Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, И. А. Круглов, Моменты весового дефицита случайной равновероятной инволюции, действующей на векторном пространстве над полем из двух элементов, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 4, 101–124

DOI: <https://doi.org/10.4213/mvk272>

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: 54.92.164.108

26 апреля 2023 г., 15:41:20

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ

2018 Т. 9 № 4 С. 101–124

УДК 519.212.2

DOI <https://doi.org/10.4213/mvk272>

Моменты весового дефицита случайной равновероятной инволюции, действующей на векторном пространстве над полем из двух элементов

В. Н. Сачков, И. А. Круглов

Академия криптографии Российской Федерации, Москва

Получено 18.IV.2018

Аннотация. Для аддитивной группы векторного пространства растущей размерности m над полем из двух элементов исследуются моменты случайной величины, равной значению весового дефицита случайной равновероятной инволюции, образованной произведением 2^{m-1} независимых двоичных циклов. Получены точные и асимптотические формулы для биномиальных моментов, а также для дисперсии.

Ключевые слова: случайные инволюции, весовой дефицит, биномиальные моменты

Moments of the weight deficit of a random equiprobable involution acting on a vector space over a field of two elements

V. N. Sachkov, I. A. Kruglov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. For the additive group of a vector space of increasing dimension m over a field of two elements we study the moments of a random variable equal to the weight deficit of a random equiprobable involution formed by the product of 2^{m-1} independent binary cycles. Exact and asymptotic formulas for the binomial moments and for the variance are obtained.

Key words: random involutions, weight deficit, binomial moments

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 101–124 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

В настоящей работе *инволюцией*, действующей на аддитивной группе $(E_{2^m}, +)$ векторного пространства размерности m над полем из двух элементов, называется произвольная подстановка множества E_{2^m} , образованная произведением 2^{m-1} независимых двоичных циклов. Множество независимых двоичных циклов в разложении заданной инволюции J определено однозначно. Каждый двоичный цикл из этого множества будем называть *двоичным циклом* J , инволюцию J можно отождествить с множеством ее двоичных циклов.

Множество $\mathcal{F}(A_{2^m})$ инволюций, действующих на группе $(E_{2^m}, +)$, есть множество инволюций, соответствующих таблице Кэли A_{2^m} группы E_{2^m} , см. [1].

В [2, 3] для инволюций введено понятие *весового дефицита*. Весом двоичного цикла (ν, μ) , $\nu, \mu \in E_{2^m}$, назовем элемент $\nu + \mu$ пространства E_{2^m} . Весовым дефицитом $d(J)$ инволюции J называется величина $d(J) = 2^m - 1 - v(J)$, где $v(J)$ — число различных весов двоичных циклов J .

В настоящей работе продолжено изучение характеристик случайной величины ζ_{2^m} , равной значению весового дефицита случайной инволюции J , которая выбрана равновероятно из множества инволюций, действующих на аддитивной группе $(E_{2^m}, +)$. Любые два векторных пространства над полем из двух элементов размерности m изоморфны, следовательно, распределения случайных величин ζ_{2^m} , соответствующих этим пространствам, совпадают. Поэтому далее E_{2^m} — арифметическое векторное пространство строк длины m над полем $E_2 = \{0, 1\}$.

Далее при любых линейно независимых элементах $\nu_{t-1}, \dots, \nu_0 \in E_{2^m}$ методом включения-исключения получены точные формулы для биномиальных моментов и для распределения случайной величины, равной числу двоичных циклов инволюции J , которые также являются двоичными циклами одной из трансляций группы E_{2^m} , соответствующих выбранным элементам $\nu_{t-1}, \dots, \nu_0$. Показано, что при фиксации линейно независимых элементов $\nu_{t-1}, \dots, \nu_0$ и стремлении m к бесконечности распределение этой случайной величины сходится к распределению Пуассона с параметром $t/2$.

На основе этих результатов получены точные и асимптотические формулы для биномиальных моментов ζ_{2^m} . А именно, для биномиального момента порядка $t \geq 1$ при $m \rightarrow \infty$ имеет место асимптотическое равенство

$$B_t(\zeta_{2^m}) = \frac{1}{t!} \left(\frac{2^m}{\sqrt{e}} \right)^t (1 + o(1)).$$

Для дисперсии доказана асимптотическая формула

$$D(\zeta_{2^m}) = 2^m \frac{2\sqrt{e} - 3}{2e} + O(1), \quad m \rightarrow \infty.$$

1. Случайные инволюции с данным числом одинаковых двоичных циклов с инволюциями, соответствующими трансляциям векторного пространства

Введем обозначения. При фиксированном $m \geq 1$ двоичный вектор $(\varepsilon_{m-1}, \dots, \varepsilon_1, \varepsilon_0)$ длины m будем отождествлять с целым неотрицательным числом $\varepsilon_{m-1} \cdot 2^{m-1} + \dots + \varepsilon_1 \cdot 2 + \varepsilon_0$. Таким образом, множество элементов двоичного арифметического пространства векторов длины m есть множество $E_{2^m} = \{0, 1, \dots, 2^m - 1\}$. При любом m пространство E_{2^m} является подпространством в $E_{2^{m+1}}$. Если некоторые элементы $\nu_{t-1}, \dots, \nu_0 \in E_{2^m}$ линейно независимы над полем $E_2 = \{0, 1\}$, то эти элементы будут линейно независимыми элементами пространства E_{2^n} при любом $n \geq m$.

Ранее в [1] для любого $\nu \in E_{2^m} \setminus 0$ была определена равновесная инволюция I_ν , соответствующая серии элементов веса ν в таблице Кэли A_{2^m} аддитивной группы пространства E_{2^m} . Если

$$E_{2^m} = \bigcup_{i=0}^{2^{m-1}-1} \{u_i, u_i + \nu\}$$

— разложение группы E_{2^m} на смежные классы по подгруппе $\{0, \nu\}$, то разложение I_ν в произведение независимых циклов имеет вид

$$I_\nu = (u_0, u_0 + \nu) \dots (u_{2^{m-1}-1}, u_{2^{m-1}-1} + \nu).$$

Предположим, что инволюция J выбрана случайно и равновероятно из множества $\mathcal{F}(A_{2^m})$. Для любых элементов $\nu_{t-1}, \dots, \nu_0 \in E_{2^m} \setminus 0$, $1 \leq t \leq m$, обозначим через $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$ случайную величину, равную числу двоичных циклов инволюции J , каждый из которых также является двоичным циклом одной из инволюций $I_{\nu_{t-1}}, \dots, I_{\nu_0}$. Кроме того, для любого $k \geq 0$ обозначим через $B_k(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)})$ биномиальный момент k -го порядка случайной величины $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$.

Рассмотрим множество двоичных циклов

$$D^{(t)} = \{(\nu, \nu + 2^j) \mid \nu = 0, 1, \dots, 2^t - 1; j = 0, 1, \dots, t-1\}.$$

Положим $n_{t,1} = |D^{(t)}| = 2^t \cdot t$. Для любого $h = 2, 3, \dots, 2^{t-1}$ обозначим через $n_{t,h}$ число способов так выбрать подмножество D_h из h двоичных циклов, лежащих в множестве $D^{(t)}$, чтобы любые два различных двоичных цикла из подмножества D_h были независимы (т. е. двоичные циклы из множества D_h попарно независимы).

Далее, обозначим через $\mathcal{Z}_{2^m}^{(t)}$ множество всех последовательностей $(\nu_{t-1}, \dots, \nu_0)$, где $1 \leq \nu_{t-1} < \dots < \nu_0 \leq 2^m$, элементы которых линейно независимы над полем E_2 как элементы пространства E_{2^m} . При любом $m \geq t$ имеем равенство

$$|\mathcal{Z}_{2^m}^{(t)}| = \frac{1}{t!} (2^m - 1) \dots (2^m - 2^{t-1}). \quad (1.1)$$

Ниже

$$(l)_k = l(l-1) \dots (l-k+1)$$

— символ Жордана.

Теорема 1. При любой последовательности $(\nu_{t-1}, \dots, \nu_0) \in \mathcal{Z}_{2^m}^{(t)}$ элементов пространства E_{2^m} для распределения случайной величины $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$ имеют место формулы

$$\mathbf{P}(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)} = r) = \sum_{k=r}^{2^{m-1}} (-1)^{k-r} \binom{k}{r} B_k(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}), \quad r = 0, 1, \dots, 2^{m-1}. \quad (1.2)$$

При этом $B_0(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}) = 1$, и для любого $k = 1, \dots, 2^{m-1}$ выполнено равенство

$$B_k(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}) = \sum_{\sum j \beta_j = k} \frac{(2^{m-t})_{(\beta_{2^{t-1}} + \dots + \beta_1)}}{\beta_{2^{t-1}}! \dots \beta_1!} n_{t, 2^{t-1}}^{\beta_{2^{t-1}}} \dots n_{t, 1}^{\beta_1} \frac{2^k \cdot (2^{m-1})_k}{(2^m)_{2k}}. \quad (1.3)$$

В правой части равенства (1.3) суммирование осуществляется по всем разбиениям числа k на слагаемые, не превосходящие 2^{t-1} :

$$k = \sum j \beta_j = 2^{t-1} \cdot \beta_{2^{t-1}} + \dots + 2 \cdot \beta_2 + \beta_1, \quad 0 \leq \beta_j \leq \left\lfloor \frac{k}{j} \right\rfloor.$$

Равенства (1.2) являются частным случаем известных соотношений между распределением и биномиальными моментами случайной величины с конечным множеством возможных значений (см. [4]).

Для доказательства равенств (1.3) в первую очередь покажем, что случайные величины $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$, $(\nu_{t-1}, \dots, \nu_0) \in \mathcal{Z}_{2^m}^{(t)}$, при фиксированном значении m одинаково распределены, т.е. для любых линейно независимых над E_2 элементов $\nu_{t-1}, \dots, \nu_0$ распределение $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$ совпадает с распределением $\xi_{2^m}^{(2^{t-1}, \dots, 1)}$.

Элементы $2^{t-1}, \dots, 1$ входят в базис $2^{m-1}, 2^{m-2}, \dots, 2, 1$ пространства E_{2^m} над полем E_2 . Так как элементы $\nu_{t-1}, \dots, \nu_0$ линейно независимы над полем E_2 , то существует базис пространства E_{2^m} вида $\nu_{m-1}, \nu_{m-2}, \dots, \nu_{t-1}, \dots, \nu_0$. Отображение базисов

$$\varphi(2^i) = \nu_i, \quad i = 0, 1, \dots, m-1,$$

однозначно по линейности продолжается до линейного обратимого преобразования φ векторного пространства E_{2^m} . Для любой инволюции $J = (i_1, j_1) \dots (i_{2^{m-1}}, j_{2^{m-1}})$, $J \in \mathcal{F}(A_{2^m})$, положим

$$\varphi(J) = (\varphi(i_1), \varphi(j_1)) \dots (\varphi(i_{2^{m-1}}), \varphi(j_{2^{m-1}})), \quad \varphi(J) = \varphi^{-1} \cdot J \cdot \varphi.$$

Таким образом, мы рассматриваем φ и как биективное преобразование множества инволюций $\mathcal{F}(A_{2^m})$. Так как φ — линейное, то вес двоичного цикла $(\varphi(i), \varphi(j))$ равен $\varphi(i+j)$. Следовательно, $\varphi(I_{2^i}) = I_{\nu_i}$ при любом $i = 0, 1, \dots, m-1$.

Рассмотрим множество

$$D_{2^m}^{(\nu_{t-1}, \dots, \nu_0)} = \{(\nu, \nu + \nu_j) \mid \nu \in E_{2^m}, j = 0, \dots, t-1\}$$

всех двоичных циклов инволюций $I_{\nu_{t-1}}, \dots, I_{\nu_0}$, а также аналогичное множество $D_{2^m}^{(2^{t-1}, \dots, 1)}$ всех двоичных циклов инволюций $I_{2^{t-1}}, \dots, I_1$. Имеем равенства

$$|D_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}| = |D_{2^m}^{(2^{t-1}, \dots, 1)}| = 2^{m-1}t.$$

Для любой инволюции $J \in \mathcal{F}(A_{2^m})$ число двоичных циклов J , которые являются циклами одной из инволюций $I_{2^{t-1}}, \dots, I_1$, совпадает с числом двоичных циклов $\varphi(J)$, которые являются циклами одной из инволюций $I_{\nu_{t-1}}, \dots, I_{\nu_0}$. Следовательно, для любого $r = 0, \dots, 2^{m-1}$ преобразование φ переводит множество инволюций $J \in \mathcal{F}(A_{2^m})$, у которых ровно r двоичных циклов являются элементами множества $D_{2^m}^{(2^{t-1}, \dots, 1)}$, на множество инволюций, у которых ровно r двоичных циклов являются элементами множества $D_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$.

Ввиду биективности преобразования φ отсюда следует совпадение распределений $\xi_{2^m}^{(2^{t-1}, \dots, 1)}$ и $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$. Таким образом, ниже при доказательстве достаточно ограничиться случаем $\nu_{t-1} = 2^{t-1}, \dots, \nu_0 = 1$.

Занумеруем элементы множества $D_{2^m}^{(2^{t-1}, \dots, 1)}$ в произвольном порядке

$$D_{2^m}^{(2^{t-1}, \dots, 1)} = \{(i_1, j_1), \dots, (i_{2^{m-1}t}, j_{2^{m-1}t})\}.$$

Определим свойства $C_1, \dots, C_{2^{m-1}t}$: инволюция $J \in \mathcal{F}(A_{2^m})$ обладает свойством C_s , если цикл (i_s, j_s) является двоичным циклом J . С использованием формулы включения-исключения при любом $r = 0, 1, \dots, 2^{m-1}$ имеем формулу для числа $N_r^{(2^{t-1}, \dots, 1)}(A_{2^m})$ инволюций $J \in \mathcal{F}(A_{2^m})$, у которых ровно r двоичных циклов содержатся в множестве $D_{2^m}^{(2^{t-1}, \dots, 1)}$ (т. е. являются циклами одной из инволюций $I_{2^{t-1}}, \dots, I_1$):

$$N_r^{(2^{t-1}, \dots, 1)}(A_{2^m}) = \sum_{k=r}^{2^{m-1}t} (-1)^{k-r} \binom{k}{r} S_{k, 2^m}^{(2^{t-1}, \dots, 1)}, \quad (1.4)$$

где

$$S_{k, 2^m}^{(2^{t-1}, \dots, 1)} = \sum_{1 \leq s_1 < \dots < s_k \leq 2^{m-1}t} |M(C_{s_1}, \dots, C_{s_k})|, \quad (1.5)$$

$M(C_{s_1}, \dots, C_{s_k})$ — множество инволюций $J \in \mathcal{F}(A_{2^m})$, обладающих свойствами $C_{s_1}, \dots, C_{s_k}$, и суммирование в (1.5) осуществляется по всем k -сочетаниям номеров из множества $\{1, \dots, 2^{m-1}t\}$.

Любые два различных двоичных цикла произвольной инволюции $J \in \mathcal{F}(A_{2^m})$ независимы. Отсюда следует, что если среди двоичных циклов

$$(i_{s_1}, j_{s_1}), \dots, (i_{s_k}, j_{s_k}) \in D_{2^m}^{(2^{t-1}, \dots, 1)}, \quad 1 \leq s_1 < \dots < s_k \leq 2^{m-1}t,$$

имеется хотя бы одна пара различных зависимых циклов, то выполнено равенство $M(C_{s_1}, \dots, C_{s_k}) = \emptyset$. В частности, в сумме (1.4) можно заменить верхний индекс суммирования на 2^{m-1} .

Если же двоичные циклы заданного набора

$$(i_{s_1}, j_{s_1}), \dots, (i_{s_k}, j_{s_k}) \in D_{2^m}^{(2^{t-1}, \dots, 1)}, \quad 1 \leq s_1 < \dots < s_k \leq 2^{m-1}t,$$

попарно независимы, то множество $M(C_{s_1}, \dots, C_{s_k})$ совпадает с множеством $\mathcal{F}(A_{2^m}[i_{s_1}, j_{s_1}, \dots, i_{s_k}, j_{s_k}])$ всех инволюций $J \in \mathcal{F}(A_{2^m})$, двоичными циклами которых являются $(i_{s_1}, j_{s_1}), \dots, (i_{s_k}, j_{s_k})$.

Подмножества множества $\mathcal{F}(A_{2^m})$ будем рассматривать как мультимножества над порождающим множеством $\mathcal{F}(A_{2^m})$. Для любых мультимножеств M, N над $\mathcal{F}(A_{2^m})$ через $M \uplus N$ обозначим объединение мультимножеств. Так как $|M \uplus N| = |M| + |N|$, то равенство (1.5) можно переписать в виде

$$\begin{aligned} S_{k, 2^m}^{(2^{t-1}, \dots, 1)} &= |\mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)}|, \\ \mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)} &= \biguplus_{1 \leq s_1 < \dots < s_k \leq 2^m} M(C_{s_1}, \dots, C_{s_k}). \end{aligned} \quad (1.6)$$

Множество $E_{2^m} = \{0, 1, \dots, 2^m - 1\}$ есть объединение 2^{m-t} попарно непересекающихся подмножеств

$$\{2^t q, 2^t q + 1, \dots, 2^t q + 2^t - 1\}, \quad q = 0, 1, \dots, 2^{m-t} - 1.$$

Одновременно множество $D_{2^m}^{(2^{t-1}, \dots, 1)}$ является объединением 2^{m-t} попарно не пересекающихся подмножеств:

$$D_{2^m}^{(2^{t-1}, \dots, 1)} = \bigcup_{q=0}^{2^{m-t}-1} D_{2^m, q}^{(2^{t-1}, \dots, 1)},$$

в котором

$$D_{2^m, q}^{(2^{t-1}, \dots, 1)} = \{(\nu, \nu + 2^j) \mid \nu = 2^t q, \dots, 2^t q + 2^t - 1; j = 0, 1, \dots, t-1\} \quad (1.7)$$

для любого $q = 0, 1, \dots, 2^{m-t} - 1$.

Отметим, что любые два двоичных цикла, выбранные из различных множеств вида (1.7), независимы. Кроме того, из каждого множества (1.7) можно выбрать не более 2^{t-1} попарно независимых двоичных циклов.

Для любого $h = 1, \dots, 2^{t-1}$ число способов так выбрать подмножество D_h из h двоичных циклов, лежащих в множестве (1.7), чтобы двоичные циклы из подмножества D_h были попарно независимы, не зависит от номера q множества (1.7) и от размерности m пространства E_{2^m} . Это число совпадает с величиной $n_{t, h}$, введенной до формулировки теоремы.

Используя введенные обозначения, можно предложить следующий алгоритм перечисления элементов мультимножества $\mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)}$. При описании алгоритма предполагается, что значение m достаточно велико по сравнению с t и k .

Алгоритм 1.

Шаг 0. Выберем разбиение числа k на слагаемые, не превосходящие 2^{t-1} :

$$k = 2^{t-1} \cdot \beta_{2^{t-1}} + \dots + 2 \cdot \beta_2 + \beta_1, \quad 0 \leq \beta_j \leq \left\lfloor \frac{k}{j} \right\rfloor.$$

Шаг 1. Из множества $\{0, 1, \dots, 2^{m-t} - 1\}$ выберем $\beta_{2^{t-1}}$ номеров $0 \leq q_1 < q_2 < \dots < q_{\beta_{2^{t-1}}} \leq 2^{m-t} - 1$ и из каждого множества $D_{2^m, q_i}^{(2^{t-1}, \dots, 1)}$, $i = 1, \dots, \beta_{2^{t-1}}$, возьмем произвольное подмножество $D_{2^{t-1}}^{(i)}$ мощности 2^{t-1} с попарно независимыми двоичными циклами.

Шаг 2. Из множества *не использованных на шаге 1 номеров* выберем $\beta_{2^{t-1}-1}$ *новых* номеров $0 \leq q_1 < q_2 < \dots < q_{\beta_{2^{t-1}-1}} \leq 2^{m-t} - 1$ и из каждого множества $D_{2^m, q_i}^{(2^{t-1}, \dots, 1)}$, $i = 1, \dots, \beta_{2^{t-1}-1}$, возьмем произвольное подмножество $D_{2^{t-1}-1}^{(i)}$ мощности $2^{t-1} - 1$ с попарно независимыми двоичными циклами.

И так далее.

Шаг $2^{t-1} - 1$. Из множества *не использованных номеров на предыдущих шагах* с номерами $1, \dots, 2^{t-1} - 2$ выберем β_2 *новых* номеров $0 \leq q_1 < q_2 < \dots < q_{\beta_2} \leq 2^{m-t} - 1$ и из каждого множества $D_{2^m, q_i}^{(2^{t-1}, \dots, 1)}$, $i = 1, \dots, \beta_2$, возьмем произвольное подмножество $D_2^{(i)}$, состоящее из двух независимых двоичных циклов.

Шаг 2^{t-1} . Из множества *не использованных номеров на предыдущих шагах* $1, \dots, 2^{t-1} - 1$ выберем β_1 *новых* номеров $0 \leq q_1 < q_2 < \dots < q_{\beta_1} \leq 2^{m-t} - 1$ и из каждого множества $D_{2^m, q_i}^{(2^{t-1}, \dots, 1)}$, $i = 1, \dots, \beta_1$, возьмем произвольное подмножество $D_1^{(i)}$, состоящее из одного двоичного цикла.

В результате выполнения шагов $1, \dots, 2^{t-1}$ алгоритма 1 мы получим множество двоичных циклов

$$\{(a_1, b_1), (a_2, b_2), \dots, (a_k, b_k)\} = \bigcup_{h=1}^{2^{t-1}} \bigcup_{i=1}^{\beta_h} D_h^{(i)} \quad (1.8)$$

мощности k с попарно независимыми двоичными циклами.

Шаг $2^{t-1} + 1$. Из матрицы суммирования A_{2^m} абелевой группы E_{2^m} вычеркнем строки и столбцы с номерами из множества $\{a_1, b_1, \dots, a_k, b_k\}$. К полученной таблице $A_{2^m}[a_1, b_1, \dots, a_k, b_k]$ применим алгоритм перечисления инволюций из § 3 работы [3]. В результате мы получим все элементы множества $\mathcal{F}(A_{2^m}[a_1, b_1, \dots, a_k, b_k])$, ровно один раз каждый.

Алгоритм 1 завершает работу после перебора всех вариантов на шагах с номерами от 0 до $(2^{t-1} + 1)$. В результате работы алгоритма 1 будет получено некоторое подмножество мультимножества инволюций $\mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)}$.

Предположим, что у некоторой инволюции $J \in \mathcal{F}(A_{2^m})$ ровно $z \geq k$ двоичных циклов $(i_{s_1}, j_{s_1}), \dots, (i_{s_z}, j_{s_z})$ содержатся в множестве $D_{2^m}^{(2^{t-1}, \dots, 1)}$. Найдем число способов получить на выходе алгоритма 1 инволюцию J .

Любое подмножество

$$\{(a_1, b_1), (a_2, b_2), \dots, (a_k, b_k)\} \subset \{(i_{s_1}, j_{s_1}), \dots, (i_{s_z}, j_{s_z})\}$$

может быть единственным способом представлено как объединение вида (1.8), в котором при любых $h = 1, \dots, 2^{t-1}$ и $i = 1, \dots, \beta_h$ множество $D_h^{(i)}$ содержится в одном из множеств $D_{2^m, q}^{(2^{t-1}, \dots, 1)}$ и имеет число элементов $|D_h^{(i)}| = h$. Следовательно, число способов получить на выходе шага 2^{t-1} алгоритма 1 множество $\{(a_1, b_1), (a_2, b_2), \dots, (a_k, b_k)\}$, которое является подмножеством множества $\{(i_{s_1}, j_{s_1}), \dots, (i_{s_z}, j_{s_z})\}$, равно $\binom{z}{k}$. Это число совпадает с числом подмножеств $M(C_{s_1}, \dots, C_{s_k})$ из правой части формулы (1.5), которые содержат инволюцию J . Далее на шаге $2^{t-1} + 1$ алгоритма 1 полученное множество $\{(a_1, b_1), (a_2, b_2), \dots, (a_k, b_k)\}$ будет однократно дополнено до инволюции J .

В итоге алгоритм 1 перечислит все элементы мультимножества $\mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)}$ в полном соответствии с их кратностью в этом мультимножестве.

Таким образом, для вычисления величины

$$S_{k, 2^m}^{(2^{t-1}, \dots, 1)} = |\mathfrak{S}_{k, 2^m}^{(2^{t-1}, \dots, 1)}|$$

достаточно подсчитать число возможных вариантов инволюций, возникающих на выходе шага $2^{t-1} + 1$ алгоритма 1.

Количество вариантов подмножества (1.8), возникающих на выходе шага 2^{t-1} алгоритма 1, равно

$$\begin{aligned} & \sum_{\sum j \beta_j = k} \binom{2^{m-t}}{\beta_{2^{t-1}}} n_{t, 2^{t-1}}^{\beta_{2^{t-1}}} \binom{2^{m-t} - \beta_{2^{t-1}}}{\beta_{2^{t-1}} - 1} n_{t, 2^{t-1} - 1}^{\beta_{2^{t-1}} - 1} \dots \\ & \dots \binom{2^{m-t} - \beta_{2^{t-1}} - \dots - \beta_3}{\beta_2} n_{t, 2}^{\beta_2} \binom{2^{m-t} - \beta_{2^{t-1}} - \dots - \beta_2}{\beta_1} n_{t, 1}^{\beta_1} = \\ & = \sum_{\sum j \beta_j = k} \frac{(2^{m-t})_{(\beta_{2^{t-1}} + \dots + \beta_1)}}{\beta_{2^{t-1}}! \dots \beta_1!} n_{t, 2^{t-1}}^{\beta_{2^{t-1}}} n_{t, 2^{t-1} - 1}^{\beta_{2^{t-1}} - 1} \dots n_{t, 2}^{\beta_2} n_{t, 1}^{\beta_1}. \end{aligned}$$

Для числа

$$N(A_{2^m}[a_1, b_1, \dots, a_k, b_k]) = |\mathcal{F}(A_{2^m}[a_1, b_1, \dots, a_k, b_k])|$$

в работе [3] получена следующая формула:

$$N(A_{2^m}[i_1, j_1, \dots, i_k, j_k]) = \frac{(2^m - 2k)!}{2^{2^{m-1}-k} (2^{m-1} - k)!}.$$

Следовательно, число возможных вариантов инволюций, возникающих на выходе шага $2^{t-1} + 1$ алгоритма 1, равно

$$S_{k, 2^m}^{(2^{t-1}, \dots, 1)} = \sum_{\sum j \beta_j = k} \frac{(2^{m-t})_{(\beta_{2^{t-1}} + \dots + \beta_1)}}{\beta_{2^{t-1}}! \dots \beta_1!} n_{t, 2^{t-1}}^{\beta_{2^{t-1}}} \dots n_{t, 1}^{\beta_1} \frac{(2^m - 2k)!}{2^{2^{m-1}-k} (2^{m-1} - k)!}. \quad (1.9)$$

Далее, в [3] для числа

$$N(A_{2^m}) = |\mathcal{F}(A_{2^m})|$$

доказана следующая формула:

$$N(A_{2^m}) = \frac{2^m!}{2^{2^{m-1}} \cdot (2^{m-1})!}. \quad (1.10)$$

Для биномиального момента случайной величины $\xi_{2^m}^{(2^{t-1}, \dots, 1)}$ имеем формулу

$$B_k(\xi_{2^m}^{(2^{t-1}, \dots, 1)}) = \frac{S_{k, 2^m}^{(2^{t-1}, \dots, 1)}}{N(A_{2^m})} \quad (1.11)$$

(см. [4]). Из равенств (1.11), (1.9), (1.10) следует формула (1.3).

Теорема 1 доказана. $\square$

Следствие 1. Для любого $t \geq 1$ и любых линейно независимых над E_2 элементов $\nu_{t-1}, \dots, \nu_0 \in E_{2^m}$ при $m \rightarrow \infty$ распределение случайной величины $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$ сходится к распределению Пуассона $\Pi(\lambda)$ с параметром $\lambda = t/2$. В частности,

$$\mathbf{P}(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)} = 0) \rightarrow e^{-t/2}. \quad (1.12)$$

Для доказательства следствия достаточно показать, что для любого $k \geq 1$ при $m \rightarrow \infty$ имеет место предельное соотношение

$$B_k(\xi_{2^m}^{(2^{t-1}, \dots, 1)}) \rightarrow \frac{1}{k!} \left(\frac{t}{2}\right)^k. \quad (1.13)$$

Рассмотрим произвольное слагаемое суммы в правой части равенства (1.3), для которого $\beta_1 < k$. В этом случае соответствующая величина β равна $\beta_{2^{t-1}} + \dots + \beta_1 < k$. Для фиксированных t, k при $m \rightarrow \infty$ имеем оценку

$$\begin{aligned} & \frac{(2^{m-t})_{(\beta_{2^{t-1}} + \dots + \beta_1)}}{\beta_{2^{t-1}}! \dots \beta_1!} n_{t, 2^{t-1}}^{\beta_{2^{t-1}}} \dots n_{t, 1}^{\beta_1} \frac{2^k \cdot (2^{m-1})_k}{(2^m)_{2k}} = \\ & = O\left(\frac{2^{m\beta} \cdot 2^{mk}}{2^{2mk}}\right) = O\left(\frac{1}{2^m}\right). \end{aligned} \quad (1.14)$$

В случае $\beta_1 = k$ с учетом равенства $n_{t, 1} = 2^{t-1}t, t \geq 1$, единственное слагаемое

$$\frac{(2^{m-t})_k}{k!} 2^{k(t-1)} t^k \frac{2^k \cdot (2^{m-1})_k}{(2^m)_{2k}}$$

суммы (1.3) можно оценить при $m \rightarrow \infty$ величиной

$$\frac{1}{k!} \left(\frac{t}{2}\right)^k \left(1 + O\left(\frac{1}{2^m}\right)\right). \quad (1.15)$$

Так как число слагаемых в сумме (1.3) не зависит от m , то из асимптотических оценок (1.14), (1.15) следует предельное соотношение (1.13). $\square$

Частным случаем теоремы 1 является следующее утверждение.

Следствие 2. Для любых элементов $\nu, \mu \in E_{2^m} \setminus 0, \nu \neq \mu$, распределение случайной величины $\xi_{2^m}^{(\nu, \mu)}$ удовлетворяет равенству

$$\mathbf{P}(\xi_{2^m}^{(\nu, \mu)} = r) = \sum_{k=r}^{2^{m-1}} (-1)^{k-r} \binom{k}{r} B_k(\xi_{2^m}^{(\nu, \mu)}), \quad r=0, 1, \dots, 2^{m-1}. \quad (1.16)$$

При этом $B_0(\xi_{2^m}^{(\nu, \mu)}) = 1$, и для любого $k=1, \dots, 2^{m-1}$ выполнено равенство

$$B_k(\xi_{2^m}^{(\nu, \mu)}) = \left[\sum_{p=0}^{[k/2]} \frac{(2^{m-2})_{k-p}}{p! (k-2p)!} 2^{3(k-p)} \right] \frac{(2^{m-1})_k}{(2^m)_{2k}}. \quad (1.17)$$

2. Асимптотика моментов весового дефицита случайной инволюции

Найдем главный член асимптотики биномиальных моментов произвольного порядка.

Теорема 2. Для биномиального момента порядка $t \geq 1$ случайной величины ζ_{2^m} при $m \rightarrow \infty$ имеет место асимптотическое равенство

$$B_t(\zeta_{2^m}) = \frac{1}{t!} \left(\frac{2^m}{\sqrt{e}} \right)^t (1 + o(1)). \quad (2.1)$$

В [3] получена формула

$$B_t(\zeta_{2^m}) = \sum_{1 \leq \nu_{t-1} < \dots < \nu_0 \leq 2^m - 1} \frac{|\mathcal{F}(A_{2^m}; \nu_{t-1}, \dots, \nu_0)|}{N(A_{2^m})}. \quad (2.2)$$

Здесь $\mathcal{F}(A_{2^m}; \nu_{t-1}, \dots, \nu_0)$ — множество всех инволюций $J \in \mathcal{F}(A_{2^m})$, у которых веса всех двоичных циклов не равны $\nu_{t-1}, \dots, \nu_0$. Таким образом, для любых $1 \leq \nu_{t-1} < \dots < \nu_0 \leq 2^m - 1$

$$\frac{|\mathcal{F}(A_{2^m}; \nu_{t-1}, \dots, \nu_0)|}{N(A_{2^m})} = \mathbf{P}(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)} = 0).$$

Из равенства (2.2) следует формула

$$B_t(\zeta_{2^m}) = \sum_{1 \leq \nu_{t-1} < \dots < \nu_0 \leq 2^m - 1} \mathbf{P}(\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)} = 0). \quad (2.3)$$

В ходе доказательства теоремы 1 было показано, что для любой последовательности $(\nu_{t-1}, \dots, \nu_0) \in \mathcal{Z}_{2^m}^{(t)}$ распределения случайных величин $\xi_{2^m}^{(\nu_{t-1}, \dots, \nu_0)}$ и $\xi_{2^m}^{(2^{t-1}, \dots, 1)}$ совпадают. Из соотношений (1.1), (2.3) следует двустороннее неравенство

$$\begin{aligned} & \frac{1}{t!} (2^m - 1) \dots (2^m - 2^{t-1}) \mathbf{P}(\xi_{2^m}^{(2^{t-1}, \dots, 1)} = 0) \leq \\ & \leq B_t(\zeta_{2^m}) \leq \frac{1}{t!} (2^m - 1) \dots (2^m - 2^{t-1}) \mathbf{P}(\xi_{2^m}^{(2^{t-1}, \dots, 1)} = 0) + \\ & + \frac{1}{t!} ((2^m - 1)_t - (2^m - 1) \dots (2^m - 2^{t-1})). \end{aligned} \quad (2.4)$$

Равенство (2.1) является следствием соотношений (1.12) и (2.4).

Перейдем к оценке дисперсии случайной величины ζ_{2^m} . Частным случаем соотношения (2.3) является равенство

$$B_2(\zeta_{2^m}) = \sum_{1 \leq \nu < \mu \leq 2^m - 1} \mathbf{P}(\xi_{2^m}^{(\nu, \mu)} = 0).$$

В ходе доказательства теоремы 1 показано, что случайные величины $\xi_{2^m}^{(\nu, \mu)}$ одинаково распределены. Следовательно,

$$B_2(\zeta_{2^m}) = (2^m - 1)(2^{m-1} - 1) \mathbf{P}(\xi_{2^m}^{(2,1)} = 0). \quad (2.5)$$

Из соотношений (1.16) и (1.17) имеем формулу

$$\mathbf{P}(\xi_{2^m}^{(2,1)} = 0) = \sum_{k=0}^{2^{m-1}} (-1)^k \left[\sum_{p=0}^{\lfloor k/2 \rfloor} \frac{(2^{m-2})_{k-p}}{p! (k-2p)!} 2^{3(k-p)} \right] \frac{(2^{m-1})_k}{(2^m)_{2k}}. \quad (2.6)$$

Для асимптотической оценки величины $B_2(\zeta_{2^m})$ нам понадобится следующая лемма. В ходе ее доказательства будем предполагать, что $m \geq 4$.

Лемма 1. *Имеет место асимптотическое равенство при $m \rightarrow \infty$:*

$$\mathbf{P}(\xi_{2^m}^{(2,1)} = 0) = \frac{1}{e} \left(1 - \frac{1}{2^m} \frac{3}{2} + O\left(\frac{1}{2^{2m}}\right) \right). \quad (2.7)$$

Начнем доказательство леммы с изменения порядка суммирования в формуле (2.6). Индексы суммирования k, p удовлетворяют следующей системе ограничений:

$$(0 \leq k \leq 2^{m-1}) \wedge (0 \leq p \leq 2^{m-2}) \wedge (0 \leq k-2p \leq 2^{m-2}-p).$$

Данная система равносильна системе

$$(0 \leq p \leq 2^{m-2}) \wedge (2p \leq k \leq 2^{m-2} + p).$$

Следовательно,

$$\mathbf{P}(\xi_{2^m}^{(2,1)} = 0) = \sum_{p=0}^{2^{m-2}} \frac{1}{p!} \left[\sum_{k=2p}^{2^{m-2}+p} (-1)^k \frac{(2^{m-2})_{k-p}}{(k-2p)!} 2^{3(k-p)} \frac{(2^{m-1})_k}{(2^m)_{2k}} \right]. \quad (2.8)$$

Во внутренней сумме из правой части равенства (2.8) сделаем замену индекса суммирования $s = k - p$:

$$\mathbf{P}(\xi_{2^m}^{(2,1)} = 0) = \sum_{p=0}^{2^{m-2}} \frac{(-1)^p}{p!} \left[\sum_{s=p}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{(s-p)!} \frac{(2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}} \right]. \quad (2.9)$$

Для удобства введем обозначение для сумм

$$\Sigma_{2^m, p} = \sum_{s=p}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{(s-p)!} \frac{(2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}}, \quad 0 \leq p \leq 2^{m-2}.$$

Оценка суммы $\Sigma_{2^m, 0}$.

Имеем выражение

$$\Sigma_{2^m, 0} = 1 + \sum_{s=1}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{s!} \frac{(2^{m-2})_s (2^{m-1})_s}{(2^m)_{2s}}. \quad (2.10)$$

Рассмотрим следующие рациональные функции вещественного переменного:

$$g_s(x) = \frac{\prod_{j=0}^{s-1} (1-4jx) \prod_{j=1}^{s-1} (1-2jx)}{\prod_{l=1}^{2s-1} (1-lx)}, \quad s \geq 1.$$

Из (2.10) следует равенство

$$\Sigma_{2^m, 0} = 1 + \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} g_s \left(\frac{1}{2^m} \right). \quad (2.11)$$

Сократив произведение $\prod_{j=1}^{s-1} (1-2jx)$ в числителе и знаменателе, получим выражение

$$g_s(x) = \prod_{j=0}^{s-1} \frac{1-4jx}{1-(2j+1)x}, \quad s \geq 1. \quad (2.12)$$

Выразим значения $g_s(2^{-m})$ с помощью разложения Тейлора $g_s(x)$ в точке $x_0 = 0$ с остаточным членом второго порядка в форме Лагранжа:

$$g_s \left(\frac{1}{2^m} \right) = g_s(0) + g'_s(0) \frac{1}{2^m} + \frac{g''_s(x_{m,s})}{2} \frac{1}{2^{2m}}, \quad 1 \leq s \leq 2^{m-2}, \quad (2.13)$$

где

$$0 < x_{m,s} < \frac{1}{2^m}.$$

Подставив выражения (2.13) в (2.11), получим равенство

$$\begin{aligned} \Sigma_{2^m,0} = 1 + \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} g_s(0) + \frac{1}{2^m} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} g'_s(0) + \\ + \frac{1}{2^{2m}} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} \frac{g''_s(x_{m,s})}{2}. \end{aligned} \quad (2.14)$$

Так как $g_s(0) = 1$ при любом $s \geq 1$, то

$$1 + \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} g_s(0) = \frac{1}{e} \left(1 + O\left(\frac{1}{(2^{m-2})!}\right) \right). \quad (2.15)$$

Имеем равенства для производных функций (2.12)

$$g'_s(x) = g_s(x) \left(\sum_{j=0}^{s-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=1}^{s-1} \frac{4j}{1-4jx} \right), \quad s \geq 1. \quad (2.16)$$

Для значений производных в нуле получим

$$g'_s(0) = \sum_{j=0}^{s-1} (2j+1) - \sum_{j=1}^{s-1} 4j = s^2 - 2s(s-1) = s - (s^2 - s).$$

Следовательно,

$$\begin{aligned} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{s!} g'_s(0) = - \sum_{s=1}^{2^{m-2}} \frac{(-1)^{s-1}}{(s-1)!} - \sum_{s=2}^{2^{m-2}} \frac{(-1)^{s-2}}{(s-2)!} = \\ = - \frac{2}{e} \left(1 + O\left(\frac{1}{(2^{m-2}-2)!}\right) \right). \end{aligned} \quad (2.17)$$

Оценим коэффициент при 2^{-2m} в последнем слагаемом из правой части равенства (2.14). Для вторых производных функций (2.12), согласно (2.16), имеем равенства

$$\begin{aligned} g''_s(x) = g_s(x) \left(\left(\sum_{j=0}^{s-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=1}^{s-1} \frac{4j}{1-4jx} \right)^2 + \right. \\ \left. + \sum_{j=0}^{s-1} \left(\frac{2j+1}{1-(2j+1)x} \right)^2 - \sum_{j=1}^{s-1} \left(\frac{4j}{1-4jx} \right)^2 \right), \quad s \geq 1. \end{aligned} \quad (2.18)$$

При $m \geq 4$ для любых $x \in (0, \frac{1}{2^m})$ и $1 \leq j \leq 2^{m-2}$ выполнены неравенства

$$0 < \frac{1}{1-x} < 2, \quad (2.19)$$

$$\frac{1}{1-x} < \frac{4}{1-4x}. \quad (2.20)$$

$$0 < \frac{1-4jx}{1-(2j+1)x} < 1, \quad (2.21)$$

$$\frac{2j+1}{1-(2j+1)x} < \frac{4j}{1-4jx}. \quad (2.22)$$

Из соотношений (2.12), (2.19), (2.21) при $x = x_{m,s}$ получим оценку

$$0 < g_s(x_{m,s}) < 2, \quad 1 \leq s \leq 2^{m-2}. \quad (2.23)$$

Сумма квадратов положительных чисел не превосходит квадрата их суммы. Используя этот факт, соотношения (2.18), (2.20), (2.22) при $x = x_{m,s}$, а также неравенство (2.23), приведем следующие оценки, справедливые для любого $1 \leq s \leq 2^{m-2}$:

$$\begin{aligned} |g_s''(x_{m,s})| &\leq 2 \left(\left(\frac{1}{1-x_{m,s}} + \sum_{j=1}^{s-1} \frac{4j}{1-4jx_{m,s}} \right)^2 + \right. \\ &\quad \left. + \frac{1}{(1-x_{m,s})^2} + \sum_{j=1}^{s-1} \left(\frac{4j}{1-4jx_{m,s}} \right)^2 \right) \leq \\ &\leq 2 \left(2 \left(2 \sum_{j=1}^{s-1} \frac{4j}{1-4jx_{m,s}} \right)^2 \right). \end{aligned}$$

Таким образом,

$$|g_s''(x_{m,s})| \leq 256 \left(\sum_{j=1}^{s-1} \frac{j}{1-4jx_{m,s}} \right)^2, \quad 1 \leq s \leq 2^{m-2}. \quad (2.24)$$

Если $1 \leq s \leq 2^{m-3}$, то для любого $1 \leq j \leq s-1$ выполнено неравенство

$$\frac{j}{1-4jx_{m,s}} \leq \frac{j}{1-4j/2^m} \leq 2j. \quad (2.25)$$

Следовательно,

$$\sum_{j=1}^{s-1} \frac{j}{1-4jx_{m,s}} \leq 2 \sum_{j=1}^{s-1} j < s^2. \quad (2.26)$$

Поэтому из соотношений (2.24), (2.26) имеем оценку

$$|g_s''(x_{m,s})| \leq 256 s^4, \quad 1 \leq s \leq 2^{m-3}. \quad (2.27)$$

Используя неравенства (2.27), получим оценку

$$\left| \sum_{s=1}^{2^{m-3}} \frac{(-1)^s}{s!} \frac{g_s''(x_{m,s})}{2} \right| \leq 128 \sum_{s=1}^{\infty} \frac{s^4}{s!}.$$

Таким образом, при $m \rightarrow \infty$

$$\sum_{s=1}^{2^{m-3}} \frac{(-1)^s}{s!} \frac{g_s''(x_{m,s})}{2} = O(1). \quad (2.28)$$

Для значений $2^{m-3} + 1 \leq s \leq 2^{m-2}$ воспользуемся очевидным неравенством

$$\sum_{j=1}^{s-1} \frac{4j}{1-4j x_{m,s}} \leq \sum_{j=1}^{s-1} \frac{4j}{1-4j/2^m} \leq 2^{3m}. \quad (2.29)$$

Из этого неравенства, с учетом (2.24), получим оценки

$$\left| \sum_{s=2^{m-3}+1}^{2^{m-2}} \frac{(-1)^s}{s!} \frac{g_s''(x_{m,s})}{2} \right| \leq 128 \cdot 2^{6m} \sum_{s=2^{m-3}+1}^{\infty} \frac{1}{s!} \leq 128 \frac{2^{6m}}{(2^{m-3})!}.$$

Таким образом, при $m \rightarrow \infty$

$$\sum_{s=2^{m-3}+1}^{2^{m-2}} \frac{(-1)^s}{s!} \frac{g_s''(x_{m,s})}{2} = o(1). \quad (2.30)$$

Подставив оценки (2.15), (2.17), (2.28), (2.30) в выражение (2.14), получим искомую асимптотическую формулу:

$$\Sigma_{2^m,0} = \frac{1}{e} \left(1 - \frac{1}{2^m} 2 + O\left(\frac{1}{2^{2m}}\right) \right), \quad m \rightarrow \infty. \quad (2.31)$$

Оценка суммы $\Sigma_{2^m,1}$.

Имеем выражение

$$\Sigma_{2^m,1} = \sum_{s=1}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{(s-1)!} \frac{(2^{m-2})_s (2^{m-1})_{s+1}}{(2^m)_{2s+2}}. \quad (2.32)$$

Рассмотрим следующие рациональные функции вещественного переменного:

$$\varphi_s(x) = \frac{\prod_{j=0}^{s-1} (1-4jx) \prod_{j=1}^s (1-2jx)}{\prod_{l=1}^{2s+1} (1-lx)}, \quad s \geq 1.$$

Из (2.32) следует равенство

$$\Sigma_{2^m,1} = \frac{1}{2^m} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{2(s-1)!} \varphi_s\left(\frac{1}{2^m}\right). \quad (2.33)$$

Сократив произведение $\prod_{j=1}^s (1-2jx)$ в числителе и знаменателе, получим выражение

$$\varphi_s(x) = \frac{\prod_{j=0}^{s-1} (1-4jx)}{\prod_{j=0}^s (1-(2j+1)x)}, \quad s \geq 1. \quad (2.34)$$

По теореме Лагранжа

$$\varphi_s\left(\frac{1}{2^m}\right) = \varphi_s(0) + \varphi'_s(y_{m,s}) \frac{1}{2^m}, \quad 1 \leq s \leq 2^{m-2}, \quad (2.35)$$

где

$$0 < y_{m,s} < \frac{1}{2^m}.$$

Подставив выражения (2.35) в (2.33), получим равенство

$$\Sigma_{2^m,1} = \frac{1}{2^m} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{2(s-1)!} \varphi_s(0) + \frac{1}{2^{2m}} \sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{2(s-1)!} \varphi'_s(y_{m,s}). \quad (2.36)$$

Так как $\varphi_s(0) = 1$ при любом $s \geq 1$, то

$$\sum_{s=1}^{2^{m-2}} \frac{(-1)^s}{2(s-1)!} \varphi_s(0) = -\frac{1}{2e} \left(1 + O\left(\frac{1}{(2^{m-2}-1)!}\right)\right). \quad (2.37)$$

Рассуждая аналогично доказательству равенств (2.28), (2.30), можно показать, что

$$\sum_{s=3}^{2^{m-2}} \frac{(-1)^s}{2(s-1)!} \varphi'_s(y_{m,s}) = O(1), \quad m \rightarrow \infty. \quad (2.38)$$

Из соотношений (2.36), (2.37), (2.38) следует асимптотическая формула

$$\Sigma_{2^m,1} = \frac{1}{2^m} \left(-\frac{1}{2e} + O\left(\frac{1}{2^m}\right) \right), \quad m \rightarrow \infty. \quad (2.39)$$

Оценка суммы $\sum_{p=2}^{2^{m-2}} \left(\frac{(-1)^p}{p!} \Sigma_{2^m,p} \right).$

Покажем, что при любых $2 \leq p \leq s \leq 2^{m-2}$ выполнено неравенство

$$\frac{2^{3s} (2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}} \leq \frac{2^m}{2^p (2^m-1)(2^m-5)(2^m-9)}. \quad (2.40)$$

В случае когда $s = p = 2$ либо $s = 3, p = 2$, неравенство (2.40) можно проверить непосредственно.

В случае $s \geq 4, p = 2$

$$\begin{aligned} \frac{2^{3s} (2^{m-2})_s (2^{m-1})_{s+2}}{(2^m)_{2s+4}} &= \frac{2^{3s}}{2^{3s+2}} \frac{2^m}{(2^m-1)(2^m-5)(2^m-9)} \times \\ &\times \frac{2^m-4}{2^m-3} \frac{2^m-8}{2^m-7} \frac{2^m-12}{2^m-11} \cdots \frac{2^m-4(s-1)}{2^m-(2s+3)}. \end{aligned} \quad (2.41)$$

При $4 \leq j \leq s$ выполнено неравенство

$$\frac{2^m-4(j-1)}{2^m-(2j+3)} < 1. \quad (2.42)$$

Из соотношений (2.41), (2.42) получим (2.40) в рассматриваемом случае.

В случае $2^{m-2} \geq s \geq p \geq 3$

$$\begin{aligned} \frac{2^{3s} (2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}} &= \frac{2^{3s}}{2^{3s+p}} \frac{2^m}{(2^m-1)(2^m-5)(2^m-9)} \times \\ &\times \frac{2^m-4}{2^m-3} \frac{2^m-8}{2^m-7} \frac{2^m-12}{2^m-11} \cdots \frac{2^m-4(s-1)}{2^m-(2s+3)} \times \\ &\times \frac{1}{(2^m-2(s+3)+1) \cdots (2^m-2(s+p)+1)}. \end{aligned} \quad (2.43)$$

Из соотношений (2.42), (2.43) опять получим (2.40).

Из неравенства (2.40) следует оценка

$$\begin{aligned} & \left| \sum_{p=2}^{2^{m-2}} \frac{(-1)^p}{p!} \sum_{s=p}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{(s-p)!} \frac{(2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}} \right| \leq \\ & \leq \sum_{p=0}^{\infty} \frac{1}{2^p p!} \sum_{s=p}^{\infty} \frac{1}{(s-p)!} \frac{2^m}{(2^m-1)(2^m-5)(2^m-9)} = \\ & = e^{3/2} \frac{2^m}{(2^m-1)(2^m-5)(2^m-9)}. \end{aligned}$$

Таким образом, при $m \rightarrow \infty$

$$\sum_{p=2}^{2^{m-2}} \frac{(-1)^p}{p!} \sum_{s=p}^{2^{m-2}} \frac{(-1)^s 2^{3s}}{(s-p)!} \frac{(2^{m-2})_s (2^{m-1})_{s+p}}{(2^m)_{2s+2p}} = O\left(\frac{1}{2^{2m}}\right). \quad (2.44)$$

Из равенства (2.9) и оценок (2.31), (2.39), (2.44) следует доказываемое соотношение (2.7).

Лемма 1 полностью доказана. $\square$

В качестве следствия леммы 1 из соотношений (2.5), (2.7) получим асимптотическое представление

$$\begin{aligned} B_2(\zeta_{2^m}) &= \frac{1}{2} (2^m-1) (2^m-2) \frac{1}{e} \left(1 - \frac{1}{2^m} \frac{3}{2} + O\left(\frac{1}{2^{2m}}\right) \right) = \\ &= \frac{1}{2e} \left(2^{2m} + 2^m \left(-\frac{9}{2} \right) + O(1) \right), \quad m \rightarrow \infty. \end{aligned} \quad (2.45)$$

Для математического ожидания случайной величины ζ_{2^m} в [3] получена формула

$$\mathbf{E} \zeta_{2^m} = (2^m-1) \left(\sum_{k=0}^{2^{m-1}} (-1)^k \frac{2^k}{k!} \frac{(2^{m-1})_k^2}{(2^m)_{2k}} \right). \quad (2.46)$$

Лемма 2. *Имеет место асимптотическое равенство*

$$\mathbf{E} \zeta_{2^m} = (2^m - 1) \frac{1}{\sqrt{e}} \left(1 - \frac{1}{2^m} \frac{1}{2} + O\left(\frac{1}{2^{2m}}\right) \right) \quad \text{при } m \rightarrow \infty. \quad (2.47)$$

Доказательство оценки (2.47) во многом аналогично доказательству формулы (2.31).

Рассмотрим следующие рациональные функции вещественного переменного

$$f_k(x) = \frac{\prod_{j=0}^{k-1} (1 - 2^j x)^2}{\prod_{l=1}^{2^k-1} (1 - l x)}, \quad k \geq 1.$$

Из (2.46) следует равенство

$$\mathbf{E} \zeta_{2^m} = (2^m - 1) \left(1 + \sum_{k=1}^{2^{m-1}} (-1)^k \frac{1}{2^k k!} f_k\left(\frac{1}{2^m}\right) \right). \quad (2.48)$$

Сократив произведение $\prod_{j=1}^s (1 - 2^j x)$ в числителе и знаменателе, получим выражение

$$f_k(x) = \prod_{j=0}^{k-1} \frac{1 - 2^j x}{1 - (2^{j+1} - 1)x}. \quad (2.49)$$

Выразим значения $f_k(2^{-m})$ с помощью разложения Тейлора функции $f_k(x)$ в точке $x_0 = 0$ с остаточным членом второго порядка в форме Лагранжа:

$$f_k\left(\frac{1}{2^m}\right) = f_k(0) + f'_k(0) \frac{1}{2^m} + \frac{f''_k(z_{m,k})}{2} \frac{1}{2^{2m}}, \quad 1 \leq k \leq 2^{m-1}, \quad (2.50)$$

где

$$0 < z_{m,k} < \frac{1}{2^m}.$$

Подставив выражения (2.50) в (2.48), получим равенство

$$\begin{aligned} \mathbf{E} \zeta_{2^m} = (2^m - 1) & \left(1 + \sum_{k=1}^{2^{m-1}} \frac{(-1)^k}{2^k k!} f_k(0) + \frac{1}{2^m} \sum_{k=1}^{2^{m-1}} \frac{(-1)^k}{2^k k!} f'_k(0) + \right. \\ & \left. + \frac{1}{2^{2m}} \sum_{k=1}^{2^{m-1}} \frac{(-1)^k}{2^{k+1} k!} f''_k(z_{m,k}) \right). \end{aligned} \quad (2.51)$$

Так как $f_k(0) = 1$ при любом $k \geq 1$, то

$$1 + \sum_{k=1}^{2^{m-1}} \frac{(-1)^k}{2^k k!} f_k(0) = \frac{1}{\sqrt{e}} \left(1 + O\left(\frac{1}{(2^{m-1})!}\right) \right). \quad (2.52)$$

Имеем равенства для производных функций (2.49)

$$f'_k(x) = f_k(x) \left(\sum_{j=0}^{k-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=0}^{k-1} \frac{2j}{1-2jx} \right), \quad k \geq 1. \quad (2.53)$$

Для значений производных в нуле получим

$$f'_k(0) = \sum_{j=0}^{k-1} (2j+1) - \sum_{j=0}^{k-1} 2j = k.$$

Следовательно,

$$\sum_{k=1}^{2^{m-1}} \frac{(-1)^k}{2^k k!} f'_k(0) = -\frac{1}{2} \sum_{k=1}^{2^{m-1}} \frac{(-1)^{k-1}}{2^{k-1} (k-1)!} = -\frac{1}{2\sqrt{e}} \left(1 + O\left(\frac{1}{(2^{m-1})!}\right) \right). \quad (2.54)$$

Оценим коэффициент в последнем слагаемом в скобке из правой части равенства (2.51). Для вторых производных функций (2.49), согласно (2.53), имеем равенства

$$\begin{aligned} f''_k(x) = f_k(x) & \left(\left(\sum_{j=0}^{k-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=0}^{k-1} \frac{2j}{1-2jx} \right)^2 + \right. \\ & \left. + \sum_{j=0}^{k-1} \left(\frac{2j+1}{1-(2j+1)x} \right)^2 - \sum_{j=0}^{k-1} \left(\frac{2j}{1-2jx} \right)^2 \right), \quad k \geq 1. \end{aligned} \quad (2.55)$$

Найдем точку максимума функции $f''_k(x)$ на отрезке $[0, 2^{-m}]$ для $1 \leq k \leq 2^{m-1}$.

Для третьих производных функций (2.49), согласно (2.55), имеем равенства

$$\begin{aligned} f_k'''(x) = f_k(x) & \left[\left(\sum_{j=0}^{k-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=0}^{k-1} \frac{2j}{1-2jx} \right)^3 + \right. \\ & + 3 \left(\sum_{j=0}^{k-1} \frac{2j+1}{1-(2j+1)x} - \sum_{j=0}^{k-1} \frac{2j}{1-2jx} \right) \times \\ & \times \left(\sum_{j=0}^{k-1} \left(\frac{2j+1}{1-(2j+1)x} \right)^2 - \sum_{j=0}^{k-1} \left(\frac{2j}{1-2jx} \right)^2 \right) + \\ & \left. + 2 \left(\sum_{j=0}^{k-1} \left(\frac{2j+1}{1-(2j+1)x} \right)^3 - \sum_{j=0}^{k-1} \left(\frac{2j}{1-2jx} \right)^3 \right) \right]. \end{aligned}$$

Для любых $0 \leq j < k \leq 2^{m-1}$ и $x \in [0, 1/2^m]$

$$\frac{2j+1}{1-(2j+1)x} - \frac{2j}{1-2jx} = \frac{1}{(1-(2j+1)x)(1-2jx)} > 0.$$

Следовательно, $f_k'''(x) > 0$; таким образом,

$$f_k''(z_{m,k}) \leq f_k''\left(\frac{1}{2^m}\right), \quad 1 \leq k \leq 2^{m-1}. \quad (2.56)$$

Используя неравенство (2.56) и рассуждая аналогично доказательству равенств (2.28), (2.30), можно доказать следующее асимптотическое равенство: при $m \rightarrow \infty$

$$\sum_{k=1}^{2^{m-1}} (-1)^k \frac{1}{2^{k+1}k!} f_k''(z_{m,k}) = O(1). \quad (2.57)$$

Подставив оценки (2.53), (2.54), (2.57) в формулу (2.51), получим соотношение (2.47).

Лемма 2 доказана полностью. $\square$

Из соотношения (2.47) следует равенство

$$(\mathbf{E}\zeta_{2^m})^2 = \frac{1}{e} (2^{2m} + 2^m \cdot (-3) + O(1)). \quad (2.58)$$

Подставляя в равенство для дисперсии

$$\mathbf{D}\zeta_{2^m} = 2B_2(\zeta_{2^m}) + \mathbf{E}\zeta_{2^m} - \mathbf{E}(\zeta_{2^m})^2$$

выражения (2.45), (2.47), (2.58), после несложных преобразований получим следующую теорему.

Теорема 3. Для дисперсии случайной величины ζ_{2^m} — весового дефицита случайной равновероятной инволюции $J \in \mathcal{F}(A_{2^m})$ — имеет место асимптотическое равенство

$$D\zeta_{2^m} = 2^m \frac{2\sqrt{e} - 3}{2e} + O(1), \quad m \rightarrow \infty.$$

Список литературы

- [1] Сачков В. Н., “Комбинаторные свойства дифференциально 2-равномерных подстановок”, *Математические вопросы криптографии*, **6**:1 (2015), 159–179.
- [2] Сачков В. Н., Круглов И. А., “Весовые дефициты инволюций и подстановок”, *Математические вопросы криптографии*, **7**:4 (2016), 95–116.
- [3] Сачков В. Н., “Инволюции с данным весовым дефицитом, соответствующие таблице Кэли конечной абелевой группы”, *Математические вопросы криптографии*, **8**:4 (2017), 117–134.
- [4] Сачков В. Н., *Курс комбинаторного анализа*, М.-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.