Math-Net.Ru

Общероссийский математический портал

В. Н. Сачков, Случайные подстановки с циклами ограниченной длины и трансформированием, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 3, 117–136

DOI: <https://doi.org/10.4213/mvk131>

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: 44.207.124.84

26 апреля 2023 г., 09:20:18

УДК 519.212.2

Случайные подстановки с циклами ограниченной длины и трансформированием

В. Н. Сачков

Академия криптографии Российской Федерации, Москва

Получено 22.IV.2013

Рассматриваются случайные подстановки степени n , имеющие равномерное распределение на множестве подстановок, длины циклов которых принадлежат множеству $A \subseteq \{1, 2, \dots, m\}$. Циклы такой подстановки трансформируются независимо с вероятностями, зависящими от длины цикла. Изучаются точные и предельные распределения числа нетрансформированных циклов.

Ключевые слова: случайные подстановки, трансформированные циклы, производящие функции, предельные теоремы

Random substitutions with cycles of bounded lengths and transforming
V. N. Sachkov

Academy of Cryptography of the Russian Federation, Moscow

Abstract. Random substitutions of degree n having the uniform distribution on the set of substitutions with cycles lengths belonging to the set $A \subseteq \{1, 2, \dots, m\}$ are considered. Cycles of such substitution are transformed independently with probabilities depending on the cycle length. Exact and limits distributions of the number of nontransformed cycles are investigated.

Keywords: random substitutions, transformed cycles, generating functions, limit theorems.

Введение

Данная работа продолжает тематику статьи [6], связанную с трансформированием циклов случайных подстановок. Для $n, m \geq 1$ и $A \subseteq \{1, 2, \dots, m\}$ рассматриваются множества A -подстановок $G_{nm}(A)$ степени n , длины циклов которых принадлежат множеству A [3]. На множестве $G_{nm}(A)$ задается равномерное вероятностное распределение. Вероятность трансформирования цикла длины l равна q_l , $p_l + q_l = 1$, и трансформирование осуществляется независимо для разных циклов с использованием процесса трансформации L [6]. Вводятся случайные величины ξ_{nm}^A (число нетрансформированных циклов в случайной A -подстановке) и $\xi_{nm}^A(l)$ (число нетрансформированных циклов длины l , $1 \leq l \leq m$).

Основными результатами являются теоремы, определяющие точные и предельные распределения случайных величин ξ_{nm}^A и $\xi_{nm}^A(l)$, $l \in A$.

Отдельно рассмотрен случай инволюций, когда $A = \{1, 2\}$, $l = m = 2$.

Дана интерпретация инволюций в виде сетей мобильной связи, когда $\xi_{n2}(2)$ – число занятых линий связи и вероятность p определяет надежность работы линии после вызова абонента.

В статье для вывода предельных распределений при различных условиях применяется единый подход, основанный на следующей теореме, впервые сформулированной и доказанной в книге [3, стр. 57, теорема 4.2].

Теорема 4.2 [3]. Если производящая функция $f_n(x)$ целочисленной неотрицательной случайной величины ξ_n при $n \rightarrow \infty$ равномерно для всех $x \in W = [1 - \delta, 1 + \delta]$, $\delta > 0$ имеет асимптотическое представление

$$f_n(x) = x^{v_n} e^{h_n(x)} (1 + o(1)), \quad (0.1)$$

где $h_n(x)$ имеет три первых производных, для которых равномерно для $x \in W$ выполнены условия

$$h'_n(1) + h''_n(1) \rightarrow \infty, \quad \frac{h'''(x)}{h'_n(1) + h''_n(1)} \rightarrow 0, \quad (0.2)$$

то случайная величина

$$\xi'_n = \frac{\xi_n - v_n - h'_n(1)}{\sqrt{h'_n(1) + h''_n(1)}} \quad (0.3)$$

асимптотически нормальна с параметрами $(0, 1)$.

Эта теорема под названием «Generalized quasi-powers Theorem» («Обобщенная квази-степенная теорема») цитируется в недавно вышедшей

книге Флажолы и Седжвика [5] со ссылкой кембриджское издание книги Сачкова В.Н. [4]. В [5] приведен класс задач, в решении которых она может быть использована.

Название теоремы связано с наличием асимптотического представления вида (0.1) для производящей функции $f_n(x)$. Такое представление может быть получено методом перевала для функции комплексного переменного, выражающей производящую функцию $f_n(x)$ с помощью интегральной формулы Коши. Этот подход используется и в данной статье.

Отметим, что в статье предложен и используется также вариант теоремы 4.2 [3], связанный с предельным пуассоновским распределением.

Теорема 4.2'. Если производящая функция $f_n(x)$ целочисленной неотрицательной случайной величины ξ_n при $n \rightarrow \infty$ равномерно для всех $x \in W = [1 - \delta, 1 + \delta]$, $\delta > 0$, имеет при $v_n = 0$ представление (0.1), где $h_n(x)$ имеет две первые производные, для которых равномерно по $x \in W$ выполнены условия

$$h'_n(1) \rightarrow \lambda > 0, \quad h''_n(x) \rightarrow 0,$$

то случайная величина ξ_n в пределе имеет распределение Пуассона с параметром λ .

1. Производящие функции цикловых индикаторов A -подстановок

Множество подстановок степени n , длины циклов которых не превосходят m , можно представить в виде

$$G_{nm} = \bigcup_A G_{nm}(A), \quad (1.1)$$

где $A \subseteq \{1, 2, \dots, m\}$ и $G_{nm}(A)$ – множество A -подстановок, для которых длины циклов принадлежат A . Если максимальная длина циклов A -подстановки меньше m , то она относится к классу подстановок $G_{nm'}(A)$, где $m' < m$. Обозначим через α_j число j -циклов в A -подстановке, через $[j^{\alpha_j}, j \in A]$ соответствующий цикловой класс A -подстановок, а через $C_{nm}(j^{\alpha_j}, j \in A)$ – число A -подстановок в этом цикловом классе.

Цикловой индикатор множества A -подстановок можно записать в следующем виде:

$$C_{nm}^A(x_j, j \in A) = \sum_{\sum_{j \in A} j\alpha_j = n} C_{nm}(j^{\alpha_j}, j \in A) \prod_{j \in A} x_j^{\alpha_j}. \quad (1.2)$$

Производящая функция этого циклового индикатора определяется равенством из [3]

$$\sum_{n=0}^{\infty} C_{nm}^A(x_j, j \in A) \frac{t^n}{n!} = \exp \left\{ \sum_{j \in A} x_j \frac{t^j}{j} \right\}. \quad (1.3)$$

На множестве $G_{nm}(A)$ зададим равномерное вероятностное распределение и обозначим через ξ_j число нетрансформированных j -циклов в случайной подстановке $s \in G_{nm}(A)$ при условии, что вероятность нетрансформации j -цикла равна p_j , $p_j + q_j = 1$, $j \in A$. Тогда

$$\mathbf{P} \left(\bigcap_{j \in A} \{ \xi_j = k_j \} \right) = \frac{1}{C_{nm}^A} \sum_{[j^{\alpha_j}, j \in A]} C_{nm}(j^{\alpha_j}, j \in A) \prod_{j \in A} \binom{\alpha_j}{k_j} p_j^{k_j} q_j^{\alpha_j - k_j}, \quad (1.4)$$

где C_{nm}^A — число всех подстановок в $G_{nm}(A)$ и суммирование по всем цикловым классам множества A -подстановок.

Отсюда следует выражение для производящей функции

$$\begin{aligned} P(x_j, j \in A) &= \sum_{k_j: j \in A} \mathbf{P} \left(\bigcap_{j \in A} \{ \xi_j = k_j \} \right) \prod_{j \in A} x_j^{k_j} = \\ &= \frac{1}{C_{nm}^A} \sum_{[j^{\alpha_j}, j \in A]} C_{nm}(j^{\alpha_j}, j \in A) \prod_{j \in A} (p_j x_j + q_j)^{\alpha_j}. \end{aligned} \quad (1.5)$$

Если ξ_{nm}^A — общее число нетрансформированных циклов в случайной подстановке $s \in G_{nm}(A)$, то

$$\mathbf{P}(\xi_{nm}^A = k) = \frac{1}{C_{nm}^A} \sum_{[j^{\alpha_j}, j \in A]} C_{nm}(j^{\alpha_j}, j \in A) \sum_{\sum_{j \in A} k_j = k} \prod_{j \in A} \binom{\alpha_j}{k_j} p_j^{k_j} q_j^{\alpha_j - k_j}, \quad (1.6)$$

и из (1.5) при $x_j = x$, $j \in A$, получаем производящую функцию ξ_{nm}^A

$$P_{nm}^A(x) = \sum_{k=0}^n \mathbf{P}(\xi_{nm}^A = k) x^k = \frac{1}{C_{nm}^A} C_{nm}^A(p_j x + q_j, j \in A). \quad (1.7)$$

Отсюда следует, что

$$\sum_{n=0}^{\infty} C_{nm}^A P_{nm}^A(x) \frac{t^n}{n!} = \exp \left\{ \sum_{j \in A} (p_j x + q_j) \frac{t^j}{j} \right\}. \quad (1.8)$$

Аналогичным способом получаем выражение для производящей функции случайной величины $\xi_{nm}^A(l)$, равной числу нетрансформированных l -циклов при $l \in A$

$$P_n^A(x; l) = \sum_{k=0}^{\lfloor n/l \rfloor} \mathbf{P}(\xi_{nm}^A(l) = k) x^k = \frac{1}{C_{nm}^A} \sum_{j^{\alpha_j}, j \in A} C_{nm}(j^{\alpha_j}, j \in A) (p_l x + q_l)^{\alpha_l}. \quad (1.9)$$

Следовательно,

$$\sum_{n=0}^{\infty} C_{nm}^A P_{nm}^A(x; l) \frac{t^n}{n!} = \exp \left\{ \sum_{j \in A} \frac{t^j}{j} + p_l (x-1) \frac{t^l}{l} \right\}. \quad (1.10)$$

Пусть $\mathbf{B}_{nm}^A(k)$ и $\mathbf{B}_{nm}^A(k; l)$ – k -е биномиальные моменты ξ_{nm}^A и $\xi_{nm}^A(l)$, соответственно. Рассмотрим производящие функции этих моментов:

$$B_{nm}^A(x) = \sum_{k=0}^{\infty} \mathbf{B}_{nm}^A(k) x^k, \quad B_{nm}^A(x; l) = \sum_{k=0}^{\infty} \mathbf{B}_{nm}^A(k; l) x^k. \quad (1.11)$$

Из равенства (1.8) имеем

$$\sum_{n=0}^{\infty} C_{nm}^A B_{nm}^A(x) \frac{t^n}{n!} = \exp \left\{ \sum_{j \in A} (p_j x + 1) \frac{t^j}{j} \right\}. \quad (1.12)$$

Так как

$$\exp \left\{ x \sum_{j \in A} p_j \frac{t^j}{j} \right\} = \sum_{n=0}^{\infty} \frac{t^n}{n!} \times \sum_{k=0}^n x^k \frac{n!}{k!} \sum_{\substack{j_1 + \dots + j_k = n \\ j_i \in A, 1 \leq i \leq k}} \frac{p_{j_1} \dots p_{j_k}}{j_1 \dots j_k} \quad (1.13)$$

и, кроме того,

$$\exp \left\{ \sum_{j \in A} \frac{t^j}{j} \right\} = \sum_{n=0}^{\infty} C_{nm}^A \frac{t^n}{n!}, \quad (1.14)$$

то из равенства (1.12) с учетом (1.13) и (1.14) получаем

$$\sum_{n=0}^{\infty} C_{nm}^A B_{nm}^A(x) \frac{t^n}{n!} = \sum_{n=0}^{\infty} \frac{t^n}{n!} \sum_{k=0}^n x^k \frac{1}{k!} \sum_{\substack{j_1 + \dots + j_k = n \\ j_i \in A, 1 \leq i \leq k}} C_{n-j_1-\dots-j_k, m}^A(n)_{j_1+\dots+j_k} \frac{p_{j_1} \dots p_{j_k}}{j_1 \dots j_k}, \quad (1.15)$$

где $(n)_k = \frac{n!}{(n-k)!}$.

Отсюда следует формула для биномиальных моментов ξ_{nm}^A :

$$\mathbf{B}_{nm}^A(k) = \frac{1}{k!} \sum_{\substack{j_1 + \dots + j_k \leq n \\ j_i \in A, 1 \leq i \leq k}} \frac{C_{n-j_1-\dots-j_k, m}^A(n)_{j_1+\dots+j_k}}{C_{nm}^A} \frac{p_{j_1} \dots p_{j_k}}{j_1 \dots j_k}, \quad k = 0, 1, \dots \quad (1.16)$$

При $k = 1$ отсюда получаем формулу для среднего значения ξ_{nm}^A

$$\mathbf{M}\xi_{nm}^A = \sum_{j \in A} \frac{C_{n-j,m}^A}{C_{nm}^A} (n)_j \frac{p_j}{j}. \quad (1.17)$$

Найдем теперь формулу для k -го биномиального момента случайной величины $\xi_{nm}^A(l)$.

Из равенства (1.10) для $B_{nm}^A(x;l)$ – производящей функции биномиальных моментов $\xi_{nm}^A(l)$ – имеем

$$\sum_{n=0}^{\infty} C_{nm}^A B_{nm}^A(x;l) \frac{t^n}{n!} = \exp \left\{ \sum_{j \in A} \frac{t^j}{j} + p_l x \frac{t_l}{l} \right\}. \quad (1.18)$$

Отсюда получаем

$$\sum_{n=0}^{\infty} C_{nm}^A B_{nm}^A(x;l) \frac{t^n}{n!} = \sum_{n=0}^{\infty} \frac{t^n}{n!} \sum_{k=0}^{\lfloor n/l \rfloor} C_{n-kl,m}^A \left(\frac{p_l}{l} \right)^k \frac{x^k}{k!}.$$

Из этого соотношения следует формула для k -го биномиального момента $\xi_{nm}^A(l)$

$$\mathbf{B}_{nm}^A(k;l) = \frac{1}{k!} \frac{C_{n-kl,m}^A}{C_{nm}^A} \left(\frac{p_l}{l} \right)^k, \quad k = 0, 1, \dots \quad (1.19)$$

Полагая $k = 1$, получаем выражение для среднего значения $\xi_{nm}^A(l)$

$$\mathbf{M}\xi_{nm}^A(l) = \frac{C_{n-l,m}^A}{C_{nm}^A} \frac{p_l}{l}. \quad (1.20)$$

Так как распределение Пуассона с параметром λ однозначно определяется своими моментами, и биномиальные моменты этого распределения имеют вид $\lambda^k / k!$, $k = 0, 1, \dots$, то имеют место следующие две теоремы, доказательства которых следуют из формул (1.16) и (1.19) соответственно.

Теорема 1. Если при $n \rightarrow \infty$ для любого k существует предел

$$\frac{1}{C_{nm}^A} \sum_{\substack{j_1 + \dots + j_k \leq n \\ j_i \in A, 1 \leq i \leq k}} C_{n-j_1-\dots-j_k,m}^A (n)_{j_1+\dots+j_k} \frac{p_{j_1} \dots p_{j_k}}{j_1! \dots j_k!} \rightarrow \lambda^k, \quad k = 0, 1, \dots,$$

то случайная величина $\xi_{nm}^A(l)$ в качестве предельного распределения имеет закон Пуассона с параметром λ .

Теорема 2. Если при $n \rightarrow \infty$ и $p_l = p_l(n)$ для любого k существует предел

$$\frac{C_{n-kl,m}^A}{C_{nm}^A} \left(\frac{p_l}{l} \right)^k \rightarrow \lambda_l^k,$$

то $\xi_{nm}^A(l)$ в пределе распределена по закону Пуассона с параметром λ_l .

2. Асимптотические формулы

Пусть $x_j \in W = [1 - x_0, 1 + x_0]$, $x_0 > 0$, и $0 < p_j < 1$, $j \in A$. Положим $y_j = p_j x_j + q_j$, $p_j + q_j = 1$, $j \in A$. Тогда $y_j \in \bar{W} = [1 - p_j x_0, 1 + p_j x_0]$, $j \in A$. Из равенства (1.3), используя интегральную формулу Коши, для циклового индикатора получаем выражение

$$C_{nm}^A(y_j : j \in A) = \frac{n!}{2\pi i} \oint_C \exp \left\{ \sum_{j \in A} y_j \frac{z^j}{j} \right\} \frac{dz}{z^{n+1}}, \quad (2.1)$$

где C – замкнутый контур в комплексной плоскости, охватывающий начало координат. Для любых $x_j \in W$ и, следовательно, для любых $y_j \in \bar{W}$ в подынтегральной функции интеграла (2.1) экспонента в показателе степени имеет многочлен с положительными коэффициентами, т.е. является целой функцией. Поэтому в конечной плоскости подынтегральная функция имеет в нуле единственную особую точку.

Будем предполагать, что если $A = \{j_1, j_2, \dots, j_n\} \subseteq \{1, 2, \dots, m\}$, то $(j_1, j_2, \dots, j_n) = 1$, т.е. НОД $\{j_1, j_2, \dots, j_n\} = 1$. Если НОД $\{j_1, j_2, \dots, j_n\} = d > 1$, то следует рассматривать производящую функцию (1.3) от переменной $t' = t^d$.

При этих условиях справедлива следующая теорема, дающая при $n \rightarrow \infty$ асимптотическое выражение для циклового индикатора.

Теорема 3. При $n \rightarrow \infty$ равномерно для всех $x_j \in W$ и $y_j \in \bar{W}$, $j \in A$, имеет место асимптотическая формула

$$C_{nm}^A(y_j, j \in A) = \frac{n! \exp \left\{ \sum_{j \in A} y_j \frac{R^j}{j} \right\}}{R^n \sqrt{2\pi \sum_{j \in A} j y_j R^j}} (1 + o(1)), \quad (2.2)$$

где R при любых $x_j \in W$, $y_j \in \bar{W}$ – единственный положительный корень уравнения

$$\sum_{j \in A} y_j R^j = n, \quad (2.3)$$

причем $y_j = p_j x_j + q_j$, $0 < p_j < 1$, $j \in A$.

Доказательство теоремы 3 опускается, так как оно может быть проведено по тому же плану, что и доказательство теоремы 4.1 в книге [3, стр. 50].

Из теоремы 3 вытекает ряд следствий, необходимых для последующего доказательства предельных теорем.

Следствие 1. Для числа A -подстановок степени n при $n \rightarrow \infty$ имеем асимптотическую формулу

$$C_{nm}^A = \frac{n!}{r^n} \frac{\exp \left\{ \sum_{j \in A} \frac{r^j}{j} \right\}}{\sqrt{2\pi \sum_{j \in A} j r^j}} (1 + o(1)), \quad (2.4)$$

где r – единственный положительный корень уравнения

$$\sum_{j \in A} r^j = n. \quad (2.5)$$

Формулы (2.4) и (2.5) следуют при $y_j = 1$, $j \in A$, соответственно из равенств (2.2) и (2.3).

Следствие 2. Для производящей функции случайной величины ξ_{nm}^A при $n \rightarrow \infty$ равномерно для всех $x \in W$ имеем асимптотическое представление

$$P_{nm}^A(x) = \left(\frac{r}{R} \right)^n \exp \left\{ \sum_{j \in A} \frac{p_j x + q_j}{j} R^j - \sum_{j \in A} \frac{r^j}{j} \right\} \times \left[\sum_{j \in A} j r^j / \sum_{j \in A} j R^j \right]^{\frac{1}{2}} (1 + o(1)), \quad (2.6)$$

где R и r для любых $x \in W$ – единственные решения уравнений (2.3) и (2.5) соответственно.

Формула (2.6) следует из равенства (2.2) при $x_j = x$, $j \in A$, и формулы (2.4).

Следствие 3. При $l \in A$ и $n \rightarrow \infty$ равномерно для всех $x \in W$ производящая функция случайной величины $\xi_{nm}^A(l)$ имеет асимптотику

$$P_{nm}^A(x;l) = \left(\frac{r}{R_l}\right) \exp \left\{ \sum_{j \in A} \frac{1}{j} (R_l^j - r^j) + \frac{1}{l} p_l (x-1) R_l^l \right\} \times \\ \times \left[\sum_{j \in A} j r^j / \left(\sum_{j \in A} j R_l^j + l p_l R_l^l (x-1) \right) \right] (1 + o(1)), \quad (2.7)$$

где R_l для любого $x \in W$ – единственный корень уравнения

$$\sum_{j \in A} R_l^j + p_l (x-1) R_l^l = n \quad (2.8)$$

и r – корень уравнения (2.5).

Асимптотическая формула (2.7) следует из асимптотики (2.2) при

$$x_j = \begin{cases} 1, & j \neq l, j \in A, \\ x, & j = l \in A, \end{cases}$$

а уравнение (2.8) – из равенства (2.3).

Отметим, что $P_{nm}^A(x;l)$ получается из $P_{nm}^A(x)$ при $x_j = 1, j \neq l; x_l = x$, поэтому $p_j x_j + q_j = 1$ для $j \neq l$ и, значит, $P_{nm}^A(x;l)$ не зависит от выбора $p_j, j \neq l$, в схеме трансформирования циклов, длины которых отличны от l . Фактически это означает, что при рассмотрении трансформированных циклов длины l циклы длины j для всех $j \neq l$ можно рассматривать как нетрансформируемые с вероятностью $p_j = 1, j \neq l$.

3. Предельные теоремы

Рассмотрим теперь предельные теоремы для распределений ξ_{nm}^A и $\xi_{nm}^A(l)$, доказательство которых проводится с использованием теоремы 3 и ее следствий.

Теорема 4. Пусть $0 < p_j \leq 1, p_j + q_j = 1, j \in A$ и r – единственный положительный корень уравнения (2.5). Тогда при $n \rightarrow \infty$:

а) если $p_m \neq 1$, то случайная величина

$$\tilde{\xi}_{nm}^A = \frac{\xi_{nm}^A - \sum_{j \in A} p_j r^j / j}{\sqrt{r^m p_m q_m / m}} \quad (3.1)$$

асимптотически нормальна с параметрами $(0,1)$;

б) если при $m > 3$ для любого $s < m/3$, определяемого условиями

- либо $m-1, \dots, m-s-1 \notin A$, $m-s \in A$,
- либо $p_{m-1}, \dots, p_{m-s-1} = 0$, $p_{m-s} > 0$, $m-s \in A$,

случайная величина

$$\tilde{\xi}_{nm}^A = \frac{\xi_{nm}^A - \sum_{j \in A} r^j / j}{\sqrt{\left[\left(\frac{s}{m} \right)^2 p_{m-s} / (m-s) + \left(1 - \frac{s}{m} \right)^2 q_{m-s} / (m-s) \right] r^{m-s}}} \quad (3.2)$$

асимптотически нормальна с параметрами $(0,1)$.

Для доказательства теоремы рассмотрим функцию

$$f_{nm}(x) = n(\ln r - \ln R) + \left(\sum_{j \in A} (p_j x + q_j) R^j / j - \sum_{j \in A} r^j / j \right) + \frac{1}{2} \ln \left[\sum_{j \in A} j r^j / \sum_{j \in A} j R^j \right]. \quad (3.3)$$

Из следствия 2 при $n \rightarrow \infty$ имеем асимптотическое представление для производящей функции ξ_{nm}^A равномерно для всех $x \in W$

$$P_{nm}^A(x) = e^{f_{nm}(x)} (1 + o(1)). \quad (3.4)$$

Представим $f_{nm}(x)$ в виде суммы

$$f_{nm}(x) = A_{nm}(x) + B_{nm}(x), \quad (3.5)$$

где

$$A_{nm}(x) = n(\ln r - \ln R) + \sum_{j \in A} (p_j x + q_j) R^j / j - \sum_{j \in A} r^j / j, \quad (3.6)$$

$$B_{nm}(x) = \frac{1}{2} \ln \left[\sum_{j \in A} j r^j / \sum_{j \in A} j R^j \right]. \quad (3.7)$$

Для производной R'_x из равенства (2.3) при $x_j = x$, $j \in A$, получаем выражение

$$\frac{R'_x}{R} = - \frac{\sum_{j \in A} p_j R^j}{\sum_{j \in A} j (p_j x + q_j) R^j}. \quad (3.8)$$

Используя эту формулу, из равенства (3.6) получаем выражение для трех первых производных $A'_{nm}(x)$

$$A'_{nm}(x) = \sum_{j \in A} p_j R^j / j, \quad (3.9)$$

$$A''_{nm}(x) = -\frac{\left(\sum_{j \in A} p_j R^j\right)^2}{\sum_{j \in A} j(p_j x + q_j) R^j}, \quad (3.10)$$

$$A'''_{nm}(x) = \frac{\left(\sum_{j \in A} p_j R^j\right)^3}{\sum_{j \in A} j(p_j x + q_j) R^j} + \frac{\left(\sum_{i \in A} p_i R^i\right)^2 \left(\sum_{j \in A} j R^j\right)}{\left[\sum_{j \in A} j(p_j x + q_j) R^j\right]^2}. \quad (3.11)$$

В соответствии с равенством (3.7) имеем выражение для первой производной $B_{nm}(x)$

$$B'_{nm}(x) = \frac{1}{2} \frac{\sum_{i \in A} i^2 R^i \sum_{j \in A} p_j R^j}{\sum_{i \in A} i R^i \sum_{j \in A} j(p_j x + q_j) R^j}. \quad (3.12)$$

Из этого выражения можно получить формулы для производных $B''_{nm}(x)$ и $B'''_{nm}(x)$. Так как входящие в выражения для $B'_{nm}(x)$ суммы являются многочленами от R ограниченной степени и с ограниченными коэффициентами, то $B'_{nm}(x)$ ограничено для всех $x \in W$ при $n \rightarrow \infty$. При дифференцировании по x и возможном умножении при этом на R_x/R свойство ограниченности $B''_{nm}(x)$ и $B'''_{nm}(x)$ для $x \in W$ при $n \rightarrow \infty$ сохраняется.

Поэтому с учетом равенства (3.5) равномерно для всех $x \in W$ при $n \rightarrow \infty$ имеем

$$f'_{nm}(1) = \sum_{j \in A} p_j r^j / j(1 + o(1)), \quad (3.13)$$

$$f''_{nm}(1) = -\frac{\left(\sum_{j \in A} p_j r^j\right)^2}{\sum_{j \in A} j r^j} (1 + o(1)), \quad (3.14)$$

$$f'''_{nm}(1) = O(R^m). \quad (3.15)$$

Полагая $\sigma^2 = f'_{nm}(1) + f''_{nm}(1)$, из равенств (3.13) и (3.15) получаем

$$\sigma^2 = \frac{p_m q_m}{m} r^m (1 + o(1)). \quad (3.16)$$

Разложим теперь функцию $f_{nm}(x)$ по формуле Тейлора в окрестности W точки $x=1$ с остаточным членом в форме Лагранжа

$$f_{nm}(x) = f'_{nm}(1)(x-1) + f''_{nm}(1)(x-1)^2/2 + f'''_{nm}(1 + \theta(x-1))(x-1)^3/3! \quad (3.17)$$

Для $x \in W$ сделаем замену переменной, заменяя x на $e^{t/\sigma}$. Если $W = [1-x_0, 1+x_0]$, то $t \in [\sigma \ln(1-x_0), \sigma \ln(1+x_0)]$. Тогда при $t \in [-\varepsilon, \varepsilon]$, $\varepsilon > 0$, получим равенство

$$f_{nm}(e^{t/\sigma}) = f'_{nm}(1)t/\sigma + (f'_{nm}(1) + f''_{nm}(1))t^2/2\sigma^2 + O(1/r^{m/2}), \quad n \rightarrow \infty. \quad (3.18)$$

Производящая функция моментов $\tilde{\xi}_{nm}^A$ имеет вид

$$M_{nm}(t) = e^{-f'_{nm}(1)t/\sigma P_{nm}^A(e^{t/\sigma})}. \quad (3.19)$$

Поэтому из равенств (2.6), (3.4) и (3.18) получаем

$$M_{nm}(t) = \exp\left\{t^2/2 + O(1/\sqrt{n})\right\}. \quad (3.20)$$

Отсюда следует, что для всех $t \in [-\varepsilon, \varepsilon]$, $\varepsilon > 0$,

$$M_{nm}(t) \rightarrow e^{t^2/2} \quad \text{при } n \rightarrow \infty, \quad (3.21)$$

и справедливость п. а) теоремы 3 вытекает из теоремы Куртисса [3].

Доказательство п. б) теоремы 3 проводится по тому же плану, что и доказательство п. а). Поэтому укажем только некоторые отличия.

Рассмотрим функцию

$$\bar{f}_{nm}(x) = \bar{A}_{nm}(x) + \bar{B}_{nm}(x), \quad (3.22)$$

где $\bar{A}_{nm}(x)$ и $\bar{B}_{nm}(x)$ отличаются, соответственно, от $A_{nm}(x)$ и $B_{nm}(x)$ тем, что A заменяется на $\bar{A} = A \setminus \{m-1, \dots, m-s-1\}$ при выполнении хотя бы одного из условий, указанных в п. б). Кроме того, равномерно для всех $x \in W$ при $n \rightarrow \infty$

$$\bar{f}_{nm}(1) = r^m/m + \sum_{j \in \bar{A}} r^j/j, \quad (3.23)$$

и для

$$\bar{\sigma}^2 = \bar{f}'_{nm}(1) + \bar{f}''_{nm}(1) \quad (3.24)$$

имеем

$$\bar{\sigma}^2 = \left(\frac{r^m}{m} + \frac{p_{m-s} r^{m-s}}{m-s} \right) (1 + o(1)) - \frac{(r^m + p_{m-s} r^{m-s})^2}{m r^m + (m-s) r^{m-s}} (1 + o(1)). \quad (3.25)$$

Отсюда получаем, что при $n \rightarrow \infty$

$$\bar{\sigma}^2 = \left[\left(\frac{s}{m} \right)^2 p_{m-s}/m - s + \left(1 - \frac{s}{m} \right)^2 q_{m-s}/m - s \right] r^{m-s} (1 + o(1)).$$

Так же, как в доказательстве п. а), имеем разложение

$$\bar{f}_{nm}(e^{t/\bar{\sigma}}) = \bar{f}'_{nm}(1)t/\bar{\sigma} + (\bar{f}'_{nm}(1) + \bar{f}''_{nm}(1))t^2/2\bar{\sigma}^2 + O(R^m/\bar{\sigma}^{3/2}), \quad (3.26)$$

из которого для производящей функции моментов

$$\bar{M}_{nm}(t) = e^{-\bar{f}'_{nm}(1)t/\bar{\sigma} P_{nm}^A(e^{t/\bar{\sigma}})}$$

получаем асимптотику

$$\bar{M}_{nm}(t) = \exp \left\{ t^2/2 + O \left(r^{\frac{m-3s}{2}} \right) \right\}.$$

Отсюда следует, что при любом t

$$\bar{M}_{nm}(t) \rightarrow e^{t^2/2} \quad \text{при } n \rightarrow \infty.$$

Отсюда и из теоремы Куртисса следует п. б) теоремы.

Для случайной величины $\xi_{nm}^A(l)$, равной числу нетрансформированных циклов длины l , $1 \leq l \leq m$, в случайной подстановке $s \in G_{nm}^A$, докажем следующую теорему.

Теорема 5. При $n \rightarrow \infty$ предельные распределения $\xi_{nm}^A(l)$ классифицируются следующим образом.

Пусть r – положительный корень уравнения (2.5), тогда:

1) для $0 < l < m$, $p_l = p_l(n)$ имеем

а) если $p_l r^l \rightarrow \infty$, то случайная величина

$$\bar{\xi}_{nm}(l) = \frac{\bar{\xi}_{nm}^A(l) - p_r r^l/l}{\sqrt{p_l r^l/l}}$$

в пределе имеет нормальное распределение с параметрами $(0, 1)$;

б) если $p_l r^l \rightarrow \gamma_l < \infty$, то $\xi_{nm}^A(l)$ имеет предельное распределение Пуассона с параметром $\lambda_l = \gamma_l/l$;

2) для $l = m$, $p_m = p_m(n)$

в) если $p_m r^m \rightarrow \infty$, то случайная величина

$$\bar{\xi}_{nm}(m) = \frac{\xi_{nm}^A(m) - n p_m/m}{\sqrt{n p_m q_m/m}}$$

асимптотически нормальна с параметрами $(0, 1)$;

е) если $p_m r^m \rightarrow \gamma_m > 0$, то $\xi_{nm}^A(m)$ в качестве предельного имеет распределение Пуассона с параметром $\lambda_m = \gamma_m/m$.

Для доказательства п. а) теоремы, используя асимптотическое представление производящей функции $\xi_{nm}^A(l)$ вида (2.7), запишем

$$P_{nm}^A(x; l) = e^{g_{nm}(x; l)} (1 + o(1)), \quad (3.27)$$

где

$$g_{nm}(x; l) = n(\ln r - \ln R_1) + \sum_{j \in A} (R_1^j - r^j) / j + p_l R_1^l (x-1) / l + \\ + \frac{1}{2} \ln \left[\frac{\sum_{j \in A} j r^j}{\sum_{j \in A} j R_1^j + l p_l R_1^l (x-1)} \right], \quad (3.28)$$

R_1 и r – положительные корни уравнений (2.8) и (2.5) соответственно. Оценка остаточного члена в (3.27) при $n \rightarrow \infty$ равномерна по $x \in W$.

Используя равенство (2.8), получим выражение для производной R'_{1x} в виде

$$\frac{R'_{1x}}{R_1} = - \frac{p_l R_1^l}{\sum_{j \in A} j R_1^j + l p_l R_1^l (x-1)}. \quad (3.29)$$

Отсюда следует, что при $n \rightarrow \infty$ равномерно по $x \in W$

$$\frac{R'_{1x}}{R_1} = - \frac{p_l}{m R_1^{m-l}} (1 + o(1)), \\ \frac{R''_{1x}}{R_1} = O\left(\frac{1}{R^{2(m-l)}}\right). \quad (3.30)$$

Из равенства (3.28) получаем выражение для первой производной $g'_{nm}(x; l)$:

$$g'_{nm}(x; l) = \frac{p_l R^l}{l} + \frac{1}{2} \frac{p_l R^l \left[\sum_{j \in A} j^2 R^j + l^2 p_l R^l \right]}{\left[\sum_{j \in A} j R^j + l p_l R^l (x-1) \right]^2} - \frac{1}{2} \frac{l p_l R^l}{\sum_{j \in A} j R^j + l p_l R^l (x-1)}. \quad (3.31)$$

Из соотношений (3.31) и (3.30) следует, что равномерно для всех $x \in W$ при $n \rightarrow \infty$

$$g'_{nm}(x;l) = \frac{p_l R^l}{l} + O\left(\frac{1}{R^{m-l}}\right), \quad (3.32)$$

$$g''_{nm}(x;l) = -\frac{lp_l R^l}{R^{m-l}} + O\left(\frac{1}{R^{2(m-l)}}\right). \quad (3.33)$$

Разложим функцию $g_{nm}(x;l)$ по формуле Тейлора в окрестности W точки $x = 1$ с остаточным членом в форме Лагранжа

$$g_{nm}(x;l) = g'_{nm}(1;l)(x-1) + g''_{nm}(1+\theta(x-1);l)(x-1)^2/2,$$

где $0 < \theta < 1$. Отсюда, используя оценки (3.32) и (3.33), получаем при $n \rightarrow \infty$ равномерно для $x \in W$

$$g_{nm}(x;l) = \frac{p_l r^l}{l}(x-1) \left[1 + O\left(\frac{1}{r^{m-l}}\right) \right]. \quad (3.34)$$

Из равенств (3.27) и (3.34) получаем при $n \rightarrow \infty$ равномерно для $x \in W$ и $0 < l < m$

$$P_{nm}^A(x;l) = \exp\left\{\frac{p_l r^l}{l}(x-1)\right\}(1+o(1)). \quad (3.35)$$

Положим

$$\sigma_1^2 = p_l r^l / l \quad (3.36)$$

и сделаем замену переменной x на e^{t/σ_1} . При выполнении условий п. а) теоремы 5 производящая функция моментов $\bar{\xi}_{nm}(l)$ имеет вид

$$M_{nm}(t;l) = e^{-\frac{p_l r^l t}{l \sigma_1}} P_{nm}^A(e^{t/\sigma_1}; l),$$

и при $n \rightarrow \infty$ для $t \in [-\varepsilon, \varepsilon]$, $\varepsilon > 0$, имеем

$$M_{nm}(t;l) = \exp\left\{t^2/2 + O\left(\frac{1}{\sqrt{p_l r^l}}\right)\right\}.$$

Отсюда следует, что при $n \rightarrow \infty$

$$M_{nm}(t;l) \rightarrow e^{t^2/2}$$

и, стало быть, согласно теореме Куртисса п. а) теоремы доказан.

При выполнении условий п. б) теоремы 5, используя формулу (3.31), нетрудно убедиться, что оценки (3.32) и (3.33) для производных сохраняются. Поэтому из равенства (3.35) при выполнении условий п. б) следует, что

$$P_{nm}^A(x;l) \rightarrow e^{\gamma_l/(x-1)} \quad \text{при } n \rightarrow \infty.$$

В соответствии с теоремой непрерывности для производящих функций п. б) теоремы 5 доказан.

Рассмотрим теперь случай $l = m$ и докажем пп. в) и г) теоремы 5. Из равенства (2.8) при $l = m$ получаем

$$\sum_{j \in A} R_1^j + p_m R_1^m (x-1) = n. \quad (3.37)$$

Отсюда находим, что равномерно по $x \in W$

$$\frac{R'_{1x}}{R_1} = -\frac{p_m}{m(p_m x + q_m)} \left(1 + O\left(\frac{1}{R_1}\right) \right) \text{ при } n \rightarrow \infty. \quad (3.38)$$

Из равенства (3.28) при $l = m$ имеем

$$g'_{nm}(x; m) = \frac{p_m R_1^m}{m} - \frac{1}{2} \frac{\left[\sum_{j \in A} j^2 R_1^j + m^2 (x-1) R_1^m \right] \frac{p_m}{m} + m p_m R_1^m}{\left[\sum_{j \in A} j R_1^j + m p_m (x-1) R_1^m \right] (p_m x + q_m)}. \quad (3.39)$$

Используя это равенство и соотношение (3.38) получаем равномерно по $x \in W$ при $n \rightarrow \infty$

$$g'_{nm}(x; m) = \frac{p_m R_1^m}{m} (1 + o(1)), \quad (3.40)$$

$$g''_{nm}(x; m) = -\frac{p_m^2 R_1^m}{m(p_m x + q_m)} (1 + o(1)).$$

Аналогичным образом получается равномерная оценка для третьей производной

$$g'''_{nm}(x; m) = O(R_1^m). \quad (3.41)$$

Из разложения по формуле Тейлора для $x \in W$

$$g_{nm}(x; m) = g'_{nm}(1; m)(x-1) + g''_{nm}(1; m)(x-1)^2/2 + O\left(R_1^m \frac{(x-1)^3}{3!}\right). \quad (3.42)$$

Полагая

$$\sigma_1^2 = \frac{1}{m} n p_m q_m \quad (3.43)$$

и проводя замену $x \in W$ на e^{t/σ_1} , $t \in [-\varepsilon, \varepsilon]$, $\varepsilon > 0$, получаем

$$g_{nm}(e^{t/\sigma_1}) = \frac{n p_m}{m} \left(t/\sigma_1 + t^2/2\sigma_1^2 + O\left(\frac{1}{\sigma_1^3}\right) \right) - \frac{n p_m^2}{m} \left(t^2/2\sigma_1^2 + O\left(\frac{1}{\sigma_1^3}\right) \right) + O\left(\frac{n}{\sigma_1^{3/2}}\right). \quad (3.44)$$

Из равенства (3.27) при $l = m$, формулы (3.43) и выражения (3.44) следует, что для производящей функции моментов $\bar{\xi}_{nm}(m)$ существует предел

$$M_{nm}(t; m) \rightarrow e^{t^2/2}.$$

Этим п. в) теоремы 5 доказан.

При выполнении условий п. г) теоремы 5 из условия $p_m r^m \rightarrow \gamma_m < \infty$ следует, что $p_m = p_m(n) \rightarrow 0$ при $n \rightarrow \infty$. Значит, при $n \rightarrow \infty$

$$g'_{nm}(x; m) \rightarrow \gamma_m/m, \quad g''_{nm}(x; m) \rightarrow 0.$$

Поэтому из разложения по формуле Тейлора

$$g_{nm}(x; m) = g'_{nm}(1; m)(x-1) + g''_{nm}(1 + \theta(x-1); m)(x-1)^2/2$$

при $n \rightarrow \infty$ имеем $g_{nm}(x; m) = \frac{\gamma_m}{m}(x-1)(1+o(1))$. Следовательно, имеет место сходимость

$$P_{nm}^A(x; m) \rightarrow e^{\gamma_m/m(x-1)}.$$

Таким образом, случайная величина $\xi_{nm}^A(m)$ в качестве предельного имеет закон Пуассона с параметром $\lambda = \gamma_m/m$. П. г) теоремы также доказан.

4. Инволюции и сети мобильной связи

Рассмотрим модель мобильной сети связи с n абонентами, описывающую состояние сети в случайно выбранный момент времени. Если номера абонентов обозначить элементами $1, 2, \dots, n$, то состоянию сети можно поставить в соответствие некоторую случайную инволюцию $s \in S_n$, в которой абонентам i и j ставится в соответствие двухэлементный или 2-цикл (i, j) , если один из этих абонентов набрал номер другого абонента. Остальным абонентам ставятся в соответствие единичные циклы. После набора номера по различным причинам связь абонентов может быть не установлена (занятость вызываемого, удаленность трансмиттеров, разрядка аккумуляторов и др.). В рассматриваемой модели это соответствует действию процесса трансформации двоичных циклов с вероятностью q , при этом нетрансформированные с вероятностью p 2-циклы соответствуют установленным связям между парами абонентов, $p + q = 1$. Случайная величина $\eta_n(p)$, равная числу нетрансформированных 2-циклов в случайной инволюции, определяет число занятых линий в сети.

Известно [3], что число инволюций степени n с r циклами длины 2 равно

$$E_{nr} = \frac{n!}{2^r r! (n-2r)!}, \quad (4.1)$$

т.е. общее число таких инволюций определяется равенством

$$E_n = \sum_{r=0}^{[n/2]} \frac{n!}{2^r r! (n-2r)!}. \quad (4.2)$$

Распределение случайной величины $\eta_n(p)$ имеет вид

$$\mathbf{P}(\eta_n(p) = k) = \frac{1}{E_n} \sum_{r=k}^{[n/2]} E_{nr} \binom{r}{k} p^k q^{r-k}. \quad (4.3)$$

Так как инволюции являются A -подстановками при $A = \{1, 2\}$, то для производящей функции

$$P_n(x; p) = \sum_{k=0}^{[n/2]} \mathbf{P}(\eta_n(p) = k) x^k \quad (4.4)$$

имеем

$$\sum_{n=0}^{\infty} E_n P_n(x; p) \frac{t^n}{n!} = \exp\{(px + q)t^2/2 + t\}. \quad (4.5)$$

При $l = m = 2$ из равенств (3.27) и (3.28) для производящей функции числа $\xi_{n2}(2)$ нетрансформированных 2-циклов равномерно по $x \in W$

$$P_{n2}(x; 2) = e^{g_{n2}(x; 2)} (1 + o(1)) \quad \text{при } n \rightarrow \infty, \quad (4.6)$$

где

$$g_{n2}(x; 2) = n(\ln r_1 - \ln R_1) + (px + q)R_1^2 + R_1 - r_1^2 - r_1 + \\ + \frac{1}{2} \ln n \left[\frac{2r_1^2 + r_1}{2(px + q)R_1^2 + R_1} \right] \quad (4.7)$$

и в соответствии с (3.37)

$$(px + q)R_1^2 + R_1 = n, \quad (4.8)$$

$$r_1^2 + r_1 = n. \quad (4.9)$$

Из (4.8) и (4.9) следует, что при $n \rightarrow \infty$ равномерно по $x \in W$

$$R_1 = \sqrt{\frac{n}{px + q}} - \frac{1}{2(px + q)} + O\left(\frac{1}{\sqrt{n}}\right), \quad (4.10)$$

$$r_1 = \sqrt{n} - \frac{1}{2} + O\left(\frac{1}{\sqrt{n}}\right). \quad (4.11)$$

Теперь из равенств (4.6) и (4.7) можно получить асимптотическое представление для производящей функции $\eta_n(p)$: при $n \rightarrow \infty$ равномерно по $x \in W$

$$P_{n2}(x; 2) = (1 + p(x-1))^{n/2} \times \\ \times \exp\left\{\sqrt{n}\left[(1 + p(x-1))^{-1/2} - 1\right] - \frac{1}{4}\left[(1 + p(x-1))^{-1} - 1\right]\right\} \left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right). \quad (4.12)$$

Теорема 6. При $n \rightarrow \infty$ случайная величина $\eta_n(p)$ имеет следующие предельные распределения:

а) если $0 < p < 1$ и $np \rightarrow \infty$, то случайная величина

$$\bar{\eta}_n(p) = \frac{\eta_n(p) - (n - \sqrt{n})p/2}{\sqrt{npq/2}}$$

асимптотически нормальна $(0, 1)$;

б) если $p = p(n)$ и $np \rightarrow \gamma < \infty$, то $\eta_n(p)$ в пределе имеет распределение Пуассона с параметром $\lambda = \gamma/2$.

Доказательство п. а) нетрудно провести используя асимптотическое представление (4.12). Проведя замену x на $e^{t/\sigma}$, можно получить асимптотическое представление для производящей функции моментов $\bar{\eta}_n(p)$ и, переходя к пределу, в качестве предельного выражения получить производящую функцию моментов нормального распределения с параметрами $(0, 1)$.

Если использовать принятый в работе способ доказательства, то нетрудно убедиться, что функция $g_{n2}(x; 2)$ при $n \rightarrow \infty$ имеет следующее разложение по формуле Тейлора равномерно по $x \in W$

$$g_{n2}(x; 2) = \frac{p}{2}(n - \sqrt{n})(x-1) - \frac{p^2}{2}(n - \sqrt{n})(x-1)^2/2 + O(n). \quad (4.13)$$

Полагая $\bar{\sigma}^2 = (n - \sqrt{n})pq$, из (4.6) и (4.13) получаем асимптотическое представление для производящей функции моментов

$$M_{n2}(t; 2) = e^{\frac{(n - \sqrt{n})p}{2} t} \bar{\sigma} P_{n2}(e^{t/\bar{\sigma}}; 2).$$

Отсюда следует, что

$$M_{n2}(t; 2) \rightarrow e^{t^2/2}, \quad n \rightarrow \infty.$$

Этим п. а) теоремы доказан. Из условий п. б) следует, что $p = p(n) \rightarrow 0$ при $n \rightarrow \infty$. Поэтому из равенства (4.12) получаем

$$P_{n2}(x; 2) = e^{\frac{np}{2}(x-1)} (1 + o(1)).$$

Следовательно, при $n \rightarrow \infty$

$$P_{n2}(x; 2) \rightarrow e^{\frac{\gamma}{2}(x-1)},$$

и п. б) следует из теоремы непрерывности для производящих функций.

Список литературы

1. *Mozer L., Wyman M.* An asymptotics for the Bell numbers // Trans. Roy. Soc. Canada. – 1955. – 49, Sec. 3. – P. 49-54.
2. *Curtiss J.N.* A note on the theory of moment generating functions // Ann. Math. Statist. – 1942. – 13, №3. – P. 430-433.
3. *Сачков В.Н.* Вероятностные методы в комбинаторном анализе. – М. : Наука, 1978.
4. *Sachkov V.N.* Probabilistic methods in combinatorial analysis // Encyclopedia of Mathematics and its Applications. V. 56. – Cambridge Univ. Press, 1997.
5. *Flajolet P., Sedgewick R.* Analytic Combinatorics. – Cambridge Univ. Press, 2009.
6. *Сачков В.Н.* Случайные подстановки с трансформированными циклами // Математические вопросы криптографии. – 2012. – Т. 3, Вып. 4. – С. 127-150.