THE TU–DENG CONJECTURE HOLDS ALMOST SURELY

LUKAS SPIEGELHOFER AND MICHAEL WALLNER

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 $1 \le t < 2^k - 1$. Then

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

We prove that the Tu–Deng Conjecture holds almost surely in the following sense: the proportion of $t \in [1, 2^k-2]$ 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 $n+t$.

1. Introduction and results

Z. Tu and Y. Deng's Conjecture [17] is concerned with the Hamming weight $w(n)$ of a nonnegative integer n (the sum of digits in base two) and addition modulo 2^k-1. This conjecture is as follows.

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

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

Then $P_{t,k} \coloneqq |S_{t,k}|/2^k \le 1/2$.

The conjecture arose in the construction of Boolean functions with optimal algebraic immunity (see Tu and Deng [17, 18]). 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 [4]. However, they are prone to serious attacks [2, 5, 6]. In order to prevent them from these known attacks algebraic immunity was introduced [12].

So far it could only be solved for some special cases [7, 8, 11, 13]. Moreover, it was checked for all $k \le 29$ by Tu and Deng [17] and for $k \in \{39, 40\}$ by Flori [10].

Let us give a probabilistic (and combinatorial) interpretation of the conjecture. Let $S_k \coloneqq \bigcup_{t=1}^{2^k-2} S_{t,k}$. Let us consider an arbitrary pair (a,b) of S_k. On the one hand, the number 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,

2010 *Mathematics Subject Classification.* Primary: 11A63, 68R05, 11T71; Secondary: 05A20, 05A16.

Key words and phrases. Tu–Deng Conjecture.

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) and the FWF (Austrian Science Fund, grant 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 partly supported by Project F50-03 (FWF), which is a part of the Special Research Program "Algorithmic and Enumerative Combinatorics".

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 $2k$ places we get

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

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

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

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 C. *Assume that t is a nonnegative integer. Then*

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

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

We note that the density exists, which follows, for example, from the "Lemma of Bésineau" [3, Lemme 1], see also [9, Lemma 2.1]. In fact, we have

$$c_t = \frac{1}{2^k}\bigl|\{n < 2^k : w(n+t) \geq w(n)\}\bigr| \tag{1.1}$$

for $k \geq \alpha + \mu$, where $\alpha = w(t)+1$ and $2^\mu \leq t < 2^{\mu+1}$ [9, Section 2]. In [9], we also studied a statement complementary to Cusick's Conjecture:

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

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

Analogously to the case c_t, we have

$$\tilde{c}_t = \frac{1}{2^{k-1}}\bigl|\{n < 2^{k-1} : w(n+t) > w(n)\}\bigr|. \tag{1.2}$$

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

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

Numerical experiments reveal that $\tilde{c}_t \leq 1/2 < c_t$ for all $t < 2^{30}$. In fact, in [9] Drmota, Kauers and the first author proved that Conjectures C and CC 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 TD.

[1] `http://oeis.org`

Theorem 1.1. *Define $P_{t,k}$ as before,*

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

As $k \to \infty$, we have

$$\left|\left\{t \in \{1,\ldots,2^k-2\} : P_{t,k} > 1/2\right\}\right| = O\left(\frac{2^k}{k}\right).$$

In particular,

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

Moreover, we will prove that Conjectures C and CC are in fact implied by Conjecture TD.

Proposition 1.2. *Conjecture TD implies Conjectures C and CC.*

The idea of the proof of Theorem 1.1 is to show a concentration result using Chebyshev's inequality. More precisely, we consider the moments

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

and derive asymptotic expansions for them. 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 in [9]. 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 1.1 and Proposition 1.2.

2. Proof of Proposition 1.2

Proof of Proposition 1.2. We first rewrite the Tu–Deng Conjecture. Let us split the set $S_{t,k}$ according to whether $a+b < 2^k-1$: set

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

These two sets form a partition of $S_{t,k}$. We define the quantity

$$\beta_{t,k,j} = \left|\left\{a \in \{0,\ldots,t\} : w\left(a+2^k-1-t\right) - w(a) = j\right|,$$

where $k \ge 1$, $0 \le t < 2^k$ and j are integers. By the identity $w\left(2^k-1-t\right) = k - w(t)$ we have

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

and

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

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

$$\begin{aligned}
|S_{t,k}| &= \bigl|S_{t,k}^{(1)}\bigr| + \bigl|S_{t,k}^{(2)}\bigr| \\
&= \bigl\{a \in \{0,\ldots,t\} : w\bigl(a+2^k-1-t\bigr) > w(a)\bigr\} \\
&+ \bigl\{a \in \{0,\ldots,2^k-1-t\} : w(a) > w(a+t)\bigr\} \\
&= \sum_{j\ge 1}\Bigl(\beta_{t,k,j} + \beta_{2^k-1-t,k,-j}\Bigr).
\end{aligned} \tag{2.1}$$

Both Conjecture C and Conjecture CC are trivial if $t = 0$. Let $t \ge 1$ be given and assume that $k' \ge 1$ is such that $t < 2^{k'}-1$; we choose $k \ge 2k'$. With this choice we have $w(a) \le w\bigl(a+2^k-1-t\bigr)$ as long as $0 \le a \le t$. This is the case since $2^k-2^{k'}+1 \le a+2^k-1-t \le 2^k-1$, therefore the tail of $\mathtt{1}$s 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 TD holds, we obtain

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

This last expression equals $2^k\bigl(1-c_t\bigr)$ if k is chosen large enough (see (1.1)), which implies $c_t > 1/2$. To derive Conjecture CC, we use the Tu–Deng Conjecture with 2^k-1-t. Noting that $\sum_{j\in\mathbb{Z}}\beta_{t,k,j} = t+1$, we obtain

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

Letting $k \to \infty$ and using (1.2) we obtain $\tilde{c}_t \le 1/2$. □

Remark. The quantities $\beta_{t,k,j}$ are linked to divisibility by powers of two in Pascal's triangle: We define (see e.g. [15])

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

(Here $\nu_2(m)$ denotes the largest j such that 2^j divides m.) Then for $k \ge 1$, $0 \le t < 2^k$ and $j \ge 0$ 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 $0 \le k \le n$. 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 Theorem 1.1

Let us define the values

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

and

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

By equation (2.1) the Tu–Deng Conjecture states that $P_{t,k} = \Gamma_{t,k,1}/2^k \leq 1/2$.

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

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

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

Proposition 3.1. *Let $k \geq 0$ and j be integers. Then*

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

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

Proof of Proposition 3.1. The last claim $\beta_{t,k,j} = 0$ for $|j| > k$ follows by induction. The first two statements are clear, and so is the case $t = 0$. We note the almost trivial identities $(2t)^{\complement}_{k+1} = 2t^{\complement}_k + 1$, $(2t+1)^{\complement}_{k+1} = 2t^{\complement}_k$ and $(t+1)^{\complement}_k = t^{\complement}_k - 1$, which hold for all t and k. We calculate for $1 \leq t < 2^k$:

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

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

$$\begin{aligned}
\beta_{2t+1,k+1,j} &= \bigl|\bigl\{a \leq 2t+1 : w\bigl(a + (2t+1)^{\complement}_{k+1}\bigr) - w(a) = j\bigr| \\
&= \bigl|\bigl\{a \leq t : w\bigl(2a + 2t^{\complement}_k\bigr) - w(2a) = j\bigr| \\
&+ \bigl|\bigl\{a \leq t : w\bigl(2a + 2t^{\complement}_k + 1\bigr) - w(2a+1) = j\bigr| \\
&= 2\beta_{t,k,j}
\end{aligned}$$

and

$$\begin{aligned}
\beta_{(2t)^{\complement}_{k+1},k+1,j} &= \bigl|\bigl\{a \leq 2t^{\complement}_k + 1 : w(a + 2t) - w(a) = j\bigr\}\bigr| \\
&= \bigl|\bigl\{a \leq t^{\complement}_k : w(2a + 2t) - w(2a) = j\bigr\}\bigr|
\end{aligned}$$

$$\begin{aligned}
&+ \left|\left\{a \le t_k^{\complement} : w(2a+2t+1) - w(2a+1) = j\right\}\right| \\
&= 2\beta_{t_k^{\complement},k,j}.
\end{aligned}$$

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

$$\begin{aligned}
\beta_{(2t+1)_k^{\complement},k+1,j} &= \left|\left\{a \le 2t_k^{\complement} : w(a+2t+1) - w(a) = j\right\}\right| \\
&= \left|\left\{a \le t_k^{\complement} : w(2a+2t+1) - w(2a) = j\right\}\right| \\
&+ \left|\left\{a \le t_k^{\complement} - 1 : w(2a+2t+2) - w(2a+1) = j\right\}\right| \\
&= \beta_{t_k^{\complement},k,j-1} + \left|\left\{a \le (t+1)_k^{\complement} : w(a+t+1) - w(a) = j+1\right\}\right| \\
&= \beta_{t_k^{\complement},k,j-1} + \beta_{(t+1)_k^{\complement},k,j+1}
\end{aligned}$$

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

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

Clearly, we have

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

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

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

We define the bivariate generating function F:

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

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

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

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

$$
\begin{aligned}
&= 1 + \frac{x}{2}F(x,y) + \sum_{k\geq 1} x^k m_{k-1,k} + xyF(x,y) + \frac{1}{2}\sum_{\substack{k\geq 1\\ 0\leq \ell\leq 1}} x^k y^\ell m_{k-1,k+1-\ell}\\
&+ \frac{xy^2}{2}F(x,y) - \frac{1}{2}\sum_{k\geq 1} x^k y^{k+1}\\
&= 1 + \frac{x}{2}(1+y)^2 F(x,y) - \frac{xy^2}{2(1-xy)},
\end{aligned}
$$

therefore

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

Moreover, we define

$$\widetilde{m}_{k,j} \coloneqq \frac{1}{2^k}\sum_{t=0}^{2^k-1} \beta_{t^{\text{ↄ}}_k,k,-j} = m_{k,-j}$$

and

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

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

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

Therefore

$$
\begin{aligned}
\widetilde{F}(x,y) &= \sum_{\substack{\ell\geq 0\\ k=0}} \widetilde{m}_{0,-\ell} y^\ell + \sum_{\substack{\ell\geq 0\\ k\geq 1}} x^k y^\ell \left(\frac{1}{2}\widetilde{m}_{k-1,k-\ell-1} + \widetilde{m}_{k-1,k-\ell} + \frac{1}{2}\widetilde{m}_{k-1,k-\ell+1} - \frac{1}{2}\delta_{k-\ell,1}\right)\\
&= 1 + \frac{x}{2}\widetilde{F}(x,y) + \sum_{k\geq 0} x^{k+1}\widetilde{m}_{k,k+1} + xy\widetilde{F}(x,y) + \sum_{\substack{k\geq 0\\ 0\leq\ell\leq 1}} x^{k+1}y^\ell \widetilde{m}_{k,k+2-\ell}\\
&+ \frac{xy^2}{2}\widetilde{F}(x,y) - \frac{1}{2}\sum_{\ell\geq 0} x^{\ell+1}y^\ell\\
&= 1 + \frac{x}{2}(1+y)^2\widetilde{F}(x,y) - \frac{x}{2(1-xy)}
\end{aligned}
$$

therefore

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

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

We define

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

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

We have

$$\begin{aligned} M_{k,\ell} &= \frac{1}{2^k} \sum_{i \geq k-\ell} \sum_{t=0}^{2^k-1} \left(\beta_{t,k,i} + \beta_{t^{\text{ↄ}}_k,k,-i}\right) = \sum_{i \geq k-\ell} \left(m_{k,i} + \widetilde{m}_{k,i}\right) \\ &= \sum_{k=0}^{\ell} \left(m_{k,k-j} + \widetilde{m}_{k,k-j}\right) = \sum_{j=0}^{\ell} \left[x^k y^j\right] \left(F(x,y) + \widetilde{F}(x,y)\right) \\ &= \left[x^k y^\ell\right] G(x,y), \end{aligned}$$

where

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

The first moment of $t \mapsto \Gamma_{t,k,1}$ is therefore given by $M_{k,k-1} = \left[x^k y^{k-1}\right] G(x,y)$.

Proposition 3.2. *We have for $k \geq 1$*

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

Proof. The idea of the proof is to extract the (shifted) diagonal $G(x,y)$. First note that $[x^k y^{k-1}]G(x,y) = [x^k y^k] y G(x,y)$. The diagonal is given by $\Delta(yG)(z) := \sum_{k \geq 1} M_{k,k-1} z^k$. The computation is then a routine exercise in enumerative combinatorics (see e.g. [16, Chapter 6.3]) and can be automatized to a great extend using computer algebra We do not present this standard argument here. More details can be found in the accompanying Maple Worksheet [1] implementing the manipulations on the power series using the gfun package [14].

We get

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

from which we extract coefficients noting $\sum_{n \geq 0} \binom{2n}{n} z^n = (1-4z)^{-1/2}$. 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

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

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

Proposition 3.3. *We have*

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

where

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

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

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

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

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

and

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

Proposition 3.4. *We have the asymptotic expansion*

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

Corollary 3.5. *Let X_k be the discrete random variable defined by $X_k(t) = P_{t,k} = |S_{t,k}|/2^k$, where $1 \le t < 2^k - 1$, 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*

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

The proof of this statement is straightforward and is omitted. Finally, in an analogous manner as in [9, Section 4.4] the proof of Theorem 1.1 is completed by Chebyshev's inequality.

The remaining part of this paper is devoted to the proofs of Propositions 3.3 and 3.4.

3.1. **Proof of Proposition 3.3.**

Proof of Proposition 3.3. 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 $k \geq 1$ and $\ell, m \geq 0$:

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

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

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

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

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

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

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

$$C(x,y,z) = \sum_{k,\ell,m\geq 0} c_{k,\ell,m} x^k y^\ell z^m$$

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

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

we obtain

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

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

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

Finally, we have

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

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

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

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 [9].

Define

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

We have for $k\ge 1$

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

Moreover

$$\begin{aligned}
b'_{k,\ell,m} &= \sum_{0\le t<2^{k-1}} \beta_{2t,k,k-\ell}\beta_{(2t+1)^{\text{ɔ}}_k,k,-k+m}\\
&+ \sum_{0\le t<2^{k-1}-1} \beta_{2t+1,k,k-\ell}\beta_{(2(t+1))^{\text{ɔ}}_k,k,-k+m}\\
&= \sum_{0\le t<2^{k-1}} \bigl(\beta_{t,k-1,k-\ell-1} + \beta_{t-1,k-1,k-\ell+1}\bigr)\bigl(\beta_{t^{\text{ɔ}}_{k-1},k-1,-k+m-1} + \beta_{(t+1)^{\text{ɔ}}_{k-1},k-1,-k+m+1}\bigr)\\
&+ 4\sum_{0\le t<2^{k-1}-1} \beta_{t,k-1,k-\ell}\beta_{(t+1)^{\text{ɔ}}_{k-1},k-1,-k+m}\\
&= a'_{k-1,\ell,m-2} + b'_{k-1,\ell-2,m-2} + b'_{k-1,\ell,m} + c'_{k-1,\ell-2,m} + 4b'_{k-1,\ell-1,m-1}
\end{aligned}$$

and

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

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

We define generating functions

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

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

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

moreover

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

We obtain

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

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

and

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

It follows that

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

and therefore

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

which gives

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

Define

$$a''_{k,\ell,m} = \sum_{0\le t<2^k} \beta_{t^{\text{ↄ}}_k,k,-k+\ell}\beta_{t,k,k-m}$$

and

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

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

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

and we have

$$\begin{aligned}
a'''_{k,\ell,m} &= \sum_{0\le t<2^{k-1}} \beta_{(2t)^{\circ}_k,k,-k+\ell}\beta_{(2t)^{\circ}_k,k,-k+m} + \sum_{0\le t<2^{k-1}} \beta_{(2t+1)^{\circ}_k,k,-k+\ell}\beta_{(2t+1)^{\circ}_k,k,-k+m}\\
&= 4 \sum_{0\le t<2^{k-1}} \beta_{t^{\circ}_{k-1},k-1,-(k-1)+\ell-1}\beta_{t^{\circ}_{k-1},k-1,-(k-1)+m-1}\\
&+ \sum_{0\le t<2^{k-1}} \bigl(\beta_{t^{\circ}_{k-1},k-1,-(k-1)+\ell-2} + \beta_{(t+1)^{\circ}_{k-1},k-1,-(k-1)+\ell}\bigr)\\
&\qquad \times \bigl(\beta_{t^{\circ}_{k-1},k-1,-(k-1)+m-2} + \beta_{(t+1)^{\circ}_{k-1},k-1,-(k-1)+m}\bigr)\\
&= 4a'''_{k-1,\ell-1,m-1} + a'''_{k-1,\ell-2,m-2} + b'''_{k-1,\ell-2,m} + c'''_{k-1,\ell,m-2} + a'''_{k-1,\ell,m}\\
&- \beta_{0^{\circ}_{k-1},k-1,-(k-1)+\ell}\beta_{0^{\circ}_{k-1},k-1,-(k-1)+m}\\
&= 4a'''_{k-1,\ell-1,m-1} + a'''_{k-1,\ell-2,m-2} + b'''_{k-1,\ell-2,m} + c'''_{k-1,\ell,m-2} + a'''_{k-1,\ell,m}\\
&- 2^{2(k-1)}\delta_{k,\ell+1}\delta_{k,m+1}
\end{aligned}$$

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

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

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

and that

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

Therefore

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

and

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

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

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

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

$$\begin{aligned} M^{(2)}_{k,\ell,m} &= \sum_{\substack{i\leq \ell \\ j\leq m}} \sum_{0\leq t<2^k} \gamma_{t,k,k-i}\gamma_{t,k,k-j} \\ &= \sum_{\substack{i\leq \ell \\ j\leq m}} \left(a_{k,i,j} + a'_{k,i,j} + a''_{k,i,j} + a'''_{k,i,j}\right) \\ &= \left[x^k y^\ell z^m\right] \frac{1}{1-y}\frac{1}{1-z}\left(A + A' + A'' + A'''\right)(x,y,z). \end{aligned}$$

□

3.2. **Proof of Proposition 3.4.** We write

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

where

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

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

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

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

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

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 [9]. We copy the following two lemmata. (We denote the open disk with radius δ around $a\in\mathbb{C}$ by $B_\delta(a)$.)

Lemma 3.6. *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*

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

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

$$[x^n]\,F(x,y,z)=\frac{1}{(1-y)(1-z)}\left(\frac{-G(f(y,z),y,z)}{H_x(f(y,z),y,z)}f(y,z)^{-n-1}+O\big(8^{(1-\varepsilon)n}\big)\right)\tag{3.1}$$

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

$$[x^n]\,F(x,y,z)=O(8^{(1-\varepsilon)n})\tag{3.2}$$

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

$$\begin{aligned}f(y,z)=&\frac{1}{8}-\frac{1}{8}(y-1)-\frac{1}{8}(z-1)+\frac{3}{32}(y-1)^2+\frac{3}{32}(z-1)^2+\frac{1}{8}(y-1)(z-1)\\&-\frac{1}{16}(y-1)^3-\frac{1}{16}(z-1)^3-\frac{3}{32}(y-1)^2(z-1)-\frac{3}{32}(y-1)(z-1)^2\\&+\frac{5}{128}(y-1)^4+\frac{5}{128}(z-1)^4+\frac{1}{16}(y-1)^3(z-1)+\frac{1}{16}(y-1)(z-1)^3\\&+\frac{13}{192}(y-1)^2(z-1)^2+O\big(|y-1|^5+|z-1|^5\big)\end{aligned}$$

and

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

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

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

Lemma 3.7. *We have*

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

and for $k \geq 0$

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

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 $1 \pm i\delta$.

By (3.1) and (3.2) the integral along γ_2, is of order $O(8^{(1-\varepsilon)n})$ 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

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

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

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

where

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

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

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

from which it follows that

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

Lemma 3.6 implies

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

so that

$$-(n+1)\,g_n(s,t) = \log 8^{n+1} - \frac{s^2}{4} - \frac{t^2}{4} + i\frac{s^3}{4\sqrt{n}} + i\frac{t^3}{4\sqrt{n}} - \frac{s^2}{4n} - \frac{t^2}{4n} + \frac{7s^4}{32n} + \frac{7t^4}{32n} + \frac{s^2t^2}{48n} + O\left(\frac{|s|^5+|t|^5}{n^{3/2}}\right). \tag{3.3}$$

As a next step we want to use the expansion $e^x = 1 + x + x^2/2 + O(x^3)$ 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 [9] 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 $\gamma_{2,1}$ 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 $\gamma_{2,2}$ which connects $1 + i\delta A_n$ and $1 + i\delta$ by a straight line, and a symmetric part $\gamma_{2,3}$ that connects $1 - i\delta A_n$ and $1 - i\delta$ by a straight line.

Due to (3.3) we get the bound

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

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

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

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 $\gamma_{2,1}$. On this part we may use the expansion of e^x to obtain

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

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

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

Finally by writing this as a sum of products of integrals and applying Lemma 3.7 term by term this expression equals

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

Summing up we arrive at the asymptotics

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

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 3.4. For details see the accompanying Maple worksheet [1].

References

[1] *http://dmg.tuwien.ac.at/mwallner/.*

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

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

[4] 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.

[5] 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.

[6] 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.

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

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

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] L. Spiegelhofer and M. Wallner, *An explicit generating function arising in counting binomial coefficients divisible by powers of primes*, (2016). Preprint. arXiv:1604.07089.

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

[17] 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.

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

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