Math-Net.Ru

Общероссийский математический портал

В. Е. Викторенков, Цикловая структура случайных подстановок на множестве двухцветных элементов. I, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 3, 9–32

DOI: <https://doi.org/10.4213/mvk297>

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: 18.234.156.22

26 апреля 2023 г., 10:31:35

Цикловая структура случайных подстановок на множестве двухцветных элементов. I

В. Е. Викторенков

Академия криптографии Российской Федерации, Москва

Получено 29.IV.2019

Аннотация. Рассматриваются случайные равновероятные подстановки на множестве, элементы которого раскрашены в два цвета. Мощность множества одного цвета является произвольной функцией степени подстановки. В этой первой части статьи приведены утверждения о характеристиках одноцветных циклов. Результаты могут использоваться при изучении цикловой структуры полиномиальных преобразований некоторых типов конечных колец.

Ключевые слова: равновероятные подстановки, оператор редуцирования, одноцветные циклы, предельные теоремы

Cycle structure of random permutations on the set of two-color elements. I

V. E. Viktorenkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Random equiprobable permutations on the set of elements marked by two colors are considered. The cardinality of the set of elements of one color is an arbitrary function of the permutation order. This first part of the paper contains statements on the characteristics of one-color cycles. Results may be used in the study of the cycle structure of polynomial transforms acting on finite rings of some types.

Keywords: equiprobable permutations, reduction operator, one-color cycles, limit theorems

1. Введение. Производящие функции

Пусть $N = \{1, \dots, n\}$ и $N = X_1 \cup X_2$ — разбиение на собственные подмножества, $|X_1| = m$, $|X_2| = n - m$, $1 \leq m$, $n - m \leq n - 1$, например, для определенности $X_1 = \{1, \dots, m\}$ и $X_2 = \{m + 1, \dots, n\}$. В этом случае будем считать, что элементы множества N раскрашены в два цвета (нумерация цветов соответствует нумерации множеств X_i , $i = 1, 2$).

Рассмотрим разложение произвольной подстановки σ_n , действующей на множестве N , в произведение независимых циклов. Это множество циклов разобьем на три класса: $C_{n,m}^{(i)}$ — множество циклов, состоящих только из элементов i -го цвета, $i = 1, 2$, и $C_{n,m}^{(1 \oplus 2)}$ — множество 2-цветных циклов. Исходную модель подстановок, отвечающую отсутствию раскраски, т. е. случаю $n = m$, будем называть *классической*.

Предлагаемая 2-цветная модель позволяет наиболее полно описать схему действия *оператора редуцирования* подстановок, который был введен В. Н. Сачковым. Основные результаты для этого оператора он получил в 1971 г. Их уточнению и развитию посвящен цикл работ [2–5]. Для полноты изложения дадим определение этого понятия. *Оператор редуцирования* $R(X_2)$ является сжимающим отображением симметрической группы подстановок в симметрическую группу меньшей степени $R(X_2)$: $S_n \rightarrow S_m$. Его действие на подстановку $\sigma_n \in S_n$ состоит в разложении σ_n в произведение независимых циклов с последующим удалением элементов множества X_2 из циклов. В результате получается редуцированная подстановка, действующая на множестве X_1 . В указанных работах изучались комбинаторно-вероятностные и некоторые алгебраические свойства таких преобразований, представляющих интерес для криптографии. В терминах оператора редуцирования класс $C_{n,m}^{(1)}$ можно трактовать как множество неповрежденных циклов (см. [4]). Отсылки к конкретным результатам этих работ будут даны по ходу изложения материала в разделе 2.

Связь 2-цветной схемы с вероятностно-комбинаторной моделью неполных подстановок будет прокомментирована сразу после замечания 1.4.

В данной работе будут уточнены и дополнены результаты об одноцветных циклах. Отметим, что все эти результаты получены с единых позиций с помощью производящих функций (в работах В. Н. Сачкова использовался метод прямого комбинаторного построения).

Двухцветные циклы предполагается рассмотреть в следующей работе. Кроме того, исследование таких (2-цветных) циклов позволит

с вероятностно-комбинаторных позиций описывать асимптотическое поведение некоторых характеристик цикловой структуры полиномиальных преобразований конечного коммутативного локального кольца главных идеалов. Предварительные результаты в этом направлении приведены в работах [11–13]. Алгебраическим аспектам проблематики полиномиальных преобразований и их применению в криптографии (для различных типов конечных коммутативных колец) посвящено значительное число публикаций (см., например, работы [10, 14–18, 21] и приведенные в них обзоры).

Дадим определения основных понятий.

Цикл длины $i + j$, в котором имеется i элементов 1-го цвета и j элементов 2-го, будем называть (i, j) -циклом, где $0 \leq i \leq m$, $0 \leq j \leq n - m$ и $i + j > 0$. Пусть в подстановке σ_n число (i, j) -циклов равно $k_{i,j}$. В этом случае будем говорить, что подстановка принадлежит (2-цветному) цикловому классу

$$\{(i, j)^{k_{i,j}}\} = \{(i, j)^{k_{i,j}}, 0 \leq i \leq m, 0 \leq j \leq n - m, i + j > 0\}.$$

Сам набор частот $\bar{k} = \bar{k}(n, m) = (k_{i,j}, 0 \leq i \leq m, 0 \leq j \leq n - m, i + j > 0)$ будем называть цикловой структурой подстановки σ_n в 2-цветной схеме/модели. Элементы цикловой структуры удовлетворяют условиям

$$\sum_{j=0}^{n-m} \sum_{i=1}^m i \cdot k_{i,j} = m, \quad \sum_{i=0}^m \sum_{j=1}^{n-m} j \cdot k_{i,j} = n - m. \quad (1.1)$$

Напомним, что в классической схеме число подстановок в цикловом классе $\{1^{k_1}, \dots, n^{k_n}\}$ согласно формуле Кэли равно

$$S_n(\bar{k}) = n! / \prod_{i=1}^n k_i! i^{k_i}. \quad (1.2)$$

Простым комбинаторным построением аналогично показывается, что в 2-цветной модели число подстановок в цикловом классе $\{(i, j)^{k_{i,j}}\}$ равно

$$S_{n,m}(\bar{k}) = m! (n - m)! \prod_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n-m, \\ i+j>0}} \frac{1}{k_{i,j}!} \left(\frac{1}{i+j} \binom{i+j}{i} \right)^{k_{i,j}}. \quad (1.3)$$

При $n = m$ формулы (1.2) и (1.3) совпадают. Поэтому $S_{n,0}(\bar{k}) = S_{n,n}(\bar{k}) = S_n(\bar{k})$. Для определенности будем считать $S_{0,0}(\bar{0}) = 1$. Для чисел подстановок $S_{n,m}(\bar{k})$ рассмотрим 2-мерную экспоненциальную производящую функцию от бесконечного числа переменных $t_1, t_2, u_{i,j}$, $i + j \geq 1$,

$$\mathcal{F}(t_1, t_2; \bar{u}) = 1 + \sum_{\substack{m, n-m \geq 0 \\ n > 0}} \frac{t_1^m t_2^{n-m}}{m!(n-m)!} \sum_{\bar{k}} S_{n,m}(\bar{k}) \prod_{i,j} u_{i,j}^{k_{i,j}}, \quad (1.4)$$

где второе суммирование проводится по всем возможным значениям цикловой структуры $\bar{k} = \bar{k}(n, m)$ с условием (1.1), а область изменения параметров i, j в произведении определена в (1.3).

Лемма 1.1. *Справедливо представление*

$$\mathcal{F}(t_1, t_2; \bar{u}) = \exp \left\{ \sum_{\substack{i+j \geq 1 \\ i,j \geq 0}} \frac{1}{i+j} \binom{i+j}{i} u_{i,j} t_1^i t_2^j \right\}. \quad (1.5)$$

Формула (1.5) вытекает из общих свойств экспоненциальных производящих функций:

$$\begin{aligned} \exp \left\{ \sum_{\substack{i+j \geq 1 \\ i,j \geq 0}} a_{i,j} t_1^i t_2^j \right\} &= \prod_{\substack{i+j \geq 1 \\ i,j \geq 0}} \sum_{k_{i,j} \geq 0} \frac{1}{k_{i,j}!} (a_{i,j} t_1^i t_2^j)^{k_{i,j}} = \\ &= 1 + \sum_{\substack{n_1, n_2 \geq 0 \\ n_1 + n_2 \geq 1}} \frac{t_1^{n_1} t_2^{n_2}}{n_1! n_2!} \sum \left(n_1! n_2! \prod_{i,j} \frac{1}{k_{i,j}!} a_{i,j}^{k_{i,j}} \right), \end{aligned}$$

где второе суммирование проводится по всем таким наборам целочисленных неотрицательных значений $k_{i,j}$, $i, j \geq 0$, $i + j \geq 1$, что

$$\sum_{i=1}^{n_1} \sum_{j=0}^{n_2} i \cdot k_{i,j} = n_1,$$

а произведение — по $i, j \geq 0$, $i + j \geq 1$.

Пусть теперь все $n!$ подстановок множества N равновероятны. Определим базовые случайные величины: $\xi_{s,r} = \xi_{s,r}(n, m)$ — число (s, r) -циклов, где $0 \leq s \leq m$, $0 \leq r \leq n - m$, $s + r \geq 1$.

Чтобы подчеркнуть принадлежность циклов определенным классам при $s, r \geq 1$, будем использовать сокращенные обозначения

$$\xi_s^{(1)} = \xi_s^{(1)}(n, m) = \xi_{s,0}(n, m), \quad \xi_r^{(2)} = \xi_r^{(2)}(n, m) = \xi_{0,r}(n, m),$$

$$\xi_{s,r}^{(1\circ 2)} = \xi_{s,r}^{(1\circ 2)}(n, m) = \xi_{s,r}(n, m),$$

т. е. $\xi_s^{(i)}$ — число s -циклов, состоящих только из элементов i -го цвета, $i = 1, 2$, где $1 \leq s \leq m$ при $i = 1$ и $1 \leq s \leq n - m$ при $i = 2$; $\xi_{s,r}^{(1\circ 2)}$ — число 2-цветных (s, r) -циклов из класса $C_{n,m}^{(1\circ 2)}$, $1 \leq s \leq m$, $1 \leq r \leq n - m$.

Определим интегральные характеристики 2-цветной схемы (они стандартно выражаются через базовые случайные величины $\xi_{s,r}(n, m)$):

$$\xi^{(i)} = \xi^{(i)}(n, m) — \text{общее число циклов в классах } C_{n,m}^{(i)}, i = 1, 2,$$

$$\xi^{(1\circ 2)} = \xi^{(1\circ 2)}(n, m) — \text{число 2-цветных циклов,}$$

объемы циклов в классах обозначим через

$$\begin{aligned} \varkappa^{(1)} = \varkappa^{(1)}(n, m) &= \sum_{s=1}^m s \cdot \xi_s^{(1)}, \quad \varkappa^{(2)} = \varkappa^{(2)}(n, m) = \sum_{r=1}^{n-m} r \cdot \xi_r^{(2)}, \\ \varkappa^{(1\circ 2)} &= n - \varkappa^{(1)} - \varkappa^{(2)}. \end{aligned}$$

Пусть $S_1 \subseteq \{1, \dots, m\}$ и $S_2 \subseteq \{1, \dots, n - m\}$. Случайные величины

$$\begin{aligned} \xi_{S_i}^{(i)} &= \sum_{s \in S_i} \xi_s^{(i)}(n, m), \quad i = 1, 2, \\ \xi_{S_1, S_2}^{(1\circ 2)} &= \sum_{s \in S_1, s' \in S_2} \xi_{s, s'}^{(1\circ 2)}(n, m) \end{aligned}$$

в соответствии со сложившейся терминологией будем называть *сечениями*.

Производящая функция совместного распределения всех случайных величин $\xi_{s,r}(n, m)$ согласно (1.5) равна

$$\begin{aligned} P_{n,m}(u_{s,r}; s + r \geq 1) &= \sum_{\bar{k}} \mathbf{P}(\xi_{s,r} = k_{s,r}; s + r \geq 1) \prod_{s,r} u_{s,r}^{k_{s,r}} = \\ &= \binom{n}{m}^{-1} \text{Coef}_{t_1^m t_2^{n-m}} \mathcal{F}(t_1, t_2; \bar{u}). \end{aligned} \quad (1.6)$$

Производящие функции распределения остальных характеристик получаются из нее соответствующей конкретизацией переменных $\bar{u}$.

Сначала рассмотрим одно общее свойство независимости целого класса характеристик цикловой структуры в 2-цветной модели.

Из общей производящей функции (1.6) выделим производящую функцию распределения цикловой структуры класса $C_{n,m}^{(1)}$ (по составу длин циклов из элементов только 1-го цвета)

$$P_{n,m}^{(1)}(x_1, x_2, \dots, x_m) = \sum \mathbf{P} \left(\xi_1^{(1)}(n, m) = k_1, \dots, \xi_m^{(1)}(n, m) = k_m \right) \times \\ \times x_1^{k_1} \dots x_m^{k_m} = P_{n,m} \left(u_{i,j} : i = \overline{0, m}, j = \overline{0, n-m}, \right. \\ \left. 1 \leq i + j \leq n \right) \Big| \begin{cases} u_{i,0} = x_i, i = \overline{1, m}, \\ u_{i,j} = 1, i = \overline{0, m}, j = \overline{1, n-m}, \end{cases}$$

где суммирование проводится по всем таким целочисленным неотрицательным наборам $k_1, \dots, k_m$, что $k_1 + 2k_2 + \dots + m \cdot k_m \leq m$.

Для циклов, состоящих только из элементов 2-го цвета, аналогичная производящая функция $P_{n,m}^{(2)}(x_1, x_2, \dots, x_{n-m})$, очевидно, совпадает с производящей функцией $P_{n,n-m}^{(1)}(x_1, x_2, \dots, x_{n-m})$.

Для объединения классов $C_{n,m}^{(2)} \cup C_{n,m}^{(1 \circ 2)}$ (в нем каждый цикл содержит элемент 2-го цвета) определим дополнительный набор случайных величин $\bar{\zeta}(n, m) = \{\zeta_i(n, m), i = \overline{1, n-m}\}$, где $\zeta_i(n, m)$ равна числу циклов в случайной равновероятной подстановке, содержащих i элементов второго цвета. Тогда

$$\zeta_i(n, m) = \sum_{s=0}^m \xi_{s,i}(n, m), \quad i = \overline{1, n-m},$$

и

$$\sum_{i=1}^{n-m} i \cdot \zeta_i(n, m) = n - m.$$

Рассмотрим производящую функцию совместного распределения компонент в наборе $\bar{\zeta}(n, m)$

$$\tilde{P}_{n,m}^{(2)}(y_1, y_2, \dots, y_{n-m}) = \\ = \sum \mathbf{P}(\zeta_1(n, m) = k_1, \dots, \zeta_{n-m}(n, m) = k_{n-m}) y_1^{k_1} \dots y_{n-m}^{k_{n-m}},$$

где суммирование проводится по всем целочисленным неотрицательным наборам $k_1, \dots, k_{n-m}$ с условием $k_1 + 2k_2 + \dots + (n-m)k_{n-m} = n-m$.

Через $\tilde{P}_{n,m}(x_1, x_2, \dots, x_m; y_1, y_2, \dots, y_{n-m})$ обозначим производящую функцию совместного распределения обоих наборов $\bar{\xi}^{(1)}(n, m) = \{\xi_1^{(1)}(n, m), \dots, \xi_m^{(1)}(n, m)\}$ и $\bar{\zeta}(n, m)$.

Напомним, что в классической схеме производящая функция совместного распределения цикловой структуры выражается через цикловой индикатор

$$\frac{C_n(x_1, x_2, \dots, x_n)}{n!} = \text{Coef}_{f^n} \exp \left\{ \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right\}.$$

Теорема 1.2. Два набора $\bar{\xi}^{(1)}(n, m)$ и $\bar{\zeta}(n, m)$ являются независимыми, т. е.

$$\begin{aligned} \tilde{P}_{n,m}(x_1, x_2, \dots, x_m; y_1, y_2, \dots, y_{n-m}) = \\ = P_{n,m}^{(1)}(x_1, x_2, \dots, x_m) \cdot \tilde{P}_{n,m}^{(2)}(y_1, y_2, \dots, y_{n-m}), \end{aligned}$$

причем

$$\tilde{P}_{n,m}^{(2)}(y_1, y_2, \dots, y_{n-m}) = \frac{C_{n-m}(y_1, y_2, \dots, y_{n-m})}{(n-m)!},$$

а производящая функция

$$P_{n,m}^{(1)}(x_1, x_2, \dots, x_m) = \sum_{k=0}^m \frac{C_k(x_1, x_2, \dots, x_k)}{k!} \cdot \frac{(n-m)(m)_k}{(n)_{k+1}}$$

соответствует смеси распределений со смешивающим распределением по суммарному числу элементов в циклах из класса $C_{n,m}^{(1)}$, т. е.

$$\mathbf{P}(\varkappa^{(1)}(n, m) = k) = \frac{n-m}{n} \cdot \frac{(m)_k}{(n-1)_k}, \quad k = 0, 1, \dots, m.$$

Доказательство. Для получения производящей функции совместного распределения случайных величин $\xi_1^{(1)}(n, m), \dots, \xi_m^{(1)}(n, m)$ и $\zeta_1(n, m), \dots, \zeta_{n-m}(n, m)$ достаточно в базовой экспоненциальной производящей функции (1.5) конкретизировать переменные

$$u_{i,o} = x_i z^i, \quad i = 1, 2, \dots, u_{i,j} = y_j, \quad i = 0, 1, \dots, j = 1, 2, \dots,$$

где дополнительная переменная z учитывает распределение случайной величины $\varkappa^{(1)}(n, m)$. Тогда

$$\begin{aligned} \tilde{P}_{n,m}(x_1 z, x_2 z^2, \dots, x_m z^m; y_1, y_2, \dots, y_{n-m}) = \\ = \binom{n}{m}^{-1} \text{Coef}_{t_1^m t_2^{n-m}} \exp \left\{ \sum_{i=1}^{\infty} \frac{x_i z^i}{i} t_1^i + \sum_{s=1}^{\infty} \frac{1}{s} \sum_{\ell=1}^s \binom{s}{\ell} y_{\ell} t_1^{s-\ell} t_2^{\ell} \right\}. \end{aligned}$$

Упростим сумму по s :

$$\sum_{s=1}^{\infty} \frac{1}{s} \sum_{\ell=1}^s \binom{s}{\ell} y_{\ell} t_1^{s-\ell} t_2^{\ell} = \sum_{\ell=1}^{\infty} y_{\ell} \frac{t_2^{\ell}}{\ell} \sum_{s=\ell}^{\infty} \binom{s-1}{s-\ell} t_1^{s-\ell} = \sum_{\ell=1}^{\infty} y_{\ell} \frac{t_2^{\ell}}{\ell} (1-t_1)^{-\ell}.$$

Следовательно,

$$\begin{aligned} \tilde{P}_{n,m}(x_1 z, x_2 z^2, \dots, x_m z^m; y_1, y_2, \dots, y_{n-m}) &= \\ &= \frac{C_{n-m}(y_1, y_2, \dots, y_{n-m})}{(n-m)!} \binom{n}{m}^{-1} \text{Coef}_{t_1^m} \frac{1}{(1-t_1)^{n-m}} \exp \left\{ \sum_{i=1}^{\infty} \frac{x_i z^i}{i} t_1^i \right\} = \\ &= \frac{C_{n-m}(y_1, y_2, \dots, y_{n-m})}{(n-m)!} \sum_{k=0}^m z^k \frac{C_k(x_1, x_2, \dots, x_k)}{k!} \cdot \binom{n-k-1}{n-m-1} \binom{n}{m}^{-1}, \end{aligned}$$

так как $C_k(x_1 z, x_2 z^2, \dots, x_k z^k) = z^k C_k(x_1, x_2, \dots, x_k)$. Отсюда при $x_1 = x_2 = \dots = x_m = 1$ в силу $C_k(1, \dots, 1) = k!$ заключаем, что

$$\binom{n-k-1}{n-m-1} \binom{n}{m}^{-1} = \frac{n-m}{n} \cdot \frac{(m)_k}{(n-1)_k} = \mathbf{P}(\mathfrak{X}^{(1)}(n, m) = k).$$

Теорема доказана.

Прокомментируем утверждение теоремы 1.2.

Распределение случайных величин $\zeta_1(n, m), \dots, \zeta_{n-m}(n, m)$ сведено к распределению цикловой структуры случайной равновероятной подстановки степени $n - m$. Поэтому на нем особо останавливаться не будем. Отметим лишь один факт. Производящая функция распределения суммарного числа циклов $\xi^{(2)}(n, m) + \xi^{(1 \circ 2)}(n, m)$ (содержащих элементы 2-го цвета) в объединении $C_{n,m}^{(2)} \cup C_{n,m}^{(1 \circ 2)}$ получается из производящей функции $\tilde{P}_{n,m}^{(2)}(y_1, y_2, \dots, y_{n-m})$ при $y_1, y_2, \dots, y_{n-m} = y$, т. е. она имеет вид $\binom{y+n-m-1}{n-m}$. Поэтому из теоремы 1.2 вытекает следующий результат.

Следствие 1.3. *Распределение цикловой структуры в классе $C_{n,m}^{(1)}$ (циклы из элементов только 1-го цвета) не зависит от распределения общего числа остальных циклов $\xi^{(2)}(n, m) + \xi^{(1 \circ 2)}(n, m)$.*

Замечание 1.4. Теорему 1.2 можно наглядно сформулировать в терминах оператора редуцирования. Согласно [2] множество операторов редуцирования $R(X)$, $X \subseteq N$, образует коммутативную полугруппу идемпотентов по умножению. Данная полугруппа изоморфна полугруппе всех подмножеств 2^N с операцией объединения. Напомним, что два идемпотента называются *ортогональными*, если их произведение равно нулю (в нашем случае последовательное применение таких операторов к подстановке приводит к пустому множеству циклов). Пусть

выбраны некоторые подмножества $X, Y \subseteq \{1, \dots, n\}$, $|X| = n_1$, $|Y| = n_2$, и $\sigma_{n_1}(X)$ — подстановка степени n_1 на множестве X , а $\sigma_{n_2}(X)$ — на множестве Y . Определим пересечение подстановок $\sigma_{n_1}(X) \cap \sigma_{n_2}(Y)$ как произведение только их общих циклов (при разложении в произведение на независимые циклы). Результирующая подстановка (в случае ее невырожденности) действует на некотором подмножестве множества $X \cap Y$. Тогда для случайной и равновероятной подстановки σ_n степени n и ортогонального идемпотента $R(\bar{X})$, где дополнение $\bar{X} = \{1, \dots, n\} \setminus X$, $X \subseteq \{1, \dots, n\}$, согласно теореме 1.2 случайные величины

$$\sigma_n \cap R(X)\sigma_n \text{ и } R(\bar{X})\sigma_n$$

являются независимыми (подстановка $\sigma_n \cap R(X)\sigma_n$ состоит только из неповрежденных циклов).

Прокомментируем утверждение теоремы 1.2 применительно к неполным подстановкам. Такие подстановки возникают в результате удаления некоторых m ребер в орграфе подстановки степени n (m переходов в неполной подстановке не определены). В этом случае орграф неполной подстановки имеет компоненты связности двух типов: циклы и цепочки (фрагменты разорванных циклов). Такую схему исследовали В.Е. Степанов (1965), А.Н. Трунов (1981) и С.П. Черкашин (1981). Для схемы Эванса соответствующие обобщения получены Г.И. Ивченко и Ю.И. Медведевым (см. [8] или обзорную главу 7 справочника [9]). Цикловая структура только циклов (биективная составляющая неполной подстановки) описывается с помощью экспоненциальной многомерной производящей функции [8, формула (18)] (обозначения приведены в соответствие с нашими)

$$\binom{n}{m}^{-1} \text{Coef}_{t^m} \frac{1}{(1-t)^{n-m}} \exp \left\{ \sum_{i=1}^{\infty} \frac{x_i}{i} t^i \right\},$$

которая в силу теоремы 1.2 совпадает с $P_{n,m}^{(1)}(x_1, x_2, \dots, x_m)$. Таким образом, данные фрагменты цикловых структур в двух моделях случайных подстановок полностью идентичны.

В заключение этого раздела кратко остановимся на обобщении полученной производящей функции на многомерный случай. Пусть задано некоторое разбиение $\{1, \dots, n\} = X_1 \cup \dots \cup X_\ell$, $\ell \geq 2$, и $|X_1| = m_1, \dots, |X_\ell| = m_\ell = n - m_1 - \dots - m_{\ell-1}$, т. е. элементы множества $\{1, \dots, n\}$ раскрашены в ℓ цветов. Повторяя, фактически дословно,

приведенные выше комбинаторные построения, убеждаемся в том, что многомерному случаю соответствует производящая функция

$$\mathcal{F}(t_1, \dots, t_\ell; \bar{u}) = \exp \left\{ \sum_{i=1}^{\infty} \frac{1}{i} \sum_{i_1 + \dots + i_\ell = i} \binom{i}{i_1, \dots, i_\ell} u_{i_1, \dots, i_\ell} t_1^{i_1} \cdot \dots \cdot t_\ell^{i_\ell} \right\},$$

где переменная $u_{i_1, \dots, i_\ell}$ отвечает перечислению i -циклов, $i = i_1 + \dots + i_\ell$, каждый из которых содержит i_s элементов s -го цвета, $s = \overline{1, \ell}$. Для получения производящей функции распределения соответствующей характеристики в ℓ -цветной цикловой структуре необходимо, как и в 2-мерном случае, конкретизировать переменные $u_{i_1, \dots, i_\ell}$ и от полученного выражения взять значение

$$\binom{n}{m_1, \dots, m_\ell}^{-1} \text{coef}_{t_1^{m_1} \dots t_\ell^{m_\ell}}.$$

Для криптографической модели оператора редуцирования разбиение $\{1, \dots, n\} = X_1 \cup \dots \cup X_\ell$ возникает, если рассматривать несколько последовательных тактов работы шифратора (некоторые аспекты математической модели таких схем колонной замены см. в [2]).

Применительно к полиномиальным преобразованиям кольца природа разложения $X_1 \cup \dots \cup X_\ell$ будет пояснена в следующей работе.

2. Предельные распределения

Всюду далее при $n \rightarrow \infty$ с точностью до переобозначения цветов полагаем

$$m/n \rightarrow p, \quad 0 \neq p \leq 1.$$

Общее число циклов $\xi^{(i)}$ и число s -циклов фиксированной длины $\xi_s^{(i)}$ $i = 1, 2$, различными методами исследованы полностью (см. обзорную главу 7 справочника [9]). Приведем некоторые уточнения и дополнения. Прокомментируем асимптотическую нормальность случайной величины $\xi^{(1)}$. Производящая функция ее распределения равна

$$\binom{x+n-1}{m} \binom{n}{m}^{-1} = \frac{(x+n-1)_m}{(n)_m}.$$

Данная функция имеет только отрицательные корни, т. е. $\xi^{(1)}$ представляется в виде суммы независимых случайных величин с распределениями Бернулли с вероятностями успехов $p_1 = 1/n, \dots, p_m =$

$1/(n-m+1)$. Поэтому использование методов из работы [19] стандартно приводит к справедливости как интегрального, так и локального варианта центральной предельной теоремы с оценкой скорости сходимости.

Теорема 2.1. Пусть $m/n \rightarrow 1$. Тогда при $\tilde{n} = n/(n-m)$

$$\sup_x \left| \mathbf{P}\left(\frac{\xi^{(1)}(n, m) - \ln \tilde{n}}{\sqrt{\ln \tilde{n}}} \right) - \Phi(x) \right| = O(1/\sqrt{\ln \tilde{n}}),$$

где $\Phi(x)$ — стандартная нормальная функция распределения, а также

$$\max_k \left| \sqrt{\ln \tilde{n}} \mathbf{P}(\xi^{(1)}(n, m) = k) - \frac{1}{\sqrt{2\pi}} e^{-x^2(k)/2} \right| = O(1/\sqrt{\ln \tilde{n}}),$$

где $x(k) = (k - \ln \tilde{n})/\sqrt{\ln \tilde{n}}$.

Приведем еще одно дополнение о поведении числа циклов $\xi_s^{(1)}$ фиксированных длин. Согласно [4] эта случайная величина имеет в пределе распределение Пуассона с параметром p^s/s . Рассмотрим многомерный случай. Пусть $1 \leq s_1 < \dots < s_r$ — фиксированные натуральные числа. Из производящей функции (1.5) с учетом (1.6) находим смешанные биномиальные моменты случайных величин $\xi_{s_1}^{(1)}, \dots, \xi_{s_r}^{(1)}$

$$\begin{aligned} B(k_1, \dots, k_r) &= \mathbf{M} \left(\xi_{s_1}^{(1)} \right) \dots \left(\xi_{s_r}^{(1)} \right) = \\ &= \binom{n}{m}^{-1} \text{Coef}_{t_1^m t_2^{n-m} (x_1-1)^{k_1} \dots (x_r-1)^{k_r}} \frac{1}{1-t_1-t_2} \exp \left\{ (x_1-1) \frac{t_1^{s_1}}{s_1} + \dots \right. \\ &\quad \left. \dots + (x_r-1) \frac{t_1^{s_r}}{s_r} \right\} = \frac{1}{k_1! s_1^{k_1} \dots k_r! s_r^{k_r}} \frac{(m)_{k_1 s_1 + \dots + k_r s_r}}{(n)_{k_1 s_1 + \dots + k_r s_r}}. \end{aligned}$$

Поэтому из многомерного варианта метода моментов вытекает справедливость следующего утверждения.

Теорема 2.2. При $m/n \rightarrow p$, $0 < p \leq 1$, случайные величины $\xi_{s_1}^{(1)}, \dots, \xi_{s_r}^{(1)}$ асимптотически независимы и распределены согласно закону Пуассона с параметрами $p^{s_1}/s_1, \dots, p^{s_r}/s_r$.

При исследовании вариационных характеристик длин циклов нам потребуется одно следствие из этой теоремы. Рассмотрим сечение правого хвоста случайной величины $\xi^{(1)}$

$$\xi^{(1)}(\ell) = \xi_{\{\ell, \dots, m\}}^{(1)} = \sum_{i=\ell}^m \xi_i^{(1)},$$

равное числу циклов 1-го цвета длин не менее ℓ , где $\ell = \text{const}$. Разобьем последнюю сумму на две (обозначения ясны из контекста)

$$\xi^{(1)}(\ell) = \sum_{i=\ell}^{L-1} \xi_i^{(1)} + \sum_{i=L}^m \xi_i^{(1)} = \xi^{(1)}(\ell, L-1) + \xi^{(1)}(L),$$

где фиксированное значение параметра L будет определено ниже. Элементарные преобразования дают

$$\begin{aligned} \mathbf{P} \left(\xi^{(1)}(\ell) = k \right) &= \mathbf{P}(\xi^{(1)}(\ell, L-1) = k) + \\ &+ \mathbf{P}(\xi^{(1)}(\ell) = k, \xi^{(1)}(L) > 0) - \mathbf{P}(\xi^{(1)}(\ell, L-1) = k, \xi^{(1)}(L) > 0). \end{aligned}$$

Пусть $m/n \rightarrow p$, $0 < p < 1$. Тогда последние две вероятности по абсолютной величине оцениваются сверху величиной

$$2\mathbf{M}\xi^{(1)}(L) = 2 \sum_{i \geq L} p^i / i + o(1).$$

За счет выбора фиксированного большого значения параметра L эта величина может быть сделана сколь угодно малой. Поэтому в распределении случайной величины $\xi^{(1)}(\ell)$ можно учитывать ограниченное число ее начальных слагаемых, и из теоремы 2.2 вытекает следующий ожидаемый результат.

Следствие 2.3. Пусть $m/n \rightarrow p$, $0 < p < 1$. Тогда при фиксированном натуральном ℓ сечение $\xi^{(1)}(\ell)$ имеет в пределе распределение Пуассона с параметром $-\ln(1-p) - \sum_{i=1}^{\ell-1} p^i / i$.

Изложение результатов о суммарных объемах циклов в классах начнем со случайной величины $\varkappa^{(1)}(n, m)$.

Пусть $\frac{m}{n} \rightarrow p$, $0 < p \leq 1$. При $p < 1$ она, очевидно, имеет предельное геометрическое распределение с вероятностью успеха $1-p$ (см. задание смеси распределений в формулировке теоремы 1.2), т. е.

$$\begin{aligned} \mathbf{P}(\varkappa^{(1)}(n, m) = k) &= \binom{n-k-1}{n-m-1} \binom{n}{m}^{-1} = \\ &= \frac{n-m}{n} \cdot \frac{(m)_k}{(n-1)_k} = (1-p)p^k + o(1), \quad k = 0, 1, \dots \end{aligned}$$

Этот простой факт отмечен в [4]. Для «симметричной» случайной величины $\varkappa^{(2)}(n, m)$ аналогичное предельное соотношение верно, если p и $1-p$ поменять местами.

Несложное обобщение последнего результата на двумерный случай при $0 < p < 1$ (см. далее лемму 2.5) позволяет легко найти предельное распределение суммарного объема 2-цветных циклов $\varkappa^{(1\circ 2)} = n - \varkappa^{(1)} - \varkappa^{(2)}$.

Теорема 2.4. Пусть $\varkappa_*^{(1\circ 2)}(n, m) = n - \varkappa^{(1\circ 2)}(n, m)$ и $\frac{m}{n} \rightarrow p$, $0 < p < 1$. Тогда:

- 1) при $p = 1/2$ случайная величина $\varkappa_*^{(1\circ 2)}(n, m)$ имеет в пределе отрицательное биномиальное распределение $\overline{Bi}(2, 1/2)$, т. е. при каждом фиксированном $k = 0, 1, \dots$

$$\mathbf{P}(\varkappa_*^{(1\circ 2)}(n, m) = k) = (k+1) \cdot (1/2)^{k+2} + o(1), \quad (2.1)$$

- 2) при $p \neq 1/2$ при каждом фиксированном $k = 0, 1, \dots$

$$\mathbf{P}(\varkappa_*^{(1\circ 2)}(n, m) = k) = \frac{p(1-p)}{2p-1} (p^{k+1} - (1-p)^{k+1}) + o(1). \quad (2.2)$$

Утверждение данной теоремы опирается на следующий вспомогательный результат, который представляет самостоятельный интерес.

Лемма 2.5. Пусть $\frac{m}{n} \rightarrow p$, $0 < p < 1$. Тогда случайные величины $\varkappa^{(1)}(n, m)$, $\varkappa^{(2)}(n, m)$ асимптотически независимы, т. е. для любых фиксированных $k_1, k_2 = 0, 1, \dots$

$$\mathbf{P}(\varkappa^{(1)}(n, m) = k_1, \varkappa^{(2)}(n, m) = k_2) = p^{k_1+1}(1-p)^{k_2+1} + o(1).$$

Доказательство леммы. Для нахождения совместной производящей функции характеристик $\varkappa^{(1)}(n, m)$ и $\varkappa^{(2)}(n, m)$ следует в общей

экспоненциальной производящей функции $\mathcal{F}(t_1, t_2; \bar{u})$ конкретизировать переменные следующим образом:

$$u_{i,j} = \begin{cases} z^i, & j = 0, \\ y^j, & i = 0, \\ 1, & i > 0, j > 0, \end{cases}$$

т. е. переменная z отвечает перечислению объема циклов в классе $C_{n,m}^{(1)}$, а y — в классе $C_{n,m}^{(2)}$. После элементарных упрощений приходим к производящей функции

$$\mathcal{F}(t_1, t_2; z, y) = \frac{(1-t_1)(1-t_2)}{(1-t_1-t_2)(1-zt_1)(1-yt_2)}.$$

Следовательно,

$$\text{Coef}_{z^{k_1}y^{k_2}}\mathcal{F}(t_1, t_2; z, y) = \mathcal{F}_{k_1, k_2}(t_1, t_2) = t_1^{k_1}t_2^{k_2} \frac{1-t_2}{1-t_2(1-t_1)^{-1}}.$$

Опуская вырожденный случай $k_2 = n - m$ (тогда $k_1 = m$ и вычитаемое в числителе последней дроби пропадает), окончательно получаем точную формулу совместного распределения

$$\begin{aligned} \mathbf{P}(\mathcal{K}^{(1)}(n, m) = k_1, \mathcal{K}^{(2)}(n, m) = k_2) &= \binom{n}{m}^{-1} \text{Coef}_{t_1^m t_2^{n-m}} \mathcal{F}_{k_1, k_2}(t_1, t_2) = \\ &= \binom{n}{m}^{-1} \left[\binom{n-k_1-k_2-1}{m-k_1} - \binom{n-k_1-k_2-2}{m-k_1} \right] = \\ &= \frac{(m)_{k_1}(n-m)_{k_2+1}}{(n)_{k_1+k_2+1}} - \frac{(m)_{k_1}(n-m)_{k_2+2}}{(n)_{k_1+k_2+2}}, \end{aligned}$$

где $k_1 + k_2 < n$. Отсюда при $m/n \rightarrow p$, $0 < p < 1$, следует асимптотическая независимость исследуемых случайных величин: при любых фиксированных $k_1, k_2 = 0, 1, \dots$

$$\mathbf{P}(\mathcal{K}^{(1)}(n, m) = k_1, \mathcal{K}^{(2)}(n, m) = k_2) = p^{k_1+1}(1-p)^{k_2+1} + o(1).$$

Лемма доказана.

Доказательство теоремы 2.4. Пусть $p = 1/2$. В силу леммы 2.5 случайная величина $\mathcal{K}^{(1)}(n, m) + \mathcal{K}^{(2)}(n, m)$ имеет в пределе распределение суммы двух независимых геометрически распределенных случайных

величин с равновероятными исходами. Следовательно, это предельное распределение является отрицательным биномиальным $\overline{\text{Bi}}(2, 1/2)$ и выполняется (2.1).

В общем случае предельное распределение суммы $\varkappa^{(1)}(n, m) + \varkappa^{(2)}(n, m)$ при $0 < p < 1$ в силу леммы 2.5 имеет вид

$$\mathbf{P}(\varkappa^{(1)}(n, m) + \varkappa^{(2)}(n, m) = k) = p(1-p) \sum_{s=0}^k p^s (1-p)^{k-s} + o(1),$$

$$k = 0, 1, \dots$$

Для завершения доказательства теоремы при $p \neq 1/2$ остается воспользоваться элементарным тождеством

$$(a-b) \sum_{s=0}^k a^s b^{k-s} = a^{k+1} - b^{k+1}, \quad a \neq b.$$

В исследовании суммарных объемов циклов в классах $C_{n,m}^{(1)}$, $C_{n,m}^{(2)}$, $C_{n,m}^{(1 \circ 2)}$ осталось рассмотреть последний случай $p = 1$. Тогда класс $C_{n,m}^{(2)}$ асимптотически вырожден, т. е. $\mathbf{P}(\varkappa^{(2)} = 0) = 1 + o(1)$. Следовательно,

$$\mathbf{P}(\varkappa^{(1 \circ 2)} = n - \varkappa^{(1)}) = 1 + o(1).$$

Поэтому случай $p = 1$ следует исследовать только для случайной величины $\varkappa^{(1)}$. Он, в свою очередь, распадается на два подслучая.

Теорема 2.6. Пусть $n - m \rightarrow \infty$ и $n - m = o(n)$. Тогда случайная величина $\varkappa^{(1)}(n, m)/\tilde{n}$, где $\tilde{n} = n/(n - m)$, имеет в пределе экспоненциальное распределение, т. е. при любом фиксированном $x > 0$ справедливы следующие локальные и интегральные соотношения:

$$\tilde{n} \cdot \mathbf{P}(\varkappa^{(1)}(n, m) = [x \cdot \tilde{n}]) = e^{-x} + o(1), \quad (2.3)$$

$$\mathbf{P}(\varkappa^{(1)}(n, m)/\tilde{n} < x) = 1 - e^{-x} + o(1). \quad (2.4)$$

Теорема 2.7. Пусть $n - m = \tau$, где τ — фиксированное натуральное число. Тогда случайная величина $\varkappa^{(1)}(n, n - \tau)/n$ имеет в пределе при $n \rightarrow \infty$ бета-распределение $\mathcal{B}(1, \tau)$, т. е. при любом фиксированном x , $0 < x < 1$, справедливы следующие локальные и интегральные соотношения:

$$n \cdot \mathbf{P}(\varkappa^{(1)}(n, n - \tau) = [x \cdot n]) = \tau(1 - x)^{\tau-1} + o(1), \quad (2.5)$$

$$\mathbf{P}(\mathfrak{x}^{(1)}(n, n - \tau)/n < x) = 1 - (1 - x)^\tau + o(1), \quad (2.6)$$

в частности при $\tau = 1$ предельное распределение является равномерным.

Доказательство теорем 2.6, 2.7. Напомним формулу точного распределения случайной величины $\mathfrak{x}^{(1)}(n, m)$

$$n - k - 1 \mathbf{P}(\mathfrak{x}^{(1)}(n, m) = k) = (n - m - 1) \binom{n}{m}^{-1} = \frac{n - m}{n} \cdot \frac{(m)_k}{(n - 1)_k}.$$

Ограничимся доказательством локальных предельных соотношений. Их интегральные аналоги (2.4) и (2.6) устанавливаются аналогично в силу формулы

$$\mathbf{P}(\mathfrak{x}^{(1)} < k) = \binom{n}{m}^{-1} \sum_{s=0}^{k-1} \binom{n-s-1}{n-m} = 1 - \binom{n-k}{n-m} \binom{n}{m}^{-1} = 1 - \frac{(m)_k}{(n)_k}.$$

Сначала установим справедливость утверждения из теоремы 2.7, т. е. $n - m = \tau$, τ — фиксированное натуральное число. Тогда

$$\mathbf{P}(\mathfrak{x}^{(1)}(n, n - \tau) = k) = \binom{n-k-1}{\tau-1} \binom{n}{\tau}^{-1} = \frac{\tau (n-k-1)_{\tau-1}}{n (n-1)_{\tau-1}}.$$

Отсюда при $k = [x \cdot n]$, $0 < x < 1$, вытекает асимптотическое равенство (2.5).

Пусть теперь выполняются условия теоремы 2.6. Тогда при $\tilde{n} = n/(n - m)$

$$\tilde{n} \cdot \mathbf{P}(\mathfrak{x}^{(1)}(n, m) = k) = \frac{(n - 1 - (n - m - 1))_k}{(n - 1)_k}.$$

Чтобы не загромождать обозначения, заменим $n - 1$ на n . При $k = [x \cdot \tilde{n}]$, $x > 0$, завершение доказательства проводим по стандартной схеме с помощью разложения логарифма в ряд (дважды)

$$\begin{aligned} \frac{(n - (n - m))_k}{(n)_k} &= \exp \left\{ \sum_{s=n-k+1}^n \ln \left(1 - \frac{n - m}{s} \right) \right\} = \\ &= \exp \left\{ -(n - m) \ln \frac{n}{n - k + 1} + o(1) \right\} = e^{-k/\tilde{n}} (1 + o(1)). \end{aligned}$$

Теоремы 2.6, 2.7 доказаны.

При $\tau = 1$ утверждение теоремы 2.7 согласуется с хорошо известным фактом: в случайной равновероятной подстановке степени n длина цикла, которому принадлежит выделенный элемент, имеет равновероятное распределение на множестве $\{1, \dots, n\}$.

Исследуем теперь сами длины циклов в классе $C_{n,m}^{(1)}$. С этой целью рассмотрим вариационный ряд длин циклов из класса $C_{n,m}^{(1)}$

$$\mu^{(1)}(n, m) = \mu_1^{(1)}(n, m) \leq \mu_2^{(1)}(n, m) \leq \dots \leq \mu_{\xi^{(1)}}^{(1)}(n, m) \leq m, \quad (2.7)$$

в частности $\mu^{(1)}(n, m)$ — минимальная длина цикла из элементов 1-го цвета. Максимальные длины (правые члены этого ряда) будем обозначать

$$\omega^{(1)}(n, m) = \omega_1^{(1)}(n, m) = \mu_{\xi^{(1)}}^{(1)}(n, m) \geq \omega_2^{(1)}(n, m) \geq \dots, \quad (2.8)$$

в частности $\omega^{(1)}(n, m)$ — максимальная длина цикла.

Исследуем предельные распределения крайних членов этих рядов при различных соотношениях между параметрами n и m .

Поскольку случайная величина $\xi^{(1)}(n, m)$ может иметь предельное распределение Пуассона, то в асимптотических соотношениях удобнее рассматривать произвольный натуральный номер s и полагать

$$\mu_s^{(1)}(n, m) = \omega_s^{(1)}(n, m) = 0 \text{ при } \xi^{(1)}(n, m) < s, \quad s = 1, 2, \dots$$

Для нахождения предельных законов распределения будем использовать стандартные представления вариационных характеристик через сечения левых и правых хвостов случайной величины $\xi^{(1)}(n, m)$

$$\begin{aligned} \xi^{(1)}(\overline{1}, \ell) &= \xi_1^{(1)}(n, m) + \dots + \xi_\ell^{(1)}(n, m), \\ \xi^{(1)}(\overline{\ell}, m) &= \xi_\ell^{(1)}(n, m) + \dots + \xi_m^{(1)}(n, m). \end{aligned}$$

Тогда

$$\mathbf{P} \left(1 \leq \mu_s^{(1)}(n, m) \leq \ell \right) = \mathbf{P} \left(\xi^{(1)}(\overline{1}, \ell) \geq s \right) = 1 - \mathbf{P} \left(\xi^{(1)}(\overline{1}, \ell) < s \right), \quad (2.9)$$

$$\mathbf{P} \left(\omega_s^{(1)}(n, m) < \ell \right) = \mathbf{P} \left(\xi^{(1)}(\overline{\ell}, m) < s \right). \quad (2.10)$$

В свою очередь, для вероятностей сечений будем использовать следующую формулу обращения для биномиальных/факториальных моментов. Пусть ξ — целочисленная неотрицательная случайная величина с факториальными моментами φ_k , $k = 1, 2, \dots$, $\varphi_0 = 1$. Тогда

при $s \geq 1$

$$\begin{aligned} \mathbf{P}(\xi < s) &= 1 - \mathbf{P}(\xi \geq s) = 1 - \sum_{k \geq s} (-1)^{k-s} \binom{k-1}{s-1} \frac{\varphi_k}{k!} = \\ &= 1 - \frac{1}{(s-1)!} \sum_{k \geq s} (-1)^{k-s} \frac{1}{k(k-s)!} \varphi_k \quad (2.11) \end{aligned}$$

(по поводу однозначности восстановления распределения по своим биномиальным/факториальным моментам в общем случае см. теорему Такача в [1]).

Перейдем к изложению результатов.

Распределения минимальных длин устроены аналогично соответствующим распределениям для случайных равновероятных подстановок из классической схемы (см. [20]). Действительно, из многомерной предельной теоремы 2.2 и равенства (2.9) сразу вытекает следующий простой результат.

Теорема 2.8. Пусть $m/n \rightarrow p$, $0 < p \leq 1$. Тогда

$$\mathbf{P}(1 \leq \mu_s^{(1)}(n, m) \leq \ell) = 1 - \sum_{k=0}^{s-1} \frac{\lambda_\ell^k}{k!} e^{-\lambda_\ell} + o(1), \quad \ell = 1, 2, \dots,$$

где $\lambda_\ell = p + p^2/2 + \dots + p^\ell/\ell$. Кроме того, при $p < 1$

$$\mathbf{P}(\mu_s^{(1)}(n, m) = 0) = \sum_{k=0}^{s-1} \frac{\lambda^k}{k!} e^{-\lambda} + o(1),$$

где $\lambda = -\ln(1-p)$.

Для максимальных длин циклов при $p < 1$ картина сохраняется с точностью до переобозначений параметров. На основании следствия 2.3 и формулы (2.10) получаем следующее утверждение.

Теорема 2.9. Пусть $m/n \rightarrow p$, $0 < p < 1$. Тогда

$$\mathbf{P}(\omega_s^{(1)}(n, m) < \ell) = \sum_{k=0}^{s-1} \frac{\tilde{\lambda}_\ell^k}{k!} e^{-\tilde{\lambda}_\ell} + o(1), \quad \ell = 1, 2, \dots$$

(для единообразия обозначений считаем $\tilde{\lambda}_1 = \lambda$).

Напомним, что предельное распределение минимальной длины цикла в классической схеме не имеет среднего [24]. Аналогичное утверждение верно для 2-цветной модели при $p = 1$. При $p < 1$ конечность асимптотических значений средних всех членов вариационного ряда длин циклов из элементов 1-го цвета сразу вытекает из того, что суммарный объем циклов имеет предельное геометрическое распределение.

Исследуем поведение максимальных длин циклов в классе $C_{n,m}^{(1)}$ в случае $m \sim n$. Он, в свою очередь, распадается на два подслучая. Справедливы следующие утверждения.

Теорема 2.10. Пусть $n \rightarrow \infty$, $m = n - \tau$, где τ — натуральное число. Тогда при $x \geq 1/s - \tau/s \cdot n$

$$\mathbf{P}(\omega_s^{(1)}(n, m)/n < x) = 1$$

и при $0 < x < 1/s - \tau/s \cdot n$

$$\mathbf{P}(\omega_s^{(1)}(n, m)/n < x) = 1 - \frac{1}{(s-1)!} \sum_{k=s}^{[1/x]} \frac{(-1)^{k-s}}{k(k-s)!} J_{\tau,k}(x) + o(1), \quad (2.12)$$

где

$$J_{\tau,k}(x) = \int \dots \int_{\mathcal{X}(x,k)} \frac{(1 - x_1 - \dots - x_k)^\tau}{x_1 \dots x_k} dx_1 \dots dx_k, \quad k = 1, 2, \dots, [1/x], \quad (2.13)$$

и интегрирование проводится по области $\mathcal{X}(x, k) = \{x_1 + \dots + x_k \leq 1; x_1, \dots, x_k \geq x\}$.

Введем обозначение

$$E(x) = \int_x^{+\infty} \frac{e^{-u}}{u} du, \quad x > 0,$$

т. е. $E(x) = -\text{Ei}(-x)$, где $\text{Ei}(y)$ — специальная интегральная показательная функция.

Теорема 2.11. Пусть $n - m \rightarrow \infty$ и $n - m = o(n)$. Тогда для любого фиксированного положительного x при $\tilde{n} = n/(n - m)$

$$\mathbf{P}(\omega_s^{(1)}(n, m)/\tilde{n} < x) = \sum_{k=0}^{s-1} \frac{E(x)^k}{k!} e^{-E(x)} + o(1).$$

В частности, для максимальной длины цикла

$$\mathbf{P}(\omega^{(1)}(n, m)/\tilde{n} < x) = \exp \left\{ - \int_x^{+\infty} \frac{e^{-u}}{u} du \right\} + o(1). \quad (2.14)$$

Доказательство теоремы 2.10. Покажем, что факториальные моменты сечения $\xi^{(1)}(\ell, m)$ при $n \rightarrow \infty$ представляются в интегральном виде (2.13). Тогда вид самого предельного распределения (2.12) вытекает из формулы обращения (2.11).

Из производящей функции (1.5) с учетом (1.6) находим вид биномиальных моментов сечения $\xi^{(1)}(\ell, m)$

$$B_k(\ell) = \frac{1}{k!} \sum_{\substack{i_1 + \dots + i_k \leq m \\ i_1, \dots, i_k \geq \ell}} \frac{1}{i_1 \dots i_k} \frac{(m)_i}{(n)_i}, \quad k = 1, 2, \dots, [m/\ell], \quad B_0(\ell) = 1, \quad (2.15)$$

где $i = i_1 + \dots + i_k$. Пусть $n - m = \tau$, τ — натуральное число, и $\ell \sim xn$, где $0 < x < 1$. Тогда

$$\frac{(m)_i}{(n)_i} = \frac{(n - \tau)_i}{(n)_i} = \frac{(n - i)_\tau}{(n)_\tau} = (1 - i/n)^\tau (1 + o(1)).$$

В силу конечности τ данное асимптотическое представление, очевидно, является равномерным по всей области суммирования из формулы биномиального момента (2.15). Полагая $i_1 = [x_1 n], \dots, i_k = [x_k n]$, где $x_1 + \dots + x_k \leq 1$; $x_1, \dots, x_k \geq x$, приходим к интегральной сумме с шагом $1/n$ по каждой переменной

$$B_k(\ell) = \frac{1}{k!} \frac{1}{n^k} \sum_{\substack{x_1 + \dots + x_k < 1 \\ x_1, \dots, x_k \geq x}} \frac{1}{x_1 \dots x_k} (1 - x_1 - \dots - x_k)^\tau (1 + o(1)).$$

Следовательно, при $n \rightarrow \infty$

$$\mathbf{B}_k(\ell) = \frac{1}{k!} \int \dots \int_{\mathcal{X}(x, k)} \frac{(1 - x_1 - \dots - x_k)^\tau}{x_1 \dots x_k} dx_1 \dots dx_k + o(1),$$

$$k = 1, 2, \dots, [1/x],$$

что завершает доказательство теоремы 2.10.

Доказательство теоремы 2.11. Для установления справедливости утверждения этой теоремы достаточно показать, что сечение $\xi^{(1)}(\ell, m)$

при $\ell = [x \cdot n/(n-m)]$ распределено в пределе по закону Пуассона с параметром $E(x)$.

Сначала рассмотрим поведение среднего

$$\mathbf{M}\xi^{(1)}(\overline{\ell, m}) = \sum_{i=\ell}^m \frac{1}{i} \frac{(m)_i}{(n)_i}. \quad (2.16)$$

Последнюю дробь преобразуем к виду

$$\frac{(m)_i}{(n)_i} = \left(1 - \frac{n-m}{n}\right) \dots \left(1 - \frac{n-m}{n-i+1}\right).$$

Отсюда вытекают двухсторонние оценки

$$\left(1 - \frac{n-m}{n-i+1}\right)^i \leq \frac{(m)_i}{(n)_i} \leq \left(1 - \frac{n-m}{n}\right)^i. \quad (2.17)$$

Следовательно, $(m)_i/(n)_i \leq \exp\{i \ln(1-1/\tilde{n})\} \leq e^{-i/\tilde{n}}$, где $\tilde{n} = n/(n-m)$. Подставим эту оценку в (2.16) и воспользуемся простейшими неравенствами для непрерывной невозрастающей функции $f(x)$

$$f(b) + \int_a^b f(y)dy \leq \sum_{i=a}^b f(i) \leq f(a) + \int_a^b f(y)dy. \quad (2.18)$$

В итоге получаем верхнюю оценку

$$\mathbf{M}\xi^{(1)}(\overline{\ell, m}) \leq \sum_{i=\ell}^m \frac{1}{i} e^{-i/\tilde{n}} \leq \int_{\ell}^{\infty} \frac{1}{y} e^{-y/\tilde{n}} dy + O\left(\frac{1}{\ell}\right).$$

Производя замену переменной $y = \tilde{n} \cdot u$ и выбирая $\ell = \tilde{n} \cdot x$, где $0 < x \leq u$, находим, что $\mathbf{M}\xi^{(1)}(\overline{\ell, m}) \leq E(x) + O(1/\ell)$. Таким образом,

$$B_k(\ell) \leq \frac{E^k(x)}{k!} + o(1). \quad (2.19)$$

Если выбрать $\ell = n'$, где параметр n' удовлетворяет условиям $n' \leq m$ и $\tilde{n} = o(n')$, то справедлива грубая оценка

$$\mathbf{M}\xi^{(1)}(\overline{n', m}) = O(\tilde{n}/n'). \quad (2.20)$$

Найдем нижнюю оценку для среднего. В силу (2.20) верхнюю границу суммирования в (2.16) можно заменить на n' .

Для левой границы из (2.17) имеем

$$\begin{aligned} \left(1 - \frac{n-m}{n-i+1}\right)^i &\geq \left(1 - \frac{n-m}{n-n'}\right)^i = \\ &= \exp \left\{ i \ln \left(1 - \frac{n-m}{n-n'}\right) \right\} \geq \exp \left\{ -i \frac{n-m}{n-n'} + O(n'/\tilde{n}^2) \right\}. \end{aligned}$$

Накладывая дополнительные условия $n' = o(\min\{\tilde{n}^2, n\})$, получаем равномерную нижнюю оценку

$$(m)_i / (n)_i \geq e^{-i/\tilde{n}}(1 + o(1)). \quad (2.21)$$

Теперь можно сразу перейти к получению нижней оценки для многомерной суммы в формуле для биномиального момента (2.15). Для этого индексы суммирования ограничим сверху $\ell \leq i_1, \dots, i_k \leq n'$. Тогда условие $i_1 + \dots + i_k \leq m$ становится лишним. Для оставшихся слагаемых в многомерной сумме воспользуемся равномерной нижней оценкой (2.21). Используя левое неравенство из (2.18), в итоге получаем

$$B_k(\ell) \geq \frac{1}{k!} \left(\sum_{i=\ell}^{n'} \frac{1}{i} e^{-i/\tilde{n}} \right)^k + o(1) = \frac{E^k(x)}{k!} + o(1),$$

что с учетом верхней оценки (2.19) завершает доказательство теоремы (2.11).

Дадим комментарии к теоремам 2.10 и 2.11.

Похожее предельное распределение максимальной длины цикла из теоремы 2.10 возникает при переходе от классической схемы к схеме Эванса (подробнее см. работу Г. И. Ивченко и Ю. И. Медведева [6], в которой приведено сопоставление полученных результатов с аналогичными результатами из работ Арратиа, Барбу, Таваре [22] и Хансена [23]).

Предельное распределение из теоремы 2.11 возникло в другой работе тех же авторов [7], где рассматривалась модель неравновесных подстановок случайной степени — степень подстановки изначально имеет отрицательное биномиальное распределение. Поэтому теорема 2.11 (с учетом того, что $\mathfrak{X}^{(1)}(n, m)$ может иметь предельное геометрическое распределение) полностью согласуется с вероятностной моделью из [7].

Приведем некоторые следствия из двух последних теорем.

Предельную функцию распределения (2.12) максимальной длины цикла в классе $C_{n,m}^{(1)}$ обозначим

$$\Phi_\tau(x) = 1 - \sum_{k=1}^{[1/x]} \frac{(-1)^{k-1}}{k!} J_{\tau,k}(x), \quad 0 < x < 1.$$

Справедливы следующие многомерные локальные теоремы, для доказательства которых требуется знание только предельной функции распределения максимальной вариационной характеристики.

Следствие 2.12. Пусть $n \rightarrow \infty$, $m = n - \tau$, где τ — натуральное число. Для фиксированного набора $0 < x_r < x_{r-1} < \dots < x_1 < 1$, $x_1 + \dots + x_r < 1$, $r \geq 1$

$$\begin{aligned} n^r \cdot \mathbf{P}(\omega_1^{(1)}(n, m) = [x_1 n], \dots, \omega_r^{(1)}(n, m) = [x_r n]) = \\ = \frac{(1 - x_1 - \dots - x_r)^\tau}{x_1 \dots x_r} \Phi_\tau \left(\frac{x_r}{1 - x_1 - \dots - x_r} \right) + o(1). \end{aligned}$$

Следствие 2.13. Пусть $n - m \rightarrow \infty$, $n - m = o(n)$ и $\tilde{n} = n/(n - m)$. Тогда для произвольных фиксированных $r \geq 1$ и $0 < x_r < x_{r-1} < \dots < x_1$

$$\begin{aligned} \tilde{n}^r \cdot \mathbf{P}(\omega_1^{(1)}(n, m) = [x_1 \tilde{n}], \dots, \omega_r^{(1)}(n, m) = [x_r \tilde{n}]) = \\ = \frac{1}{x_1 \dots x_r} \exp \left\{ - \sum_{s=1}^r x_s - \int_{x_r}^{\infty} \frac{e^{-u}}{u} du \right\} + o(1). \end{aligned}$$

Эти следствия являются в определенном смысле стандартными для данной проблематики и не нуждаются в самостоятельном доказательстве. Поэтому ограничимся лишь приведенными формулировками. Все необходимые обоснования неоднократно воспроизводились в цикле работ Г. И. Ивченко и Ю. И. Медведева, и нет необходимости повторять их (см. подробный обзор в [9]).

Список литературы

- [1] Сачков В.Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.
- [2] Сачков В.Н., “Оператор редуцирования. I.”, *Труды по дискретной математике*, **2** (1998), 282–295.
- [3] Сачков В.Н., “Оператор редуцирования и преобразования со свойствами наследственности, ч. II”, *Труды по дискретной математике*, **10** (2007), 269–286.
- [4] Сачков В.Н., “Случайные подстановки с трансформированными циклами”, *Математические вопросы криптографии*, **3:4** (2012), 127–150.

- [5] Сачков В.Н., “Случайные подстановки с циклами ограниченной длины и трансформированием”, *Математические вопросы криптографии*, **5:3** (2014), 117–136.
- [6] Ивченко Г.И., Медведев Ю.И., “Метод В. Л. Гончарова и его развитие в анализе различных моделей случайных подстановок”, *Теория вероятностей и ее применения*, **47:3** (2002), 558–566.
- [7] Ивченко Г.И., Медведев Ю.И., “Об одном классе неравновероятных подстановок случайной степени”, *Труды по дискретной математике*, **7** (2003), 75–88.
- [8] Ивченко Г.И., Медведев Ю.И., “Случайные неполные подстановки”, *Труды по дискретной математике*, **11** (2008), 35–46.
- [9] Ивченко Г.И., Медведев Ю.И., *Дискретные распределения. Вероятностно-статистический справочник. Многомерные распределения*, М.: ЛЕНАНД, 2016, 336 с.
- [10] Викторенков В.Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозр. прикл. и промышл. матем.*, **7:2** (2000), 327.
- [11] Викторенков В.Е., “Об асимптотической нормальности логарифма порядка случайной полиномиальной подстановки над примарным кольцом вычетов с ограниченной разрядностью”, *Обозр. прикл. и промышл. матем.*, **7:2**, 486.
- [12] Викторенков В.Е., “Объемы циклов случайных полиномиальных преобразований колец”, *Обозр. прикл. и промышл. матем.*, **9:2** (2002), 347–348.
- [13] Викторенков В.Е., “О некоторых характеристиках цикловой структуры случайных равновероятных подстановок с помеченными циклами и их применение для исследования полиномиальных преобразований колец”, *Обозр. прикл. и промышл. матем.*, **10:3** (2003), 621.
- [14] Викторенков В.Е., “О строении полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29:3** (2017), 3–23.
- [15] Ларин М.В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14:2** (2002), 20–32.
- [16] Ермилов Д.М., Козлитин О.А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4:1** (2013), 27–57.
- [17] Ермилов Д.М., Козлитин О.А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **3:6** (2015), 47–73.
- [18] Козлитин О.А., “Оценка длины максимального цикла в графе полиномиального преобразования кольца Галуа – Эйзенштейна”, *Дискретная математика*, **29:4** (2017), 41–58.
- [19] Ватутин В.А., Михайлов В.Г., “Предельные теоремы для числа пустых ячеек в равновероятной схеме размещения частиц комплектами”, *Теория вероятн. и ее примен.*, **27:4** (1982), 684–692.
- [20] Колчин В.Ф., *Случайные отображения*, М.: Наука, 1984, 206 с.
- [21] Anashin V.S., “Uniformly distributed sequences in computer algebra or how construct program generators of random numbers”, *J. Math. Sci.*, **8** (1999), 193–208.
- [22] Arratia R., Barbour A.D., Tavaré S., “On Poisson-Dirichlet limits for random decomposable combinatorial structures”, *Comb., Probab. and Comput.*, **8** (1999), 193–208.
- [23] Hansen J.C., “Order statistics for decomposable combinatorial structures”, *Random Structures & Algorithms*, **5:4** (1994), 517–533.
- [24] Shepp L.A., Lloyd S.P., “Ordered cycle lengths in random permutations”, *Trans. Amer. Math. Soc.*, **121:21** (1966), 340–357.