

Math-Net.Ru

Общероссийский математический портал

В. О. Миронкин, Слои в графе композиции независимых
равновероятных случайных отображений,
Матем. вопр. криптогр., 2020, том 11, выпуск 1, 101–114

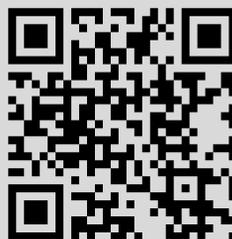
<https://www.mathnet.ru/mvk316>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<https://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.97.14.81

13 июня 2025 г., 14:02:04



Слои в графе композиции независимых равновероятных случайных отображений

В. О. Миронкин

*Национальный исследовательский университет
«Высшая школа экономики», Москва*

Получено 29.IV.2019

Аннотация. Изучаются вероятностные характеристики графа композиции независимых равновероятных случайных отображений. Получены точные выражения и оценки для распределений расстояний вершин от циклов. Приведены формулы для математических ожиданий чисел вершин, находящихся на заданных расстояниях от циклов.

Ключевые слова: равновероятное случайное отображение, композиция отображений, итерация отображений, граф отображения, слой в графе, циклические вершины

Layers in a graph of the composition of independent uniform random mappings

V. O. Mironkin

National Research University Higher School of Economics, Moscow

Abstract. The probabilistic characteristics of graph corresponding to the composition of independent uniform random mappings are studied. Exact expressions and estimates for the distribution of distances from vertices to cycles are obtained. Formulas for mean values of numbers of vertices at the given distance from cycles are derived.

Keywords: uniform random mapping, composition of mappings, iteration of mapping, graph of a mapping, layer in a graph, cyclic vertices

Введение

Настоящая статья продолжает цикл работ, посвященных изучению вероятностных свойств и характеристик композиции независимых равновероятных случайных отображений [1–5], используемой при моделировании итерационных алгоритмов выработки производных ключей (см. [6,7]), в которых разные итерации строятся с помощью разных процедур и разных случайных элементов (например, раундовых ключей, векторов инициализации).

Аналогично [8] рассмотрим конечное множество $S = \{1, \dots, n\}$, $n > 1$, и вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество \mathfrak{S} всех n^n отображений $f: S \rightarrow S$, алгеброй событий \mathcal{F} — множество всех подмножеств Ω , а вероятностная мера \mathbf{P} , соответствующая равновероятным случайным отображениям, задана следующим образом:

$$\mathbf{P}(f) = \frac{1}{n^n} \quad \forall f \in \Omega. \quad (1)$$

При изложении результатов будем использовать следующие определения для характеристик графа отображения (см. также [10–13]; в определениях отображение f считается детерминированным).

Определение 1. *Графом отображения f* называется ориентированный граф $G_f = (S, E_f)$ с множеством вершин S и множеством ориентированных ребер $E_f = \{(x, f(x)): x \in S\} \subset S^2$.

Определение 2. Вершина $x \in S$ называется *циклической вершиной* графа G_f отображения f , если существует такое $b \geq 1$, что $f^b(x) = x$ (через f^b обозначается b -кратная итерация f).

Обозначим через $C(G_f)$ множество циклических вершин графа G_f , а через $C_l(G_f)$ — множество вершин, лежащих на циклах длины $l \in \{1, \dots, n\}$.

Определение 3. *Высотой $\alpha_f(x)$* вершины $x \in S$ в графе G_f называется расстояние от этой вершины до ближайшей циклической вершины:

$$\alpha_f(x) = \min\{m \geq 0: f^m(x) \in C(G_f)\}.$$

Через $\beta_f(x)$ обозначим длину цикла компоненты $\mathcal{K}_f(x) = \{y \in S: f^l(y) = f^k(x) \text{ для некоторых } k, l \geq 0\}$ графа G_f , содержащей вершину x .

Как и в [9], зависимость случайных величин $\alpha_f(x)$, $\beta_f(x)$ от параметра n отображать не будем.

Определение 4. Для произвольного $t \in \{0, \dots, n - 1\}$ назовем t -м слоем в графе G_f множество вершин $H_f^{(t)} = \{x \in S : \alpha_f(x) = t\}$.

Определение 5. Для произвольных $l \in \{1, \dots, n\}$, $t \in \{0, \dots, n - l\}$ назовем t -м слоем циклов длины l в графе G_f множество вершин $H_f^{(t,l)} = \{x \in S : \alpha_f(x) = t, \beta_f(x) = l\}$.

Далее для произвольного $k \in \mathbb{N}$ рассмотрим последовательность независимых отображений f_1, \dots, f_k , имеющих распределение (1) на \mathfrak{S} . Через $f_{[k]}$ обозначим композицию отображений: $f_k(\dots(f_1(x))\dots)$, $x \in S$; $f_{[0]}$ будет пониматься как тождественное отображение.

Отметим, что если случайные отображения f_1, \dots, f_k имеют равновероятное распределение (1), то распределение $f_{[k]}$ при $k > 1$ не является равновероятным на \mathfrak{S} , так как $|f_{[1]}(S)| \geq |f_{[2]}(S)| \geq \dots$

В настоящей статье изучаются вероятностные характеристики слоев в случайных графах $G_{f_{[k]}}$, когда f_1, \dots, f_k имеют распределение (1), а $k \geq 1$ фиксировано.

1. Слои и циклические вершины в графе отображения $f_{[k]}$

Отметим, что структуры множеств $H_{f_{[k]}}^{(t)}$ и $H_{f_{[k]}}^{(t,l)}$ графа $G_{f_{[k]}}$ при $t = 0$ и $t > 0$ различны. В связи с этим будем рассматривать эти множества отдельно для соответствующих значений параметра t .

Так в случае $t = 0$ указанные множества слоев совпадают с $C(G_{f_{[k]}})$ и $C_l(G_{f_{[k]}})$ соответственно.

Теорема 1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда для любых $x \in S$ и $l \in \{1, \dots, n\}$ справедливы равенства

$$\mathbf{P} \left\{ x \in C_l \left(G_{f_{[k]}} \right) \right\} = \frac{1}{n} \left(\frac{\binom{n}{l}}{n^l} \right)^k, \tag{2}$$

$$\mathbf{P} \left\{ x \in C \left(G_{f_{[k]}} \right) \right\} = \frac{1}{n} \sum_{l=1}^n \left(\frac{\binom{n}{l}}{n^l} \right)^k,$$

где $(n)_l = n(n - 1) \dots (n - l + 1)$ — l -я факториальная степень n .

Доказательство. Зафиксируем $x \in S$. Тогда согласно итерационной процедуре формирования последовательности вершин

$x, f_{[1]}(x), \dots, f_{[k]}(x), f_{[1]}(f_{[k]}(x)), \dots, f_{[k]}^2(x), f_{[1]}(f_{[k]}^2(x)), \dots$ (см. рисунок) событие $\{x \in C_l(G_{f_{[k]}})\}$ выполняется тогда и только тогда, когда при любом $m = 1, \dots, k$ вершины $f_{[m]}(f_{[k]}^j(x)), j = 0, 1, \dots, l-1$, различны и $f_{[k]}(f_{[k]}^{l-1}(x)) = x$. В силу независимости отображений f_1, \dots, f_k

$$\mathbf{P}\{x \in C_l(G_{f_{[k]}})\} = \frac{1}{n} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right)^k. \tag{3}$$

Второе утверждение теоремы получаем с использованием (3) и формулы полной вероятности. Теорема доказана. \square

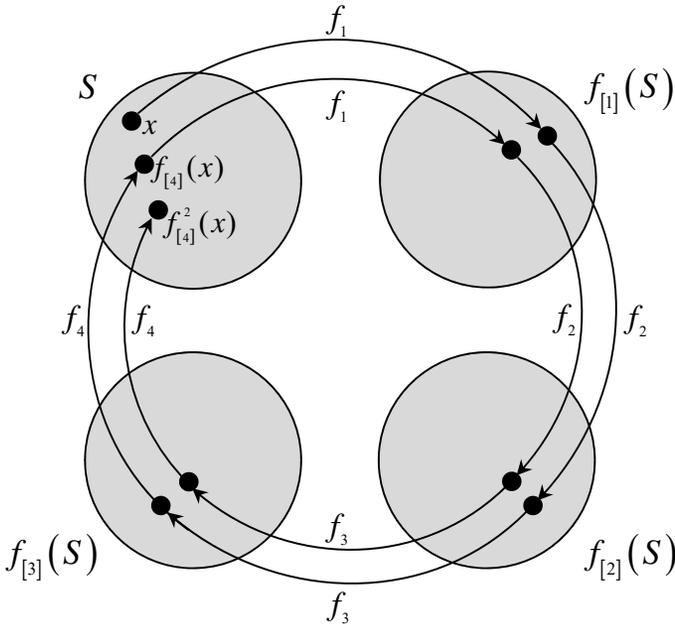


Рис. Процесс формирования компоненты $\mathcal{K}_{f_{[4]}}(x)$

Через $\lambda_{f_{[k]}}(l)$ обозначим число вершин в графе $G_{f_{[k]}}$, лежащих на циклах длины $l \in \{1, \dots, n\}$, а через $\lambda_{f_{[k]}}$ — общее число циклических вершин в графе $G_{f_{[k]}}$. Теорема 1 позволяет выписать равенства для

средних значений

$$\mathbf{E}\lambda_{f_{[k]}}(l) = \left(\frac{(n)_l}{n^l}\right)^k, \quad \mathbf{E}\lambda_{f_{[k]}} = \sum_{l=1}^n \left(\frac{(n)_l}{n^l}\right)^k. \quad (4)$$

Следствие 1. Пусть $k \in \mathbb{N}$ – произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда

$$e^{-k\left(1+\frac{l}{n}\right)\frac{l(l-1)}{2n}} \leq \mathbf{E}\lambda_{f_{[k]}}(l) \leq e^{-k\frac{l(l-1)}{2n}}, \quad (5)$$

$$\mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{\pi n}{2k}}. \quad (6)$$

Если при этом $n \rightarrow \infty$, то

$$\mathbf{E}\lambda_{f_{[k]}} = (1 + o(1)) \sqrt{\frac{\pi n}{2k}}.$$

Доказательство. Оценки (5) следуют из (2) и неравенства

$$e^{-(1+\frac{l}{n})\frac{l(l-1)}{2n}} \leq \frac{(n)_l}{n^l} = \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right) \leq e^{-\frac{l(l-1)}{2n}}, \quad (7)$$

справедливого для произвольного $l \in \{1, \dots, n\}$ (доказательство неравенства (7) приведено в приложениях).

Перейдем к доказательству (6). Учитывая неравенство

$$e^{-k\frac{l(l-1)}{2n}} < \int_{l-1}^l e^{-k\frac{x(x-1)}{2n}} dx, \quad l \geq 1,$$

из соотношений (4) и (5) получаем

$$\mathbf{E}\lambda_{f_{[k]}} \leq \sum_{l=1}^n e^{-k\frac{l(l-1)}{2n}} < 1 + \int_1^\infty e^{-k\frac{(x-1)^2}{2n}} dx = 1 + \int_0^\infty e^{-k\frac{z^2}{2n}} dz.$$

Сделав замену переменных $x = z\sqrt{\frac{n}{k}}$, с использованием равенства $\int_0^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{z^2}{2}} dz = \frac{1}{2}$ выводим верхнюю оценку:

$$\mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{n}{k}} \int_0^\infty e^{-\frac{z^2}{2}} dz = 1 + \sqrt{\frac{n}{k}} \frac{\sqrt{2\pi}}{2} = 1 + \sqrt{\frac{\pi n}{2k}}. \quad (8)$$

С другой стороны, из (7) следует, что при $0 < l \leq n^{\frac{7}{12}}$

$$\prod_{i=1}^l \left(1 - \frac{i}{n}\right) > e^{-(1+\frac{l}{n})\frac{l(l-1)}{2n}} > e^{-\frac{l^2}{2n}(1+n^{-\frac{5}{12}})}.$$

Тогда с учетом неравенства

$$\int_l^{l+1} e^{-k\frac{x^2}{2n}} dx < e^{-k\frac{l^2}{2n}}, \quad l \geq 1,$$

получаем цепочку соотношений при $n \rightarrow \infty$

$$\begin{aligned} \mathbf{E}\lambda_{f_{[k]}} &> \sum_{l=1}^{\lfloor n^{7/12} \rfloor} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right)^k = \sum_{l=1}^{\lfloor n^{7/12} \rfloor} e^{-k\frac{(l-1)^2}{2n}(1+n^{-\frac{5}{12}})} \\ &> \int_0^{n^{7/12}} e^{-k\frac{x^2}{2n}(1+n^{-\frac{5}{12}})} dx = (1+o(1)) \sqrt{\frac{\pi n}{2k(1+n^{-\frac{5}{12}})}} = (1+o(1)) \sqrt{\frac{\pi n}{2k}}, \end{aligned}$$

откуда с учетом (8) получаем $\mathbf{E}\lambda_{f_{[k]}} = (1+o(1)) \sqrt{\frac{\pi n}{2k}}$ при $n \rightarrow \infty$. Следствие доказано. \square

Замечание 1. При усложнении рассматриваемой модели за счет d -кратной итерации [14–17] композиции k независимых равновероятных случайных отображений множество циклических вершин остается неизменным:

$$C(G_{f_{[k]}^d}) = C(G_{f_{[k]}^{k-1}}) = \dots = C(G_{f_{[k]}}),$$

и поэтому с учетом теоремы 1 получаем равенство вероятностей

$$\mathbf{P}\left\{x \in C(G_{f_{[k]}^d})\right\} = \dots = \mathbf{P}\left\{x \in C(G_{f_{[k]}})\right\} = \frac{1}{n} \sum_{l=1}^n \left(\frac{\binom{n}{l}}{n^l}\right)^k.$$

При этом распределение числа циклических вершин по компонентам графа $G_{f_{[k]}^d}$, очевидно, зависит от величины $d \in \mathbb{N}$.

Следуя [16], для произвольных $k, l, i, j \in \mathbb{N}: i \leq j$, введем обозначения

$$Q_i^j(k, l) = \left\{m \in \mathbb{N}: i \leq m \leq j, \frac{m}{(m, k)} = l\right\}, \quad (9)$$

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

Следствие 2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда для любых $d \in \mathbb{N}$, $l \in \{1, \dots, n\}$ и $x \in S$ справедливо равенство

$$\mathbf{P} \left\{ x \in C_l \left(G_{f_{[k]}^d} \right) \right\} = \frac{1}{n} \sum_{m \in Q_1^n(d, l)} \left(\frac{\binom{n}{m}}{n^m} \right)^k,$$

где $Q_1^n(d, l)$ определяется соотношением (9).

Доказательство. Для произвольного фиксированного $x \in S$ выполняется равенство

$$\left\{ x \in C_l \left(G_{f_{[k]}^d} \right) \right\} = \bigcup_{m \in Q_1^n(d, l)} \left\{ x \in C_m \left(G_{f_{[k]}} \right) \right\},$$

в котором под знаком объединения стоят несовместные события. Поэтому, переходя к вероятностям, получаем

$$\mathbf{P} \left\{ x \in C_l \left(G_{f_{[k]}^d} \right) \right\} = \sum_{m \in Q_1^n(d, l)} \mathbf{P} \left\{ x \in C_m \left(G_{f_{[k]}} \right) \right\},$$

откуда с учетом (2) следует искомый результат. Следствие доказано. \square

Далее для произвольных вершин $x, y \in S$: $x \neq y$, вычислим совместную вероятность их попадания на циклы фиксированных длин в графе $G_{f_{[k]}}$.

Теорема 2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда при любых $x, y \in S$: $x \neq y$, и $l_1, l_2 \in \mathbb{N}$: $l_1 + l_2 \leq n(1 + \delta_{l_1, l_2})$, справедливо равенство

$$\begin{aligned} \mathbf{P} \left\{ x \in C_{l_1} \left(G_{f_{[k]}} \right), y \in C_{l_2} \left(G_{f_{[k]}} \right) \right\} \\ = \frac{\delta_{l_1, l_2} (l - 1)}{n(n - 1)} \left(\frac{\binom{n}{l}}{n^l} \right)^k + \frac{1}{n(n - 1)} \left(\frac{\binom{n}{l_1 + l_2}}{n^{l_1 + l_2}} \right)^k, \end{aligned}$$

где $\delta_{l_1, l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2, \end{cases}$ — символ Кронекера.

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

$$I_{x, y} = \begin{cases} 1, & \text{если } x, y \text{ — на одном цикле,} \\ 0 & \text{в противном случае.} \end{cases} \quad (10)$$

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

$$\mathbf{P} \left\{ x, y \in C_l \left(G_{f_{[k]}} \right) \right\} = \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}} \right) \\ I_{x,y} = 1 \end{array} \right\} + \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}} \right) \\ I_{x,y} = 0 \end{array} \right\}. \quad (11)$$

Вычислим первое слагаемое в правой части (11). Для произвольной вершины $y \in S$, $y \neq x$, существует в точности $l - 1$ вариантов расположения на содержащем x цикле длины $l \in \{2, \dots, n\}$ в графе $G_{f_{[k]}}$. Тогда, повторяя рассуждения теоремы 1, с учетом дополнительной вершины y получаем равенство

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}} \right) \\ I_{x,y} = 1 \end{array} \right\} &= \frac{l-1}{n^2} \prod_{i=2}^{l-1} \left(1 - \frac{i}{n} \right) \cdot \prod_{i=1}^{l-1} \left(1 - \frac{i}{n} \right)^{k-1} \\ &= \frac{l-1}{n(n-1)} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n} \right)^k. \end{aligned} \quad (12)$$

Если вершины x, y лежат на различных циклах длины $l \in \{1, \dots, \lfloor \frac{n}{2} \rfloor\}$ в графе $G_{f_{[k]}}$, то

$$\mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}} \right) \\ I_{x,y} = 0 \end{array} \right\} = \frac{1}{n(n-1)} \prod_{i=1}^{2l-1} \left(1 - \frac{i}{n} \right)^k. \quad (13)$$

Подставив (12) и (13) в равенство (11), получим выражение для искомой вероятности в случае $l_1 = l_2 = l$.

Пусть теперь $l_1 \neq l_2$. Тогда вершины x, y могут лежать только на разных циклах в графе $G_{f_{[k]}}$, и поэтому

$$\mathbf{P} \left\{ \begin{array}{l} x \in C_{l_1} \left(G_{f_{[k]}} \right), y \in C_{l_2} \left(G_{f_{[k]}} \right) \\ l_1 \neq l_2 \end{array} \right\} = \frac{1}{n(n-1)} \prod_{i=1}^{l_1+l_2-1} \left(1 - \frac{i}{n} \right)^k. \quad (14)$$

Объединив выражения (11) и (14) с использованием символа Кронекера, получим утверждение теоремы. Теорема доказана. \square

Повторяя рассуждения теоремы 2, можно получить аналогичные формулы для совместных вероятностей

$$\mathbf{P} \left\{ x_1 \in C_{l_1} \left(G_{f_{[k]}} \right), x_2 \in C_{l_2} \left(G_{f_{[k]}} \right), \dots, x_s \in C_{l_s} \left(G_{f_{[k]}} \right) \right\}$$

при подходящих значениях $l_1, \dots, l_s \in \{1, \dots, n\}$, где $s \leq n$.

Следствие 3. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда при любых $d \in \mathbb{N}$, $x, y \in S$: $x \neq y$, и $l_1, l_2 \in \{1, \dots, n\}$: $l_1 + l_2 \leq n(1 + \delta_{l_1, l_2})$, справедливо равенство

$$\begin{aligned} & \mathbf{P} \left\{ x \in C_{l_1} \left(G_{f_{[k]}}^d \right), y \in C_{l_2} \left(G_{f_{[k]}}^d \right) \right\} \\ &= \delta_{l_1, l_2} \sum_{m \in Q_1^n(d, l_1)} \frac{m-1}{n(n-1)} \left(\frac{\binom{n}{m}}{n^m} \right)^k \\ &+ \frac{1}{n(n-1)} \sum_{m_1 \in Q_1^n(d, l_1)} \sum_{m_2 \in Q_1^{n-m_1}(d, l_2)} \left(\frac{\binom{n}{m_1+m_2}}{n^{m_1+m_2}} \right)^k, \end{aligned}$$

где $\delta_{l_1, l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2, \end{cases}$ — символ Кронекера, а $Q_1^n(d, l)$ определяется соотношением (9).

Доказательство. Используя обозначения (10), рассмотрим случай $l_1 = l_2 = l$. Тогда для произвольных $x, y \in S$ по формуле полной вероятности имеем

$$\begin{aligned} & \mathbf{P} \left\{ x, y \in C_l \left(G_{f_{[k]}}^d \right) \right\} \\ &= \mathbf{P} \left\{ \begin{matrix} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 1 \end{matrix} \right\} + \mathbf{P} \left\{ \begin{matrix} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 0 \end{matrix} \right\}. \quad (15) \end{aligned}$$

Вычислим первое слагаемое в правой части (15). Для произвольной вершины $y \in S$, $y \neq x$, существует в точности $m-1$ вариантов расположения на содержащем x цикле длины m в графе $G_{f_{[k]}}$. Тогда

$$\begin{aligned} & \mathbf{P} \left\{ \begin{matrix} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 1 \end{matrix} \right\} \\ &= \sum_{m \in Q_2^n(d, l)} \frac{m-1}{n(n-1)} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right)^k = \sum_{m \in Q_1^n(d, l)} \frac{m-1}{n(n-1)} \left(\frac{\binom{n}{m}}{n^m} \right)^k. \quad (16) \end{aligned}$$

Если вершины x, y лежат на циклах различных длин $m_1, m_2 \in$

$\{1, \dots, n\}$, $m_1 + m_2 \leq n$, в графе G_f , то

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 0 \end{array} \right\} \\ = \sum_{m_1 \in Q_1^n(d,l)} \sum_{m_2 \in Q_1^{n-m_1}(d,l)} \frac{1}{n(n-1)} \prod_{i=1}^{m_1+m_2-1} \left(1 - \frac{i}{n} \right)^k \\ = \frac{1}{n(n-1)} \sum_{m_1 \in Q_1^n(d,l)} \sum_{m_2 \in Q_1^{n-m_1}(d,l)} \left(\frac{\binom{n}{m_1+m_2}}{n^{m_1+m_2}} \right)^k. \quad (17) \end{aligned}$$

Подставив (16) и (17) в (15), получим выражение для искомой вероятности при $l_1 = l_2 = l$.

Пусть теперь $l_1 \neq l_2$. В этом случае вершины x, y могут лежать только на разных циклах в графе $G_{f_{[k]}}$, и поэтому

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x \in C_{l_1} \left(G_{f_{[k]}}^d \right), y \in C_{l_2} \left(G_{f_{[k]}}^d \right) \\ l_1 \neq l_2 \end{array} \right\} \\ = \frac{1}{n(n-1)} \sum_{m_1 \in Q_1^n(d,l_1)} \sum_{m_2 \in Q_1^{n-m_1}(d,l_2)} \left(\frac{\binom{n}{m_1+m_2}}{n^{m_1+m_2}} \right)^k. \quad (18) \end{aligned}$$

Объединяя выражения (15) и (18), получаем искомую формулу. Следствие доказано. \square

Далее перейдем к описанию вероятностных характеристик множества слоев $H_{f_{[k]}}^{(t,l)}$ в случае $t \geq 1$.

Теорема 3. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда для любых $x \in S$, $t \in \{1, \dots, n-1\}$, $l \in \{1, \dots, n-t\}$

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\} \\ = \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) \left(\frac{\binom{n}{t+l-1}}{n^{t+l-1}} \right)^k. \quad (19) \end{aligned}$$

Доказательство. Зафиксируем $x \in S$ и рассмотрим указанную выше итерационную процедуру формирования последовательности

вершин $x, f_{[1]}(x), \dots, f_{[k]}(x), f_{[1]}(f_{[k]}(x)), \dots, f_{[k]}^2(x), f_{[1]}(f_{[k]}^2(x)), \dots$ (см. рисунок). Событие $\{x \in H_{f_{[k]}}^{(t,l)}\}$ выполняется тогда и только тогда, когда вершины $f_{[j]}(x), f_{[j]}(f_{[k]}(x)), f_{[j]}(f_{[k]}^2(x)), \dots, f_{[j]}(f_{[k]}^{t+l-2}(x))$ различны при $j = 1, \dots, k-1$, вершины $x, f_{[k]}(x), \dots, f_{[k]}^{t+l-1}(x)$ также различны, но $f_{[k]}^{t+l}(x) = f_{[k]}^t(x)$, т.е. существует такое $j \in \{1, \dots, k\}$, что $f_{[i]}(f_{[k]}^{t+l-1}(x)) \notin \{f_{[i]}(f_{[k]}^m(x)), m = 0, \dots, t+l-2\}$ при $i = 0, \dots, j-1$, но $f_{[j]}(f_{[k]}^{t+l-1}(x)) = f_{[j]}(f_{[k]}^{t-1}(x))$.

Таким образом, имеет место равенство

$$\begin{aligned} \{x \in H_{f_{[k]}}^{(t,l)}\} &= \{f_{[k]}^m(x), m = 0, \dots, t+l-1, \text{ попарно различны}\} \\ &\cap \left\{ \bigcap_{j=1}^{k-1} \{f_{[j]}(f_{[k]}^m(x)), m = 0, \dots, t+l-2, \text{ попарно различны}\} \right\} \\ &\cap \left\{ \bigcup_{j=1}^k \left\{ \min \left\{ m \neq t-1 : f_{[j]}(f_{[k]}^m(x)) = f_{[j]}(f_{[k]}^{t-1}(x)) \right\} = t+l-1, \right. \right. \\ &\quad \left. \left. f_{[j-1]}(f_{[k]}^{t+l-1}(x)) \neq f_{[j-1]}(f_{[k]}^{t-1}(x)) \right\} \right\}, \end{aligned}$$

где под знаком объединения стоят несовместные события. Поэтому, переходя к вероятностям, получаем

$$\begin{aligned} \mathbf{P} \{x \in H_{f_{[k]}}^{(t,l)}\} &= \frac{1}{n} \prod_{i=1}^{t+l-2} \left(1 - \frac{i}{n}\right)^{k-1} \cdot \prod_{i=1}^{t+l-1} \left(1 - \frac{i}{n}\right) \cdot \sum_{v=0}^{k-1} \left(1 - \frac{t+l-1}{n}\right)^v \\ &= \frac{1}{n} \left(1 - \frac{t+l-1}{n}\right)^{t+l-2} \prod_{i=1}^{t+l-2} \left(1 - \frac{i}{n}\right)^k \cdot \sum_{v=0}^{k-1} \left(1 - \frac{t+l-1}{n}\right)^v \\ &= \left(\frac{1}{t+l-1} - \frac{1}{n}\right) \left(1 - \left(1 - \frac{t+l-1}{n}\right)^k\right)^{t+l-2} \prod_{i=1}^{t+l-2} \left(1 - \frac{i}{n}\right)^k, \end{aligned}$$

откуда следует искомая формула. Теорема доказана. \square

Замечание 2. Теорема 3 позволяет выписать выражение для среднего значения мощности множества $H_{f_{[k]}}^{(t,l)}$. Действительно, так как

$$\left| H_{f_{[k]}}^{(t,l)} \right| = \sum_{x \in S} I \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\},$$

то в силу равноправия всех вершин $x \in S$

$$\mathbf{E} \left| H_{f_{[k]}}^{(t,l)} \right| = \mathbf{E} \sum_{x \in S} I \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\} = n \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\}.$$

Следствие 4. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения f_1, \dots, f_k независимы и имеют распределение (1) на \mathfrak{S} . Тогда для любых $x \in S$ и $z \in \{1, \dots, n-1\}$

$$\mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z)} \right\} = \sum_{l=z}^{n-1} \left(\frac{1}{l} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{l}{n} \right)^k \right) \left(\frac{(n)_l}{n^l} \right)^k.$$

Доказательство. Для произвольных $z \in \{1, \dots, n-1\}$ и $x \in S$ из равенства $H_{f_{[k]}}^{(z)} = \bigcup_{l=1}^{n-z} H_{f_{[k]}}^{(z,l)}$, где $H_{f_{[k]}}^{(z,l_1)} \cap H_{f_{[k]}}^{(z,l_2)} = \emptyset$ при $l_1 \neq l_2$, и соотношения (19) получаем

$$\mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z)} \right\} = \sum_{l=1}^{n-z} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z,l)} \right\} = \sum_{l=z}^{n-1} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z,l-z+1)} \right\},$$

откуда следует искомое выражение. Следствие доказано. \square

2. Приложение: доказательство неравенства (7)

Верхняя оценка следует из того, что $\ln(1-x) < -x$ при $x \in (0, 1)$. Для доказательства нижней оценки достаточно показать, что

$$u(n, l) = \ln \frac{(n)_l}{n^l} + \left(1 + \frac{l}{n} \right) \frac{l(l-1)}{2n} \geq 0, \quad l \in \{1, \dots, n\}.$$

Но $u(n, 1) = 0$, $u(n, n) = \ln(n!/n^n) - (n-1) > 0$ (последнее неравенство следует из огрубленной до неравенства формулы Стирлинга для $n!$). Если

$$\Delta(n, l) = u(n, l+1) - u(n, l) = \ln \left(1 - \frac{l}{n} \right) + \frac{l(3l+2n+1)}{2n^2},$$

то $\Delta(n, 1) = \ln(1 - \frac{1}{n}) + \frac{n+2}{n^2} > 0$ при $n \geq 2$, а производная

$$\frac{\partial}{\partial l} \Delta(n, l) = -\frac{6l^2 - l(4n - 1) - n}{2n^2(-n + l)}$$

положительна при $l = 1$ и имеет единственный положительный корень $l_+ = \frac{1}{12}(4n - 1 + \sqrt{16n(n + 1) + 1})$. Значит, $\Delta(n, l)$ возрастает по l на отрезке от 1 до l_+ , а затем убывает. Отсюда и из неотрицательности $u(n, l)$ при $l = 1$ и $l = n$ следует неотрицательность $u(n, l)$ во всех промежуточных точках.

Это доказательство автору сообщил А.М.Зубков.

Автор благодарен А.М. Зубкову за интерес к работе и полезные замечания.

Список литературы

- [1] Зубков А.М., Серов А.А., “Предельная теорема для мощности образа подмножества при композиции случайных отображений”, *Дискретная математика*, **29**:1 (2017), 17–26.
- [2] Зубков А.М., Серов А.А., “Оценки среднего размера образа подмножества при композиции случайных отображений”, *Дискретная математика*, **30**:2 (2018), 27–36.
- [3] Серов А.А., “Образы конечного множества при итерациях двух случайных зависимых отображений”, *Дискретная математика*, **27**:4 (2015), 133–140.
- [4] Dalal A., Schmutz E., “Compositions of random functions on a finite set”, *Electr. J. Comb.*, **9**:R26 (2002), 1–7.
- [5] Fill J.A., “On compositions of random functions on a finite set”, 2002 <http://www.mts.jhu.edu/~fill/>, 1–15.
- [6] Миронкин В.О., “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”, *Проблемы информационной безопасности. Компьютерные системы*, СПб.: СПбПУ, 2015, № 4, 140–146.
- [7] Ahmetzyanova L.R., Alekseev E.K., Oshkin I.B., Smyshlyayev S.V., Sonina L.A., “On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing”, *Математические вопросы криптографии*, **8**:2 (2017), 39–50.
- [8] Миронкин В.О., “Распределение длины отрезка аperiodичности в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **10**:3 (2019), 89–99.
- [9] Зубков А.М., Миронкин В.О., “Распределение длины отрезка аperiodичности в графе k -кратной итерации случайного равновероятного отображения”, *Математические вопросы криптографии*, **8**:4 (2017), 63–74.
- [10] Колчин В.Ф., *Случайные отображения*, М.: Наука, 1984, 208 с.
- [11] Сачков В.Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.
- [12] Harris B., “Probability distributions related to random mappings”, *Ann. Math. Statist.*, **31**:4 (1960), 1045–1062.

- [13] Flajolet P., Odlyzko A., “Random mapping statistics”, *Lect. Notes Comput. Sci.*, **434** (1989), 329–354.
- [14] МИРОНКИН В.О., МИХАЙЛОВ В.Г., “О множестве образов k -кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **9:3** (2018), 99–108.
- [15] МИРОНКИН В.О., “Об оценках распределения длины отрезка аperiodичности в графе k -кратной итерации равновероятного случайного отображения”, *Прикладная дискретная математика*, **42** (2018), 6–17.
- [16] МИРОНКИН В.О., “Слои в графе k -кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **10:1** (2019), 73–82.
- [17] МИРОНКИН В. О., “Коллизии и инцидентность вершин компонентам в графе k -кратной итерации равновероятного случайного отображения”, *Дискретная математика*, **31:4** (2019), 38–52.