

УДК 519.212.2

Случайные преобразования множеств с ограничениями на параметры. I

В. Н. Сачков

Академия криптографии Российской Федерации, Москва

Получено 11.X.2010

Рассматриваются случайные отображения $\sigma: X \rightarrow X$ множества X из n элементов с ограничениями на кратность вершин ориентированного графа $\Gamma(\sigma)$, частным случаем которых при $n = 2^l$ являются преобразования, реализуемые регистром сдвига длины l со случайной функцией обратной связи.

Ключевые слова: случайные отображения с ограничениями, регистры сдвига, функция обратной связи

Random mappings of sets with restrictions on parameters. I

V. N. Sachkov

Academy of Cryptography of Russian Federation, Moscow

Abstract. Random mappings $\sigma: X \rightarrow X$ of n -set X with constraints on degrees of vertices in a directed graph $\Gamma(\sigma)$ are considered. Mappings corresponding to the binary shift register of length l with a random feedback function are particular cases of this model.

Key words: random mappings with constraints, shift register, feedback function

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 1, pp. 125–144 (Russian).

Введение

Для орграфа $\Gamma(\sigma)$ преобразования $\sigma: X \rightarrow X$ множества X из n элементов число входящих в вершину дуг называется кратностью этой вершины.

В § 1 работы рассматриваются преобразования σ множества из n элементов, для которых кратности вершин орграфа $\Gamma(\sigma)$ принимают только значения 0, 1, 2. Вторичная спецификация вершин имеет вид $\left[\left[0^r 1^{n-2r} 2^r \right] \right]$, где r — число начальных вершин [2]. Для получения асимптотических формул используется подход, который можно условно назвать методом максимального элемента. В работе находится асимптотика числа E_n преобразований данного вида при $n \rightarrow \infty$. Для случайной величины ξ_n , равной числу начальных вершин $\Gamma(\sigma)$ случайного преобразования вторичной спецификации $\left[\left[0^r 1^{n-2r} 2^r \right] \right]$, найдены также асимптотики среднего и дисперсии

$$\mathbf{M}\xi_n = \frac{n}{2 + \sqrt{2}}(1 + o(1)), \quad \mathbf{D}\xi_n = \frac{n}{8 + 6\sqrt{2}}(1 + o(1))$$

и доказана асимптотическая нормальность с параметрами (0, 1) случайной величины $(\xi_n - \mathbf{M}\xi_n) / \sqrt{\mathbf{D}\xi_n}$.

Пусть V_ℓ — векторное пространство размерности ℓ над полем $GF(2)$, $(x_0, x_1, \dots, x_{\ell-1}) \in V_\ell$, $f(x_0, x_1, \dots, x_{\ell-1})$ — булева функция обратной связи регистра сдвига. В § 2 рассматриваются регистровые преобразования $R: V_\ell \rightarrow V_\ell$:

$$R((x_0, x_1, \dots, x_{\ell-1})) = ((x_1, x_2, \dots, x_{\ell-1}, f(x_0, x_1, \dots, x_{\ell-1}))).$$

Орграф $\Gamma(R)$ преобразования R имеет вторичную спецификацию вершин вида $\left[\left[0^r 1^{n-2r} 2^r \right] \right]$. Найдено выражение для числа начальных вершин r через веса функций $f(0, x_1, \dots, x_\ell)$ и $f(1, x_1, \dots, x_{\ell-1})$.

Для случайной величины η_ℓ , равной числу начальных вершин преобразования R , отвечающего случайным функциям $f(0, x_1, \dots, x_{\ell-1})$ и $f(1, x_1, \dots, x_{\ell-1})$, при $\ell \rightarrow \infty$ найдены асимптотики среднего и дисперсии

$$\mathbf{M}\eta_\ell = 2^{\ell-2}(1 + o(1)), \quad \mathbf{D}\eta_\ell = 2^{\ell-3}(1 + o(1));$$

методом максимального элемента доказана асимптотическая нормальность с параметрами (0, 1) случайной величины $(\eta_\ell - \mathbf{M}\eta_\ell) / \sqrt{\mathbf{D}\eta_\ell}$. Отметим, что асимптотика среднего значения $\mathbf{M}\eta_\ell$ приведена в работе [1].

В § 3 рассматриваются преобразования n -множества, для которых кратности вершин орграфов имеют вторичную спецификацию $[[[0^{\beta_0} d^{\beta_d}]]]$, и в этом случае $\beta_0 = n \left(1 - \frac{1}{d}\right)$, $\beta_d = \frac{n}{d}$. Отдельно рассмотрен случай, когда $d = 2$ и, следовательно, $n = 2m$, $\beta_0 = \beta_1 = m$. Найдена формула для числа $D_{2m,k}(2)$ преобразований $2m$ -множества с вторичной спецификацией кратностей вершин орграфа $[[[0^m 2^m]]]$, орграфы которых имеют k циклических вершин. С использованием этой формулы найдены точное и предельное распределения случайной величины, равной числу циклических вершин случайного отображения данного вида. Предельным, как и для случайных преобразований без ограничений, является распределение Релея.

§ 1. Преобразования регистрового типа

Будем рассматривать класс преобразований n -множества, для которых кратности вершин имеют вторичную спецификацию $[[[0^{\beta_0} 1^{\beta_1} 2^{\beta_2}]]]$. При $n = 2^l$ этот класс содержит преобразования, осуществляемые двоичным регистром сдвига. Поэтому преобразования из данного класса будем называть преобразованиями регистрового типа.

1°. *Точные и асимптотические формулы.*

Если r — число начальных вершин, то вторичная спецификация преобразований n -множества регистрового типа имеет вид $[[[0^r 1^{n-2r} 2^r]]]$. Поэтому для числа $E_n(r)$ преобразований с r начальными вершинами имеем выражение [2]

$$E_n(r) = \text{coef}_{x^r \frac{t^n}{n!}} \left(x + t + \frac{t^2}{2} \right)^n.$$

Отсюда следует, что

$$E_n(r) = \frac{(n!)^2}{2^r (r!)^2 (n-2r)!}, \quad r = 0, 1, \dots, \left[\frac{n}{2} \right], \quad (1.1)$$

и общее число преобразований регистрового типа равно

$$E_n = \sum_{r=0}^{\lfloor n/2 \rfloor} E_n(r), \quad n = 0, 1, \dots, \quad (1.2)$$

где $E_0 = E_1 = E_1(0) = 1$.

Заменим факториалы в формуле (1.1) соответствующими значениями Γ -функции и будем рассматривать функцию $E_n(y)$ со значениями аргумента $y \in [0, [n/2]]$. При натуральных значениях аргумента из этого отрезка она совпадает с $E_n(r)$, $r = 0, 1, \dots, [n/2]$.

При отыскании асимптотической формулы для E_n при $n \rightarrow \infty$ будем использовать прием, связанный с нахождением значения $r_0 \in [0, [n/2]]$, для которого $E_n([r_0])$ принимает максимальное значение. Асимптотическое представление для r_0 при $n \rightarrow \infty$ получается как единственное подходящее решение r_0 квадратного уравнения, вытекающего из соотношения

$$E_n(r+1)/E_n(r) = 1 + o(1).$$

Это позволяет записать равенство

$$\max_{0 \leq r \leq [n/2]} E_n(r) = E_n(r_0)(1 + o(1)). \quad (1.3)$$

Для r_0 можно получить при $n \rightarrow \infty$ следующее асимптотическое представление:

$$r_0 = \frac{n}{2 + \sqrt{2}} - \frac{3 - \sqrt{2}}{2\sqrt{2}} + O\left(\frac{1}{n}\right). \quad (1.4)$$

Доказательство асимптотической формулы для E_n и предельного распределения для числа начальных вершин в случайном преобразовании основываются на следующей лемме.

Лемма 1. Для любого $0 < \varepsilon < \frac{1}{6}$ равномерно для всех $x \in [1 - \delta, 1 + \delta]$, $\delta > 0$, при $n \rightarrow \infty$ для производящей функции

$$f_n(x) = \sum_{k=0}^{[n/2]} E_n(k)x^k \quad (1.5)$$

имеет место асимптотическое представление

$$f_n(x) = E_n(r_0)x^r \sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} x^j e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} (1 + o(1)), \quad (1.6)$$

где r — натуральное число, определяемое неравенствами $r \leq r_0 < r + 1$.

Доказательство. Представим $f_n(x)$ в виде

$$f_n(x) = E_n(r_0)x^r \left[\sum_{j=0}^r \frac{E_n(r-j)}{E_n(r_0)}x^{-j} + \sum_{j=1}^{\lfloor n/2 \rfloor - r} \frac{E_n(r+j)}{E_n(r_0)}x^j \right]. \quad (1.7)$$

При $n \rightarrow \infty$, используя формулу Стирлинга и равенство (1.1), получаем асимптотическое представление

$$\frac{E_n(r-j)}{E_n(r_0)} = e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} (1+o(1)) \quad (1.8)$$

с равномерной по $-n^{\frac{1}{2}+\varepsilon} \leq j \leq n^{\frac{1}{2}+\varepsilon}$ оценкой остаточного члена. Общий вклад для $n^{\frac{1}{2}+\varepsilon} \leq j \leq r$ в первую сумму и для $n^{\frac{1}{2}+\varepsilon} \leq j \leq \lfloor n/2 \rfloor - r$ во вторую сумму в правой части равенства (1.7) имеет порядок $O(ne^{-n^{2\varepsilon}})$ равномерно для всех $x \in [1-\delta, 1+\delta]$. Поэтому из равенств (1.7) и (1.8) следует асимптотическое представление (1.6).

Отметим, что из условия $|r_0 - r| < 1$ при $n \rightarrow \infty$ следует формула

$$r = \frac{n}{2 + \sqrt{2}} \left(1 + O\left(\frac{1}{n}\right) \right), \quad (1.9)$$

совпадающая с аналогичной асимптотикой для r_0 , вытекающей из равенства (1.4).

Лемма 2. При $n \rightarrow \infty$ имеет место асимптотическая формула

$$E_n(r_0) = \frac{1}{\sqrt{\pi}} (\sqrt{2} + 1)^{3/2} \left(\frac{\sqrt{2} + 1}{e} \right)^n n^{n-1/2} (1+o(1)). \quad (1.10)$$

Доказательство. Используя формулу Стирлинга, при $n \rightarrow \infty$ имеем

$$2^{r_0} (r_0!)^2 (n - 2r_0)! = \frac{\sqrt{2\pi} \cdot n \cdot n!}{(\sqrt{2} + 1)^{n+3/2}} (1+o(1)).$$

В соответствии с формулой (1.1) получаем

$$E_n(r_0) = \frac{(n-1)! (\sqrt{2} + 1)^{n+3/2}}{\sqrt{2\pi}} (1+o(1)). \quad (1.11)$$

Применяя формулу Стирлинга, отсюда получаем соотношение (1.10).

В качестве следствия из лемм 1 и 2 получаем асимптотическую формулу для числа E_n преобразований n -множества регистрового типа.

Следствие 1. При $n \rightarrow \infty$ имеет место асимптотика

$$E_n = \sqrt{\frac{e}{\sqrt{2}}} \left(\frac{\sqrt{2}+1}{e} \right)^{n+1/2} n^n (1+o(1)). \quad (1.12)$$

Доказательство. Действительно, при $n \rightarrow \infty$ из равенства (1.6) имеем

$$E_n = f_n(1) = E_n(r_0) \sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} (1+o(1)). \quad (1.13)$$

Заменяя в правой части этого равенства сумму интегралом, находим, что

$$\sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} = \sqrt{n} \int_{-n^\varepsilon}^{n^\varepsilon} e^{-\sqrt{2}(\sqrt{2}+1)^2 y^2} dy (1+o(1)). \quad (1.14)$$

После замены переменной в интеграле и перехода к бесконечным пределам, вносящего погрешность экспоненциально малого характера, получаем

$$\sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} = \frac{1}{\sqrt{2}+1} \sqrt{\frac{n}{2\sqrt{2}}} \int_{-\infty}^{\infty} e^{-\frac{z^2}{2}} dz (1+o(1)).$$

Таким образом,

$$\sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} e^{-\frac{j^2 \sqrt{2}(\sqrt{2}+1)^2}{n}} = \frac{1}{\sqrt{2}+1} \sqrt{\frac{\pi n}{\sqrt{2}}} (1+o(1)). \quad (1.15)$$

Теперь из равенств (1.10), (1.13) и (1.15) находим, что

$$E_n = \sqrt{1 + \frac{1}{\sqrt{2}}} \left(\frac{\sqrt{2}+1}{e} \right)^n n^n (1+o(1)). \quad (1.16)$$

Отсюда после очевидных преобразований получаем формулу (1.12).

2°. Точные и предельные распределения

На множестве всех преобразований n -множества регистрового типа зададим равномерное вероятностное распределение и рассмотрим случайную величину ξ_n , равную числу начальных вершин орграфа случайного преобразования. Точное распределение ξ_n с учетом равенств (1.1) и (1.2) имеет вид

$$\mathbf{P}(\xi_n = r) = \frac{E_n(r)}{E_n}, \quad r = 0, 1, \dots, \left[\frac{n}{2} \right]. \quad (1.17)$$

Производящая функция ξ_n определяется равенством

$$P_n(x) = \frac{f_n(x)}{f_n(1)}, \quad n = 1, 2, \dots \quad (1.18)$$

Из равенств (1.6) и (1.10) получаем следующую лемму.

Лемма 3. При $n \rightarrow \infty$ для любого $0 < \varepsilon < 1/6$ при $r \leq r_0 < r + 1$ имеет место асимптотическое представление

$$P_n(x) = x^r (\sqrt{2} + 1) \sqrt{\frac{\sqrt{2}}{\pi n}} \sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} x^j e^{\frac{-j^2 \sqrt{2} (\sqrt{2}+1)^2}{n}} (1 + o(1)), \quad (1.19)$$

где остаточный член стремится к нулю равномерно для всех $x \in [1 - \delta, 1 + \delta]$, $\delta > 0$.

Для первых двух производных $f_n(x)$ в точке $x = 1$ можно получить при $n \rightarrow \infty$ асимптотические оценки, аналогичные (1.6), с использованием которых, а также формул (1.10), (1.12) и (1.18), можно вывести асимптотические представления для среднего и дисперсии случайной величины ξ_n

$$\begin{aligned} \mathbf{M}\xi_n &= \frac{n}{2 + \sqrt{2}} (1 + o(1)), \\ \mathbf{D}\xi_n &= \frac{n}{8 + 6\sqrt{2}} (1 + o(1)). \end{aligned} \quad (1.20)$$

Теорема 1. При $n \rightarrow \infty$ распределение случайной величины

$$\xi'_n = (\xi_n - \mathbf{M}\xi_n) / \sqrt{\mathbf{D}\xi_n} \quad (1.21)$$

сходится к нормальному распределению с параметрами $(0, 1)$.

Доказательство. Для производящей функции моментов $M_n(t)$ случайной величины ξ_n с учетом равенства $M_n(t) = P_n(e^t)$ для всех $t \in [-\gamma, \gamma]$, $\gamma > 0$, в соответствии с леммой 3 имеем асимптотическое представление при $n \rightarrow \infty$

$$M_n\left(\frac{t}{\sqrt{n}}\right) = e^{\frac{rt}{\sqrt{n}}} \sqrt{\frac{4 + 3\sqrt{2}}{\pi n}} \sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} e^{-\frac{(4+3\sqrt{2})t^2}{n} + \frac{jt}{\sqrt{n}}} (1 + o(1)). \quad (1.22)$$

Заменяя сумму интегралом, имеем

$$M_n\left(\frac{t}{\sqrt{n}}\right) = e^{\frac{rt}{\sqrt{n}}} \sqrt{\frac{4 + 3\sqrt{2}}{\pi}} \int_{-n^\varepsilon}^{n^\varepsilon} e^{-(4+3\sqrt{2})y^2 + yt} dy (1 + o(1)).$$

Переход к бесконечным пределам интегрирования вносит при $n \rightarrow \infty$ погрешность экспоненциально малого характера, поэтому с учетом равенства

$$\sqrt{2\pi} = \int_{-\infty}^{\infty} e^{-\frac{z^2}{2}} dz \quad (1.23)$$

получаем

$$M_n\left(\frac{t}{\sqrt{n}}\right) = e^{\frac{rt}{\sqrt{n}}} e^{t^2/2(8+6\sqrt{2})} (1+o(1)). \quad (1.24)$$

Сделаем замену переменной

$$z = \frac{t}{\sqrt{8+6\sqrt{2}}},$$

получаем

$$e^{-r \cdot z \sqrt{\frac{8+6\sqrt{2}}{n}}} M_n\left(z \sqrt{\frac{8+6\sqrt{2}}{n}}\right) = e^{\frac{z^2}{2}} (1+o(1)). \quad (1.25)$$

Левая часть последнего равенства представляет собой производящую функцию моментов $\overline{M}_n(x)$ случайной величины $\xi'_n(z)$. Так как при $n \rightarrow \infty$

$$\overline{M}_n(x) \rightarrow e^{\frac{x^2}{2}}, \quad (1.26)$$

то теорема доказана.

§ 2. Регистровые преобразования

Пусть V_ℓ — ℓ -мерное векторное пространство над полем $GF(2)$. Преобразование

$$R: V_\ell \rightarrow V_\ell \quad (2.1)$$

называется регистровым с функцией обратной связи

$$f: V_\ell \rightarrow GF(2), \quad (2.2)$$

если для любого вектора $(x_0, x_1, \dots, x_{\ell-1}) \in V_\ell$ выполнено равенство

$$R((x_0, x_1, \dots, x_{\ell-1})) = ((x_1, x_2, \dots, x_{\ell-1}, f(x_0, x_1, \dots, x_{\ell-1}))). \quad (2.3)$$

Так как регистровое преобразование является преобразованием регистрового типа, то его орграф $\Gamma(R)$ имеет вторичную спецификацию

$\left[\left[0^r 1^{2^\ell - 2^r} 2^r \right] \right]$, зависящую от одного параметра r : числа начальных вершин. Значение параметра r зависит от свойств функции обратной связи f . Для установления этой зависимости рассмотрим разложение функции f по переменной x_0 следующего вида:

$$f(x_0, x_1, \dots, x_{\ell-1}) = \varphi(x_1, \dots, x_{\ell-1}) \oplus x_0 \psi(x_1, \dots, x_{\ell-1}), \quad (2.4)$$

где

$$\varphi(x_1, \dots, x_{\ell-1}) = f(0, x_1, \dots, x_{\ell-1}), \quad (2.5)$$

$$\psi(x_1, \dots, x_{\ell-1}) = f(0, x_1, \dots, x_{\ell-1}) \oplus f(1, x_1, \dots, x_{\ell-1}) \quad (2.6)$$

и \oplus — знак сложения в поле $GF(2)$.

Лемма 4. Величина r , равная числу начальных вершин орграфа $\Gamma(R)$ регистрового преобразования с функцией обратной связи f , существенно зависящей от переменной x_0 , определяется равенством

$$r = \left| \{ (x_1, \dots, x_{\ell-1}) : \psi(x_1, \dots, x_{\ell-1}) = 0 \} \right|. \quad (2.7)$$

Доказательство. Действительно, если $\psi(x_1, \dots, x_{\ell-1}) = 0$, то для любого $x_0 \in GF(2)$ имеем

$$R((x_0, x_1, \dots, x_{\ell-1})) = (x_1, x_2, \dots, x_{\ell-1}, \varphi(x_1, \dots, x_{\ell-1})) \quad (2.8)$$

и, следовательно, для любого x_0 имеет место соотношение

$$R((x_0, x_1, \dots, x_{\ell-1})) \neq (x_1, x_2, \dots, x_{\ell-1}, \varphi(x_1, \dots, x_{\ell-1}) \oplus 1). \quad (2.9)$$

Это означает, что для орграфа $\Gamma(R)$ вершина $(x_1, x_2, \dots, x_{\ell-1}, \varphi(x_1, \dots, x_{\ell-1}) \oplus 1)$ является начальной.

Обратно, если вершина $(x_1, x_2, \dots, x_{\ell-1}, \varphi(x_1, \dots, x_{\ell-1}) \oplus 1)$ начальная, то выполнено соотношение (2.9), а, следовательно, и равенство (2.8), из которого вытекает, что $\psi(x_1, \dots, x_{\ell-1}) = 0$.

Будем предполагать, что таблица истинности функции f представляет собой реализацию бернуллиевской последовательности с вероятностями появления единиц и нулей, равными p и q соответственно и, стало быть, таблица истинности для функции $f(0, x_1, \dots, x_{\ell-1}) \oplus f(1, x_1, \dots, x_{\ell-1}) \oplus 1$ также является бернуллиевской последовательностью с вероятностями появления единиц и нулей соответственно, равными $p^2 + q^2$ и $2pq$. Рассмотрим множество

$$W_\ell^{(r)} = \{ f : \| f(0, x_1, \dots, x_{\ell-1}) \oplus f(1, x_1, \dots, x_{\ell-1}) \oplus 1 \| = r \},$$

где символ $\|\cdot\|$ означает вес соответствующей булевой функции. Если $G_\ell(r)$ — число регистровых преобразований с r начальными вершинами в их орграфах, то, согласно лемме 4,

$$G_\ell(r) = |W_\ell^{(r)}|, \quad r = 0, 1, \dots, 2^{\ell-1}.$$

При указанных предположениях относительно таблиц истинности булевой функции $f(0, x_1, \dots, x_{\ell-1}) \oplus f(1, x_1, \dots, x_{\ell-1}) \oplus 1$ случайная величина $\eta_\ell = \eta_\ell(p^2 + q^2)$, равная весу этой функции, имеет биномиальное распределение

$$\mathbf{P}(\eta_\ell = r) = \binom{2^{\ell-1}}{r} (p^2 + q^2)^r (2pq)^{2^{\ell-1}-r}, \quad r = 0, 1, \dots, 2^{\ell-1}$$

со средним и дисперсией

$$\mathbf{M}\eta_\ell = 2^{\ell-1}(p^2 + q^2), \quad \mathbf{D}\eta_\ell = 2^{\ell-1}(p^2 + q^2)(2pq);$$

стало быть, распределение случайной величины $\frac{\eta_\ell - 2^{\ell-1}(p^2 + q^2)}{\sqrt{2^{\ell-1}(p^2 + q^2)(2pq)}}$ при $\ell \rightarrow \infty$ сходится к нормальному распределению с параметрами $(0, 1)$. Для сбалансированной случайной функции $f(x_0, x_1, \dots, x_{\ell-1})$ параметры нормировки $(2^{\ell-2}, \sqrt{2^{\ell-3}})$.

Отметим, что из вида распределения вершин нулевой кратности $\Gamma(R)$ следуют очевидным образом выражения для распределений вершин кратностей 1 и 2.

Метод максимального элемента для доказательства предельного распределения числа начальных вершин можно применить и к регистровым преобразованиям при различных видах распределения веса случайной функции обратной связи.

В качестве иллюстрации такого применения приведем вывод указанного выше предельного распределения $\eta_\ell = \eta_\ell\left(\frac{1}{2}\right)$ при $\ell \rightarrow \infty$. Рассмотрим производящую функцию

$$f_\ell(x) = \sum_{r=0}^{2^{\ell-1}} G_\ell(r) x^r.$$

Если величина r_0 определяется равенством при $\ell \rightarrow \infty$

$$G_\ell(r_0) = \max_{0 \leq r \leq 2^{\ell-1}} G_\ell(r),$$

то очевидно, что

$$r_0 = 2^{\ell-2} (1 + o(1))$$

и, следовательно,

$$G_\ell(r_0) = \left(\frac{2^{\ell-1}}{2^{\ell-2}} \right) 2^{2^{\ell-1}} (1 + o(1)).$$

Как и в лемме 1, можно установить, что при $\ell \rightarrow \infty$ для любого $0 < \varepsilon < \frac{1}{6}$ существует такое $\delta > 0$, что равномерно для всех $x \in [1 - \delta, 1 + \delta]$ имеет место асимптотическое представление

$$f_\ell(x) = x^r G_\ell(r_0) \sum_{j=-2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}}^{2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}} x^j e^{-\frac{j^2}{2^{\ell-2}}} (1 + o(1)),$$

где $r \leq r_0 < r + 1$, r — натуральное число.

Отсюда следует асимптотическое представление для производящей функции случайной величины η_ℓ

$$P_\ell(x) = \frac{x^{2^{\ell-2}}}{\sqrt{\pi} 2^{\ell-2}} \sum_{j=-2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}}^{2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}} x^j e^{-\frac{j^2}{2^{\ell-2}}} (1 + o(1))$$

с равномерной оценкой остаточного члена для всех $x \in [1 - \delta, 1 + \delta]$, $\delta > 0$. Из этого соотношения следует, что существует такое $\theta > 0$, что для любых $t \in [-\theta, \theta]$, $\theta > 0$, справедливо асимптотическое представление

$$P_\ell \left(e^{\frac{t}{\sqrt{2^{\ell-2}}}} \right) = \frac{1}{\sqrt{\pi} 2^{\ell-2}} e^{\frac{2^{\ell-2}}{\sqrt{2^{\ell-2}}} t} \sum_{j=-2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}}^{2^{\left(\frac{1}{2}+\varepsilon\right)(\ell-2)}} e^{-\frac{j^2}{2^{\ell-2}} + \frac{jt}{\sqrt{2^{\ell-2}}}} (1 + o(1)).$$

Заменяя сумму интегралом, отсюда получаем, что

$$P_\ell \left(e^{\frac{t}{\sqrt{2^{\ell-2}}}} \right) e^{-\frac{2^{\ell-2}}{\sqrt{2^{\ell-2}}} t} = \frac{1}{\sqrt{\pi}} \int_{-2^{\varepsilon(\ell-2)}}^{2^{\varepsilon(\ell-2)}} e^{-y^2 + yt} dy (1 + o(1)).$$

Переходя в интеграле к бесконечным пределам и внося при этом погрешность экспоненциально малого характера, получаем

$$P_\ell \left(e^{\frac{t}{\sqrt{2^{\ell-2}}}} \right) e^{-\frac{2^{\ell-2}}{\sqrt{2^{\ell-2}}t}} = \frac{1}{\sqrt{\pi}} e^{\frac{t^2}{4}} \int_{-\infty}^{\infty} e^{-(y-\frac{t}{2})^2} dy (1+o(1)).$$

После замены переменной под знаком интеграла и использования известной формулы (1.23) для интеграла от экспоненциальной функции получаем

$$P_\ell \left(e^{\frac{t}{\sqrt{2^{\ell-2}}}} \right) e^{-\frac{2^{\ell-2}}{\sqrt{2^{\ell-2}}t}} = e^{\frac{t^2}{4}} (1+o(1)).$$

Проводя замену переменной $t = \sqrt{2}\omega$, находим, что при $\ell \rightarrow \infty$

$$P_\ell \left(e^{\frac{\omega}{\sqrt{2^{\ell-3}}}} \right) e^{-\frac{2^{\ell-2}}{\sqrt{2^{\ell-3}}}\omega} \rightarrow e^{\frac{\omega^2}{2}}.$$

Левая часть этого соотношения представляет собой производящую функцию моментов случайной величины $(\eta_\ell - 2^{\ell-2}) / \sqrt{2^{\ell-3}}$. Поэтому из соотношения следует, что эта случайная величина асимптотически нормальна с параметрами $(0, 1)$.

§ 3. d -ичные преобразования

Преобразование σ n -множества будем называть d -ичным с параметром d , если орграф $\Gamma(\sigma)$ имеет вторичную спецификацию вида $[[0^{\beta_0} d^{\beta_d}]]$. В этом

случае очевидно, что $\beta_0 = n \left(1 - \frac{1}{d}\right)$, $\beta_d = \frac{n}{d}$.

Если $D_n(d)$ — число d -ичных преобразований с параметром d , то [2]

$$D_n(d) = \text{coef}_{t^n/n!} \left(1 + \frac{t^d}{d!} \right)^n$$

и, следовательно,

$$D_n(d) = \begin{cases} \binom{n}{n/d} \frac{n!}{(d!)^{n/d}}, & d | n, \\ 0, & d \nmid n. \end{cases} \quad (3.1)$$

Свободные деревья с n вершинами, имеющие вторичную спецификацию $\left[\left[0^{\beta_0} d^{\beta_d} \right] \right]$, называются d -ичными с параметром d . Для числа таких деревьев имеем следующее выражение [2]:

$$\tilde{T}_n(d) = \text{coef}_{t^{n-2}/(n-2)!} \left(1 + \frac{t^d}{d!} \right)^n.$$

Так как в этом случае $\beta_0 = n - \frac{n-2}{d}$, $\beta_d = \frac{n-2}{d}$, то

$$\tilde{T}_n(d) = \begin{cases} \binom{n}{(n-2)/d} \frac{(n-2)!}{(d!)^{(n-2)/d}}, & d \mid n-2, \\ 0, & d \nmid n-2. \end{cases} \quad (3.2)$$

Отметим, что при $d > 2$ требования к числу n : $d \mid n$ и $d \mid n-2$, необходимые для существования как двоичных преобразований, так и свободных d -ичных деревьев с параметром d , являются несовместимыми. Совместимость имеет место в единственном случае, когда $d = 2$ и для преобразований имеем $\beta_0 = \beta_2 = m$, $n = 2m$, а для свободных деревьев $\beta_0 = m+1$, $\beta_2 = m-1$, $n = 2m$. При $d = 2$ d -ичные преобразования и деревья будем называть двоичными. Соответствующие формулы для числа двоичных преобразований и свободных двоичных деревьев имеют вид

$$D_{2m}(2) = \binom{2m}{m} \frac{(2m)!}{2^m}, \quad (3.3)$$

$$\tilde{T}_{2m}(2) = \binom{2m}{m-1} \frac{(2m-2)!}{2^{m-1}}. \quad (3.4)$$

Так как при изучении двоичных преобразований представляют интерес только такие корневые двоичные деревья, которые являются составными частями орграфов двоичных преобразований, то в качестве корней в свободных деревьях могут выбираться только начальные вершины. Отсюда следует, что для числа корневых двоичных деревьев имеет место следующее выражение:

$$T_{2m}(2) = (m+1) \binom{2m}{m-1} \frac{(2m-2)!}{2^{m-1}}. \quad (3.5)$$

Последнюю формулу можно представить в виде

$$T_{2m}(2) = \frac{(2m)!}{2^{m-1}} C_{m-1}, \quad (3.6)$$

где C_{m-1} — числа Каталана, которым соответствует производящая функция [2]

$$\sum_{m=1}^{\infty} C_{m-1} t^m = \frac{1}{2} [1 - (1 - 4t)^{1/2}], \quad |t| < \frac{1}{4}. \quad (3.7)$$

Обозначим через $D_{2m,k}(2)$ число преобразований $2m$ -множества вторичной спецификации $[[0^m 2^m]]$, орграфы которых имеют k циклических вершин. Орграфы таких преобразований получаются из корневых деревьев вторичной спецификации такого же вида после соединения корней дугами в соответствии с некоторой подстановкой степени k . В соответствии с этим, учитывая формулу (3.6), получаем

$$D_{2m,k}(2) = \frac{(2m)!}{2^{m-k}} \sum_{\substack{m_1+\dots+m_k=m \\ m_i \geq 1}} C_{m_1-1} \dots C_{m_k-1}. \quad (3.8)$$

Из равенства (3.7) следует соотношение

$$\sum_{m=k}^{\infty} t^m \frac{(2m)!}{2^{m-k}} \sum_{\substack{m_1+\dots+m_k=m \\ m_i \geq 1}} C_{m_1-1} \dots C_{m_k-1} = \frac{1}{2^k} [1 - (1 - 4t)^{1/2}]^k. \quad (3.9)$$

Из равенства (3.8) находим, что

$$\sum_{\substack{m_1+\dots+m_k=m \\ m_i \geq 1}} C_{m_1-1} \dots C_{m_k-1} = (-1)^m 2^{2m-k} \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{j/2}{m}. \quad (3.10)$$

Теперь из равенств (3.8) и (3.10) следует, что

$$D_{2m,k}(2) = (-1)^m 2^m (2m)! \sum_{j=0}^k (-1)^j \binom{k}{j} \binom{j/2}{m}, \quad k = 1, 2, \dots, m. \quad (3.11)$$

Формула (3.11) неудобна как для вычислений, так и получения из нее асимптотических оценок. Для преобразования этой формулы к приемлемому виду заметим, что при $m \geq 1$ и $k \leq m$ имеем $\left\lfloor \frac{k}{2} \right\rfloor < m$ и, следовательно,

$$\sum_{\nu=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k}{2\nu} \binom{\nu}{m} = 0, \quad k \leq m. \quad (3.12)$$

Поэтому из равенств (3.11) и (3.12) следует, что

$$D_{2m,k}(2) = (-1)^{m-1} 2^m (2m)! \sum_{\nu=0}^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k}{2\nu+1} \binom{\nu+1/2}{m}. \quad (3.13)$$

По определению биномиальных коэффициентов общего вида

$$\binom{\nu + 1/2}{m} = \frac{(-1)^{m-\nu-1} (2\nu + 1)! (2m - 2\nu - 2)!}{2^{2m} m! \nu! (m - \nu - 1)!}. \quad (3.14)$$

С использованием соотношения (3.14) из равенства (3.13) получаем окончательную формулу

$$D_{2m,k}(2) = \frac{(2m)!}{2^{m-1} m!} \sum_{\nu=0}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^\nu}{\nu!} (k)_{2\nu+1} (2m - 2\nu - 2)_{m-\nu-1}, \quad k = 1, 2, \dots, m. \quad (3.15)$$

При $k = 1$ из формулы (3.15), как и следовало ожидать, вытекает формула (3.5).

На совокупности преобразований $2m$ -множества вторичной спецификации $\left[\left[0^n 2^m \right] \right]$ зададим равномерное вероятностное распределение и рассмотрим случайную величину κ_{2m} , равную числу циклических элементов случайного отображения из рассматриваемой совокупности. Вероятностное распределение κ_{2m} имеет вид

$$\mathbf{P}(\kappa_{2m} = k) = \frac{(m-1)!}{(2m-1)!} \sum_{\nu=0}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^\nu}{\nu!} (k)_{2\nu+1} (2m - 2\nu - 2)_{m-\nu-1}, \quad k = 1, 2, \dots, m. \quad (3.16)$$

После несложных преобразований отсюда следует, что

$$\mathbf{P}(\kappa_{2m} = k) = \frac{k}{2m-1} \sum_{\nu=1}^{\lfloor \frac{k}{2} \rfloor} \frac{(-1)^\nu (k-1)_{2\nu} (m-1)_\nu}{\nu! (2m-2)_{2\nu}}, \quad k = 1, 2, \dots, m. \quad (3.17)$$

Из точного распределения κ_{2m} вида (3.17) вытекает предельная теорема.

Теорема 2. При $n = 2m$ и $n \rightarrow \infty$ для любого $0 < \varepsilon < \frac{1}{8}$ для всех $0 < x < n^{\frac{1}{2}-\varepsilon}$ таких, что $x\sqrt{n}$ — натуральное число, имеем

$$\mathbf{P}\left(\frac{\kappa_n}{\sqrt{n}} = x\right) = xe^{-\frac{x^2}{2}} \frac{1}{\sqrt{n}} (1 + o(1)). \quad (3.18)$$

Действительно, из формулы (3.16) при выполнении условий теоремы имеем

$$\mathbf{P}\left(\frac{\kappa_n}{\sqrt{n}} = x\right) = \frac{x}{\sqrt{n}} \left[\sum_{\nu=0}^{\lfloor \frac{1}{4}-2\varepsilon \rfloor} \frac{(-1)^\nu}{\nu!} \left(\frac{x^2}{2}\right)^\nu + o(1) \right].$$

Отсюда, переходя к пределу при $n \rightarrow \infty$, получаем соотношение (3.18).
Из равенства (3.18) в качестве следствия получаем, что

$$\mathbf{P}\left(\frac{\kappa_n}{\sqrt{n}} \leq \alpha\right) = \left(1 - e^{-\frac{\alpha^2}{2}}\right)(1 + o(1)). \quad (3.19)$$

Для определения среднего и дисперсии κ_{2m} рассмотрим двойную производящую функцию

$$F(t, x) = \sum_{m=1}^{\infty} t^m \sum_{k=1}^{\infty} \frac{2^m}{(2m)!} D_{2m,k}(2) x^k. \quad (3.20)$$

Из равенства (3.8) имеем

$$F(t, x) = \sum_{k=1}^{\infty} x^k 2^k \sum_{m=k}^{\infty} t^m \sum_{\substack{m_1+\dots+m_k=m \\ m_i \geq 1}} C_{m_1-1} \dots C_{m_k-1}.$$

Отсюда с учетом соотношения (3.9) получаем

$$F(t, x) = \sum_{k=1}^{\infty} x^k \left[1 - (1 - 4t)^{1/2}\right]^k. \quad (3.21)$$

Полагая

$$\frac{2^m}{(2m)!} D_{2m,0}(2) = \begin{cases} 1, & m = 0, \\ 0, & m > 0, \end{cases}$$

из равенства (3.21) находим, что при $|t| < \frac{1}{4}$ имеет место следующее выражение для двойной производящей функции:

$$F(t, x) = \frac{1}{1 - x \left[1 - (1 - 4t)^{1/2}\right]}. \quad (3.22)$$

Дифференцируя по x обе части равенства (3.22), получаем

$$F'_x(t, x)|_{x=1} = (1 - 4t)^{-1} - (1 - 4t)^{-1/2}. \quad (3.23)$$

Так как из формулы (3.22) следует, что

$$F(t, 1) = (1 - 4t)^{-1/2} = \sum_{m=0}^{\infty} \binom{2m}{m} t^m,$$

то из равенства (3.23) находим, что

$$F'_x(t, x)|_{x=1} = \sum_{m=1}^{\infty} \left[4^m - \binom{2m}{m}\right] t^m. \quad (3.24)$$

С другой стороны,

$$F'_x(t, x)|_{x=1} = \sum_{m=1}^{\infty} t^m \frac{2m}{(2m)!} \sum_{k=1}^m k D_{2m,k}(2). \quad (3.25)$$

Поэтому из равенств (3.24) и (3.25) получаем формулу для среднего значения κ_{2m} :

$$\mathbf{M} \kappa_{2m} = \frac{2^{2m}}{\binom{2m}{m}} - 1.$$

Отсюда, применяя формулу Стирлинга, получаем

$$\mathbf{M} \kappa_n = \sqrt{\pi m} (1 + o(1)), \quad m \rightarrow \infty.$$

Так как $n = 2m$, то окончательное выражение для асимптотики при $n \rightarrow \infty$ имеет вид

$$\mathbf{M} \kappa_n = \sqrt{\frac{\pi n}{2}} (1 + o(1)). \quad (3.26)$$

Аналогичным образом, находя выражение для второй производной $F''(t, x)$ при $x = 1$, можно получить асимптотику для дисперсии

$$\mathbf{D} \kappa_n = \left(2 - \frac{\pi}{2}\right) n (1 + o(1)). \quad (3.27)$$

Предельная теорема данного параграфа и асимптотические формулы (3.26) и (3.27) показывают, что при $n \rightarrow \infty$ предельное распределение числа циклических элементов, а также среднее и дисперсия даже при почти максимально возможных ограничениях на вторичную спецификацию вершин орграфа имеют такие же выражения, как и при отсутствии каких-либо ограничений.

§ 4. Двоичные регистры сдвига

Рассмотрим регистры сдвига, которым соответствуют двоичные преобразования. Пусть регистр сдвига с функцией обратной связи f вида (2.2) определяет отображение R , удовлетворяющее условиям (2.1) и (2.3).

Лемма 5. *Вершины орграфа отображения $R: V_\ell \rightarrow V_\ell$ регистра сдвига с функцией обратной связи $f(x_0, x_1, \dots, x_{\ell-1})$ имеют вторичную спецификацию $\left[\left[0^{2^{\ell-1}} 2^{2^{\ell-1}} \right] \right]$ тогда и только тогда, когда переменная x_0 является несущественной для функции f .*

Рассмотрим разложение функции f по переменной x_0 вида (2.4) с условиями (2.5) и (2.6). Если переменная x_0 несущественна для функции f , то $\psi(x_1, \dots, x_{\ell-1}) \equiv 0$ для всех $x_1, x_2, \dots, x_{\ell-1}$. Следовательно,

$$R(x_0, x_1, \dots, x_{\ell-1}) = (x_1, \dots, x_{\ell-1}, f(0, x_1, \dots, x_{\ell-1})) \quad (4.1)$$

для всех $x_1, x_2, \dots, x_{\ell-1}$. Отсюда вытекает, что для всех $x_1, x_2, \dots, x_{\ell-1}$

$$R(x_0, x_1, \dots, x_{\ell-1}) \neq (x_1, \dots, x_{\ell-1}, f(x_0, x_1, \dots, x_{\ell-1})). \quad (4.2)$$

Таким образом, для любого набора $x_1, x_2, \dots, x_{\ell-1}$ вершина $(x_1, \dots, x_{\ell-1}, f(0, x_1, \dots, x_{\ell-1}) \oplus 1)$ является начальной. Стало быть, общее число начальных вершин равно $2^{2^{\ell-1}}$, а значит, число вершин кратности 2 равно $2^{2^{\ell-1}}$.

Пусть теперь вершины орграфа преобразования R , соответствующего регистру сдвига, имеют вторичную спецификацию $\left[\left[0^{2^{\ell-1}} 2^{2^{\ell-1}} \right] \right]$. Тогда для каждого набора $x_1, x_2, \dots, x_{\ell-1}$ имеет место либо соотношение (4.1), либо соотношение (4.2). Из равенств (2.4) и (2.6) следует, что $\psi(x_1, \dots, x_{\ell-1}) \equiv 0$. Это означает, что переменная x_0 несущественна для функции f .

§ 5. Деревья с ограниченной вторичной спецификацией вершин

Для свободных деревьев с n вершинами для вторичной спецификации $\left[\left[0^{\beta_0} 1^{\beta_1} 2^{\beta_2} \right] \right]$ имеем $\beta_0 = r$, $\beta_1 = n - 2r + 2$, $\beta_2 = r - 2$. Если $\tilde{T}_n^{(2)}(r)$ — число свободных деревьев вторичной спецификации $\left[\left[0^r 1^{n-2r+2} 2^{r-2} \right] \right]$, то

$$\tilde{T}_n^{(2)}(r) = \text{coef}_{x^r t^{n-2r+2} / (n-2)!} \left(x + t + \frac{t^2}{2} \right)^n.$$

Отсюда следует формула

$$\tilde{T}_n^{(2)}(r) = \frac{n!(n-2)!}{2^{r-2} r! (r-2)! (n-2r+2)!}, \quad r = 2, 3, \dots, \left\lfloor \frac{n}{2} \right\rfloor + 1. \quad (5.1)$$

Корневые деревья вторичной спецификации $\left[\left[0^r 1^{n-2r+2} 2^{r-2} \right] \right]$ являются составными частями орграфов преобразований вторичной спецификации $\left[\left[0^r 1^{n-2r} 2^r \right] \right]$, поэтому в качестве корней могут выбираться только r началь-

ных вершин. Если $T_n^{(2)}(r)$ — число n -вершинных деревьев с r вершинами нулевой кратности, одна из которых корневая, то

$$T_n^{(2)}(r) = \frac{n!(n-2)!}{2^{r-2}(r-1)!(r-2)!(n-2-r+2)!}, \quad r = 2, 3, \dots, \left\lfloor \frac{n}{2} \right\rfloor + 1. \quad (5.2)$$

Общее число корневых деревьев рассматриваемого вида равно

$$T_n^{(2)} = \sum_{r=1}^{\left\lfloor \frac{n}{2} \right\rfloor + 1} T_n^{(2)}(r).$$

Для асимптотической оценки $T_n^{(2)}$ при $n \rightarrow \infty$ применим такой же способ, как при выводе формулы (1.12) для величины E_n . Положим

$$\max_{2 \leq r \leq \left\lfloor \frac{n}{2} \right\rfloor + 1} T_n^{(2)}(r) = T_n^{(2)}(r_0).$$

Можно показать, что r_0 определяется единственным образом и при $n \rightarrow \infty$

$$r_0 = \frac{n}{2 + \sqrt{2}} \left(1 + O\left(\frac{1}{n}\right) \right).$$

С использованием равенства (5.2) и формулы Стирлинга находим, что

$$T_n^{(2)}(r_0) = \frac{(\sqrt{2} + 1)^{n+1/2} (n-2)!}{\pi} (1 + o(1)).$$

Лемма 6. Для любого $0 < \varepsilon < \frac{1}{2}$ равномерно для всех $x \in [1 - \delta, 1 + \delta]$, $\delta > 0$, при $n \rightarrow \infty$ для производящей функции

$$\varphi_n(x) = \sum_{r=1}^{\left\lfloor \frac{n}{2} \right\rfloor + 1} T_n^{(2)}(r) x^r$$

имеет место асимптотическое представление

$$\varphi_n(x) = T_n^{(2)}(r_0) x^{r_0} \sum_{j=-n^{\frac{1}{2}+\varepsilon}}^{n^{\frac{1}{2}+\varepsilon}} x^j e^{-\frac{j^2}{n} \sqrt{2}(\sqrt{2}+1)^2} (1 + o(1)),$$

где $r \leq r_0 < r+1$, r — натуральное число.

Доказательство аналогично доказательству леммы 1 в § 1.

При $x = 1$ из леммы 6 получаем асимптотическую формулу для общего числа корневых деревьев

$$T_n^{(2)} = \sqrt{\frac{2}{2+\sqrt{2}}} \left(\frac{\sqrt{2}+1}{e} \right)^n n^{n-1} (1+o(1)).$$

Если $\tilde{\xi}_n$ — число начальных вершин в случайном равновероятном дереве вторичной спецификации $\left[\left[0^r 1^{n-2r+2} 2^{r-2} \right] \right]$, то так же, как в § 1, можно показать, что для среднего и дисперсии $\tilde{\xi}_n$ имеют место при $n \rightarrow \infty$ асимптотические формулы

$$\mathbf{M}\tilde{\xi}_n = \frac{n}{2+\sqrt{2}}(1+o(1)), \quad \mathbf{D}\tilde{\xi}_n = \frac{n}{8+6\sqrt{2}}(1+o(1))$$

и распределение случайной величины $(\tilde{\xi}_n - \mathbf{M}\tilde{\xi}_n) / \sqrt{\mathbf{D}\tilde{\xi}_n}$ при $n \rightarrow \infty$ сходится к нормальному распределению с параметрами $(0,1)$.

Обозначим через $E_{nk}^{(2)}$ число преобразований n -множества вторичной спецификации $\left[\left[0^r 1^{n-2r} 2^r \right] \right]$, имеющих k циклических элементов.

Выбор остова рассматриваемого преобразования, содержащего k вершин, из которых j являются корневыми деревьями, и выбор корневого леса из $n-k+j$ вершин и j деревьев определяют общее число вариантов построения орграфа преобразования рассматриваемого вида. В результате получаем формулу

$$E_{nk}^{(2)} = n! \left(1 + \sum_{j=1}^k \binom{k}{j} \sum_{\substack{n_1+\dots+n_j=n-k+j \\ n_i \geq 2}} \frac{T_{n_1}^{(2)}}{n_1!} \dots \frac{T_{n_j}^{(2)}}{n_j!} \right).$$

Отметим, что при $k = n$ в орграфе отсутствуют деревья и все вершины являются циклическими.

Список литературы

1. Arney Y., Bender E. Random mappings with constraints on coalescence and number of origins // Pacific J. Math. — 1982. — V. 103. No. 2. — P. 269–294.
2. Сачков В. Н. Введение в комбинаторные методы дискретной математики, 2-е изд. — М.: МЦНМО, 2004.