

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.212.2+519.719.2

ОБ ОЦЕНКАХ РАСПРЕДЕЛЕНИЯ ДЛИНЫ ОТРЕЗКА АПЕРИОДИЧНОСТИ В ГРАФЕ k -КРАТНОЙ ИТЕРАЦИИ РАВНОВЕРОЯТНОГО СЛУЧАЙНОГО ОТОБРАЖЕНИЯ

В. О. МIRONKIN

*Национальный исследовательский университет «Высшая школа экономики»,
г. Москва, Россия*

Работа посвящена исследованию случайной величины $\tau_{fk}(x_0)$, равной длине отрезка апериодичности произвольной вершины $x_0 \in S = \{1, \dots, n\}$, $n \in \mathbb{N}$, в графе k -кратной итерации равновероятного случайного отображения $f : S \rightarrow S$. Отрезком апериодичности, начинающимся в вершине $x_0 \in S$, называется отрезок выходящей из x_0 траектории от x_0 до её первого самопересечения. Исследовано поведение локальной вероятности $\mathbb{P}\{\tau_{fk}(x_0) = z\}$ как функционала от $z \in S$ при фиксированных значениях параметров $k, n \in \mathbb{N}$. Получена двусторонняя оценка $\mathbb{P}\{\tau_{fk}(x_0) = z\}$ для произвольных $k \in \mathbb{N}$, $x_0, z \in S$, таких, что $kz < n$. Для случаев простого k и $k^2 z \leq n$ получены эффективно вычисляемые для используемых на практике значений n (2^{256} и более) двусторонние оценки $\mathbb{P}\{\tau_{fk}(x_0) = z\}$, выраженные в элементарных функциях. Для произвольных $k \in \mathbb{N}$, $x_0, z \in S$ выписаны двусторонние оценки для функции распределения $F_{\tau_{fk}(x_0)}(z)$ в случаях $kz < n/2$ и $kz \leq \sqrt{n}$.

Ключевые слова: равновероятное случайное отображение, итерация случайного отображения, граф отображения, отрезок апериодичности, локальная вероятность, распределение.

DOI 10.17223/20710410/42/1

ON ESTIMATIONS OF DISTRIBUTION OF THE LENGTH OF APERIODICITY SEGMENT IN THE GRAPH OF k -FOLD ITERATION OF UNIFORM RANDOM MAPPING

V. O. MIRONKIN

National Research University Higher School of Economics, Moscow, Russia

E-mail: mironkin.v@mail.ru

Given $k, n \in \mathbb{N}$, $x_0 \in S = \{1, \dots, n\}$, and $f : S \rightarrow S$, define $x_{i+1} = f^k(x_i)$ for every $i \in \{0, 1, \dots\}$ and $\tau_{fk}(x_0)$ as the least integer i such that $f^k(x_i) = x_j$ for some j , $j < i$. For the local probability $\mathbb{P}\{\tau_{fk}(x_0) = z\}$ and for the distribution function $F_{\tau_{fk}(x_0)}(z)$, the following estimates are obtained. If $kz < n$, then

$$P\{\tau_{fk}(x_0)=z\} > \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)}=z}} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} + \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \frac{1}{r+k} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right),$$

$$P\{\tau_{fk}(x_0)=z\} < \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)}=z}} e^{-\frac{(m-1)^2}{2n}} + \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \frac{1}{r} e^{-\frac{(r-1)^2}{2n}} \left(1 - \left(1 - \frac{r}{n}\right)^k\right),$$

where $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$. If $k^2z \leq n$, then

$$\frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)}=z}} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} + \left(1 - \frac{k^2z}{2n}\right) \frac{k}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} <$$

$$< P\{\tau_{fk}(x_0)=z\} < \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)}=z}} e^{-\frac{(m-1)^2}{2n}} + \frac{k}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} e^{-\frac{(r-1)^2}{2n}},$$

which, for a prime k , is expressed in elementary functions and efficiently computable for used in practice values of n (2^{256} and more). Also, if $kz \leq \sqrt{n}$, then

$$\sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \frac{r}{n} \left(1 - \frac{r(m+r)}{2n}\right) e^{-(1+\frac{m}{n})\frac{m^2}{2n}} < F_{\tau_{fk}(x_0)}(z) < \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \frac{r+1}{n} e^{-\frac{(m-1)^2}{2n}},$$

where $r = m + \left(z - \frac{m}{(m,k)}\right)k$. In some cases, the obtained results allow to estimate the allowable period of usage of the encryption keys generated by iterative algorithms and to build criteria for quality assessment of random sequences.

Keywords: *equiprobable random mapping, iteration of random mapping, graph of a mapping, aperiodicity segment, local probability, distribution.*

Введение

Изучение моделей отображений, построенных на основе случайных равновероятных отображений, представляет собой важную задачу современной теории вероятностей и криптографии. Методика решения большого класса задач, связанных со случайными отображениями, достаточно полно проработана [1, 2], что позволяет строить новые математические модели [3, 4], адекватно описывающие особенности функционирования современных криптографических примитивов. Подобные модели находят применение, например, в рамках исследований свойств и характеристик итерационных алгоритмов преобразования данных, алгоритмов хэширования и выработки псевдослучайных последовательностей.

Данная работа посвящена изучению класса отображений, состоящего из итераций равновероятного случайного отображения, и продолжает цикл исследований [5–10].

Рассмотрим конечное множество $S = \{1, \dots, n\}$, $n > 1$, и пространство равновероятных случайных отображений $(\Omega, \mathcal{F}, P)$, в котором пространством элементарных исходов Ω является множество всех n^n отображений S в себя, алгеброй событий $\mathcal{F}$ — множество всех подмножеств Ω , а вероятностная мера P задана следующим образом:

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

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

Для произвольного $k \in \mathbb{N}$ через f^k обозначим k -кратную итерацию $\underbrace{f(\dots(f(x)\dots))}_k$ отображения f и введём множества отображений

$$\Omega_k = \{f^k : f \in \Omega\}.$$

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

Замечание 1. Распределение f^k не является равновероятным ни на Ω , ни на Ω_k .

Вопросы, связанные с описанием момента первого возвращения в пройденную траекторию, начатую в произвольной вершине $x_0 \in S$ графа G_{f^k} , при действии случайного отображения f^k , $k \geq 1$,

$$x_{i+1} = f^k(x_i), i = 0, 1, 2, \dots,$$

представляют как теоретический, так и практический интерес для ряда приложений криптографии [11–13]. Так, например, при исследовании криптографических свойств итерационных алгоритмов выработки производных ключей одной из наиболее существенных характеристик является число тактов работы алгоритма до появления ранее использованного ключа [14]. В частности, указанная характеристика позволяет определить допустимый срок эксплуатации долговременных ключей шифрования в зависимости от используемого алгоритма выработки производных ключей.

Определение 2. Отрезком апериодичности, начинающимся в вершине $x_0 \in S$ графа G_f , называется отрезок выходящей из x_0 траектории от x_0 до её первого самопересечения.

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

$$\tau_f(x_0) = \min_{t \in \mathbb{N}} \{t : f^t(x_0) \in \{x_0, f(x_0), \dots, f^{t-1}(x_0)\}\}.$$

При этом справедливо соотношение

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

где $\alpha_f(x_0)$ — высота вершины x_0 (расстояние от x_0 до ближайшей циклической вершины); $\beta_f(x_0)$ — длина цикла компоненты G_f , содержащей вершину x_0 .

Замечание 2. Случайные величины $\tau_f(x_0)$, $\alpha_f(x_0)$, $\beta_f(x_0)$ зависят от параметра n . Однако с целью упрощения восприятия материала данная зависимость отражаться не будет.

1. Оценки локальной вероятности

Для любых $i_0, i_1 \in \mathbb{Z}$, $i_0 > i_1$, положим $\prod_{j=i_0}^{i_1} (\dots) \equiv 1$. В работе [5] получено точное выражение для локальной вероятности $P\{\tau_{f^k}(x_0) = z\}$:

$$P\{\tau_{f^k}(x_0) = z\} = \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right) + \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \sum_{v=1}^k \prod_{i=1}^{m + \left(z - \frac{m}{(m,k)}\right)k - v} \left(1 - \frac{i}{n}\right), \quad (2)$$

которое может быть использовано при описании вероятностных свойств ряда криптографических алгоритмов. Так, например, для алгоритмов выработки ключевых последовательностей величина $P\{\tau_{fk}(x_0) = 1\}$ соответствует событию, заключающемуся в выборе самого «слабого» долговременного ключа x_0 , порождающего вырожденную последовательность производных ключей вида $x_0, x_0, \dots$, а величина $P\{\tau_{fk}(x_0) = n\}$ — событию, заключающемуся в выработке максимального числа неповторяющихся ключей, позволяющих обеспечить шифрование максимального объёма данных.

В таблице для случая $n = 256$ представлены приближённые значения вероятности $P\{\tau_{fk}(x_0) = z\}$ при некоторых z, k и произвольном выборе $x_0 \in S$.

$z \setminus k$	1	2	3	4
1	$3,9 \cdot 10^{-3}$	$7,8 \cdot 10^{-3}$	$7,8 \cdot 10^{-3}$	$1,2 \cdot 10^{-2}$
2	$7,8 \cdot 10^{-3}$	$1,9 \cdot 10^{-2}$	$3,0 \cdot 10^{-2}$	$4,9 \cdot 10^{-2}$
2^2	$1,5 \cdot 10^{-2}$	$4,0 \cdot 10^{-2}$	$5,6 \cdot 10^{-2}$	$8,7 \cdot 10^{-2}$
2^4	$3,9 \cdot 10^{-2}$	$4,0 \cdot 10^{-2}$	$2,7 \cdot 10^{-2}$	$2,3 \cdot 10^{-2}$
2^6	$4,5 \cdot 10^{-5}$	$2,7 \cdot 10^{-6}$	$2,3 \cdot 10^{-6}$	$2,3 \cdot 10^{-6}$
2^8	$2,7 \cdot 10^{-110}$	$1,0 \cdot 10^{-112}$	$1,0 \cdot 10^{-112}$	$1,0 \cdot 10^{-112}$

Анализ выражения (2) показал, что при фиксированных n и k максимум вероятности $P\{\tau_{fk}(x_0) = z\}$ достигается при z , принадлежащем некоторой окрестности $\sqrt{\frac{\pi n}{2k}}$. При этом в случае простого k величина $P\{\tau_{fk}(x_0) = z\}$ монотонно возрастает до своего единственного максимума и затем монотонно убывает, а в случае составного k ведёт себя немонотонно (рис. 1).

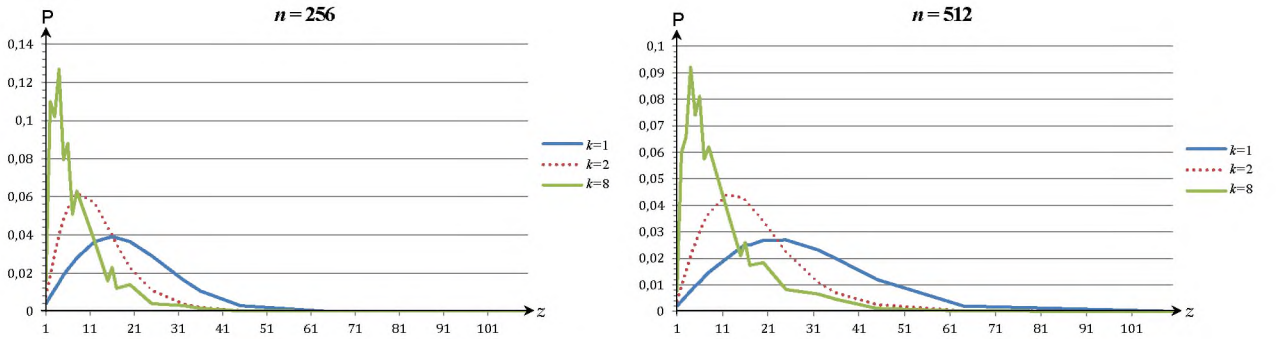


Рис. 1. Зависимость $P\{\tau_{fk}(x_0) = z\}$ от величины z

Следует заметить, что выражение (2) имеет достаточно сложный аналитический вид, что может создавать трудности при вычислении $P\{\tau_{fk}(x_0) = z\}$ для больших значений n . В связи с этим становится актуальной задача получения оценочных выражений величины $P\{\tau_{fk}(x_0) = z\}$, эффективно вычисляемых без привлечения высокопроизводительных ЭВМ.

Утверждение 1. Пусть случайное отображение $f : S \rightarrow S$ имеет распределение (1) на Ω . Тогда при любых таких $k \in \mathbb{N}$, $x_0, z \in S$, что $kz < n$, справедливы следующие неравенства:

$$P\{\tau_{fk}(x_0) = z\} > \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} + \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \frac{1}{r+k} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right); \quad (3)$$

$$P\{\tau_{fk}(x_0) = z\} < \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} e^{-\frac{(m-1)^2}{2n}} + \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \frac{1}{r} e^{-\frac{(r-1)^2}{2n}} \left(1 - \left(1 - \frac{r}{n}\right)^k\right), \quad (4)$$

где $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$.

Доказательство. Представим выражение (2) в эквивалентном виде:

$$P\{\tau_{fk}(x_0) = z\} = \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right) + \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} \sum_{v=1}^k \prod_{i=1}^{m + \left(z - \frac{m}{(m,k)} - 1\right)k + v - 1} \left(1 - \frac{i}{n}\right). \quad (5)$$

Рассмотрим второе слагаемое в (5) и преобразуем сумму вида $\sum_{v=1}^k \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n}\right)$, где $r \geq 1$, таким образом:

$$\sum_{v=1}^k \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n}\right) = \prod_{i=1}^{r-1} \left(1 - \frac{i}{n}\right) \sum_{w=0}^{k-1} \prod_{j=0}^w \left(1 - \frac{r+j}{n}\right).$$

При этом для $0 < \frac{r}{n} < \frac{r+k}{n} < 1$ справедливы следующие оценки сверху и снизу:

$$\begin{aligned} \sum_{w=0}^{k-1} \prod_{j=0}^w \left(1 - \frac{r+j}{n}\right) &< \sum_{w=0}^{k-1} \left(1 - \frac{r}{n}\right)^w = \frac{n}{r} \left(1 - \left(1 - \frac{r}{n}\right)^k\right), \\ \sum_{w=0}^{k-1} \prod_{j=0}^w \left(1 - \frac{r+j}{n}\right) &> \sum_{w=0}^{k-1} \left(1 - \frac{r+k}{n}\right)^w = \frac{n}{r+k} \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right). \end{aligned} \quad (6)$$

Тогда с учётом (6) и двустороннего неравенства [15]

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

справедливого для $1 \leq r \leq n$, получаем выражение

$$\frac{n}{r+k} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right) < \sum_{v=1}^k \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n}\right) < \frac{n}{r} e^{-\frac{(r-1)^2}{2n}} \left(1 - \left(1 - \frac{r}{n}\right)^k\right). \quad (7)$$

Положим $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$. Из ограничений на суммирование во втором слагаемом в (5) $\left(\frac{m}{(m,k)} < z \text{ и } m \geq 1\right)$ следует, что $r \geq 1$. Далее из условия $kz < n$ получаем цепочку неравенств:

$$r+k = m + \left(z - \frac{m}{(m,k)}\right)k = kz + m \left(1 - \frac{k}{(m,k)}\right) \leq kz < n.$$

Таким образом, $0 < \frac{r}{n} < \frac{r+k}{n} < 1$ и поэтому неравенство (7) выполняется для искомой вероятности. ■

При $k = 1$ результат утверждения 1 позволяет получить известное неравенство [4]:

$$\frac{z}{n} e^{-(1+\frac{z}{n})\frac{z^2}{2n}} < P \{ \tau_f(x_0) = z \} < \frac{z}{n} e^{-\frac{(z-1)^2}{2n}}.$$

Следует также заметить, что в случаях, когда число итераций k отображения f невелико или когда множество S имеет большую мощность, оценочные выражения для величины $P \{ \tau_f(x_0) = z \}$ имеют более простой вид.

Следствие 1. Пусть случайное отображение $f : S \rightarrow S$ имеет равномерное распределение (1) на Ω . Тогда при любых таких $k \in \mathbb{N}$ и $x_0, z \in S$, что $k^2 z \leq n$, справедливо двойное неравенство

$$\begin{aligned} & \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} + \left(1 - \frac{k^2 z}{2n}\right) \frac{k}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} < \\ & < P \{ \tau_{f^k}(x_0) = z \} < \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} = z}} e^{-\frac{(m-1)^2}{2n}} + \frac{k}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} < z}} e^{-\frac{(r-1)^2}{2n}}, \end{aligned} \quad (8)$$

где $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$.

Доказательство. Для оценки второй группы слагаемых в (3) и (4) рассмотрим двустороннее неравенство [16]

$$1 - kx \leq (1 - x)^k \leq 1 - kx + C_k^2 x^2, \quad (9)$$

справедливое при $-1 < x < 1$, где $k \in \mathbb{N}$. При этом левое неравенство в (9) является содержательным при $1 - kx \geq 0$, т. е. при $x \leq 1/k$. Покажем, что $x = r/n$ удовлетворяет неравенству $x \leq 1/k$. Учитывая, что $1 - \frac{k}{(m,k)} \leq 0$, имеем цепочку неравенств

$$\frac{r}{n} = \frac{m + \left(z - \frac{m}{(m,k)} - 1\right)k}{n} \leq \frac{kz + m \left(1 - \frac{k}{(m,k)}\right) - k}{n} \leq \frac{kz - k}{n} < \frac{kz}{n} \leq \frac{1}{k}.$$

Тогда искомая оценка сверху величины $P \{ \tau_{f^k}(x_0) = z \}$ следует из соотношений (3), (4) и (9) при $x = r/n$.

Содержательность правого неравенства в (9) имеет место при $1 - kx + C_k^2 x^2 \leq 1$, т. е. в случае $0 \leq x \leq \frac{2}{k-1}$, что справедливо для $x = \frac{r+k}{n}$:

$$0 < \frac{r+k}{n} = \frac{m + \left(z - \frac{m}{(m,k)}\right)k}{n} = \frac{kz + m \left(1 - \frac{k}{(m,k)}\right)}{n} \leq \frac{kz}{n} \leq \frac{2}{k-1}.$$

В итоге оценка снизу для $P \{ \tau_{f^k}(x_0) = z \}$ следует из соотношений (3), (4) и (9) при $x = \frac{r+k}{n}$. ■

Замечание 3. Точность неравенства (9) возрастает с уменьшением значения kx (увеличением n , соответственно). Поэтому для значений параметра n , используемых в ряде практических приложений и имеющих порядок 2^{256} и выше, выражение (8) позволяет получать достаточно точные приближения.

Отметим, что неравенства (3), (4) и (8) существенно зависят от канонического разложения k . Для значений k с малым числом собственных делителей соответствующие нерегулярные суммы заметно упрощаются.

Следствие 2. Пусть случайное отображение $f : S \rightarrow S$ имеет равномерное распределение (1) на Ω и k — простое. Тогда при любых таких $x_0, z \in S$, что $k^2 z \leq n$, справедливы следующие оценки сверху:

— при $z = 1$

$$\mathbf{P} \{ \tau_{fk}(x_0) = 1 \} < \frac{1}{n} \left(1 + e^{-\frac{(k-1)^2}{2n}} \right);$$

— при $z > 1, k \nmid z$

$$\mathbf{P} \{ \tau_{fk}(x_0) = z \} < \frac{kz - z + 2}{n} e^{-\frac{(z-2)^2}{2n}} + \frac{kz - k + 1}{n} e^{-\frac{k^2(z-2)^2}{2n}};$$

— при $z > 1, k|z$

$$\mathbf{P} \{ \tau_{fk}(x_0) = z \} < \frac{kz - z + 1}{n} e^{-\frac{(z-2)^2}{2n}} + \frac{kz - k + 1}{n} e^{-\frac{k^2(z-2)^2}{2n}}.$$

Доказательство. Пусть $z = 1$. При этом $\frac{m}{(m, k)} \geq 1$. Тогда равенство $\frac{m}{(m, k)} = 1$ выполняется только при $m \in \{1, k\}$, поэтому с учётом (8) оценка сверху принимает следующий вид:

$$\mathbf{P} \{ \tau_{fk}(x_0) = 1 \} < \frac{1}{n} \sum_{\substack{m \geq 1, \\ (m, k) = 1}} e^{-\frac{(m-1)^2}{2n}} = \frac{1}{n} \left(1 + e^{-\frac{(k-1)^2}{2n}} \right).$$

Пусть теперь $z > 1$, тогда

$$\frac{m}{(m, k)} = \begin{cases} m, & k \nmid m, \\ \frac{m}{k}, & k|m, \end{cases} \Rightarrow r = \begin{cases} m(1-k) + k(z-1), & k \nmid m, \\ k(z-1), & k|m. \end{cases}$$

Рассмотрим случай $k \nmid z$. Группируя слагаемые, стоящие в правой части неравенства (8) и соответствующие значениям m , таким, что $k \nmid m$ и $k|m$, получаем цепочку неравенств:

$$\begin{aligned} \mathbf{P} \{ \tau_{fk}(x_0) = z \} &< \frac{1}{n} \left(e^{-\frac{(z-1)^2}{2n}} + e^{-\frac{(kz-1)^2}{2n}} \right) + \frac{k}{n} \left(z - \frac{z-1}{k} \right) e^{-\frac{(z-2)^2}{2n}} + \\ &+ \frac{k(z-1)}{n} e^{-\frac{(k(z-1)-1)^2}{2n}} < \frac{kz - z + 2}{n} e^{-\frac{(z-2)^2}{2n}} + \frac{kz - k + 1}{n} e^{-\frac{k^2(z-2)^2}{2n}}. \end{aligned}$$

Для случая $k|z$, рассуждая аналогично, получаем

$$\begin{aligned} \mathbf{P} \{ \tau_{fk}(x_0) = z \} &< \frac{1}{n} e^{-\frac{(kz-1)^2}{2n}} + \frac{k}{n} \left(z - \frac{z-1}{k} \right) e^{-\frac{(z-2)^2}{2n}} + \\ &+ \frac{k(z-1)}{n} e^{-\frac{(k(z-1)-1)^2}{2n}} < \frac{kz - z + 1}{n} e^{-\frac{(z-2)^2}{2n}} + \frac{kz - k + 1}{n} e^{-\frac{k^2(z-2)^2}{2n}}. \end{aligned}$$

Следствие доказано. ■

Следствие 3. Пусть случайное отображение $f : S \rightarrow S$ имеет равномерное распределение (1) на Ω и k — простое. Тогда при любых таких $x_0, z \in S$, что $k^2 z < n$, справедливы следующие оценки снизу:

— при $z = 1$

$$\mathbb{P} \{ \tau_{fk}(x_0) = 1 \} > \frac{1}{n} \left(1 + e^{-(1+\frac{k}{n})\frac{k^2}{2n}} \right);$$

— при $z > 1, k \nmid z$

$$\mathbb{P} \{ \tau_{fk}(x_0) = z \} > \frac{1}{n} e^{-(1+\frac{z}{n})\frac{z^2}{2n}} + \frac{(2k-1)(z-1)(2n-k^2z) + 2n}{2n^2} e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}};$$

— при $z > 1, k|z$

$$\mathbb{P} \{ \tau_{fk}(x_0) = z \} > \frac{(2k-1)(z-1)(2n-k^2z) + 2n}{2n^2} e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}}.$$

Доказательство. Для $z = 1$ неравенство очевидно. Для $z > 1$, повторяя рассуждения следствия 2, при $k \nmid z$ получаем

$$\begin{aligned} \mathbb{P} \{ \tau_{fk}(x_0) = z \} &> \frac{1}{n} \left(e^{-(1+\frac{z}{n})\frac{z^2}{2n}} + e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}} \right) + \\ &+ \left(1 - \frac{k^2z}{2n} \right) \frac{k}{n} \left((z-1) \left(1 - \frac{1}{k} \right) e^{-\frac{(k(z-2)+1)^2}{2n}} + (z-1) e^{-\frac{k^2(z-1)^2}{2n}} \right) > \\ &> \frac{1}{n} e^{-(1+\frac{z}{n})\frac{z^2}{2n}} + \frac{(2k-1)(z-1)(2n-k^2z) + 2n}{2n^2} e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}}. \end{aligned}$$

Для случая $k|z$ имеем

$$\begin{aligned} \mathbb{P} \{ \tau_{fk}(x_0) = z \} &> \frac{1}{n} e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}} + \\ &+ \left(1 - \frac{k^2z}{2n} \right) \frac{k}{n} \left((z-1) \left(1 - \frac{1}{k} \right) e^{-\frac{(k(z-2)+1)^2}{2n}} + (z-1) e^{-\frac{k^2(z-1)^2}{2n}} \right) > \\ &> \frac{(2k-1)(z-1)(2n-k^2z) + 2n}{2n^2} e^{-(1+\frac{kz}{n})\frac{k^2z^2}{2n}}. \end{aligned}$$

Следствие доказано. ■

Замечание 4. Оценки, полученные в следствиях 2 и 3, могут быть эффективно вычислены для используемых на практике значений n .

Через $\nu_{fk}^{(z)}$, $k \in \mathbb{N}$, обозначим случайную величину, равную числу вершин в случайном графе G_{fk} , длина отрезка аperiodичности которых равна $z \in S$. Так как $E\nu_{fk}^{(z)} = n \mathbb{P} \{ \tau_{fk}(x_0) = z \}$, то с соответствующей поправкой на множитель n для величины $E\nu_{fk}^{(z)}$ справедливы все представленные выше результаты.

2. Оценки функции распределения

Из работы [5] известно точное выражение для функции распределения $F_{\tau_{fk}(x_0)}(z)$, $z \in S$, случайной величины $\tau_{fk}(x_0)$:

$$F_{\tau_{fk}(x_0)}(z) = \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \sum_{t=0}^{(z-\frac{m}{(m,k)})k} \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n} \right), \quad (10)$$

имеющее также ряд практических приложений. В частности, значения $F_{\tau_{fk}(x_0)}(z)$ могут быть использованы при оценке среднего допустимого объёма ключевого множества, вырабатываемого на основе фиксированного долговременного ключа с помощью некоторого итерационного алгоритма.

По причине, связанной со сложностью вычисления (10), получим оценочные выражения для величины $F_{\tau_{fk}(x_0)}(z)$.

Утверждение 2. Пусть случайное отображение $f : S \rightarrow S$ имеет распределение (1) на Ω . Тогда при любых таких $k \in \mathbb{N}$, $x_0, z \in S$, что $kz < n/2$, справедливо следующее двустороннее неравенство:

$$F_{\tau_{fk}(x_0)}(z) > \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} \left(\frac{1}{n} + \frac{1}{m+r} \left(1 - \left(1 - \frac{m+r}{n} \right)^r \right) \right); \quad (11)$$

$$F_{\tau_{fk}(x_0)}(z) < \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} e^{-\frac{(m-1)^2}{2n}} \left(\frac{1}{n} + \frac{1}{m} \left(1 - \left(1 - \frac{m}{n} \right)^r \right) \right). \quad (12)$$

Здесь $r = m + \left(z - \frac{m}{(m,k)} \right) k$.

Доказательство. Выделим в (10) слагаемые, соответствующие значению $t = 0$:

$$F_{\tau_{fk}(x_0)}(z) = \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right) + \frac{1}{n} \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \sum_{t=1}^{(z-\frac{m}{(m,k)})k} \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n} \right).$$

Рассмотрим сумму вида $\sum_{t=1}^r \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n} \right)$, где $m \geq 1$. При этом выполняется неравенство $0 < \frac{m}{n} < \frac{m+r}{n} < 1$. Действительно,

$$0 < \frac{m}{n} < \frac{m+r}{n} = \frac{2m + \left(z - \frac{m}{(m,k)} \right) k}{n} = \frac{kz + m \left(2 - \frac{k}{(m,k)} \right)}{n} \leq \frac{kz + m}{n} \leq \frac{2kz}{n} < 1.$$

Тогда, рассуждая, как в утверждении 1, получаем искомое выражение. ■

Следствие 4. Пусть случайное отображение $f : S \rightarrow S$ имеет распределение (1) на Ω . Тогда при любых таких $k \in \mathbb{N}$, $x_0, z \in S$, что $kz \leq \sqrt{n}$, справедливо

$$\sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \frac{r}{n} \left(1 - \frac{r(m+r)}{2n} \right) e^{-(1+\frac{m}{n})\frac{m^2}{2n}} < F_{\tau_{fk}(x_0)}(z) < \sum_{\substack{m \geq 1, \\ \frac{m}{(m,k)} \leq z}} \frac{r+1}{n} e^{-\frac{(m-1)^2}{2n}},$$

где $r = m + \left(z - \frac{m}{(m,k)} \right) k$.

Доказательство. Оценим снизу выражение $\frac{1}{n} + \frac{1}{m+r} \left(1 - \left(1 - \frac{m+r}{n} \right)^r \right)$, стоящее под знаком суммы в (11). Для $k = r$ правое неравенство в (9) содержательно при условии $x \leq \frac{2}{r-1}$, которое выполняется для $x = \frac{m+r}{n}$. Действительно,

$$\frac{m+r}{n} = \frac{2m + \left(z - \frac{m}{(m,k)} \right) k}{n} = \frac{kz + m \left(2 - \frac{k}{(m,k)} \right)}{n} \leq \frac{kz + m}{n} \leq \frac{2kz}{n} \leq \frac{2}{r-1},$$

где последнее неравенство справедливо в условиях следствия $kz(r-1) < (kz)^2 \leq n$. Тогда имеет место цепочка соотношений

$$\begin{aligned} \frac{1}{n} + \frac{1}{m+r} \left(1 - \left(1 - \frac{m+r}{n} \right)^r \right) &> \frac{1}{m+r} \left(1 - \left(1 - \frac{r(m+r)}{n} + \frac{r(r-1)(m+r)^2}{2n^2} \right) \right) = \\ &= \frac{r}{n} - \frac{r(r-1)(m+r)}{2n^2} > \frac{r}{n} - \frac{r^2(m+r)}{2n^2}, \end{aligned}$$

с учётом которой из (11) следует искомая нижняя оценка.

Левое неравенство в (9) для $k=r$ содержательно при $x \leq \frac{1}{r}$, что выполняется для $x = \frac{m}{n}$:

$$\frac{m}{n} \leq \frac{1}{r} \leq \frac{2}{r-1},$$

поскольку $mr \leq kZR < (kz)^2 \leq n$. Поэтому, оценивая сверху выражение $\frac{1}{n} + \frac{1}{m} \left(1 - \left(1 - \frac{m}{n} \right)^r \right)$ с помощью (9), получаем искомую оценку. ■

Заключение

В работе [5] для локальной вероятности и распределения длины отрезка аперiodичности получены точные выражения, которые находят применение в рамках исследований и развития модели k -кратной итерации равновероятного случайного отображения [17, 18]. Однако на практике размер задач (величина n), как правило, достигает значений порядка 2^{256} и выше, вследствие чего вычисление по полученным в [5] формулам на персональных ЭВМ (без привлечения дополнительного оборудования) становится затруднительным.

Результаты настоящей работы позволяют эффективно оценивать значения соответствующих характеристик для практических задач современной криптографии. В частности, они могут быть использованы при построении статистических критериев выявления неравновероятности в последовательностях, формируемых на основе итерационных алгоритмов.

ЛИТЕРАТУРА

1. Колчин В. Ф. Случайные отображения. М.: Наука, 1984.
2. Harris B. Probability distributions related to random mapping // Ann. Math. Statist. 1960. V. 31. No. 4. P. 1045–1062.
3. Dalal A. and Schmutz E. Compositions of random functions on a finite set // Electr. J. Comb. 2002. V. 9. No. R26.
4. Flajolet P. and Odlyzko A. Random mapping statistics // LNCS. 1989. V. 434. P. 329–354.
5. Зубков А. М., Миронкин В. О. Распределение длины отрезка аперiodичности в графе k -кратной итерации случайного равновероятного отображения // Математические вопросы криптографии. 2017. Т. 8. № 4. С. 63–74.
6. Миронкин В. О., Михайлов В. Г. О множестве образов k -кратной итерации равновероятного случайного отображения // Математические вопросы криптографии. 2018. Т. 9. № 3. С. 99–108.
7. Миронкин В. О. Исследование свойств и характеристик степени случайного отображения // Обзорение прикладной и промышленной математики. 2014. Т. 21. № 1. С. 70–73.
8. Миронкин В. О. Вероятностные характеристики слоев в графе случайного отображения // Обзорение прикладной и промышленной математики. 2015. Т. 22. № 1. С. 80–82.

9. МIRONKIN В. О. Совместная вероятность длин отрезков аперидичности двух вершин в графе степени случайного отображения // Обозрение прикладной и промышленной математики. 2015. Т. 22. № 4. С. 482–484.
10. МIRONKIN В. О. Об особенностях строения графа степени случайного отображения // Обозрение прикладной и промышленной математики. 2016. Т. 23. № 1. С. 57–62.
11. Oechslin P. Making a faster cryptanalytic time-memory trade-off // LNCS. 2003. V. 2729. P. 617–630.
12. 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. 2014. Т. 5. № 2. С. 103–108.
13. Pilshchikov D. V. On the limiting mean values in probabilistic models of time-memory-data tradeoff methods // Математические вопросы криптографии. 2015. Т. 6. № 2. С. 59–65.
14. МIRONKIN В. О. О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING» // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 140–146.
15. Токарева Н. Н. Симметричная криптография. Краткий курс: учебное пособие. Новосибирск: Новосиб. гос. ун-т, 2012.
16. Сачков В. Н. Вероятностные методы в комбинаторном анализе. М.: Наука, 1978.
17. Зубков А. М., Серов А. А. Совокупность образов подмножества конечного множества при итерациях случайных отображений // Дискретная математика. 2014. Т. 26. № 4. С. 43–50.
18. Пильщиков Д. В. Асимптотическое поведение мощности полного прообраза случайного множества при итерациях отображений конечного множества // Математические вопросы криптографии. 2017. Т. 8. № 1. С. 95–106.

REFERENCES

1. Kolchin V. F. Sluchaynie otobrazeniya [Random Mappings]. Moscow, Nauka Publ., 1984. (in Russian)
2. Harris B. Probability distributions related to random mapping. Ann. Math. Statist., 1960, vol. 31, no. 4, pp. 1045–1062.
3. Dalal A. and Schmutz E. Compositions of random functions on a finite set. Electr. J. Comb., 2002, vol. 9, no. R26.
4. Flajolet P. and Odlyzko A. Random mapping statistics. LNCS, 1989, vol. 434, pp. 329–354.
5. Zubkov A. M. and Mironkin V. O. Raspredelenie dlini otrezka aperiodichnosti v grafe k -kratnoy iteracii sluchaynogo ravnoveryatnogo otobrazeniya [Distribution of the length of aperiodicity segment in the graph of k -fold iteration of uniform random mapping]. Mat. Vopr. Kriptogr., 2017, vol. 8, no. 4, pp. 63–74. (in Russian)
6. Mironkin V. O. and Mikhailov V. G. O mnozestve obrazov k -kratnoy iteracii ravnoveryatnogo sluchaynogo otobrazeniya [On the sets of images of k -fold iteration of uniform random mapping]. Mat. Vopr. Kriptogr., 2018, vol. 9, no. 3, pp. 99–108. (in Russian)
7. Mironkin V. O. Issledovanie svoystv i harakteristik stepeni sluchaynogo otobrazeniya [Investigation of properties and characteristics of iteration of random mapping]. Obozrenie Prikladnoj i Promyshlennoj Matematiki, 2014, vol. 21, no. 1, pp. 70–73. (in Russian)
8. Mironkin V. O. Veroyatnostnie harakteristiki slojov v grafe sluchaynogo otobrazeniya [Probabilistic characteristics of layers in a random mapping draph]. Obozrenie Prikladnoj i Promyshlennoj Matematiki, 2015, vol. 22, no. 1, pp. 80–82. (in Russian)
9. Mironkin V. O. Sovmestnaya veroyatnost dlin otrezkov aperiodichnosti dvuh vershin v grafe stepeni sluchaynogo otobrazeniya [The joint probability of lengths of aperiodicity segments

- of two vertices in the graph of iteration of random mapping]. *Obozrenie Prikladnoj i Promyshlennoj Matematiki*, 2015, vol. 22, no. 4, pp. 482–484. (in Russian)
10. *Mironkin V. O.* Ob osobennostyah stroeniya grafa stepeni sluchaynogo otobrazeniya [On singularities of the structure of the graph of iteration of random mapping]. *Obozrenie Prikladnoj i Promyshlennoj Matematiki*, 2016, vol. 23, no. 1, pp. 57–62. (in Russian)
 11. *Oechslin P.* Making a faster cryptanalytic time-memory trade-off. *LNCS*, 2003, vol. 2729, pp. 617–630.
 12. *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. *Mat. Vopr. Kriptogr.*, 2014, vol. 5, no. 2, pp. 103–108.
 13. *Pilshchikov D. V.* On the limiting mean values in probabilistic models of time-memory-data tradeoff methods. *Mat. Vopr. Kriptogr.*, 2015, vol. 6, no. 2, pp. 59–65.
 14. *Mironkin V. O.* O nekotoryh veroyatnostnih harakteristikah algoritma virabotki klucha “CRYPTOPRO KEY MESHING” [On some probabilistic characteristics of key derivation function “CRYPTOPRO KEY MESHING”]. *Problemy Informacionnoj Bezopasnosti. Komp'yuternye Sistemy*, 2015, no. 4, pp. 140–146. (in Russian)
 15. *Tokareva N. N.* Simmetrichnaya kriptografiya. Kratkiy kurs: uchebnoe posobie [Symmetric Cryptography. A Short Course: a Tutorial]. Novosibirsk, NSU Publ., 2012. (in Russian)
 16. *Sachkov V. N.* Veroyatnostnie metodi kombinatornogo analiza [Probabilistic Methods in Combinatorial Analysis]. Moscow, Nauka Publ., 1978. (in Russian)
 17. *Zubkov A. M. and Serov A. A.* Sovokupnost obrazov podmnozestva konechnogo mnozestva pri iteratsiyah sluchaynih otobrazeni [Images of subset of finite set under iterations of random mappings]. *Discr. Math.*, 2014, vol. 26, no. 4, pp. 43–50. (in Russian)
 18. *Pilshchikov D. V.* Asimptoticheskoe povedenie mochnosti polnogo proobraza sluchaynogo mnozestva pri iteratsiyah otobrazeniy konechnogo mnozestva [Asymptotic behaviour of the complete preimage cardinality for the image of a random set under iterations of mappings of a finite set]. *Mat. Vopr. Kriptogr.*, 2017, vol. 8, no. 1, pp. 95–106. (in Russian)