Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, И. А. Круглов, Дисперсия аддитивного весового дефицита равновероятной инволюции на группе вычетов, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 3, 101–116

DOI: <https://doi.org/10.4213/mvk303>

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: 3.95.254.165

26 апреля 2023 г., 12:18:41

Дисперсия аддитивного весового дефицита равновероятной инволюции на группе вычетов

В. Н. Сачков, И. А. Круглов

Академия криптографии Российской Федерации, Москва

Получено 29.IV.2019

Аннотация. В работе получены точные и асимптотические формулы для дисперсии случайной величины ζ_n , равной весовому дефициту случайной инволюции, заданной на аддитивной группе кольца вычетов по натуральному модулю n . Асимптотическая формула при $n \rightarrow \infty$ имеет следующий вид:

$$D\zeta_n = n \left(e^{-\frac{1}{2}} - \frac{3}{2}e^{-1} \right) \left(1 + O \left(\frac{1}{n^{\frac{1}{3}}} \right) \right).$$

Ключевые слова: случайная инволюция, аддитивный вес двоичного цикла, весовой дефицит

Variance of the additive weight deficit of equiprobable involution on the residue group

V. N. Sachkov, I. A. Kruglov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. We find exact and asymptotic formulas for the variance of the random variable ζ_n which is equal to the weight deficit of random involution defined on the additive group of residues modulo natural number n . The asymptotic formula for $n \rightarrow \infty$ has the following form:

$$D\zeta_n = n \left(e^{-\frac{1}{2}} - \frac{3}{2}e^{-1} \right) \left(1 + O \left(\frac{1}{n^{\frac{1}{3}}} \right) \right).$$

Keywords: random involution, additive weight of the two-element cycle, weight deficit

1. Введение

В данной работе продолжены исследования, начатые в [1–4]. Напомним основные понятия. Пусть $(C_n, +)$ — аддитивная группа кольца вычетов по натуральному модулю $n \geq 3$, $C_n = \{0, 1, \dots, n-1\}$. Через $S(C_n)$ обозначим симметрическую группу подстановок множества C_n . Произвольная неединичная подстановка $I \in S(C_n)$ называется инволюцией, если $I^2 = e$ — единичная подстановка. Если (a, b) — двоичный цикл из разложения инволюции I в произведение независимых циклов (двоичных и единичных), то его *аддитивный вес* равен $a + b \pmod n$. Определим специальные *равновесные инволюции*. Пусть $\mu \in C_n$. Обозначим через L_μ инволюцию, равную произведению всех циклов (a, b) , $0 \leq a < b \leq n-1$, аддитивный вес которых равен μ . Указанные циклы являются независимыми. В зависимости от четности n и μ возможны следующие случаи.

(1) Если n — нечетное, то для любого μ инволюция L_μ есть произведение $\frac{n-1}{2}$ независимых двоичных циклов и одного единичного цикла (x) (x — решение уравнения $2x \equiv \mu \pmod n$).

(2) Если n — четное, то либо инволюция L_μ есть произведение $\frac{n}{2}$ независимых двоичных циклов (при нечетном μ), либо (при четном μ) — произведение $\frac{n}{2} - 1$ независимых двоичных циклов и двух единичных циклов (соответствующих решениям уравнения $2x \equiv \mu \pmod n$).

Инволюции $L_0, L_1, \dots, L_{n-1}$ будем называть *равновесными*. Множество таких инволюций можно считать одной из форм представления таблицы Кэли группы $(C_n, +)$ (см. подробнее [3]).

Любое произведение некоторых независимых двоичных циклов будем называть *частичной инволюцией* (действующей на соответствующем подмножестве группы C_n). Для независимых двоичных циклов будем также использовать термин *неколлинеарные*.

Через J будем обозначать инволюцию, действующую на множестве C_n , которая содержит максимально возможное число $\lfloor \frac{n}{2} \rfloor$ независимых двоичных циклов. Инволюцию J будем называть *максимальной инволюцией*. Обозначим через $\nu(J)$ число различных аддитивных весов независимых двоичных циклов из разложения инволюции J . *Весовым дефицитом* (или *аддитивным весовым дефицитом*) максимальной инволюции J называется число $d(J) = n - \nu(J)$.

Пусть J выбирается случайно и равновероятно из множества всех максимальных инволюций симметрической группы $S(C_n)$. Через ζ_n обозначим случайную величину, равную аддитивному весовому дефициту J .

В [3] получены точные формулы для распределения случайной величины ζ_n на основе свойств равновесных инволюций $L_0, L_1, \dots, L_{n-1}$. Кроме того, найдены следующие точные формулы для ее математического ожидания $M\zeta_n$.

Для нечетных $n \geq 3$:

$$M\zeta_n = n \sum_{k=0}^{\frac{n-1}{2}} (-1)^k \frac{2^k \left(\left(\frac{n-1}{2}\right)_k\right)^2}{k!(n)_{2k}}. \quad (0.1)$$

Для четных $n \geq 4$ (случай $\omega = 0$ в обозначениях работы [3]):

$$M\zeta_n = \frac{n}{2} \left[\sum_{k=0}^{\frac{n}{2}} (-1)^k \frac{2^k \left(\left(\frac{n}{2}\right)_k\right)^2}{k!(n)_{2k}} + \sum_{k=0}^{\frac{n}{2}-1} (-1)^k \frac{2^k \left(\frac{n}{2}\right)_k \left(\frac{n}{2} - 1\right)_k}{k!(n)_{2k}} \right]. \quad (0.2)$$

Из точных формул (0.1) и (0.2) в [3] выведена асимптотическая формула для математического ожидания $M\zeta_n$ при $n \rightarrow \infty$:

$$M\zeta_n = ne^{-\frac{1}{2}} (1 + o(1)). \quad (0.3)$$

При выводе асимптотической формулы для дисперсии $D\zeta_n$ случайной величины ζ_n воспользуемся известной формулой [5]

$$D\zeta_n = 2B_2\zeta_n + M\zeta_n - (M\zeta_n)^2, \quad (0.4)$$

в которой $B_2\zeta_n$ — второй биномиальный момент случайной величины ζ_n . Для ее применения будет уточнено асимптотическое представление (0.3) математического ожидания $M\zeta_n$.

2. Распределение числа двоичных циклов из заданной пары равновесных инволюций

Для нахождения второго биномиального момента случайной величины ζ_n введем набор вспомогательных случайных величин.

Обозначим через $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, случайную величину, равную суммарному числу двоичных циклов случайной максимальной инволюции J , входящих в разложения равновесных инволюций L_μ и L_ν . Ее распределение может быть представлено с помощью биномиальных моментов [5].

Теорема 1. Вероятностное распределение случайной величины $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, имеет вид

$$\mathbf{P}(\xi_n(L_\mu, L_\nu) = r) = \sum_{k=r}^{\lfloor \frac{n}{2} \rfloor} (-1)^{k-r} \binom{k}{r} \mathbf{B}_{kn}(\mu, \nu), r = 0, 1, \dots, \quad (1.1)$$

где $\mathbf{B}_{kn}(\mu, \nu)$ – k -й биномиальный момент $\xi_n(L_\mu, L_\nu)$.

Биномиальные моменты $\mathbf{B}_{kn}(\mu, \nu)$ в общем случае зависят от четности весов μ и ν двоичных циклов, входящих в разложения равновесных инволюций L_μ и L_ν .

Если для двоичных циклов L_μ вес μ – нечетный, то обозначим ее L_μ^1 , а если четный, то L_μ^0 . Далее нам потребуется выражение для числа неупорядоченных пар $\{L_\mu, L_\nu\}$ с заданной четностью весов элементов.

Лемма 1. При любом $n \geq 3$ все $\binom{n}{2}$ неупорядоченных пар $\{L_\mu, L_\nu\}$, $\mu \neq \nu$, разбиваются на три класса, числа элементов в которых определяются следующими равенствами:

а) при нечетном n

$$|\{L_\mu^0, L_\nu^0\}| = \frac{(n+1)(n-1)}{8},$$

$$|\{L_\mu^1, L_\nu^1\}| = \frac{(n-1)(n-3)}{8},$$

$$|\{L_\mu^1, L_\nu^0\}| = \frac{(n-1)(n+1)}{4},$$

б) при четном n

$$|\{L_\mu^1, L_\nu^1\}| = \frac{n(n-2)}{8},$$

$$|\{L_\mu^0, L_\nu^0\}| = \frac{n(n-2)}{8},$$

$$|\{L_\mu^1, L_\nu^0\}| = \frac{n^2}{4}.$$

Справедливость леммы непосредственно вытекает из рассмотрения вида цикловой структуры равновесных инволюций.

Для определения биномиальных моментов $\mathbf{B}_{kn}(\mu, \nu)$ случайной величины $\xi_n(L_\mu, L_\nu)$ зададим вероятностную схему построения частичных инволюций с k двоичными циклами для случайной инволюции J .

Для каждой частичной инволюции с k двоичными циклами можно рассмотреть последовательность T_k длины k , в которой (при некотором $0 \leq i \leq k$) первые i членов — независимые двоичные циклы из разложения L_μ , а следующие $k-i$ членов — независимые двоичные циклы из разложения L_ν . Так как порядок записи двоичных циклов в инволюции несуществен, то число способов выбрать последовательность T_k , соответствующую заданной частичной инволюции с i двоичными циклами из L_μ и $k-i$ двоичными циклами из L_ν , равно произведению $i!(k-i)!$.

Пусть $\mathfrak{A}(L_\mu)$ и $\mathfrak{A}(L_\nu)$ — упорядоченные множества двоичных циклов L_μ и L_ν соответственно. Для каждого из этих множеств определим схемы случайного выбора (без возвращения) двоичных циклов, которые обозначим как схема A и схема B . Для этих схем рассмотрим случайные события A_u^t и B_v^d , $t \in \{1, 2, \dots, i\}$, $d \in \{i+1, \dots, k\}$. Наступление события A_u^t означает, что t -й член последовательности T_k совпадает с двоичным циклом из $\mathfrak{A}(L_\mu)$, имеющим номер u , а наступление события B_v^d — что d -й член T_k совпадает с двоичным циклом из $\mathfrak{A}(L_\nu)$, имеющим номер v .

События $A_{u_1}^1, \dots, A_{u_i}^i, B_{v_1}^{i+1}, \dots, B_{v_{k-i}}^k$ являются совместными, если соответствующие им двоичные циклы обладают свойством попарной независимости (отсутствия общих элементов). Вероятность пересечения несовместных событий равна нулю. С использованием рассмотренной выше вероятностной схемы получаем следующую лемму.

Лемма 2. Для биномиальных моментов случайной величины $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, справедливы следующие представления:

$$\begin{aligned} \mathbf{B}_{kn}(\mu, \nu) &= \frac{1}{k!} \sum_{i=0}^k \binom{k}{i} \times \\ &\times \sum_{(u_1, u_2, \dots, u_i)} \sum_{(v_1, v_2, \dots, v_{k-i})} \mathbf{P} \left(A_{u_1}^1 \cap \dots \cap A_{u_i}^i \cap B_{v_1}^{i+1} \cap \dots \cap B_{v_{k-i}}^k \right), \end{aligned} \quad (1.2)$$

где $(u_1, u_2, \dots, u_i)$ и $(v_1, v_2, \dots, v_{k-i})$ — упорядоченные выборки без возвращения номеров двоичных циклов из множеств $\mathfrak{A}(L_\mu)$ и $\mathfrak{A}(L_\nu)$ соответственно.

Из леммы 2 следует, что вычисление биномиальных моментов $\mathbf{B}_{kn}(\mu, \nu)$ с использованием формулы (1.2) на основе вероятностных схем A и B для выбора двоичных циклов из $\mathfrak{A}(L_\mu)$ и $\mathfrak{A}(L_\nu)$ требует до применения схемы B предварительного определения запретных

двоичных циклов, нарушающих попарную независимость при образовании совместной выборки объема k в качестве частичной инволюции для максимальной инволюции J .

Построение частичных инволюций, соответствующих последовательности T_k , состоит из трех этапов.

На первом этапе с использованием вероятностной схемы A строится частичная инволюция из i , $1 \leq i \leq k$, двоичных циклов, которую можно записать в следующем виде:

$$(a_1, \mu - a_1)(a_2, \mu - a_2) \dots (a_i, \mu - a_i), \quad (1.3)$$

где $a_j < \mu - a_j$, $1 \leq j \leq i$. Частичная инволюция (1.3) определяется вектором $(a_1, a_2, \dots, a_i)$. Если N_μ — число двоичных циклов в множестве $\mathfrak{A}(L_\mu)$, то имеем $(N_\mu)_i$ частичных инволюций с двоичными циклами из множества $\mathfrak{A}(L_\mu)$.

На втором этапе на основе множества

$$\{a_1, a_2, \dots, a_i, \mu - a_1, \mu - a_2, \dots, \mu - a_i\} \quad (1.4)$$

определяется число запретных двоичных циклов из множества $\mathfrak{A}(L_\nu)$.

Рассмотрим мультимножество $2i$ двоичных циклов из множества $\mathfrak{A}(L_\nu)$, в которые входят элементы множества (1.4). Это мультимножество запретных двоичных циклов имеет вид

$$\begin{aligned} & \langle (a_1, \nu - a_1), (a_2, \nu - a_2), \dots, (a_i, \nu - a_i), \\ & (\mu - a_1, \nu - \mu + a_1), (\mu - a_2, \nu - \mu + a_2), \dots, (\mu - a_i, \nu - \mu + a_i) \rangle, \end{aligned} \quad (1.5)$$

где операции сложения и вычитания осуществляются в группе вычетов.

Если в мультимножестве (1.5) все двоичные циклы различны, то число запретов максимально и равно $2i$. В этом случае третий этап заключается в применении вероятностной схемы B выбора (без возвращения) $k - i$ двоичных циклов из некоторого подмножества $\mathfrak{A}(L_\nu)$ с числом элементов, равным $N_\nu - 2i$.

Сокращение числа запретных двоичных циклов по сравнению с максимальным, равным $2i$, определяется некоторыми соотношениями для членов последовательности $(a_1, a_2, \dots, a_i)$, где $1 \leq i \leq k$. Дадим описание этих соотношений.

Лемма 3. *Сокращение максимального числа запретов двоичных циклов на единицу по сравнению с максимальным числом $2i$ существует тогда и только тогда, когда найдутся такие $1 \leq r < s \leq i$, что для членов последовательности $(a_1, a_2, \dots, a_i)$ выполнено одно из равенств*

$$a_r + a_s = \nu, \quad a_r - a_s = \nu - \mu, \quad a_r + a_s = 2\mu - \nu. \quad (1.6)$$

Действительно, сокращение на единицу максимального числа запретных циклов означает совпадение некоторых двоичных циклов в мультимножестве (1.5). Это совпадение порождает для некоторых $1 \leq r < s \leq i$ соотношения вида

$$a_r + a_s = \nu, \quad a_r - a_s + \mu = \nu, \quad \mu - a_r + \mu - a_s = \nu,$$

которые равносильны равенствам (1.6).

Для оценки вероятности события $D_{rs}, 1 \leq r < s \leq i$, состоящего в том, что для случайного вектора $(a_1, a_2, \dots, a_i)$ выполнено хотя бы одно из равенств (1.6), рассмотрим вероятностную схему A выбора без возвращения, в которой выбор i двоичных циклов проводится из N_μ двоичных циклов множества $\mathfrak{A}(L_\mu)$. В общем случае число вариантов выбора i двоичных циклов без возвращения равно $(N_\mu)_i$. Если при выборке выполнено какое-нибудь из соотношений (1.6), то в вероятностной схеме реализуется событие D_{rs} , состоящее в появлении двоичных циклов, один из которых однозначно определяется другим. В этом случае число соответствующих выборок равно $(N_\mu)_{i-1}$ и вероятность события D_{rs} равна

$$\mathbf{P}(D_{rs}) = \frac{(N_\mu)_{i-1}}{(N_\mu)_i}. \quad (1.7)$$

Из формулы (1.7) следует, что вероятность появления соотношений вида (1.6) для вероятностной схемы A выбора без возвращения двоичных циклов из $\mathfrak{A}(L_\mu)$ удовлетворяет неравенству

$$\mathbf{P}_{n,i}(A) \leq \frac{3i^2}{N_\mu - i + 1}. \quad (1.8)$$

Ввиду общности значений координат вектора $(a_1, a_2, \dots, a_i)$ аналогичное событие $\bar{D}_{rs}$, связанное с соотношениями вида (1.6), должно независимо произойти и в вероятностной схеме B выбора без возвращения из множества $\mathfrak{A}(L_\nu)$, причем вероятность $\mathbf{P}(\bar{D}_{rs})$ определяется аналогично формулой

$$\mathbf{P}(\bar{D}_{rs}) = \frac{(N_\nu)_{k-i-1}}{(N_\nu)_{k-i}}. \quad (1.9)$$

Согласно (1.9) для вероятностной схемы B выбора с возвращением $k-i$ двоичных циклов из множества $\mathfrak{A}(L_\nu)$ вероятность выполнения для элементов циклов хотя бы одного соотношения вида (1.6) удовлетворяет неравенству

$$\mathbf{P}_{n,k-i}(B) \leq \frac{3(k-i)^2}{N_\nu - k + i + 1}. \quad (1.10)$$

В силу независимости событий для вероятностных схем A и B для $\mathbf{Q}_{n,k,i}$ — вероятности того, что максимальное число запретных двоичных циклов уменьшится, — верно неравенство

$$\mathbf{Q}_{n,k,i} \leq \mathbf{P}_{ni}(A) \cdot \mathbf{P}_{n,k-i}(B).$$

В результате, применив неравенства (1.8) и (1.10), получим оценку

$$\mathbf{Q}_{n,k,i} \leq \frac{9(i(k-i))^2}{(N_\mu - i + 1)(N_\nu - k + i + 1)}, \quad (1.11)$$

которая обосновывает следующее утверждение.

Лемма 4. При $n \rightarrow \infty$ и $\frac{k^2}{n} \rightarrow 0$ для любых $1 \leq i \leq k$ вероятность $\mathbf{Q}_{n,k,i}$ того, что максимальное значение $2i$ числа запретных двоичных циклов уменьшится хотя бы на единицу, имеет следующую асимптотическую оценку:

$$\mathbf{Q}_{n,k,i} = O\left(\frac{k^4}{n^2}\right). \quad (1.12)$$

3. Дисперсия случайной величины ζ_n

Вычисление биномиальных моментов $\xi_n(L_\mu, L_\nu)$ имеет ряд особенностей, зависящих от четности числа n . По этой причине рассмотрим сначала случай нечетного n , когда число двоичных циклов в L_μ и L_ν равно $N = \frac{n-1}{2}$.

При нечетном n вне зависимости от четности весов двоичных циклов равновесных инволюций L_μ и L_ν имеем следующую лемму.

Лемма 5. При нечетном n для любой пары равновесных инволюций L_μ и L_ν , $\mu \neq \nu$, асимптотическое выражение для k -го биномиального момента случайной величины $\xi_n(L_\mu, L_\nu)$ имеет при $n \rightarrow \infty$ вид

$$\begin{aligned} & \mathbf{B}_{kn}(\mu, \nu) = \\ &= \frac{1}{2^k k!} \sum_{i=0}^k \binom{k}{i} \prod_{j=0}^{i-1} \left(1 - \frac{1}{n-2j}\right) \prod_{j=0}^{k-i-1} \left(1 - \frac{2i+1}{n-2i-2j}\right) \left(1 + O\left(\frac{k^4}{n^2}\right)\right). \end{aligned} \quad (2.1)$$

Формула (2.1) вытекает из леммы 2 и последующего использования вероятностных схем A и B выбора двоичных циклов из множеств $\mathfrak{A}(L_\mu)$ и $\mathfrak{A}(L_\nu)$ с учетом указанного в лемме 3 возможного сокращения максимального числа $2i$ запретных двоичных циклов, выбираемых по схемам A и B . Для вероятности такого сокращения $\mathbf{Q}_{n,k,i}$ выполнены неравенство (1.11) и асимптотическая оценка (1.12).

Используя эти условия, формулу для k -го биномиального момента ξ_n можно записать в виде

$$\mathbf{B}_{kn}(\mu, \nu) = \frac{1}{k!} \sum_{i=0}^k \binom{k}{i} \frac{\left(\frac{n-1}{2}\right)_i \left(\frac{n-1}{2} - 2i\right)_{k-i}}{\prod_{j=0}^{k-1} (n-2j)} (1 - \mathbf{Q}_{n,k,i}). \quad (2.2)$$

В формуле (2.2) знаменатель дроби определяет при нечетном n число способов выбора k двоичных циклов, удовлетворяющих условию попарной независимости элементов. Произведение $\left(\frac{n-1}{2}\right)_i \left(\frac{n-1}{2} - 2i\right)_{k-i}$ равно числу способов выбора без возвращения двоичных циклов из $\mathfrak{A}(L_\mu)$ и $\mathfrak{A}(L_\nu)$ при условии, что число запретных двоичных циклов максимально и равно $2i$. Выражение $(1 - \mathbf{Q}_{n,k,i})$ определяет для указанных схем A и B случайного выбора двоичных циклов с возвращением, что число запретных двоичных циклов равно $2i$.

Используя лемму 5, докажем следующую теорему.

Теорема 2. При нечетном n для любой пары равновесных инволюций L_μ и L_ν , $\mu \neq \nu$, равномерно по $0 \leq k \leq n^{\frac{1}{6}}$ для k -го биномиального момента случайной величины $\xi_n(L_\mu, L_\nu)$ выполнено равенство

$$\mathbf{B}_{kn}(\mu, \nu) = \frac{1}{k!} \left(1 - \frac{k}{n} - \frac{k(k-1)}{2n} \right) (1 + R_n), \quad (2.3)$$

где $R_n = O\left(\frac{1}{n^{\frac{4}{3}}}\right)$ при $n \rightarrow \infty$.

Входящие в формулу (2.1) для k -го момента $\mathbf{B}_{kn}(\mu, \nu)$ произведения при выполнении условий теоремы 2 имеют следующие асимптотические представления:

$$\prod_{j=0}^{i-1} \left(1 - \frac{1}{n-2j} \right) = 1 - \frac{i}{n} + O\left(\frac{1}{n^{\frac{5}{3}}}\right), \quad (2.4)$$

$$\prod_{j=0}^{k-i-1} \left(1 - \frac{2i+1}{n-2i+j} \right) = 1 - \frac{(2i+1)(k-i)}{n} + O\left(\frac{1}{n^{\frac{4}{3}}}\right). \quad (2.5)$$

Используя формулы (2.4) и (2.5), из равенства (2.1) получим

$$\begin{aligned} \mathbf{B}_{kn}(\mu, \nu) = \\ = \frac{1}{2^k k!} \sum_{i=0}^k \binom{k}{i} \left(1 - \frac{i}{n} - \frac{(2i+1)(k-i)}{n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \end{aligned} \quad (2.6)$$

После очевидных преобразований из формулы (2.6) следует равенство

$$\mathbf{B}_{kn}(\mu, \nu) = \frac{1}{2^k k!} \sum_{i=0}^k \binom{k}{i} \left(1 - \frac{k}{n} - \frac{2i(k-i)}{n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \quad (2.7)$$

После суммирования в правой части равенства (2.7) получим формулу (2.3). Теорема доказана.

Следствие 1. Для любой пары равновесных инволюций L_μ и L_ν , $\mu \neq \nu$, при нечетном $n \rightarrow \infty$ случайная величина $\xi_n(L_\mu, L_\nu)$ имеет в качестве предельного распределение Пуассона с параметром $\lambda = 1$.

Из теоремы 2 следует, что при любом $k \geq 0$ для k -го биномиального момента $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, при $n \rightarrow \infty$

$$\mathbf{B}_{kn}(\mu, \nu) \rightarrow \frac{1}{k!}, \quad (2.8)$$

т. е. распределение $\xi_n(L_\mu, L_\nu)$ имеет в качестве предельного распределение Пуассона с параметром $\lambda = 1$.

Из теорем 1 и 2 в качестве следствия получим основную асимптотическую формулу, которая необходима для нахождения дисперсии аддитивного весового дефицита.

Следствие 2. Для любой пары равновесных инволюций L_μ и L_ν , $\mu \neq \nu$, при нечетном $n \rightarrow \infty$ для вероятности нулевого значения случайной величины $\xi_n(L_\mu, L_\nu)$ выполнено асимптотическое равенство

$$\mathbf{P}(\xi_n(L_\mu, L_\nu) = 0) = \left(1 + \frac{1}{2n} \right) e^{-1} \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \quad (2.9)$$

Действительно, из равенства (1.1) теоремы 1, в соответствии с неравенством Бонферрони, следует асимптотическая формула при $n \rightarrow \infty$

$$\mathbf{P}(\xi_n(L_\mu, L_\nu) = 0) = \sum_{k=0}^{\left[n^{\frac{1}{6}} \right]} (-1)^k \mathbf{B}_{kn}(\mu, \nu) + O\left(\frac{1}{\left(\left[n^{\frac{1}{6}} \right] \right)!} \right). \quad (2.10)$$

Из равенства (2.10) и формулы (2.3) теоремы 2 при $n \rightarrow \infty$ получим

$$\begin{aligned} \mathbf{P}(\xi_n(L_\mu, L_\nu) = 0) = \\ = \left[\sum_{k=0}^{\left[\frac{1}{n^{\frac{1}{6}}}\right]} \frac{(-1)^k}{k!} - \frac{1}{n} \sum_{k=0}^{\left[\frac{1}{n^{\frac{1}{6}}}\right]} \frac{(-1)^k k}{k!} - \frac{1}{2n} \sum_{k=0}^{\left[\frac{1}{n^{\frac{1}{6}}}\right]} \frac{(-1)^k k(k-1)}{k!} \right] \left(1 + O\left(\frac{1}{n^{\frac{1}{6}}}\right) \right) + \\ + O\left(\frac{1}{\left(\left[\frac{1}{n^{\frac{1}{6}}}\right]\right)!}\right). \end{aligned} \quad (2.11)$$

Заменяя в правой части равенства (2.11) частичные суммы для e^{-1} их предельными значениями и опуская члены более высокого порядка малости, получаем формулу (2.9) следствия 2.

Для применения формулы (0.4) при выводе асимптотической формулы для дисперсии случайной величины ζ_n уточним асимптотическое представление (0.3) математического ожидания $\mathbf{M}\zeta_n$ при $n \rightarrow \infty$.

Формула (0.1) получена методом включения-исключения, поэтому, применяя неравенство Бонферрони, получим

$$\mathbf{M}\zeta_n = n \sum_{k=0}^{\left[\frac{1}{n^{\frac{1}{6}}}\right]} (-1)^k \frac{2^k \left(\left(\frac{n-1}{2}\right)_k\right)^2}{k!(n)_{2k}} + O\left(\frac{1}{\left(\left[\frac{1}{n^{\frac{1}{6}}}\right]\right)!}\right). \quad (2.12)$$

При любом $k \geq 1$ имеем представление

$$\frac{\left(\frac{n-1}{2}\right)_k^2}{(n)_{2k}} = \frac{1}{2^{2k}} \prod_{j=0}^{k-1} \left(1 - \frac{1}{n-2j}\right). \quad (2.13)$$

Из соотношений (2.4), (2.13) следует, что равномерно по $0 \leq k \leq \left[\frac{1}{n^{\frac{1}{6}}}\right]$ при $n \rightarrow \infty$

$$\frac{\left(\left(\frac{n-1}{2}\right)_k\right)^2}{(n)_{2k}} = \frac{1}{2^{2k}} \left(1 - \frac{k}{n} + O\left(\frac{1}{n^{\frac{5}{3}}}\right)\right). \quad (2.14)$$

Учитывая равенство (2.14) и отбрасывая члены более высокого порядка малости, равенство (2.12) при $n \rightarrow \infty$ представим в следующем виде:

$$\mathbf{M}\zeta_n = n \sum_{k=0}^{\left[\frac{1}{n^{\frac{1}{6}}}\right]} \frac{(-1)^k}{2^k k!} \left(1 - \frac{k}{n}\right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right). \quad (2.15)$$

Используя представление правой части равенства (2.15) через частичные суммы ряда для $e^{-\frac{1}{2}}$ и свойства частичных сумм ряда лейбницевского типа, получаем при $n \rightarrow \infty$

$$\mathbf{M}\zeta_n = ne^{-\frac{1}{2}} \left(1 + \frac{1}{2n}\right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right). \quad (2.16)$$

Из формулы (2.16) при $n \rightarrow \infty$ следует асимптотика для величины $(\mathbf{M}\zeta_n)^2$, необходимая для оценки дисперсии ζ_n :

$$\mathbf{M}(\zeta_n)^2 = n^2 e^{-1} \left(1 + \frac{1}{n}\right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right). \quad (2.17)$$

Используя полученные результаты, докажем следующую теорему.

Теорема 3. *Для дисперсии случайной величины ζ_n , равной аддитивному весовому дефициту случайной равновероятной инволюции при нечетном модуле n , $n \rightarrow \infty$, справедлива асимптотическая формула*

$$\mathbf{D}\zeta_n = n \left(e^{-\frac{1}{2}} - \frac{3}{2}e^{-1}\right) \left(1 + O\left(\frac{1}{n^{\frac{1}{3}}}\right)\right). \quad (2.18)$$

Для доказательства теоремы 3 используем формулу (0.4) и следующую формулу для биномиального момента второго порядка случайной величины ζ_n (см. [3]):

$$\mathbf{B}_2\zeta_n = \sum_{1 \leq \mu < \nu < n-1} \mathbf{P}(\xi_n(L_\mu, L_\nu) = 0). \quad (2.19)$$

Из равенств (2.19), (2.9), (2.16), (2.17) при $n \rightarrow \infty$ находим

$$\begin{aligned} \mathbf{D}(\zeta_n) &= n(n-1) \left(1 + \frac{1}{2n}\right) e^{-1} \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right) + \\ &+ ne^{-\frac{1}{2}} \left(1 + \frac{1}{2n}\right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right) - n^2 \left(1 + \frac{1}{n}\right) e^{-1} \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right)\right). \end{aligned} \quad (2.20)$$

Из равенства (2.20) после упрощений получаем асимптотику вида (2.18) для дисперсии $\mathbf{D}\zeta_n$ при нечетных $n \rightarrow \infty$.

Рассмотрим случай четного n . Доказательства основных результатов в этом случае проводятся по той же схеме, что и для нечетного n . Одним из отличий случая четного n является зависимость асимптотики биномиальных моментов случайной величины $\xi_n(L_\mu, L_\nu)$ от четности

весов двоичных циклов, входящих в равновесные инволюции L_μ и L_ν (обозначения для инволюций вида L_μ^0 и L_μ^1 введены перед леммой 1).

Асимптотическая формула для биномиальных моментов случайной величины $\xi_n(L_\mu, L_\nu)$ при четном $n \rightarrow \infty$ приведена в следующей теореме.

Теорема 4. При натуральных четных $n \rightarrow \infty$ биномиальные моменты случайных величин $\xi_n(L_\mu^\rho, L_\nu^\tau)$, $\mu \neq \nu$, $\rho, \tau \in \{0, 1\}$, имеют место асимптотические представления:

$$\mathbf{B}_{kn}(L_\mu^1, L_\nu^1) = \frac{1}{k!} \left(1 + \frac{k}{n} - \frac{k(k-1)}{2n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right), \quad (2.21)$$

$$\mathbf{B}_{kn}(L_\mu^0, L_\nu^0) = \frac{1}{k!} \left(1 - \frac{k}{n} - \frac{k(k-1)}{2n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right), \quad (2.22)$$

$$\mathbf{B}_{kn}(L_\mu^1, L_\nu^0) = \frac{1}{k!} \left(1 - \frac{k(k-1)}{2n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right) \quad (2.23)$$

равномерно для всех $0 \leq k \leq n^{\frac{1}{6}}$ при $n \rightarrow \infty$.

Доказательство каждой из асимптотических формул теоремы 4 проводится таким же путем, как доказательства асимптотического представления (2.3) из теоремы 2. По этой причине приведем только схему доказательства формулы (2.21).

Применяя при четном n схему вывода формулы (2.2) для нечетных весов μ, ν , получаем формулу

$$\begin{aligned} \mathbf{B}_{kn}(L_\mu^1, L_\nu^1) &= \\ &= \frac{1}{k!} \left(\sum_{i=0}^k \binom{k}{i} \frac{\left(\frac{n}{2}\right)_i \left(\frac{n}{2} - 2i\right)_{k-i}}{\prod_{j=0}^k (n+1-2j)} \right) \prod_{j=0}^k \left(1 + \frac{2}{n-1-2j} \right) (1 - Q_{n,k,i}). \end{aligned}$$

Сомножитель, равный сумме по индексу i , в правой части данной формулы с точностью до замены n на $n-1$ совпадает с аналогичным сомножителем в формуле (2.2). Поэтому можно воспользоваться асимптотической формулой (2.3) и получить формулу (2.21).

Аналогичным способом выводятся формулы (2.22) и (2.23).

С использованием леммы 1 и теоремы 4 докажем следующую теорему.

Теорема 5. При натуральном четном $n \rightarrow \infty$ для k -го биномиального момента случайной величины $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, справедлива асимптотическая формула

$$\mathbf{B}_{kn}(L_\mu, L_\nu) = \frac{1}{k!} \left(1 - \frac{k(k-1)}{2n} \right) (1 + R_n), \quad (2.24)$$

где $R_n = O\left(\frac{1}{n^{\frac{4}{3}}}\right)$ равномерно для всех $0 \leq k \leq n^{\frac{1}{6}}$.

При четном n на множестве из $\binom{n}{2}$ пар (L_μ, L_ν) зададим равномерное распределение. Тогда вероятности выбора пар $(L_\mu^1, L_\nu^1), (L_\mu^0, L_\nu^0), (L_\mu^1, L_\nu^0)$ определяются п. б) леммы 1. Рассматривая формулы (2.21)–(2.23) как асимптотики условных биномиальных моментов ξ_n , при четном n , биномиальный момент $\xi(L_\mu, L_\nu)$ k -го порядка можно записать в виде

$$\mathbf{B}_{kn}(L_\mu, L_\nu) = \frac{1}{\binom{n}{2}} \left[\begin{aligned} & \frac{n(n-2)}{8} \frac{1}{k!} \left(1 + \frac{k}{n} - \frac{k(k-1)}{2n} \right) + \\ & + \frac{n(n-2)}{8} \frac{1}{k!} \left(1 - \frac{k}{n} - \frac{k(k-1)}{2n} \right) + \\ & + \frac{n^2}{4} \frac{1}{k!} \left(1 - \frac{k(k-1)}{2n} \right) \end{aligned} \right] (1 + R_{nk}). \quad (2.25)$$

Из равенства (2.25) после упрощений следует формула (2.24).

Из теоремы 5 вытекают два следствия.

Следствие 3. При четном $n \rightarrow \infty$ для вероятности нулевого значения случайной величины $\xi_n(L_\mu, L_\nu)$, $\mu \neq \nu$, справедлива асимптотическая формула

$$\mathbf{P}(\xi_n(L_\mu, L_\nu) = 0) = e^{-1} \left(1 - \frac{1}{2n} \right) (1 + R_n), \quad (2.26)$$

где $R_n = O\left(\frac{1}{n^{\frac{4}{3}}}\right)$.

Формула (2.26) следует из теоремы 1 и асимптотики (2.24).

Следствие 4. При четном $n \rightarrow \infty$ для второго биномиального момента $\mathbf{B}_2 \zeta_n$ справедлива асимптотическая формула

$$\mathbf{B}_2 \zeta_n = \frac{n(n-1)}{2} e^{-1} \left(1 - \frac{1}{2n} \right) \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \quad (2.27)$$

Формула (2.27) следует из равенства (2.19) и асимптотики (2.26).

Для четных $n \geq 4$ асимптотическая оценка при $n \rightarrow \infty$ правой части равенства (0.2) приводит к формуле

$$\mathbf{M}\zeta_n = ne^{-\frac{1}{2}} \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \quad (2.28)$$

Отсюда следует равенство

$$(\mathbf{M}\zeta_n)^2 = n^2 e^{-1} \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right). \quad (2.29)$$

Используя формулы (0.4), (2.27)–(2.29), получим

$$\mathbf{D}(\zeta_n) = \left[n(n-1) \left(1 - \frac{1}{2n} \right) e^{-1} + ne^{-\frac{1}{2}} - n^2 e^{-1} \right] \left(1 + O\left(\frac{1}{n^{\frac{4}{3}}}\right) \right).$$

Очевидные преобразования для четного $n \rightarrow \infty$ приводят к равенству

$$\mathbf{D}(\zeta_n) = n \left(e^{-\frac{1}{2}} - \frac{3}{2} e^{-1} \right) \left(1 + O\left(\frac{1}{n^{\frac{1}{3}}}\right) \right).$$

С учетом этого равенства и теоремы 3 сформулируем основной результат данной работы.

Теорема 6. *Асимптотическая формула для дисперсии случайной величины ζ_n , равной аддитивному весовому дефициту случайной максимальной инволюции, действующей на группе вычетов по модулю n , при $n \rightarrow \infty$ имеет вид*

$$\mathbf{D}(\zeta_n) = n \left(e^{-\frac{1}{2}} - \frac{3}{2} e^{-1} \right) \left(1 + O\left(\frac{1}{n^{\frac{1}{3}}}\right) \right). \quad (2.30)$$

Отметим, что полученная в [4] асимптотика дисперсии случайной величины ζ_n , $n = 2^m$, для случая аддитивной группы поля $GF(n)$ имеет такой же главный член, как и в формуле (2.30). Однако относительная погрешность равна $(1 + O(\frac{1}{n}))$.

Список литературы

- [1] Сачков В.Н., “Комбинаторные свойства дифференциально 2-равномерных подстановок”, *Математические вопросы криптографии*, **6:1** (2015), 159–180.
- [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., Круглов И.А., “Моменты весового дефицита случайной равновероятной инволюции, действующей на конечном векторном пространстве над полем из двух элементов”, *Математические вопросы криптографии*, **9**:4 (2018), 101–124.
- [5] Сачков В.Н., *Курс комбинаторного анализа*, Москва–Ижевск : НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.