ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 30 МАТЕМАТИКИ Выпуск 1
2023

В. О. Мironкин (Москва, МИРЭА — Российский технологический университет)**. О некоторых свойствах цикловой структуры итераций равновероятных случайных подстановок.**

УДК 519.212.2 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Резюме: Реализован подход [1, 2] к получению точных формул для ряда вероятностных характеристик графов равновероятных случайных подстановок. Выписана вероятность попадания произвольной фиксированной вершины $x \in S$ на цикл заданной длины в графе k-кратной итерации равновероятной случайной подстановки $\pi\colon S \to S$, получено выражение для среднего числа неподвижных точек в этом графе.

Ключевые слова: равновероятная случайная подстановка, итерация подстановки, граф подстановки, неподвижные точки.

Введение. Пусть $S = \{1, \ldots, n\}$, $n > 1$, и задано вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество $\mathfrak{S}$ 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:

$$\mathbf{P}(\pi) = \frac{1}{n!} \quad \forall \pi \in \Omega. \tag{1}$$

Для произвольного $k \in \mathbb{N}$ обозначим k-кратную итерацию $\underbrace{\pi(\ldots(\pi}_{k}(x)\ldots)$ подстановки π через π^k.

Напомним, что *графом подстановки* $\pi \in \Omega$ называется ориентированный граф $G_\pi = (S, E_\pi)$ с множеством вершин S и множеством ориентированных ребер $E_\pi = \{(x,\, \pi(x))\colon x \in S\} \subset S^2$.

Через $C_l(G_\pi)$ обозначим множество вершин графа G_π, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Аналогично [1] для произвольных $k, l, i, j \in \mathbb{N}:\ i \leqslant j$ введем обозначение

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

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

Далее с целью упрощения формулировок основных результатов для произвольного $u \in \mathbb{N}$, $u > 1$, будем использовать представление

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

где $p_1 = 2 < p_2 < \cdots < p_t$ — последовательные простые числа, $a_t > 0$, $a_i \geqslant 0$, $i = 1, \ldots, t-1$. При этом через Δ_u будем обозначать множество индексов ненулевых элементов мультимножества $\{a_1, \ldots, a_t\}$, а через $\overline{\Delta_u} = \{1, \ldots, t\} \setminus \Delta_u$ — множество индексов нулевых элементов соответственно.

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 неравенств

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

где $i_1 < \dots < i_r$.

Здесь и далее будем полагать $\prod\limits_{i \in \emptyset} (\dots) \equiv 1$, $\sum\limits_{i \in \emptyset} (\dots) \equiv 0$.

Утверждение 1. *Пусть $n \in \mathbb{N}$, $n > 1$, и пусть случайная подстановка $\pi\colon S \to S$ имеет распределение (1) на Ω. Тогда для любого фиксированного $x \in S$, 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 форме (3), справедливо равенство*

$$\mathbf{P}\left\{x \in C_l\left(G_{\pi^k}\right)\right\} = \frac{1}{n} \left| W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i \colon i \in \Delta_k \cap \overline{\Delta_l}\})} \left(n, 1 - \sum_{i \in \Delta_l} (a_i + b_i) \log_n p_i \right) \right|.$$

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

$$\mathbf{P}\left\{x \in C_l\left(G_{\pi^k}\right)\right\} = \frac{1}{n} \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1).$$

Если при этом $k = p^a$, где p — простое, $a > 0$, то

$$\mathbf{P}\left\{x \in C_l\left(G_{\pi^k}\right)\right\} = \begin{cases} \frac{a+1}{n}, & p \nmid l, \\ \frac{1}{n}, & p \mid l. \end{cases}$$

Через $\lambda_{\pi^k}(l)$ обозначим случайную величину, равную числу вершин в графе G_{π^k}, лежащих на циклах длины $l \in \{1, \dots, n\}$. Заметим, что при $l = 1$ случайная величина $\lambda_{\pi^k}(1)$ представляет собой не что иное, как число неподвижных точек подстановки π^k.

Следствие 2. *Пусть в условиях утверждения 1 выполнено условие $kl \leqslant n$. Тогда справедлива формула*

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

В частности, для простого $k \leqslant n$ имеет место равенство $\mathbf{E}\lambda_{\pi^k}(1) = 2$.

СПИСОК ЛИТЕРАТУРЫ

1. *Миронкин В. О.* Слои в графе k-кратной итерации равновероятного случайного отображения. — Математические вопросы криптографии, 2019, т. 10, № 1, с. 73–82. // *Mironkin V. O.* Sloyi v grafe k-kratnoy iteracii ravnoveroyatnogo sluchaynogo otobrazeniya [On the layers in the graph of k-fold iteration of uniform random mapping]. — Mat. Vopr. Kriptogr. 2019, v. 10, № 1, p. 73–82. (in Russian)
2. *Миронкин В. О.* Слои в графе композиции независимых равновероятных случайных отображений. — Математические вопросы криптографии. 2020, т. 11, № 1, с. 101–114. *Mironkin V. O.* Sloyi v grafe kompozicii nezavisimih ravnoveroyatnih sluchaynih otobrazeniy [Layers in a graph of the composition of independent uniform random mappings]. Mat. Vopr. Kriptogr. 2020, v. 11, № 1, p. 101–114. (in Russian)

UDC 519.212.2 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Mironkin V. O. (Moscow, MIREA — Russian Technological University)**. On some properties of the cyclic structure of iterations of the iniform random substitutions.**

Abstract: The approach [1, 2] to obtaining exact formulas for a number of probabilistic characteristics of graphs of equally probable random substitutions is implemented. The probability of hitting an arbitrary fixed vertex $x \in S$ on a cycle of a given length in a graph k-multiple iteration of an equally probable random substitution $\pi\colon S \to S$ is written out, an expression is obtained for the average number of fixed points in this graph.

Keywords: uniform random substitution, iteration of a substitution, graph of a substitution, fixed points.