Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, Разностные спецификации подстановок и разбиения в кольцо вычетов, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 1, 127–150

DOI: <https://doi.org/10.4213/mvk110>

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: 3.85.7.115

26 апреля 2023 г., 16:46:52

УДК 519.12

Разностные спецификации подстановок и разбиения в кольце вычетов

В. Н. Сачков

Академия криптографии Российской Федерации, Москва

Получено 22.IV.2013

Для подстановки $s \in S_n$ разностную спецификацию можно понимать как неупорядоченное мультимножество разностей $\Delta_i \equiv (s(i) - i) \pmod{n}$, $1 \leq i \leq n$; число отсутствующих разностей называется дефицитом подстановки. Подстановки с одинаковыми спецификациями считаются эквивалентными. В статье найдены формулы для числа C_{nm} классов эквивалентности подстановок из S_n , имеющих дефицит $\eta_n = n - m$, а также формула для общего числа C_n классов эквивалентности. При случайном равновероятном выборе классов эквивалентности найдено точное распределение η_n , а при простом n и $n \rightarrow \infty$ — предельные гипергеометрические и нормальные распределения.

Ключевые слова: разностные характеристики, разностные спецификации подстановок, дефициты классов эквивалентности подстановок

Difference specification of substitutions and partitions in a residue ring

V. N. Sachkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. The difference specification of a substitution $s \in S_n$ may be defined as an unordered multiset of differences $\Delta_i \equiv (s(i) - i) \pmod{n}$, $1 \leq i \leq n$; the number of unappeared differences is called a deficit of substitution. We find formulas for the number of all possible difference specifications and for the number of difference specifications for substitutions with given deficit. Under some conditions exact and asymptotic distributions of the deficit are found.

Key words: difference characteristics, difference specifications of substitutions, deficits of equivalence classes of substitutions

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 5, no. 1, pp. 127–150 (Russian).

© 2014 Сачков В. Н.

Для подстановки $s = \begin{pmatrix} 1 & 2 & \dots & n \\ s(1) & s(2) & \dots & s(n) \end{pmatrix}$ вектор $(\Delta_1, \Delta_2, \dots, \Delta_n)$,

где Δ_i — наименьший неотрицательный вычет, определяемый сравнением $\Delta_i \equiv (s(i) - i) \pmod{n}$, $1 \leq i \leq n$, называется *разностной характеристикой* этой подстановки. *Разностная спецификация* подстановки s определяется как вектор $(x_0, x_1, \dots, x_{n-1})$, для которого

$$x_k = \left| \{i : \Delta_i = k, i = 1, 2, \dots, n\} \right|, \quad k = 0, 1, \dots, n-1. \quad (0.1)$$

Координаты вектора $(x_0, x_1, \dots, x_{n-1})$ удовлетворяют соотношениям

$$\sum_{k=0}^{n-1} kx_k \equiv 0 \pmod{n}, \quad \sum_{k=0}^{n-1} x_k = n, \quad (0.2)$$

первое из которых определяет совокупность разбиений чисел, кратных n , на не более чем n слагаемых, не превосходящих n . Такие разбиения будем называть разбиениями в кольце вычетов по модулю n .

На множестве S_n всех подстановок степени n рассматривается отношение эквивалентности, при котором $s \sim s'$, $s, s' \in S_n$, тогда и только тогда, когда их разностные спецификации совпадают. С использованием теоремы М. Холла о свойствах разностных характеристик подстановок в п. 1 доказано, что каждому вектору $(x_0, x_1, \dots, x_{n-1})$ с условиями (0.2) соответствует непустой класс эквивалентности подстановок.

Если ξ_n — число ненулевых, а η_n — число нулевых координат $(x_0, x_1, \dots, x_{n-1})$ с условиями (0.2), то η_n называется *дефицитом* любой подстановки из класса эквивалентности. Ясно, что $\xi_n + \eta_n = n$. Элементарным способом показывается, что при четном n не существует подстановок степени n с $\xi_n = n$, а при нечетном n — с $\xi_n = n-1$.

С использованием подстановочных матриц и стандартной циклической матрицы в п. 1 дается описание подстановок, принадлежащих классу эквивалентности, определяемому вектором $(x_0, x_1, \dots, x_{n-1})$ с условием (0.2). Подстановки $s \in S_n$, принадлежащие таким классам эквивалентности, что

$$\{k : x_k \neq 0, 0 \leq k \leq n-1\} \subseteq L \subseteq N_0 = \{0, 1, \dots, n-1\}, \quad (0.3)$$

называются L -подстановками. Для таких подстановок понятие L -дефицита r определено равенством

$$r = |\{k : x_k = 0, k \in L\}|, \quad r = 0, 1, \dots, |L| - 1. \quad (0.4)$$

В конце п. 1 получена формула для числа L -подстановок со значением L -дефицита, равным r :

$$S_{nr}(L) = \sum_{k=r}^{|L|-1} (-1)^{k-r} \binom{k}{r} \sum_{\substack{L' : L' \subseteq L \\ |L'|=k}} \text{per } A(L \setminus L'), \quad r = 0, 1, \dots, |L| - 1, \quad (0.5)$$

где $\text{per } A(L \setminus L')$ — перманент циклической $(0, 1)$ -матрицы $A(L \setminus L')$, в которой ненулевые диагонали имеют номера, составляющие множество $L \setminus L'$, $L' \subseteq L \subseteq N_0 = \{0, 1, \dots, n-1\}$. Формула (0.4) является обобщением известной формулы, выражающей число подстановок $s \in S_n$, имеющих дефицит r , через перманенты циклических $(0, 1)$ -матриц [4].

Основные результаты статьи связаны с получением формул для C_{nm} — числа классов эквивалентности подстановок из S_n , для которых дефицит равен $n - m$, т. е. соответствующие разбиения в классе вычетов по модулю n имеют m различных слагаемых, а также для C_n — общего числа классов эквивалентности подстановок $s \in S_n$. Эти формулы имеют вид

$$C_{nm} = \frac{1}{n} \sum_{d|n} \varphi(d) \sum_{j:m/d \leq j \leq n/d} (-1)^{j+m} \binom{n/d}{j} \binom{2n/d - j - 1}{n/d - j} \binom{dj}{m}, \quad (0.6)$$

$$m = 1, 2, \dots, n,$$

$$C_n = \sum_{d|n} \varphi(d) \binom{2n/d - 1}{n/d}, \quad (0.7)$$

где $\varphi(d)$ — функция Эйлера.

При случайном равновероятном выборе классов эквивалентности подстановок точные формулы для распределений случайных величин ξ_n и η_n следуют из формул (0.6) и (0.7). Для n простого и $n \rightarrow \infty$ найдена асимптотика этих распределений:

$$\mathbf{P}(\xi_n = m) = \frac{\binom{n}{m} \binom{n-1}{m-1}}{\binom{2n-1}{n}} \left(1 + O\left(\frac{1}{n}\right) \right) \quad (0.8)$$

равномерно для всех $m \in [3, n-2]$. Аналогичное асимптотическое представление получено для распределения η_n . Из этих представлений следует, что равномерно для всех допустимых значений $w = o(n^{1/6})$ при $n \rightarrow \infty$

$$\mathbf{P}\left((\xi_n - n/2) / \sqrt{n/8} = w\right) = \frac{2}{\sqrt{\pi n}} e^{-w^2/2} (1 + o(1)). \quad (0.9)$$

Соответствующий результат получен и для случайной величины η_n .

Формулы (0.6) и (0.7) выводятся с помощью общей производящей функции $F_n(w, z, y)$ для чисел $a_{nl}(n, m)$, равных количеству классических разбиений числа r на l различных слагаемых из множества $N_0 = \{0, 1, \dots, n-1\}$. Для этой функции получено представление

$$F_n(w, z, y) = \sum_{l=0}^{\infty} z^l \sum_{s=0}^r A_{ns}(w, y) B_{n,r-s}(w), \quad (0.10)$$

в котором производящие функции $A_{nl}(w, y)$ и $B_{n,r-s}(w)$ выражаются через коэффициенты Гаусса [6]. Формулы для C_{nm} и C_n находятся из представлений для $A_{nl}(w, y)$ и $B_{n,r-s}(w)$ с использованием свойств первообразных корней из единицы.

При выводе формул (0.6) и (0.7) в качестве следствия получено новое доказательство тождества Радемахера для функции Эйлера $\varphi(d)$:

$$\sum_{d|n} (-1)^{n+n/d} \varphi(d) = \begin{cases} n, & n - \text{нечетное,} \\ 0, & n - \text{четное,} \end{cases}$$

доказанного ранее Брауэром [2].

В заключение отметим, что формула (0.7) в связи с другой задачей была впервые получена Риорданом [3].

1. Разностные характеристики и спецификации подстановок. Разбиения в кольце вычетов

Для подстановки $s \in S_n$, действующей на множестве $N_0 = \{0, 1, \dots, n-1\}$, разностной характеристикой называется вектор $\Delta(s) = (\Delta_1, \Delta_2, \dots, \Delta_n)$, координаты которого являются наименьшими неотрицательными вычетами по модулю n , определяемыми сравнениями

$$\Delta_i \equiv (s(i) - i) \pmod{n}, \quad i = 1, 2, \dots, n. \quad (1.1)$$

Для координат разностной характеристики выполнено соотношение

$$\Delta_1 + \Delta_2 + \dots + \Delta_n \equiv 0 \pmod{n}. \quad (1.2)$$

Этому соотношению соответствует совокупность композиций чисел из множества $H_n = \{hn, h = 0, 1, \dots, n-1\}$ со слагаемыми из множества $\{0, 1, \dots, n-1\}$. Если m — число различных слагаемых в композиции, то величина $n - m$ называется дефицитом подстановки $s \in S_n$, удовлетворяющей условию (1.1), и обозначается $\text{def}(s) = n - m$ [4].

Так как некоторые характеристики подстановки, например, дефицит, не зависят от порядка слагаемых в композиции (1.2), то удобно перейти от композиций к разбиениям соответствующих чисел, где порядок слагаемых несуществен. Разностной спецификацией подстановки $s \in S_n$ называется вектор $X(s) = (x_0, x_1, \dots, x_{n-1})$, определяемый равенствами

$$x_k = \left| \{i : \Delta_i = k, i = 1, 2, \dots, n\} \right|, \quad k = 0, 1, \dots, n-1. \quad (1.3)$$

Координаты вектора $X(s)$ удовлетворяют соотношениям

$$\sum_{k=0}^{n-1} x_k = n, \quad (1.4)$$

$$\sum_{k=0}^{n-1} kx_k \equiv 0 \pmod{n}. \quad (1.5)$$

Векторы $(x_0, x_1, \dots, x_{n-1})$, удовлетворяющие условиям (1.4) и (1.5), будем называть *разбиениями на n слагаемых в кольце вычетов по модулю n* . Разбиение $(x_0, x_1, \dots, x_{n-1})$ в кольце вычетов по модулю n называется L -разбиением, если

$$L = \{k : x_k \neq 0, 0 \leq k \leq n-1\}. \quad (1.6)$$

Число L -разбиений в кольце вычетов определяется равенством

$$C_n(L) = \left| \left\{ (x_0, x_1, \dots, x_{n-1}) : \sum_{k \in L} x_k = n, \sum_{k \in L} kx_k \equiv 0 \pmod{n} \right\} \right|. \quad (1.7)$$

Если C_{nm} — число разбиений в кольце вычетов по модулю n , имеющих m различных слагаемых, то для $L \subseteq N$

$$C_{nm} = \sum_{L: |L|=m} C_n(L), \quad (1.8)$$

и C_n — общее число таких разбиений — определяется равенством

$$C_n = \sum_{m=1}^n C_{nm}. \quad (1.9)$$

Очевидно, что каждой подстановке $s \in S_n$ соответствует единственный вектор $\Delta(s) = (\Delta_1, \Delta_2, \dots, \Delta_n)$, удовлетворяющий условиям (1.1) и (1.2). На вопрос о том, при каких условиях вектору $(\Delta_1, \Delta_2, \dots, \Delta_n)$ с координатами из множества $N_0 = \{0, 1, \dots, n-1\}$, удовлетворяющему условию (1.2), соответствует подстановка, для которой выполнены соотношения (1.1), отвечает следующая теорема М. Холла [1].

Теорема 1. Пусть $G = \{a_1, a_2, \dots, a_n\}$ — абелева группа и $(b_1, b_2, \dots, b_n)$ — некоторая последовательность элементов G . Тогда для существования такой подстановки $s \in S_n$, что последовательность $(a_{s(1)} - a_1, a_{s(2)} - a_2, \dots, a_{s(n)} - a_n)$ совпадает с последовательностью $(b'_1, b'_2, \dots, b'_n)$, полученной из $(b_1, b_2, \dots, b_n)$ некоторой перестановкой, необходимо и достаточно выполнение условия

$$b_1 + b_2 + \dots + b_n = 0. \quad (1.10)$$

В рассматриваемом случае, когда абелевой группой является аддитивная группа кольца вычетов по модулю n , из теоремы 1 имеем следствие 1.

Следствие 1. Каждому вектору $(x_0, x_1, \dots, x_{n-1})$ с координатами из множества $N_0 = \{0, 1, \dots, n-1\}$, удовлетворяющему соотношениям (1.4) и (1.5), соответствует непустое множество подстановок $s \in S_n$, для которых этот вектор является разностной спецификацией.

Действительно, рассмотрим некоторый вектор $(\Delta_1, \Delta_2, \dots, \Delta_n)$ с координатами из множества $\{0, 1, \dots, n-1\}$, удовлетворяющий условиям (1.3). Тогда из соотношения (1.5) получаем, что $\Delta_1 + \Delta_2 + \dots + \Delta_n \equiv 0 \pmod{n}$. Из теоремы 1 следует, что существует подстановка $s \in S_n$, для которой перестановка $(\Delta'_1, \Delta'_2, \dots, \Delta'_n)$ координат вектора $(\Delta_1, \Delta_2, \dots, \Delta_n)$ является разностной характеристикой. Так как соотношения (1.4) и (1.5) выполнены для $(\Delta_1, \Delta_2, \dots, \Delta_n)$, то они имеют место и для $(\Delta'_1, \Delta'_2, \dots, \Delta'_n)$. Следовательно, подстановка $s \in S_n$ имеет разностную спецификацию $(x_0, x_1, \dots, x_{n-1})$. Число различных подстановок $s \in S_n$, соответствующих вектору $(x_0, x_1, \dots, x_{n-1})$, зависит от числа различных векторов $(\Delta_1, \Delta_2, \dots, \Delta_n)$, отвечающих $(x_0, x_1, \dots, x_{n-1})$.

На множестве S_n , содержащем все подстановки степени n , зададим бинарное отношение, обозначаемое знаком « $\sim$ ». Будем считать, что $s \sim s'$, $s, s' \in S_n$, если разностные спецификации s и s' совпадают. Это бинарное отношение является отношением эквивалентности, и ему соответствует разбиение множества S_n на C_n непересекающихся классов, где C_n — число различных разбиений в кольце вычетов по модулю n . Число классов подстановок, имеющих дефицит $n - m$, равно C_{nm} , $m = 0, 1, \dots, n - 1$. В соответствии со следствием из теоремы 1 некоторые классы могут быть пустыми тогда и только тогда, когда соответствующие разбиения в кольце вычетов по модулю n , а следовательно, разностные спецификации, не существуют. Оказывается, что это может зависеть от четности или нечетности n . Приведем некоторые свойства чисел C_{nm} при $m = n, n - 1$.

Свойство 1 [4]. Для любых натуральных значений $n \geq 2$ имеем

$$C_{nn} = \begin{cases} 1, & n - \text{нечетное}, \\ 0, & n - \text{четное}. \end{cases} \quad (1.11)$$

Так как при $m = n$ единственный вектор $(x_0, x_1, \dots, x_{n-1})$, удовлетворяющий соотношениям (1.4) и (1.5), имеет вид $(1, 1, \dots, 1)$, то имеем сравнение

$$\binom{n}{2} \equiv 0 \pmod{n}, \quad (1.12)$$

которое выполнено тогда и только тогда, когда n нечетное.

Следствие 2. Подстановки степени n , имеющие дефицит, равный нулю, существуют тогда и только тогда, когда n нечетное.

Свойство 2 [4]. Для любых натуральных значений $n \geq 2$ имеем

$$C_{n,n-1} = \begin{cases} n, & n - \text{четное}, \\ 0, & n - \text{нечетное}. \end{cases} \quad (1.13)$$

При $m = n - 1$ вектор $(x_0, x_1, \dots, x_{n-1})$ удовлетворяет соотношению (1.5) тогда и только тогда, когда существуют такие вычеты $i, j \in \{0, 1, \dots, n - 1\}$, $i \neq j$, что $x_i = 0$, $x_j = 2$, и для всех вычетов $k \neq i, j$ имеем $x_k = 1$. Поэтому из (1.5) следует сравнение

$$\binom{n}{2} + j - i \equiv 0 \pmod{n}. \quad (1.14)$$

Если n нечетное, то сравнение (1.14) противоречит условию $i \neq j$ и не может быть выполнено. Если же n четное, то имеется n пар (i, j) , удовлетворяющих сравнению (1.14).

Следствие 3. *Подстановки степени n , имеющие дефицит, равный единице, существуют тогда и только тогда, когда n четное.*

Минимальное значение дефицита подстановки $s \in S_n$ определяется следствием из свойств 1 и 2.

Следствие 4. *Имеет место следующее соотношение:*

$$\min_{s \in S_n} \text{def}(s) = \begin{cases} 0, & n - \text{нечетное}, \\ 1, & n - \text{четное}. \end{cases} \quad (1.15)$$

Дадим теперь наглядное матричное описание подстановок множества S_n , принадлежащих классам эквивалентности, определяемым с использованием разностных спецификаций. Рассмотрим матрицу $D = (d_{ij})$, где $d_{ij} \in \{0, 1, \dots, n-1\}$ и

$$d_{ij} \equiv (j - i) \pmod{n}, \quad i, j = 1, 2, \dots, n. \quad (1.16)$$

Матрица D — циклическая, и элементы d_{ij} , для которых

$$i - j \equiv k \pmod{n}, \quad 0 \leq k \leq n-1, \quad (1.17)$$

расположены на k -й циклической диагонали. Возьмем произвольную подстановку $s \in S_n$ и рассмотрим элементы $d_{i, s(i)}$, $i = 1, 2, \dots, n$. Все эти элементы лежат в разных строках и столбцах и соответствуют ненулевым элементам подстановочной матрицы, отвечающей подстановке s . С другой стороны, совокупность этих элементов образует разностную характеристику указанной подстановки s . Если для этой разностной характеристики разностная спецификация s определяется вектором $(x_0, x_1, \dots, x_{n-1})$, то ровно x_k элементов разностной характеристики s располагается на k -й циклической диагонали матрицы D , $k = 0, 1, \dots, n-1$.

Следующее свойство дает описание подстановки $s \in S_n$ с заданной разностной спецификацией.

Свойство 3. *Для того, чтобы n элементов матрицы D соответствовали подстановке $s \in S_n$ с заданной разностной спецификацией $(x_0, x_1, \dots, x_{n-1})$, необходимо и достаточно выполнение следующих условий.*

1. Элементы должны лежать в разных строках и столбцах.

2. На k -й диагонали матрицы D должны находиться x_k элементов, $k = 0, 1, \dots, n-1$, $x_0 + x_1 + \dots + x_{n-1} = n$.

Действительно, n элементов матрицы D соответствуют некоторой подстановке $s \in S_n$ тогда и только тогда, когда они лежат в разных строках и столбцах, причем эти элементы определяют вектор $(\Delta_1, \Delta_2, \dots, \Delta_n)$, являющийся разностной характеристикой подстановки s . Разностная характеристика имеет x_k координат, равных k , $k = 0, 1, \dots, n-1$. Так как $\Delta_1 + \Delta_2 + \dots + \Delta_n \equiv 0 \pmod{n}$, то $\sum_{k=0}^{n-1} kx_k \equiv 0 \pmod{n}$.

Свойство 4. Совокупность всех подстановок s степени n , имеющих разностные спецификации $(x_0, x_1, \dots, x_{n-1})$, может быть получена путем последовательного перебора по n элементов из разных строк и столбцов матрицы D с условием, что x_k элементов выбираются с k -й циклической диагонали, $x_0 + x_1 + \dots + x_{n-1} = n$.

Для $Q(x_0, x_1, \dots, x_{n-1})$ — числа подстановок $s \in S_n$, имеющих разностную спецификацию $(x_0, x_1, \dots, x_{n-1})$, имеет место оценка

$$Q(x_0, x_1, \dots, x_{n-1}) \leq \frac{n!}{x_0! x_1! \dots x_{n-1}!}, \quad x_0 + x_1 + \dots + x_{n-1} = n. \quad (1.18)$$

Рассмотрим подстановки $s \in S_n$, для которых на разностные спецификации наложены некоторые ограничения.

Пусть $A(L)$ — циклическая $(0,1)$ -матрица, для которой номера всех циклических диагоналей из единиц образуют множество $L \subseteq \{0, 1, \dots, n-1\}$, а остальные циклические диагонали нулевые. Каждой совокупности из n попарно неколлинеарных единиц $A(L)$ соответствует подстановка степени n . Множество всех таких подстановок обозначим через $S_n(L)$. Каждая подстановка $s \in S_n(L)$ имеет разностную спецификацию $(x_0, x_1, \dots, x_{n-1})$, удовлетворяющую условию

$$\{k : x_k \neq 0, \quad 0 \leq k \leq n-1\} \subseteq L. \quad (1.19)$$

Число подстановок $|S_n(L)|$ определяется формулой

$$|S_n(L)| = \text{per } A(L), \quad (1.20)$$

где $\text{per } A(L)$ — перманент циклической $(0,1)$ -матрицы, имеющей $|L|$ циклических диагоналей из единиц и $(n - |L|)$ — из нулей.

Рассмотрим множество $\tilde{S}_n(L) \subseteq S_n(L)$ таких подстановок, что их разностные спецификации $(x_0, x_1, \dots, x_{n-1})$ удовлетворяют условию

$$L = \{k : x_k \neq 0, \quad 0 \leq k \leq n-1\}. \quad (1.21)$$

В соответствии с (1.6) и (1.7) такие разностные спецификации отвечают L -разбиениям в кольце вычетов по модулю n .

Подстановки $s \in \tilde{S}_n(L)$ будем называть L -полными. Для определения числа L -полных подстановок $|\tilde{S}_n(L)|$ применим метод включения-исключения. Для $L' \subseteq L$ обозначим через $A(L \setminus L')$ матрицу, полученную из $A(L)$ заменой единичных циклических диагоналей с номерами, образующими множество L' , нулевыми циклическими диагоналями с теми же номерами. В результате получаем

$$|\tilde{S}_n(L)| = \text{per } A(L) + \sum_{k=1}^{|L|-1} (-1)^k \sum_{\substack{L' : L' \subseteq L \\ |L'|=k}} \text{per } A(L \setminus L'). \quad (1.22)$$

Из этой формулы при $L = N_0 = \{0, 1, \dots, n-1\}$ следует известная формула для $M_n(0)$ — числа подстановок степени n , имеющих дефицит, равный нулю. Такие подстановки называются *полными*. Эту формулу можно записать в следующем виде [4]:

$$M_n(0) = n! + \sum_{k=1}^{n-1} (-1)^k \sum_{0 \leq j_1 < \dots < j_k \leq n-1} \text{per}(J - \tilde{C}^{-j_1} - \dots - \tilde{C}^{-j_k}), \quad (1.23)$$

где J — матрица $n \times n$, все элементы которой равны единице, и $\tilde{C}$ — подстановочная матрица, соответствующая подстановке $C(i) = i-1$, $i = 1, 2, \dots, n$.

В частности, если $L = \{i_1, i_2\}$, то из формулы (1.22) имеем

$$|\tilde{S}_n(\{i_1, i_2\})| = \text{per}(\tilde{C}^{-i_1} + \tilde{C}^{-i_2}) - 2. \quad (1.24)$$

Известно [5], что

$$\text{per}(\tilde{C}^{-i_1} + \tilde{C}^{-i_2}) = 2^{(i_1 - i_2, n)},$$

где $(i_1 - i_2, n)$ — общий наибольший делитель $(i_1 - i_2)$ и n , равный числу циклов подстановки $C^{i_1 - i_2}$. Поэтому из равенства (1.22) имеем

$$|\tilde{S}_n(\{i_1, i_2\})| = \begin{cases} 0, & (i_1 - i_2, n) = 1, \\ 2^{(i_1 - i_2, n)} - 2, & (i_1 - i_2, n) > 1. \end{cases} \quad (1.25)$$

Подстановки степени n , разностные спецификации которых удовлетворяют условию (1.19), будем называть L -подстановками. Число L -подстановок степени n определяется формулой (1.20). Обозначим через $S_{nr}(L)$ множество L -подстановок степени n , для разностных спецификаций которых выполнено условие

$$|\{k : x_k = 0, k \in L\}| = r, \quad r = 0, 1, \dots, |L| - 1. \quad (1.26)$$

Величину r будем называть L -дефицитом L -подстановки. Используя обозначения, введенные при выводе формулы (1.22), и применяя метод включения-исключения, получаем формулу для числа L -подстановок, для которых L -дефицит равен r :

$$|S_{nr}(L)| = \sum_{k=r}^{|L|-1} (-1)^{k-r} \binom{k}{r} \sum_{\substack{L' \subseteq L \\ |L'|=k}} \text{per } A(L \setminus L'), \quad r = 0, 1, \dots, |L| - 1. \quad (1.27)$$

При $L = N_0 = \{0, 1, \dots, n-1\}$ из формулы (1.27), используя те же обозначения, что в формуле (1.23), получаем известную формулу для числа подстановок $s \in S_n$, имеющих дефицит, равный r [4]:

$$M_n(r) = \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{\substack{0 \leq j_1 < \dots < j_k \leq n-1 \\ r = 0, 1, \dots, n-1}} \text{per}(J - \tilde{C}^{-j_1} - \dots - \tilde{C}^{-j_k}), \quad (1.28)$$

2. Производящие функции и формулы для числа разбиений в кольце вычетов

Обозначим через $a_{nl}(n, m)$ количество разбиений натурального числа r на l слагаемых, принимающих значения из множества $N_0 = \{0, 1, \dots, n-1\}$, среди которых имеется ровно m различных. Такие разбиения можно записать в следующем виде. Положим

$$\tilde{N} = \{k : l_k \neq 0, k \in N_0\}, \quad |\tilde{N}| = m. \quad (2.1)$$

Тогда разбиения удовлетворяют условиям

$$\sum_{k: k \in \tilde{N}} k l_k = r, \quad (2.2)$$

$$\sum_{k \in \bar{N}} l_k = l. \quad (2.3)$$

Производящая функция для чисел $a_{rl}(n, m)$

$$F_n(w, z, y) = 1 + \sum_{r=1}^{\infty} \sum_{l=1}^r \sum_{m=1}^n a_{rl}(n, m) w^r z^l y^m \quad (2.4)$$

может быть записана в виде произведения

$$F_n(w, z, y) = \prod_{j=0}^{n-1} \left(1 + y \sum_{l_j=1}^{\infty} w^{j l_j} z^{l_j} \right). \quad (2.5)$$

Эту производящую функцию при $n > 1$ можно представить в виде

$$F_n(w, z, y) = f_n(w, z, y) g_n(w, z), \quad (2.6)$$

где

$$f_n(w, z, y) = \prod_{j=1}^{n-1} (1 + (y-1)w^j z), \quad (2.7)$$

$$g_n(w, z) = \prod_{j=1}^{n-1} \frac{1}{1 - w^j z}. \quad (2.8)$$

Докажем две леммы, позволяющие находить коэффициенты при z^l из представлений (2.7) и (2.8) функций $f_n(w, z, y)$ и $g_n(w, z)$.

Лемма 1. Коэффициенты при z^l в производящей функции

$$f_n(w, z, y) = \sum_{l=0}^r A_{nl}(w, y) z^l \quad (2.9)$$

выражаются формулами

$$A_{n0}(w, y) = 1, \quad (2.10)$$

$$A_{nl}(w, y) = (y-1)^l w^{\binom{l}{2}} \frac{(1-w^n)(1-w^{n-1}) \dots (1-w^{n-l+1})}{(1-w)(1-w^2) \dots (1-w^l)}, \quad (2.11)$$

$$l = 1, 2, \dots, n-1,$$

$$A_{nn}(w, y) = (y-1)^n w^{\binom{n}{2}}. \quad (2.12)$$

Для доказательства леммы 1 из формулы (2.7) находим соотношение

$$[1 + (y-1)z] f_n(w, wz, y) = [1 + (y-1)w^n z] f_n(w, z, y).$$

Приравнивая коэффициенты при z^l в обеих частях равенства (2.12) с учетом формулы (2.9), получаем

$$A_{nl}(w, y) = (y-1) \frac{w^n - w^{l-1}}{w^l - 1} A_{n,l-1}(w, y), \quad l = 1, 2, \dots, n. \quad (2.13)$$

Применяя многократно соотношение (2.13) и проводя упрощения, получаем формулы (2.11) и (2.12). Формула (2.10) очевидна.

Коэффициенты Гаусса от переменной w определяются равенствами [6]

$$\left[\begin{matrix} n \\ l \end{matrix} \right]_w = \frac{(1-w^n)(1-w^{n-1})\dots(1-w^{n-l+1})}{(1-w^l)(1-w^{l-1})\dots(1-w)}, \quad l = 0, 1, \dots, n. \quad (2.14)$$

Индукцией по n нетрудно показать, что $\left[\begin{matrix} n \\ l \end{matrix} \right]_w$ является многочленом от w степени $l(n-l)$.

Из леммы 1 и формулы (2.14) имеем следствие.

Следствие 5. Коэффициенты $A_{nl}(w, y)$ в равенстве (2.9) выражаются через коэффициенты Гаусса с помощью равенства

$$A_{nl}(w, y) = (y-1)^l w^{\binom{l}{2}} \left[\begin{matrix} n \\ l \end{matrix} \right]_w, \quad l = 0, 1, \dots, n, \quad (2.15)$$

и являются многочленами от w степени $nl - \binom{l+1}{2}$.

Докажем теперь следующую лемму.

Лемма 2. Коэффициенты при z^l в разложении функции

$$g_n(w, z) = \sum_{l=0}^{\infty} B_{nl}(w) z^l \quad (2.16)$$

выражаются формулами

$$B_{n0} = 1, \quad (2.17)$$

$$B_{nl}(w) = \frac{(1-w^n)(1-w^{n+1})\dots(1-w^{n+l-1})}{(1-w)(1-w^2)\dots(1-w^l)}, \quad l = 1, 2, \dots, n-1, \quad (2.18)$$

$$B_{nn}(w) = \frac{(1-w^{n+1})(1-w^{n+2})\dots(1-w^{2n-1})}{(1-w)(1-w^2)\dots(1-w^{n-1})}. \quad (2.19)$$

Для доказательства используем соотношение

$$(1 - w^n z) g_n(w, wz) = (1 - z) g_n(w, z), \quad (2.20)$$

которое следует из равенства (2.8). Далее, используя равенство (2.16), преобразуем соотношение (2.20) и в полученном равенстве вычисляем коэффициенты при z^l , $l = 1, 2, \dots, n$. В результате получаем равенство

$$B_{nl}(w) = \frac{1 - w^{n+l-1}}{1 - w^l} B_{n,l-1}(w), \quad l = 1, 2, \dots, n. \quad (2.21)$$

Множественно применяя (2.21) и используя очевидное условие $B_{n0}(w) = 1$, получаем формулы (2.18) и (2.19).

Из леммы 2 и формулы (2.14) получаем следствие 6.

Следствие 6. Коэффициенты $B_{nl}(w)$ выражаются через коэффициенты Гаусса равенствами

$$B_{nl}(w) = \left[\begin{matrix} n+l-1 \\ l \end{matrix} \right]_w, \quad l = 0, 1, \dots, n, \quad (2.22)$$

и являются многочленами от w степени $l(n-1)$.

Из формул (2.6), (2.7), (2.9) и (2.16) имеем

$$\begin{aligned} F_n(w, z, y) &= \sum_{l=0}^{\infty} z^l \sum_{r=l}^{\infty} \sum_{m=0}^{\min(r,n)} a_{rl}(n, m) w^r y^m = \\ &= \sum_{l=0}^{\infty} z^l \sum_{s=0}^r A_{ns}(w, y) B_{n,r-s}(w). \end{aligned} \quad (2.23)$$

Отсюда, используя леммы 1 и 2 и следствия из них, можно вывести следующие равенства.

Следствие 7. Для производящих функций чисел $a_{rl}(n, m)$ справедливы следующие выражения через коэффициенты Гаусса:

$$\sum_{r=l}^{\infty} \sum_{m=1}^n a_{rl}(n, m) w^r y^m = \sum_{s=0}^{\min(r,n)} (y-1)^s w^{\binom{s}{2}} \left[\begin{matrix} n \\ s \end{matrix} \right]_w \left[\begin{matrix} n+l-s-1 \\ l-s \end{matrix} \right]_w, \quad (2.24)$$

$$\sum_{r=l}^{\infty} a_{rl}(n, m) w^r = \sum_{s=m}^{\min(r,n)} (-1)^{s-m} \binom{s}{m} w^{\binom{s}{2}} \left[\begin{matrix} n \\ s \end{matrix} \right]_w \left[\begin{matrix} n+l-s-1 \\ l-s \end{matrix} \right]_w. \quad (2.25)$$

Перейдем теперь к выводу формулы для производящей функции чисел C_{nm} разбиений n над кольцом вычетов по модулю n , имеющих m различных слагаемых. Для этого в формулах (2.2) и (2.3) полагаем

$$r = nt, \quad l = n, \quad t = 0, 1, \dots, n-1. \quad (2.26)$$

Теперь из второго выражения для производящей функции $F_n(w, z, y)$ имеем

$$C_n(y) = \sum_{m=1}^n C_{nm} y^m = \sum_{t=0}^{n-1} \text{coef}_{w^m} \sum_{s=0}^n A_{ns}(w, y) B_{n, n-s}(w). \quad (2.27)$$

Так как $A_{ns}(w, y)$ и $B_{n, n-s}(w)$ в соответствии с формулами (2.15), (2.17)–(2.19) — многочлены от w , то внутренняя сумма в (2.27) является многочленом от w степени $n(n-1)$. Поэтому для определения значений правой части (2.27) можно использовать известные свойства корней из единицы.

Если $\mathbb{C}$ — множество комплексных чисел и $\alpha \in \mathbb{C}$ — корень n -й степени из единицы, то

$$\sum_{\alpha \in \mathbb{C}: \alpha^n = 1} \alpha^r = \begin{cases} n, & \text{если } n \mid r, \\ 0, & \text{если } n \nmid r. \end{cases} \quad (2.28)$$

Используя это свойство, из равенства (2.27) получаем

$$C_n(y) = \frac{1}{n} \sum_{\alpha \in \mathbb{C}: \alpha^n = 1} \lim_{w \rightarrow \alpha} \left[A_{nn}(w, y) + B_{nn}(w) + \sum_{s=1}^{n-1} A_{ns}(w, y) B_{n, n-s}(w) \right]. \quad (2.29)$$

Если α — первообразный корень, то степени $\alpha^0, \alpha, \alpha^2, \dots, \alpha^{n-1}$ исчерпывают все корни n -й степени из единицы. Кроме того, α^k — первообразный корень тогда и только тогда, когда $(k, n) = 1$, т. е. число первообразных α^k , $1 \leq k \leq n$, равно значению функции Эйлера $\varphi(n)$. Перейдем теперь к вычислению пределов отдельных слагаемых в квадратных скобках в правой части равенства (2.29).

Лемма 3. Для любого натурального числа n имеет место равенство

$$\frac{1}{n} \sum_{\alpha \in \mathbb{C}: \alpha^n = 1} \lim_{w \rightarrow \alpha} A_{nn}(w, y) = \begin{cases} (y-1)^n, & n - \text{нечетное}, \\ 0, & n - \text{четное}. \end{cases} \quad (2.30)$$

Выберем в качестве первообразного корня из единицы $\alpha = e^{2\pi i/n}$. Тогда все корни из единицы имеют вид $e^{2\pi i k/n}$, $k = 0, 1, \dots, n-1$. Поэтому с учетом формулы (2.12) имеем

$$\begin{aligned} \frac{1}{n} \sum_{\alpha: \alpha^n=1} \lim_{w \rightarrow \alpha} A_{nn}(w, y) &= \frac{(y-1)^n}{n} \sum_{k=0}^{n-1} e^{\pi(n-1)ki} = \\ &= \frac{(y-1)^n}{n} \sum_{k=0}^{n-1} [\cos \pi(n-1)k + i \sin \pi(n-1)k]. \end{aligned} \quad (2.31)$$

Аргументы синусов и косинусов в квадратных скобках либо кратны π , либо равны нулю. При нечетном n аргумент $\cos \pi(n-1)k$ кратен 2π и каждое слагаемое в сумме равно единице. Если n четное, то сумма состоит из четного числа чередующихся слагаемых $+1$ и -1 и равна нулю.

Лемма 4. Для любого натурального числа n имеем

$$\frac{1}{n} \sum_{\alpha: \alpha^n=1} \lim_{w \rightarrow \alpha} B_{nn}(w) = \frac{1}{n} \sum_{d|n} \varphi(d) \left(\frac{2^{n/d} - 1}{n/d} \right). \quad (2.32)$$

Пусть α — корень n -й степени из единицы, являющийся первообразным корнем d -й степени из единицы. Тогда $d | n$ и число таких корней равно $\varphi(d)$. Формулу (2.19) запишем в виде

$$B_{nn}(w) = \prod_{r=1}^{n-1} \frac{1 - w^{n+r}}{1 - wr}. \quad (2.33)$$

Для членов произведения (2.33) имеем предельные выражения

$$\lim_{w \rightarrow \infty} \frac{1 - w^{n+r}}{1 - wr} = \begin{cases} \frac{n+r}{r}, & d | r, \\ 1, & d \nmid r. \end{cases} \quad (2.34)$$

Из равенств (2.33) и (2.34) получаем

$$\lim_{w \rightarrow \infty} B_{nn}(w) = \prod_{r=1}^{n-1} \frac{n+r}{r} = \prod_{\substack{i=1 \\ d|r}}^{n/d-1} \frac{n/d+i}{i} = \binom{2n/d-1}{n/d}. \quad (2.35)$$

Отсюда следует равенство (2.32).

Следствие 8. Для числа C_n , равного общему количеству разбиений над кольцом вычетов по модулю n , определяемых векторами $(x_0, x_1, \dots, x_{n-1})$ с условиями (1.4) и (1.5), справедлива формула

$$C_n = \sum_{d|n} \varphi(d) \binom{2n/d-1}{n/d}. \quad (2.36)$$

Из формул (2.6)–(2.8) и разложения (2.16) следует, что

$$g_n(w, z) = F_n(w, z, 1),$$

значит,

$$C_n = C_n(1) = \sum_{t=0}^{n-1} \text{coef}_{w^n} B_{nn}(w).$$

Таким образом,

$$C_n = \frac{1}{n} \sum_{\alpha: \alpha^n=1} \lim_{w \rightarrow \alpha} B_{nn}(w),$$

и формула (2.36) следует из равенства (2.32).

Отметим, что формула (2.36) впервые получена Риорданом [3].

Лемма 5. Если α — корень n -й степени из единицы, являющийся первообразным корнем d -й степени из единицы, то

$$\lim_{w \rightarrow \alpha} A_{ns}(y, w) = \begin{cases} (y-1)^s \binom{n/d}{s/d} (-1)^{s-s/d}, & d|s, \\ 0, & d \nmid s, \end{cases} \quad 1 \leq s \leq n-1. \quad (2.37)$$

Из формулы (2.11) имеем

$$A_{ns}(y, w) = (y-1)^s w^{\binom{s}{2}} \frac{1-w^n}{1-w^s} \prod_{r=1}^{s-1} \frac{1-w^{n-r}}{1-w^r}. \quad (2.38)$$

При $d \nmid s$ из равенства (2.38) следует, что

$$\lim_{w \rightarrow \alpha} A_{ns}(y, w) = \lim_{w \rightarrow \alpha} (y-1)^s \frac{1-w^n}{1-w^s} (-1)^{s-1} = 0. \quad (2.39)$$

Если $d \mid s$, то

$$\lim_{w \rightarrow \alpha} (y-1)^s w^{\binom{s}{2}} \frac{1-w^n}{1-w^s} \prod_{\substack{r=1 \\ r:d \nmid r}}^{s-1} \frac{1-w^{n-r}}{1-w^r} = (y-1)^s \alpha^{\binom{s}{2}} \binom{n/d}{s/d}, \quad (2.40)$$

и, кроме того,

$$\lim_{w \rightarrow \alpha} \prod_{\substack{r=1 \\ d \nmid r}}^{s-1} \frac{1-w^{n-r}}{1-w^r} = (-1)^{s-s/d} \alpha^{-\binom{s}{2}}. \quad (2.41)$$

Теперь первое из соотношений в (2.37) следует из равенств (2.38), (2.40) и (2.41), а второе — из (2.39).

Лемма 6. Если α — корень n -й степени из единицы, являющийся первообразным корнем d -й степени из единицы, то

$$\lim_{w \rightarrow \alpha} B_{n,n-s}(w) = \begin{cases} \binom{2n/d - s/d - 1}{n/d - s/d}, & d \mid s, \\ 0, & d \nmid s, \end{cases} \quad 1 \leq s \leq n-1. \quad (2.42)$$

Из равенства (2.18) следует, что

$$B_{ns}(w) = \frac{1-w^n}{1-w^{n-s}} \prod_{r=1}^{n-s-1} \frac{1-w^{n+r}}{1-w^r}. \quad (2.43)$$

Так как $d \mid n$, то при $d \mid s$ имеем

$$\begin{aligned} \lim_{w \rightarrow \alpha} \frac{1-w^n}{1-w^{n-s}} \prod_{r=1}^{n-s-1} \frac{1-w^{n+r}}{1-w^r} &= \frac{n/d}{n/d - s/d} \prod_{\substack{i=1 \\ r:d \nmid r}}^{\frac{n-s}{d}-1} \frac{(n/d + i)}{i} = \\ &= \binom{2n/d - s/d - 1}{n/d - s/d}. \end{aligned} \quad (2.44)$$

Кроме того,

$$\lim_{w \rightarrow \alpha} \prod_{\substack{r=1 \\ r:d \nmid r}}^{n-s-1} \frac{1-w^{n+r}}{1-w^r} = 1. \quad (2.45)$$

Теперь соотношения (2.42) следуют из формулы (2.43) и равенств (2.44) и (2.45). Из равенства (2.29) и доказанных лемм следует теорема 2.

Теорема 2. Для производящей функции $C_n(y) = \sum_{m=1}^n C_{nm} y^m$ справедлива формула

$$C_n(y) = \frac{1}{n} \sum_{d|n} \varphi(d) \sum_{j=0}^{n/d} (-1)^{dj-j} \binom{n/d}{j} \binom{2n/d-j-1}{n/d-j} (y-1)^{jd}, \quad (2.46)$$

$n = 1, 2, \dots$

Используя равенство (2.29) и леммы 3, 4, 5 и 6, получаем

$$C_n(y) = \frac{1}{n} \sum_{d|n} \varphi(d) [(y-1)^n \delta(n) - (-1)^{n-n/d} (y-1)^n + \\ + \sum_{j=0}^{n/d} (-1)^{jd-j} \binom{n/d}{j} \binom{2n/d-j-1}{n/d-j} (y-1)^{jd}], \quad (2.47)$$

где

$$\delta(n) = \begin{cases} 1, & n - \text{нечетное,} \\ 0, & n - \text{четное.} \end{cases} \quad (2.48)$$

Из равенства (2.27) следует, что $C_n(0) = 0$ для всех $n = 1, 2, \dots$. Кроме того, нетрудно убедиться, что

$$\sum_{j=0}^{n/d} (-1)^j \binom{n/d}{j} \binom{2n/d-j-1}{n/d-j} = 0. \quad (2.49)$$

Поэтому из равенства (2.47) при $y = 0$ с учетом соотношения (2.48) получаем соотношение

$$\sum_{d|n} (-1)^{n+n/d} \varphi(d) = \begin{cases} n, & n - \text{нечетное,} \\ 0, & n - \text{четное.} \end{cases} \quad (2.50)$$

В результате получено новое доказательство тождества (2.50), известного как тождество Радемахера. Другое доказательство этого тождества было дано Брауэром [2].

Используя равенство (2.49), формулу (2.46) можно записать в следующем виде:

$$C_n(y) = \sum_{m=1}^n C_{nm} y^m = \\ = \frac{1}{n} \sum_{d|n} \varphi(d) \sum_{j=1}^{n/d} (-1)^{dj-j} \binom{n/d}{j} \binom{2n/d-j-1}{n/d-j} [(y-1)^{dj} - (-1)^{dj}]. \quad (2.51)$$

Из равенства (2.51) получаем формулу для чисел C_{nm} :

$$C_{nm} = \frac{1}{n} \sum_{d|n} \varphi(d) \sum_{j:m/d \leq j \leq n/d} (-1)^{j+m} \binom{n/d}{j} \binom{2n/d - j - 1}{n/d - j} \binom{dj}{m}, \quad (2.52)$$

$$m = 1, 2, \dots, n.$$

Из формулы (2.52) с учетом тождества (2.50) получаем равенства из свойств 1 и 2:

$$C_{nn} = \frac{1}{n} \sum_{d|n} (-1)^{n+n/d} \varphi(d) = \begin{cases} 1, & n - \text{нечетное,} \\ 0, & n - \text{четное,} \end{cases} \quad (2.53)$$

$$C_{n,n-1} = n - \sum_{d|n} (-1)^{n+n/d} \varphi(d) = \begin{cases} n, & n - \text{четное,} \\ 0, & n - \text{нечетное.} \end{cases}$$

Если n — простое число, то формула для чисел C_{nm} значительно упрощается и имеет вид

$$C_{nm} = \frac{1}{n} \binom{n}{m} \left[\binom{n-1}{m-1} + (-1)^{m+1} (n-1) \right], \quad m = 1, 2, \dots, n. \quad (2.54)$$

Действительно, при n простом из формулы (2.52) имеем

$$C_{nm} = \frac{1}{n} \sum_{s=m}^n (-1)^{s-m} \binom{s}{m} \binom{n}{s} \binom{2n-s-1}{n-s} + \frac{n-1}{n} \binom{n}{m} (-1)^{m+1}.$$

Преобразуя правую часть последнего равенства, получаем

$$C_{nm} = \frac{1}{n} \binom{n}{m} \left[\sum_{s=0}^{n-m} (-1)^s \binom{n-m}{s} \binom{2n-m-s-1}{n-m-s} + (-1)^{m+1} (n-1) \right].$$

Из этого равенства, используя соотношение

$$\sum_{s=0}^{n-m} (-1)^s \binom{n-m}{s} \binom{2n-m-s-1}{n-m-s} = \binom{n-1}{m-1},$$

получаем формулу (2.54).

Из формулы (2.54) вытекает следствие.

Следствие 9. Для любого простого числа n условие $C_{nm} = 0$ выполнено тогда и только тогда, когда или $m = 2$, или $m = n - 1$.

В соответствии с формулой (2.54) $C_{nm} = 0$ тогда и только тогда, когда m является решением уравнения

$$\binom{n-1}{m-1} = (-1)^m (n-1).$$

Соответствующее следствие для подстановок формулируется следующим образом.

Следствие 9'. Подстановка s простой степени n , имеющая дефицит $\text{def}(s) = n - m$, $1 \leq m \leq n$, не существует тогда и только тогда, когда либо $m = 2$, либо $m = n - 1$.

Суммируя по m обе части равенства (2.54) для простого n , получаем формулу для $C_n = \sum_{m=1}^n C_{nm}$:

$$C_n = \frac{1}{n} \left[\binom{2n-1}{n-1} + (n-1) \right]. \quad (2.55)$$

3. Случайные разбиения в кольцах вычетов

В соответствии с данным в п. 2 определением отношения эквивалентности на множестве подстановок S_n каждому разбиению в кольце вычетов по модулю n ставится во взаимно однозначное соответствие содержащий его класс эквивалентности. Совокупности из C_{nm} таких разбиений отвечает совокупность классов эквивалентности подстановок, разностные характеристики которых содержат точно m различных координат. На множестве всех C_n разбиений в кольце вычетов по модулю n зададим равномерное вероятностное распределение и рассмотрим случайную величину ξ_n , равную числу различных слагаемых в случайном разбиении. В силу указанного соответствия ξ_n представляет также число различных координат разностных характеристик подстановок, принадлежащих случайно выбранному классу эквивалентности. Если η_n — значение дефицита подстановок в случайно выбранном классе эквивалентности, то $\eta_n = n - \xi_n$. Вероятностное распределение ξ_n имеет вид

$$P(\xi_n = m) = \frac{C_{nm}}{C_n}, \quad m = 1, 2, \dots, n, \quad (3.1)$$

где C_n и C_{nm} определяются формулами (2.36) и (2.52) соответственно. Производящая функция ξ_n записывается в виде

$$P_n(y) = \sum_{m=1}^n P(\xi_n = m) y^m = \frac{C_n(y)}{C_n},$$

где $C_n(y)$ выражается формулой (2.51). Из формулы (2.52) получаем выражение для распределения ξ_n :

$$P(\xi_n = m) = \frac{1}{C_n} \frac{1}{n} \sum_{d|n} \varphi(d) \sum_{j:m/d \leq j \leq n/d} (-1)^{j+m} \binom{n/d}{j} \binom{2n/d - j - 1}{n/d - j} \binom{dj}{m}, \quad (3.2)$$

$$m = 1, 2, \dots, n.$$

Если n — простое число, то распределение ξ_n в соответствии с формулами (2.54) и (2.55) выглядит следующим образом:

$$P(\xi_n = m) = \frac{\binom{n}{m} \left[\binom{n-1}{m-1} + (-1)^{m+1} (n-1) \right]}{\binom{2n-1}{n-1} + (n-1)}, \quad m = 1, 2, \dots, n. \quad (3.3)$$

Значения вероятностей в (3.3) для $m = 1, 2, n-1, n$ в соответствии с (2.53) имеют вид

$$P(\xi_n = 1) = \frac{n^2}{\binom{2n-1}{n-1} + (n-1)}, \quad P(\xi_n = n) = \frac{n}{\binom{2n-1}{n-1} + (n-1)}, \quad (3.4)$$

$$P(\xi_n = 2) = P(\xi_n = n-1) = 0.$$

Для простого n при $n \rightarrow \infty$ распределения случайных величин ξ_n и $\eta_n = n - \xi_n$ на отрезке $[3, n-2]$ аппроксимируются гипергеометрическим распределением.

Теорема 3. Для простого n при $n \rightarrow \infty$ равномерно для всех $3 \leq m \leq n-2$

$$P(\xi_n = m) = \frac{\binom{n}{m} \binom{n-1}{m-1}}{\binom{2n-1}{n-1}} \left(1 + O\left(\frac{1}{n}\right) \right), \quad (3.5)$$

$$\mathbf{P}(\eta_n = m) = \frac{\binom{n-1}{m} \binom{n}{m}}{\binom{2n-1}{n-1}} \left(1 + O\left(\frac{1}{n}\right) \right). \quad (3.6)$$

Доказательство теоремы непосредственно следует из формулы (3.3) для точного распределения ξ_n . Используя формулы (3.3), нетрудно получить точные выражения для первых двух моментов и дисперсии случайных величин ξ_n и η_n , а затем найти их асимптотические представления при $n \rightarrow \infty$. Однако формулы (3.4) – (3.6) позволяют получить такие представления непосредственно.

Следствие 10. Для простого n при $n \rightarrow \infty$ асимптотические представления для средних и дисперсий случайных величин ξ_n и η_n имеют вид

$$\begin{aligned} \mathbf{M}\xi_n &= \frac{n^2}{2n-1}(1+o(1)), \quad \mathbf{D}\xi_n = \frac{n^2(n-1)}{2(2n-1)^2}(1+o(1)), \\ \mathbf{M}\eta_n &= \frac{n(n-1)}{2n-1}(1+o(1)), \quad \mathbf{D}\eta_n = \frac{n^2(n-1)}{2(2n-1)^2}(1+o(1)). \end{aligned} \quad (3.7)$$

Формулы (3.6) следуют из выражений для распределений ξ_n и η_n вида (3.5), (3.6) и формул (3.4). Для средних и дисперсий случайных величин ξ_n и η_n для простого n , $n \rightarrow \infty$ из формул (3.7) следуют упрощенные асимптотики соответственно вида

$$\frac{n}{2}(1+o(1)), \quad \frac{n}{8}(1+o(1)).$$

Для случайных величин

$$\xi'_n = \frac{\left(\xi_n - \frac{n}{2}\right)}{\sqrt{\frac{n}{8}}}, \quad \eta'_n = \frac{\left(\eta_n - \frac{n}{2}\right)}{\sqrt{\frac{n}{8}}}$$

справедлива следующая теорема.

Теорема 4. Для простого n при $n \rightarrow \infty$ равномерно для всех допустимых значений $w = o(n^{1/6})$ имеем асимптотические представления

$$\mathbf{P}(\xi'_n = w) = \frac{2}{\sqrt{\pi n}} e^{-w^2/2} (1+o(1)), \quad (3.8)$$

$$\mathbf{P}(\eta'_n = w) = \frac{2}{\sqrt{\pi n}} e^{-w^2/2} (1+o(1)). \quad (3.9)$$

Теорема доказывается с использованием формул (3.5) и (3.6) и стандартного применения формулы Стирлинга.

Так, из формулы (3.6) при $n, m \rightarrow \infty$ имеем

$$\mathbf{P}(\eta_n = m) = n^{4n} \left[\sqrt{2\pi} (2n)^{2n-\frac{1}{2}} m^{2m+1} (n-m)^{2(n-m)} \right]^{-1} (1+o(1)). \quad (3.10)$$

При выполнении условий теоремы 4 получаем

$$m^{2m+1} = \left(\frac{n}{2}\right)^{n+w\sqrt{n/2}+1} \exp \left[w\sqrt{n/2} + \frac{w^2}{4} + O\left(\frac{w^3}{\sqrt{n}}\right) \right],$$

$$(n-m)^{2(n-m)} = \left(\frac{n}{2}\right)^{n-w\sqrt{n/2}} \exp \left[-w\sqrt{n/2} + \frac{w^2}{4} + O\left(\frac{w^3}{\sqrt{n}}\right) \right].$$

Подставляя эти выражения в правую часть равенства (3.10), после некоторых упрощений получаем формулу (3.9). Аналогично доказывается формула (3.8).

Список литературы

1. *Hall M. A combinatorial problem on abelian groups* // Proc. Amer. Soc. — 1952. — V. 3. No 4. — P. 584–587.
2. *Brauer A., Brauer R., Hopf H. Über die Irreduzibilität einiger spezieller Klassen von Polynomen* // Jber. Deutsch. Math.-Verein. — 1926. — V. 35. — P. 99–112.
3. *Riordan J. Enumerations for permutations in difference form* // Proc. Amer. Math. Soc. — 1962. — V. 13. No 1. — P. 107–110.
4. *Сачков В. Н. Цепи Маркова итерационных систем преобразований* // В сб.: Труды по дискретной математике, т. 6. — М.: Физматлит, 2002. — 165–183.
5. *Сачков В. Н. Комбинаторные методы дискретной математики.* — М.: Наука, 1977.