerkin, *On Furstenberg's intersection conjecture, self-similar measures, and the* L^q *norms of convolutions*, Ann. Math. (2) **189** (2019), no. 2, 319–391 (English).

[140] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, 2022, Published electronically at `https://oeis.org`.

[141] Lukas Spiegelhofer, *Piatetski-Shapiro sequences via Beatty sequences*, Acta Arith. **166** (2014), no. 3, 201–229. MR 3283620

[142] ———, *Normality of the Thue–Morse sequence along Piatetski-Shapiro sequences*, Q. J. Math. **66** (2015), no. 4, 1127–1138. MR 3436173

[143] ———, *Discrepancy results for the van der Corput sequence*, Unif. Distrib. Theory **13** (2018), no. 2, 57–69. MR 3883506

[144] ———, *Approaching Cusick's conjecture on the sum-of-digits function*, Integers **19** (2019), Paper No. A53, 8 pages.

[145] ———, *The level of distribution of the Thue–Morse sequence*, Compos. Math. **156** (2020), no. 12, 2560–2587. MR 4208896

[146] ———, *Collisions of digit sums in bases 2 and 3*, 2021.

[147] ———, *Gaps in the Thue–Morse word*, 2021.

[148] ———, *A lower bound for Cusick's conjecture on the digits of* $n + t$, Math. Proc. Cambridge Philos. Soc. **172** (2022), no. 1, 139–161. MR 4354419

[149] ———, *A lower bound for Cusick's conjecture on the digits of* $n + t$, Math. Proc. Cambridge Philos. Soc. **172** (2022), no. 1, 139–161. MR 4354419

[150] Lukas Spiegelhofer and Michael Wallner, *An explicit generating function arising in counting binomial coefficients divisible by powers of primes*, Acta Arith. **181** (2017), no. 1, 27–55. MR 3720001

[151] ———, *Divisibility of binomial coefficients by powers of two*, J. Number Theory **192** (2018), 221–239. MR 3841553

[152] ———, *The Tu–Deng conjecture holds almost surely*, Electron. J. Combin. **26** (2019), no. 1, Paper 1.28, 28. MR 3919615

[153] Lukas Spiegelhofer and Michael Wallner, *The binary digits of $n + t$*, 2021, Accepted for publication in Ann. Sc. norm. super. Pisa Cl. sci. Preprint available on arXiv.

[154] M. A. Stern, *Ueber eine zahlentheoretische Funktion*, J. Reine Angew. Math. **55** (1858), 193–220.

[155] C. L. Stewart, *On the representation of an integer in two different bases*, J. Reine Angew. Math. **319** (1980), 63–72 (English).

[156] Terence Tao, *Higher order Fourier analysis*, Graduate Studies in Mathematics, vol. 142, American Mathematical Society, Providence, RI, 2012. MR 2931680

[157] ———, *Sendov's conjecture for sufficiently high degree polynomials*, 2021, Preprint, available at http://arxiv.org/abs/2012.04125.

[158] A. Thue, *Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen.*, Kristiania: J. Dybwad. 67 S. Lex. 8° (1912)., 1912.

[159] Ziran Tu and Yingpu Deng, *A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity*, Des. Codes Cryptogr. **60** (2011), no. 1, 1–14. MR 2795745

[160] ———, *Boolean functions optimizing most of the cryptographic criteria*, Discrete Appl. Math. **160** (2012), no. 4-5, 427–435. MR 2876325

[161] Meng Wu, *A proof of Furstenberg's conjecture on the intersections of $\times p$- and $\times q$-invariant sets*, Ann. Math. (2) **189** (2019), no. 3, 707–751 (English).

[162] Qiang Wu and Lihong Wang, *On the irrationality measure of* $\log 3$, J. Number Theory **142** (2014), 264–273 (English).

[163] Światomir Ząbek, *Sur la périodicité modulo m des suites de nombres* $\binom{n}{k}$, Ann. Univ. Mariae Curie-Sklodowska. Sect. A **10** (1956), 37–47 (1958). MR 0095147 (20 #1653)

[164] Yitang Zhang, *Bounded gaps between primes*, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174. MR 3171761

[165] Volker Ziegler, *Effective results for linear equations in members of two recurrence sequences*, Acta Arith. **190** (2019), no. 2, 139–169 (English).