Probabilistic Properties of Modular Addition (Extended abstract)

Victoria Vysotskaya

JSC «InfoTeCS», Russia
NPK «Kryptonite», Russia
vysotskaya.victory@gmail.com

Abstract

We studied the applicability of differential cryptanalysis to cryptosystems based on operation of addition modulo 2^n. We obtained an estimate (accurate up to an additive constant) of expected value of entropy H_n in rows of DDT of corresponding mapping. Moreover, the k-th moments of 2^{H_n} are explored. In particular, asymptotic inequalities that describe the behavior of values $\mathbb{E}2^{H_n}$ and $\mathbb{D}2^{H_n}$ as $n \to \infty$ were obtained. A simple analytical formula for the size of any given equivalence class was obtained. This formula helped to effectively compute the entropy distribution.

Keywords: modular addition, differential cryptanalysis, entropy of distribution.

1 Introduction

A number of cryptographic schemes use the operation of addition modulo 2^n for some $n > 1$. Denote $\mathbb{Z}_N$ the ring modulo N. The first function under consideration is $f : \mathbb{Z}_{2^n}^2 \to \mathbb{Z}_{2^n}$ defined by $f(x, y) = x \boxplus_n y$, where $\boxplus_n$ denotes addition in ring $\mathbb{Z}_{2^n}$, i.e. modulo 2^n, and $\oplus$ is bitwise exclusive-OR. We are interested in study of the function $P_n(\Delta x, \Delta f) : \mathbb{Z}_{2^n}^2 \to \mathbb{N}_0$:

$$P_n(\Delta x, \Delta f) = \frac{1}{2^{2n}} \Big| \{(x, y) \in \mathbb{Z}_{2^n}^2 : \Delta f = f(x \oplus \Delta x, y) \oplus f(x, y)\} \Big|.$$

(it is analogous to a special case of the differential probability of addition modulo 2^n studied in [1]).

In this work we study the properties of this operation through the concept of entropy. The article [2] investigated the function $2^n \cdot P_n(\Delta x, \Delta f)$, but all the results are similar in these two cases, therefore we will briefly describe what is already known.

The table of values of the function $P_n(\Delta x, \Delta f)$ is called a difference distribution table (DDT). The rows of this table are indexed by Δx and columns by Δf. In [2] it has been shown that this table has a special form: the table for addition modulo 2^{n+1} is

naturally expressed through a similar table for addition modulo 2^n. That is, if the matrix for $P_n(\Delta x, \Delta f)$ has the form

$$P_n = \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$$

then matrix P_{n+1} has form

$$P_{n+1} = \frac{1}{2}\left[\begin{array}{cc|cc} 2A & B & 0 & B \\ C & D & C & D \\ \hline 0 & B & 2A & B \\ C & D & C & D \end{array}\right]$$

It was also shown that $A = D$ and $B = C$. This led to the following recurrent representation for the matrix P_n:

$$P_n = \left[\begin{array}{c|c} A_n & B_n \\ \hline B_n & A_n \end{array}\right], \tag{1}$$

where

$$A_n = \frac{1}{2}\left[\begin{array}{c|c} 2A_{n-1} & B_{n-1} \\ \hline B_{n-1} & A_{n-1} \end{array}\right], \quad B_n = \frac{1}{2}\left[\begin{array}{c|c} 0 & B_{n-1} \\ \hline B_{n-1} & A_{n-1} \end{array}\right]. \tag{2}$$

Rows of P_n with the same but maybe permuted elements are called *equivalent* (obviously, equivalent rows have the same entropy). It was shown in [2] that one can associate a polynomial of degree not greater than $2n$ with each of equivalence classes. These polynomials can be constructed from the parameters of the corresponding equivalence class. So one can enumerate all the distinct distributions in time proportional to their number, that is

$$\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} = O\left(2^{3{,}7007\sqrt{n}}\right) \text{ as } n \to \infty.$$

When considering $P_n(\Delta x, \Delta f)$ as a part of a cryptosystem from the point of view of differential cryptanalysis the following problem arises: for a given (or randomly chosen) Δx it is necessary to determine the minimum cardinality K_c of the set of numbers $\{\Delta f_1, \ldots, \Delta f_{K_c}\}$ such that

$$\sum_{i=1}^{K_c} P_n(\Delta x, \Delta f_i) \geqslant c,$$

where c, $0 < c \leqslant 1$, is some fixed constant. The value of K_c corresponds to the "degree of branching", that is, the coefficient by which the number of considered variants is multiplied when moving to the next round of the cryptosystem. In practice, it was found that for the distributions in DDT rows the described value $K_{\frac{1}{2}}$ does not exceed 2^H, where H is the entropy of this distribution (this is not true in the general case, for arbitrary distributions, it is enough to consider an example distribution $\{\frac{1}{4}, \frac{1}{2^n}, \ldots, \frac{1}{2^n}\}$ for sufficiently large n).

In this article we obtained an estimate (accurate up to an additive constant) of expected value of entropy H_n in rows of DDT and asymptotic inequalities describing the behavior of values $\mathbb{E}2^{qH_n}$ and $\mathbb{D}2^{qH_n}$ as $n \to \infty$ (for $q \in \mathbb{N}$). We also implemented the equivalence class enumeration algorithm and justified (for some practical values of n) our assumption concerning closeness of 2^{H_n} and $K_{1/2}$. The theoretically estimated values of moments of 2^{H_n} also turned out to be close to the real ones.

We also introduced a simple analytical formula for the size of any given equivalence class was obtained and used it, in particular, to effectively compute the entropy distribution.

2 Properties of DDT row entropy

By definition the entropy in the i-th row of matrix P_n may be found according to the formula

$$H_n^i = -\sum_{j=0}^{2^n-1} P_n(i,j)\log_2 P_n(i,j),\ i = 0,\dots,2^n-1.$$

For convenience we denote

$$\alpha_n^i = \sum_{j=0}^{2^{n-1}-1} A_n(i,j), \quad \beta_n^i = \sum_{j=0}^{2^{n-1}-1} B_n(i,j)$$

and

$$\alpha_n = \sum_{i=0}^{2^{n-1}-1} \alpha_n^i, \quad \beta_n = \sum_{i=0}^{2^{n-1}-1} \beta_n^i.$$

Lemma 1.

$$H_{n+1}^i = \begin{cases} H_n^{i \bmod 2^n} + 1, & \text{if } \ i \in [2^{n-1}, 2^n-1] \cup [3\cdot 2^{n-1}, 2^{n+1}-1], \\ H_n^{i \bmod 2^n} + \beta_n^{i \bmod 2^n}, & \text{if } \ i \in [0, 2^{n-1}-1] \cup [2^n, 3\cdot 2^{n-1}-1]. \end{cases}$$

Proof. From (1) and (2) it is clear that for $i \in [2^{n-1}, 2^n-1] \cup [3\cdot 2^{n-1}, 2^{n+1}-1]$ the i-th row has the form $\frac{1}{2}\begin{bmatrix} a & b & a & b \end{bmatrix}$ and thus the entropy can be written as

$$H_{n+1}^i = -2\cdot \sum_{j=0}^{2^n-1} \frac{P_n(i,j)}{2}\log_2 \frac{P_n(i,j)}{2} = -\sum_{j=0}^{2^n-1} P_n(i,j)_{i,j}\log_2 \frac{P_n(i,j)}{2} =$$
$$= -\sum_{j=0}^{2^n-1} P_n(i,j)\log_2 P_n(i,j) + \sum_{j=0}^{2^n-1} P_n(i,j)\log_2 2 = H_n^{i \bmod 2^n} + 1.$$

On the other hand, for $i \in [0, 2^{n-1}-1] \cup [2^n, 3\cdot 2^{n-1}-1]$ we have the row of form $\frac{1}{2}\begin{bmatrix} 2a & b & 0 & b \end{bmatrix}$ and thus

$$H_{n+1}^i = -\sum_{j=0}^{2^{n-1}-1} P_n(i,j)\log_2 P_n(i,j) - 2\cdot \sum_{j=2^{n-1}}^{2^n-1} \frac{P_n(i,j)}{2}\log_2 \frac{P_n(i,j)}{2} =$$
$$= -\sum_{j=0}^{2^{n-1}-1} P_n(i,j)\log_2 P_n(i,j) - \sum_{j=2^{n-1}}^{2^n-1} P_n(i,j)\log_2 P_n(i,j) + \sum_{j=2^{n-1}}^{2^n-1} P_n(i,j) =$$
$$= H_n^{i \bmod 2^n} + \beta_n^{i \bmod 2^n}.$$

□

Lemma 2. *For every $n \geqslant 1$ holds $\mathbb{E}H_{n+1} = \frac{n}{2} + \frac{\beta_n}{2^n} + \dots + \frac{\beta_3}{8} + \frac{\beta_2}{4}$.*

Proof. Taking into account the previous lemma, we can write:

$$\mathbb{E}H_{n+1} = \frac{1}{2^{n+1}} \sum_{i=0}^{2^{n+1}-1} H_{n+1}^i = \frac{1}{2^n} \sum_{i=0}^{2^{n-1}-1} (H_n^i + \beta_n^i) + \frac{1}{2^n} \sum_{i=2^{n-1}}^{2^n-1} (H_n^i + 1) =$$
$$= \frac{1}{2^n} \sum_{i=0}^{2^n-1} H_n^i + \frac{1}{2^n} \sum_{i=0}^{2^{n-1}-1} \beta_n^j + \frac{1}{2} = \mathbb{E}H_n + \frac{\beta_n}{2^n} + \frac{1}{2}.$$

It remains to "unroll" this equality and note that $H_1 = 0$ and $\beta_1 = 0$. □

Lemma 3. *For every $n \geqslant 1$ holds $\beta_n = \frac{1}{3} \cdot 2^{n-1}(1 - 4^{1-n})$.*

Proof. Obviously, $\alpha_n^i + \beta_n^i = 1$, so $\alpha_n + \beta_n = 2^{n-1}$. From (2) it follows that

$$\beta_{n+1} = \beta_n + \frac{\alpha_n}{2}.$$

From the last two equalities it follows that

$$\beta_{n+1} = 2^{n-2} + \frac{\beta_n}{2}.$$

Unrolling this equality we come to

$$\begin{aligned}\beta_{n+1} = 2^{n-2} + \frac{\beta_n}{2} = 2^{n-2} + \frac{1}{2}\Big(\beta_{n-1} + \frac{\alpha_{n-1}}{2}\Big) = 2^{n-2} + 2^{n-4} + \frac{\beta_{n-1}}{4} = \\ = 2^{n-2} + 2^{n-4} + \cdots + 2^{-n} = \frac{2^{n-2}\big(1 - \big(2^{-2}\big)^n\big)}{1 - 2^{-2}} = \frac{1}{3} \cdot 2^n(1 - 4^{-n}).\end{aligned}$$

□

Theorem 1. *$\mathbb{E}H_n = \frac{2}{3}n + O(1)$ as $n \to \infty$.*

Proof. Let us substitute values obtained in Lemma 3 into the representation of $\mathbb{E}H_{n+1}$ obtained in Lemma 2:

$$\mathbb{E}H_{n+1} = \frac{n}{2} + \frac{1}{6}(1 - 4^{1-n}) + \cdots + \frac{1}{6}(1 - 4^{-1}) = \frac{n}{2} + \frac{n}{6} + \frac{1}{3}(1 - 4^{1-n}) = \frac{2}{3}n + O(1).$$

So $\mathbb{E}H_n = \frac{2}{3}(n-1) + O(1) = \frac{2}{3}n + O(1)$. □

Now we will consider the q-th moment of a random variable 2^{H_n}:

$$\mathbb{E}\big(2^{H_n}\big)^q = \mathbb{E}2^{qH_n} = \frac{1}{2^n}\sum_{i=0}^{2^n-1} 2^{qe_{n,i}} = \frac{1}{2^n}\sum_{i=0}^{2^n-1} Q^{e_{n,i}},$$

where $e_{n,i}$ is the entropy in i-th row of matrix P_n and Q denotes 2^q. To avoid multilevel exponentiation we will use the notation $\mathcal{Q}(x) = Q^x$.

Corollary 1. *$\mathbb{E}2^{qH_n} = \Omega\left(Q^{\frac{2}{3}n}\right)$.*

Proof. It is sufficient to use the inequality of arithmetic and geometric means and the result of Theorem 1:

$$\mathbb{E}2^{qH_n} = \frac{1}{2^n}\sum_{i=0}^{2^n-1} 2^{qe_{n,i}} \geqslant \sqrt[2^n]{\prod_{k=1}^{2^n} 2^{qe_{n,i}}} = 2^{\mathbb{E}(qH_n)} = 2^{\frac{2}{3}qn} \cdot \Omega(1) = \Omega\left(Q^{\frac{2}{3}n}\right).$$

□

Lemma 4. *For $i = 0, \ldots, 2^{n-1} - 1$*

$$\beta_n^i = \begin{cases} 0, & \text{if } i = 0, \\ 2^{-(n-1-\lfloor \log_2 i \rfloor)}, & \text{otherwise.} \end{cases} \tag{3}$$

Proof. Let us prove by induction. For $n = 1$ the proposition is obvious as $B_1 = \begin{bmatrix} 0 \end{bmatrix}$. Now let's suppose that it is also true for β^i_{n-1}, $i = 0, \ldots, 2^{n-2} - 1$ and let us prove it for β^i_n.

For $2^{n-2} \leqslant i \leqslant 2^{n-1} - 1$ from (2) we get $\beta^i_n = \frac{1}{2}$ as the sum in any row of matrix $\left[\begin{array}{c|c} B_{n-1} & A_{n-1} \end{array}\right]$ is 1. This agrees with (3) as $\lfloor \log_2 i \rfloor = n - 2$.

For $0 \leqslant i \leqslant 2^{n-2} - 1$ from (2) we have

$$\beta^i_n = \frac{1}{2}\beta^i_{n-1}.$$

and by the inductive hypothesis we come to (3). □

Remark. *The vector of values β^i_n has the following form:*

$$\left[0, \underbrace{\frac{1}{2^{n-1}}}_{1}, \underbrace{\frac{1}{2^{n-2}}, \frac{1}{2^{n-2}}}_{2}, \ldots, \underbrace{\frac{1}{8}, \ldots, \frac{1}{8}}_{2^{n-4}}, \underbrace{\frac{1}{4}, \ldots, \frac{1}{4}}_{2^{n-3}}, \underbrace{\frac{1}{2}, \ldots, \frac{1}{2}}_{2^{n-2}}\right].$$

For convenience we extend the definition (3) for $2^{n-1} \leqslant i \leqslant 2^n - 1$. Then according to Lemma 1,

$$e_{n,i} = \beta^{i \bmod 2^{n-1}}_{n-1} + \beta^{i \bmod 2^{n-2}}_{n-2} + \cdots + \beta^{i \bmod 4}_2.$$

Moreover, obviously, $e_{1,0} = e_{1,1} = 0$. For $k \in \{0, \ldots, n-2\}$ let us introduce sets

$$Z_k = \left\{ i \in \mathbb{Z} : 2^{n-k-1} \leqslant i \leqslant 2^{n-k} - 1 \right\}.$$

The set Z_k consists of integers which binary representation has the form $\underbrace{0 \ldots 0}_{k}\, 1\, \underbrace{* \cdots *}_{n-k-1}$.

Let us denote $\omega_n = \sum_{i=0}^{2^n-1} \mathcal{Q}(e_{n,i})$. Then

$$\begin{aligned}
\omega_n = \sum_{i=0}^{2^n-1} \mathcal{Q}(e_{n,i}) &= \sum_{k=0}^{n-1} \sum_{i' \in Z_k} \mathcal{Q}\left(\sum_{c=1}^{k} \beta^{i' \bmod 2^{n-c}}_{n-c} + e_{n-k,i'} \right) + 1 = \\
&= \sum_{k=0}^{n-1} \sum_{i' \in Z_k} \mathcal{Q}\left(\sum_{c=1}^{k} \beta^{i' \bmod 2^{n-c}}_{n-c} \right) \mathcal{Q}(e_{n-k,i'}) + 1 = \\
&= \sum_{k=0}^{n-1} \mathcal{Q}\left(\sum_{c=0}^{k-1} 2^{-c} \right) \sum_{i' \in Z_k} \mathcal{Q}(e_{n-k,i'}) + 1 = \sum_{k=0}^{n-1} \mathcal{Q}\left(2 - 2^{-k+1}\right) \frac{\omega_{n-k}}{2} + 1.
\end{aligned}$$

Obviously,

$$\mathbb{E}\left(2^{H_n}\right)^q = \frac{\omega_n}{2^n}. \tag{4}$$

Thus we need to investigate the following recurrence relation:

$$f'(n) = \sum_{\ell=1}^{n-1} f'(\ell) \cdot \mathcal{Q}(2 - 2^{-n+\ell+1}) + 2, \tag{5}$$

First, we compare it with the similar relation:

$$\begin{aligned}
f(n) &= \sum_{\ell=1}^{n-1} f(\ell) \cdot \mathcal{Q}(2 - 2^{-n+\ell+1}), n \geqslant 2 \\
f(1) &= 2.
\end{aligned} \tag{6}$$

Let us denote $\Delta(n) = f'(n) - f(n)$.

Lemma 5. $\Delta(n) \leqslant f(n)$.

Proof. Let us prove by induction. Obviously,

$$0 = \Delta(1) \leqslant f(1) = 2.$$

Suppose the proposition is true for all $\ell \leqslant n$ (i.e. $\Delta(\ell) \leqslant f(\ell)$) and write down

$$f(n+1) = \sum_{\ell=2}^{n} f(\ell) + \mathcal{Q}(2 - 2^{-n+\ell+1}) f(1),$$
$$\Delta(n+1) = \sum_{\ell=2}^{n} \Delta(\ell) + \mathcal{Q}(2 - 2^{-n+\ell+1}) \Delta(1) + 2.$$

For $n \geqslant 2$ we have $\mathcal{Q}(2 - 2^{-n+3}) \geqslant 1$, from which and the inductive hypothesis follows:

$$\Delta(n+1) \leqslant \sum_{\ell=2}^{n} f(\ell) + \mathcal{Q}(2 - 2^{-n+\ell+1}) \Delta(1) + 2 \leqslant$$
$$\leqslant \sum_{\ell=2}^{n} f(\ell) + 0 + 2 \leqslant \sum_{\ell=2}^{n} f(\ell) + \mathcal{Q}(2 - 2^{-n+\ell+1}) f(1) = f(n+1),$$

and it is the required inequality. □

With the use of Lemma 5 we estimate $f'(n)$ as

$$f(n) \leqslant f'(n) = f(n) + \Delta(n) \leqslant 2f(n),$$

and will work with homogeneous equation (6).

Let us note that coefficients $\mathcal{Q}(2 - 2^{-n+\ell+1}) = Q^{2-2^{-n+\ell+1}}$ are bounded from above by the number $\mathcal{Q}(2)$. Then let us consider the next family of recurrence relations:

$$\widehat{f}_k(n) = \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) \widehat{f}_k(\ell) + \mathcal{Q}(2) \sum_{\ell=1}^{n-k-1} \widehat{f}_k(\ell),$$
$$\widehat{f}_k(1) = 2,$$

solutions to which bound $f(n)$ from above. Denote

$$\widehat{F}_k(n) = \sum_{\ell=1}^{n-1} \widehat{f}_k(\ell). \tag{7}$$

Then

$$\widehat{F}_k(n) - \widehat{F}_k(n-1) = \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) \big(\widehat{F}_k(\ell) - \widehat{F}_k(\ell-1)\big) + \mathcal{Q}(2) \widehat{F}_k(n-k-1), \tag{8}$$
$$\widehat{F}_k(1) = 2.$$

Note that this recurrence relation has constant "length" and can be solved using well-known methods. Let us first find the form of the characteristic polynomial corresponding

to this relation:

$$\begin{aligned}\lambda^{k+1}-\lambda^k &= \sum_{\ell=n-k}^{n-1}(\lambda^{\ell-n+k+1}-\lambda^{\ell-n+k})\mathcal{Q}(2-2^{-n+\ell+1})+\mathcal{Q}(2)= \\ &= \sum_{\ell=n-k}^{n-1}\lambda^{\ell-n+k+1}\mathcal{Q}(2-2^{-n+\ell+1})-\sum_{\ell=n-k}^{n-1}\lambda^{\ell-n+k}\mathcal{Q}(2-2^{-n+\ell+1})+\mathcal{Q}(2)= \\ &= \sum_{\ell=n-k}^{n-1}\lambda^{\ell-n+k+1}\mathcal{Q}(2-2^{-n+\ell+1})-\sum_{\ell=n-k-1}^{n-2}\lambda^{\ell-n+k+1}\mathcal{Q}(2-2^{-n+\ell+2})+\mathcal{Q}(2)= \\ &= \mathcal{Q}(1)\lambda^{k+1-1}-\mathcal{Q}(2-2^{-k-1+2})+ \\ &+ \sum_{\ell=n-k}^{n-2}\lambda^{\ell-n+k+1}\left(\mathcal{Q}(2-2^{-n+\ell+1})-\mathcal{Q}(2-2^{-n+\ell+2})\right)+\mathcal{Q}(2).\end{aligned}$$

Thus the final form of the characteristic polynomial is

$$\begin{aligned}\widehat{H}_k(\lambda) = \lambda^{k+1}-(1+\mathcal{Q}(1))\lambda^k-\sum_{\ell=0}^{k-2}\mathcal{Q}(2)\left(\mathcal{Q}(-2^{-k+\ell+1})-\mathcal{Q}(-2^{-k+\ell+2})\right)\lambda^{\ell+1}- \\ -\mathcal{Q}(2)\left(1-\mathcal{Q}(-2^{-k+1})\right).\end{aligned}$$

We will denote $\widehat{\varphi}_s$ the coefficient of λ^s. Let $y_1,\ldots,y_{k+1}$ be the roots of this polynomial. It is known [3] that the solution to the equation (8) has form

$$\widehat{F}_k(n)=\widehat{\gamma}_1 y_1^n+\cdots+\widehat{\gamma}_{k+1}y_{k+1}^n \tag{9}$$

for some constant $\widehat{\gamma}_i$.

On the other hand, coefficients $\mathcal{Q}(2-2^{-n+\ell+1})$ decrease with growth of ℓ and reach the minimum value on the interval $\ell\in[1,n-k-1]$ at the point $\ell=n-k-1$, where the coefficient is $\mathcal{Q}(2-2^{-k})$. From this considerations we obtain a new family of recurrences limiting the original one from *below*:

$$\begin{aligned}\breve{f}_k(n) &= \sum_{\ell=n-k}^{n-1}\mathcal{Q}(2-2^{-n+\ell+1})\breve{f}_k(\ell)+\mathcal{Q}(2-2^{-k})\sum_{\ell=1}^{n-k-1}\breve{f}_k(\ell), \\ \breve{f}_k(1) &= 2.\end{aligned}$$

Just as it was done above we introduce

$$\breve{F}_k(n)=\sum_{\ell=1}^{n-1}\breve{f}_k(\ell). \tag{10}$$

Thus

$$\begin{aligned}&\breve{F}_k(n)-\breve{F}_k(n-1)=\sum_{\ell=n-k}^{n-1}\mathcal{Q}(2-2^{-n+\ell+1})\left(\breve{F}_k(\ell)-\breve{F}_k(\ell-1)\right)+\mathcal{Q}(2-2^{-k})\breve{F}_k(n-k-1), \\ &\breve{F}_k(1)=2.\end{aligned} \tag{11}$$

In this case the characteristic polynomial has the following form:

$$\breve{H}_k(\lambda) = \lambda^{k+1} - (1+\mathcal{Q}(1))\lambda^k - \sum_{\ell=0}^{k-2} \mathcal{Q}(2)\left(\mathcal{Q}(-2^{-k+\ell+1}) - \mathcal{Q}(-2^{-k+\ell+2})\right)\lambda^{\ell+1} - \tag{12}$$

$$- \mathcal{Q}(2)\left(\mathcal{Q}(-2^{-k}) - \mathcal{Q}(-2^{-k+1})\right). \tag{13}$$

We will denote $\breve{\varphi}_s$ the coefficient of λ^s. The solution to the equation (11) has the following form:

$$\breve{F}_k(n) = \breve{\gamma}_1 y_1^n + \cdots + \breve{\gamma}_{k+1} y_{k+1}^n, \tag{14}$$

where $y_1, \ldots, y_{k+1}$ are the roots of $\breve{H}_k(\lambda)$ and $\breve{\gamma}_i$ are some constants.

Consider the following family of polynomials ($t \in [0,1]$):

$$\widehat{u}_t(\lambda) = \lambda^{k+1} - (1+Q)\lambda^k - t\cdot\widehat{\varphi}_{k-1}\lambda^{k-1} - \cdots - t\cdot\widehat{\varphi}_0 \tag{15}$$

and the similar one for $\breve{\varphi}_i$ (denote it $\breve{u}_t(\lambda)$). We will prove the following lemmas describing these families (note that $\breve{\varphi}_i = \widehat{\varphi}_i$ for $i \geqslant 1$).

Lemma 6. *For every $t \in [0,1]$ the polynomials $\widehat{u}_t(\lambda)$ and $\breve{u}_t(\lambda)$:*

(a) have no root in the annulus $1 < |\lambda| \leqslant 2$, if $Q = 2$;

(b) have no root λ such that $|\lambda| = \frac{Q}{2} + 1$, if $Q > 2$.

Proof. We prove the case (a) by contradiction. Assume that $\widehat{u}_t(\lambda)$ has a root λ such that $1 < |\lambda| \leqslant 2$. Then taking absolute values in both parts in the equality

$$\lambda^{k+1} - t\cdot\widehat{\varphi}_{k-1}\lambda^{k-1} - \cdots - t\cdot\widehat{\varphi}_0 = 3\lambda^k$$

and applying the triangle inequality, we get

$$|\lambda|^{k+1} + t\cdot\widehat{\varphi}_{k-1}|\lambda|^{k-1} + \cdots + t\cdot\widehat{\varphi}_0 \geqslant 3|\lambda|^k.$$

Then

$$|\lambda|^{k-1}\left(|\lambda|^2 - 3|\lambda| + t\cdot\widehat{\varphi}_{k-1}\right) \geqslant -t\cdot\widehat{\varphi}_{k-2}|\lambda|^{k-2} - \cdots - t\cdot\widehat{\varphi}_0.$$

Since the branches of the parabola $y(|\lambda|) = |\lambda|^2 - 3|\lambda| + t\cdot\widehat{\varphi}_{k-1}$ are directed upwards, it reaches its maximum on one of the boundaries of the considered segment. In our case

$$y(1) = y(2) = -2 + t\cdot\widehat{\varphi}_{k-1}.$$

That is,

$$|\lambda|^{k-1}(-2 + t\cdot\widehat{\varphi}_{k-1}) \geqslant -t\cdot\widehat{\varphi}_{k-2}|\lambda|^{k-2} - \cdots - t\cdot\widehat{\varphi}_0.$$

Dividing by $|\lambda|^{k-1}$ we get

$$-2 \geqslant -t\cdot\widehat{\varphi}_{k-1} - t\cdot\widehat{\varphi}_{k-2}|\lambda|^{-1} - \cdots - t\cdot\widehat{\varphi}_0|\lambda|^{-k+1}.$$

Noting that simultaneously $t \leqslant 1$ by premise and $|\lambda|^{-1} < 1$ in the considered annulus, we arrive at:

$$2 < \widehat{\varphi}_{k-1} + \widehat{\varphi}_{k-2} + \cdots + \widehat{\varphi}_0. \tag{16}$$

At the same time it is easy to prove that for $Q = 2$

$$\widehat{\varphi}_{k-1} + \widehat{\varphi}_{k-2} + \cdots + \widehat{\varphi}_0 = 2,$$

so we have come the contradiction with (16). The same line of reasoning works for $\breve{u}_t(\lambda)$ except that instead of the last equality we get strict inequality.

We turn to the case (b): $Q \geqslant 4$. If under this condition there is a root such that $|\lambda| = \frac{Q}{2} + 1$, then

$$\left(\frac{Q}{2}+1\right)^{k+1} + \left(\frac{Q}{2}+1\right)^{k-1} \cdot t \cdot \widehat{\varphi}_{k-1} + \cdots + t \cdot \widehat{\varphi}_0 \geqslant (Q+1) \cdot \left(\frac{Q}{2}+1\right)^{k}.$$

As far as $\max\limits_i \widehat{\varphi}_i = \widehat{\varphi}_{k-1} = Q^{\frac{3}{2}} - Q$ and $t \leqslant 1$ then

$$\left(\frac{Q}{2}+1\right)^{k+1} - (Q+1)\left(\frac{Q}{2}+1\right)^{k} + \frac{2}{Q}\left(Q^{\frac{3}{2}} - Q\right)\left(\frac{Q}{2}+1\right)^{k} > 0$$

or

$$(\sqrt{Q}-2)^2 < 0,$$

which contradicts $Q \geqslant 4$. Absolutely the same arguments work for $\breve{u}_t(\lambda)$. □

Lemma 7. *None of the derivatives of $\widehat{u}_t(\lambda)$ and $\breve{u}_t(\lambda)$ have a root λ such that $|\lambda| = \frac{Q}{2}+1$.*

Proof. We firstly note that polynomials $\widehat{u}_t(\lambda)$ and $\breve{u}_t(\lambda)$ differ only in the constant term, which implies equality of derivatives

$$\widehat{u}_t^{(s)}(\lambda) = \breve{u}_t^{(s)}(\lambda) \text{ for all } s \geqslant 1. \tag{17}$$

So we will prove the lemma only for $\widehat{u}_t(\lambda)$.

Suppose that there exists λ, $|\lambda| = \frac{Q}{2}+1$, such that $\widehat{u}_t^{(s)}(\lambda) = 0$. Then similarly to Lemma 6 we get:

$$\begin{aligned}(k+1)^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{k+1-s} &+ (k-1)^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{k-1-s} \cdot t\widehat{\varphi}_{k-1} + \cdots + \\ &+ 0^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{-s} \cdot t\widehat{\varphi}_0 \;\geqslant\; (Q+1)k^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{k-s}\end{aligned}$$

(here $x^{\underline{s}}$ denotes $x(x-1)\dots(x-s+1)$). As noted above, $\max\limits_i \widehat{\varphi}_i = Q^{\frac{3}{2}} - Q$, so

$$(k-1)^{\underline{s}}(Q^{\frac{3}{2}} - Q) \cdot \frac{2}{Q}\left(\frac{Q}{2}+1\right)^{k-s} \;\geqslant\; (Q+1)k^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{k-s} - (k+1)^{\underline{s}} \cdot \left(\frac{Q}{2}+1\right)^{k+1-s},$$

therefore,

$$(k-s)(k-s+1)(Q^{\frac{3}{2}} - Q) \cdot \frac{2}{Q} \geqslant k(k-s+1)(Q+1) - k(k+1)\left(\frac{Q}{2}+1\right).$$

This inequality can be viewed as

$$a(Q,s)k^2 + b(Q,s)k + c(Q,s) \geqslant 0.$$

But

$$\begin{cases} a(Q,s) < 0, \text{ if } Q \neq 4, \\ a(Q,s) = 0, \text{ otherwise.} \end{cases}$$

Moreover, in the case of $Q = 4$, it is true that $b(Q,s) < 0$. Thus, there exists a certain number k starting from which this inequality will not be satisfied. □

Lemma 8. *The polynomials $\widehat{u}_t(\lambda)$ and $\breve{u}_t(\lambda)$ have exactly one root λ such that $|\lambda| > \frac{Q}{2}+1$.*

Proof. For the considered polynomials it is known [4] that their roots are continuous functions of variable t. As

$$\widehat{u}_0(\lambda) = \breve{u}_0(\lambda) = \lambda^{k+1} - (1+Q)\lambda^k,$$

these two polynomials have 0 as a root of multiplicity k and $(1+Q)$ as a root of multiplicity one.

By Lemma 6, $\widehat{u}_t(\lambda)$ and $\breve{u}_t(\lambda)$ do not have roots in the annulus $1 < |\lambda| \leqslant 2$ (for $Q = 2$) or the circle $|\lambda| = \frac{Q}{2} + 1$ (for $Q \geqslant 4$). Thus, all curves corresponding to the first k roots do not leave the circle $|\lambda| \leqslant 1$ (for $Q = 2$) and the circle $|\lambda| < \frac{Q}{2} + 1$ (for $Q \geqslant 4$). The curve corresponding to the last root does not leave the sets $|\lambda| > 2$ and $|\lambda| > \frac{Q}{2} + 1$ respectively. □

Note that $\widehat{H}_k(Q+1) < 0$ since

$$\widehat{H}_k(Q+1) = (Q+1)^{k+1} - (Q+1)\cdot(Q+1)^k - \widehat{\varphi}_{k-1}\cdot(Q+1)^{k-1} - \cdots - \widehat{\varphi}_0,$$

and $\widehat{\varphi}_i > 0,\ i \in [0, k-1]$. On the other hand, $\widehat{\varphi}_i < Q^{\frac{3}{2}} - Q$ for $i \in [0, k-1]$, so

$$\begin{aligned}\widehat{H}_k(3Q) &= (3Q)^{k+1} - (Q+1)(3Q)^k - \widehat{\varphi}_{k-1}\cdot(3Q)^{k-1} - \cdots - \widehat{\varphi}_0 > \\ &> (3Q)^{k+1} - (Q+1)(3Q)^k - (Q^{\frac{3}{2}} - Q)\frac{(3Q)^k}{3Q-1} > \\ &> \frac{(3Q)^k}{3Q-1}\left(6Q^2 - Q^{\frac{3}{2}} - 4Q - 1\right) > \frac{(3Q)^k}{3Q-1}(5Q^2 - 4Q - 1) > 0,\end{aligned}$$

for $Q \geqslant 2$. Absolutely similar statements are true for $\breve{H}_k(Q+1)$ and $\breve{H}_k(3Q)$.

Hence by the intermediate value theorem both functions $\widehat{H}_k(\lambda)$ and $\breve{H}_k(\lambda)$ have a real root on the segment $[Q+1, 3Q]$ which can be found by halving the segment. In this case, for n steps the root can be found with an accuracy $O(2^{-n})$.

Then equalities (9) and (14) take form:

$$\widehat{F}_k(n) = \widehat{\gamma}_k\widehat{y}_k^n + \widehat{\rho}_k(n), \tag{18}$$

$$\breve{F}_k(n) = \breve{\gamma}_k\breve{y}_k^n + \breve{\rho}_k(n), \tag{19}$$

where $\widehat{y}_k, \breve{y}_k$ are maximum (by the absolute value) roots of polynomials $\widehat{H}_k(\lambda)$ and $\breve{H}_k(\lambda)$ respectively (they are real, positive and lie inside $[Q+1, 3Q]$ as we have proved). $\widehat{\gamma}_k$ and $\breve{\gamma}_k$ are some real positive constants. Next, we note that if $Q = 2$ then $\widehat{\rho}_k(n) = O(1)$ and $\breve{\rho}_k(n) = O(1)$ as $n \to \infty$. If $Q \geqslant 4$ then

$$\widehat{\rho}_k(n) = O\left(\left(\frac{Q}{2}+1\right)^n\right),\quad \breve{\rho}_k(n) = O\left(\left(\frac{Q}{2}+1\right)^n\right)$$

The case $Q = 2$ is illustrated on Fig. 1.

Lemma 9. *The difference $\widehat{y}_k - \breve{y}_k$ tends to zero as $k \to \infty$.*

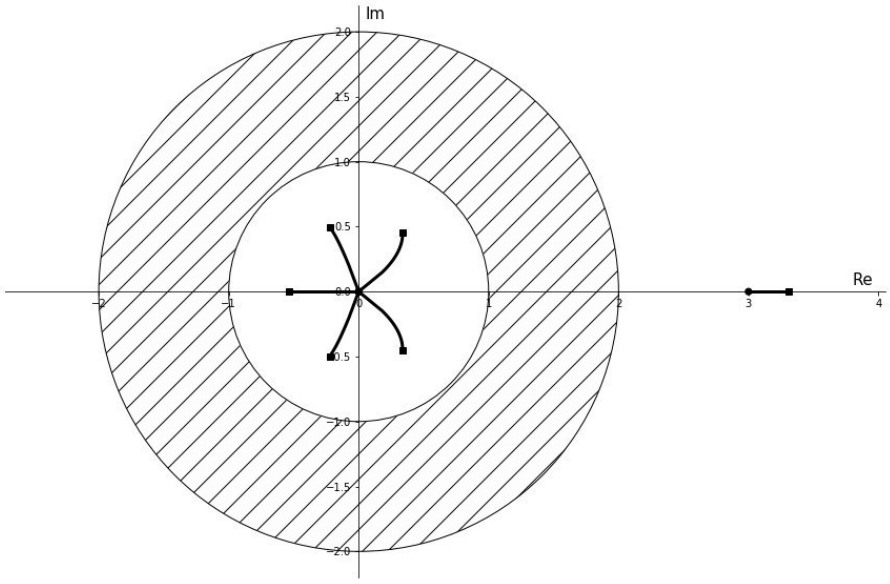


Figure 1: Trajectories traversed by roots of $\widehat{H}_5(\lambda)$ with t from 0 to 1; the round mark corresponds to $t = 0$, the square mark corresponds to $t = 1$

Proof. Using Lemma 7, similarly to the proof of Lemma 8, it can be shown that the first

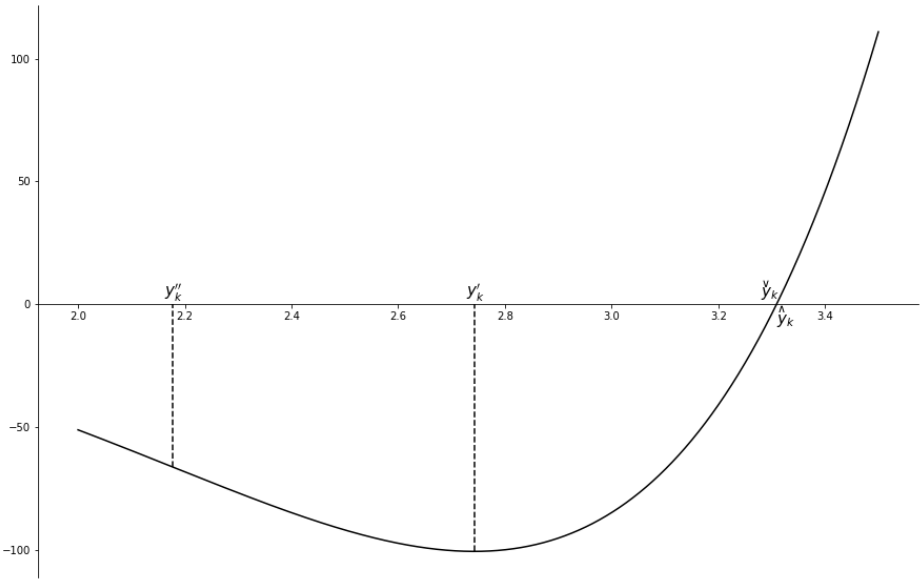


Figure 2: The plot of the function $\widehat{H}_5(\lambda)$

and second derivatives of the functions $\widehat{H}_k(\lambda)$ and $\breve{H}_k(\lambda)$ have exactly one root, whose module exceeds $\frac{Q}{2}+1$. We denote them by y'_k and y''_k respectively (by (17) these values are the same for $\widehat{H}_k$ and $\breve{H}_k$).

Since the function $\breve{H}_k(\lambda)$ can take negative values, $\min \breve{H}_k(\lambda) < 0$ and $\arg\min \breve{H}_k(\lambda) < \breve{y}_k$. At the same time $\arg\min \breve{H}_k(\lambda) = y'_k$. Thus $y'_k < \breve{y}_k$.

Carrying out similar reasoning, but considering $\breve{H}'_k(\lambda)$ instead of $\breve{H}_k(\lambda)$, it is easy to show that $y''_k < y'_k$. Then starting with some number k the following inequalities are held (see Fig. 2 for $Q=2$):

$$\frac{Q}{2}+1 \leqslant y''_k < y'_k < \breve{y}_k < \widehat{y}_k \leqslant 3Q.$$

Therefore functions $\widehat{H}_k(\lambda)$ and $\breve{H}_k(\lambda)$ are convex functions on $[y'_k, \widehat{y}_k]$, so for any $\delta \in [0,1]$ holds the convexity inequality:

$$\widehat{H}_k\big(\delta y'_k + (1-\delta)\widehat{y}_k\big) \leqslant \delta \widehat{H}_k(y'_k) + (1-\delta)\widehat{H}_k(\widehat{y}_k).$$

Note that

$$\breve{y}_k = \delta y'_k + (1-\delta)\widehat{y}_k \ \text{ for } \delta = \frac{\widehat{y}_k - \breve{y}_k}{\widehat{y}_k - y'_k},$$

therefore, finally we get the following chain of inequalities:

$$\widehat{H}_k(\breve{y}_k) \ \leqslant \ \delta \widehat{H}(y'_k) \ + \ (1 \ - \ \delta) \underbrace{\widehat{H}(\widehat{y}_k)}_{=0} \ = \ \frac{\widehat{y}_k - \breve{y}_k}{\widehat{y}_k - y'_k}\widehat{H}_k(y'_k) \ \leqslant \ \frac{\widehat{y}_k - \breve{y}_k}{\frac{5Q}{2}-1}\widehat{H}_k\left(\frac{Q}{2}+1\right),$$

where at the last inequality we used the fact that $\widehat{H}_k(y'_k)$ is the minimum value of function $\widehat{H}_k$ on the ray $\big[\frac{Q}{2}+1, +\infty\big)$ and also that $\widehat{y}_k - y'_k \leqslant \frac{5Q}{2}-1$. For function ν_k introduced in Lemma 7 the equality $\widehat{H}_k(\breve{y}_k) = -\nu_k$ obviously holds. Then we finally get:

$$\widehat{y}_k - \breve{y}_k \leqslant \frac{(-\frac{5Q}{2}+1)\nu_k}{\widehat{H}_k(\frac{Q}{2}+1)}.$$

It remains to show that the right part of the last inequality tends to zero at $k \to \infty$. This follows from the tendency of ν_k to zero and also from the fact that

$$\widehat{H}_k\left(\frac{Q}{2}+1\right) = \left(\frac{Q}{2}+1\right)^{k+1} - \ (1+Q)\left(\frac{Q}{2}+1\right)^{k} - \varphi_{k-1}\left(\frac{Q}{2}+1\right)^{k} - \cdots - \varphi_0 =$$
$$= -\frac{Q}{2}\left(\frac{Q}{2}+1\right)^{k} - \varphi_{k-1}\left(\frac{Q}{2}+1\right)^{k} - \cdots - \varphi_0 \to -\infty \text{ as } k \to \infty.$$

□

Now we can estimate the value of $\mathbb{E}2^{H_n}$.

Theorem 2. *For all $\varepsilon > 0$ and all $q \in \mathbb{N}$ there exist real positive numbers $\widehat{z}$, $\breve{z}$, c_1 and c_2 such that $|\widehat{z} - \breve{z}| \leqslant \varepsilon$ and*

$$c_1 \breve{z}^n \lesssim \mathbb{E}2^{qH_n} \lesssim c_2 \widehat{z}^n \ \textit{as} \ n \to \infty.$$

Proof. According to Lemma 8 polynomials $\widehat{H}_k(\lambda)$ and $\breve{H}_k(\lambda)$ have exactly one root greater than $\left(\frac{Q}{2}+1\right)$. From (7) and (18) $\big($also (10) and (19)$\big)$ it follows that

$$\widehat{f}_k(n) = \widehat{F}_k(n) - \widehat{F}_k(n-1) \sim \widehat{\gamma}_k(\widehat{y}_k - 1)\widehat{y}_k^{n-1} = \widehat{\gamma}'_k\widehat{y}_k^n,$$

$$\breve{f}_k(n) = \breve{F}_k(n) - \breve{F}_k(n-1) \sim \breve{\gamma}_k(\breve{y}_k - 1)\breve{y}_k^{n-1} = \breve{\gamma}'_k\breve{y}_k^n.$$

At the same time,

$$\breve{f}_k(n) \leqslant f(n) \leqslant \widehat{f}_k(n),$$

so

$$\breve{\gamma}'_k\breve{y}_k^n \lesssim f(n) \lesssim \widehat{\gamma}'_k\widehat{y}_k^n,$$

$$\breve{\gamma}'_k\breve{y}_k^n \lesssim f'(n) \lesssim 2\widehat{\gamma}'_k\widehat{y}_k^n = \widehat{\gamma}''_k\widehat{y}_k^n.$$

Finally,

$$c_1\breve{z}^n = \breve{\gamma}'_k \cdot \frac{\breve{y}_k^n}{2^n} \lesssim \mathbb{E}2^{qH_n} \lesssim \widehat{\gamma}''_k \cdot \frac{\widehat{y}_k^n}{2^n} = c_2\widehat{z}^n,$$

moreover, Lemma 9 guarantees that $\widehat{z}$ and $\breve{z}$ can be made arbitrarily close. □

Let us use the result of Theorem 2. Chose $\varepsilon = 10^{-20}$, Then such $\widehat{y}_k$ and $\breve{y}_k$ exist that $|\widehat{y}_k - \breve{y}_k| < \varepsilon$, that is they are both equal to $\widetilde{y}$ with the specified accuracy. This value will correspond to $\widetilde{z} = \frac{\widetilde{y}}{2}$. Moreover, value $\log_2 \widetilde{y} - 1$ is interesting as

$$c_1 2^{n\cdot(\log_2 \widetilde{y}-1-\varepsilon)} \lesssim \mathbb{E}2^{qH_n} \lesssim c_2 \cdot 2^{n\cdot(\log_2 \widetilde{y}-1+\varepsilon)}.$$

Q	$\widetilde{y}$	$\widetilde{z}$	$\log_2 \widetilde{y} - 1$
2	3.30921306134212177240	1.65460653067106088620	0.72648818154049951037
4	5.80027271324371478340	2.90013635662185739172	1.53612073348070167305
8	10.53733221939675028493	5.26866610969837514246	2.39743775493525848727
16	19.61999911051941379160	9.80999955525970689580	3.29425307103935297681
32	37.19179236569642652549	18.59589618284821326274	4.21691237160283720288
64	71.45569997172021204310	35.72784998586010602155	5.15897719358341460680
128	138.69767829225482267831	69.34883914612741133915	6.11579982787398693748
256	271.32073664755570805747	135.66036832377785402874	7.08385550468282259524
512	533.89365096936984102274	266.94682548468492051137	8.06040858243800754807

Table 1: Approximate values associated with $\mathbb{E}Q^{H_n}$ for different values of Q

Now we can evaluate the variance of the value 2^{H_n}:

$$\mathbb{D}2^{H_n} = \mathbb{E}\big(2^{H_n}\big)^2 - \big(\mathbb{E}2^{H_n}\big)^2 = \mathbb{E}2^{2H_n} - \big(\mathbb{E}2^{H_n}\big)^2.$$

It is easy to observe from this table that $\big(\mathbb{E}2^{H_n}\big)^2 = o\big(\mathbb{E}2^{2H_n}\big)$. Thus, the variance $\mathbb{D}2^{H_n}$ can be estimated by the second moment:

$$c'_1 \cdot 2^{(1.5361-\varepsilon)n} \lesssim \mathbb{D}2^{H_n} \lesssim c'_2 \cdot 2^{(1.5361+\varepsilon)n}.$$

Finally we estimate the probability of deviating from the expectation $\mathbb{E}2^{H_n}$. We use Chebyshev's inequality:

$$\mathbb{P}\Big(\big|2^{H_n} - \mathbb{E}2^{H_n}\big| \geqslant a\Big) \leqslant \frac{\mathbb{D}2^{H_n}}{a^2}.$$

Choose $a = v^n\sqrt{\mathbb{D}2^{H_n}}, v > 1$ then

$$\mathbb{P}\left(\left|2^{H_n} - \mathbb{E}2^{H_n}\right| \geqslant v^n\sqrt{\mathbb{D}2^{H_n}}\right) \leqslant \frac{1}{v^{2n}} \to 0 \text{ as } n \to \infty.$$

Thus with probability tending to one

$$2^{H_n} \leqslant \mathbb{E}2^{H_n} + v^n\sqrt{\mathbb{D}2^{H_n}}$$

or, for example,

$$2^{H_n} = o\left(2^{0.76807n}\right) \text{ as } n \to \infty.$$

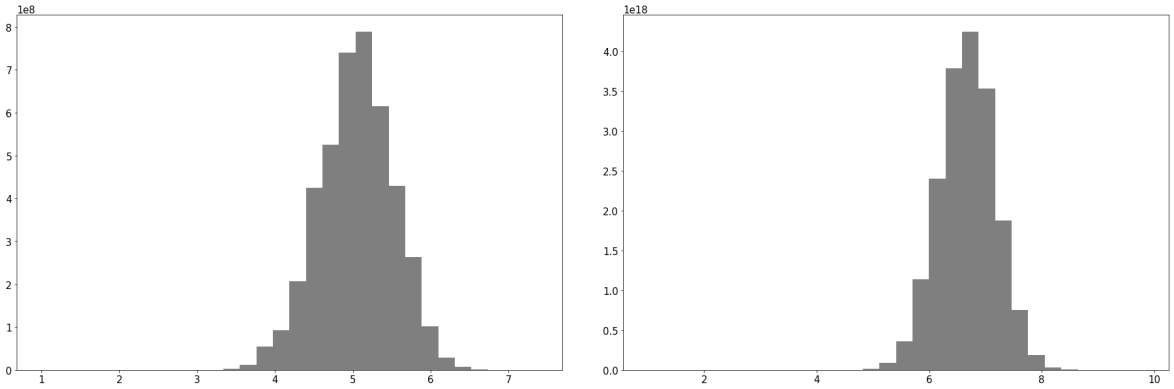


Figure 3: Distribution of $2^{H_{32}}/K_{\frac{1}{2}}$ and $2^{H_{64}}/K_{\frac{1}{2}}$.

For $n = 64$ theoretical expectation $\mathbb{E}2^{H_n}$ is approximately $9,92 \cdot 10^{13}$ and computed one is $5,38 \cdot 10^{13}$. So real value is only 1,8 times smaller than calculated one. On Fig. 3 one can see that $K_{\frac{1}{2}}(i) \leqslant 2^{H_n^i}$ for $n = 32$ and $n = 64$. So at least in these cases our hypothesis is true. Besides, the relation $2^{H_n^i}/K_{\frac{1}{2}}(i)$ is small.

3 Equivalence classes' sizes

It turns out that there is a simple analytical formula for the size of any given equivalence class.

Let n-bit number $i = (\alpha_{n-1}\alpha_{n-2}, \alpha_{n-3}, \ldots, \alpha_0)$ be the number of $(2^n \times 2^n)$ - matrix row and $i' = (\alpha_{n-2}, \alpha_{n-3}, \ldots, \alpha_0)$.

Theorem 1. *For each number i' the row of DDT-matrix with this number belongs to the equivalence class of size*

$$\rho_i = 2 \cdot C_K^{s-1} C_{s-1}^{c_1} C_{s-1-c_1}^{c_2} \ldots C_{s-1-c_1-\cdots-c_{r-2}}^{c_{r-1}},$$

where

(a) K is the number of 1's in binary representation of i',

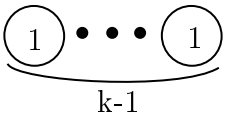
(b) s is the number of groups of 0's and 1's in i',

(c) $c_1, c_2, \ldots$ is the number of 0's of size $1, 2, \ldots$.

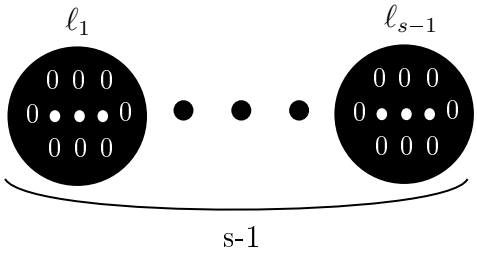
Proof. Row distributions of the second half of the DDT-matrix fully duplicate distributions of the first half, so it is enough to compose a formula for the first part and multiply it by two.

Since the last group of 0's is fixed, we need to position $n-1-K-\ell_s$ 0's. In addition, before the last group of 0's we strictly have to put at least one 1, in order to separate it. So we need to find place for only $K-1$ 1's.

Let us consider a model problem. We associate with each 1 a white ball



and each group $\ell_1, \ldots, \ell_{s-1}$ a black one.



It is required to find the number of variants to locate $K-1$ white ball and $s-1$ black ball so that between two black ones there is at least one white.

Let us imagine that the goal is to place $s-1$ partition in a box with $K-1$ elements. We can put a partition on one of K places (between elements and on the sides), but in the way the elements are always separated from each other. So the number of variants is C_K^{s-1}.

Now let us note that in fact black balls are multicolour balls where each colour corresponds to a specific length of a group of 0's:

$$c_i = color_i = \left|\{\ell_j \mid \ell_j = i, j = 1, \ldots, s-1\}\right|,\ i = 1, \ldots, r.$$

Thus, in order to get all possible distribution of balls, that is, all possible row numbers included in one equivalence class, it remains to calculate the number of representations of $s-1$ black ball through colored ones, provided that a set of colored balls is given.

It can be proved by induction that the number of representations of black balls through colored ones is:

$$C_{s-1}^{c_1} C_{s-1-c_1}^{c_2} \ldots C_{s-1-c_1-\cdots-c_{r-2}}^{c_{r-1}}.$$

You can split black balls into balls of the same color in a unique way. Now let the formula be true for black balls partitioning into balls of $r-1$ colours. Let us consider that the number of balls of colours $1, \ldots, r-1$ equals respectively $c'_1, \ldots, c'_{r-1}$. Then the number of variants is

$$C_{s-1}^{c'_1} C_{s-1-c'_1}^{c'_2} \ldots C_{s-1-c'_1-\cdots-c'_{r-3}}^{c'_{r-2}}.$$

Now let $(r-1)$-th colour be actually a union of $(r-1)$-th and r-th colour. In other words, $c'_1 = c_1, c'_2 = c_2, \ldots, c'_{r-2} = c_{r-2}, c'_{r-1} = c_{r-1} + c_r$. Then the number of variants to partition $s-1-c_1-\cdots-c_{r-2}$ in two colour is $C_{s-1-c_1-\cdots-c_{r-2}}^{c_{r-1}}$. □

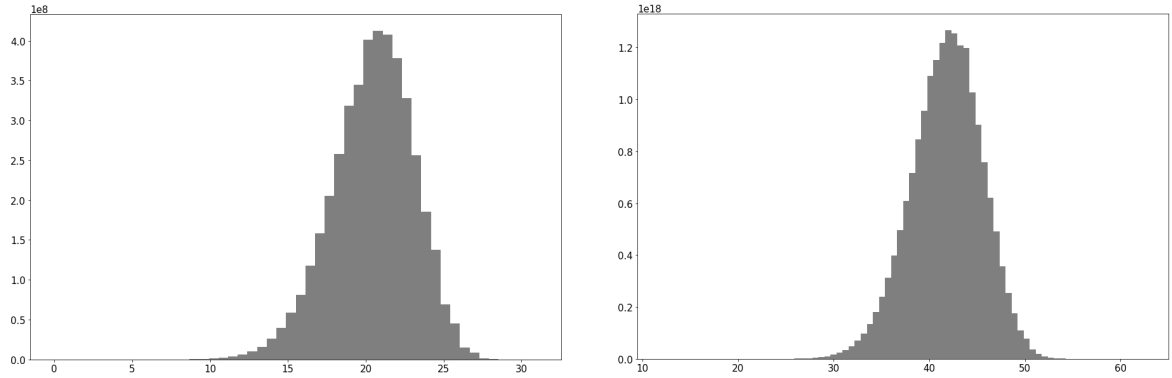


Figure 4: Distribution of H_{32} and H_{64}

Usually one needs $\Omega(2^{3n})$ operations to calculate H_n (to get the DDT-table and then consistently by definition calculate entropy). For example, for $n = 32$ it is 2^{96} bit operations or approximately $6.4 \cdot 10^{19}$ seconds and for $n = 64$ it is 2^{192} operations or $4 \cdot 10^{48}$ seconds. But using our short representation of an equivalence class and the ability to enumerate all classes in time proportional to their number the problem can be solved on a laptop in 0.1 and 62 seconds for $n = 32$ and $n = 64$ respectively. Distributions for these cases are shown on Fig. 4.

References

[1] Lipmaa H., Moriai S., "Efficient Algorithms for Computing Differential Properties of Addition", *Fast Software Encryption*, ed. Matsui M., 2002, 336–350.

[2] Vysotskaya V., *Some Properties of Modular Addition (Extended abstract)*, Cryptology ePrint Archive, https://eprint.iacr.org/2018/1103.

[3] Graham R. L, Knuth D. E., Patashnik O., *Concrete Mathematics: A Foundation for Computer Science*, (2 ed.), Addison-Welsey, 1994, ISBN: 978-0-201-55802-9, 672 pp.

[4] Tyrtyshnikov E., *A Brief Introduction to Numerical Analysis*, Birkhäuser Basel, 1997, ISBN: 978-0-8176-8136-4, 202 pp.