A lower bound for Cusick’s conjecture on the digits of \( n + t \)

BY LUKAS SPIEGELHOFER†

Dept. Mathematics and Information Technology, Montanuniversität Leoben, Franz-Josef-Straße 18, 8700 Leoben, Austria.

and TU Wien, Wiedner Hauptstraße 8–10, 1040 Vienna, Austria.

e-mail: lukas.spiegelhofer@unileoben.ac.at

(Received 4 December 2019; revised 4 November 2020; accepted 26 October 2020)

Abstract

Let \( s \) be the sum-of-digits function in base 2, which returns the number of 1s in the base-2 expansion of a nonnegative integer. For a nonnegative integer \( t \), define the asymptotic density

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

T. W. Cusick conjectured that \( c_t > 1/2 \). We have the elementary bound \( 0 < c_t < 1 \); however, no bound of the form \( 0 < \alpha \leq c_t \) or \( c_t \leq \beta < 1 \), valid for all \( t \), is known. In this paper, we prove that \( c_t > 1/2 - \varepsilon \) as soon as \( t \) contains sufficiently many blocks of 1s in its binary expansion. In the proof, we provide estimates for the moments of an associated probability distribution; this extends the study initiated by Emme and Prikhod’ko (2017) and pursued by Emme and Hubert (2018).

2020 Mathematics Subject Classification: 11A63, 05A20 (Primary); 05A16, 11T71 (Secondary)

1. Introduction and main result

It is an elementary problem of deceptive simplicity to study the behaviour of the base-\( q \) digits of an integer under addition of a constant. For example, it is clear that addition of the constant 1 to an even integer in base 2 replaces the right-most digit 0 by 1, and addition of 1 to an odd integer replaces the right-most block of 1s by a block of 0s and the digit 0 directly adjacent to this block by 1. Considerations of this kind can be carried out for each given constant \( t \) in place of 1, which gives a complete description of the digits of \( n \) and \( n + t \).

However, due to carry propagation the situation quickly turns into an unwieldy case distinction for growing \( t \), and a general structural principle describing these cases is out of sight. We therefore consider a simplification of this problem (which is still difficult) by studying a

† The author acknowledges support by the project MuDeRa, which is a joint project between the FWF (Austrian Science Fund) and the ANR (Agence Nationale de la Recherche, France). Moreover, the author was supported by the FWF project F5502-N26, which is a part of the Special Research Program “Quasi Monte Carlo methods: Theory and Applications”.

© The Author(s), 2021. Published by Cambridge University Press on behalf of Cambridge Philosophical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.
parameter associated to the binary expansion: the sum of digits $s(n)$ of $n$ in base $2$, which is just the number of $1$s occurring in the binary expansion of $n$. More precisely, we are interested in the quantities

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

where $\text{dens} A$ is the asymptotic density of a set $A \subseteq \mathbb{N}$, which exists in our case. (In fact, the set in question is a finite union of arithmetic progressions, see Bésineau [5] or the proof following (1.2).) Cusick’s conjecture on the binary sum-of-digits function concerns the values

$$c_t = \text{dens} \{ n \in \mathbb{N} : s(n + t) \geq s(n) \} = \delta(0, t) + \delta(1, t) + \cdots$$

and states that for all $t \geq 0$,

$$c_t > 1/2. \quad (1.1)$$

This conjecture was presented to the author as “question by Cusick” in 2011, by J. F. Morgenbesser; Cusick, in a private communication (2015) upgraded his question to “conjecture”. This easy-to-state elementary problem appears to be difficult, despite its apparent simpless. Moreover, we think that it is not an artificial conjecture. In our opinion, this combination of characteristics constitutes the beauty of this problem. The proof below uses interesting techniques; this highlights the complex structure of the problem and further adds to the interest of this question.

We note the partial results [8, 10, 11, 12, 20] on Cusick’s conjecture, among which we find an almost-all result by Drmota, Kauers, and the author [8] and a central limit-type result by Emme and Hubert [10].

Cusick formulated his conjecture while he was working on the related Tu–Deng conjecture [22, 23], which is relevant in cryptography: assume that $k$ is a positive integer and $t \in \{1, \ldots, 2^k - 2\}$. Then this conjecture states that

$$\left| \left\{ (a, b) \in \{0, \ldots, 2^k - 2\}^2 : a + b \equiv t \mod 2^k - 1, s(a) + s(b) < k \right\} \right| \leq 2^{k-1}.$$ 

Partial results are known, see [6, 7, 14, 15, 21, 22], but the full conjecture is still open. Besides an almost-all result on Tu and Deng’s conjecture [21], Wallner and the author proved in that paper that this conjecture in fact implies Cusick’s conjecture.

We return to Cusick’s conjecture and begin with the case $t = 1$. From the introductory observation we obtain $s(n + 1) - s(n) = 1 - v_2(n + 1)$, where $v_2(m) = \max\{k \geq 0 : 2^k | m\}$, which implies that $\delta(\cdot, 1)$ describes a geometric distribution with mean $0$: we have

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

and therefore $c_1 = 3/4$. In other words, the sum of digits of $n + 1$ is smaller than the sum of digits of $n$ if and only if $n \equiv 3 \mod 4$, since only in this case we lose at least one $1$ by replacing the rightmost block $01^k$ by $10^k$ in the binary expansion.

Next, we consider the general case $t \in \mathbb{N}$. It follows from a recurrence due to Bésineau [5] that the values $\delta(j, t)$ satisfy the following recurrence for all $k \in \mathbb{Z}$ and $t \geq 0$:

$$\delta(j, 2t) = \delta(j, t),$$

$$\delta(j, 2t + 1) = \frac{1}{2} \delta(j - 1, t) + \frac{1}{2} \delta(j + 1, t + 1). \quad (1.2)$$
The proof of the first identity is as follows: we have the disjoint union
\[
\{n \in \mathbb{N} : s(n + 2t) - s(n) = k\} = 2\{n \in \mathbb{N} : s(2n + 2t) - s(2n) = k\}
\cup (2\{n \in \mathbb{N} : s(2n + 1 + 2t) - s(2n + 1) = k\} + 1),
\]
and using the identities \(s(2n) = s(n)\) and \(s(2n + 1) = s(n) + 1\), the first line of the recurrence follows. In an analogous way, the second line can be proved. This proof also shows inductively that the sets defining \(\delta(j, t)\) are finite unions of arithmetic progressions.

Using the recurrence (1.2), we verified (1.1) by numerical computation for all \(t < 2^{30}\), yielding the minimal value 18169025645289/2^{45} = 0.516394... at the position \(t = (1111011101110111101111011111)\) and at the position \(t^R\) obtained by reversing the base-2 expansion of \(t\). (By a result of Morgenbesser and the author [16] we always have \(\delta(j, t^R)\).)

Using a generating function approach and Chebyshev’s inequality, Drmota, Kauers and the author [8] obtained an almost-all result for Cusick’s conjecture: for all \(\varepsilon > 0\), we have
\[
|\{t < T : 1/2 < c_t < 1/2 + \varepsilon\}| = T - \mathcal{O}(T / \log T).
\]

Moreover, the probability distribution defined by \(\mu_t : j \mapsto \delta(j, t)\) for given \(t\) was studied by Emme and Hubert [10, 11], continuing work by Emme and Prikhod’ko [12]. In [10], Emme and Hubert considered the moments of \(\mu_t\) and proved a central limit law. We introduce the notation \(a_X(\lambda) = \sum_{0 \leq i \leq \lambda} X_i 2^i\) for \(X \in \{0, 1\}^\mathbb{N}\) and \(\lambda \geq 0\), and we write \(\Phi(x) = 1/\sqrt{2\pi} \int_{-\infty}^{x} e^{-x^2/2} \, dx\). Then their result states the following. For almost all \(X\) with respect to the balanced Bernoulli measure, we have
\[
\lim_{\lambda \to \infty} \text{dens} \left\{ n \in \mathbb{N} : \frac{s(n + a_X(\lambda)) - s(n)}{\sqrt{\lambda/2}} \leq x \right\} = \Phi(x) \quad \text{for all } x \in \mathbb{R}. \tag{1.3}
\]
Recall that this measure is the unique probability measure on the Borel \(\sigma\)-algebra \(B_X\) such that for each \((\omega_1, \ldots, \omega_k) \in \{0, 1\}^k\), the cylinder set \([\omega_1, \ldots, \omega_k]\) has measure \(2^{-k}\).

In particular, excluding the negligible case that \(s(n + a_X(k)) - s(n) = 0\) and considering \(x = 0\), this statement implies that
\[
\lim_{k \to \infty} c_{a_X(k)} = 1/2 \tag{1.4}
\]
almost surely. Note that this latter result does not follow directly from the Drmota–Kauers–Spiegelhofer result [8], since our error term is not strong enough. On the other hand, the theorem by Emme and Hubert does not give us a statement of the form \(c_t > 1/2\) as in [8].

From (1.3) we obtain the result that \(c_t > 1/2 - \varepsilon\) for almost all \(t\) with respect to asymptotic density. The proof of this fact is by contradiction: assume that \(c_t \leq 1/2 - \varepsilon\) for at least \(2^{\lambda+1}\) many \(t < 2^{\lambda+1}\) and infinitely many \(\lambda\), where \(\delta > 0\). Define
\[
A_k = \{X \in \{0, 1\}^\mathbb{N} : c_{a_X(\lambda)} > 1/2 - \varepsilon \text{ for all } \lambda \geq k\}.
\]
By the almost sure convergence to 1/2 and since the sequence of sets \(A_k\) is ascending, we have \(\mu(A_N) > 1 - \delta\) for some \(N\). Then for all \(X \in A_N\) and \(\lambda > N\) we have \(c_{a_X(\lambda)} > 1/2 - \varepsilon\). By definition of the balanced Bernoulli measure, there exist at least \((1 - \delta)2^{\lambda+1}\) many
142  Lukas Spiegelhofer

$t < 2^{λ+1}$ such that $c_t > 1/2 - ε$. This is a contradiction to our assumption, by which there exists $λ > N$ such that $c_t \leq 1/2 - ε$ for at least $2^{λ+1}δ$ many $t < 2^{λ+1}$.

While this result clearly also follows from the theorem by Drmota, Kauers and the author, it is this particular formulation that we want to sharpen. Our main theorem gives a lower bound for Cusick’s conjecture for all $t$ not contained in a very small exceptional set having a simple structure. In this theorem and in the following, we will be concerned with blocks of 0s or 1s in the binary expansion of $t$; by this, we will always mean contiguous blocks of maximal size, where we omit the lowest block of 0s for even integers $t$. In particular, if we have the binary expansion $t = (1^{m_0} 0^{n_0} 1^{m_1} 0^{n_1} \ldots 1^{m_{ℓ-1}} 0^{n_{ℓ-1}} 1^{m_ℓ} 0^{n_ℓ})_2$ with positive integers $m_i$ and $n_i$ (with the exception of $n_ℓ$, which may be zero), then $t$ contains $ℓ$ blocks of 0s and $ℓ+1$ blocks of 1s.

Our main result is the following lower bound for $c_t$ for many values $t$.

**Theorem 1.1.** For all $ε > 0$ there exists an $L ≥ 0$ such that the following holds: if the binary expansion of $t \in \mathbb{N}$ contains at least $L$ blocks of 1s, then

$$c_t > 1/2 - ε.$$  

In particular, for all $ε > 0$ there exist $δ > 0$ and $C > 0$ such that for $T ≥ 2$,

$$|[0 ≤ t < T : c_t ≤ 1/2 - ε]| ≤ C \log^{δ} T.$$

The “in particular”-part results from counting the number of integers with less than $L$ blocks of 1s in their binary expansion. A rough upper bound is given as follows: up to $2^k$, there are not more than $λ^{2L-2}$ many such natural numbers, since the length of each block of 1s as well as the position of the least significant 1 in each block is bounded by $λ$.

The error term $\log^{δ} T$ should be compared to Drmota–Kauers–Spiegelhofer’s [8] much weaker error term $T / \log T$. Certainly, the statement $c_t > 1/2 - ε$ in Theorem 1.1 is weaker than the bound $c_t > 1/2$ in [8], but the constant 1/2 is optimal: for all $ε > 0$, we have $c_t < 1/2 + ε$ for almost all $t$ with respect to asymptotic density (this follows, as above, from [10], or from [8, theorem 1]).

From Theorem 1.1 we also obtain (1.4) almost surely, since the measure of the set of $X \in [0, 1]^{\mathbb{N}}$ having only finitely many blocks of 1s is zero.

Moreover, we note that Theorem 1.1 significantly sharpens the main theorem in the recent paper [20] by the author: in that paper, it was proved that $c_t + c_τ > 1 - ε$ if $t$ contains many blocks of 1s; here $τ' = 3 \cdot 2^λ - t$, where $2^λ ≤ t < 2^{λ+1}$. The new Theorem 1.1 gives a bound for individual values $c_t$.

Finally, we note that the proof presented below allows to explicitly compute a bound $L = L(ε)$ for Theorem 1.1. This is the case since all of the implied constants appearing in the proof are effective.

**Notation.** In this paper, $0 \in \mathbb{N}$. For an integer $n > 0$, we use the notation $ν_2(n)$ to denote the largest $k$ such that $2^k \mid n$. We will use Big O notation, employing the symbol $O$. For an integer $t ≥ 1$, the number of blocks in $t$ is the number of blocks of 1s in the binary expansion of $t$ plus the number of blocks of 0s in the proper binary expansion of $t/2^{ν_2(t)}$. Clearly, if $ℓ$ is the number of blocks of 1s in the binary expansion of $t$, then $2ℓ - 1$ is the number of blocks in $t$. We also define the number of blocks in 0 to be 0. The variable $r$ is used to denote
the number of blocks in \( t \). We let \( e(x) \) denote \( e^{2\pi ix} \) for real \( x \), and \( \|x\| = \min_{k \in \mathbb{Z}} |x - k| \) is the distance to the nearest integer. For convenience, we define the maximum over an empty index set to be 0.

The remainder of this paper is dedicated to the proof of Theorem 1.1.

2. Proof of the main theorem

The proof consists of several steps. We consider the characteristic function \( \gamma_t \) of a certain probability distribution. Using the link between \( \gamma_t \) and \( c_t \) expressed by (2.3), we see that we have to find upper bounds for \( \text{Im} \gamma_t \). We do so in two stages: for \( \vartheta \) not close to \( \mathbb{Z} \), we estimate the absolute value of \( \gamma_t(\vartheta) \) using a matrix identity from [16]. For \( \vartheta \) close to \( \mathbb{Z} \), we estimate the imaginary part of \( \gamma_t(\vartheta) \) using the link (2.16) to the moments \( m_k(t) \). The principal part of the proof is concerned with finding upper bounds for these moments (captured in Proposition 2.6), thus extending the study performed by Emme and Prikhod’ko [12], and Emme and Hubert [10, 11].

2.1. Relating \( c_t \) to a characteristic function

For \( \vartheta \in \mathbb{R} \) and \( t \geq 0 \), we define

\[
\gamma_t(\vartheta) = \lim_{N \to \infty} \frac{1}{N} \sum_{0 \leq n < N} e(\vartheta s(n + t) - \vartheta s(n)).
\]

These limits exist, see Bésineau [5], and we have

\[
\gamma_t(\vartheta) = \sum_{-\infty \leq j < m} \delta(j, t) e(j \vartheta) \tag{2.1}
\]

for some \( m \) (which can be shown by induction easily). We have

\[
\delta(j, t) = \int_0^1 \gamma_t(\vartheta) e(-j \vartheta) \, d\vartheta \tag{2.2}
\]

(see [16]); using these identities and a geometric sum, we will prove the following identity.

**Proposition 2.1.** Let \( t \geq 0 \). We have

\[
c_t = \frac{1}{2} + \frac{\delta(0, t)}{2} + \frac{1}{2} \int_0^1 \text{Im} \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta, \tag{2.3}
\]

where the integrand is a bounded function.

In the proof of this statement, we are also going to use the following fact.

**Lemma 2.2.** For \( k \geq 1 \) we have

\[
\int_0^1 \sin(2\pi k \vartheta) \cot(\pi \vartheta) \, d\vartheta = 1, \tag{2.4}
\]

where the integrand is bounded on \((0, 1)\).
we have the formulas

\[
\sum_{j} \text{ where all occurring summands are bounded functions. Since } \sum_{j}^{\infty} \delta(j, t) = 1, \text{ it follows that }
\]

\[
\gamma_t(\vartheta) e(-m \vartheta) = \sum_{\ell \geq 1} a_{\ell} e(-\ell \vartheta)
\]
for some nonnegative \( a_\ell \) such that \( \sum_{\ell \geq 1} a_\ell = 1 \). Since \( m \) is large enough, the integral over the second summand in the second line of (2.7) is zero. We obtain

\[
c_t = \int_0^1 \Re \frac{\gamma(\vartheta)}{1 - e(-\vartheta)} + \frac{1}{2} \sum_{\ell \geq 1} a_\ell \sin(-2\pi \ell \vartheta) \cot(-\pi \vartheta) \, d\vartheta.
\]

The partial sums \( \sum_{1 \leq \ell < L} a_\ell \sin(-2\pi \ell \vartheta) \cot(-\pi \vartheta) \) are bounded, uniformly in \( L \), by an integrable function on \([0, 1]\), therefore the statement follows by interchanging the summation and the integral, an application of the identity (2·7), and another application of (2·6).

2.2. Moments of \( \mu_t \)

Define

\[
\tilde{m}_k(t) = \sum_{j \in \mathbb{Z}} \delta(j, t) j^k.
\]

The moment generating function is

\[
M_t(x) = \sum_{k \geq 0} \frac{\tilde{m}_k(t)}{k!} x^k.
\]

The moments exist and the moment generating function is convergent for \( t = 1 \) and \( |x| < \log 2 \); this is just a geometric distribution and we obtain

\[
M_1(x) = \frac{e^x}{2 - e^{-x}} = 1 + x^2 - x^3 + \frac{19}{12} x^4 - \ldots
\]

(see entry A052841 in Sloane’s OEIS\(^1\)). By basic analytic combinatorics [13], we obtain

\[
m_k(t) \sim c (\log 2)^{-k}
\]

for some absolute \( c \), as \( k \to \infty \).

For \( t \geq 2 \), we note that the recurrence relation (1·2) implies that \( \delta(j, t) = c 2^j \) for \( j < -\lambda \), where \( 2^\lambda \leq t < 2^{\lambda+1} \). This implies that \( \tilde{m}_k(t) \) exists for all \( k \) and \( |\tilde{m}_k(t)| \ll \lambda^k + \tilde{m}_k(1) \). Considering also the series for the exponential function and the asymptotic estimate (2·9), we see that the series for \( M_t(x) \) is convergent as long as \( |x| < \log 2 \).

From (1·2) we wish to derive a recurrence for the moment generating functions. We define

\[
m_k(t) = \frac{\tilde{m}_k(t)}{k!},
\]

such that \( M_k(x) = \sum_{k \geq 0} m_k(t) x^k \).

**Lemma 2.3.** Assume that \( |x| < \log 2 \) and \( t \geq 0 \). We have

\[
M_{2t}(x) = M_t(x) \quad \text{and} \quad M_{2t+1}(x) = \frac{e^x}{2} M_t(x) + \frac{e^{-x}}{2} M_{t+1}(x).
\]

\(^1\)http://oeis.org
In particular,

\[ m_k(2t) = m_k(t) \text{ and } m_k(2t + 1) = \frac{1}{2} \sum_{0 \leq \ell \leq k} \frac{1}{\ell!} (m_{k-\ell}(t) + (-1)^\ell m_{k-\ell}(t + 1)). \] (2.11)

Note that setting \( t = 0 \), we obtain (2.8).

**Proof.** The first line of (2.10) is trivial since \( \delta(j, 2t) = \delta(j, t) \). Concerning the second line, we have

\[ M_t(x) = \sum_{j \in \mathbb{Z}} \delta(j, t)e^{ix}, \]

therefore by (1.2)

\[ M_{2t+1}(x) = \sum_{j \in \mathbb{Z}} \delta(j, 2t + 1)e^{ix} = \frac{1}{2} \sum_{j \in \mathbb{Z}} \delta(j - 1, t)e^{ix} + \frac{1}{2} \sum_{j \in \mathbb{Z}} \delta(j + 1, t + 1)e^{ix} \]

\[ = \frac{e^x}{2} M_t(x) + \frac{e^{-x}}{2} M_{t+1}(x) \]

after a shift of indices. The “in particular”-part follows from expanding Cauchy products.

The first few moments are as follows: \( m_0(t) = 1 \), \( m_1(t) = 0 \), and \( m_2(t) \) satisfies the recurrence

\[ m_2(0) = 0, \quad m_2(1) = 1, \quad m_2(2t) = m_2(t), \quad m_2(2t + 1) = \frac{m_2(t) + m_2(t + 1) + 1}{2}. \]

This particular sequence also arises in a different context: it is the *star-discrepancy* of the van der Corput sequence in base 2 [9, 19]. It is known that

\[ m_2(t) \leq \frac{\log t}{3 \log 2} + 1 \] (2.12)

for all \( t \geq 1 \) (see Bejian and Faure [4]). The following interesting exact representation of \( m_2(t) \) follows from Proinov and Atanassov [17], and Beck [3] (as was pointed out to the author by the anonymous referee of the article [19]); see the remark after [19, corollary 2.5]: if \( t = \sum_{0 \leq i \leq v} \varepsilon_i 2^i \) with \( \varepsilon_i \in \{0, 1\} \), we have

\[ m_2(t) = \sum_{0 \leq i \leq v} \varepsilon_i - \sum_{0 \leq i < j \leq v} \varepsilon_i \varepsilon_j 2^{i-j}. \] (2.13)

At this point we wish to emphasise the usefulness of the moments as opposed to \( \delta(j, t) \). In order to compute \( \delta(j, t) \), we need to consider values \( \delta(j + \ell, t') \) for large \( \ell \) (depending on the number of 1s and 0s in the binary expansion of \( t/2^{\nu_2(t)} \)); for computing \( m_2(t) \) we only need to consider moments \( m_i(t') \) for \( i \leq k \). In particular, \( m_k \) is a 2-regular sequence [1], while this is not so clear and perhaps wrong for \( \delta(j, \cdot) \).

Using Chebyshev’s inequality and the bound (2.12) for \( m_2(t) \) we can already find a nontrivial bound related to Cusick’s conjecture: with \( \sigma = \sqrt{(\log t)/(3 \log 2) + 1} \) we have
A lower bound for Cusick’s conjecture

$$\sum_{|j| \leq K} \delta(j, t) \geq 1 - 1/K^2.$$  
In particular, choosing $K$ close to $\sqrt{2}$, we obtain

$$\sum_{j \geq -\sqrt{\log t} - 1} \delta(j, t) \geq \sum_{j \geq -\sqrt{\log t} + 2} \delta(j, t) > 1/2$$  \hfill (2.14)

for $t \geq 1$.

We are going to establish recurrences for the values

$$a_k(t) = m_k(t) + m_k(t + 1),$$

$$b_k(t) = m_k(t) - m_k(t + 1),$$

and the corresponding generating functions

$$F_t(x) = \sum_{k \geq 0} a_k(t) x^k \quad \text{and} \quad G_t(x) = \sum_{k \geq 0} b_k(t) x^k.$$

By (2.11), we have

$$2a_k(2t) = 2m_k(t) + m_k(t) + m_k(t + 1) + \sum_{2 \leq \ell \leq k} \frac{1}{\ell!} a_{k-\ell}(t) + \sum_{1 \leq \ell \leq k} \frac{1}{\ell!} b_{k-\ell}(t)$$

$$= a_k(t) + \sum_{0 \leq \ell \leq k/2} \frac{1}{\ell!} a_{k-\ell}(t) + b_k(t) + \sum_{1 \leq \ell \leq k/2} \frac{1}{\ell!} b_{k-\ell}(t)$$

and

$$2b_k(2t) = 2m_k(t) - m_k(t) - m_k(t + 1) - \sum_{2 \leq \ell \leq k} \frac{1}{\ell!} a_{k-\ell}(t) - \sum_{1 \leq \ell \leq k} \frac{1}{\ell!} b_{k-\ell}(t)$$

$$= a_k(t) - \sum_{0 \leq \ell \leq k/2} \frac{1}{\ell!} a_{k-\ell}(t) + b_k(t) - \sum_{1 \leq \ell \leq k/2} \frac{1}{\ell!} b_{k-\ell}(t).$$

We want to write this as a matrix recurrence; we define

$$C(x) = \cosh(x) = \frac{1}{2} (e^x + e^{-x}) = \sum_{j \geq 0} \frac{x^{2j}}{(2j)!};$$

$$S(x) = \sinh(x) = \frac{1}{2} (e^x - e^{-x}) = \sum_{j \geq 0} \frac{x^{2j+1}}{(2j + 1)!};$$

We are concerned with the matrix

$$M_0 = \frac{1}{2} (A_0 + B_0),$$

where

$$A_0 = \begin{pmatrix} C(x) & S(x) \\ -C(x) & -S(x) \end{pmatrix} \quad \text{and} \quad B_0 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$
We also study appending 1 to the binary expansion.

\[
2a_k(2t + 1) = m_k(t) + m_k(t + 1) + 2m_k(t + 1) + \sum_{2 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}a_{k-\ell}(t) + \sum_{1 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}b_{k-\ell}(t)
\]

\[
= a_k(t) + \sum_{0 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}a_{k-\ell}(t) - b_k(t) + \sum_{1 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}b_{k-\ell}(t)
\]

and

\[
2b_k(2t + 1) = m_k(t) + m_k(t + 1) - 2m_k(t + 1) + \sum_{2 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}a_{k-\ell}(t) + \sum_{1 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}b_{k-\ell}(t)
\]

\[
= -a_k(t) + \sum_{0 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}a_{k-\ell}(t) + b_k(t) + \sum_{1 \leq \ell \leq k \atop \ell \neq 2k} \frac{1}{\ell!}b_{k-\ell}(t).
\]

Clearly, we are interested in the matrix

\[
M_1 = \frac{1}{2}(A_1 + B_1),
\]

where

\[
A_1 = \begin{pmatrix} C(x) & S(x) \\ C(x) & S(x) \end{pmatrix} \quad \text{and} \quad B_1 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.
\]

Using Cauchy products and the recurrence formula (2.11), we see that

\[
\begin{pmatrix} F_{2r}(x) \\ G_{2r}(x) \end{pmatrix} = M_0 \begin{pmatrix} F_r(x) \\ G_r(x) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} F_{2r+1}(x) \\ G_{2r+1}(x) \end{pmatrix} = M_1 \begin{pmatrix} F_r(x) \\ G_r(x) \end{pmatrix}.
\]

(2.15)

Note that these identities are also valid for \( t = 0 \) (since (2.11) is also valid for \( t = 0 \)).

2.3. Estimating the characteristic function using moments

For \( \vartheta \leq \vartheta_0 \), where \( \vartheta_0 \) is defined later, we will use a representation of \( \text{Im} \ \gamma_j(\vartheta) \) in terms of moments. For this, we use Taylor approximation of the sine function and (2.1): for all \( j \in \mathbb{Z} \) there exists \( \xi_j \) between 0 and \( 2\pi \vartheta \) such that

\[
\text{Im} \ \gamma_j(\vartheta) = \text{Im} \ \sum_{j \in \mathbb{Z}} \delta(j, t) e(j \vartheta) = \sum_{j \in \mathbb{Z}} \delta(j, t) \sin(2\pi j \vartheta)
\]

\[
= \sum_{j \in \mathbb{Z}} \delta(j, t) \sum_{0 \leq k < K} \frac{(-1)^k}{(2k + 1)!} (2\pi \vartheta)^{2k+1} j^{2k+1} + \sum_{j \in \mathbb{Z}} \delta(j, t) \frac{(-1)^K}{(2K + 1)!} j^{2K+1} \xi_j^{2K+1}
\]

and therefore

\[
|\text{Im} \ \gamma_j(\vartheta)| \leq \sum_{0 \leq k < K} (2\pi \vartheta)^{2k+1} |m_{2k+1}(t)| + \frac{(2\pi \vartheta)^{2K+1}}{(2K + 1)!} \sum_{j \in \mathbb{Z}} \delta(j, t) |j|^{2K+1}.
\]
Applying the Cauchy–Schwarz inequality to the sum
\[ \sum_{j \in \mathbb{Z}} \delta(j, t)|j|^{2K+1} = \sum_{j \in \mathbb{Z}} \sqrt{\delta(j, t)} |j|^K \sqrt{\delta(j, t)} |j|^{K+1}, \]
we obtain
\[ |\text{Im} \gamma_t(\theta)| \leq \sum_{0 \leq k < K} (2\pi \theta)^{2k+1} |m_{2k+1}(t)| \]
\[ + (2\pi \theta)^{2K+1} \frac{\sqrt{(2K)!(2K+2)!}}{(2K+1)!} m_{2K}(t)^{1/2} m_{2K+2}(t)^{1/2}. \]
(2.16)
The moments \(m_{2K}\) and \(m_{2K+2}\) will give us a factor \((K!(K+1)!)^{1/2} \geq K!\) in the denominator, which we will see later; this gain will enable us to prove that for all \(\varepsilon > 0\), we have \(c_t > 1/2 - \varepsilon\) for most \(t\) (the exceptional set depending on \(\varepsilon\)).

2.4. Upper bounds for the moments of \(\mu_t\)
We wish to study repeated application of the recurrence (2.11), corresponding to appending a block of 0s or 1s to the binary expansion of \(t\).

Using an elementary proof by induction, we obtain
\[ A_0^m = (C(x) - S(x))^{m-1} A_0 = e^{-(m-1)x} A_0 \]
and
\[ B_0^m = 2^{m-1} B_0 \]
for \(m \geq 1\). Moreover, \(B_0 A_0 = \left( \begin{array}{c} 0 \\ 0 \end{array} \right)\) and \(A_0 B_0 = (C(x) + S(x)) D_0 = e^x D_0\), where \(D_0 = \left( \begin{array}{cc} 1 & 1 \\ -1 & -1 \end{array} \right)\). Appending a block of 0s of length \(m\) corresponds to the matrix power \(M_0^m\).

Noting that \(A_0\) and \(B_0\) do not commute, we consider all ordered products of \(A_0\) and \(B_0\) of length \(m_0\); since \(B_0 A_0\) vanishes, we are only interested in the products \(A_0^{m_0-\ell} B_0^\ell\). This yields
\[ 2^{m_0} M_0^{m_0} = \sum_{0 \leq \ell \leq m_0} A_0^{m_0-\ell} B_0^\ell = e^{-(m_0-1)x} A_0 + 2^{m_0-1} B_0 + \sum_{1 \leq \ell \leq m_0-1} A_0^{m_0-\ell} B_0^\ell. \]

We have
\[ \sum_{1 \leq \ell \leq m_0-1} A_0^{m_0-\ell} B_0^\ell = \sum_{1 \leq \ell \leq m_0-1} e^{-(m_0-\ell-1)x} A_0 2^{\ell-1} B_0 = e^{(3-m_0)x} D_0 \sum_{0 \leq \ell \leq m_0-2} (2e^x)^\ell = e^x \frac{2^{m_0-1} - e^{(1-m_0)x}}{2 - e^{-x}} D_0, \]
which is also valid for \(m = 1\), and therefore
\[ 2M_0^{m_0} = \left( \frac{e^x}{2} \right)^{m_0-1} A_0 + B_0 + \frac{e^x}{2 - e^{-x}} \left( 1 - \left( \frac{e^x}{2} \right)^{m_0-1} \right) D_0. \]
(2.17)
Also, we study appending a block of 1s. By induction, we obtain
\[ A_1^m = (C(x) + S(x))^{m-1} A_1 = e^{(m-1)x} A_1 \]
and
\[ B_1^m = 2^{m-1} B_1 \]
for $m \geq 1$. Moreover, $B_1 A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $A_1 B_1 = \begin{pmatrix} C(x) - S(x) \end{pmatrix} D_1 = e^{-x} D_1$, where $D_1 = \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}$. Appending a block of $1$s of length $m$ corresponds to the matrix power $M_1^m$. Again, the matrices $A_1$ and $B_1$ do not commute, but $B_1 A_1$ vanishes. This yields

$$2^m M_1^m = \sum_{0 \leq \ell \leq m_1} A_1^{m_1-\ell} B_1^\ell = e^{(m_1-1)x} A_1 + 2^{m_1-1} B_1 + \sum_{1 \leq \ell \leq m_1-1} A_1^{m_1-\ell} B_1^\ell.$$ 

We have

$$\sum_{1 \leq \ell \leq m_1-1} A_1^{m_1-\ell} B_1^\ell = \sum_{1 \leq \ell \leq m_1-1} e^{(m_1-\ell-1)x} A_1 2^{\ell-1} B_1$$

$$= e^{(m_1-3)x} D_1 \sum_{0 \leq \ell \leq m_1-2} \left( \frac{2}{e^x} \right)^\ell = \frac{1}{e^x} \left[ \frac{2^{m_1-1} - e^{(m_1-1)x}}{2 - e^x} \right] D_1,$$

which is also valid for $m = 1$, and therefore

$$2 M_1^m = \left( \frac{e^x}{2} \right)^{m_1-1} A_1 + B_1 + \frac{e^{-x}}{2 - e^x} \left( 1 - \left( \frac{e^x}{2} \right)^{m_1-1} \right) D_1. \quad (2.18)$$

We are interested in the entries of these matrix powers; they are generating functions in the variable $x$, convergent in the whole of $\mathbb{C}$, and we consider their coefficients. First, we prove a statement on the low powers of $x$.

**Lemma 2.4.** Assume that $m \geq 1$. Let

$$M_0^m = \begin{pmatrix} a_0(x) & b_0(x) \\ c_0(x) & d_0(x) \end{pmatrix}.$$ 

Then as $x \to 0$,

$$a_0(x) = 1 + \frac{2^m - 1}{2^{m+1}} x^2 + O(x^3); \quad b_0(x) = \frac{2^m - 1}{2^m} + O(x);$$

$$c_0(x) = -\frac{2^m - 1}{2^{m+1}} x^2 + O(x^3); \quad d_0(x) = \frac{1}{2^m} + O(x). \quad (2.19)$$

Let

$$M_1^m = \begin{pmatrix} a_1(x) & b_1(x) \\ c_1(x) & d_1(x) \end{pmatrix}.$$ 

Then

$$a_1(x) = 1 + \frac{2^m - 1}{2^{m+1}} x^2 + O(x^3); \quad b_1(x) = -\frac{2^m - 1}{2^m} + O(x);$$

$$c_1(x) = \frac{2^m - 1}{2^{m+1}} x^2 + O(x^3); \quad d_1(x) = \frac{1}{2^m} + O(x). \quad (2.20)$$

**Proof.** The proof of this statement is easy, using (2.17) and (2.18), and the expansions of $(e^{\pm x})^m$, $e^{\pm x} (2 - e^{\mp x})$, $C(x)$, and $S(x)$. We leave the details of this straightforward calculation to the reader.
We also prove bounds for the error terms occurring in Lemma 2.4. That is, we need upper bounds for the coefficients \([x^s] a_i(x)\) and \([x^s] c_i(x)\) for \(s \geq 3\), and for the coefficients \([x^s] b_i(x)\) and \([x^s] d_i(x)\) for \(s \geq 1\).

**Lemma 2.5.** Let \(f \in \{a_0, b_0, c_0, d_0, a_1, b_1, c_1, d_1\}\). Then for \(k \geq 1\),

\[
[x^k] f(x) \leq \frac{2}{(\log 2)^k}.
\]

**Proof.** We first note that

\[
[x^k] (e^x / 2)^m = \frac{m^k}{2^m k!}.
\]

This function in \(m\) attains its maximum at \(m = k/\log 2\), yielding

\[
[x^k] (e^x / 2)^m \leq \left(\frac{k}{e}\right)^k \frac{1}{k! (\log 2)^k} \leq \frac{1}{\sqrt{2\pi} k (\log 2)^k},
\]

using Robbins [18]. Also, the third summands in (2·17) and (2·18) can be estimated by resorting to an asymptotic formula for the Fubini numbers (the coefficients of the exponential generating function for \(1/(2 - e^x)\)). Such an estimate follows easily from basic analytic combinatorics [13]: as \(k \to \infty\), we have

\[
[x^k] \frac{1}{2 - e^x} = \frac{1}{2(\log 2)^k} (1 + o(1)).
\]

Taking all singularities of \(1/(2 - e^x)\) into account, we obtain the exact formula [2]

\[
[x^k] \frac{1}{2 - e^x} = \frac{1}{2} \sum_{n=-\infty}^{\infty} (\log(2) + 2\pi i n)^{-k-1}, \tag{2·21}
\]

valid for \(k \geq 1\). The contribution of the terms \(|k| \geq 1\) can be estimated using an integral: for \(n \geq 1\) we have

\[
\sum_{k \geq 1} k^{-n-1} \leq 1 + \int_1^{\infty} x^{-n-1} dx = 1 + \frac{1}{n} \leq 2.
\]

Therefore

\[
[x^k] \frac{1}{2 - e^x} \leq \frac{1}{2(\log 2)^k + 1} + \frac{2}{(2\pi)^{k+1}} \leq \frac{1}{(\log 2)^k} \tag{2·22}
\]

for \(k \geq 1\), the outer estimate also being valid for \(k = 0\).

For the estimation of coefficients of \(M_i^n\), we are also interested in partial sums. We show the statements for \(M_i\). The case \(M_0\) can be obtained replacing \(\pm x\) by \(\mp x\), noting that for a generating function \(H(x)\), the generating functions \(H(x)\) and \(H(-x)\) differ only by the sign of their respective coefficients. We first show that \(k \mapsto [x^k] 1/(2 - e^x)\) is nondecreasing, using (2·21). Passing from \(k\) to \(k + 1\), the summand in (2·21) corresponding to \(n = 0\)
increases by a quantity bounded below by 0.6. The other terms, in total, change by less, as we show now. For an integer \( n \geq 1 \), we have
\[
\left| (\log 2 + 2\pi in)^{-k-2} - (\log 2 + 2\pi in)^{-k-1} \right| \leq \left| (\log 2 + 2\pi in)^{-k-1} \right| \frac{1}{(\log 2 + 2\pi in)^{-1} - 1} \leq 2 \cdot (6n)^{-k-1},
\]
and since \( \zeta(2) = \pi^2/6 \), it is clear that the total contribution of \( n \neq 0 \) is bounded above by 0.6. Also, we have \([x^1]1/(2 - e^x) = [x^0]1/(2 - e^x) = 1\), and therefore monotonicity for \( k \geq 0 \) follows.

Next, this monotonicity implies that \([x^k] e^{-x}/(2 - e^x)\) is nonnegative and bounded by \([x^k] 1/(2 - e^x)\): expanding the Cauchy product \( e^{-x} \cdot (2 - e^x)^{-1} \), we see that the coefficients are given by an alternating sum of nonincreasing values, which immediately implies the claim.

Using this nonnegativity property, and also the fact that \( e^x \) has nonnegative coefficients, we obtain
\[
\left| [x^k] \frac{e^{-x}}{2 - e^x} \left( 1 - \left( \frac{e^x}{2} \right)^{m_0-1} \right) \right| \leq [x^k] \frac{e^{-x}}{2 - e^x} \leq [x^k] 1 \leq \left( \frac{1}{2} \cdot e^x \right). 
\]
Moreover, since \( C \) has nonnegative coefficients bounded by the coefficients of \( e^x \), we have
\[
\left| [x^k] \left( e^x/2 \right)^{m_0-1} \right| \left( C(x) \right) \leq 2 [x^k] \left( e^x/2 \right)^{m_0} \leq \frac{2}{\sqrt{2\pi k}} \frac{1}{(\log 2)^k}. 
\]
The same is true for \( S \) in place of \( C \). It follows that the coefficients of the entries of \( M_0^n \) and \( M_1^n \) are bounded by
\[
\frac{1}{2} + \frac{1}{\sqrt{2\pi k(\log 2)^k}} + \frac{1}{2(\log 2)^k} \leq \frac{2}{(\log 2)^k}
\]
for \( k \geq 1 \). This finishes the proof of Lemma 2.5.

In particular, using (2.8), it follows from this proof that
\[
a_k(0) \leq (\log 2)^{-k} \quad \text{and} \quad |b_k(0)| \leq (\log 2)^{-k} \quad \text{for} \ k \geq 1.
\]

We are now prepared to prove upper bounds for the moments \( m_k(t) \).

**Proposition 2.6.** Set \( A_k = 2 \cdot (3/2)^{k-1}/k! \) for \( k \geq 1 \). There exist constants \( B_k, C_k, \) and \( E_k \) (for \( k \geq 1 \)) and \( D_k \) (for \( k \geq 2 \)) such that for all \( r \geq 1 \), and all \( t \geq 1 \) having \( r \) blocks we have:

\[
\begin{align*}
k = 0 & \quad |a_0(t)| = 2; \\
k = 1 & \quad |a_2(t)| \leq A_1 r + B_1; \\
& \quad |a_3(t)| \leq C_1 r; \\
& \quad |b_0(t)| = 0; \\
& \quad |b_2(t)| \leq 1; \\
& \quad |b_3(t)| \leq E_1;
\end{align*}
\]

\[
\begin{align*}
k = 2 & \quad |a_2k(t)| \leq A_k r^k + B_k r^{k-1}; \\
& \quad |a_{2k+1}(t)| \leq C_k r^k; \\
& \quad |b_{2k}(t)| \leq A_{k-1} r^{k-1} + D_k r^{k-2}; \\
& \quad |b_{2k+1}(t)| \leq E_k r^{k-1}.
\end{align*}
\]

**Proof.** We proceed by induction on \( k \), using Lemmas 2.4 and 2.5. Clearly, the statement is true for \( k = 0 \), since \( m_0(t) = 1 \) and \( m_1(t) = 0 \) for all \( t \geq 0 \).
In the induction step, we will make use of the following identities, valid for $k \geq 2$: we have

\begin{align}
    a_2(2^m t) &= a_2(t) + \frac{2^m - 1}{2} a_2(t) + \frac{2^m - 1}{2} b_2(t); \\
    b_2(2^m t) &= -\frac{2^m - 1}{2} a_2(t) + \frac{1}{2} b_2(t); \\
    a_2(2^m t + 2^m - 1) &= a_2(t) + \frac{2^m - 1}{2^m} - \frac{2^m - 1}{2} b_2(t); \\
    b_2(2^m t + 2^m - 1) &= \frac{2^m - 1}{2^m} + \frac{1}{2} b_2(t).
\end{align}

We begin with the treatment of the even moments. The first step is to verify the following identities for the case $k = 1$:

\begin{align}
    a_2(2^m t) &= a_2(t) + \frac{2^m - 1}{2^m} a_2(t) + \frac{2^m - 1}{2^m} b_2(t); \\
    b_2(2^m t) &= -\frac{2^m - 1}{2^m} a_2(t) + \frac{1}{2^m} b_2(t); \\
    a_2(2^m t + 2^m - 1) &= a_2(t) + \frac{2^m - 1}{2^m} - \frac{2^m - 1}{2^m} b_2(t); \\
    b_2(2^m t + 2^m - 1) &= \frac{2^m - 1}{2^m} + \frac{1}{2^m} b_2(t).
\end{align}

Proof of (2.24) and (2.25). We begin with the first and third lines of (2.24) and (2.25). By (2.15) we have

\begin{align}
    \left( \begin{array}{c} F_t(x) \\ G_t(x) \end{array} \right) = M_i^m \left( \begin{array}{c} F_i(x) \\ G_i(x) \end{array} \right),
\end{align}

where $i \in \{0, 1\}$. Using Lemma 2.4 and expanding Cauchy products, we obtain

\begin{align}
    a_{2k}(t') = a_{2k}(t) + \frac{2^m - 1}{2^m} a_{2k-2}(t) + \sum_{3 \leq \ell \leq 2k} a_{2k-\ell}(t) \left[ x^\ell \right] a_0(x) \\
    \pm \frac{2^m - 1}{2^m} b_{2k}(t) + \sum_{1 \leq \ell \leq 2k} b_{2k-\ell}(t) \left[ x^\ell \right] b_0(x).
\end{align}

Here, the “+”-part corresponds to appending a block of 0s and the “−”-part to appending a block of 1s. Clearly, for $k = 1$ we have

\[ \sum_{3 \leq \ell \leq 2k} a_{2k-\ell}(t) \left[ x^\ell \right] a_0(x) = \sum_{1 \leq \ell \leq 2k} b_{2k-\ell}(t) \left[ x^\ell \right] b_0(x) = 0, \]

which implies the statements concerning $a_2$ in (2.24).
Inserting the estimates for the coefficients of $M_i^m$ (Lemma 2.5) and the induction hypothesis, we obtain for $k \geq 2$, using $a_0(t) = 2$,

$$
S_1 := \sum_{3 \leq \ell \leq 2k} a_{2k-\ell}(t) \left[ x^\ell \right] a_0(x) \leq \sum_{4 \leq \ell \leq 2k} a_{2k-\ell}(t) \frac{2}{(\log 2)^\ell} + \sum_{3 \leq \ell \leq 2k-1} a_{2k-\ell}(t) \frac{2}{(\log 2)^\ell}
$$

$$
\leq 4(\log 2)^{-2k} + \sum_{2 \leq j < k} (A_{k-j} r^{k-j} + B_{k-j} r^{k-j-1}) \frac{2}{(\log 2)^{2j}} + \sum_{2 \leq j < k} C_{k-j} \frac{2r^{k-j}}{(\log 2)^{2j-1}}.
$$

The sums are identically zero if $r = 0$ or $k < 3$; for the other cases, we note that for all integers $m \geq 1$,

$$
\sum_{0 \leq j < m} (\log 2)^{-2j} = \frac{(\log 2)^{-2m} - 1}{(\log 2)^{-2} - 1} \leq (\log 2)^{-2m}
$$

(2.27)

since the appearing denominator is greater than 1. Therefore

$$
\sum_{2 \leq j < k} A_{k-j} \frac{r^{k-j}}{(\log 2)^{2j}} \leq \max_{1 \leq j \leq k-2} A_j \frac{r^{k-2}}{(\log 2)^{2j}} \sum_{0 \leq \ell \leq k-2} \frac{1}{(\log 2)^{2\ell}} \leq \frac{r^{k-2}}{(\log 2)^{2k}} \max_{1 \leq j \leq k-2} A_j,
$$

which is also valid for $A$ replaced by $B$ resp. $C$. We obtain for $k \geq 2$

$$
S_1 \leq d_1^{(1)}(k) r^{k-2},
$$

where

$$
d_1^{(1)}(k) = 2(\log 2)^{-2k} \left( 2 + \max_{1 \leq j \leq k-2} A_j + \max_{1 \leq j \leq k-2} B_j + \max_{1 \leq j \leq k-2} C_j \right).
$$

Here and in the following the maximum over the empty index set is defined as 0.

In an analogous fashion, we treat the second sum in (2.26), which is nonzero only if $k \geq 2$. We use the hypothesis $|b_2(t)| \leq 1$, and obtain for $k \geq 2$

$$
S_2 := \sum_{1 \leq \ell \leq 2k} b_{2k-\ell}(t) \left[ x^\ell \right] b_0(x) \leq \sum_{2 \leq \ell \leq 2k} b_{2k-\ell}(t) \frac{2}{(\log 2)^\ell} + \sum_{1 \leq \ell \leq 2k-1} b_{2k-\ell}(t) \frac{2}{(\log 2)^\ell}
$$

$$
\leq \sum_{1 \leq j \leq k-2} (A_{k-j-1} r^{k-j-1} + D_{k-j} r^{k-j-2}) \frac{2}{(\log 2)^{2j}} + 2(\log 2)^{-2k+2}
$$

$$
+ \sum_{1 \leq j \leq k-1} E_{k-j} r^{k-j-1} \frac{2}{(\log 2)^{2j-1}}.
$$

Similarly to the treatment of $S_1$, using (2.27), we have for $k \geq 2$

$$
S_2 \leq d_1^{(2)}(k) r^{k-2},
$$

where

$$
d_1^{(2)}(k) = 2(\log 2)^{-2k} \left( 1 + \max_{1 \leq j \leq k-2} A_j + \max_{2 \leq j \leq k-1} D_j + \max_{1 \leq j \leq k-1} E_j \right).
$$
A lower bound for Cusick’s conjecture

This implies the statements for $a_{2k}$ in (2.25). We proceed to $b_{2k}$ and obtain

$$b_{2k}(t') = \pm \frac{2^m - 1}{2^{m+1}} a_{2k-2}(t) + \sum_{3 \leq \ell \leq 2k} a_{2k-\ell}(t) \left[x^{\ell}\right] c_0(x)$$

$$+ \frac{1}{2^m} b_{2k}(t) + \sum_{1 \leq \ell \leq 2k} b_{2k-\ell}(t) \left[x^{\ell}\right] d_0(x).$$

Again, for $k = 1$, the sums vanish, and we obtain the second and fourth lines of (2.24).

For $k \geq 2$, the two sums occurring in (2.28) can be estimated by $d_1^{(1)}(k)r^{k-2}$ and $d_2^{(2)}(k)r^{k-2}$ respectively. This follows by replacing $a$ by $c$ and $b$ by $d$ and recycling the argument from above. This implies lines two and four of (2.25).

It follows that $d_1(k) = d_1^{(1)}(k) + d_1^{(2)}(k)$ is an admissible constant for all of the four formulas in (2.25).

Deriving bounds for the even moments. We apply the eight equations in (2.24) and (2.25) successively in order to obtain the “even part” of the statement, that is, the estimates for $a_{2k}(t)$ and $b_{2k}(t)$.

We begin with $b_{2}$ and show $|b_2(t)| \leq 1$ by induction: we have $b_2(0) = m_2(0) - m_2(1) = -1$, and by (2.24) we obtain

$$|b_2(t')| \leq \frac{2^m - 1}{2^m} + \frac{1}{2^m} \leq 1$$

for both $t' = 2^m t$ and $t' = 2^m t + 2^m - 1$. Moreover, $a_2(0) = 1$ and

$$a_2(t') = a_2(t) + \frac{2^m - 1}{2^m} \pm \frac{2^m - 1}{2^m} b_2(t) \leq a_2(t) + 2,$$

which implies $a_2(t) \leq 2r + 1$ for all $t \geq 0$ having $r$ blocks. We therefore set $A_1 = 2$ and $B_1 = 1$. Clearly $|a_2(t)| \leq A_1 r^1 + B_1 r^0$, and the estimates for $a_2$ and $b_2$ in the proposition are proved.

We assume now that $k \geq 2$ and we consider $b_{2k}$: we have

$$|b_{2k}(t')| \leq \left| \frac{2^m - 1}{2^{m+1}} a_{2k-2}(t) + \frac{1}{2^m} b_{2k} \right| + d_1(k)r^{k-2} \leq \frac{|b_{2k}(t)| + a_{2k-2}(t)}{2} + d_1(k)r^{k-2},$$

where $t'$ results from $t$ by appending 0s (if $t$ is odd) or by appending 1s (if $t$ is even).

Here $r$ is the number of blocks in $t$. By iteration, exploiting the denominator 2 (geometric series!), and by applying the induction hypothesis and

$$|b_{2k}(0)| \leq \frac{1}{(\log 2)^{2k}},$$

we obtain

$$|b_{2k}(t)| \leq A_{k-1} r^{k-1} + B_{k-1} r^{k-2} + 2d_1(k)r^{k-2} + \frac{1}{(\log 2)^{2k}}$$

if $t$ has $r$ blocks. We therefore set $D_k = B_{k-1} + 2d_1(k) + (\log 2)^{-2k}$ and this case is completed. We proceed to the case $a_{2k}$, where $k \geq 2$: each time we append a block of 0s or 1s to $t$, we add at most
Deriving bounds for the odd moments. which proves the part of the induction statement concerning the even moments.

Noting that products, we obtain

\[ k \text{ proceed similarly. Suppose that } a \]

This follows from (2.25) and line three of the induction statement. We wish to successively append a block of 0s or 1s; this corresponds to summing this inequality in \( r \). For \( \ell \geq 1 \) and \( N \geq 0 \) we have

\[
\sum_{1 \leq n < N} n^{\ell-1} \leq \int_1^N n^{\ell-1} \, dn \leq \frac{N^{\ell}}{\ell}.
\]

Noting that \( a_{2k}(0) = m_{2k}(1) \leq (\log 2)^{-2k} \) for \( k \geq 1 \) by (2.23), we obtain therefore

\[ a_{2k}(t) \leq A_k r^k + B_k r^{k-1} \]

with

\[
A_k = \frac{3}{2k} A_{k-1} \quad \text{and} \quad B_k = \frac{1}{k-1} \left( B_{k-1} + D_k + d_1(k) \right) + \frac{1}{(\log 2)^{2k}} \]

\[ = \frac{1}{k-1} \left( 2B_{k-1} + 3d_1(k) \right) + \frac{2}{(\log 2)^{2k}}, \tag{2.29} \]

which proves the part of the induction statement concerning the even moments.

\emph{Deriving bounds for the odd moments.} For the odd case, concerning \( a_{2k+1} \) and \( b_{2k+1} \), we proceed similarly. Suppose that \( k \geq 1 \). Using (2.15), Lemma 2.4 and expanding Cauchy products, we obtain

\[
a_{2k+1}(t') = a_{2k+1}(t) + \sum_{2 \leq \ell \leq 2k+1} a_{2k+1-\ell}(t) \left[ x^\ell \right] a_0(x)
\]

\[
\pm \frac{2^m}{2^m} b_{2k+1}(t) + \sum_{1 \leq \ell \leq 2k+1} b_{2k+1-\ell}(t) \left[ x^\ell \right] b_0(x),
\]

where “+” corresponds to appending a block of 0s. By Lemma 2.5 and the induction hypothesis, using \( a_1(t) = 0 \) and \( a_0(t) = 2 \), we have for \( k \geq 1 \)

\[
\sum_{2 \leq \ell \leq 2k+1} a_{2k+1-\ell}(t) \left[ x^\ell \right] a_0(x) \leq \sum_{2 \leq \ell \leq 2k} a_{2k+1-\ell}(t) \frac{2}{(\log 2)^{\ell}} + \sum_{3 \leq \ell \leq 2k+1} a_{2k+1-\ell}(t) \frac{2}{(\log 2)^{\ell}}
\]

\[
\leq \sum_{1 \leq j < k} C_{k-j} r^{k-j} \frac{2}{(\log 2)^{2j}} + \sum_{1 \leq j < k} \left( A_{k-j} r^{k-j} + B_{k-j} r^{k-j-1} \right) \frac{2}{(\log 2)^{2j+1}}
\]

\[
+ \frac{4}{(\log 2)^{2k+1}} \leq d_2^{(1)}(k) r^{k-1}.
\]
This estimate is valid for $k \geq 1$. Therefore
\begin{equation}
\tag{2.30}
\alpha_{2k+1}(t') = \alpha_{2k+1}(t) + \frac{2}{2^m} b_{2k+1}(t) + O_1(d_2(k)r^{k-1}),
\end{equation}
where $r$ is the number of blocks in $t$ and $d_2(k) = d_2^{(1)}(k) + d_2^{(2)}(k)$, and where we use the symbol $O_1$ to indicate that the implied constant is bounded by 1.

Concerning $b_{2k+1}$, we obtain from Lemma 2.4
\begin{equation}
\tag{2.31}
b_{2k+1}(t') = \sum_{2 \leq \ell \leq 2k+1} \alpha_{2k+1-\ell}(t) \left[ \frac{1}{2^m} b_{2k+1}(t) + \sum_{1 \leq \ell \leq 2k+1} b_{2k+1-\ell}(t) \left[ x^\ell \right] \right] \circ_0(x),
\end{equation}
and therefore by the above argument (replacing $a$ and $b$ by $c$ and $\circ$ respectively)
\begin{equation}
\tag{2.31}
b_{2k+1}(t') = \frac{1}{2^m} b_{2k+1}(t) + O_1(d_2(k)r^{k-1}).
\end{equation}

By repeated application of this identity, using (2.23), we obtain
\begin{equation}
|b_{2k+1}(t)| \leq \frac{1}{2} |b_{2k+1}(t)| + 2d_2(k)r^{k-1} \leq E_k r^{k-1}
\end{equation}
for all $t$, where $E_k = 2d_2(k) + (\log 2)^{-2k-1}$ for $k \geq 1$. Inserting this into (2.30), we obtain
\begin{equation}
|\alpha_{2k+1}(t')| \leq |\alpha_{2k+1}(t)| + \left( 3d_2(k) + (\log 2)^{-2k-1} \right) r^{k-1}
\end{equation}
and therefore by summation, using (2.23) again,
\begin{equation}
\tag{2.23}
\alpha_{2k+1}(t) \leq C_k r^k,
\end{equation}
where $C_k = 3d_2(k)/k + 2(\log 2)^{-2k-1}$. This is valid for all $k \geq 1$. The proof is complete.
Summarising, the recurrence for the quantities $A_j$ through $E_j$, used in the proof, is as follows:

$$
\begin{array}{ll}
  k = 1 & A_1 = 2; \\
  k \geq 2 & A_k = 3A_{k-1}/(2k); \\
  & B_1 = 0; \\
  & B_k = (2B_{k-1} + 3d_1(k))/(k - 1) + 2(\log 2)^{-2k}; \\
  & C_1 = 3d_2(1); \\
  & C_k = 3d_2(k)/k + 2(\log 2)^{-2k-1}; \\
  & D_k = B_{k-1} + 2d_1(k) + (\log 2)^{-2k}; \\
  & E_1 = 2d_2(1); \\
  & E_k = 2d_2(k) + (\log 2)^{-2k-1},
\end{array}
$$

where

\[
d_1(k) = \frac{2}{(\log 2)^{2k}} \left( 3 + 2 \max_{1 \leq j \leq k-2} A_j + \max_{1 \leq j \leq k-2} B_j \right. \\
+ \left. \max_{1 \leq j \leq k-2} C_j + \max_{2 \leq j \leq k-1} D_j + \max_{1 \leq j \leq k-1} E_j \right)
\]

for $k \geq 2$ and

\[
d_2(k) = \frac{2}{(\log 2)^{2k+1}} \left( 3 + 2 \max_{1 \leq j \leq k-1} A_j + \max_{1 \leq j \leq k-1} B_j \right. \\
+ \left. \max_{1 \leq j \leq k-1} C_j + \max_{2 \leq j \leq k} D_j + \max_{1 \leq j \leq k-1} E_j \right)
\]

for $k \geq 1$. Using this recurrence, it is easy to compute explicit bounds for the values $A_j$ through $E_j$, in particular, choosing $\varepsilon < 1/4$, this leads to an effective bound $r_0$ such that $c_\varepsilon > 1/4$ as soon as $t$ has at least $r_0$ blocks. However, we do not believe that these numerical values are particularly enlightening (and fairly large). We therefore limit ourselves to a short summary: for $k = 1$, we see that $d_2(1) = 6(\log 2)^{-4}$, from which we obtain $C_1$ and $E_1$. In the step $k - 1 \rightarrow k$, we have to compute $d_1(k)$ first; then $B_k$ and $D_k$ can be obtained, and $d_2(k)$ as the next step (note that for the maximum $\max_{2 \leq j \leq k} D_j$ we need $D_k$). Finally, $C_k$ and $E_k$ can be computed.

2.5. Bounding the characteristic function using a matrix product

The correlations $\gamma_t(\vartheta)$ satisfy the following recurrence (see Bèsineau [5]): for all $t \geq 0$,

$$
\gamma_0(\vartheta) = 1, \quad \gamma_{2t}(\vartheta) = \gamma_t(\vartheta), \quad \gamma_{2t+1}(\vartheta) = \frac{e(\vartheta)}{2} \gamma_t(\vartheta) + \frac{e(-\vartheta)}{2} \gamma_{t+1}(\vartheta).
$$

In order to capture this using a matrix product, we define

$$
A(0) = \begin{pmatrix} 1 & 0 \\ e(\vartheta)/2 & e(-\vartheta)/2 \end{pmatrix}, \quad A(1) = \begin{pmatrix} e(\vartheta)/2 & e(-\vartheta)/2 \\ 0 & 1 \end{pmatrix}.
$$

In [16] we used the representation

$$
\gamma_t(\vartheta) = \begin{pmatrix} 1 & 0 \end{pmatrix} A(\varepsilon_0) \cdots A(\varepsilon_t) \begin{pmatrix} 1 \\ u \end{pmatrix},
$$

where $t = (\varepsilon_0 \ldots \varepsilon_t)$ and $u = \gamma_1(\vartheta) = e(\vartheta)/(2 - e(-\vartheta))$. 

https://doi.org/10.1017/503050041210000153 Published online by Cambridge University Press
A lower bound for Cusick’s conjecture

Using this matrix identity, we proved [20, Lemma 2] an upper bound for \( \gamma_t(\vartheta) \) depending on the number \( r \) of blocks of 1s occurring in \( t \). By a slight variation (we handled the values \( \omega_t(\vartheta) = \gamma_t(\vartheta)/u \), where \( u \) is bounded by 1 in absolute value) we obtain the following statement.

**Lemma 2.7.** Assume that \( t \geq 1 \) contains at least \( 4M + 1 \) blocks. Then

\[
|\gamma_t(\vartheta)| \leq \left(1 - \frac{1}{2}\|\vartheta\|^2\right)^M.
\]

2.6. **Splitting the integral**

We are interested in bounding the integral

\[
\int_{0}^{1/2} \text{Im} \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta
\]

by \( \varepsilon \). (Note that the integrand is an even function and therefore the integrals over \([0, 1/2]\) and \([1/2, 1]\) yield the same value.) We split the integration at the point \( \vartheta_0 = r^{-1/2}R \), where the integer \( R \) is chosen in a moment and \( r \) is the number of blocks in \( t \).

We begin with the estimation of the right part of the integral. Let \( M \) be maximal such that \( 4M + 1 \leq r \). Then by Lemma 2.7, we have

\[
|\gamma_t(\vartheta)| \leq \left(1 - \frac{1}{2}\|\vartheta\|^2\right)^M \leq \exp\left(-\frac{M}{2}\|\vartheta\|^2\right).
\]

We have \( (r - 4)/4 \leq M \leq (r - 1)/4 \) (because \( (r - 5)/4 \geq M \) is impossible due to the maximality of \( M \), therefore \( 4M + 5 > r \), which implies \( 4M + 4 \geq r \)). Also, for \( 0 \leq x \leq \pi/2 \), we have the elementary inequality

\[
cot x \leq 1/x. \tag{2.32}
\]

We obtain

\[
\int_{\vartheta_0}^{1/2} \text{Im} \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta \leq \int_{\vartheta_0}^{1/2} \frac{1}{\vartheta} \exp\left(-\frac{M}{2}\|\vartheta\|^2\right) \, d\vartheta
\]

\[
\leq \sum_{m=R}^{\infty} \int_{mr^{-1/2}}^{(m+1)r^{-1/2}} \frac{1}{\vartheta} \exp\left(-\frac{M}{2}\vartheta^2\right) \, d\vartheta \leq r^{-1/2} \sum_{m=R}^{\infty} \frac{1}{mr^{-1/2}} \exp\left(-\frac{M}{2}m^2/r\right)
\]

\[
\leq \sum_{m=R}^{\infty} \frac{1}{m} \exp\left(-\frac{m^2}{8}\left(1 - \frac{4}{r}\right)\right) \leq \sum_{m=R}^{\infty} \frac{1}{m} \exp\left(-\frac{m^2}{16}\right).
\]

This is valid for \( r \geq 8 \). Since \( \exp(-m^2/16) = O(1/m) \) for \( m \to \infty \), this infinite sum is bounded by \( c/R \) for some absolute (effective) constant \( c \). We therefore choose the integer \( R = R(\varepsilon) \) large enough such that \( c/R \leq \varepsilon/3 \), and we obtain

\[
\int_{\vartheta_0}^{1/2} \text{Im} \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta \leq \frac{\varepsilon}{3}. \tag{2.33}
\]

The left part of the integral will be estimated using upper bounds for the odd moments, which is Proposition 2.6.

https://doi.org/10.1017/S0305004121000153 Published online by Cambridge University Press
From the estimate of $a_{2k+1}(t)$ and $b_{2k+1}$ in Proposition 2.6 we get by the triangle inequality

$$|m_{2k+1}(t)| \leq E'_k r^k$$

for some constant $E'_k$ only depending on $k$. Moreover, from the estimate for $a_{2k}(t)$ we obtain by nonnegativity of the even moments

$$m_{2k}(t) \leq A_k r^K + B_{k-1} r^{K-1}$$

and

$$m_{2k+2}(t) \leq A_{k+1} r^{K+1} + B_K r^K.$$ 

For $r$ greater than some $r_0(K)$ we therefore have

$$m_{2k}(t) \leq 2A_k r^K \text{ and } m_{2k+2}(t) \leq 2A_{k+1} r^{K+1} \quad \text{(2.34)}$$

for all $t$ having at least $r$ blocks. Let $K$ be large enough so that

$$L_K = 2\sqrt{(2K)! (2K + 2)! A_k A_{k+1} (2\pi)^{2K+1}} \leq \frac{\varepsilon/3}{R^{2K+1}}.$$ 

(2.35)

Note that for this inequality, we use the factor $k!$ in the denominator of $A_k$ in an essential way! By (2.16) and (2.34) we obtain for $r \geq r_0(K)$

$$|\text{Im } \gamma_t(\vartheta)| \leq \sum_{0 \leq k < K} (2\pi \vartheta)^{2k+1} E'_k r^k + L_K \vartheta^{2K+1} r^{K+1/2}.$$ 

Using (2.32), we obtain for $\vartheta \geq \vartheta_0$

$$|\text{Im } \gamma_t(\vartheta) \cot(\pi \vartheta)| \leq \sum_{0 \leq k < K} (2\pi)^{2k+1} E'_k \vartheta_0^{2k} r^k + L_K \vartheta_0^{2K} r^{K+1/2}$$

$$= \sum_{0 \leq k < K} (2\pi)^{2k+1} E'_k R^{2k} + L_K R^{2K} r^{1/2}.$$ 

Integrating from 0 to $\vartheta_0$ yields for $r \geq r_0(K)$

$$\int_0^{\vartheta_0} \text{Im } \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta \leq r^{-1/2} \sum_{0 \leq k < K} (2\pi R)^{2k+1} E'_k + L_K R^{2K+1}.$$ 

The second summand is bounded by $\varepsilon/3$, using (2.35). The sum over $k$ does not depend on $r$. For $r \geq r_1(K)$, we therefore have

$$\int_0^{\vartheta_0} \text{Im } \gamma_t(\vartheta) \cot(\pi \vartheta) \, d\vartheta \leq \frac{2\varepsilon}{3}$$

and the theorem is proved.

**Remark 2.8.** We plan to prove more detailed estimates for the moments $m_k$ in the future. For example, it is known [10] that $m_{2k}(t)$ is usually of size $r^k/(2^k k!)$, where $r$ is the number of blocks in $t$ (we skip the precise formulation of the property proved in [10]). We wish to sharpen this estimate, and consequently prove a **lower bound** for the values $\delta(0, t) = \int_0^1 \text{Re } \gamma_t(\vartheta) \, d\vartheta$ for $T - \mathcal{O}(T^{1-\varepsilon})$ many $t < T$. Using (2.3), and also improving the estimates of the odd moments, we hope to obtain $c_t > 1/2$ for these $t$ in this way, thus significantly improving the error term in the result [8] by Drmota, Kauers and the author.
Acknowledgements. The author is thankful to Johannes F. Morgenbesser, who introduced him to Cusick’s conjecture, on one of the author’s first days as a PhD student in Vienna, in 2011. Moreover, we wish to thank Dmitry Badziahin, Michael Drmota, Jordan Emme, Wolfgang Steiner and Thomas Stoll for fruitful discussions on the topic. Finally, we thank Thomas Cusick for constant encouragement and interest in our work.

REFERENCES
[1] J.-P. Allouche and J. Shallit. The ring of $k$-regular sequences. Theoret. Comput. Sci. 98 (1992), 163–197.
[2] R. W. Bailey. The number of weak orderings of a finite set. Soc. Choice Welf. 15 (1998), 559–562.
[3] J. Beck. Probabilistic Diophantine approximation (Springer Monographs in Mathematics, Springer, Cham, 2014).
[4] R. Béjian and H. Faure. Discrépance de la suite de Van der Corput. Séminaire Delange-Pisot–Poitou. 19e année: 1977/78, Théorie des nombres, Fasc. 1, Secrétariat Math. (Paris, 1978), Exp. No. 13.
[5] J. Bésineau. Indépendance statistique d’ensembles liés à la fonction “somme des chiffres”. Acta Arith. 20 (1972), 401–416.
[6] T. W. Cusick, Y. Li, and P. Stănică. On a combinatorial conjecture. Integers 11 (2011).
[7] G. Deng and P. Yuan. On a combinatorial conjecture of Tu and Deng. Integers 12 (2012).
[8] M. Drmota, M. Kauers, and L. Spiegelhofer. On a conjecture of Cusick concerning the sum of digits of $n$ and $n + t$. SIAM J. Discrete Math. 30 (2016), 621–649.
[9] M. Drmota, G. Larcher, and F. Pillichshammer. Precise distribution properties of the van der Corput sequence and related sequences. Manuscripta Math. 118 (2005), 11–41.
[10] J. Emme and P. Hubert. Central limit theorem for probability measures defined by sum-of-digits function in Base 2. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) 19 (2019), 757–780.
[11] J. Emme and P. Hubert. Normal distribution of correlation measures of binary sum-of-digits functions. Preprint (2018), http://arxiv.org/abs/1810.11234.
[12] J. Emme and A. Prikhod’ko. On the asymptotic behavior of density of sets defined by sum-of-digits function in base 2. Integers 17 (2017).
[13] P. Flajolet and R. Sedgewick. Analytic Combinatorics. (Cambridge University Press, Cambridge, 2009).
[14] J.-P. Flori. Fonctions booléennes, courbes algébriques et multiplication complexe. Doctoral thesis, Télécom ParisTech (2012).
[15] J.-P. Flori, H. Randriambololona, G. Cohen and S. Mesnager. On a conjecture about binary strings distribution. In Sequences and Their Applications - SETA 2010 Springer Berlin/Heidelberg (Ed.), (2010), 346–358.
[16] J. F. Morgenbesser and L. Spiegelhofer. A reverse order property of correlation measures of the sum-of-digits function. Integers 12 (2012).
[17] P. D. Proinov and E. Y. Atanassov. On the distribution of the van der Corput generalised sequences. C. R. Acad. Sci. Paris Sér. I Math. 307 (1988), 895–900.
[18] H. Robbins. A remark on Stirling’s formula. Amer. Math. Monthly 62 (1955), 26–29.
[19] L. Spiegelhofer. Discrepancy results for the van der Corput sequence. Unif. Distrib. Theory 13 (2018), 57–69.
[20] L. Spiegelhofer. Approaching Cusick’s conjecture on the sum-of-digits function. Integers 19 (2019).
[21] L. Spiegelhofer and M. Wallner. The Tu–Deng conjecture holds almost surely. Electron. J. Comb. 26 (2019)
[22] Z. Tu and Y. Deng. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Des. Codes Cryptogr. 60 (2011), 1–14.
[23] Z. Tu and Y. Deng. Boolean functions optimizing most of the cryptographic criteria. Discrete Appl. Math. 160 (2012), 427–435.

https://doi.org/10.1017/S0305004121000153 Published online by Cambridge University Press
