А. М. Зубков, В. О. Миронкин, Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 4, 63–74

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 4 С. 63–74

УДК 519.212.2+519.719.2

Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения

А. М. Зубков [1], **В. О. Миронкин** [2]

[1] *Математический институт им. В. А. Стеклова РАН, Москва*

[2] *Национальный исследовательский университет Высшая школа экономики, Москва*

Получено 15.III.2017

Аннотация. Изучается распределение длины отрезка апериодичности в графе отображения, являющегося k-кратной итерацией случайного равновероятного отображения конечного множества. Получены точные выражения для этого распределения, найдено предельное распределение нормированной длины отрезка апериодичности при стремлении числа элементов множества к бесконечности.

Ключевые слова: случайное равновероятное отображение, итерации случайного отображения, граф отображения, отрезок апериодичности

Distribution of the length of aperiodicity segment in the graph of k-fold iteration of uniform random mapping

A. M. Zubkov [1], **V. O. Mironkin** [2]

[1] *Steklov Mathematical Institute of RAS, Moscow*

[2] *National Research University Higher School of Economics, Moscow*

Abstract. The distribution of the length of the aperiodicity segment in a graph of k-fold iteration of random uniform mapping of a finite set is studied. Exact formulas for this distribution are obtained, the limit distribution of the normed length of aperiodicity segment is found for the case when the cardinality of the set tends to infinity.

Key words: equiprobable random mapping, iterations of random mapping, graph of a mapping, aperiodicity segment

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 4, pp. 63–74 (Russian)

1. Введение

В последнее время активно развивается раздел теории вероятностей, связанный с изучением случайных равновероятных отображений конечных множеств [1,6,9–14] и их итераций. В частности, это обусловлено широким использованием криптографических примитивов, имеющих итерационную структуру. Число работ, в которых изучались свойства случайных равновероятных отображений, довольно велико (см., например, [1, 5, 6, 9, 10]), свойства неравновероятных отображений исследованы слабее (см., например, [2, 14]). Одним из примеров неравновероятных отображений является k-кратная итерация равновероятного случайного отображения. Такие отображения могут рассматриваться как модели алгоритмов преобразования данных, хэширования и выработки псевдослучайных последовательностей [3, 4], алгоритмов решения уравнений с однонаправленными функциями [15–24]. Например, при исследовании итерационных алгоритмов выработки ключевой информации [21] важной характеристикой является число тактов работы до момента повторного появления уже появлявшегося ключа. При этом результаты тактов работы могут использоваться как последовательно (что соответствует модели случайного равновероятного отображения), так и с некоторым фиксированным шагом k (что соответствует модели k-кратной итерации равновероятного случайного отображения).

Рассмотрим конечное множество $S = \{1, \ldots, n\}$, $n > 1$, и вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, где пространство элементарных исходов $\Omega = \{f\colon S \to S\}$ — множество всех n^n отображений S в себя, алгебра событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$ является равновероятной:

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

Это вероятностное пространство будем называть вероятностным пространством случайных равновероятных отображений.

О п р е д е л е н и е 1. Пусть $f\colon S \to S$. Будем называть *графом отображения* f ориентированный граф $G_f = (S, E_f)$ с множеством вершин S и множеством ориентированных ребер $E_f = \{(x,\, f(x))\colon x \in S\} \subset S^2$.

В графе G_f из каждой вершины выходит ровно одно ребро; он состоит из связных компонент, каждая из которых содержит единственный цикл. Из любой вершины $x_0 \in S$ графа G_f выходит траектория, порожденная последовательным применением отображения $f : x_{i+1} = f(x_i)$, $i = 0, 1, 2, \ldots$, и заканчивающаяся бесконечным прохождением по циклу связной компоненты графа G_f, содержащей вершину x_0.

Для произвольного $k \in \mathbb{N}$ будем обозначать k-кратную итерацию $\underbrace{f(\ldots(f}_{k}(x)\ldots)$ функции f через f^k и введем множества отображений

$$\Omega_k = \{f^k \colon f \in \Omega\}. \tag{2}$$

Будем считать, что f^0 — тождественное отображение $S \to S$.

Заметим, что Ω_k является собственным подмножеством Ω при любом $k > 1$ и что если случайное отображение f имеет равновероятное распределение (1), то распределение f^k не является равновероятным ни на Ω, ни на Ω_k.

В настоящей статье изучаются распределения длин отрезков апериодичности траекторий в случайных графах G_{f^k}, когда f имеет равновероятное распределение на Ω, а k — фиксированное натуральное число, большее 1.

2. Длина отрезка апериодичности

Введем несколько необходимых для дальнейшего изложения характеристик графов отображений.

О п р е д е л е н и е 2. Вершина $x_0 \in S$ называется *циклической вершиной* графа G_f, если существует такое $b \geqslant 1$, что $f^b(x_0) = x_0$. Множество циклических вершин графа G_f обозначим $C(G_f)$.

Высотой $\alpha_f(x_0)$ вершины $x_0 \in S$ в графе G_f называется расстояние от этой вершины до ближайшей циклической вершины:

$$\alpha_f(x_0) = \min\{m \geqslant 0 \colon f^m(x_0) \in C(G_f)\}.$$

Множества циклических вершин графов G_f и G_{f^k} при любом натуральном $k > 1$ совпадают, но при переходе от графа G_f к графу G_{f^k} каждый цикл графа G_f длины b превращается в НОД $(b,k) \stackrel{\text{def}}{=} (b,k)$ отдельных циклов графа G_{f^k} длины $b/(b,k)$.

О п р е д е л е н и е 3. *Отрезком апериодичности*, начинающимся в вершине $x_0 \in S$ графа G_f, называется отрезок выходящей из x_0 траектории от x_0 до ее первого самопересечения.

Через $\tau_f(x_0)$ обозначим случайную величину, равную длине отрезка апериодичности в графе G_f, начинающегося в вершине $x_0 \in S$:

$$\tau_f(x_0) = \min_{t \in \mathbb{N}} \left\{ t \,|\, f^t(x_0) \in \left\{x_0, f(x_0), \ldots, f^{t-1}(x_0)\right\}\right\},$$

тогда $\tau_f(x_0) = \alpha_f(x_0) + \beta_f(x_0)$, где $\beta_f(x_0)$ — длина цикла компоненты графа G_f, содержащей вершину x_0. Распределения случайных величин $\tau_f(x_0)$, $\alpha_f(x_0)$, $\beta_f(x_0)$ зависят от n; мы не будем отражать это в обозначениях, чтобы не загромождать формулы.

Для любых $i_0, i_1 \in \mathbb{Z}\colon i_0 > i_1$ положим $\prod_{j=i_0}^{i_1}(\ldots) \equiv 1$.

Теорема 1. *Пусть случайное отображение $f\colon S \to S$ имеет распределение* (1) *на Ω. Тогда при любых таких $k \in \mathbb{N}$, $x_0 \in S$ и $z \in \{1, \ldots, n\}$, что $kz \leqslant n$, справедливо равенство*

$$\mathbf{P}\left\{\tau_{f^k}(x_0) = z\right\} = \tag{3}$$
$$= \frac{1}{n} \sum_{m \geqslant 1\colon \frac{m}{(m,k)} = z} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right) + \frac{1}{n} \sum_{m \geqslant 1\colon \frac{m}{(m,k)} < z} \sum_{v=1}^{k} \prod_{i=1}^{m + \left(z - \frac{m}{(m,k)}\right)k - v} \left(1 - \frac{i}{n}\right).$$

Доказательство. Зафиксируем $x_0 \in S$ и рассмотрим событие $\{\tau_{f^k}(x_0) = z\}$. Обозначим через m длину цикла компоненты графа G_f, содержащей вершину x_0. При этом $m \leqslant kz$, так как в противном случае не произойдет зацикливания траектории, начатой в x_0, за z шагов в графе G_{f^k}. Тогда число циклических вершин на отрезке апериодичности длины z в графе G_{f^k}, лежащих на соответствующем цикле, равно $\frac{m}{(m,k)}$, а число вершин, не лежащих на цикле, равно $z - \frac{m}{(m,k)}$ (если данная разность неотрицательна). Если при этом $\frac{m}{(m,k)} < z$, то высота t вершины x_0 в графе G_f может принимать любое из значений $\left(z - \frac{m}{(m,k)}\right)k - v$, где $v \in \overline{0, k-1}$, если же $\frac{m}{(m,k)} = z$, то $t = 0$ (см. рисунок).

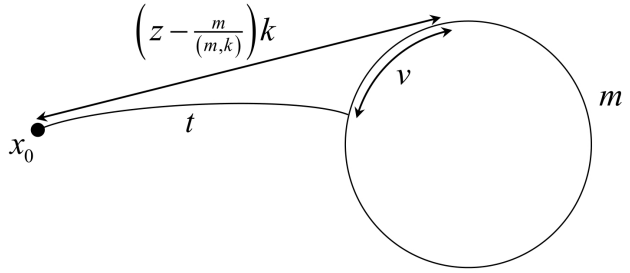

Рис. Расположение вершины x_0 в компоненте графа G_f

Справедливо равенство событий

$$\left\{\tau_{f^k}(x_0) = z\right\} = \bigcup_{s=1}^{z} \left\{\alpha_{f^k}(x_0) = z - s, \beta_{f^k}(x_0) = s\right\} =$$
$$= \left(\bigcup_{m \geqslant 1\colon \frac{m}{(m,k)} = z} \bigcup^{kz} \left\{ \begin{matrix} \alpha_f(x_0) = 0, \\ \beta_f(x_0) = m \end{matrix} \right\} \right) \bigcup \left(\bigcup_{m \geqslant 1\colon \frac{m}{(m,k)} < z} \bigcup_{t = \left(z - \frac{m}{(m,k)} - 1\right)k + 1}^{\left(z - \frac{m}{(m,k)}\right)k} \left\{ \begin{matrix} \alpha_f(x_0) = t, \\ \beta_f(x_0) = m \end{matrix} \right\} \right).$$

Заметим, что события под знаком объединения несовместны и что при фиксированных z, m и t вероятность каждого из них равна [10]

$$\frac{1}{n}\prod_{i=1}^{m+t-1}\Big(1-\frac{i}{n}\Big).$$

Поэтому вероятность события $\{\tau_{f^k}(x_0)=z\}$ равна

$$\mathbf{P}\left\{\tau_{f^k}(x_0)=z\right\}=$$

$$=\frac{1}{n}\sum_{m\geqslant 1:\ \frac{m}{(m,k)}=z}\prod_{i=1}^{m-1}\Big(1-\frac{i}{n}\Big)+\frac{1}{n}\sum_{m\geqslant 1:\ \frac{m}{(m,k)}<z}\sum_{v=0}^{k-1}\prod_{i=1}^{m+\left(z-\frac{m}{(m,k)}\right)k-v-1}\Big(1-\frac{i}{n}\Big),$$

что соответствует утверждению теоремы. □

Получим точное выражение для функции распределения $F_{\tau_{f^k}(x_0)}(z)$, $z\in\overline{1,n}$, случайной величины $\tau_{f^k}(x_0)$.

Теорема 2. *Пусть случайное отображение $f\colon S\to S$ имеет распределение* (1) *на Ω. Тогда при любых таких $k\in\mathbb{N}$, $x_0\in S$ и $z\in\{1,\dots,n\}$, что $kz\leqslant n$, справедливы равенства*

$$F_{\tau_{f^k}(x_0)}(z)=\frac{1}{n}\sum_{m\geqslant 1:\ \frac{m}{(m,k)}\leqslant z}\ \sum_{t=0}^{\left(z-\frac{m}{(m,k)}\right)k}\prod_{i=1}^{m+t-1}\Big(1-\frac{i}{n}\Big) \tag{4}$$

и

$$F_{\tau_{f^k}(x_0)}(z)=\frac{1}{n}\sum_{u=1}^{k}\sum_{j=0}^{\left[\frac{(k,u)z-u}{k}\right]}S\left(kj+u,\left(z-\tfrac{kj+u}{(u,k)}\right)k\right), \tag{5}$$

где

$$S(m,W)=\sum_{t=0}^{W}\prod_{i=1}^{m+t-1}\Big(1-\frac{i}{n}\Big).$$

Доказательство. Пусть m — длина цикла компоненты графа G_f, содержащей фиксированную вершину x_0, тогда $m\leqslant kz$. При фиксированном значении m событие $\left\{\tau_{f^k}(x_0)<z\right\}$ имеет место для всех значений

$$\alpha_{f^k}(x_0)\leqslant\left(z-\tfrac{m}{(m,k)}\right)k.$$

Тогда имеет место равенство событий

$$\{\tau_{f^k}(x_0) \leqslant z\} = \bigcup_{m\geqslant 1:\ \frac{m}{(m,k)}\leqslant z}^{kz} \ \bigcup_{t=0}^{\left(z-\frac{m}{(m,k)}\right)k} \{\alpha_f(x_0)=t,\ \beta_f(x_0)=m\}.$$

При этом события под знаком объединения несовместны, и вероятность каждого из них равна

$$\frac{1}{n}\prod_{i=1}^{m+t-1}\left(1-\frac{i}{n}\right).$$

Отсюда следует равенство (4).

Чтобы доказать справедливость формулы (5), положим при $m \geqslant 1,\ W \geqslant 0$

$$S(m,W) = \sum_{t=0}^{W}\prod_{i=1}^{m+t-1}\left(1-\frac{i}{n}\right),$$

тогда формулу (4) можно переписать в виде

$$F_{\tau_{f^k}(x_0)}(z) = \frac{1}{n}\sum_{m\geqslant 1:\ \frac{m}{(m,k)}\leqslant z} S\left(m, \left(z-\tfrac{m}{(m,k)}\right)k\right).$$

Значения (m,k), $m = 1,2,\ldots,$ образуют периодическую последовательность с периодом k. Разобьем сумму в правой части последнего равенства на k сумм, проводя в u-й $(u=1,\ldots,k)$ сумме суммирование по значениям m, не превосходящим $(u,k)z$ и сравнимым с u по модулю k:

$$F_{\tau_{f^k}(x_0)}(z) = \frac{1}{n}\sum_{u=1}^{k}\sum_{j=0}^{\left[\frac{(k,u)z-u}{k}\right]} S\left(kj+u, \left(z-\tfrac{kj+u}{(u,k)}\right)k\right). \tag{6}$$

Теорема доказана. □

Замечание 1. Формула (5) позволяет получать явные, но довольно громоздкие двусторонние оценки для функции распределения случайной величины $\tau_{f^k}(x_0)$. Наметим способ вывода таких оценок.

Из неравенства $-x-x^2 \leqslant \ln(1-x) \leqslant -x, 0<x<\frac{1}{2},$ следует, что

$$e^{-\frac{m(m-1)}{2n}\left(1+\frac{2m-1}{3n}\right)} \leqslant \prod_{i=1}^{m-1}\left(1-\tfrac{i}{n}\right) \leqslant e^{-\frac{m(m-1)}{2n}},\ 1\leqslant m\leqslant \frac{n}{2}.$$

Учитывая неравенства

$$\int_t^{t+1} e^{\frac{-x(x-1)}{2n}}\,dx < e^{-\frac{t(t-1)}{2n}} < \int_{t-1}^{t} e^{-\frac{x(x-1)}{2n}}\,dx, \quad t \geqslant 1,$$

находим, что при $1 \leqslant m \leqslant n/2$

$$\begin{aligned} S(m,W) &\leqslant \sum_{t=0}^{W} e^{-\frac{(m+t)(m+t-1)}{2n}} = \sum_{t=m}^{m+W} e^{-\frac{t(t-1)}{2n}} < \int_{m-1}^{m+W} e^{-\frac{x(x-1)}{2n}}\,dx = \\ &= \int_{m-1}^{m+W} e^{-\frac{(x-1/2)^2}{2n}+\frac{1}{8n}}\,dx = \sqrt{2\pi n}\,e^{\frac{1}{8n}}\left(\Phi\left(\frac{m+W-1/2}{\sqrt{n}}\right) - \Phi\left(\frac{m-1-1/2}{\sqrt{n}}\right)\right), \end{aligned} \tag{7}$$

где $\Phi(x)$ — функция стандартного нормального распределения, и

$$\begin{aligned} S(m,W) &\geqslant \sum_{t=0}^{W} e^{-\left(1+\frac{2(m+t)}{3n}\right)\frac{(m+t)(m+t-1)}{2n}} > \sum_{t=0}^{W} e^{-c^2\,\frac{(m+t)(m+t-1)}{2n}} > \\ &> \int_{m}^{m+W} e^{-\frac{(x-1/2)^2}{2n/c^2}+\frac{c^2}{8n}}\,dx = \frac{\sqrt{2\pi n}}{c}\,e^{\frac{c^2}{8n}}\left(\Phi\left(\frac{(m+W+1/2)}{\sqrt{n}}\,c\right) - \Phi\left(\frac{m-1/2}{\sqrt{n}}\,c\right)\right) \end{aligned} \tag{8}$$

при

$$c = \sqrt{1+\frac{2(m+W)}{3n}}.$$

Далее суммы двусторонних оценок (7) и (8) значений $S(m,W)$, входящих в (5), можно получить с помощью равенства

$$\int_a^b \Phi(x)\,dx = b\Phi(b) - a\Phi(a) + \varphi(b) - \varphi(a), \quad \varphi(x) = \Phi'(x) = \frac{e^{-x^2/2}}{\sqrt{2\pi}}.$$

Предельное распределение случайных величин $\tau_{f^k}(x_0)$ при $k = \text{const}$, $n \to \infty$ существенно зависит от множества делителей числа k.

Теорема 3. *Если целое $k > 1$ фиксировано, а $|S| = n \to \infty$, то*

$$\lim_{n\to\infty} \mathbf{P}\left\{\tau_{f^k}(x_0) \leqslant x\sqrt{n}\right\} = \mathbf{P}\left\{\theta \cdot \left(\frac{\gamma}{(\nu,k)} + \frac{1-\gamma}{k}\right) \leqslant x\right\}, \tag{9}$$

где случайные величины θ, γ, ν независимы, $\mathbf{P}\{\theta \leqslant x\} = 1 - e^{-x^2/2}$, $x \geqslant 0$, γ имеет равномерное распределение на отрезке $[0,\,1]$, а ν имеет равновероятное распределение на $\{1, 2, \ldots, k\}$.

Доказательство. Пусть f — случайное отображение множества $S=\{1,\dots,n\}$ в себя, имеющее равновероятное распределение на множестве всех n^n таких отображений, и

$$\tau_f(x_0)=\alpha_f(x_0)+\beta_f(x_0),$$

где $\alpha_f(x_0)$ — высота вершины x_0, а $\beta_f(x_0)$ — длина цикла компоненты графа G_f, содержащей вершину x_0. В силу равновероятности отображения f случайная величина $\beta_f(x_0)$ при условии, что $\tau_f(x_0)=y$, имеет равновероятное распределение на $\{1,\dots,y\}$, и при том же условии

$$\tau_{f^k}(x_0)=\frac{\beta_f(x_0)}{(\beta_f(x_0),k)}+\left]\frac{y-\beta_f(x_0)}{k}\right[, \tag{10}$$

где $]z[=\min\{n\in\mathbb{Z}\colon n\geqslant z\}$. Хорошо известно (см., например, [10]), что

$$\lim_{n\to\infty}\mathbf{P}\bigl\{\tau_f(x_0)\leqslant x\sqrt{n}\bigr\}=1-e^{-x^2/2}, \tag{11}$$

таким образом, при $n\to\infty$ вероятность того, что $\tau_f(x_0)$ больше любого наперед заданного числа, стремится к 1. Так как

$$\mathbf{P}\bigl\{\beta_f(x_0)\equiv u\,(\mathrm{mod}\,k)\,\big|\,\tau_f(x_0)\bigr\}=\frac{1}{\tau_f(x_0)}\left[\frac{\tau_f(x_0)+((k-u)\bmod k)}{k}\right],$$

то при фиксированном k

$$\begin{aligned}&\lim_{n\to\infty}\mathbf{P}\bigl\{\beta_f(x_0)\equiv u\,(\mathrm{mod}\,k)\bigr\}=\\&=\lim_{n\to\infty}\mathbf{E}\,\mathbf{P}\bigl\{\beta_f(x_0)\equiv u\,(\mathrm{mod}\,k)\,\big|\,\tau_f(x_0)\bigr\}=\frac{1}{k},\quad u=1,\dots,k.\end{aligned} \tag{12}$$

С другой стороны, так как $\beta_f(x_0)$ при условии $\tau_f(x_0)=y$ имеет равновероятное распределение на $\{1,\dots,y\}$, то

$$\lim_{n\to\infty}\mathbf{P}\left\{\frac{\beta_f(x_0)}{\tau_f(x_0)}\leqslant w\right\}=w,\quad w\in[0,1], \tag{13}$$

и при $n\to\infty$ случайные величины

$$\nu_n=\beta_f(x_0)\bmod k\quad\text{и}\quad\gamma_n=\frac{\beta_f(x_0)}{\tau_f(x_0)}$$

асимптотически независимы.

Объединяя (10), (11), (12), (13), находим, что предельное распределение случайной величины $n^{-1/2}\,\tau_{f^k}(x_0)$ при $n \to \infty$ совпадает с распределением случайной величины

$$\theta \cdot \left(\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k} \right),$$

где случайные величины θ, γ, ν независимы, θ имеет функцию распределения (11), γ имеет равномерное распределение на отрезке $[0,\,1]$, а ν имеет равновероятное распределение на $\{1, 2, \ldots, k\}$. Теорема доказана. $\square$

Замечание 2. При фиксированном k распределение случайной величины

$$\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k}$$

является смесью k распределений, соответствующих значениям $\nu = 1, 2, \ldots, k$; каждое из этих распределений входит в смесь с весом $\frac{1}{k}$. Значению $\nu = k$ соответствует атом в точке $\frac{1}{k}$, каждому значению $\nu = j \in \{1, 2, \ldots, k-1\}$ соответствует равномерное распределение на отрезке

$$\left[\frac{1}{k}, \frac{1}{(j, k)} \right].$$

Например, если k — простое число, то распределение случайной величины

$$\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k}$$

имеет атом веса $\frac{1}{k}$ в точке $\frac{1}{k}$ и плотность $\frac{k}{k-1}$ на отрезке $\left[\frac{1}{k}, 1\right]$, так что

$$\mathbf{E}\left(\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k} \right) = \frac{1}{k} + \frac{k-1}{k}\,\frac{1}{2}\left(1 - \frac{1}{k}\right) = \frac{1}{2} - \frac{1}{k} + \frac{1}{2k^2}.$$

Если k — составное число, то распределение случайной величины

$$\frac{\gamma}{(\nu, k)} + \frac{1-\gamma}{k}$$

имеет атом веса $\frac{1}{k}$ в точке $\frac{1}{k}$ и кусочно-постоянную невозрастающую плотность на отрезке $\left[\frac{1}{k}, 1\right]$, т. е. функция распределения имеет скачок в точке $\frac{1}{k}$ и выпукла вверх на отрезке $[\frac{1}{k}, 1]$.

Явные выражения для моментов распределения

$$\frac{\gamma}{(\nu,k)}+\frac{1-\gamma}{k}$$

представляются суммами по всем делителям

$$1=d_0<d_1<\ldots<d_{m(k)}=\frac{k}{d_1}<k$$

числа k, например:

$$\begin{aligned}&\mathbf{E}\Big(\frac{\gamma}{(\nu,k)}+\frac{1-\gamma}{k}\Big)=\\&=\ \frac{1}{k}+\frac{1}{2}\sum_{j=0}^{m(k)}\left(\frac{1}{d_j}-\frac{1}{k}\right)\big|\{i\in\{1,\ldots,k-1\}\colon (i,k)=d_j\}\big|.\end{aligned}$$

Используя неравенства

$$\frac{d_1}{k}-\frac{1}{k}\leqslant\frac{1}{d_j}-\frac{1}{k}\leqslant 1-\frac{1}{k}\quad\text{при}\quad j=0,1,\ldots,m(k)$$

и обозначение $\varphi(k)=|\{i\in\{1,\ldots,k-1\}\colon (i,k)=d_0=1\}|$ для функции Эйлера, можно получить грубые оценки

$$\begin{aligned}&\mathbf{E}\Big(\frac{\gamma}{(\nu,k)}+\frac{1-\gamma}{k}\Big)\leqslant\\&\leqslant\frac{1}{k}+\frac{1}{2}\left(\frac{\varphi(k)}{k}\Big(1-\frac{1}{k}\Big)+\frac{k-1-\varphi(k)}{k}\Big(\frac{1}{d_1}-\frac{1}{k}\Big)\right)<\\&<\frac{\varphi(k)+2}{2k}+\frac{1}{2d_1}\Big(1-\frac{\varphi(k)+1}{k}\Big),\\&\mathbf{E}\Big(\frac{\gamma}{(\nu,k)}+\frac{1-\gamma}{k}\Big)\geqslant\\&\geqslant\frac{1}{k}+\frac{1}{2}\left(\frac{\varphi(k)}{k}\Big(1-\frac{1}{k}\Big)+\frac{k-1-\varphi(k)}{k}\Big(\frac{d_1}{k}-\frac{1}{k}\Big)\right)>\\&>\frac{\varphi(k)+d_1+1}{2k}-\frac{d_1\,(\varphi(k)+1)}{2k^2}\,.\end{aligned}$$

Список литературы

[1] Колчин В. Ф., *Случайные отображения*, М. : Наука, 1984.

[2] Зубков А. М., “Вычисление распределения характеристик числа компонент и циклических точек случайного отображения”, *Математические вопросы криптографии*, **1**:2 (2010), 5–18.

[3] Миронкин В. О., “Исследование свойств и характеристик степени случайного отображения”, *Обозрение прикл. и промышл. матем.*, **21**:1 (2014), 70–73.

[4] Миронкин В. О., “Об особенностях строения графа степени случайного отображения”, *Обозрение прикл. и промышл. матем.*, **23**:1 (2016), 57–62.

[5] Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978..

[6] Степанов В. Е., “Предельные распределения некоторых характеристик случайных отображений”, *Теория вероятн. и ее примен.*, **14**:4 (1969), 639–653.

[7] Токарева Н. Н., *Симметричная криптография. Краткий курс: учебное пособие*, Новосибирск: Новосиб. гос. ун-т., 2012, 234 с.

[8] Феллер В., *Введение в теорию вероятностей и ее приложения* (2-*е изд.*), М.: Мир, 1964.

[9] Flajolet P., Odlyzko A., “Random mapping statistics”, Lect. Notes Comput. Sci., **434**, 1989, 329–354.

[10] Harris B., “Probability distributions related to random mapping”, *Ann. Math. Statist.*, **31**:4 (1960), 1045–1062.

[11] Dalal A., Schmutz E., “Compositions of random functions on a finite set”, *Electr. J. Comb.*, **9**:R26(2002).

[12] Goh W. M. Y., Hitczenko P., Schmutz E., “Iterating random functions on a finite set” (2012), arXiv: math/0207276v2, 7 pp.

[13] Kingman J. F. C., “The coalescent”, *Stoch.Proc. Appl.*, **13** (1982), 235–248.

[14] McSweeney J. K., Pittel B. G., “Expected coalescence time for a nonuniform allocation process”, *Adv. Appl. Probab.*, **40**:4 (2008), 1002–1032.

[15] Hellman M. E., “A cryptanalytic time–memory trade-off”, *IEEE Trans. Inf. Theory* (1980), 401–406.

[16] Hong J., Ma D., “Success probability of the Hellman trade-off”, *Inf. Process. Lett.*, **109**:7 (2009), 347–351.

[17] Oechslin P., “Making a faster cryptanalytic time-memory trade-off”, *Lect. Notes Comput. Sci.*, **2729** (2003), 617–630.

[18] Pilshchikov D. V., “Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process”, *Математические вопросы криптографии*, **5**:2 (2014), 103–108.

[19] Pilshchikov D. V., “On the limiting mean values in probabilistic models of time-memory-data tradeoff methods”, *Математические вопросы криптографии*, **6**:2 (2015), 59–65.

[20] Пильщиков Д. В., “Асимптотическое поведение мощности полного прообраза случайного множества при итерациях отображений конечного множества”, *Математические вопросы криптографии*, **8**:1 (2017), 95–106.

[21] Миронкин В. О., “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”, *Проблемы информационной безопасности. Компьютерные системы*, № 4 (2015), 140–146.

[22] Зубков А. М., Серов А. А., “Совокупность образов подмножества конечного множества при итерациях случайных отображений”, *Дискретная математика*, **26**:4 (2014), 43–50.

[23] Серов А. А., “Образы конечного множества при итерациях двух случайных зависимых отображений”, *Дискретная математика*, **27**:4 (2015), 133–140.

[24] Зубков А. М., Серов А.А., “Предельная теорема для мощности образа подмножества при композиции случайных отображений”, *Дискретная математика*, **29**:1 (2017), 17–26.