V. V. Vysotskaya, Некоторые свойства модульного сложения,
Матем. вопр. криптогр., 2019, том 10, выпуск 2, 75–88

https://www.mathnet.ru/mvk285

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2019 Т. 10 № 2 С. 75–88

УДК 519.719.2 DOI https://doi.org/10.4213/mvk285

Some properties of modular addition

V. V. Vysotskaya

JSC "InfoTeCS", Moscow, Russia

Получено 06.II.2018

Abstract. We study a problem which emerged during an attempt to apply a differential cryptanalysis method to the "Magma" algorithm. We obtain a general formula of distribution in the difference distribution table of addition modulo 2^n and provide an efficient method for computing the distribution in a row with given index. By means of this formula an asymptotic estimate of the number of different distributions is established. Finally, we design an algorithm generating all distributions in $2^{O(\sqrt{(n)})}$ operations (whereas the corresponding brute-force method takes $2^{\Omega(n)}$ operations).

Key words: modular addition, partitions, differential cryptanalysis

Некоторые свойства модульного сложения

В. В. Высоцкая

ОАО «ИнфоТеКС», Москва, Россия

Аннотация. Исследуется задача, которая возникла при попытке применить разностный криптоанализ к алгоритму «Магма». Получена общая формула распределения в строке разностной таблицы сложения по модулю 2^n и построен эффективный метод вычисления распределения в строке с заданным номером. С помощью этой формулы найдена асимптотическая оценка числа различных распределений. В работе приводится также алгоритм генерации всех возможных распределений за $2^{O(\sqrt{n})}$ операций (соответствующий алгоритм, использующий полный перебор, требует $2^{\Omega(n)}$ операций).

Ключевые слова: модульное сложение, разбиения, разностный криптоанализ

Citation: *Mathematical Aspects of Cryptography*, 2019, v. 10, № 2, pp. 75–88 (Russian)

1. Introduction

The problem studied in the paper had emerged during an attempt to estimate the applicability of differential cryptanalysis to the Russian government standard symmetric key block cipher (GOST 28147-89) [1]. It is vital since the algorithm (called "Magma") is still present in the modern Russian GOST R 34.12-2015 of symmetric key block cipher [2].

Denote by $\mathbb{Z}_N$ the ring of residues modulo N. The first function under consideration is $f\colon \mathbb{Z}_{2^n}^2 \to \mathbb{Z}_{2^n}$ 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 the study of the function $P_n(\Delta x, \Delta f)\colon \mathbb{Z}_{2^n}^2 \to \mathbb{N}_0$:

$$P_n(\Delta x, \Delta f) = \left|\left\{(x,y) \in \mathbb{Z}_{2^n}^2 \colon \Delta f = f(x \oplus \Delta x, y) \oplus f(x,y)\right\}\right|$$

(it is analogous to a special case of the differential probability of addition modulo 2^n studied in [3]). Let us consider the table of values of P_n. In this table rows are indexed by Δx and columns by Δf. Such a table is usually called difference distribution table (DDT). Note that the sum of values in each row equals 2^{2n}. In what follows we will also identify the function P_n with DDT and use the same notation for both.

Let us introduce an equivalence relation on the rows of matrix P_n as follows: two rows are called *equivalent* if they coincide up to permutations of elements. Next, we study the set of equivalence classes into which the set of matrix rows are splitted. Let us call such equivalence classes by *distributions*.

Note. Let us consider the calculation of the number of different distributions or enumerating them as algorithmic problems. Then trivial (brute force) algorithm requires $2^{\Omega(n)}$ operations as one needs to calculate the value of Δf for all x, y, $\Delta x \in \{0, \ldots, 2^n - 1\}$. At the same time the algorithm based on the results presented in our paper requires polynomial in n number of operations for the first problem and $2^{O(\sqrt{n})}$ operations for the second.

2. Parametrization of distributions

Lemma 1. *Let matrix P_n be of the form*

$$P_n = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

Then matrix P_{n+1} *has the form*

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

The proof of Lemma 1 is given in [4].

This Lemma may be reformulated: if

$$P_n = 2^{n+1} \begin{bmatrix} A_n & B_n \\ B_n & A_n \end{bmatrix},$$

then

$$A_n = \begin{bmatrix} 2A_{n-1} & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}, \quad B_n = \begin{bmatrix} 0 & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}.$$

Note that an obvious corollary from this lemma is the fact that all elements of the matrix P_n are either zeros or powers of two.

Let us denote by $(\alpha_{n-1}, \alpha_{n-2}, \ldots, \alpha_1, \alpha_0)$ the binary representation of the number i. Then we match each distribution located in some row of matrix P_n with a polynomial in the following way. The row p_i corresponds to polynomial $\sum_{j=0}^{2n-1} c_j x^j$, where c_j is the amount of numbers 2^j in p_i. Hence multiplication of the row p_i by 2 results in the multiplication of corresponding polynomial by x. At the same time, the concatenation of two rows corresponds to the addition of polynomials. For polynomials $a_n^i(x)$ and $b_n^i(x)$ corresponding to i-th rows of A_n and B_n respectively we have:

$$a_n^i(x) = \begin{cases} x a_{n-1}^i(x) + b_{n-1}^i(x), & \text{if } \alpha_{n-2} = 0, \\ a_{n-1}^i(x) + b_{n-1}^i(x), & \text{if } \alpha_{n-2} = 1, \end{cases}$$

$$b_n^i(x) = \begin{cases} b_{n-1}^i(x), & \text{if } \alpha_{n-2} = 0, \\ a_{n-1}^i(x) + b_{n-1}^i(x), & \text{if } \alpha_{n-2} = 1. \end{cases}$$

Thus,

$$\begin{bmatrix} a_n^i(x) \\ b_n^i(x) \end{bmatrix} = W_{\alpha_{n-2}} \begin{bmatrix} a_{n-1}^i(x) \\ b_{n-1}^i(x) \end{bmatrix},$$

where

$$W_0 = \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix}, \quad W_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Moreover,

$$A_1 = \left[\,1\,\right],\ B_1 = \left[\,0\,\right],\ a_1 = 1,\ b_1 = 0.$$

Repeating the same argument $n-2$ more times we finally get

$$\begin{aligned} a_n^i(x) + b_n^i(x) &= \left[\,1\ 1\,\right] \begin{bmatrix} a_n^i(x) \\ b_n^i(x) \end{bmatrix} = \\ &= \left[\,1\ 1\,\right] W_{\alpha_{n-2}} W_{\alpha_{n-3}} \ \dots\ W_{\alpha_0} \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \end{aligned} \tag{1}$$

Let us denote by i' the number with binary representation

$$(\alpha_{n-2}, \alpha_{n-3}, \dots, \alpha_0).$$

This choice is based on the knowledge that the most significant bit α_{n-1} does not affect the distribution in the corresponding row. Let us separate runs of 0's and 1's in i'. We assume that the first one is a group of 1's, and the last one is a group of 0's (both may be empty). The number of 1's is $K = k_1 + k_2 + \dots + k_s$, the number of 0's is $L = \ell_1 + \dots + \ell_s$, and $L + K = n - 1$. Then

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

and expression (1) becomes

$$a_n^i(x) + b_n^i(x) = \left[\,1\ 1\,\right] W_1^{k_1} W_0^{\ell_1} \dots W_1^{k_s} W_0^{\ell_s} \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{2}$$

We will use the following statements, easily provable by induction:

$$W_1^k = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \cdots \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = 2^{k-1} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

$$W_0^\ell = \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix} \cdots \begin{bmatrix} x & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} x^\ell & x^{\ell-1} + x^{\ell-2} + \dots + 1 \\ 0 & 1 \end{bmatrix}.$$

Then (2) may be represented as

$$a_n^i(x) + b_n^i(x) = \left[\,1\ 1\,\right] \begin{bmatrix} 1 \\ 1 \end{bmatrix} 2^{k_1-1} \left[\,1\ 1\,\right] \begin{bmatrix} x^{\ell_1} & x^{\ell_1-1} + \dots + 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cdots$$

$$\dots \left[\,1\ 1\,\right] \begin{bmatrix} x^{\ell_s} & x^{\ell_s-1} + \dots + 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Note that

$$\begin{bmatrix}1 & 1\end{bmatrix}\begin{bmatrix}x^{\ell} & x^{\ell-1}+\cdots+1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1\\1\end{bmatrix}=x^{\ell}+x^{\ell-1}+x^{\ell-2}+\cdots+2.$$

Then

$$a_n^i(x)+b_n^i(x)=$$
$$=2\cdot 2^{K-s}(x^{\ell_1}+x^{\ell_1-1}+\cdots+2)\ \cdots\ (x^{\ell_s}+x^{\ell_s-1}+\cdots+2)x^{\ell_s}.$$

Hence

$$p_n^i(x)=2^{K-s+1}\prod_{j=1}^{s-1}(x^{\ell_j}+x^{\ell_j-1}+\cdots+2)x^{\ell_s}. \tag{3}$$

Let us denote by Q_n the set of tuples $(s,L,\ell_s,\widetilde{\ell})$, where $s\in\{1,\ldots,n-1\}$, $\ell_s\in\{0,\ldots,n-1\}, L\in\{0,\ldots,n-s\}$ and $\widetilde{\ell}$ is a multiset of $s-1$ positive integers summing up to $L-\ell_s$. We now want to prove that there is a one-to-one correspondence between the set of polynomials $p_n^i(x)$ and the set Q_n. It is obvious that for each polynomial $p_n^i(x)$ there exists a corresponding tuple $q_i\in Q_n$, and vice versa. So it is enough to show that if two polynomials are equal then corresponding sets of parameters coincides.

Let us fix numbers d_1 and d_2 and then compare two expressions

$$p_n^{d_1}(x)=2^{K'-s'+1}\prod_{j=1}^{s'-1}(x^{\ell'_j}+x^{\ell'_j-1}+\cdots+2)x^{\ell'_{s'}},$$

$$p_n^{d_2}(x)=2^{K''-s''+1}\prod_{j=1}^{s''-1}(x^{\ell''_j}+x^{\ell''_j-1}+\cdots+2)x^{\ell''_{s''}}.$$

If polynomials are equal, then

$$2^{K'-s'+1}x^{L'}=2^{K''-s''+1}x^{L''},$$

hence $L'=L''$ and

$$K'-s'+1=K''-s''+1.$$

Since the counts of 0's are equal, the counts of 1's are equal too, so $s'=s''$. Besides, the minimal degrees of monoms of the polynomials must coincide, hence $\ell'_{s'}=\ell''_{s''}$. Now it remains to prove that under stated assumptions the equality of polynomials also mean the equality of parameters $\ell'_1,\ldots,\ell'_{s'}$ and $\ell''_1,\ldots,\ell''_{s''}$ up to a permutation.

Let $\mathcal{G}_\ell(x) = x^\ell + x^\ell + \cdots + 2$. We now show that if

$$\prod_{j=1}^{s'-1} \mathcal{G}_{\ell'_j}(x) = \prod_{j=1}^{s''-1} \mathcal{G}_{\ell''_j}(x), \tag{4}$$

then the multiset $\{\mathcal{G}_{\ell'_j}(x)\}_{j=1}^{s'-1}$ equals to the multiset $\{\mathcal{G}_{\ell''_j}(x)\}_{j=1}^{s''-1}$, or in other words the decomposition of such polynomials into factors of form $\mathcal{G}_j(x)$ is unique. For this purpose we prove that polynomials $\mathcal{G}_j(x)$ are pairwise co-prime. Let us compute the greatest common divisor of $\mathcal{G}_u(x)$ and $\mathcal{G}_v(x)$ for $u > v$:

$$\begin{aligned}(\mathcal{G}_u(x), \mathcal{G}_v(x)) &= (x^u + x^{u-1} + \cdots + 2, x^v + x^{v-1} + \cdots + 2) = \\ &= (x^{u-v-1} + \cdots + 1, x^v + x^{v-1} + \cdots + 2) = \\ &= \left(\frac{x^{u-v} - 1}{x-1}, \frac{x^{v+1} - 1}{x-1} + 1\right) = \\ &= \frac{1}{x-1}\left(x^{u-v} - 1,\ x^{v+1} + x - 2\right).\end{aligned}$$

The roots of the polynomial $f(x) = x^{u-v} - 1$ are all roots of unity of the degree $(u - v)$. Let us check which of these roots may be roots of polynomial $h(x) = x^{v+1} + x - 2$.

Let

$$\varepsilon = \cos\frac{2\pi}{u-v} + i \cdot \sin\frac{2\pi}{u-v}$$

be a primitive root of unity of the degree $(u - v)$, then $\{\varepsilon^\ell\}_{\ell=0}^{u-v-1}$ is a set of all roots of unity of the degree $(u - v)$. So

$$\varepsilon^{\ell(v+1)} + \varepsilon^\ell - 2 = 0.$$

Therefore $\varepsilon^{\ell(v+1)} = \varepsilon^\ell = 1$, as $|\varepsilon^k| \leqslant 1$ for all k. Hence

$$\frac{1}{x-1}\left(x^{u-v} - 1, x^{v+1} + x - 2\right) = \frac{1}{x-1}(x-1) = 1.$$

Now let us return to the case (4). We decompose polynomials in the left and right sides into products of irreducible ones. Then we consider the first irreducible polynomial $f(x)$ in the left-hand side. In order for equality to hold, $f(x)$ also has to be present on the right-hand side. So there are some $\mathcal{G}_u$ on the left-hand side and $\mathcal{G}_v$ on the right-hand side divisible by $f(x)$. Hence, u must be equal to v. Dividing both sides by $\mathcal{G}_u$ and continuing in the same fashion, we arrive at the conclusion that the decomposition is unique up to a permutation.

Thus, we had proved the following statement.

Theorem 1. *There is a one-to-one correspondence between the set of distributions of the rows of matrix* P_n *and the set* Q_n *of tuples of parameters*.

Using Theorem 1 one can enumerate the distributions in time proportional to their number. More precisely, one can iterate over all distinct distributions and list them in time $O\left(|Q_n| \cdot \mathrm{poly}(n)\right)$, where $\mathrm{poly}(n)$ is a polynomial of n. The only tricky part is to enumerate all the multisets with given sum, but it may be done using one of various recursive algorithms in $O(1)$ amortized time per iteration (e. g. see [5]).

3. The number of distributions

Let $p(n,k)$ be the number of partitions of n into exactly k parts. Moreover, let $p(n,k) = 0$, if $k \leqslant 0$ or $n \leqslant 0$, but $p(0,0) = 1$.

If we fix s, L and ℓ_s then the number of tuples from the set Q_n with these parameters is equal to $p(L - \ell_s, s-1)$. Obviously there are only n tuples with $s = 1:\ (1,1,\ldots,1,1), (1,1,\ldots,1,0), \ldots, (1,0,\ldots,0,0), (0,0,\ldots,0,0)$. We will consider this case separately and we will assume that $s \geqslant 2$. Finally, note that

$$\sum_{L=\ell_s}^{n-s} p(L-\ell_s, s-1) = \sum_{L=0}^{n-s-\ell_s} p(L, s-1).$$

Then

$$|Q_n| = \left[\sum_{s=2}^{n-1}\sum_{\ell_s=0}^{n-1}\sum_{L=0}^{n-s-\ell_s} p(L, s-1)\right] + n. \tag{5}$$

We make one more note to be used later.

Lemma 2. $p(n,k) = p(n-1,k-1) + p(n-k,k)$.

Proof. Note that the partition of the number n into k parts may either include some number of 1's or not include any. In the first case, there is a one-to-one correspondence between such partitions and (unconstrained) partitions of $n-1$ into $k-1$ parts (just put additional 1 to a partition) – there are $p(n-1,k-1)$ of them. In the second case, there is a correspondence between such partitions and (unconstrained) partitions of $n-k$ into k parts (just add 1 to each number in partition) — there are $p(n-k,k)$ of them. □

We now show that the expression (5) may be simplified.

Theorem 2. $|Q_n| = \sum_{j=1}^{n-1} p(j) + 1$, *where* $p(j) = \sum_{s=1}^{j} p(j,s)$, $n > 3$.

Proof (by induction). For $n = 4$ formula (5) gives $|Q_4| = 7$. At the same time

$$p(3) + p(2) + p(1) + 1 = 3 + 2 + 1 + 1 = 7.$$

Let us show the induction step. In other words, we have to prove that identity transformations yield:

$$\sum_{s=2}^{n} \sum_{\ell_s=0}^{n} \sum_{L=0}^{n-s+1-\ell_s} p(L, s-1) - \sum_{s=2}^{n-1} \sum_{\ell_s=0}^{n-1} \sum_{L=0}^{n-s-\ell_s} p(L, s-1) =$$

$$= p(n) - 1,$$

$$\sum_{s=2}^{n} \sum_{\ell_s=0}^{n} \sum_{L=0}^{n-s+1-\ell_s} p(L, s-1) - \sum_{s=2}^{n-1} \sum_{\ell_s=0}^{n-1} \sum_{L=0}^{n-s-\ell_s} p(L, s-1) =$$

$$= \sum_{s=2}^{n-1} \left[\sum_{\ell_s=0}^{n} \sum_{L=0}^{n-s+1-\ell_s} p(L, s-1) - \sum_{\ell_s=0}^{n-1} \sum_{L=0}^{n-s-\ell_s} p(L, s-1) \right] +$$

$$+ \underbrace{\sum_{\ell_s=0}^{n} \sum_{L=0}^{n-n+1-\ell_s} p(L, n-1)}_{=0} =$$

$$= \sum_{s=2}^{n-1} \left[\sum_{\ell_s=0}^{n-1} \left[\sum_{L=0}^{n-s+1-\ell_s} p(L, s-1) - \sum_{L=0}^{n-s-\ell_s} p(L, s-1) \right] + \right.$$

$$\left. + \underbrace{\sum_{L=0}^{n+1-s-n} p(L, s-1)}_{=0} \right] =$$

$$= \sum_{s=2}^{n-1} \sum_{\ell_s=0}^{n-1} p(n+1-s-\ell_s, s-1).$$

Now we prove by induction that the latter is equal to $p(n) - 1$. For $n = 4$ both sides are equal to 4.

Induction step: let us check the validity of equation

$$
\begin{aligned}
&p(n+1)-1= \\
&=\sum_{s=2}^{n}\sum_{\ell_s=0}^{n} p(n+2-s-\ell_s,s-1)= \\
&=\sum_{s=2}^{n}\sum_{\ell_s=-1}^{n-1} p(n+1-s-\ell_s,s-1)= \\
&=\sum_{s=2}^{n-1}\sum_{\ell_s=0}^{n-1} p(n+1-s-\ell_s,s-1)+ \\
&\quad+\underbrace{\sum_{\ell_s=-1}^{n-1} p(n+1-n-\ell_s,n-1)}_{=p(1-\ell_s,n-1)=0}+\sum_{s=2}^{n} p(n+1-s-(-1),s-1)= \\
&=p(n)-1+\sum_{s=2}^{n} p(n+2-s,s-1).
\end{aligned}
$$

Since

$$
p(n)=\sum_{s=1}^{n} p(n,s),\ p(n+1)=\sum_{s=1}^{n+1} p(n+1,s),
$$

the equation becomes

$$
\sum_{s=1}^{n+1} p(n+1,s)=\sum_{s=1}^{n+1} p(n,s)+\sum_{s=1}^{n-1} p(n+1-s,s). \tag{6}
$$

Let us continue to transform the expression (6):

$$
\begin{aligned}
&\sum_{s=1}^{n} p(n+1,s)+\underbrace{p(n+1,n+1)}_{=1}= \\
&=\sum_{s=2}^{n+1} p(n,s-1)+\sum_{s=1}^{n} p(n+1-s,s)-\underbrace{p(n+1-n,n)}_{=p(1,n)=0}= \\
&=\sum_{s=1}^{n} p(n,s-1)+\underbrace{p(n,n)}_{=1}-\underbrace{p(n,0)}_{=0}+\sum_{s=1}^{n} p(n+1-s,s).
\end{aligned}
$$

Eventually,

$$\sum_{s=1}^{n} p(n+1,s) = \sum_{s=1}^{n} p(n,s-1) + \sum_{s=1}^{n-1} p(n+1-s,s).$$

Lemma 2 ends the proof. □

Theorem 2 makes it possible to solve the problem of counting all distributions. We just have to calculate values of $p(j,s)$ for $j \in \{1,\dots,n-1\}$, $s \in \{1,\dots,j\}$, then all the $p(j)$ and finally $|Q_n|$. The complexity of computing $p(j,s)$ dominates the other steps and according to Lemma 2 may be done in $O(n^2)$ additions of n-bit numbers. Thus we need $O(n^3)$ bit operations for the counting problem.

4. Asymptotic approximation

In [6] the following asymptotic formula for the number of partitions $p(n)$ was obtained:

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{\frac{2n}{3}}}.$$

Hence

$$|Q_n| \sim \sum_{j=1}^{n-1} \frac{1}{4\sqrt{3}j} e^{\pi\sqrt{\frac{2j}{3}}} + 1 \quad \text{as} \quad n \to \infty. \tag{7}$$

The equation (7) is a consequence of definition of Q_n and the following Lemma.

Lemma 3. *Let* $f(n) \sim g(n)$ *as* $n \to \infty$, $f(n) \geqslant 0$, $g(n) \geqslant 0$, $f(n)$ *and* $g(n)$ *monotonically increase and are unbounded*,

$$F(n) = \sum_{k=1}^{n} f(k), \quad G(n) = \sum_{k=1}^{n} g(k),$$

then

$$F(n) \sim G(n), \qquad n \to \infty.$$

You can find the proof of Lemma 3 in [4].

Lemma 4.

$$\sum_{j=1}^{n-2\sqrt{n}\ln n} \frac{1}{4\sqrt{3}j} e^{\pi\sqrt{\frac{2j}{3}}} = o\left(\frac{1}{4\sqrt{3}n} e^{\pi\sqrt{\frac{2n}{3}}}\right) \quad \text{as} \quad n \to \infty.$$

Proof. Let us show that

$$\lim_{n\to\infty} \sum_{j=1}^{n-2\sqrt{n}\ln n} \frac{n}{j}\, e^{\pi\sqrt{\frac{2}{3}}\left(\sqrt{j}-\sqrt{n}\right)} = 0.$$

Since

$$\frac{n}{j} \leqslant n, \quad j \leqslant n - 2\sqrt{n}\,\ln n \quad \text{and} \quad n - 2\sqrt{n}\ln n < n,$$

it is sufficient to prove that

$$\lim_{n\to\infty} n^2 e^{\pi\sqrt{\frac{2}{3}}\left(\sqrt{n-2\sqrt{n}\,\ln n}-\sqrt{n}\right)} = 0.$$

From

$$\begin{aligned}\sqrt{n - 2\sqrt{n}\ln n} &= \sqrt{n}\sqrt{1 - \frac{2\ln n}{\sqrt{n}}} = \\ &= \sqrt{n}\left(1 - \frac{2\ln n}{2\sqrt{n}} + o\left(\frac{\ln n}{\sqrt{n}}\right)\right) = \\ &= \sqrt{n} - \ln n + o(\ln n)\end{aligned}$$

it follows that

$$\begin{aligned}&\lim_{n\to\infty} n^2 e^{\pi\sqrt{\frac{2}{3}}\left(\sqrt{n-2\sqrt{n}\ln n}-\sqrt{n}\right)} = \\ &= \lim_{n\to\infty} n^2 e^{\pi\sqrt{\frac{2}{3}}(-\ln n+o(\ln n))} = \\ &= \lim_{n\to\infty} n^{2-\pi\sqrt{\frac{2}{3}}+o(1)}.\end{aligned}$$

Whereas the exponent is negative, Lemma is proved. □

Theorem 3.

$$\sum_{j=1}^{n} p(j) \sim \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} \quad as \quad n \to \infty.$$

Proof. It may be proved that there exists a number N_0 such that the function on the right-hand side monotonically increases on $[N_0; +\infty)$. We will estimate the sum from N_0 to n as the first $N_0 - 1$ summands do not influence the asymptotic.

The following holds as $n \to \infty$:

$$\sum_{j=N_0}^{n} p(j)! \sim \int_{N_0}^{n} \frac{e^{\pi\sqrt{\frac{2x}{3}}} dx}{4\sqrt{3}x} =$$

$$= \int_{N_0}^{n} \frac{1}{2\sqrt{2}\pi\sqrt{x}} de^{\pi\sqrt{\frac{2x}{3}}} =$$

$$= \frac{e^{\pi\sqrt{\frac{2x}{3}}}}{2\sqrt{2}\pi\sqrt{x}}\Bigg|_{N_0}^{n} + \int_{N_0}^{n} \frac{e^{\pi\sqrt{\frac{2x}{3}}}}{2\sqrt{2}\pi x^{3/2}} dx =$$

$$= \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} - \frac{e^{\pi\sqrt{\frac{2N_0}{3}}}}{2\sqrt{2}\pi\sqrt{N_0}} + \int_{N_0}^{n} \frac{e^{\pi\sqrt{\frac{2x}{3}}}}{2\sqrt{2}\pi x^{3/2}}\, dx.$$

Now we will show that the last two summands here are $o\left(e^{\pi\sqrt{2n/3}} / \sqrt{n}\right)$. For the first of them it is obvious, so let us focus on the second. For this purpose we note that

$$\sum_{j=N_0}^{n-1} f(j) \leqslant \int_{N_0}^{n} f(x)dx \leqslant \sum_{j=N_0+1}^{n} f(j)$$

for non-decreasing function f. So by Lemma 4

$$\int_{N_0}^{n} \frac{e^{\pi\sqrt{\frac{2x}{3}}}}{2\sqrt{2}\pi x^{3/2}} \leqslant \sum_{j=N_0+1}^{n} \frac{e^{\pi\sqrt{\frac{2j}{3}}}}{2\sqrt{2}\pi j^{3/2}} \sim \sum_{j=n-2\sqrt{n}\ln n}^{n} \frac{e^{\pi\sqrt{\frac{2j}{3}}}}{2\sqrt{2}\pi j^{3/2}} \leqslant$$

$$\leqslant \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi(n - 2\sqrt{n}\ln n)^{\frac{3}{2}}} \cdot 2\sqrt{n}\ln n \sim \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{\sqrt{2}\pi n^{\frac{3}{2}}}\sqrt{n}\ln n =$$

$$= \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{\sqrt{2}\pi n}\ln n.$$

Finally for $n \to \infty$

$$\left(\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{\sqrt{2}\pi n}\ln n\right)\left(\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{\sqrt{n}}\right)^{-1} = \frac{\ln n}{\sqrt{2}\,\pi\sqrt{n}} \to 0.$$

In addition,

$$\sum_{j=N_0+1}^{n} f(x) - \sum_{j=N_0}^{n-1} f(x) = f(n) - f(N_0) = \\ = \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4\sqrt{3}\,n} - \frac{e^{\pi\sqrt{\frac{2N_0}{3}}}}{4\sqrt{3}\,N_0} = \\ = o\left(\frac{e^{\pi\sqrt{\frac{2n}{3}}}}{\sqrt{n}}\right)$$

and the following asymptotic relations

$$\sum_{j=1}^{n} p(j) \sim \sum_{j=N_0}^{n} p(j) \sim \sum_{j=N_0}^{n} \frac{e^{\pi\sqrt{\frac{2j}{3}}}}{4\sqrt{3}j} \sim \int_{N_0}^{n} \frac{e^{\pi\sqrt{\frac{2x}{3}}}}{4\sqrt{3}x}dx$$

conclude the proof of the Theorem. □

According to the above Theorem and the note after Theorem 1 we can enumerate all the distributions in time $2^{O(\sqrt{n})}$ that is obviously substantially better than brute force algorithm with complexity $2^{\Omega(n)}$.

5. Conclusion

We obtain a general form of distributions in DDT. Moreover, we provide an efficient method for computing the distribution in a row with given index. The obtained results imply a possibility to substantially accelerate the construction of all possible distributions. We show that all distributions may be generated in time proportional to the amount of them. We have proved that the number of distinct distributions is $2^{O(\sqrt{n})}$, so the whole generating algorithm would take $2^{O(\sqrt{n})}$ operations. At the same time the brute-force algorithm requires $2^{\Omega(n)}$ operations.

References

[1] *GOST 28147-89. National Standard of the USSR. Cryptographic Protection for Data Processing System*, M.: Standardinform, 1996 (in Russian).

[2] *GOST R 34.12-2015. National Standard of the Russian Federation. Cryptographic Data Security. Block Ciphers*, M.: Standardinform, 2016 (in Russian).

[3] Lipmaa H., Moriai S., "Efficient algorithms for computing differential properties of addition", *Lect. Notes Comput. Sci.*, **2355** (2002), 336–350.

[4] Vysotskaya V., *Some properties of modular addition (Extended abstract)*, Cryptology ePrint Archive https://eprint.iacr.org/2018/1103, 2018.

[5] Kelleher J., O'Sullivan B., "Generating all partitions: a comparison of two encodings" (2009), arXiv: http://arxiv.org/abs/0909.2331.

[6] Hardy G. H., Ramanujan S., "Asymptotic formulæ in combinatory analysis", *Proc. London Math. Soc.* (2), **XVII**:1 (2018), 75–115.