ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.212.2 DOI 10.17223/20710410/62/1

О РАСПРЕДЕЛЕНИИ ДЛИН ЦИКЛОВ В ГРАФЕ k-КРАТНОЙ ИТЕРАЦИИ РАВНОВЕРОЯТНОЙ СЛУЧАЙНОЙ ПОДСТАНОВКИ

В. О. Миронкин

МИРЭА — Российский технологический университет, г. Москва, Россия

E-mail: mironkin.v@mail.ru

Изучается влияние процесса итерирования на структуру графа G_π исходной равновероятной случайной подстановки $\pi\colon S \to S$. Выписаны точные формулы для распределения длины $\beta_\pi(x)$ цикла $\mathcal{K}_\pi(x)$, содержащего произвольную фиксированную вершину $x \in S$. Получено выражение для математического ожидания случайной величины $\lambda_{\pi^k}(l)$, равной числу вершин в графе G_{π^k}, лежащих на циклах длины $l \in \{1, \ldots, |S|\}$. Для $k \in \mathbb{N}$ и произвольных фиксированных вершин $x, y \in S$, $x \neq y$, вычислена совместная вероятность их попадания на циклы фиксированных длин в графе G_{π^k}.

Ключевые слова: *равновероятная случайная подстановка, итерация подстановки, граф подстановки, распределение длин циклов, неподвижные точки.*

ON THE DISTRIBUTION OF CYCLE LENGTHS IN THE GRAPH OF k-MULTIPLE ITERATION OF THE UNIFORM RANDOM SUBSTITUTION

V. O. Mironkin

MIREA — Russian Technological University, Moscow, Russia

The influence of the iteration process on the structure of the graph G_π of the uniform random substitution $\pi\colon S \to S$ is studied. Exact formulas are written out for the distribution of the length $\beta_\pi(x)$ of the cycle $\mathcal{K}_\pi(x)$ containing an arbitrary fixed vertex $x \in S$. An expression is written for the mathematical expectation of a random variable $\lambda_{\pi^k}(l)$ equal to the number of vertices in the graph G_{π^k} lying on cycles of length $l \in \{1, \ldots, |S|\}$. For $k \in \mathbb{N}$ and arbitrary fixed vertices $x, y \in S$, $x \neq y$, the joint probability of their falling on cycles of fixed lengths in the graph G_{π^k} is calculated.

Keywords: *uniform random substitution, iteration of a substitution, graph of a substitution, distribution of cycle lengths, fixed points.*

Введение

Наряду с равновероятными случайными отображениями конечного множества в себя [1–4] особую практическую роль при синтезе и анализе алгоритмических методов

защиты информации (далее — АМЗИ) играют равновероятные случайные подстановки — биективные отображения конечного множества в себя. Так, в частности, класс указанных отображений представляет собой основной математический инструментарий, используемый при моделировании алгоритмов блочного шифрования, которые, как правило, имеют итерационную структуру. Такое построение АМЗИ нацелено на повышение их криптографического качества. При этом может возникнуть естественный вопрос о целесообразности дополнительного итерирования уже отдельных блоков АМЗИ, например блока подстановок. Как подобная модификация скажется на криптографическом качестве АМЗИ в целом? Для того чтобы ответить на этом вопрос, требуются знания о свойствах и характеристиках итераций упомянутых блоков.

В работе изучаются вероятностные свойства и характеристики одной модификации класса равновероятных случайных подстановок, состоящего из их кратных итераций.

Следует отметить, что результаты исследований равновероятных случайных отображений [5, 6] не могут быть в явном виде распространены на указанные математические объекты из-за неравновероятности распределения случайных подстановок на множестве всех отображений некоторого конечного множества в себя.

1. Теоретико-вероятностная модель

Рассмотрим конечное множество $S = \{1, \ldots, n\}$, $n > 1$, и вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество S_n всех $n!$ биективных отображений $\pi\colon S \to S$, алгеброй событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$, соответствующая равновероятным случайным отображениям, задана следующим образом:

$$\mathsf{P}[\pi] = \frac{1}{n!}, \quad \pi \in \Omega. \tag{1}$$

Определение 1. *Графом подстановки* $\pi \in \Omega$ называется ориентированный граф $G_\pi = (S, E_\pi)$ с множеством вершин S и множеством ориентированных рёбер $E_\pi = \{(x, \pi(x))\colon x \in S\} \subset S^2$.

Определение 2. *Циклом* $\mathcal{K}_\pi(x)$ графа G_π, содержащим вершину $x \in S$, называется множество вершин

$$\{y \in S\colon \pi^u(y) = \pi^v(x) \text{ для некоторых } u, v \geqslant 0\}.$$

Здесь $\pi^0(y) = y$ и $\pi^u(y) = \underbrace{\pi(\ldots(\pi}_{u}(y)\ldots)$ в случае $u > 0$.

Через $\beta_\pi(x)$ обозначим длину цикла $\mathcal{K}_\pi(x)$, а через $C_l(G_\pi)$ — множество вершин графа G_π, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Замечание 1. Распределение случайной величины $\beta_\pi(x)$ зависит от n. Однако во избежание загромождения формул данный факт в тексте отражать не будем.

2. Вспомогательные результаты

Для произвольных $k, l, i, j \in \mathbb{N}$, $i \leqslant j$, введём обозначение

$$Q_i^j(k, l) = \left\{m \in \mathbb{N} : i \leqslant m \leqslant j,\ \frac{m}{(m, k)} = l\right\}, \tag{2}$$

где (m, k) — наибольший общий делитель m и k.

Далее для произвольного $u \in \mathbb{N}$, $u > 1$, будем использовать следующее представление:

$$u = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}, \tag{3}$$

где $p_1 = 2 < p_2 < \ldots < p_t$ — последовательные простые числа; $a_t > 0$; $a_i \geqslant 0$, $i = 1, \dots, t-1$. При этом через Δ_u будем обозначать множество номеров ненулевых элементов последовательности $a_1, \dots, a_t$, а через $\overline{\Delta_u} = \{1, \dots, t\} \setminus \Delta_u$ — множество номеров нулевых элементов. Кроме того, для произвольных $n \in \mathbb{N}$, $n > 1$, $r \in \mathbb{N}$ и $D \in \mathbb{R}$ через $W_{\{i_1,\dots,i_r\}}^{(\{a_{i_1},\dots,a_{i_r}\})}(n, D)$ будем обозначать множество решений из $(\mathbb{N} \cup \{0\})^r$ системы линейных неравенств

$$\begin{cases} x_1 \log_n p_{i_1} + x_2 \log_n p_{i_2} + \ldots + x_r \log_n p_{i_r} \leqslant D, \\ x_j \leqslant a_{i_j}, \ j = 1, \dots, r, \end{cases}$$

где $i_1 < \ldots < i_r$. Здесь и далее положим $\prod\limits_{i \in \varnothing} (\ldots) \equiv 1$, $\sum\limits_{i \in \varnothing} (\ldots) \equiv 0$.

Утверждение 1. Пусть $n \in \mathbb{N}$, $n > 1$. Тогда для любых $k = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t} \in \mathbb{N}$ и $l = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s} \in \{1, \dots, n\}$, представленных в виде (3), справедливо равенство

$$|Q_1^n(k, l)| = \left| W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i \colon i \in \Delta_k \cap \overline{\Delta_l}\})} \left(n, 1 - \sum_{i \in \Delta_l} (a_i + b_i) \log_n p_i \right) \right|. \tag{4}$$

Доказательство. Зафиксируем $m \in \{1, \dots, n\}$ и запишем его в следующем виде:

$$m = \prod_{i \in \left(\Delta_m \cap \Delta_k \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{c_i},$$

где $c_i > 0$ в соответствии с (3). Тогда в условиях утверждения равенство $\dfrac{m}{(m,k)} = l$ имеет вид

$$\frac{m}{(m,k)} = \prod_{i \in (\Delta_m \cap \Delta_k \cap \overline{\Delta_l})} p_i^{c_i - \min(c_i, a_i)} \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{c_i - \min(c_i, a_i)} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{c_i} =$$

$$= \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{b_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{b_i}.$$

При этом для произвольного фиксированного $i \in \Delta_m$

$$c_i - \min(c_i, a_i) = \begin{cases} 0, & c_i \leqslant a_i, \\ c_i - a_i & \text{в противном случае.} \end{cases}$$

В частности, при условии $m \in \{1, \dots, n\}$ выполняется следующее:

1) для $i \in \left(\Delta_m \cap \Delta_k \cap \overline{\Delta_l}\right)$ уравнение

$$c_i - \min(c_i, a_i) = 0 \tag{5}$$

относительно c_i имеет в точности $a_i + 1$ различных решений вида $c_i = 0, \dots, a_i$;

2) для $i \in (\Delta_m \cap \Delta_k \cap \Delta_l)$ уравнение

$$c_i - \min(c_i, a_i) = b_i \neq 0 \tag{6}$$

имеет единственное решение вида $c_i = a_i + b_i$;

3) для $i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)$ уравнение (5) имеет единственное решение $c_i = 0$;

4) для $i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)$ уравнение (6) имеет единственное решение $c_i = b_i$.

Таким образом, число различных m, удовлетворяющих (2), совпадает с мощностью множества $W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i:\, i \in \Delta_k \cap \overline{\Delta_l}\})}\left(n, 1 - \sum\limits_{i \in \Delta_l} (a_i + b_i) \log_n p_i\right)$. ■

Следствие 1. Пусть в условиях утверждения 1 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$|Q_1^n(k,l)| = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1). \tag{7}$$

В частности, если k — простое, то

$$|Q_1^n(k,l)| = \begin{cases} 2, & (k,l) = 1, \\ 1, & (k,l) \neq 1. \end{cases} \tag{8}$$

3. Распределение длин циклов в графе G_{π^k}

Прежде чем перейти к описанию распределения случайной величины β_{π^k}, $k > 1$, выясним, как процесс итерирования произвольной подстановки $\pi \in S_n$ влияет на структуру её графа G_π.

Отметим, что распределение числа вершин по циклам графа G_{π^k}, $k > 1$, сформированного на основе графа G_π, определяется величиной k, а именно: каждый цикл графа G_π длины $m \in \{1, \ldots, n\}$ распадается на (m,k) отдельных циклов графа G_{π^k} длины $\dfrac{m}{(m,k)}$ (рис. 1).

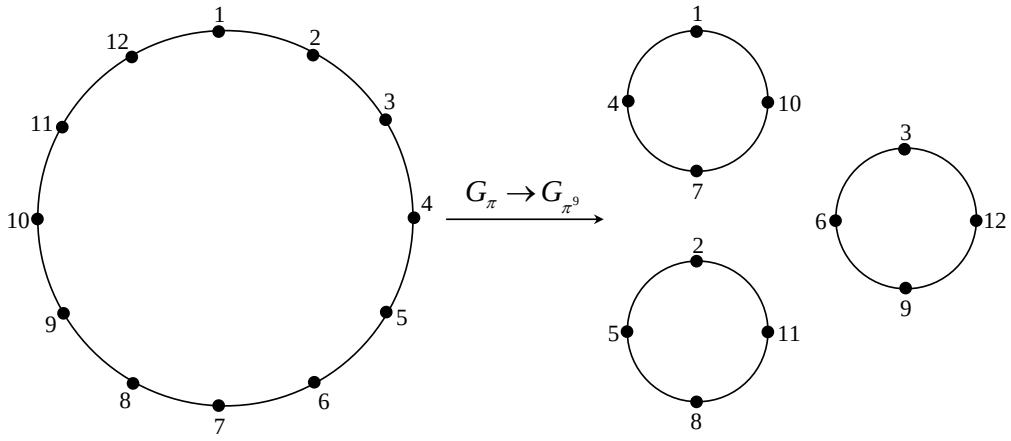

Рис. 1. Распад цикла при 9-кратном итерировании равновероятной случайной подстановки π

Этот факт позволяет выписать точную формулу для локальной вероятности $\mathsf{P}\left[\beta_{\pi^k}(x) = l\right]$ с использованием распределения случайной величины β_π.

Утверждение 2. Пусть $n \in \mathbb{N}$, $n > 1$ и случайная подстановка $\pi\colon S \to S$ имеет распределение (1). Тогда для любого фиксированного $x \in S$, любых $k = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \in \in \mathbb{N}$ и $l = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s} \in \{1, \ldots, n\}$, представленных в виде (3), справедливо равенство

$$\mathsf{P}\left[\beta_{\pi^k}(x) = l\right] = \frac{1}{n} \left| W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i:\, i \in \Delta_k \cap \overline{\Delta_l}\})}\left(n, 1 - \sum_{i \in \Delta_l} (a_i + b_i) \log_n p_i\right) \right|.$$

Доказательство. Зафиксируем вершину $x \in S$ и обозначим через m длину цикла $\mathcal{K}_\pi(x)$, где $m \leqslant n$. Тогда для произвольного $k \in \mathbb{N}$ соответствующий цикл $\mathcal{K}_{\pi^k}(x)$ имеет длину $l = \dfrac{m}{(m,k)}$. Используя обозначение (2), запишем равенство событий

$$[\beta_{\pi^k}(x) = l] = \bigcup_{m \in Q_n(k,l)} [\beta_\pi(x) = m]. \tag{9}$$

Заметим, что события, стоящие под знаком объединения в (9), несовместны и что величина

$$\mathsf{P}[\beta_\pi(x) = m] = \left(1 - \frac{1}{n}\right)\left(1 - \frac{1}{n-1}\right)\ldots\left(1 - \frac{1}{n-m+2}\right)\frac{1}{n-m+1} = \frac{1}{n}$$

не зависит от m.

Поэтому, переходя в (9) к вероятностям, получаем

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \sum_{m \in Q_n(k,l)} \mathsf{P}[\beta_\pi(x) = m] = \frac{|Q_1^n(k,l)|}{n}, \tag{10}$$

что с учётом (4) даёт искомый результат. ■

Следствие 2. Пусть в условиях утверждения 2 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \frac{1}{n} \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1). \tag{11}$$

В частности, если k — простое, то

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \begin{cases} 2/n, & (k,l) = 1, \\ 1/n, & (k,l) \neq 1. \end{cases}$$

Доказательство. Искомые выражения естественным образом следуют из (10) и соотношений (7) и (8). ■

Через $\lambda_{\pi^k}(l)$ обозначим случайную величину, равную числу вершин в графе G_{π^k}, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Следствие 3. Пусть в условиях утверждения 2 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$\mathbf{E}\lambda_{\pi^k}(l) = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1).$$

Доказательство. Действительно, так как $\lambda_{\pi^k}(l) = \sum\limits_{x \in S} I\{x \in C_l(G_{\pi^k})\}$, где $I\{A\}$ — индикатор события A, то в силу равноправия всех $x \in S$ и с учётом (11) получаем цепочку соотношений

$$\mathbf{E}\lambda_{\pi^k}(l) = \mathbf{E}\sum_{x \in S} I\{x \in C_l(G_{\pi^k})\} = n\,\mathsf{P}[x \in C_l(G_{\pi^k})] = n\,\mathsf{P}[\beta_{\pi^k}(x) = l] = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1).$$

Следствие доказано. ■

В результатах следствий 2 и 3 выделим частный случай, представляющий особый интерес для анализа криптографических примитивов (например, s-боксов), используемых в составе алгоритмов блочного шифрования.

Определение 3. Неподвижной точкой подстановки $\pi\colon S \to S$ называется элемент $x \in S$, для которого $\pi(x) = x$.

С учётом введённых обозначений множество неподвижных точек k-кратной итерации произвольной подстановки $\pi\colon S \to S$ совпадает с $C_1(G_{\pi^k})$.

Следствие 4. Пусть в условиях утверждения 2 число k — простое и выполнено неравенство $k \leqslant n$. Тогда справедливы формулы

$$\mathsf{P}\left[x \in C_1(G_{\pi^k})\right] = \frac{2}{n},$$
$$\mathbf{E}\lambda_{\pi^k}(1) = 2.$$

Замечание 2. Результаты следствий 3 и 4 могут найти применение в рамках статистической проверки гипотезы о равновероятности распределения подстановок. Действительно, имея реализацию $\pi_1, \pi_2, \ldots, \pi_N$ выборки объёма $N \in \mathbb{N}$ из некоторого неизвестного распределения, заданного на измеримом пространстве $(\Omega, \mathcal{F})$, можно для произвольного $k > 1$ сформировать и работать с набором производных реализаций

$$\pi_1, \ldots, \pi_N,\ \pi_1^2, \ldots, \pi_N^2,\ \ldots,\ \pi_1^k, \ldots, \pi_N^k,$$

получив при этом вместо одной оценки $\overline{X}_1$ величины $\mathbf{E}\lambda_\pi(l)$, $l \in \{1, \ldots, n\}$, набор из k оценок $\overline{X}_1, \ldots, \overline{X}_k$ величин $\mathbf{E}\lambda_\pi(l), \ldots, \mathbf{E}\lambda_{\pi^k}(l)$ соответственно.

Далее для $k \in \mathbb{N}$ и произвольных фиксированных вершин $x, y \in S$, $x \neq y$, вычислим совместную вероятность их попадания на циклы фиксированных длин в графе G_{π^k}.

Утверждение 3. Пусть $n \in \mathbb{N}$, $n > 1$ и случайная подстановка $\pi\colon S \to S$ имеет распределение (1). Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $k \in \mathbb{N}$ и $l_1, l_2 \in \{1, \ldots, n\}$, $l_1 + l_2 \leqslant n(1 + \delta_{l_1,l_2})$, справедливо равенство

$$\mathsf{P}\left[x \in C_{l_1}(G_{\pi^k}), y \in C_{l_2}(G_{\pi^k})\right] = \delta_{l_1,l_2} \sum_{m \in Q_1^n(k,l_1)} \frac{m-1}{n(n-1)} + \sum_{m_1 \in Q_1^n(k,l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k,l_2)} \frac{1}{n(n-1)},$$

где $\delta_{l_1,l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2 \end{cases}$ — символ Кронекера; $Q_1^n(k,l)$ определяется соотношением (2).

Доказательство. Для произвольных $x, y \in S$, $x \neq y$, определим индикатор

$$I_{x,y} = \begin{cases} 1, & \text{если } x, y \text{ лежат на одном цикле графа } G_\pi, \\ 0 & \text{в противном случае.} \end{cases}$$

Рассмотрим случай $l_1 = l_2 = l$. По формуле полной вероятности

$$\mathsf{P}\left[x, y \in C_l(G_{\pi^k})\right] = \mathsf{P}\left[x, y \in C_l(G_{\pi^k}), I_{x,y} = 1\right] + \mathsf{P}\left[x, y \in C_l(G_{\pi^k}), I_{x,y} = 0\right]. \tag{12}$$

Вычислим первое слагаемое в правой части (12). Зафиксируем вершину $x \in S$. Для произвольной фиксированной вершины $y \in S$, $y \neq x$, существует в точности $m-1$ вариантов расположения на содержащем x цикле длины $m \in Q_n(k,l)$ в графе G_π.

Тогда получаем следующую цепочку равенств:

$$\begin{gathered}\mathsf{P}\left[x,y\in C_l(G_{\pi^k}),I_{x,y}=1\right]=\\ =\sum_{m\in Q_2^n(k,l)}\frac{1}{n}\left(1-\frac{1}{n-1}\right)\left(1-\frac{1}{n-2}\right)\ldots\left(1-\frac{1}{n-m+2}\right)\frac{1}{n-m+1}+\\ +\sum_{m\in Q_2^n(k,l)}\left(1-\frac{2}{n}\right)\frac{1}{n-1}\left(1-\frac{1}{n-2}\right)\ldots\left(1-\frac{1}{n-m+2}\right)\frac{1}{n-m+1}+\ldots+\\ +\sum_{m\in Q_2^n(k,l)}\left(1-\frac{2}{n}\right)\left(1-\frac{2}{n-1}\right)\ldots\left(1-\frac{2}{n-m+3}\right)\frac{1}{n-m+2}\frac{1}{n-m+1}=\\ =\sum_{m\in Q_1^n(k,l)}\frac{m-1}{n\,(n-1)}.\end{gathered}\tag{13}$$

Для случая, когда вершины x,y лежат на различных циклах длин $m_1,m_2\in$ $\in\{1,\ldots,n\}$, $m_1+m_2\leqslant n$, в графе G_π, имеем

$$\begin{gathered}\mathsf{P}\left[x,y\in C_l(G_{\pi^k}),I_{x,y}=0\right]=\sum_{m_1\in Q_1^n(k,l)}\prod_{i=0}^{m_1-2}\left(1-\frac{2}{n-i}\right)\frac{1}{n-m_1+1}\times\\ \times\sum_{m_2\in Q_1^{n-m_1}(k,l)}\prod_{i=m_1}^{m_1+m_2-2}\left(1-\frac{1}{n-i}\right)\frac{1}{n-m_1-m_2+1}=\\ =\sum_{m_1\in Q_1^n(k,l)}\sum_{m_2\in Q_1^{n-m_1}(k,l)}\frac{1}{n\,(n-1)}.\end{gathered}\tag{14}$$

Подставив (13) и (14) в равенство (12), получим выражение для искомой вероятности в случае $l_1=l_2=l$.

Пусть теперь $l_1\neq l_2$. В этом случае вершины x,y могут лежать только на разных циклах в графе G_{π^k}, а следовательно, и в графе G_π. Поэтому

$$\mathsf{P}\left[x\in C_{l_1}(G_{\pi^k}),y\in C_{l_2}(G_{\pi^k}),l_1\neq l_2\right]=\sum_{m_1\in Q_1^n(k,l_1)}\sum_{m_2\in Q_1^{n-m_1}(k,l_2)}\frac{1}{n(n-1)}.\tag{15}$$

Объединяя выражения (12) и (15) с использованием символа Кронекера, приходим к искомому выражению. ■

Заключение

Полученные результаты позволяют описывать строение и некоторые вероятностные свойства графа G_{π^k}, $k\geqslant 1$, используемые при синтезе и анализе АМЗИ. Кроме того, точные распределения исследованных случайных величин расширяют возможности статистической проверки гипотезы о согласии распределения анализируемых подстановок с равновероятным.

ЛИТЕРАТУРА

1. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984. 208 с.
2. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978. 288 с.
3. *Flajolet P. and Odlyzko A.* Random mapping statistics // LNCS. 1989. V. 434. P. 329–354.
4. *Harris B.* Probability distributions related to random mapping // Ann. Math. Statist. 1960. V. 31. No. 4. P. 1045–1062.

5. *Миронкин В. О.* Слои в графе k-кратной итерации равновероятного случайного отображения // Математические вопросы криптографии. 2019. Т. 10. № 1. С. 73–82.
6. *Миронкин В. О.* Слои в графе композиции независимых равновероятных случайных отображений // Математические вопросы криптографии. 2020. Т. 11. № 1. С. 101–114.

REFERENCES

1. *Kolchin V. F.* Sluchaynie otobrazeniya [Random Mappings]. Moscow, Nauka Publ., 1984. (in Russian)
2. *Sachkov V. N.* Veroyatnostnie metodi v kombinatornom analize [Probabilistic Methods in Combinatorial Analysis]. Moscow, Nauka Publ., 1978. (in Russian)
3. *Flajolet P. and Odlyzko A.* Random mapping statistics. LNCS, 1989, vol. 434, pp. 329–354.
4. *Harris B.* Probability distributions related to random mapping. Ann. Math. Statist., 1960, vol. 31, no. 4, pp. 1045–1062.
5. *Mironkin V. O.* Sloi v grafe k-kratnoy iteratsii ravnoveroyatnogo sluchaynogo otobrazheniya [On the layers in the graph of k-fold iteration of uniform random mapping]. Mat. Vopr. Kriptogr., 2019, vol. 10, no. 1, pp. 73–82. (in Russian)
6. *Mironkin V. O.* Sloi v grafe kompozitsii nezavisimykh ravnoveroyatnykh sluchaynykh otobrazheniy [Layers in a graph of the composition of independent uniform random mappings]. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 1, pp. 101–114. (in Russian)