The Tu–Deng Conjecture holds almost surely

Lukas Spiegelhofer

Institut für Diskrete Mathematik und Geometrie
Technische Universität Wien
Wiedner Hauptstrasse 8–10, 1040 Wien, Austria.

lukas.spiegelhofer@tuwien.ac.at

Michael Wallner

Laboratoire Bordelais de Recherche en Informatique
Université de Bordeaux
351 Cours de la Libération, 33405 Talence, France

michael.wallner@tuwien.ac.at

Submitted: Jul 25, 2017; Accepted: Nov 9, 2018; Published: Feb 22, 2019

© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

The Tu–Deng Conjecture is concerned with the sum of digits $w(n)$ of n in base 2 (the Hamming weight of the binary expansion of n) and states the following: assume that k is a positive integer and $t \in \{1, \ldots, 2^k - 2\}$. Then

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

We prove that the Tu–Deng Conjecture holds almost surely in the following sense: the proportion of $t \in \{1, \ldots, 2^k - 2\}$ such that the above inequality holds approaches 1 as $k \to \infty$.

Moreover, we prove that the Tu–Deng Conjecture implies a conjecture due to T. W. Cusick concerning the sum of digits of n and $n + t$.

Mathematics Subject Classifications: Primary: 11A63, 68R05, 11T71; Secondary: 05A20, 05A16

1 Introduction and results

Z. Tu and Y. Deng's Conjecture [16] is concerned with the Hamming weight $w(n)$ of the binary expansion of a nonnegative integer n (the sum of digits of n in base two) and addition modulo $2^k - 1$. This conjecture is as follows.

Key words and phrases. Tu–Deng Conjecture, Hamming weight, sum of digits, Cusick conjecture.

Conjecture 1. TD Assume that k is a positive integer and $t \in \{1, \dots, 2^k - 2\}$. Define

$$S_{t,k} = \Big\{(a, b) \in \big\{0, \dots, 2^k - 2\big\}^2 : a + b \equiv t \bmod 2^k - 1, w(a) + w(b) < k\Big\}.$$

Then $P_{t,k} := |S_{t,k}|/2^k \leqslant 1/2$.

The conjecture arose in the construction of Boolean functions with optimal algebraic immunity (see Tu and Deng [16, 17]). Indeed, if the conjecture is true, the functions defined by Tu and Deng have this property.

Such functions are used in the construction of stream ciphers, which are widely used encryption methods due to their high speed and low hardware requirements [3]. However, they are prone to serious attacks [1, 4, 5]. In order to prevent them from these known attacks algebraic immunity was introduced [11]. We refer the reader to the above-cited papers by Tu and Deng for a more extensive discussion of the rôle of their conjecture within the cryptographic context.

So far the conjecture could only be solved for some special cases:

- Cusick, Li and Stănică [6] identified six different classes for which it holds using three different counting strategies. These are $t = 2^i$, $t = 2^j + 2^i$; $t = 2^k - 2^i$, $t = 2^k - 2^j - 2^i$; $t = 2^k - 2^j - 2^i - 1$, and $t = 2^k - 2^l - 2^j - 2^i - 1$. They also proposed an equivalent conjecture.

- Flori, Randriambololona, Cohen and Mesnager [10] reformulate the problem in terms of carries and, among other things, prove that it is true for certain values of t such that the blocks of 1s and/or 0s are long enough. Moreover, they prove convergence of $P_{t,k}$ to 1/2 for certain families of values of t.

- Deng and Yuan [7] show that it is true for special binary block structures of t, like for example $t = 10^{s_1}10^{s_2}\dots1^{s_r}$ such that $s_i + s_j \geqslant r - 2$. This includes the cases $w(t) \leqslant 6$.

- Qarboua, Schreck and Fontaine [12] deduced another family of integers t with a special mirror-symmetry for which the conjecture holds using the previous two results.

- Moreover, it was checked using a computer algorithms for all $k \leqslant 29$ by Tu and Deng [16] and for $k \leqslant 40$ by Flori [9, Section 2.9.3] who distributed his computations on about 400 cores.

Let us give a probabilistic (and combinatorial) interpretation of the conjecture. Let $S_k := \bigcup_{t=1}^{2^k-2} S_{t,k}$. Let us consider an arbitrary pair (a, b) of S_k. On the one hand, the number of 1s in the binary expansion of a (and b) is at most $k-1$. On the other hand, the constraint on the Hamming weights implies that the total number of 1s in both integers is less than k. Finally, note that all such pairs except $(0, 0)$ are part of S_k. Therefore, considering how we may (or actually may not) distribute 1s on the $2k$ digits in base 2 of a and b together we get

$$|S_k| = 2^{2k} - \sum_{i=k}^{2k} \binom{2k}{i} - 1 = \frac{1}{2}\left(2^{2k} - \binom{2k}{k}\right) - 1. \tag{1}$$

The sequence including $(0,0)$, i.e., the sequence for $|S_k|+1$ is `A000346` in Sloane's OEIS[1].

It is then easy to compute the asymptotic expansion of this sequence as

$$|S_k| = \frac{2^{2k}}{2}\left(1 - \frac{1}{\sqrt{\pi k}} + \mathcal{O}\left(\frac{1}{k^{3/2}}\right)\right). \tag{2}$$

As there are $2^k - 2$ possible choices for t we see by the pigeonhole principle that at least one of the sets $S_{t,k}$ has to be asymptotically of size $2^k/2$. Therefore, the Tu–Deng Conjecture describes a uniform distribution among the possible sets $S_{t,k}$.

While working on the Tu–Deng Conjecture, T. W. Cusick (private communication, 2011, 2015) formulated a related conjecture on the Hamming weight:

Conjecture 2. C Assume that t is a nonnegative integer. Then

$$c_t \coloneqq \operatorname{dens}\{n \in \mathbb{N} : w(n+t) \geqslant w(n)\} > \frac{1}{2},$$

where $\operatorname{dens} A$ denotes the asymptotic density of a set $A \subseteq \mathbb{N}$ (which exists in this case).

Also, note that the density in Conjecture 2 exists, which follows, for example, from the "Lemma of Bésineau" [2, Lemme 1], see also [8, Lemma 2.1]. In fact, we have

$$c_t = \frac{1}{2^k}\left|\{n < 2^k : w(n+t) \geqslant w(n)\}\right| \tag{3}$$

for $k \geqslant \alpha + \mu$, where $\alpha = w(t) + 1$ and $2^\mu \leqslant t < 2^{\mu+1}$ [8, equation (10) and Section 3.3]. We also studied [8] a statement complementary to Cusick's Conjecture:

Conjecture 3. CC Assume that t is a nonnegative integer. Then

$$\tilde{c}_t \coloneqq \operatorname{dens}\{n \in \mathbb{N} : w(n+t) > w(n)\} \leqslant \frac{1}{2}.$$

Analogously to the case c_t, we have

$$\tilde{c}_t = \frac{1}{2^{k-1}}\left|\{n < 2^{k-1} : w(n+t) > w(n)\}\right|. \tag{4}$$

for k large enough. Taken together, Conjectures 2 and 3 locate quite precisely the median of the random variable X_t on $\mathbb{Z}$ defined by

$$j \mapsto \operatorname{dens}\{n : w(n+t) - w(n) = j\}.$$

Numerical experiments reveal that $\tilde{c}_t \leqslant 1/2 < c_t$ for all $t < 2^{30}$. In fact, Drmota, Kauers, and the first author [8] proved that Conjectures 2 and 3 are satisfied for almost all t in the sense of asymptotic density. In the present paper, we want to show that an analogous result holds for Conjecture 1.

[1] http://oeis.org

Theorem 4. *Define $P_{t,k}$ as before,*

$$P_{t,k} = \frac{1}{2^k} \left| \left\{ (a,b) \in \left\{0, \ldots, 2^k - 2\right\}^2 : a + b \equiv t \bmod 2^k - 1, w(a) + w(b) < k \right\} \right| .$$

For each $\varepsilon > 0$, we have for $k \to \infty$

$$\left| \left\{ t \in \{1, \ldots, 2^k - 2\} : P_{t,k} \not\in (1/2 - \varepsilon, 1/2) \right\} \right| = \mathcal{O}\left(\frac{2^k}{k} \right) .$$

In particular,

$$\lim_{k \to \infty} \frac{1}{2^k} \left| \left\{ t \in \{1, \ldots, 2^k - 2\} : 1/2 - \varepsilon < P_{t,k} < 1/2 \right\} \right| = 1.$$

Moreover, we will prove that Conjectures 2 and 3 are in fact implied by Conjecture 1.

Proposition 5. *Conjecture 1 implies Conjectures 2 and 3.*

In fact, we will see that Conjectures 2 and 3 are contained as “extremal cases” in Conjecture 1, choosing t and letting $k \to \infty$.

However, so far we did not succeed in proving the opposite implication. Meanwhile, due to the similarity of the conjectures, it is reasonable to expect that a proof of Conjecture 2, when one is found (and if it is found first), will lead to a proof of Conjecture 1. We wish to highlight this similarity between the conjectures.

Proposition 6. *For integers $k \geqslant 1$ and a, b we define*

$$a \oplus_k b = (a + b) \bmod (2^k - 1).$$

Conjecture 1 is equivalent to the statement that

$$|\{n \in \{0, \ldots, 2^k - 1\} : w(n \oplus_k t) \geqslant w(n)\}| \geqslant 2^{k-1} \tag{5}$$

for all $k \geqslant 1$ and $t \in \{1, \ldots, 2^k - 2\}$. Conjecture 2 is equivalent to the statement that

$$|\{n \in \{0, \ldots, 2^k - 1\} : w(n + t) \geqslant w(n)\}| > 2^{k-1} \tag{6}$$

for all $k, t \geqslant 1$.

The binary operation $\oplus_k$ can also be seen as “circular addition” in base 2: if a carry occurs at the index $k - 1$ in the addition $a + b$, this carry does not propagate into position k, but into the lowest bit instead. Moreover, if $a + b = 2^k - 1$, the result is set to zero.

By Proposition 6, we may summarize the content of Conjectures 1 and 2 by the following elementary question: how does the sum of digits change under (modular) addition of a constant? It is this formulation in particular that makes the Tu–Deng Conjecture a mathematically interesting problem.

Remark 7. We do not have an analogous formulation of Conjecture 3 as in Proposition 6: if we define

$$A_{t,k} = 2^{-k} \lvert \{ n \in \{0, \ldots, 2^k - 1\} : w(n+t) > w(n) \} \rvert,$$

then $A_{3,0} = 1 > 1/2$ and $A_{3,3} = 3/8 < 1/2$, while indeed $\tilde{c}_t = 3/8 < 1/2$.

The idea of the proof of Theorem 4 is to show a concentration result using Chebyshev's inequality. More precisely, we consider the moments

$$\frac{1}{2^k} \sum_{0 \leqslant t < 2^k} |S_{t,k}| \quad \text{and} \quad \frac{1}{2^k} \sum_{0 \leqslant t < 2^k} |S_{t,k}|^2$$

and derive asymptotic expansions for them. (Note that $|S_{0,k}| = 1$ and $|S_{2^k-1,k}| = 1$, so that the cases $t \in \{0, 2^k - 1\}$ will not matter asymptotically.) These expansions are then used to prove that the values $P_{t,k}$ concentrate well below $1/2$, as $k \to \infty$. This idea of proof is analogous to the method used by Drmota, Kauers, and the first author [8]. In fact, the trivariate rational generating function we are going to encounter is very similar to the one in that paper.

The remaining part of this paper is dedicated to the proofs of Theorem 4 and Propositions 5 and 6.

2 Proof of Proposition 5

We first rewrite the Tu–Deng Conjecture. Let us split the set $S_{t,k}$ according to whether $a + b < 2^k - 1$: set

$$\begin{aligned} S_{t,k}^{(1)} &= \bigl\{ a \in \{0, \ldots, t\} : w(a) + w(t-a) < k \bigr\}, \\ S_{t,k}^{(2)} &= \bigl\{ a \in \bigl\{t+1, \ldots, 2^k - 2\bigr\} : w(a) + w\bigl(2^k - 1 + t - a\bigr) < k \bigr\}. \end{aligned}$$

Note that the sets $M_{t,k}^{(1)} = \{(a, t-a) : a \in S_{t,k}^{(1)}\}$ and $M_{t,k}^{(2)} = \{(a, 2^k - 1 + t - a) : a \in S_{t,k}^{(2)}\}$ form a partition of $S_{t,k}$. We define the quantity

$$\beta_{t,k,j} = \bigl\lvert \bigl\{ a \in \bigl\{0, \ldots, t\bigr\} : w\bigl(a + 2^k - 1 - t\bigr) - w(a) = j \bigr\rvert,$$

where $k \geqslant 1$, $0 \leqslant t < 2^k$ and j are integers. By the identity $w\bigl(2^k - 1 - t\bigr) = k - w(t)$ we have

$$S_{t,k}^{(1)} = \bigl\{ a \in \{0, \ldots, t\} : w(a) < w\bigl(a + 2^k - 1 - t\bigr) \bigr\}$$

and

$$\begin{aligned} S_{t,k}^{(2)} &= \bigl\{ a \in \bigl\{t+1, \ldots, 2^k - 2\bigr\} : w(a) < w(a-t) \bigr\} \\ &= \bigl\{ a \in \bigl\{0, \ldots, 2^k - 2 - (t+1)\bigr\} : w\bigl(2^k - 1 - (a+1)\bigr) < w\bigl(2^k - 1 - (a+t+1)\bigr) \bigr\} \\ &= \bigl\{ a \in \bigl\{1, \ldots, 2^k - 2 - t\bigr\} : w(a) > w(a+t) \bigr\}. \end{aligned}$$

Since $w(0) \not> w(0+t)$ and $w\bigl(2^k-1-t\bigr) \not> w\bigl(2^k-1\bigr)$, we obtain

$$\begin{aligned} |S_{t,k}| &= \bigl|S_{t,k}^{(1)}\bigr| + \bigl|S_{t,k}^{(2)}\bigr| \\ &= \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(a+2^k-1-t\bigr) > w(a)\bigr\}\bigr| \\ &\quad + \bigl|\bigl\{a \in \{0,\ldots,2^k-1-t\} : w(a) > w(a+t)\bigr\}\bigr| \\ &= \sum_{j \geqslant 1} \Bigl(\beta_{t,k,j} + \beta_{2^k-1-t,k,-j}\Bigr). \end{aligned} \tag{7}$$

Both Conjecture 2 and Conjecture 3 are trivial if $t=0$. Let $t \geqslant 1$ be given and assume that $k' \geqslant 1$ is such that $t < 2^{k'}-1$; we choose $k \geqslant 2k'$. With this choice we have $w(a) \leqslant w\bigl(a+2^k-1-t\bigr)$ as long as $0 \leqslant a \leqslant t$. This is the case since $2^k - 2^{k'} + 1 \leqslant a + 2^k - 1 - t \leqslant 2^k - 1$, therefore the tail of 1s at the left of the binary expansion of 2^k-1-t, having length at least k', is not touched by the addition of a. Therefore $\bigl|S_{t,k}^{(1)}\bigr| = t+1$ for large k. Assuming that Conjecture 1 holds, we obtain

$$\begin{aligned} 2^{k-1} &\geqslant t+1+\bigl|\bigl\{a \in \{0,\ldots,2^k-1-t\} : w(a) > w(a+t)\bigr\}\bigr| \\ &> \bigl|\bigl\{a \in \{0,\ldots,2^k-1\} : w(a) > w(a+t)\bigr\}\bigr| \end{aligned}$$

This last expression equals $2^k\bigl(1-c_t\bigr)$ if k is chosen large enough (see (3)), which implies $c_t > 1/2$. To derive Conjecture 3, we replace t in the Tu–Deng Conjecture by 2^k-1-t. Noting that $\sum_{j\in\mathbb{Z}} \beta_{t,k,j} = t+1$, we obtain

$$\begin{aligned} 2^{k-1} \geqslant |S_{2^k-1-t,k}| &= \sum_{j \geqslant 1} \bigl(\beta_{2^k-1-t,k,j} + \beta_{t,k,-j}\bigr) \\ &= \bigl|\{a \in \{0,\ldots,2^k-1-t\} : w(a+t)-w(a) > 0\}\bigr| + \mathcal{O}(t) \\ &= \bigl|\{a \in \{0,\ldots,2^k-1\} : w(a+t)-w(a) > 0\}\bigr| + \mathcal{O}(t). \end{aligned}$$

Letting $k \to \infty$ and using (4) we obtain $\tilde{c}_t \leqslant 1/2$.

Remark 8. The quantities $\beta_{t,k,j}$ are linked to divisibility by powers of two in Pascal's triangle: We define (see e.g. [14])

$$\vartheta(j,n) = \left|\left\{k \in \{0,\ldots,n\} : \nu_2\binom{n}{k} = j\right\}\right|.$$

(Here $\nu_2(m)$ denotes the largest j such that 2^j divides m.) Then for $k \geqslant 1$, $0 \leqslant t < 2^k$ and $j \geqslant 0$ we have the identity

$$\beta_{t,k,k-w(t)-j} = \vartheta(j,t).$$

Proof. By the identity $\nu_2(n!) = n - w(n)$ we have $\nu_2\binom{n}{k} = w(k) + w(n-k) - w(n)$ for $0 \leqslant k \leqslant n$. By the substitution $a \mapsto t-a$ and the formula $w\bigl(2^k-1-m\bigr) = k - w(m)$, valid for $m < 2^k$, we obtain

$$\begin{aligned} \beta_{t,k,k-w(t)-j} &= \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(2^k-1-t+a\bigr) - w(a) = k-w(t)-j\bigr\}\bigr| \\ &= \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(2^k-1-t+(t-a)\bigr) - w(t-a) = k-w(t)-j\bigr\}\bigr| \\ &= \bigl|\bigl\{a \in \{0,\ldots,t\} : w(a)+w(t-a)-w(t) = j\bigr\}\bigr| \\ &= \vartheta(j,t). \end{aligned}$$

□

3 Proof of Proposition 6

In what follows, we will use the notation $t_k^{\mathrm{c}} = 2^k - 1 - t$. We will assume that $0 \leqslant t < 2^k$; then the binary expansion of t_k^{c} is the Boolean complement of the binary expansion of t, padded with 1s up to the index $k-1$.

Using the identity $w(2^k - 1 - t) = k - w(t)$ (see also the proof of Proposition 5 from the previous section), we see that

$$\begin{aligned}|S_{t,k}| = {} & |\{a \in \{0,\ldots,t\} : w(a) < w(a + t_k^{\mathrm{c}})\}| \\ & + |\{a \in \{t+1,\ldots,2^k-2\} : w(a) < w(a + t_k^{\mathrm{c}} - 2^k + 1)\}|.\end{aligned}$$

We wish to replace addition by $\oplus_k$. To do so, we note that $w(t) < w(t + t_k^{\mathrm{c}})$, but $w(t) \not< w(t \oplus_k t_k^{\mathrm{c}})$. It follows that

$$|S_{t,k}| = 1 + |\{a \in \{0,\ldots,2^k-2\} : w(a) < w(a \oplus_k t_k^{\mathrm{c}})\}|,$$

the correction term 1 being due to the aforementioned inequalities at $a = t$.

For all $t \in \{1,\ldots,2^k-2\}$ and $a \in \{0,\ldots,2^k-2\}$ we have the identity $(a \oplus_k t) \oplus_k t_k^{\mathrm{c}} = a$, therefore

$$\begin{aligned}|S_{t,k}| &= 1 + |\{a \in \{0,\ldots,2^k-2\} : w(a \oplus_k t) < w(a)\}| \\ &= |\{a \in \{0,\ldots,2^k-1\} : w(a \oplus_k t) < w(a)\}|,\end{aligned}$$

where we used $w((2^k-1) \oplus_k t) < w(2^k-1)$. From this the first equivalence follows.

We proceed to the proof of the second statement. Define

$$C_{t,k} = 2^{-k}\bigl|\{n \in \{0,\ldots,2^k-1\} : w(n+t) \geqslant w(n)\}\bigr|.$$

By (3), we have $C_{t,k} = c_t$ for $k \geqslant k_0$. We prove that it is sufficient to show that the values $C_{t,k}$ are nonincreasing in k: assume that we have this monotonicity and $c_t > 1/2$. Then for k_0 large enough, $C_{t,k} \geqslant C_{t,k_0} = c_t > 1/2$ for $k \leqslant k_0$, moreover the same holds if $k > k_0$ by the equality $C_{t,k} = c_t$; on the other hand, if $C_{t,k} > 1/2$ for all $k \geqslant 1$, then $c_t = C_{t,k} > 1/2$ for some k. (Note that this monotonicity does not hold for Tu–Deng; otherwise we would have a proof of the implication 2⇒1.) We proceed by induction on t and show the more general statement that the values $v_{t,k,j} = 2^{-k}\bigl|\{n \in \{0,\ldots,2^k-1\} : w(n+t) - w(n) \geqslant j\}\bigr|$ are nonincreasing in k, for each $j \in \mathbb{Z}$.

We first prove the statement for $t = 1$, using the identity $w(n+1) - w(n) = 1 - \nu_2(n+1)$. Here $\nu_2(a)$ is the 2-valuation of $a \geqslant 1$, that is, the largest k such that $2^k \mid a$. By this identity we have $v_{1,k,j} = 0$ for $j \geqslant 2$. Moreover, $\nu_2(n+1) \geqslant \ell$ if and only if the lowest ℓ digits of n are 1. Therefore we obtain

$$|\{n \in \{0,\ldots,2^k-1\} : \nu_2(n+1) \geqslant \ell\}| = \begin{cases} 0, & k < \ell; \\ 2^{k-\ell}, & k \geqslant \ell \end{cases}$$

for all $\ell \geqslant 0$, and the statement follows.

In the following, we write $d(n,t) = w(n+t) - w(n)$ for brevity. Assume that the statement holds for t; we wish to prove it for $2t$ and $2t+1$ in place of t. We have $d(2n,2t) = d(2n+1,2t) = d(n,t)$, therefore $v_{2t,0,j} = v_{2t,1,j}$ for all j. Moreover, for $k \geqslant 0$ we get

$$\begin{aligned}\bigl|\{n \in \{0,\ldots,2^{k+1}-1\} : d(n,2t) \geqslant j\}\bigr| &= \bigl|\{2n : n \in \{0,\ldots,2^k-1\}, d(2n,2t) \geqslant j\}\bigr| \\ &\quad + \bigl|\{2n+1 : n \in \{0,\ldots,2^k-1\}, d(2n+1,2t) \geqslant j\}\bigr| \\ &= 2\bigl|\{n \in \{0,\ldots,2^k-1\}, d(n,t) \geqslant j\}\bigr|,\end{aligned}$$

therefore $v_{2t,k+1,j} = v_{t,k,j} \leqslant v_{t,k-1,j} = v_{2t,k,j}$ for $k \geqslant 1$.

It remains to treat the case $2t+1$. We have $d(0,2t+1) = w(2t+1) - w(0) = w(t)+1$ and $d(1,2t+1) = w(2t+2) - w(1) = w(t+1) - 1$, which implies $v_{2t+1,0,j} \geqslant v_{2t+1,1,j}$ by the inequality $w(n+1) \leqslant w(n)+1$.

Moreover, we have $d(2n,2t+1) = d(n,t)+1$ and $d(2n+1,2t+1) = d(n,t+1)-1$, therefore we have for all $k \geqslant 0$

$$\begin{aligned}&\bigl|\{n \in \{0,\ldots,2^{k+1}-1\} : d(n,2t+1) \geqslant j\}\bigr| \\ &\quad = \bigl|\{2n : n \in \{0,\ldots,2^k-1\}, d(2n,2t+1) \geqslant j\}\bigr| \\ &\qquad + \bigl|\{2n+1 : n \in \{0,\ldots,2^k-1\}, d(2n+1,2t+1) \geqslant j\}\bigr| \\ &\quad = \bigl|\{2n : n \in \{0,\ldots,2^k-1\}, d(n,t) \geqslant j-1\}\bigr| \\ &\qquad + \bigl|\{2n+1 : n \in \{0,\ldots,2^k-1\}, d(n,t+1) \geqslant j+1\}\bigr|.\end{aligned}$$

It follows that $v_{2t+1,k+1,j} = \frac{1}{2}v_{t,k,j-1} + \frac{1}{2}v_{t+1,k,j+1} \leqslant \frac{1}{2}v_{t,k-1,j-1} + \frac{1}{2}v_{t+1,k-1,j+1} = v_{2t+1,k,j}$ for $k \geqslant 1$.

4 Proof of Theorem 4

Let us define the values

$$\gamma_{t,k,j} = \beta_{t,k,j} + \beta_{t^{\mathrm{c}}_k,k,-j}.$$

and

$$\Gamma_{t,k,j} = \sum_{i \geqslant j} \gamma_{t,k,i}.$$

By equation (7) the Tu–Deng Conjecture states that $P_{t,k} = \Gamma_{t,k,1}/2^k \leqslant 1/2$.

Our strategy is to show that the standard deviation of the random variable $t \mapsto \Gamma_{t,k,1}$ is much smaller than the distance to 2^{k-1}, such that the values $P_{t,k}$ concentrate below $1/2$ by Chebyshev's inequality. We are therefore interested in the mean value and the variance of $t \mapsto \Gamma_{t,k,1}$ on the intervals $[0,2^k)$. First, we want to find a recurrence for the values

$$\beta_{t,k,j} = \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(a+t^{\mathrm{c}}_k\bigr) - w(a) = j\bigr\}\bigr|,$$

where $k \geqslant 1$, $0 \leqslant t < 2^k$ and $j \in \mathbb{Z}$. For convenience, we set $\beta_{-1,j,k} = 0$.

Proposition 9. *Let $k \geqslant 0$ and j be integers. Then*

$$\begin{aligned}
\beta_{0,k,j} &= \delta_{k,j}, \\
\beta_{0_k^{\mathrm{c}},k,j} &= 2^k \delta_{j,0}, \\
\beta_{2t,k+1,j} &= \beta_{t,k,j-1} + \beta_{t-1,k,j+1} && \textit{for } 0 \leqslant t < 2^k, \\
\beta_{2t+1,k+1,j} &= 2\beta_{t,k,j} && \textit{for } 0 \leqslant t < 2^k, \\
\beta_{(2t)_{k+1}^{\mathrm{c}},k+1,j} &= 2\beta_{t_k^{\mathrm{c}},k,j} && \textit{for } 0 \leqslant t < 2^k, \\
\beta_{(2t+1)_{k+1}^{\mathrm{c}},k+1,j} &= \beta_{t_k^{\mathrm{c}},k,j-1} + \beta_{(t+1)_k^{\mathrm{c}},k,j+1} && \textit{for } 0 \leqslant t < 2^k.
\end{aligned}$$

Furthermore, we have $\beta_{t,k,j} = 0$ for $|j| > k$.

Proof. The last claim $\beta_{t,k,j} = 0$ for $|j| > k$ follows by induction. The first two statements and the cases $t = 0$ are clear. We note the almost trivial identities $(2t)_{k+1}^{\mathrm{c}} = 2t_k^{\mathrm{c}} + 1$, $(2t+1)_{k+1}^{\mathrm{c}} = 2t_k^{\mathrm{c}}$ and $(t+1)_k^{\mathrm{c}} = t_k^{\mathrm{c}} - 1$, which hold for all t and k. We calculate for $1 \leqslant t < 2^k$:

$$\begin{aligned}
\beta_{2t,k+1,j} &= \bigl|\bigl\{a \in \{0,\ldots,2t\} : w\bigl(a + (2t)_{k+1}^{\mathrm{c}}\bigr) - w(a) = j\bigr| \\
&= \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(2a + 2t_k^{\mathrm{c}} + 1\bigr) - w(2a) = j\bigr| \\
&\quad + \bigl|\bigl\{a \in \{0,\ldots,t-1\} : w\bigl(2a + 2t_k^{\mathrm{c}} + 2\bigr) - w(2a+1) = j\bigr| \\
&= \beta_{t,k,j-1} + \bigl|\bigl\{a \in \{0,\ldots,t-1\} : w\bigl(a + (t-1)_k^{\mathrm{c}}\bigr) - w(a) = j+1\bigr| \\
&= \beta_{t,k,j-1} + \beta_{t-1,k,j+1}.
\end{aligned}$$

The statement also holds for $t = 0$, using $\beta_{-1,k,j} = 0$. Moreover, for $0 \leqslant t < 2^k$ we have

$$\begin{aligned}
\beta_{2t+1,k+1,j} &= \bigl|\bigl\{a \in \{0,\ldots,2t+1\} : w\bigl(a + (2t+1)_{k+1}^{\mathrm{c}}\bigr) - w(a) = j\bigr| \\
&= \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(2a + 2t_k^{\mathrm{c}}\bigr) - w(2a) = j\bigr| \\
&\quad + \bigl|\bigl\{a \in \{0,\ldots,t\} : w\bigl(2a + 2t_k^{\mathrm{c}} + 1\bigr) - w(2a+1) = j\bigr| \\
&= 2\beta_{t,k,j}
\end{aligned}$$

and

$$\begin{aligned}
\beta_{(2t)_{k+1}^{\mathrm{c}},k+1,j} &= \bigl|\bigl\{a \in \{0,\ldots,2t_k^{\mathrm{c}}+1\} : w(a+2t) - w(a) = j\bigr\}\bigr| \\
&= \bigl|\bigl\{a \in \{0,\ldots,t_k^{\mathrm{c}}\} : w(2a+2t) - w(2a) = j\bigr\}\bigr| \\
&\quad + \bigl|\bigl\{a \in \{0,\ldots,t_k^{\mathrm{c}}\} : w(2a+2t+1) - w(2a+1) = j\bigr\}\bigr| \\
&= 2\beta_{t_k^{\mathrm{c}},k,j}.
\end{aligned}$$

Finally, for $0 \leqslant t < 2^k - 1$ we have

$$\begin{aligned}
\beta_{(2t+1)_k^{\mathrm{c}},k+1,j} &= \bigl|\bigl\{a \in \{0,\ldots,2t_k^{\mathrm{c}}\} : w(a+2t+1) - w(a) = j\bigr\}\bigr| \\
&= \bigl|\bigl\{a \in \{0,\ldots,t_k^{\mathrm{c}}\} : w(2a+2t+1) - w(2a) = j\bigr\}\bigr| \\
&\quad + \bigl|\bigl\{a \in \{0,\ldots,t_k^{\mathrm{c}}-1\} : w(2a+2t+2) - w(2a+1) = j\bigr\}\bigr|
\end{aligned}$$

$$\begin{aligned}&= \beta_{t_k^{\mathrm{c}},k,j-1} + \left|\left\{a \in \{0,\dots,(t+1)_k^{\mathrm{c}}\} : w(a+t+1) - w(a) = j+1\right\}\right| \\ &= \beta_{t_k^{\mathrm{c}},k,j-1} + \beta_{(t+1)_k^{\mathrm{c}},k,j+1}\end{aligned}$$

and the last statement also holds for $t = 2^k - 1$. □

We want to compute the first moments of the values $\beta_{t,k,j}$. Define

$$m_{k,j} = \sum_{t=0}^{2^k-1} \beta_{t,k,j}.$$

Clearly, we have

$$m_{0,j} = \delta_{0,j}.$$

Using the above recurrence, we obtain for $k \geqslant 1$

$$\begin{aligned} m_{k,j} &= \sum_{t=0}^{2^{k-1}-1} \beta_{2t,k,j} + \sum_{t=0}^{2^{k-1}-1} \beta_{2t+1,k,j} \\ &= \sum_{t=0}^{2^{k-1}-1} \left(\beta_{t,k-1,j-1} + \beta_{t-1,k-1,j+1}\right) + 2\sum_{t=0}^{2^{k-1}-1} \beta_{t,k-1,j} \\ &= \sum_{t=0}^{2^{k-1}-1} \beta_{t,k-1,j-1} + \sum_{t=0}^{2^{k-1}-2} \beta_{t,k-1,j+1} + 2m_{k-1,j} \\ &= m_{k-1,j-1} + 2m_{k-1,j} + m_{k-1,j+1} - \beta_{2^{k-1}-1,k-1,j+1} \\ &= m_{k-1,j-1} + 2m_{k-1,j} + m_{k-1,j+1} - 2^{k-1}\delta_{j,-1} \end{aligned}$$

We define the bivariate generating function F:

$$F(x,y) = \sum_{\substack{k\geqslant 0\\ \ell\geqslant 0}} m_{k,k-\ell} x^k y^\ell.$$

Since $\beta_{t,k,j} = 0$ for $j > k$ and $0 \leqslant t < 2^k$ (which can be proved by induction) this function captures all interesting values. Moreover, we have $\beta_{t,k,j} = 0$ for $j \leqslant -k+1$.

Using the recurrence for $m_{k,j}$, we obtain

$$\begin{aligned} F(x,y) &= \sum_{\ell\geqslant 0} m_{0,-\ell} y^\ell + \sum_{\substack{k\geqslant 1\\ \ell\geqslant 0}} m_{k,k-\ell} x^k y^\ell \\ &= 1 + \sum_{\substack{k\geqslant 1\\ \ell\geqslant 0}} x^k y^\ell \left(m_{k-1,k-1-\ell} + 2m_{k-1,k-\ell} + m_{k-1,k+1-\ell} - 2^{k-1}\delta_{k-\ell,-1} \right) \\ &= 1 + xF(x,y) + 2\sum_{k\geqslant 1} x^k m_{k-1,k} + 2xyF(x,y) + \sum_{\substack{k\geqslant 1\\ 0\leqslant \ell\leqslant 1}} x^k y^\ell m_{k-1,k+1-\ell} \end{aligned}$$

$$
\begin{aligned}
&+ xy^2F(x,y) - \sum_{k\geqslant 1} 2^{k-1}x^k y^{k+1}\\
&= 1 + x(1+y)^2F(x,y) - \frac{xy^2}{1-2xy},
\end{aligned}
$$

therefore

$$F(x,y) = \frac{1-2xy-xy^2}{(1-2xy)\big(1-x(1+y)^2\big)}$$

Moreover, we define

$$\widetilde{m}_{k,j} := \sum_{t=0}^{2^k-1} \beta_{t_k^{\mathrm{c}},k,-j} = m_{k,-j}$$

and

$$\widetilde{F}(x,y) := \sum_{\substack{k\geqslant 0\\ \ell\geqslant 0}} \widetilde{m}_{k,k-\ell}x^k y^\ell.$$

As above, we calculate for $k \geqslant 1$:

$$
\begin{aligned}
\widetilde{m}_{k,j} &= \sum_{t=0}^{2^{k-1}-1} \beta_{(2t)_k^{\mathrm{c}},k,-j} + \sum_{t=0}^{2^{k-1}-1} \beta_{(2t+1)_k^{\mathrm{c}},k,-j}\\
&= 2\sum_{t=0}^{2^{k-1}-1} \beta_{t_{k-1}^{\mathrm{c}},k-1,-j} + \beta_{(2^k-1)_k^{\mathrm{c}},k,-j} + \sum_{t=0}^{2^{k-1}-2} \beta_{t_{k-1}^{\mathrm{c}},k-1,-j-1}\\
&\quad + \sum_{t=0}^{2^{k-1}-2} \beta_{(t+1)_{k-1}^{\mathrm{c}},k-1,-j+1}\\
&= 2\widetilde{m}_{k-1,j} + \widetilde{m}_{k-1,j-1} + \widetilde{m}_{k-1,j+1}\\
&\quad - \beta_{(2^{k-1}-1)_{k-1}^{\mathrm{c}},k-1,-j-1} - \beta_{0_{k-1}^{\mathrm{c}},k-1,-j+1} + \delta_{k,-j}\\
&= \widetilde{m}_{k-1,j-1} + 2\widetilde{m}_{k-1,j} + \widetilde{m}_{k-1,j+1} - 2^{k-1}\delta_{j,1}
\end{aligned}
$$

Therefore

$$
\begin{aligned}
\widetilde{F}(x,y) &= \sum_{\ell\geqslant 0} \widetilde{m}_{0,-\ell}y^\ell + \sum_{\substack{\ell\geqslant 0\\ k\geqslant 1}} x^k y^\ell \Big(\widetilde{m}_{k-1,k-\ell-1} + 2\widetilde{m}_{k-1,k-\ell} + \widetilde{m}_{k-1,k-\ell+1} - 2^{k-1}\delta_{k-\ell,1}\Big)\\
&= 1 + x\widetilde{F}(x,y) + 2\sum_{k\geqslant 0} x^{k+1}\widetilde{m}_{k,k+1} + 2xy\widetilde{F}(x,y) + \sum_{\substack{k\geqslant 0\\ 0\leqslant \ell\leqslant 1}} x^{k+1}y^\ell \widetilde{m}_{k,k+2-\ell}\\
&\quad + xy^2\widetilde{F}(x,y) - \sum_{k\geqslant 0} 2^{k-1}x^{k+1}y^k\\
&= 1 + x(1+y)^2\widetilde{F}(x,y) - \frac{x}{1-2xy}
\end{aligned}
$$

and we get

$$\widetilde{F}(x,y) = \frac{1-2xy-x}{(1-2xy)\bigl(1-x(1+y)^2\bigr)}.$$

The first moments of the random variable $t \mapsto \beta_{t,k,j}$, where $t \in \{0,\dots,2^k-1\}$ are contained in certain *diagonals* of the bivariate rational function $F(x,y)$ (to be precise, the diagonal contains the values $m_{k,j}$, which are first moments multiplied by 2^k). The moments corresponding to $j=0$ are contained in the main diagonal.

We define

$$M_{k,l} = \sum_{t=0}^{2^k-1} \Gamma_{t,k,k-\ell}$$

and are interested in $M_{k,k-1}$.

We have

$$\begin{aligned} M_{k,\ell} &= \sum_{i \geqslant k-\ell} \sum_{t=0}^{2^k-1} \bigl(\beta_{t,k,i} + \beta_{t_k^c,k,-i}\bigr) = \sum_{i \geqslant k-\ell} \bigl(m_{k,i} + \widetilde{m}_{k,i}\bigr) \\ &= \sum_{j=0}^{\ell} \bigl(m_{k,k-j} + \widetilde{m}_{k,k-j}\bigr) = \sum_{j=0}^{\ell} \bigl[x^k y^j\bigr] \bigl(F(x,y) + \widetilde{F}(x,y)\bigr) \\ &= \bigl[x^k y^\ell\bigr] G(x,y), \end{aligned}$$

where

$$G(x,y) = \frac{2-4xy-x-xy^2}{(1-y)(1-2xy)\bigl(1-x(1+y)^2\bigr)}.$$

The first moment of $t \mapsto 2^k\Gamma_{t,k,1}$ is therefore given by $M_{k,k-1} = \bigl[x^k y^{k-1}\bigr]G(x,y)$. Extracting this diagonal, we rediscover the result given in the introduction.

Recall from the introduction $S_k = \bigcup_{t=1}^{2^k-2} S_{t,k}$. Now, we have that $M_{k,k-1} = |S_k| + 1$, as we changed the range of t to $\{0,1,\dots,2^k-1\}$. In the introduction we presented a simple combinatorial argument proving the following result, compare (1) and (2). However, we decided to also keep this longer proof for two reasons: on the one hand, we have captured the first moments of all $\Gamma_{t,k,k-\ell}$ in one generating function, which better shows the underlying structure; on the other hand, this proof is a gentle introduction to the method used for the second moment later.

Proposition 10. *We have for $k \geqslant 1$*

$$\begin{aligned} M_{k,k-1} &= \frac{1}{2}\left(4^k - \binom{2k}{k}\right) \\ &= \frac{4^k}{2}\left(1 - \frac{1}{\sqrt{\pi k}} + \frac{1}{8\sqrt{\pi k^3}} - \frac{1}{128\sqrt{\pi k^5}} + \mathcal{O}\left(\frac{1}{\sqrt{k^7}}\right)\right). \end{aligned}$$

Proof. The idea of the proof is to extract the (shifted) diagonal of $G(x,y)$. First note that $[x^ky^{k-1}]G(x,y) = [x^ky^k]yG(x,y)$. The diagonal is given by $\Delta(yG)(z) := \sum_{k\geqslant 1} M_{k,k-1}z^k$. The computation is then a routine exercise in enumerative combinatorics (see e.g. [15, Chapter 6.3]) and can be automatized to a great extent using computer algebra. We do not present this standard argument here. More details can be found in the accompanying Maple Worksheet [18] implementing the manipulations on the power series using the `gfun` package [13].

We get

$$\Delta(yG)(z) = \frac{1}{2}\left(\frac{1}{1-4z} - \frac{1}{\sqrt{1-4z}}\right)$$

from which we extract coefficients noting $\sum_{n\geqslant 0}\binom{2n}{n}z^n = (1-4z)^{-1/2}$. The asymptotics is directly computed (to any needed order) from the known asymptotics of the central binomial coefficient. □

We proceed to the second moments of the values $\Gamma_{t,k,j}$. Define

$$M^{(2)}_{k,\ell,m} = \sum_{0\leqslant t<2^k} \Gamma_{t,k,k-\ell}\Gamma_{t,k,k-m}.$$

The second moment of $t \mapsto \Gamma_{t,k,1} = P_{t,k}$ is obviously given by $\frac{1}{8^k}M^{(2)}_{k,k-1,k-1}$, which we want to realize as a diagonal of a trivariate rational generating function.

Proposition 11. *We have*

$$M^{(2)}_{k,\ell,m} = \left[x^ky^\ell z^m\right]F(x,y,z),$$

where

$$F(x,y,z) = \frac{1}{1-y}\frac{1}{1-z}\big(A + A' + A'' + A'''\big)(x,y,z),$$

$$\begin{aligned}
A(x,y,z) &= \frac{1 - \frac{xy^2z^2}{1-4xyz}\left(1 + \frac{2xy}{1-2xy(1+yz)} + \frac{2xz}{1-2xz(1+yz)}\right)}{D(x,y,z)}\\
A'(x,y,z) &= \frac{1}{1-2xz(1+yz)}\cdot\frac{1 - x(1+yz)^2 - \frac{xyz}{1-2xy(1+yz)} - xyz}{D(x,y,z)}\\
A''(x,y,z) &= \frac{1}{1-2xy(1+yz)}\cdot\frac{1 - x(1+yz)^2 - \frac{xyz}{1-2xz(1+yz)} - xyz}{D(x,y,z)}\\
A'''(x,y,z) &= \frac{1 - \frac{x}{1-4xyz}\left(1 + \frac{2xy^2z}{1-2xy(1+yz)} + \frac{2xyz^2}{1-2xz(1+yz)}\right)}{D(x,y,z)}
\end{aligned}$$

and

$$D(x,y,z) = 1 - x(1+yz)^2 - \frac{xyz}{1-2xy(1+yz)} - \frac{xyz}{1-2xz(1+yz)}.$$

Proposition 12. *We have the asymptotic expansion*

$$\frac{1}{8^k}M^{(2)}_{k,k-1,k-1} = \frac{1}{4} - \frac{1}{2\sqrt{\pi k}} + \frac{1}{4\pi k} + \frac{1}{16\sqrt{\pi}k^{3/2}} + \frac{17}{72\pi k^2} + \mathcal{O}(k^{-5/2}).$$

Corollary 13. *Let X_k be the discrete random variable defined by $X_k(t) = P_{t,k} = |S_{t,k}|/2^k$, where $1 \leqslant t < 2^k - 1$, and let $\sigma_k = \sqrt{\mathbb{E}(X_k - \mathbb{E}X_k)^2}$ be the corresponding standard deviation. Then for $k \to \infty$ we have*

$$\sigma_k \sim \frac{\sqrt{43}}{12\sqrt{\pi}}k^{-1}.$$

Proof. The first and second moments of the random variable $t \mapsto \frac{1}{2^k}|S_{t,k}|$ are given by $\frac{1}{4^k}M_{k,k-1}$ and $\frac{1}{8^k}M^{(2)}_{k,k-1,k-1}$, of which the asymptotics have been computed in Propositions 10 and 12. By considering $\mathbb{E}(X_k^2) - (\mathbb{E}X_k)^2$, we see that all terms up to $\mathcal{O}(k^{-2})$ cancel, leaving only the asymptotics $43/(144\pi k^2) + \mathcal{O}(k^{-5/2})$. □

Finally, in an analogous manner as in [8, Section 4.4] the proof of Theorem 4 is completed by Chebyshev's inequality.

The remaining part of this paper is devoted to the proofs of Propositions 11 and 12.

4.1 Proof of Proposition 11

Define

$$a_{k,\ell,m} = \sum_{t=0}^{2^k-1} \beta_{t,k,k-\ell}\beta_{t,k,k-m}.$$

and auxiliary values

$$b_{k,\ell,m} = \sum_{t=0}^{2^k-2} \beta_{t,k,k-\ell}\beta_{t+1,k,k-m},$$
$$c_{k,\ell,m} = \sum_{t=0}^{2^k-2} \beta_{t+1,k,k-\ell}\beta_{t,k,k-m}.$$

We calculate, for $k \geqslant 1$ and $\ell, m \geqslant 0$:

$$\begin{aligned} a_{k,\ell,m} &= \sum_{t=0}^{2^{k-1}-1} \beta_{2t,k,k-\ell}\beta_{2t,k,k-m} + \sum_{t=0}^{2^{k-1}-1} \beta_{2t+1,k,k-\ell}\beta_{2t+1,k,k-m} \\ &= \sum_{0 \leqslant t < 2^{k-1}} \big(\beta_{t,k-1,k-1-\ell} + \beta_{t-1,k-1,k+1-\ell}\big)\big(\beta_{t,k-1,k-1-m} + \beta_{t-1,k-1,k+1-m}\big) \\ &\quad + 4 \sum_{0 \leqslant t < 2^{k-1}} \beta_{t,k-1,k-\ell}\beta_{t,k-1,k-m} \end{aligned}$$

$$\begin{aligned}
&= \sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-1-\ell}\beta_{t,k-1,k-1-m} + \sum_{0\leqslant t<2^{k-1}-1} \beta_{t,k-1,k+1-\ell}\beta_{t+1,k-1,k-1-m} \\
&\quad + \sum_{0\leqslant t<2^{k-1}-1} \beta_{t+1,k-1,k-1-\ell}\beta_{t,k-1,k+1-m} + \sum_{0\leqslant t<2^{k-1}-1} \beta_{t,k-1,k+1-\ell}\beta_{t,k-1,k+1-m} \\
&\quad + 4\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-\ell}\beta_{t,k-1,k-m} \\
&= a_{k-1,\ell,m} + b_{k-1,\ell-2,m} + c_{k-1,\ell,m-2} + a_{k-1,\ell-2,m-2} + 4a_{k-1,\ell-1,m-1} \\
&\quad - \beta_{2^{k-1}-1,k-1,k+1-\ell}\beta_{2^{k-1}-1,k-1,k+1-m} \\
&= a_{k-1,\ell,m} + b_{k-1,\ell-2,m} + c_{k-1,\ell,m-2} + a_{k-1,\ell-2,m-2} + 4a_{k-1,\ell-1,m-1} \\
&\quad - 2^{2(k-1)}\delta_{k+1,\ell}\delta_{k+1,m}
\end{aligned}$$

Assume now that $k \geqslant 1$. We have

$$\begin{aligned}
b_{k,\ell,m} &= \sum_{0\leqslant t<2^{k-1}} \beta_{2t,k,k-\ell}\beta_{2t+1,k,k-m} + \sum_{0\leqslant t<2^{k-1}-1} \beta_{2t+1,k,k-\ell}\beta_{2t+2,k,k-m} \\
&= \sum_{0\leqslant t<2^{k-1}} \bigl(\beta_{t,k-1,k-1-\ell} + \beta_{t-1,k-1,k+1-\ell}\bigr)2\beta_{t,k-1,k-m} \\
&\quad + \sum_{0\leqslant t<2^{k-1}-1} 2\beta_{t,k-1,k-\ell}\bigl(\beta_{t+1,k-1,k-1-m} + \beta_{t,k-1,k+1-m}\bigr)
\end{aligned}$$

Noting that $\beta_{1,k,k-m} = 2\beta_{0,k-1,k-m}$, we obtain

$$\begin{aligned}
b_{k,\ell,m} &= 2\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-1-\ell}\beta_{t,k-1,k-m} \\
&\quad + 2\sum_{0\leqslant t<2^{k-1}-1} \beta_{t,k-1,k+1-\ell}\beta_{t+1,k-1,k-m} + 2\sum_{0\leqslant t<2^{k-1}-1} \beta_{t,k-1,k-\ell}\beta_{t+1,k-1,k-1-m} \\
&\quad + 2\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-\ell}\beta_{t,k-1,k+1-m} - 2\beta_{2^{k-1}-1,k-1,k-\ell}\beta_{2^{k-1}-1,k-1,k+1-m} \\
&= 2a_{k-1,\ell,m-1} + 2b_{k-1,\ell-2,m-1} + 2b_{k-1,\ell-1,m} + 2a_{k-1,\ell-1,m-2} - 2^{2k-1}\delta_{k,\ell}\delta_{k+1,m}.
\end{aligned}$$

By the obvious identities $a_{k,\ell,m} = a_{k,m,\ell}$ and $b_{k,\ell,m} = c_{k,m,\ell}$ we have

$$c_{k,\ell,m} = 2a_{k-1,\ell-1,m} + 2c_{k-1,\ell-1,m-2} + 2c_{k-1,\ell,m-1} + 2a_{k-1,\ell-2,m-1} - 2^{2k-1}\delta_{k+1,\ell}\delta_{k,m}.$$

We define generating functions

$$\begin{aligned}
A(x,y,z) &= \sum_{k,\ell,m\geqslant 0} a_{k,\ell,m}x^k y^\ell z^m \\
B(x,y,z) &= \sum_{k,\ell,m\geqslant 0} b_{k,\ell,m}x^k y^\ell z^m \\
C(x,y,z) &= \sum_{k,\ell,m\geqslant 0} c_{k,\ell,m}x^k y^\ell z^m
\end{aligned}$$

Summing over k, ℓ, m, the above recurrences translates to identities for these functions: noting that $a_{k,\ell,m} = 0$ for $\ell < 0$ or $m < 0$, and that

$$\sum_{\ell,m\geqslant 0} a_{0,\ell,m} y^\ell z^m = \sum_{\ell,m\geqslant 0} \beta_{0,0,-\ell}\beta_{0,0,-m} y^\ell z^m = 1,$$

we obtain

$$\begin{aligned} A(x,y,z) &= 1 + x(1+4yz+y^2z^2)A(x,y,z) + xy^2B(x,y,z) + xz^2C(x,y,z) \\ &\quad - \frac{1}{4}\sum_{k\geqslant 1} 4^k x^k y^{k+1} z^{k+1} \\ &= 1 + x(1+4yz+y^2z^2)A(x,y,z) + xy^2B(x,y,z) + xz^2C(x,y,z) \\ &\quad - \frac{yz}{4}\frac{4xyz}{1-4xyz}. \end{aligned}$$

Moreover, we have $\sum_{\ell,m\geqslant 0} b_{0,\ell,m} y^\ell z^m = 0$, therefore

$$\begin{aligned} B(x,y,z) &= 2xz(1+yz)A(x,y,z) + 2xy(1+yz)B(x,y,z) - \frac{1}{2}\sum_{k\geqslant 1} 4^k x^k y^k z^{k+1} \\ &= 2xz(1+yz)A(x,y,z) + 2xy(1+yz)B(x,y,z) - \frac{z}{2}\frac{4xyz}{1-4xyz}. \end{aligned}$$

Finally, we have

$$\begin{aligned} C(x,y,z) &= 2xy(1+yz)A(x,y,z) + 2xz(1+yz)C(x,y,z) - \frac{1}{2}\sum_{k\geqslant 1} 4^k x^k y^{k+1} z^k \\ &= 2xy(1+yz)A(x,y,z) + 2xz(1+yz)C(x,y,z) - \frac{y}{2}\frac{4xyz}{1-4xyz}. \end{aligned}$$

We have

$$B(x,y,z) = \frac{2xz(1+yz)A(x,y,z) - \frac{z}{2}\frac{4xyz}{1-4xyz}}{1-2xy(1+yz)}$$

and

$$C(x,y,z) = \frac{2xy(1+yz)A(x,y,z) - \frac{y}{2}\frac{4xyz}{1-4xyz}}{1-2xz(1+yz)}.$$

Inserting these identities into the equation for $A(x,y,z)$, we obtain

$$\begin{aligned} A(x,y,z)\biggl(1 - x(1+4yz+y^2z^2) - xy^2\frac{2xz(1+yz)}{1-2xy(1+yz)} - xz^2\frac{2xy(1+yz)}{1-2xz(1+yz)}\biggr) \\ = 1 - \frac{yz}{4}\frac{4xyz}{1-4xyz} - xy^2\frac{\frac{z}{2}\frac{4xyz}{1-4xyz}}{1-2xy(1+yz)} - xz^2\frac{\frac{y}{2}\frac{4xyz}{1-4xyz}}{1-2xz(1+yz)} \end{aligned}$$

After some rewriting we obtain

$$A(x,y,z)=\frac{1-\frac{xy^2z^2}{1-4xyz}\left(1+\frac{2xy}{1-2xy(1+yz)}+\frac{2xz}{1-2xz(1+yz)}\right)}{1-x(1+yz)^2-\frac{xyz}{1-2xy(1+yz)}-\frac{xyz}{1-2xz(1+yz)}}$$

Note that the denominator is the same as in [8, Equation (19)].

Define

$$\begin{aligned}
a'_{k,\ell,m} &= \sum_{0\leqslant t<2^k} \beta_{t,k,k-\ell}\beta_{t^{\mathrm{c}}_k,k,-k+m}\\
b'_{k,\ell,m} &= \sum_{0\leqslant t<2^k-1} \beta_{t,k,k-\ell}\beta_{(t+1)^{\mathrm{c}}_k,k,-k+m}\\
c'_{k,\ell,m} &= \sum_{0\leqslant t<2^k-1} \beta_{t-1,k,k-\ell}\beta_{(t+1)^{\mathrm{c}}_k,k,-k+m}
\end{aligned}$$

We have for $k \geqslant 1$

$$\begin{aligned}
a'_{k,\ell,m} &= \sum_{0\leqslant t<2^{k-1}} \beta_{2t,k,k-\ell}\beta_{(2t)^{\mathrm{c}}_k,k,-k+m} + \sum_{0\leqslant t<2^{k-1}} \beta_{2t+1,k,k-\ell}\beta_{(2t+1)^{\mathrm{c}}_k,k,-k+m}\\
&= \sum_{0\leqslant t<2^{k-1}} \bigl(\beta_{t,k-1,k-\ell-1}+\beta_{t-1,k-1,k-\ell+1}\bigr)2\beta_{t^{\mathrm{c}}_{k-1},k-1,-k+m}\\
&\quad+\sum_{0\leqslant t<2^{k-1}} 2\beta_{t,k-1,k-\ell}\bigl(\beta_{t^{\mathrm{c}}_{k-1},k-1,-k+m-1}+\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-k+m+1}\bigr)\\
&= 2\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-1-\ell}\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-1}\\
&\quad+2\sum_{0\leqslant t<2^{k-1}-1} \beta_{t,k-1,k-1-(\ell-2)}\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-1}\\
&\quad+2\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-1-(\ell-1)}\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-2}\\
&\quad+2\sum_{0\leqslant t<2^{k-1}} \beta_{t,k-1,k-1-(\ell-1)}\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+m}\\
&= 2a'_{k-1,\ell,m-1}+2b'_{k-1,\ell-2,m-1}+2a'_{k-1,\ell-1,m-2}+2b'_{k-1,\ell-1,m}
\end{aligned}$$

Moreover

$$\begin{aligned}
b'_{k,\ell,m} &= \sum_{0\leqslant t<2^{k-1}} \beta_{2t,k,k-\ell}\beta_{(2t+1)^{\mathrm{c}}_k,k,-k+m}\\
&\quad+\sum_{0\leqslant t<2^{k-1}-1} \beta_{2t+1,k,k-\ell}\beta_{(2(t+1))^{\mathrm{c}}_k,k,-k+m}\\
&= \sum_{0\leqslant t<2^{k-1}} \bigl(\beta_{t,k-1,k-\ell-1}+\beta_{t-1,k-1,k-\ell+1}\bigr)\bigl(\beta_{t^{\mathrm{c}}_{k-1},k-1,-k+m-1}+\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-k+m+1}\bigr)
\end{aligned}$$

$$\begin{aligned}&+4\sum_{0\leqslant t<2^{k-1}-1}\beta_{t,k-1,k-\ell}\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-k+m}\\ &=a'_{k-1,\ell,m-2}+b'_{k-1,\ell-2,m-2}+b'_{k-1,\ell,m}+c'_{k-1,\ell-2,m}+4b'_{k-1,\ell-1,m-1}\end{aligned}$$

and

$$\begin{aligned}c'_{k,\ell,m}&=\sum_{0\leqslant t<2^{k-1}}\beta_{2t-1,k,k-\ell}\beta_{(2t+1)^{\mathrm{c}}_{k},k,-k+m}+\sum_{0\leqslant t<2^{k-1}}\beta_{2t,k,k-\ell}\beta_{(2(t+1))^{\mathrm{c}}_{k},k,-k+m}\\ &=2\sum_{0\leqslant t<2^{k-1}}\beta_{t-1,k-1,k-\ell}\big(\beta_{t^{\mathrm{c}}_{k-1},k-1,-k+m-1}+\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-k+m+1}\big)\\ &\quad+2\sum_{0\leqslant t<2^{k-1}}\big(\beta_{t,k-1,k-\ell-1}+\beta_{t-1,k-1,k-\ell+1}\big)\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-k+m}\\ &=2b_{k-1,\ell-1,m-2}+2c_{k-1,\ell-1,m}+2b_{k-1,\ell,m-1}+2c_{k-1,\ell-2,m-1}\end{aligned}$$

We define generating functions

$$\begin{aligned}A'(x,y,z)&=\sum_{k,\ell,m\geqslant 0}a'_{k,\ell,m}x^ky^\ell z^m\\ B'(x,y,z)&=\sum_{k,\ell,m\geqslant 0}b'_{k,\ell,m}x^ky^\ell z^m\\ C'(x,y,z)&=\sum_{k,\ell,m\geqslant 0}c'_{k,\ell,m}x^ky^\ell z^m.\end{aligned}$$

We have $a_{k,\ell,m}=0$ for $\ell<0$ or $m<0$, and

$$\sum_{\ell,m\geqslant 0}a'_{0,\ell,m}y^\ell z^m=\sum_{\ell,m\geqslant 0}\beta_{0,0,-\ell}\beta_{0,0,-m}y^\ell z^m=1,$$

moreover

$$\sum_{\ell,m\geqslant 0}b'_{0,\ell,m}y^\ell z^m=\sum_{\ell,m\geqslant 0}c'_{0,\ell,m}y^\ell z^m=0.$$

We obtain

$$\begin{aligned}A'(x,y,z)&=1+2xzA'(x,y,z)+2xy^2zB'(x,y,z)+2xyz^2A'(x,y,z)+2xyB'(x,y,z)\\ &=1+2xz(1+yz)A'(x,y,z)+2xy(1+yz)B'(x,y,z),\end{aligned}\tag{8}$$

$$B'(x,y,z)=xz^2A'(x,y,z)+(xy^2z^2+x+4xyz)B'(x,y,z)+xy^2C'(x,y,z)$$

and

$$C'(x,y,z)=2xz(1+yz)B'(x,y,z)+2xy(1+yz)C'(x,y,z).$$

It follows that

$$A'(x,y,z)=\frac{1+2xy(1+yz)B'(x,y,z)}{1-2xz(1+yz)}$$
$$C'(x,y,z)=\frac{2xz(1+yz)B'(x,y,z)}{1-2xy(1+yz)}$$

and therefore

$$B'(x,y,z)=\left(xz^2\frac{2xy(1+yz)}{1-2xz(1+yz)}+x(1+4yz+y^2z^2)+xy^2\frac{2xz(1+yz)}{1-2xy(1+yz)}\right)B'(x,y,z)$$
$$+\frac{xz^2}{1-2xz(1+yz)}.$$

Inserting this into (8), we obtain after some elementary manipulation

$$A'(x,y,z)=\frac{1}{1-2xz(1+yz)}\cdot\frac{1-x(1+yz)^2-\frac{xyz}{1-2xy(1+yz)}-xyz}{1-x(1+yz)^2-\frac{xyz}{1-2xy(1+yz)}-\frac{xyz}{1-2xz(1+yz)}}.$$

Define

$$a''_{k,\ell,m}=\sum_{0\leqslant t<2^k}\beta_{t_k^{\mathrm{c}},k,-k+\ell}\beta_{t,k,k-m}$$

and

$$A''(x,y,z)=\sum_{k,\ell,m\geqslant 0}a''_{k,\ell,m}x^ky^\ell z^m$$

By exchanging the roles of ℓ and m resp. y and z we obtain

$$A''(x,y,z)=\frac{1}{1-2xy(1+yz)}\cdot\frac{1-x(1+yz)^2-\frac{xyz}{1-2xz(1+yz)}-xyz}{1-x(1+yz)^2-\frac{xyz}{1-2xy(1+yz)}-\frac{xyz}{1-2xz(1+yz)}}.$$

Finally, we define

$$a'''_{k,\ell,m}=\sum_{0\leqslant t<2^k}\beta_{t_k^{\mathrm{c}},k,-k+\ell}\beta_{t_k^{\mathrm{c}},k,-k+m}$$
$$b'''_{k,\ell,m}=\sum_{0\leqslant t<2^k}\beta_{t_k^{\mathrm{c}},k,-k+\ell}\beta_{(t+1)_k^{\mathrm{c}},k,-k+m}$$
$$c'''_{k,\ell,m}=\sum_{0\leqslant t<2^k}\beta_{(t+1)_k^{\mathrm{c}},k,-k+\ell}\beta_{t_k^{\mathrm{c}},k,-k+m}$$

and we have

$$a'''_{k,\ell,m}=\sum_{0\leqslant t<2^{k-1}}\beta_{(2t)_k^{\mathrm{c}},k,-k+\ell}\beta_{(2t)_k^{\mathrm{c}},k,-k+m}+\sum_{0\leqslant t<2^{k-1}}\beta_{(2t+1)_k^{\mathrm{c}},k,-k+\ell}\beta_{(2t+1)_k^{\mathrm{c}},k,-k+m}$$
$$=4\sum_{0\leqslant t<2^{k-1}}\beta_{t_{k-1}^{\mathrm{c}},k-1,-(k-1)+\ell-1}\beta_{t_{k-1}^{\mathrm{c}},k-1,-(k-1)+m-1}$$

$$\begin{aligned}
&+ \sum_{0\leqslant t<2^{k-1}} \left(\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell-2} + \beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell}\right)\\
&\quad \times \left(\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-2} + \beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+m}\right)\\
&= 4a'''_{k-1,\ell-1,m-1} + a'''_{k-1,\ell-2,m-2} + b'''_{k-1,\ell-2,m} + c'''_{k-1,\ell,m-2} + a'''_{k-1,\ell,m}\\
&\quad - \beta_{0^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell}\beta_{0^{\mathrm{c}}_{k-1},k-1,-(k-1)+m}\\
&= 4a'''_{k-1,\ell-1,m-1} + a'''_{k-1,\ell-2,m-2} + b'''_{k-1,\ell-2,m} + c'''_{k-1,\ell,m-2} + a'''_{k-1,\ell,m}\\
&\quad - 2^{2(k-1)}\delta_{k,\ell+1}\delta_{k,m+1}
\end{aligned}$$

$$\begin{aligned}
b'''_{k,\ell,m} &= \sum_{0\leqslant t<2^{k-1}} \beta_{(2t)^{\mathrm{c}}_{k},k,-k+\ell}\beta_{(2t+1)^{\mathrm{c}}_{k},k,-k+m} + \sum_{0\leqslant t<2^{k-1}} \beta_{(2t+1)^{\mathrm{c}}_{k},k,-k+\ell}\beta_{(2(t+1))^{\mathrm{c}}_{k},k,-k+m}\\
&= 2\sum_{0\leqslant t<2^{k-1}} \beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell-1}\left(\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-2} + \beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+m}\right)\\
&\quad + 2\sum_{0\leqslant t<2^{k-1}} \left(\beta_{t^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell-2} + \beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+\ell}\right)\beta_{(t+1)^{\mathrm{c}}_{k-1},k-1,-(k-1)+m-1}\\
&= 2a'''_{k-1,\ell-1,m-2} + 2b'''_{k-1,\ell-1,m} + 2b'''_{k-1,\ell-2,m-1} + 2a'''_{k-1,\ell,m-1}\\
&\quad - 2\beta_{0^{\mathrm{c}}_{k-1},k-1,-k+\ell+1}\beta_{0^{\mathrm{c}}_{k-1},k-1,-k+m}\\
&= 2a'''_{k-1,\ell-1,m-2} + 2b'''_{k-1,\ell-1,m} + 2b'''_{k-1,\ell-2,m-1} + 2a'''_{k-1\ell,m-1} - 2^{2k-1}\delta_{k,\ell+1}\delta_{k,m}
\end{aligned}$$

and

$$\begin{aligned}
c'''_{k,\ell,m} &= b'''_{k,m,\ell}\\
&= 2a'''_{k-1,m-1,\ell-2} + 2b'''_{k-1,m-1,\ell} + 2b'''_{k-1,m-2,\ell-1} + 2a'''_{k-1,m,\ell-1} - 2^{2k-1}\delta_{k,m+1}\delta_{k,\ell}\\
&= 2a'''_{k-1,\ell-2,m-1} + 2c'''_{k-1,\ell,m-1} + 2c'''_{k-1,\ell-1,m-2} + 2a'''_{k-1,\ell-1,m} - 2^{2k-1}\delta_{k,\ell}\delta_{k,m+1}.
\end{aligned}$$

Again we translate this to generating functions. We note that

$$\sum_{\ell,m\geqslant 0} a'''_{0,\ell,m}y^{\ell}z^{m} = \sum_{\ell,m\geqslant 0} \beta_{0,0,-\ell}\beta_{0,0,m} = \sum_{\ell,m\geqslant 0} \delta_{\ell,0}\delta_{m,0} = 1$$

and that

$$\sum_{\ell,m\geqslant 0} b'''_{0,\ell,m}y^{\ell}z^{m} = \sum_{\ell,m\geqslant 0} c'''_{0,\ell,m}y^{\ell}z^{m} = 0.$$

Therefore

$$\begin{aligned}
A'''(x,y,z) = 1 &+ x(4yz + y^2z^2 + 1)A'''(x,y,z) + xy^2B(x,y,z) + xz^2C(x,y,z)\\
&- \sum_{k\geqslant 1} 4^{k-1}x^{k}y^{k-1}z^{k-1}
\end{aligned}$$

$$= 1 + x(4yz + y^2z^2 + 1)A'''(x,y,z) + xy^2B(x,y,z) + xz^2C(x,y,z) \\ - \frac{x}{1-4xyz}$$

and

$$B'''(x,y,z) = 2xz(1+yz)A'''(x,y,z) + 2xy(1+yz)B'''(x,y,z) - 2\sum_{k\geqslant 1} 4^{k-1}x^ky^{k-1}z^k \\ = 2xz(1+yz)A'''(x,y,z) + 2xy(1+yz)B'''(x,y,z) - \frac{2xz}{1-4xyz}$$

$$C'''(x,y,z) = 2xy(1+yz)A'''(x,y,z) + 2xz(1+yz)C'''(x,y,z) - \frac{2xy}{1-4xyz}.$$

It follows that

$$B'''(x,y,z) = \frac{2xz(1+yz)A'''(x,y,z) - \frac{2xz}{1-4xyz}}{1-2xy(1+yz)}$$

and

$$C'''(x,y,z) = \frac{2xy(1+yz)A'''(x,y,z) - \frac{2xy}{1-4xyz}}{1-2xz(1+yz)}$$

and therefore

$$A'''(x,y,z)\left(1 - x(1+4yz+y^2z^2) - xy^2\frac{2xz(1+yz)}{1-2xy(1+yz)} - xz^2\frac{2xy(1+yz)}{1-2xz(1+yz)}\right) \\ = 1 - \frac{x}{1-4xyz} - xy^2\frac{\frac{2xz}{1-4xyz}}{1-2xy(1+yz)} - xz^2\frac{\frac{2xy}{1-4xyz}}{1-2xz(1+yz)}.$$

It follows that

$$A'''(x,y,z) = \frac{1 - \frac{x}{1-4xyz}\left(1 + \frac{2xy^2z}{1-2xy(1+yz)} + \frac{2xyz^2}{1-2xz(1+yz)}\right)}{1 - x(1+yz)^2 - \frac{xyz}{1-2xy(1+yz)} - \frac{xyz}{1-2xz(1+yz)}}.$$

We have

$$M^{(2)}_{k,\ell,m} = \sum_{\substack{i\leqslant\ell \\ j\leqslant m}} \sum_{0\leqslant t<2^k} \gamma_{t,k,k-i}\gamma_{t,k,k-j} \\ = \sum_{\substack{i\leqslant\ell \\ j\leqslant m}} \big(a_{k,i,j} + a'_{k,i,j} + a''_{k,i,j} + a'''_{k,i,j}\big) \\ = \big[x^ky^\ell z^m\big]\frac{1}{1-y}\frac{1}{1-z}\big(A + A' + A'' + A'''\big)(x,y,z).$$

4.2 Proof of Proposition 12

We write

$$F(x,y,z) = \frac{1}{(1-y)(1-z)} \frac{G(x,y,z)}{D(x,y,z)},$$

where

$$G = B + B' + B'' + B''',$$

$$\begin{aligned}
B(x,y,z) &= 1 - \frac{xy^2z^2}{1-4xyz}\left(1 + \frac{2xy}{1-2xy(1+yz)} + \frac{2xz}{1-2xz(1+yz)}\right)\\
B'(x,y,z) &= \frac{1 - x(1+yz)^2 - \frac{xyz}{1-2xy(1+yz)} - xyz}{1-2xz(1+yz)}\\
B''(x,y,z) &= \frac{1 - x(1+yz)^2 - \frac{xyz}{1-2xz(1+yz)} - xyz}{1-2xy(1+yz)}\\
B'''(x,y,z) &= 1 - \frac{x}{1-4xyz}\left(1 + \frac{2xy^2z}{1-2xy(1+yz)} + \frac{2xyz^2}{1-2xz(1+yz)}\right)
\end{aligned}$$

and

$$D(x,y,z) = 1 - x(1+yz)^2 - \frac{xyz}{1-2xy(1+yz)} - \frac{xyz}{1-2xz(1+yz)}.$$

The proof is analogous to [8, Proposition 10]. We copy the following two lemmata. (We denote the open disk with radius δ around $a \in \mathbb{C}$ by $B_\delta(a)$.)

Lemma 14. *There exist $\delta, \delta_1, \varepsilon > 0$ and a unique smooth function $f : B_\delta(1) \times B_\delta(1) \to \mathbb{C}$ such that $f(1,1) = 1/8$ and*

$$D(f(y,z), y, z) = 0$$

for $|y-1| < \delta$ and $|z-1| < \delta$, such that

$$[x^n]\, F(x,y,z) = \frac{1}{(1-y)(1-z)}\left(\frac{-G(f(y,z),y,z)}{D_x(f(y,z),y,z)} f(y,z)^{-n-1} + \mathcal{O}\big(8^{(1-\varepsilon)n}\big)\right) \tag{9}$$

uniformly for $|y-1| < \delta$ and $|z-1| < \delta$, and such that

$$[x^n]\, F(x,y,z) = \mathcal{O}(8^{(1-\varepsilon)n}) \tag{10}$$

uniformly for all y, z satisfying $|y| \leqslant 1 + \delta_1$, $|z| \leqslant 1 + \delta_1$ and ($|y-1| \geqslant \delta$ or $|z-1| \geqslant \delta$). Furthermore, we have the local expansions

$$\begin{aligned}
f(y,z) = \frac{1}{8} &- \frac{1}{8}(y-1) - \frac{1}{8}(z-1) + \frac{3}{32}(y-1)^2 + \frac{3}{32}(z-1)^2 + \frac{1}{8}(y-1)(z-1)\\
&- \frac{1}{16}(y-1)^3 - \frac{1}{16}(z-1)^3 - \frac{3}{32}(y-1)^2(z-1) - \frac{3}{32}(y-1)(z-1)^2\\
&+ \frac{5}{128}(y-1)^4 + \frac{5}{128}(z-1)^4 + \frac{1}{16}(y-1)^3(z-1) + \frac{1}{16}(y-1)(z-1)^3
\end{aligned}$$

$$+\frac{13}{192}(y-1)^2(z-1)^2+\mathcal{O}\big(|y-1|^5+|z-1|^5\big)$$

and

$$\begin{aligned}\log f(y,z) = &-\log 8-(y-1)-(z-1)+\frac{1}{4}(y-1)^2+\frac{1}{4}(z-1)^2\\ &-\frac{1}{12}(y-1)^3-\frac{1}{12}(z-1)^3+\frac{1}{32}(y-1)^4+\frac{1}{32}(z-1)^4\\ &-\frac{1}{48}(y-1)^2(z-1)^2+\mathcal{O}\big(|y-1|^5+|z-1|^5\big)\end{aligned}$$

at $(1,1)\in\mathbb{C}^2$.

The next lemma will be needed for computing the asymptotic expansion of the coefficients of $y^n z^n$. It summarizes results on the normal distribution.

Lemma 15. *We have*

$$\int_{-\infty,\Im(s)>0}^{\infty} e^{-s^2/4}\frac{\mathrm{d}s}{s}=-\pi i,$$

and for $k\geqslant 0$

$$\int_{-\infty}^{\infty} e^{-s^2/4}s^k\mathrm{d}s=\begin{cases}2\sqrt{\pi}\frac{k!}{(k/2)!}, & k \text{ even},\\ 0, & k \text{ odd}.\end{cases}$$

We begin by determining the coefficient $[y^{n-1}z^{n-1}]$ using Cauchy integration,

$$[x^n y^{n-1} z^{n-1}]\,F(x,y,z)=\frac{1}{(2\pi i)^2}\iint\limits_{\gamma\times\gamma}[x^n]\,F(x,y,z)\frac{\mathrm{d}y}{y^n}\frac{\mathrm{d}z}{z^n},$$

where the contour of integration γ consists of two pieces: a part γ_1 inside the disk of radius δ around 1, which connects the points $1\pm i\delta$ and passes 1 on the left hand side, and a part γ_2, which is just a circular arc around 0 connecting the points $1\pm i\delta$, see Figure 1.

By (9) and (10) the integral along γ_2, is of order $\mathcal{O}(8^{(1-\varepsilon)n})$ which will turn out to be exponentially smaller than the main part arising from the integral along γ_1. Therefore we may replace γ by γ_1, obtaining

$$\begin{aligned}{}[x^n y^{n-1} z^{n-1}]\,F(x,y,z) &= \mathcal{O}\big(8^{(1-\varepsilon)n}\big)\\ &+\frac{1}{(2\pi i)^2}\iint\limits_{\gamma_1\times\gamma_1}\frac{1}{(1-y)(1-z)}\frac{-yz\,G(f(y,z),y,z)}{D_x(f(y,z),y,z)}\big(f(y,z)yz\big)^{-n-1}\mathrm{d}y\,\mathrm{d}z.\end{aligned}$$

For $y,z\in\gamma_1$ we set

$$y=1+i\frac{s}{\sqrt{n}}\quad\text{and}\quad z=1+i\frac{t}{\sqrt{n}}$$

and obtain after this substitution

$$[x^n y^{n-1} z^{n-1}]\, F(x,y,z) = \frac{1}{(2\pi i)^2} \iint\limits_{\substack{|s|,|t|\leqslant\delta\sqrt{n},\\ \Im(s),\Im(t)>0}} P_n(s,t) e^{-(n+1)\, g_n(s,t)} \frac{\mathrm{d}s\,\mathrm{d}t}{st} + \mathcal{O}\big(8^{(1-\varepsilon)n}\big),$$

where

$$P_n(s,t) = \left.\frac{-yz\, G(f(y,z),y,z)}{D_x(f(y,z),y,z)}\right|_{y=1+is/\sqrt{n},\, z=1+it/\sqrt{n}}$$

and

$$g_n(s,t) = \left(\log f(y,z) + \log y + \log z\right)\big|_{y=1+is/\sqrt{n},\, z=1+it/\sqrt{n}}\,.$$

Using the Taylor expansion of $f(x,y)$ and a computer algebra system, we obtain

$$\frac{-yz\, G(f(y,z),y,z)}{D_x(f(y,z),y,z)} = \frac{1}{8} - \frac{1}{32}(y-1)^2 - \frac{1}{32}(z-1)^2 + \mathcal{O}\big(|y-1|^3 + |z-1|^3\big),$$

from which it follows that

$$P_n(s,t) = \frac{1}{8}\left(1 + \frac{s^2}{4n} + \frac{t^2}{4n} + \mathcal{O}\left(\frac{|s|^3+|t|^3}{n^{3/2}}\right)\right).$$

Lemma 14 implies

$$\begin{aligned}\log f(y,z) + \log y + \log z = &-\log 8 - \frac{1}{4}(y-1)^2 - \frac{1}{4}(z-1)^2 + \frac{1}{4}(y-1)^3 + \frac{1}{4}(z-1)^3 \\ &- \frac{7}{32}(y-1)^4 - \frac{7}{32}(y-1)^4 - \frac{1}{48}(y-1)^2(z-1)^2 \\ &+ \mathcal{O}\big(|y-1|^5 + |z-1|^5\big),\end{aligned}$$

so that

$$\begin{aligned}-(n+1)\, g_n(s,t) = \log 8^{n+1} &- \frac{s^2}{4} - \frac{t^2}{4} + i\frac{s^3}{4\sqrt{n}} + i\frac{t^3}{4\sqrt{n}} - \frac{s^2}{4n} - \frac{t^2}{4n} \\ &+ \frac{7s^4}{32n} + \frac{7t^4}{32n} + \frac{s^2t^2}{48n} + \mathcal{O}\left(\frac{|s|^5+|t|^5}{n^{3/2}}\right).\end{aligned} \tag{11}$$

As a next step we want to use the expansion $e^x = 1 + x + x^2/2 + \mathcal{O}(x^3)$ for $x = o(1)$ on the part involving exponents in s and t of order 3 and higher. Therefore we need to split the contour γ_1 into 3 parts. (Remark. At this point the argument in [8] is incomplete, but can be repaired in the same way.)

For their definition we need to choose a sequence A_n such that $A_n = o(n^{-1/3})$ and $A_n = \omega(n^{-1/2})$. Thus, we choose $A_n = n^{-1/2+\nu}$ for $0 < \nu < 1/6$. Then we define a part $\gamma_{1,1}$ which connects the points $1 \pm i\delta A_n$ inside the disc of radius δA_n around 1 and passes 1 on the left hand side, a part $\gamma_{1,2}$ which connects $1 + i\delta A_n$ and $1 + i\delta$ by a straight line, and a symmetric part $\gamma_{1,3}$ that connects $1 - i\delta A_n$ and $1 - i\delta$ by a straight line, see Figure 1.

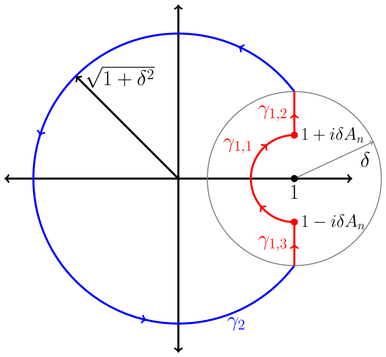

Figure 1: The path of integration used in Lemma 15. The contour consists of two main parts γ_1 and γ_2, where γ_1 is split into 3 smaller parts $\gamma_{1,1}, \gamma_{1,2}$, and $\gamma_{1,3}$. The asymptotic main contribution arises at $\gamma_{1,1}$. The constant δ is defined in Lemma 14 and $A_n = n^{-1/2+\nu}$ with $0 < \nu < 1/6$.

Due to (11) we get the bound

$$\Re\left(-(n+1)g_n(s,t)\right) \leqslant \log(8^{n+1}) - \frac{s^2}{3} - \frac{t^2}{3},$$

for large enough n. Hence, the integral along $\gamma_{1,2}$ (and also $\gamma_{1,3}$) is negligible as

$$\int\limits_{\delta n^\nu \leqslant |s|,|t| \leqslant \delta\sqrt{n}} e^{-(n+1)g_n(s,t)}\, ds\, dt = o\left(8^n e^{-\frac{n^{2\nu}}{3}}\right).$$

The lower bound is computed as $A_n\sqrt{n} = n^\nu$, where the choice of A_n is crucial.

What remains is to treat the integral along $\gamma_{1,1}$. On this part we may use the expansion of e^x to obtain

$$\begin{aligned} e^{-(n+1)\,g_n(s,t)} = 8^{n+1} e^{-\frac{s^2}{4}-\frac{t^2}{4}} \Bigg(1 - \frac{s^2+t^2}{4n} + i\frac{s^3+t^3}{4\sqrt{n}} + \frac{7(s^4+t^4)}{32n} + \frac{s^2t^2}{48n} \\ - \frac{s^6+t^6}{32n} - \frac{s^3t^3}{16n} + \mathcal{O}\left(\frac{|s|^5+|s|^7+|t|^5+|t|^7}{n^{3/2}}\right)\Bigg) \end{aligned}$$

for $|s| \leqslant n^\nu$ and $|t| \leqslant \delta n^\nu$. This leads to

$$\begin{aligned} &\frac{1}{(2\pi i)^2} \iint\limits_{|s|,|t|\leqslant \delta n^\nu, \Im(s),\Im(t)>0} P_n(s,t) e^{-(n+1)\,g_n(s,t)} \frac{\mathrm{d}s\,\mathrm{d}t}{st} \\ &\qquad = \frac{8^n}{(2\pi i)^2} \iint\limits_{|s|,|t|\leqslant \delta n^\nu, \Im(s),\Im(t)>0} e^{-\frac{s^2}{4}-\frac{t^2}{4}} \Bigg(1 + \frac{is^3+it^3}{4\sqrt{n}} + \frac{7s^4+7t^4}{32n} + \frac{s^2t^2}{48n} \\ &\qquad\quad - \frac{s^6+t^6}{32n} - \frac{s^3t^3}{16n}\Bigg) \frac{\mathrm{d}s\,\mathrm{d}t}{st} + \mathcal{O}\left(\frac{8^n}{n^{3/2}}\right) \end{aligned}$$

$$= \frac{8^n}{(2\pi i)^2} \iint\limits_{-\infty<s,t<\infty,\Im(s),\Im(t)>0} e^{-\frac{s^2}{4}-\frac{t^2}{4}} \left(1 + \frac{is^3+it^3}{4\sqrt{n}} + \frac{7s^4+7t^4}{32n} + \frac{s^2t^2}{48n} - \frac{s^6+t^6}{32n} - \frac{s^3t^3}{16n}\right) \frac{\mathrm{d}s\,\mathrm{d}t}{st} + \mathcal{O}\left(\frac{8^n}{n^{3/2}}\right).$$

Finally by writing this as a sum of products of integrals and applying Lemma 15 term by term this expression equals

$$= 8^n \left(\frac{1}{4} - \frac{1}{2\sqrt{\pi n}} + \frac{1}{4\pi n} + \mathcal{O}(n^{-3/2})\right).$$

Summing up we arrive at the asymptotics

$$\frac{1}{8^n}[x^n y^{n-1} z^{n-1}]\, F(x,y,z) = \frac{1}{4} - \frac{1}{2\sqrt{\pi n}} + \frac{1}{4\pi n} + \mathcal{O}(n^{-3/2}).$$

By extending the above argument, which is only a computational issue, we obtain more terms in the asymptotic expansion, which yields the statement of Proposition 12. For details see the accompanying Maple worksheet [18].

5 Conclusion

It is an elementary problem to study the behaviour of the digital expansion of an integer under addition of a constant. More specifically, we wish to understand the *sum of digits* in base 2 of n and $n+t$, which amounts to study the number of *carries* occurring in the addition of the binary expansions of n and t. The question arises how often a certain number of carries is attained when adding n to a given integer t. At first, this has the appearance of an easy task. However, we soon meet the difficulty that carries may propagate through several blocks of 1s; it is not clear how to capture all of the appearing patterns simultaneously. Both Conjecture 1 and Conjecture 2 concern this question, and neither of them could be solved for the past seven years since their introduction. Only partial results have been obtained so far, including an almost-all result for Cusick's conjecture proved by Drmota, Kauers, and the first author. The current paper adds to our knowledge on the Tu–Deng conjecture by proving an analogous result: Conjecture 1 holds almost surely in a precise sense.

Our method certainly can be applied to related questions. While analoga of (5) and (6) fail for the sum-of-digits function in base 3, they seem to hold for the Hamming weight of the ternary expansion of n (the number of nonzero digits of n in base 3). We are confident that our method yields almost-all results for these questions.

A different kind of extension of the considered problems concerns the sum of digits of n, $n+t$ and $n+2t$: do we have $|\{n \in \{0,\ldots,2^k-1\} : s(n) \leqslant s(n+t), s(n) \leqslant s(n+2t)\}| > 2^{k-2}$? Is the same true for $\oplus_k$ instead of $+$? Again, we expect that nontrivial results can be obtained using our method.

Meanwhile, the full statement of Conjecture 1 remains an open problem. One possible approach to proving it is to assume a hypothetical counterexample to the conjecture, and from it construct a large set of counterexamples, which would contradict the asymptotical statement of our main theorem. However, it is a nontrivial task to compare the values $P_{t,k}$ for different t, in particular to construct (many) integers t' and k' satisfying $P_{t',k'} \geqslant P_{t,k}$. It follows that this approach cannot yet be used to prove the conjecture.

In a similar vein, we may consider the following approach to proving Conjecture 2: we have numerically $c_{t'} \leqslant c_t$, where t' is obtained by appending $01\cdots 1$ to the binary expansion and the number of 1s is large enough. If this can be proved, we may iterate the procedure of appending $01\cdots 1$, obtaining $t^{(k)}$; moreover, by asymptotic considerations one can certainly prove that $c_{t^{(k)}} > 1/2$ for k large enough. By monotonicity, we obtain $c_t > 1/2$. Again, the problem to overcome is the comparison of values of c_t for different t, which seems to be difficult.

Acknowledgements

The first author acknowledges support by the project MuDeRa (Multiplicativity, Determinism, and Randomness), which is a joint project between the ANR (Agence Nationale de la Recherche, ANR-14-CE34-0009) and the FWF (Austrian Science Fund, I-1751-N26), and also by project F5502-N26 (FWF), which is a part of the Special Research Program "Quasi Monte Carlo Methods: Theory and Applications". The second was partially supported by the SFB project F50-03 "Algorithmic and Enumerative Combinatorics" and by the Erwin Schrödinger Fellowship of the Austrian Science Fund (FWF): J 4162-N35. Last but not least, we thank Michael Drmota for many insightful discussions, and the referees for the detailed feedback and enthusiasm!

References

[1] F. Armknecht, *Improving fast algebraic attacks*, in Fast Software Encryption, Springer, 2004, pp. 65–82.

[2] J. Bésineau, *Indépendance statistique d'ensembles liés à la fonction "somme des chiffres"*, Acta Arith., 20 (1972), pp. 401–416.

[3] C. Carlet, *Boolean models and methods in mathematics, computer science, and engineering*, vol. 134 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, 2010, ch. Boolean functions for cryptography and error correcting codes, pp. 257–397.

[4] N. T. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, in Advances in cryptology—CRYPTO 2003, vol. 2729 of Lecture Notes in Comput. Sci., Springer, Berlin, 2003, pp. 176–194.

[5] N. T. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, in Advances in cryptology—EUROCRYPT 2003, vol. 2656 of Lecture Notes in Comput. Sci., Springer, Berlin, 2003, pp. 345–359.

[6] T. W. Cusick, Y. Li, and P. Stănică, *On a combinatorial conjecture*, Integers, 11 (2011), pp. A17, 17.

[7] G. Deng and P. Yuan, *On a combinatorial conjecture of Tu and Deng*, Integers, 12 (2012), pp. Paper No. A48, 9.

[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), pp. 621–649. arXiv:1509.08623.

[9] J.-P. Flori, *Fonctions booléennes, courbes algébriques et multiplication complexe*, PhD thesis, Télécom ParisTech, 2012.

[10] J.-P. Flori, H. Randriambololona, G. Cohen, and S. Mesnager, *On a Conjecture about Binary Strings Distribution*, Sequences and Their Applications - SETA 2010 Springer Berlin/Heidelberg (Ed.), (2010), pp. 346–358.

[11] W. Meier, E. Pasalic, and C. Carlet, *Algebraic attacks and decomposition of Boolean functions*, in Advances in cryptology—EUROCRYPT 2004, vol. 3027 of Lecture Notes in Comput. Sci., Springer, Berlin, 2004, pp. 474–491.

[12] S. Qarboua, J. Schrek, and C. Fontaine, *New results about Tu-Deng's conjecture*, 2016 IEEE International Symposium on Information Theory (ISIT), (2016), pp. 485–489.

[13] B. Salvy and P. Zimmermann, *Gfun: a maple package for the manipulation of generating and holonomic functions in one variable*, ACM Transactions on Mathematical Software (TOMS), 20 (1994), pp. 163–177.

[14] L. Spiegelhofer and M. Wallner, *An explicit generating function arising in counting binomial coefficients divisible by powers of primes*, Acta Arith., 181 (2017), pp. 27–55.

[15] R. P. Stanley, *Enumerative combinatorics. Vol. 2*, vol. 62 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1999.

[16] 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), pp. 1–14.

[17] ——, *Boolean functions optimizing most of the cryptographic criteria*, Discrete Appl. Math., 160 (2012), pp. 427–435.

[18] M. Wallner, http://dmg.tuwien.ac.at/mwallner, 2019.