Math-Net.Ru

Общероссийский математический портал

V. V. Vysotskaya, Вероятностные свойства сложения по модулю, *Матем. вопр. криптогр.*, 2021, том 12, выпуск 1, 109–130

DOI: <https://doi.org/10.4213/mvk351>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.253.173

26 апреля 2023 г., 12:40:49

Probabilistic properties of modular addition*

V. V. Vysotskaya

*JSC «InfoTeCS», Moscow, Russia
JSC «NPK Kryptonite», Moscow, Russia*

Получено 05.XI.2019

Abstract. We study the applicability of differential cryptanalysis to the operation of addition modulo 2^n used in different cryptosystems. We obtain an analytical formula for expected value of entropy H_n of rows of the difference distribution table of the corresponding mapping. Moreover, the moments of 2^{H_n} are studied. In particular, asymptotic inequalities describing the behavior of values $\mathbb{E}2^{qH_n}$ (for $q \in \mathbb{N}$) and $\mathbb{D}2^{H_n}$ as $n \rightarrow \infty$ are obtained. We also find a simple analytical formula for the number of table rows with the same distribution. It permits to compute efficiently the statistical characteristics of the entropy.

Keywords: modular addition, differential cryptanalysis, entropy of distribution

Вероятностные свойства сложения по модулю

В. В. Высоцкая

*ОАО «ИнфоТеКС», Москва, Россия
АО «НПК Криптонит», Москва, Россия*

Аннотация. Изучается возможность применения разностного криптоанализа к операции сложения по модулю 2^n , используемой в различных криптосистемах. Получена аналитическая формула математического ожидания энтропии H_n таблицы распределений разностей соответствующего отображения. Рассматриваются также моменты 2^{H_n} . В частности, получены асимптотические неравенства для $\mathbb{E}2^{qH_n}$ (для $q \in \mathbb{N}$) и $\mathbb{D}2^{H_n}$ при $n \rightarrow \infty$. Найдена простая аналитическая формула для числа строк в таблице, задающих одно и то же распределение. Она позволяет эффективно вычислять статистические характеристики энтропии.

Ключевые слова: модульное сложение, разностный криптоанализ, энтропия распределения

*The article was submitted by the Organizing Committee of the Symposium CTCrypt'2019.

1. Introduction

There is a number of cryptographic schemes that use the operation of addition modulo 2^n for some $n > 1$. Denote $\mathbb{Z}_N$ the ring of residues modulo N . The first function under consideration is $f: \mathbb{Z}_{2^n}^2 \rightarrow \mathbb{Z}_{2^n}$ defined by $f(x, y) = x \boxplus_n y$, where $\boxplus_n$ denotes addition in the ring $\mathbb{Z}_{2^n}$, i. e. addition modulo 2^n . We consider the function $P_n(i, j): \mathbb{Z}_{2^n}^2 \rightarrow \mathbb{N}_0$,

$$P_n(i, j) = \frac{1}{2^{2n}} \left| \{(x, y) \in \mathbb{Z}_{2^n}^2 : j = f(x \oplus i, y) \oplus f(x, y)\} \right|,$$

where $\oplus$ is bitwise exclusive-OR (it is analogous to the special case of the differential probability of addition modulo 2^n studied in [1]). In this work we study the properties of this operation in terms of the entropy

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

where $p \log_2 p$ is assumed to be equal to zero if $p = 0$.

In [2] we have 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 was shown that this table has a special form: the table for addition modulo 2^{n+1} is naturally expressed via 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 :

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

where

$$A_n = \frac{1}{2} \left[\frac{2A_{n-1}}{B_{n-1}} \middle| \frac{B_{n-1}}{A_{n-1}} \right], \quad B_n = \frac{1}{2} \left[\frac{0}{B_{n-1}} \middle| \frac{B_{n-1}}{A_{n-1}} \right] \quad (2)$$

and $A_1 = [1]$, $B_1 = [0]$.

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 enumerate all the distinct distributions in time proportional to their number, that is asymptotically in time

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

When considering $P_n(i, j)$ as a part of a cryptosystem from the point of view of differential cryptanalysis the following problem arises: to find for a given (or randomly chosen) i the minimum cardinality $K_c(i)$ of the set of numbers $\{j_1, \dots, j_{K_c(i)}\}$ such that

$$\sum_{m=1}^{K_c(i)} P_n(i, j_m) \geq c, \quad (3)$$

where c , $0 < c \leq 1$, is some fixed constant. The value of $K_c(\Delta x)$ 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 $K_{1/2}(i)$ does not exceed $2^{H_n^i}$, where H_n^i is the entropy of this distribution (this is not true for arbitrary distributions, a counterexample is given by the distribution $\{\frac{1}{4}, r_n, \dots, r_n\}$, $r_n = \frac{3}{4(2^n-1)}$: in this case $2^{H_n^i} = O(2^{3n/4}) = o(2^n)$, $n \rightarrow \infty$).

Now let us consider a random variable $\eta_n = H_n^\kappa$, where κ is uniformly distributed on the set $\{0, \dots, 2^n - 1\}$, so η_n is the entropy of random row of DDT. In this paper we obtain an analytical formula for the expected value of entropy of η_n and asymptotic inequalities describing the behavior of values $\mathbb{E}2^{q\eta_n}$ (for $q \in \mathbb{N}$) and $\mathbb{D}2^{\eta_n}$ as $n \rightarrow \infty$. We also implement the equivalence class enumeration algorithm and justify (for some practical values of n) our assumption concerning closeness of 2^{η_n} and $K_{1/2}(i)$. The theoretically estimated values of moments of 2^{η_n} also appear to be close to the experimental ones.

We also derive a simple analytical formula for the size of any given equivalence class and used it, in particular, to efficiently compute the distribution of η_n . After that any its statistical characteristics may be calculated.

2. Properties of DDT row entropy

Let us remind that the entropy of the i -th row of matrix P_n is defined by

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

where $p \log_2 p$ is assumed equal to zero for $p = 0$. For convenience we denote for matrices A_n and B_n from (2)

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

and put

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

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 $\frac{1}{2}[a, b, a, b]$ for some rows a, b of length 2^{n-1} and thus the entropy may be written as

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

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 $\frac{1}{2}[2a, b, 0, b]$ for some rows a, b of length 2^{n-1} and thus

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

□

Let us proceed to the study of the value $\mathbb{E}\eta_n = \left(\sum_{i=0}^{2^n-1} H_n^i \right) / 2^n$.

Lemma 2. *For every $n \geq 1$*

$$\mathbb{E}\eta_{n+1} = \frac{n}{2} + \frac{\beta_n}{2^n} + \dots + \frac{\beta_3}{8} + \frac{\beta_2}{4}.$$

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

$$\begin{aligned} \mathbb{E}\eta_{n+1} &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^{n+1}-1} H_{n+1}^i = \frac{1}{2^n} \sum_{i=0}^{2^{n-1}-1} (H_n^i + \beta_n^i) + \frac{1}{2^n} \sum_{i=2^{n-1}}^{2^n-1} (H_n^i + 1) \\ &= \frac{1}{2^n} \sum_{i=0}^{2^n-1} H_n^i + \frac{1}{2^n} \sum_{i=0}^{2^{n-1}-1} \beta_n^i + \frac{1}{2} = \mathbb{E}H_n + \frac{\beta_n}{2^n} + \frac{1}{2}. \end{aligned}$$

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

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

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 obtain

$$\begin{aligned} \beta_{n+1} &= 2^{n-2} + \frac{\beta_n}{2} = 2^{n-2} + 2^{n-4} + \frac{\beta_{n-1}}{4} \\ &= 2^{n-2} + 2^{n-4} + \dots + 2^{-n} = \frac{2^{n-2}(1 - (2^{-2})^n)}{1 - 2^{-2}} = \frac{1}{3} \cdot 2^n(1 - 4^{-n}). \end{aligned}$$

□

Theorem 1. *The following equality is valid:*

$$\mathbb{E}\eta_n = \frac{2}{3}n - \frac{8}{9}(1 - 4^{-n}).$$

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

$$\mathbb{E}\eta_{n+1} = \frac{n}{2} + \frac{1}{6}(1 - 4^{1-n}) + \dots + \frac{1}{6}(1 - 4^{-1}) = \frac{n}{2} + \frac{n-1}{6} - \frac{1}{18}(1 - 4^{1-n}).$$

So

$$\mathbb{E}\eta_n = \frac{n-1}{2} + \frac{n-2}{6} - \frac{1}{18}(1 - 4^{-n}) = \frac{2}{3}n - \frac{8}{9}(1 - 4^{-n}).$$

□

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

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

where Q denotes 2^q . To avoid multilevel exponentiation we will use the notation

$$\mathcal{Q}(x) = Q^x.$$

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

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

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

□

Lemma 4. For $i = 0, \dots, 2^{n-1} - 1$ it holds that

$$\beta_n^i = \begin{cases} 0, & \text{if } i = 0, \\ 2^{-(n-1-\lfloor \log_2 i \rfloor)}, & \text{otherwise.} \end{cases} \quad (4)$$

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_{n-1}^i , $0 \leq i \leq 2^{n-2} - 1$, and let us prove it for β_n^i .

For $2^{n-2} \leq i \leq 2^{n-1} - 1$ from (2) we get $\beta_n^i = \frac{1}{2}$ as the sum of elements in any row of matrix $\begin{bmatrix} B_{n-1} & A_{n-1} \end{bmatrix}$ is 1. This agrees with (4) as $\lfloor \log_2 i \rfloor = n - 2$ in this case.

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

$$\beta_n^i = \frac{1}{2} \beta_{n-1}^i,$$

and by the inductive hypothesis we come to (4). $\square$

Remark. The vector of values of β_n^i has the following form:

$$\left[0, \underbrace{\frac{1}{2^{n-1}}}_1, \underbrace{\frac{1}{2^{n-2}}, \frac{1}{2^{n-2}}}_2, \dots, \underbrace{\frac{1}{8}, \dots, \frac{1}{8}}_{2^{n-4}}, \underbrace{\frac{1}{4}, \dots, \frac{1}{4}}_{2^{n-3}}, \underbrace{\frac{1}{2}, \dots, \frac{1}{2}}_{2^{n-2}} \right].$$

For convenience we extend the definition (4) for $2^{n-1} \leq i \leq 2^n - 1$. Then according to Lemma 1 and noting that $H_1^0 = H_1^1 = 0$ we claim that

$$\begin{aligned} H_n^i &= \beta_{n-1}^{\text{mod } 2^{n-1}} + H_{n-1}^{i \text{ mod } 2^{n-1}} = \beta_{n-1}^{\text{mod } 2^{n-1}} + H_{n-2}^{i \text{ mod } 2^{n-2}} + \beta_{n-2}^{\text{mod } 2^{n-2}} \\ &= \dots = \beta_{n-1}^{i \text{ mod } 2^{n-1}} + \beta_{n-2}^{i \text{ mod } 2^{n-2}} + \dots + \beta_2^{i \text{ mod } 4}. \end{aligned} \quad (5)$$

For $k \in \{0, \dots, n-1\}$ let us introduce sets

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

The set Z_k consists of integers having binary representation of the form $\underbrace{0 \dots 0}_k 1 \underbrace{* \dots *}_{n-k-1}$. Then $j = (j \text{ mod } 2^{n-c})$ for all $j \in Z_k$ and $c \leq k$. Let us

denote $\omega_n = \sum_{i=0}^{2^n-1} \mathcal{Q}(H_n^i)$. Then with the method used in (5) we can claim that

$$\begin{aligned} \omega_n &= \sum_{k=0}^{n-1} \sum_{j \in Z_k} \mathcal{Q} \left(\sum_{c=1}^k \beta_{n-c}^j + H_{n-k}^j \right) + 1 \\ &= \sum_{k=0}^{n-1} \sum_{j \in Z_k} \mathcal{Q} \left(\sum_{c=1}^k \beta_{n-c}^j \right) \mathcal{Q}(H_{n-k}^j) + 1 \\ &= \sum_{k=0}^{n-1} \mathcal{Q} \left(\sum_{c=0}^{k-1} 2^{-c} \right) \sum_{j \in Z_k} \mathcal{Q}(H_{n-k}^j) + 1 = \sum_{k=0}^{n-1} \mathcal{Q}(2 - 2^{-k+1}) \frac{\omega_{n-k}}{2} + 1. \end{aligned}$$

And if $n = 0$ then $\omega_n = 1$.

Obviously,

$$\mathbb{E}(2^{\eta_n})^q = \frac{\omega_n}{2^n}.$$

Thus we need to investigate the following recurrence relation:

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

First, we compare it with the similar relation:

$$f(n) = \sum_{\ell=1}^{n-1} f(\ell) \cdot \mathcal{Q}(2 - 2^{-n+\ell+1}), \quad n \geq 2, \quad f(1) = 2. \quad (6)$$

Let us denote $\Delta(n) = \tilde{f}(n) - f(n)$.

Lemma 5. *For $n \in \mathbb{N}$ it holds that $\Delta(n) \leq f(n)$.*

Proof. Let us prove by induction. Obviously,

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

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

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

For $n \geq 1$ we have $\mathcal{Q}(2 - 2^{-n+2}) \geq 1$ from this inequality the inductive hypothesis follows:

$$\begin{aligned} \Delta(n+1) &\leq \sum_{\ell=2}^n f(\ell) \cdot \mathcal{Q}(2 - 2^{-n+\ell+1}) + \Delta(1) \cdot \mathcal{Q}(2 - 2^{-n+2}) + 2 \\ &\leq \sum_{\ell=2}^n f(\ell) \cdot \mathcal{Q}(2 - 2^{-n+\ell+1}) + 0 + 2 \\ &\leq \sum_{\ell=2}^n f(\ell) \mathcal{Q}(2 - 2^{-n+\ell+1}) + f(1) \cdot \mathcal{Q}(2 - 2^{-n+2}) = f(n+1). \end{aligned}$$

The latter is the required inequality. □

Using the Lemma 5 we estimate $\tilde{f}(n)$:

$$f(n) \leq \tilde{f}(n) = f(n) + \Delta(n) \leq 2f(n),$$

and further we will work with homogeneous equation (6). Let us note that coefficients $\mathcal{Q}(2 - 2^{-n+\ell+1})$ are bounded from above by the number $\mathcal{Q}(2)$. Then let us consider the following family of recurrence relations:

$$\begin{aligned}\hat{f}_k(n) &= \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) \hat{f}_k(\ell) + \mathcal{Q}(2) \sum_{\ell=1}^{n-k-1} \hat{f}_k(\ell), \\ \hat{f}_k(1) &= 2, \quad \hat{f}_k(i) = 0, \quad i \leq 0,\end{aligned}\tag{7}$$

solutions of these relations bound $f(n)$ from above. Denote

$$\hat{F}_k(n) = \sum_{\ell=1}^n \hat{f}_k(\ell).\tag{8}$$

Then using definition (8) and noting that $\hat{f}_k(m) = \hat{F}_k(m) - \hat{F}_k(m-1)$ we can rewrite the representation (7) as

$$\begin{aligned}\hat{F}_k(n) - \hat{F}_k(n-1) &= \hat{f}_k(n) = \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) \hat{f}_k(\ell) + \mathcal{Q}(2) \sum_{\ell=1}^{n-k-1} \hat{f}_k(\ell) \\ &= \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) (\hat{F}_k(\ell) - \hat{F}_k(\ell-1)) + \mathcal{Q}(2) \hat{F}_k(n-k-1), \\ \hat{F}_k(1) &= 2, \quad \hat{F}_k(i) = 0, \quad i \leq 0.\end{aligned}\tag{9}$$

Note that this recurrence relation has constant “length” and may be solved using well-known methods, for example, the one described in [3]. Let us first find the form of the characteristic polynomial corresponding to this relation:

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

Thus the final form of the characteristic polynomial is

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

We will denote by $(-\hat{\varphi}_s)$ the coefficient at l^s , $0 \leq s \leq k$ (so, $\hat{\varphi}_s$ are non-negative). Let $\hat{y}_1, \dots, \hat{y}_{k+1}$ be the roots of this polynomial. It is known [3] that the solution of equation (9) has the form

$$\hat{F}_k(n) = \hat{\gamma}_1 \hat{y}_1^n + \dots + \hat{\gamma}_{k+1} \hat{y}_{k+1}^n \quad (10)$$

for some constants $\hat{\gamma}_i$. Let us assume that $\hat{y}_k$ has the maximal absolute value among $\hat{y}_1, \dots, \hat{y}_{k+1}$.

On the other hand, coefficients $\mathcal{Q}(2 - 2^{-n+\ell+1})$ decrease with growth of ℓ and attain the minimal value on the segment $[1, n - k - 1]$ at the point $\ell = n - k - 1$, where the coefficient is equal to $\mathcal{Q}(2 - 2^{-k})$. From this considerations we obtain a new family of recurrences bounding $f(n)$ from below:

$$\begin{aligned} \check{f}_k(n) = \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) \check{f}_k(\ell) + \mathcal{Q}(2 - 2^{-k}) \sum_{\ell=1}^{n-k-1} \check{f}_k(\ell), \\ \check{f}_k(1) = 2, \quad \check{f}_k(i) = 0, \quad i \leq 0. \end{aligned}$$

Just as it was done above we introduce

$$\check{F}_k(n) = \sum_{\ell=1}^{n-1} \check{f}_k(\ell). \quad (11)$$

Thus

$$\begin{aligned} \check{F}_k(n) - \check{F}_k(n-1) \\ = \sum_{\ell=n-k}^{n-1} \mathcal{Q}(2 - 2^{-n+\ell+1}) (\check{F}_k(\ell) - \check{F}_k(\ell-1)) + \mathcal{Q}(2 - 2^{-k}) \check{F}_k(n-k-1), \\ \check{F}_k(1) = 2, \quad \check{F}_k(i) = 0, \quad i \leq 0. \end{aligned} \quad (12)$$

In this case the characteristic polynomial has the following form:

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

We will denote by $(-\check{\varphi}_s)$ the coefficient at l^s , $0 \leq s \leq k$. The solution of the equation (12) has the following form:

$$\check{F}_k(n) = \check{\gamma}_1 \check{y}_1^n + \dots + \check{\gamma}_{k+1} \check{y}_{k+1}^n, \quad (13)$$

where $\check{y}_1, \dots, \check{y}_{k+1}$ are the roots of $\check{H}_k(l)$, $\check{\gamma}_i$ are some constants and $\check{y}_k$ has maximum absolute value among $\check{y}_1, \dots, \check{y}_{k+1}$.

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

$$\hat{u}_t(l) = l^{k+1} - (1 + Q)l^k - t \cdot \hat{\varphi}_{k-1}l^{k-1} - \dots - t \cdot \hat{\varphi}_0$$

and the similar one for $\check{\varphi}_i$ (denote it by $\check{u}_t(l)$). We will prove the following lemmas on these families (note that $\check{\varphi}_i = \hat{\varphi}_i$ for $i \geq 1$).

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

- (a) *have no root in the annulus $1 < |l| \leq 2$, if $Q = 2$,*
- (b) *have no root l such that $|l| = \frac{Q}{2} + 1$, if $Q > 2$.*

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

$$l^{k+1} - t \cdot \hat{\varphi}_{k-1}l^{k-1} - \dots - t \cdot \hat{\varphi}_0 = 3l^k$$

and applying the triangle inequality, we get

$$|l|^{k+1} + t \cdot \hat{\varphi}_{k-1}|l|^{k-1} + \dots + t \cdot \hat{\varphi}_0 \geq 3|l|^k.$$

Then

$$|l|^{k-1} (|l|^2 - 3|l| + t \cdot \hat{\varphi}_{k-1}) \geq -t \cdot \hat{\varphi}_{k-2}|l|^{k-2} - \dots - t \cdot \hat{\varphi}_0.$$

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

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

That is,

$$|l|^{k-1}(-2 + t \cdot \hat{\varphi}_{k-1}) \geq -t \cdot \hat{\varphi}_{k-2}|l|^{k-2} - \dots - t \cdot \hat{\varphi}_0.$$

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

$$-2 \geq -t \cdot \hat{\varphi}_{k-1} - t \cdot \hat{\varphi}_{k-2}|l|^{-1} - \dots - t \cdot \hat{\varphi}_0|l|^{-k+1}.$$

Noting that simultaneously $t \leq 1$ by premise and $|l|^{-1} < 1$ in the considered annulus, we conclude that:

$$2 < \hat{\varphi}_{k-1} + \hat{\varphi}_{k-2} + \dots + \hat{\varphi}_0. \quad (14)$$

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

$$\hat{\varphi}_{k-1} + \hat{\varphi}_{k-2} + \dots + \hat{\varphi}_0 = 2,$$

so we obtain the contradiction with (14). The same line of reasoning works for $\check{u}_t(l)$ except that instead of the last equality we get a strict inequality.

We turn to the case (b): $Q > 2$ or, as $Q = 2^q$, equivalently, $Q \geq 4$. If under this condition there is a root such that $|l| = \frac{Q}{2} + 1$, then

$$\left(\frac{Q}{2} + 1\right)^{k+1} + \left(\frac{Q}{2} + 1\right)^{k-1} \cdot t \cdot \hat{\varphi}_{k-1} + \dots + t \cdot \hat{\varphi}_0 \geq (Q + 1) \cdot \left(\frac{Q}{2} + 1\right)^k.$$

As far as $\max_i \hat{\varphi}_i = \hat{\varphi}_{k-1} = Q^{\frac{3}{2}} - Q$ and $t \leq 1$, we have

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

or, equivalently,

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

which contradicts $Q \geq 4$. Absolutely the same arguments work for $\check{u}_t(l)$. $\square$

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

Proof. Note that polynomials $\hat{u}_t(l)$ and $\check{u}_t(l)$ differ only in the constant term, which implies the equality of their derivatives

$$\hat{u}_t^{(s)}(l) = \check{u}_t^{(s)}(l) \text{ for all } s \geq 1. \quad (15)$$

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

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

$$\begin{aligned} (k+1)^{[s]} \cdot \left(\frac{Q}{2} + 1\right)^{k+1-s} + (k-1)^{[s]} \cdot \left(\frac{Q}{2} + 1\right)^{k-1-s} \cdot t \hat{\varphi}_{k-1} + \dots \\ + 0^{[s]} \cdot \left(\frac{Q}{2} + 1\right)^{-s} \cdot t \hat{\varphi}_0 \geq (Q+1)k^{[s]} \cdot \left(\frac{Q}{2} + 1\right)^{k-s} \end{aligned}$$

(here $x^{[s]}$ denotes $x(x-1)\dots(x-s+1)$). As was noted above, $\max_i \hat{\varphi}_i = Q^{\frac{3}{2}} - Q$, so

$$\begin{aligned} (k-1)^{[s]}(Q^{3/2} - Q) \cdot \frac{2}{Q} \left(\frac{Q}{2} + 1 \right)^{k-s} \\ \geq (Q+1)k^{[s]} \cdot \left(\frac{Q}{2} + 1 \right)^{k-s} - (k+1)^{[s]} \cdot \left(\frac{Q}{2} + 1 \right)^{k+1-s}, \end{aligned}$$

therefore,

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

This inequality can be viewed as

$$a(Q, s)k^2 + b(Q, s)k + c(Q, s) \geq 0. \quad (16)$$

But

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

Moreover, in the case $Q = 4$ we have $b(Q, s) < 0$. Thus, there exists a certain number k_0 such that the inequality (16) will not be satisfied for $k > k_0$. $\square$

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

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

$$\hat{u}_0(l) = \check{u}_0(l) = l^{k+1} - (1+Q)l^k,$$

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

By Lemma 6, $\hat{u}_t(l)$ and $\check{u}_t(l)$ do not have roots in the annulus $1 < |l| \leq 2$ (for $Q = 2$) or on the circle $|l| = \frac{Q}{2} + 1$ (for $Q \geq 4$). Thus, all curves corresponding to the first k roots do not leave the circle $|l| \leq 1$ (for $Q = 2$) and the circle $|l| < \frac{Q}{2} + 1$ (for $Q \geq 4$). The curve corresponding to the last root does not leave the sets $|l| > 2$ and $|l| > \frac{Q}{2} + 1$ respectively. $\square$

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

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

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

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

for $Q \geq 2$. Identical statements are true for $\check{H}_k(Q+1)$ and $\check{H}_k(3Q)$.

Hence the continuous functions $\hat{H}_k(l)$ and $\check{H}_k(l)$ (taking real values on the real axis) have a real root on the segment $[Q+1, 3Q]$, this root may be found by successive dividing of the segment in two equal parts. So, the root may be found by n steps with an accuracy $O(2^{-n})$.

Then equalities (10) and (13) take form:

$$\hat{F}_k(n) = \hat{\gamma}_k \hat{y}_k^n + \hat{\rho}_k(n), \quad (17)$$

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

where $\hat{y}_k, \check{y}_k$ are maximal (in the absolute value) roots of polynomials $\hat{H}_k(l)$ and $\check{H}_k(l)$ respectively (they are real, positive and lie inside $[Q+1, 3Q]$ as we have proved). Numbers $\hat{\gamma}_k$ and $\check{\gamma}_k$ are some real positive constants. Next, we note that if $Q = 2$ then $\hat{\rho}_k(n) = O(1)$ and $\check{\rho}_k(n) = O(1)$ as $n \rightarrow \infty$. If $Q \geq 4$, then

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

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

Lemma 9. *The difference $\hat{y}_k - \check{y}_k$ tends to zero as $k \rightarrow \infty$.*

Proof. Using Lemma 7, similarly to the proof of Lemma 8, it may be shown that the first and second derivatives of the functions $\hat{H}_k(l)$ and $\check{H}_k(l)$ have exactly one root with absolute value exceeding $Q/2 + 1$. We denote them by $\tilde{y}_k$ and $\tilde{\check{y}}_k$ respectively (by (15) these values are the same for $\hat{H}_k$ and $\check{H}_k$).

Fig. 1: Trajectories traversed by roots of $\hat{H}_5(l)$ for t increasing from 0 to 1; the round mark corresponds to $t = 0$, the square mark corresponds to $t = 1$

Since the function $\check{H}_k(l)$ may take negative values, $\min \check{H}_k(l) < 0$ and $\arg \min \check{H}_k(l) < \check{y}_k$. At the same time $\arg \min \check{H}_k(l) = \check{y}_k$. Thus $\check{y}_k < \check{y}_k$.

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

$$\frac{Q}{2} + 1 \leq \check{\check{y}}_k < \check{y}_k < \check{y}_k < \hat{y}_k \leq 3Q.$$

Therefore functions $\hat{H}_k(l)$ and $\check{H}_k(l)$ are convex functions on the segment $[\check{y}_k, \hat{y}_k]$ of real axis, so for any $\delta \in [0, 1]$ the convexity inequality holds:

$$\hat{H}_k(\delta \check{\check{y}}_k + (1 - \delta) \hat{y}_k) \leq \delta \hat{H}_k(\check{y}_k) + (1 - \delta) \hat{H}_k(\hat{y}_k).$$

Note that

$$\check{y}_k = \tilde{y}_k + (1 - \delta)\hat{y}_k \quad \text{for } \delta = \frac{\hat{y}_k - \check{y}_k}{\hat{y}_k - \tilde{y}_k},$$

therefore, finally we get the following chain of inequalities:

$$\hat{H}_k(\check{y}_k) \leq \delta \hat{H}(\check{y}_k) + (1 - \delta) \underbrace{\hat{H}(\hat{y}_k)}_{=0} = \frac{\hat{y}_k - \check{y}_k}{\hat{y}_k - \tilde{y}_k} \hat{H}_k(\tilde{y}_k) \leq \frac{\hat{y}_k - \check{y}_k}{\frac{5Q}{2} - 1} \hat{H}_k\left(\frac{Q}{2} + 1\right),$$

where in the last inequality we use the fact that $\hat{H}_k(\check{y}_k)$ is the minimal value of function $\hat{H}_k$ on the ray $[\frac{Q}{2} + 1, +\infty)$ and also that $\hat{y}_k - \tilde{y}_k \leq \frac{5Q}{2} - 1$. For the constant

$$\nu_k = \check{H}_k(l) - \hat{H}_k(l)$$

Fig. 2: The plot of the function $\hat{H}_5(l)$

the equality $\widehat{H}_k(\check{y}_k) = -\nu_k$ obviously holds. Then we finally get:

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

It remains to show that the right part of the last inequality tends to zero as $k \rightarrow \infty$.

Note that $\nu_k \rightarrow 0$ as $k \rightarrow \infty$, because

$$\nu_k = \mathcal{Q}(2)(1 - \mathcal{Q}(-2^{-k})) \text{ and } \lim_{k \rightarrow \infty} \mathcal{Q}(-2^{-k}) = 1.$$

Then the following argument ends the proof:

$$\begin{aligned} \widehat{H}_k\left(\frac{Q}{2} + 1\right) &= \left(\frac{Q}{2} + 1\right)^{k+1} \\ &\quad - (1 + Q)\left(\frac{Q}{2} + 1\right)^k - \widehat{\varphi}_{k-1}\left(\frac{Q}{2} + 1\right)^k - \dots - \widehat{\varphi}_0 \\ &= -\frac{Q}{2}\left(\frac{Q}{2} + 1\right)^k - \widehat{\varphi}_{k-1}\left(\frac{Q}{2} + 1\right)^k - \dots - \widehat{\varphi}_0 \rightarrow -\infty \text{ as } k \rightarrow \infty. \end{aligned}$$

□

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

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

$$c_1 \check{z}^n \lesssim \mathbb{E}2^{q\eta_n} \lesssim c_2 \widehat{z}^n \text{ as } n \rightarrow \infty.$$

Proof. According to Lemma 8 polynomials $\widehat{H}_k(l)$ and $\check{H}_k(l)$ have exactly one root on $(\frac{Q}{2} + 1, \infty)$. From (8) and (17) (also (11) and (18)) it follows that

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

where $\widehat{\gamma}_k$ and $\check{\gamma}_k$ are the same as in (17) and (18) respectively, $\widehat{\gamma}'_k = \widehat{\gamma}_k(\widehat{y}_k - 1)/\widehat{y}_k$, $\check{\gamma}'_k = \check{\gamma}_k(\check{y}_k - 1)/\check{y}_k$. At the same time,

$$\check{f}_k(n) \leq f(n) \leq \widehat{f}_k(n),$$

so

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

$$\check{\gamma}'_k \check{y}_k^n \lesssim \tilde{f}(n) \lesssim 2\hat{\gamma}'_k \hat{y}_k^n = \hat{\gamma}''_k \hat{y}_k^n,$$

where $\hat{\gamma}''_k = 2\hat{\gamma}'_k$. Finally,

$$c_1 \check{z}^n = \check{\gamma}'_k \cdot \frac{\check{y}_k^n}{2^n} \lesssim \mathbb{E}2^{q\eta_n} \lesssim \hat{\gamma}''_k \cdot \frac{\hat{y}_k^n}{2^n} = c_2 \hat{z}^n,$$

moreover, Lemma 9 guarantees that $\hat{z}$ and $\check{z}$ may be made arbitrarily close. □

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

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

Table 1 helps to approximate the values of $\mathbb{E}Q^{\eta_n}$. For example, for $n = 64$ the theoretical estimate of $\mathbb{E}2^{\eta_n}$ lies between $3,75 \cdot 10^{13}$ and $7,50 \cdot 10^{13}$ and the exact value of $\mathbb{E}2^{\eta_n}$ is approximately $5,38 \cdot 10^{13}$.

Table 1 shows the values of $\tilde{y}$, c_1 and c_2 corresponding to different values of q . To fill the table we found the roots of characteristic polynomial of recurrences $\hat{F}_k(n)$ and $\check{F}_k(n)$ by halving the segment as it was done in the proof of Lemma 8. Then we iteratively calculated $\hat{F}_k(n)$ and $\check{F}_k(n)$ up to the value of n that gives necessary accuracy. Dividing by $\hat{y}_k^n$ and $\check{y}_k^n$ from (17)–(18) we evaluated approximate values of $\hat{\gamma}_k$ and $\check{\gamma}_k$ that finally gave c_1 and c_2 by the formulas from Theorem 2.

To find the exact value of $\mathbb{E}2^{\eta_n}$ we use the results of [2]. We enumerate all different distributions (called equivalence classes there) according to Theorem 1 (or, more precisely, formula (4)) of that paper. Then we count the size of each class, using the result of Theorem 3 of the current paper. After that the computation of expectation took little effort.

Table 1: Approximate values associated with $\mathbb{E}2^{q\eta_n}$ for different values of q

q	$\tilde{y}$	$\log_2 \tilde{y} - 1$	c_1	c_2
1	3.30921306134212177240	0.72648818154049951037	0.378	0.757
2	5.80027271324371478340	1.53612073348070167305	0.246	0.492
3	10.53733221939675028493	2.39743775493525848727	0.148	0.296
4	19.61999911051941379160	3.29425307103935297681	0.085	0.169
5	37.19179236569642652549	4.21691237160283720288	0.047	0.094
6	71.45569997172021204310	5.15897719358341460680	0.025	0.050
7	138.69767829225482267831	6.11579982787398693748	0.013	0.027
8	271.32073664755570805747	7.08385550468282259524	0.007	0.014
9	533.89365096936984102274	8.06040858243800754807	0.004	0.007

Now we can evaluate the variance of the random variable 2^{η_n} :

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

It is easy to observe from Table 1 that $(\mathbb{E}2^{\eta_n})^2 = o(\mathbb{E}2^{2\eta_n})$. Thus, the variance $\mathbb{D}2^{\eta_n}$ may be estimated by the second moment:

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

Finally we estimate the probability of deviating from the expectation $\mathbb{E}2^{\eta_n}$. We use the Tchebyshev inequality:

$$\mathbb{P}\left(|2^{\eta_n} - \mathbb{E}2^{\eta_n}| \geq a\right) \leq \frac{\mathbb{D}2^{\eta_n}}{a^2}.$$

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

$$\mathbb{P}\left(|2^{\eta_n} - \mathbb{E}2^{\eta_n}| \geq v^n \sqrt{\mathbb{D}2^{\eta_n}}\right) \leq \frac{1}{v^{2n}} \rightarrow 0 \text{ as } n \rightarrow \infty.$$

Thus with probability tending to one

$$2^{\eta_n} \leq \mathbb{E}2^{\eta_n} + v^n \sqrt{\mathbb{D}2^{\eta_n}}$$

or, for example,

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

Let us consider value $K_c(i)$ defined in the Introduction and satisfying (3). On Fig. 3 one can see that $K_{1/2}(i) \leq 2^{H_n^i}$ for $n = 32$ and $n = 64$. So at least in these cases our hypothesis is true. Besides, the ratio $2^{H_n^i}/K_{1/2}(i)$ is small.

Fig. 3: Distribution of $2^{732}/K_{1/2}(i)$ and $2^{764}/K_{1/2}(i)$

3. Sizes of equivalence classes

It turns out that there is a simple analytical formula for the size of any given equivalence class. Let n -bit number $i = (\alpha_{n-1}\alpha_{n-2}, \alpha_{n-3}, \dots, \alpha_0)$ be the index of a $(2^n \times 2^n)$ -matrix row and $i' = (\alpha_{n-2}, \alpha_{n-3}, \dots, \alpha_0)$. We can represent i' in the form

$$i' = \underbrace{11\dots1}_{k_1} \underbrace{0\dots0}_{\ell_1} \underbrace{1\dots1}_{k_2} \underbrace{0\dots0}_{\ell_2} \dots \underbrace{1\dots1}_{k_s} \underbrace{0\dots0}_{\ell_s},$$

where k_1 and ℓ_s may be equal to zero.

Theorem 3. *For each $i' \in [0, 2^{n-1} - 1]$ the i' -th row of the DDT-matrix of order 2^n belongs to an equivalence class of size*

$$\rho_{i'} = 2 \cdot C_K^{s-1} C_{s-1}^{c_1} C_{s-1-c_1}^{c_2} \dots C_{s-1-c_1-\dots-c_{n-2}}^{c_{n-1}},$$

where

(a) $K = k_1 + k_2 + \dots + k_s,$

(b) c_t is the number of j , $1 \leq j \leq s$, such that $\ell_j = t$, $1 \leq t \leq n$.

Proof. Row distributions of the second half of the DDT-matrix exactly repeat distributions of the first half, so it is sufficient to find a formula for the first part and multiply it by two.

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

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

and with each group $\ell_1, \dots, \ell_{s-1}$ a black one:

We have to find the number of variants to place $(K-1)$ white balls and $(s-1)$ black balls so that between any two black ones there is at least one white.

Let us imagine that the goal is to place $(s-1)$ partitions in a box with $(K-1)$ balls. We can put a partition on one of K places (between elements and on the both 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 coloured ones where each colour corresponds to a certain length of a group of zeros:

$$c_i = \text{colour}_i = |\{\ell_j \mid \ell_j = i, j = 1, \dots, s-1\}|, \quad i = 1, \dots, n.$$

Thus, in order to get all possible distribution of balls, that is, all possible row numbers included in the same equivalence class, it remains to calculate the number of ways to replace the $(s-1)$ black balls with coloured ones, provided that a set of coloured balls is given. It may be proved by induction that this number is

$$C_{s-1}^{c_1} C_{s-1-c_1}^{c_2} \dots C_{s-1-c_1-\dots-c_{n-2}}^{c_{n-1}}.$$

One can replace black balls with balls of the same colour in a unique way. Now assume that the formula is true for $(n-1)$ colours. Let us suppose that the numbers of balls of colours $1, \dots, n-1$ equal $c'_1, \dots, c'_{n-1}$ respectively. Then the number of variants is

$$C_{s-1}^{c'_1} C_{s-1-c'_1}^{c'_2} \dots C_{s-1-c'_1-\dots-c'_{n-3}}^{c'_{n-2}}.$$

Now let $(n-1)$ -th colour be actually a union of $(n-1)$ -th and n -th colour. In other words, $c'_1 = c_1, c'_2 = c_2, \dots, c'_{n-2} = c_{n-2}, c'_{n-1} = c_{n-1} + c_n$. Then

the number of variants to partition $(s - 1 - c_1 - \dots - c_{n-2})$ balls in two parts is $C_{s-1-c_1-\dots-c_{n-2}}^{c_{n-1}}$. $\square$

Fig. 4: Distribution of η_{32} and η_{64}

Usually one needs to do $\Omega(2^{3n})$ operations to calculate the distribution of η_n (to get the DDT-table and then calculate the entropy by definition). 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 our results on the enumeration of all classes in time proportional to their number the problem may 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. So for example for $n = 64$ we have accelerated the computation by $6.45 \cdot 10^{46}$ times.

Acknowledgement: The author thanks Lev Vysotsky for valuable help in calculations and bringing the original idea to mind and anonymous reviewers for lots of useful notes.

References

- [1] Lipmaa H., Moriai S., “Efficient algorithms for computing differential properties of addition”, *Fast Software Encryption*, Lect. Notes Comput. Sci., **2355**, 2002, 336–350.
- [2] Vysotskaya V. V., “Some properties of modular addition”, *Matematicheskie Voprosy Kriptografii*, **10:2** (2019), 75–88.
- [3] Greene D. H., Knuth D. E., *Mathematics for the Analysis of Algorithms*, (3 ed.), Basel: Birkhäuser, 1990, 132 pp.
- [4] Tyrtshnikov E., *A Brief Introduction to Numerical Analysis*, Basel: Birkhäuser, 1997, 202 pp.