Math-Net.Ru

Общероссийский математический портал

Д. В. Пильщиков, Асимптотическое поведение мощности полного прообраза образа случайного множества при итерациях отображений конечного множества, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 1, 95–106

DOI: <https://doi.org/10.4213/mvk217>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 16:31:41

**Асимптотическое поведение мощности полного
прообраза образа случайного множества при итерациях
отображений конечного множества**

Д. В. Пильщиков

Лаборатории ТВП, Москва

Получено 30.V.2016

Аннотация. В связи с оценками сложности алгоритмов балансировки времени-памяти-данных возникают задачи оценки мощности полного прообраза образа случайного множества при многократных итерациях отображений. Предложена вероятностная модель, описывающая мощности исследуемых случайных множеств величинами, зависящими от числа частиц и суммарного числа частиц в процессе Гальтона – Ватсона. Найдены пределы математических ожиданий этих случайных величин.

Ключевые слова: образ случайного множества, мощность прообраза, метод Хеллмана, балансировка времени-памяти с особыми точками

**Asymptotic behaviour of the complete preimage cardinality for
the image of a random set under iterations of mappings of a finite set**

D. V. Pilshchikov

TVP Laboratories, Moscow

Abstract. The estimation of complexity of time-memory-data tradeoff algorithms leads to the estimation problems of the complete preimage cardinality for the image of a random set under multiple iterations of mappings. We describe a probabilistic model allowing to estimate the cardinalities of the random sets considered via the number of particles and the total number of particles in the Galton – Watson process. The limits of mean values of these random variables are found.

Key words: image of a random set, preimage cardinality, Hellman method, time-memory tradeoff with distinguished points

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 95–106 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

Задачу обращения однонаправленной функции можно сформулировать следующим образом. Пусть имеется однонаправленная функция

$$G : X \rightarrow X,$$

заданная на множестве X , $|X| = N$, и набор $\mathcal{D}$, состоящий из D элементов множества X вида

$$\mathcal{D} = \{y_i \in X \mid y_i = G(x_i), i \in \{1, \dots, D\}\},$$

где $\{x_i \in X, i \in \{1, \dots, D\}\} = \overline{\mathcal{D}}$ — некоторое неизвестное множество. Требуется по множеству $\mathcal{D}$ найти хотя бы один элемент множества $\overline{\mathcal{D}}$.

Для решения данной задачи широко используются три следующих переборных метода, относящихся к классу балансировок времени-памяти-данных:

- метод Хеллмана [3] (далее *HM*-метод),
- метод с особыми точками [2, 6] (далее *DP*-метод),
- метод с радужными таблицами [5] (далее *RM*-метод).

Все методы данного класса состоят из двух этапов: предварительного и оперативного. В течение обоих этапов строятся цепочки F -операций. Каждая из цепочек представляет собой последовательное вычисление функций (далее F -операций) вида

$$F(x) = R(G(x)), \quad x \in X,$$

где $R : X \rightarrow X$ — некоторое биективное отображение.

На предварительном этапе производятся наработка и сохранение таблиц. Для построения одной таблицы вычисляется m цепочек F -операций (табличных цепочек), которые начинаются из элементов псевдослучайного множества $S \subset X$. В таблице записываются начала и концы вычисляемых цепочек.

Решение задачи обращения однонаправленной функции происходит на оперативном этапе, при этом используются построенные таблицы. В процессе выполнения оперативного этапа строятся цепочки двух типов: основные и дополнительные. Основные цепочки начинаются из элементов множества $\mathcal{D}$. Если конец основной цепочки совпадает с записанным в таблице концом одной из табличных цепочек, то из ее начала проводится дополнительная цепочка F -операций. Решение x ищется среди элементов дополнительных цепочек с помощью проверки соотношений вида

$$G(x) = y_i, \quad i \in 1, \dots, D.$$

В целях понижения сложности НМ-, DP- и RM-методов в [1, 6, 7] были предложены их модификации. В [1] описаны DP- и RM-методы с совершенными таблицами (далее *DPP*- и *RMP*-методы). В [6] указана возможность использования в DP- и DPP-методах ограничений на длину цепочек, а также размещения в таблице, кроме начала и конца цепочки, некоторой дополнительной информации о ее длине.

Методы балансировки времени-памяти-данных характеризуются такими параметрами, как мощность множества X , длина цепочек, размер и количество таблиц. Их характеризуют также такие величины, как надежность, (среднее) число F -операций, выполненных на предварительном и оперативном этапах (при построении как основных, так и дополнительных цепочек). В связи с задачей эффективной реализации методов балансировки времени-памяти-данных возникает задача построения оценок, описывающих взаимосвязь параметров и характеристик метода. Обзор результатов по данной тематике можно найти в [8].

В [4] отмечена связь между задачами оценки среднего числа F -операций, выполненных при построении дополнительных цепочек в НМ- и DPP-методах, и задачей оценки средней мощности полного прообраза образа случайного подмножества при итерациях случайного отображения.

В данной работе предлагается теоретико-вероятностная модель, отличная от использованной в [4]. Она позволяет уточнить и обобщить приведенные в [4] оценки. Полученные результаты можно применять для расчета оценок сложности построения дополнительных цепочек в DPP-методе при использовании ограничений на длину цепочки и записи в таблицу дополнительной информации о длине цепочки.

1. Описание изучаемых величин

Рассмотрим множества

$$S \subset X, \quad |S| = m, \quad \Theta \subset X, \quad |\Theta| = \frac{1}{t}N, \quad t > 1,$$

пусть t_1 — натуральное число.

Множество S будем называть множеством *начальных точек*, множество Θ — множеством *особых точек*, а число t_1 — *ограничением длины цепочки сверху*.

Зафиксируем отображение

$$F: X \rightarrow X.$$

Введем следующие обозначения:

$F^{(k)}$ — k -кратная итерация отображения F :

$$F^{(k)}(x) = \underbrace{F \circ F \circ \dots \circ F}_k(x), \quad F^{(0)}(x) = x,$$

$\tilde{F}^{(k)}(x)$, $k \in \{0, \dots, N\}$, — множество точек полного прообраза x относительно $F^{(k)}$ при $k > 0$, удовлетворяющих дополнительным условиям:

$$\tilde{F}^{(k)}(x) = \{x' \in X \mid F^{(k)}(x') = x, F^{(i)}(x') \neq x, i \in \{0, \dots, k-1\}\},$$

$\tau(x)$ — наименьшее целое число из диапазона $0, \dots, t_1$, при котором выполняется либо условие $F^{(\tau(x))}(x) \in \Theta$, либо условие $\tau(x) = t_1$,

F_Θ — отображение, задаваемое соотношением

$$F_\Theta(x) = F^{(\tau(x))}(x),$$

$\tilde{F}_\Theta^{(k)}(\theta)$, $k \in \{0, \dots, t_1\}$, — множество точек полного прообраза точки $\theta \in \Theta$ относительно F_Θ , удовлетворяющих дополнительным условиям:

$$\tilde{F}_\Theta^{(k)}(\theta) = \{x' \in X \mid F_\Theta(x') = \theta, \tau(x') = k\},$$

$S_\Theta^{(j)}$, $1 \leq j \leq t_1$, — подмножество S , задаваемое формулой

$$S_\Theta^{(j)} = S \cap \left\{ \bigcup_{k=j}^{t_1} \tilde{F}_\Theta^{(k)}(\Theta) \right\},$$

$\underline{q}(i, j)$ — мощность множества $\tilde{F}^{(i)}(F^{(j)}(S))$,

$\underline{q}_\Theta(i, j)$ — мощность множества $\tilde{F}_\Theta^{(i)}(F_\Theta(S_\Theta^{(j)}))$.

Далее в работе изучаются величины $\underline{q}(i, j)$ и $\underline{q}_\Theta(i, j)$. Они следующим образом связаны с характеристиками этапа построения дополнительных цепочек в НМ- и DPP-методах.

Пусть в НМ-методе на оперативном этапе обрабатывается таблица, порожденная цепочками длины j . В этом случае для основной цепочки длины i дополнительная цепочка существует тогда и только тогда, когда основная цепочка начинается в одном из $\underline{q}(i, j)$ элементов множества $\tilde{F}^{(i)}(F^{(j)}(S))$.

Пусть в DPP-методе на оперативном этапе обрабатывается таблица, в которой использовалось множество особых точек Θ . В этом случае основная цепочка имеет длину i , и для нее дополнительная цепочка длины не менее j существует тогда и только тогда, когда основная цепочка начинается в одном из $\underline{q}_\Theta(i, j)$ элементов множества $\tilde{F}_\Theta^{(i)}(F_\Theta(S_\Theta^{(j)}))$.

2. Представление среднего значения изучаемых величин

Пусть теперь каждый элемент множества X независимо от других элементов множества X с вероятностью $\frac{m}{N}$ является началом цепочки, а с вероятностью $1 - \frac{m}{N}$ не является началом цепочки. В данной вероятностной модели множество начал цепочек S является случайным и для любого фиксированного множества $A \subset X$ выполняется соотношение

$$\mathbf{E} I \{A \cap S = \emptyset\} = \left(1 - \frac{m}{N}\right)^{|A|}.$$

Подсчитаем средние значения $\bar{q}(i, j)$ и $\bar{q}_{\Theta}(i, j)$ случайных величин $\underline{q}(i, j)$ и $\underline{q}_{\Theta}(i, j)$.

Верна следующая цепочка равенств:

$$\begin{aligned} \underline{q}(i, j) &= |\tilde{F}^{(i)}(F^{(j)}(S))| = \\ &= \sum_{x \in X} |\tilde{F}^{(i)}(x)| I \{x \in F^{(j)}(S)\} = \\ &= \sum_{x \in X} |\tilde{F}^{(i)}(x)| \left(1 - I \{\tilde{F}^{(j)}(x) \cap S = \emptyset\}\right). \end{aligned}$$

Следовательно,

$$\begin{aligned} \bar{q}(i, j) &= \mathbf{E} |\tilde{F}^{(i)}(F^{(j)}(S))| = \\ &= \sum_{x \in X} |\tilde{F}^{(i)}(x)| \cdot (1 - \mathbf{E} I \{\tilde{F}^{(j)}(x) \cap S = \emptyset\}) = \\ &= \sum_{x \in X} |\tilde{F}^{(i)}(x)| \cdot \left(1 - \left(1 - \frac{m}{N}\right)^{|\tilde{F}^{(j)}(x)|}\right). \end{aligned}$$

Используя формулу Тейлора, легко получить следующую двустороннюю оценку:

$$\frac{m}{N} |\tilde{F}^{(j)}(x)| - \frac{1}{2} |\tilde{F}^{(j)}(x)|^{[2]} \left(\frac{m}{N}\right)^2 \leq 1 - \left(1 - \frac{m}{N}\right)^{|\tilde{F}^{(j)}(x)|} \leq \frac{m}{N} |\tilde{F}^{(j)}(x)|,$$

где $y^{[k]} = y(y-1) \cdots (y-k+1)$ — это k -я факториальная степень числа y .

Отсюда следуют оценки

$$\bar{q}_1(i, j) - \bar{q}_0(i, j) \leq \bar{q}(i, j) \leq \bar{q}_1(i, j), \quad (1)$$

$$\bar{q}_0(i, j) = \frac{1}{2} \left(\frac{m}{N} \right)^2 \sum_{x \in X} |\tilde{F}^{(i)}(x)| \cdot |\tilde{F}^{(j)}(x)|^2, \quad (2)$$

$$\bar{q}_1(i, j) = \frac{m}{N} \sum_{x \in X} |\tilde{F}^{(i)}(x)| \cdot |\tilde{F}^{(j)}(x)|. \quad (3)$$

Из равенств

$$\begin{aligned} q_{\Theta}(i, j) &= |\tilde{F}_{\Theta}^{(i)}(F_{\Theta}(S_{\Theta}^{(j)}))| = \\ &= \sum_{\theta \in \Theta} |\tilde{F}_{\Theta}^{(i)}(\theta)| \cdot I \{ \theta \in F_{\Theta}(S_{\Theta}^{(j)}) \} = \\ &= \sum_{\theta \in \Theta} |\tilde{F}_{\Theta}^{(i)}(\theta)| \cdot (1 - I \{ \bigcup_{k=j}^{t_1} \tilde{F}_{\Theta}^{(k)}(\theta) \cap S = \emptyset \}) \end{aligned}$$

следует, что

$$\begin{aligned} \bar{q}(i, j) = \mathbf{E} q_{\Theta}(i, j) &= \sum_{\theta \in \Theta} |\tilde{F}_{\Theta}^{(i)}| \cdot \left(1 - \mathbf{E} I \{ \bigcup_{k=j}^{t_1} \tilde{F}_{\Theta}^{(k)}(\theta) \cap S = \emptyset \} \right) = \\ &= \sum_{\theta \in \Theta} |\tilde{F}_{\Theta}^{(i)}| \cdot \left(1 - \left(1 - \frac{m}{N} \right)^{|\bigcup_{k=j}^{t_1} \tilde{F}_{\Theta}^{(k)}(\theta)|} \right). \end{aligned} \quad (4)$$

3. Некоторые оценки среднего значения изучаемых величин

Пусть теперь F — случайное равновероятное отображение. Так как значения $\bar{q}(i, j)$, $\bar{q}_0(i, j)$, $\bar{q}_1(i, j)$ и $\bar{q}_{\Theta}(i, j)$, определенные формулами (1)–(4), зависят от F , то они становятся случайными величинами. Опишем подход, с помощью которого получим оценки $\hat{q}(i, j)$, $\hat{q}_0(i, j)$, $\hat{q}_1(i, j)$, $\hat{q}_{\Theta}(i, j)$ среднего значения данных случайных величин.

При построении оценок $\hat{q}_0(i, j)$, $\hat{q}_1(i, j)$ будем пренебрегать зависимостью между случайными величинами $\xi(x)$, $x \in X$, равными количеству непосредственных прообразов точки x из множества $X \setminus x$ относительно отображения F , и считать, что они независимы в совокупности.

Поэтому распределение случайных величин вида $|\tilde{F}^{(k)}(x)|$, $x \in X$, будем считать совпадающим с распределением числа $\mu(k)$ частиц, существующих в момент времени k , в процессе Гальтона–Ватсона $\mu(k)$, $k = 0, 1, \dots$, определяемом соотношениями

$$\mu(0) = 1, \quad \mathbf{P}\{\mu(1) = j\} = \mathbf{P}\{\xi(x) = j\}, \quad j = 0, 1, \dots$$

(распределение в правой части индуцируется F и не зависит от x).

Можно показать, что первый момент случайной величины $\mu(1)$ равен 1, а два ее следующих факториальных момента при $N \rightarrow \infty$ стремятся к 1.

В качестве оценок $\hat{q}_0(i, j)$, $\hat{q}_1(i, j)$ средних значений случайных величин $\bar{q}_0(i, j)$, $\bar{q}_1(i, j)$ рассмотрим средние значения случайных величин, полученных из формул (2), (3) посредством замены случайных величин вида $|\tilde{F}^{(k)}(x)|$, $k = 0, 1, \dots$, при любых $x \in X$ случайными величинами $\mu(k)$.

Проведя необходимые вычисления, приходим к следующим оценкам:

$$\hat{q}_1(i, j) - \hat{q}_0(i, j) \leq \hat{q}(i, j) \leq \hat{q}_1(i, j), \quad (5)$$

$$\hat{q}_0(i, j) = \frac{1}{2} \frac{m^2}{N} \mathbf{E} \mu(i) \mu^{[2]}(j), \quad (6)$$

$$\hat{q}_1(i, j) = m \mathbf{E} \mu(i) \mu(j). \quad (7)$$

При построении оценки $\hat{q}_\Theta(i, j)$ будем пренебрегать зависимостью между случайными величинами $\xi_\Theta(x)$, $x \in X$, равными количествам непосредственных прообразов точек x из множества $X \setminus \{\Theta \cup x\}$ относительно отображения F , и считать, что они независимы в совокупности.

В этом случае распределение случайных величин вида $|\tilde{F}_\Theta^{(k)}(\theta)|$, $\theta \in \Theta$, совпадает с распределением числа $\mu_\Theta(k)$ частиц, существующих в момент времени k , в процессе Гальтона–Ватсона $\mu_\Theta(k)$, $k = 0, 1, \dots$, определяемом соотношениями

$$\mu_\Theta(0) = 1, \quad \mathbf{P}\{\mu_\Theta(1) = j\} = \mathbf{P}\{\xi_\Theta(x) = j\}, \quad j = 0, 1, \dots$$

(распределение в правой части индуцируется F и не зависит от x).

Можно показать, что первый момент случайной величины $\mu_\Theta(1)$ равен $1 - 1/t$, а два ее следующих факториальных момента при $N \rightarrow \infty$ стремятся к 1.

Также заметим, что при сделанном предположении распределение случайных величин вида

$$\left| \bigcup_{k=j}^{t_1} \tilde{F}_{\Theta}^{(k)}(\theta) \right|, \quad \theta \in \Theta, \quad 1 \leq j \leq t_1,$$

совпадает с распределением суммарного числа частиц

$$v_{\Theta}(j) = \sum_{k=j}^{t_1} \mu_{\Theta}(k),$$

существовавших в процессе Гальтона–Ватсона $\mu_{\Theta}(k)$, $k = 0, 1, \dots$, с момента времени $j, \dots, t_1$.

В качестве оценки $\hat{q}_{\Theta}(i, j)$ среднего значения случайной величины $\bar{q}_{\Theta}(i, j)$ рассмотрим среднее значение случайной величины, полученной из формулы (4) посредством замены при любых $\theta \in \Theta$ случайных величин вида $|\tilde{F}_{\Theta}^{(k)}(\theta)|$, $|\bigcup_{k=j}^{t_1} \tilde{F}_{\Theta}^{(k)}(\theta)|$ случайными величинами $\mu_{\Theta}(k)$, $v_{\Theta}(j)$ соответственно.

Проводя необходимые вычисления, получим оценку

$$\hat{q}_{\Theta}(i, j) = \frac{N}{t} \mathbf{E} \mu_{\Theta}(i) \left(1 - \left(1 - \frac{m}{N} \right)^{v_{\Theta}(j)} \right). \quad (8)$$

4. Вычисление предельных значений оценок

Оценки $\hat{q}(i, j)$, $\hat{q}_0(i, j)$, $\hat{q}_1(i, j)$, $\hat{q}_{\Theta}(i, j)$ сложным образом зависят как от параметров m, t, N, t_1 , так и от распределений процессов μ , μ_{Θ} . Тем не менее, как будет показано далее, при определенном асимптотическом изменении параметров величины $\hat{q}(i, j)$, $\hat{q}_{\Theta}(i, j)$ сближаются со значениями некоторых функций, зависящих только от параметров и первых двух моментов процессов μ , μ_{Θ} . Мы будем использовать значения данных функций от параметров в качестве итоговых оценок исследуемых величин и обозначать их символами $q(i, j)$, $q_{\Theta}(i, j)$.

Приведенные далее теоремы 1 и 2 позволяют представить функции $q(i, j)$, $q_{\Theta}(i, j)$ равенствами

$$q(i, j) = \gamma_1(x_0, x_1) \cdot m t, \quad x_0 = \frac{i}{t}, \quad x_1 = \frac{j}{t},$$

$$q_{\Theta}(i, j) = \gamma_2(\alpha, x_0, x_1, x_2) \cdot \frac{N}{t}, \quad \alpha = \frac{1}{2} \cdot \frac{m t^2}{N}, \quad x_2 = \frac{t_1}{t}$$

и получить точный вид функций γ_1, γ_2 .

Далее будем полагать, что для каждого натурального s заданы набор параметров N_s, m_s, i_s, j_s, t_s , процесс Гальтона – Ватсона $\mu_s, \mu_s(0) = 1, \mathbf{E} \mu_s(1) = 1$, и по формулам (5)–(7) определены величины $\widehat{q}_s(i_s, j_s), \widehat{q}_{0,s}(i_s, j_s), \widehat{q}_{1,s}(i_s, j_s)$.

Теорема 1. Пусть при $s \rightarrow \infty$ выполняются асимптотические соотношения

$$\begin{aligned} N_s, m_s, t_s, i_s, j_s &\rightarrow \infty, \\ \frac{m_s t_s^2}{2N_s} &\rightarrow \alpha, \quad \frac{i_s}{t_s} \rightarrow x_0, \quad \frac{j_s}{t_s} \rightarrow x_1, \\ \mathbf{E} \mu_s^{[2]}(1) &\rightarrow 1, \quad \mathbf{E} \mu_s^{[3]}(1) < R < \infty. \end{aligned}$$

Тогда

$$\frac{1}{m_s t_s} \widehat{q}_s(i_s, j_s) \rightarrow \gamma_1(x_0, x_1) \quad \text{при } s \rightarrow \infty,$$

где $\gamma_1(x_0, x_1) = x_0 \wedge x_1$ (минимум величин x_0, x_1).

Доказательство. Справедливо представление

$$\frac{1}{m_s t_s} \widehat{q}_{1,s}(i_s, j_s) = \frac{1}{t_s} \mathbf{E} \mu_s(i_s) \mu_s(j_s).$$

В [9, теорема 1, п. 2] утверждается, что в условиях теоремы существует предел

$$\frac{1}{t_s} \mathbf{E} \mu_s(i_s) \mu_s(j_s) \rightarrow x_0 \wedge x_1, \quad s \rightarrow \infty.$$

Следовательно, с учетом оценки (5), для доказательства теоремы достаточно показать, что последовательность

$$\frac{1}{m_s t_s} \widehat{q}_{0,s}(i_s, j_s) = \frac{1}{2} \frac{m_s}{t_s N_s} \mathbf{E} \mu_s(i_s) \mu_s^{[2]}(j_s)$$

при $s \rightarrow \infty$ сходится к нулю.

Получим оценку сверху для математического ожидания $\mathbf{E} \mu(i) \mu^{[2]}(j)$ критического процесса Гальтона – Ватсона $\mu(k), k = 1, 2, \dots$:

$$\begin{aligned} \mathbf{E} \mu(i) \mu^{[2]}(j) &\leq \mathbf{E} \mu(i) \mu^2(j) \leq \\ &\leq \mathbf{E} \left(\frac{1}{3} \mu(i) + \frac{2}{3} \mu(j) \right)^3 \leq \frac{1}{3} \mathbf{E} \mu^3(i) + \frac{2}{3} \mathbf{E} \mu^3(j) = \\ &= \mathbf{E} \left(\frac{1}{3} \mu^{[3]}(i) + \mu^{[2]}(i) + \frac{1}{3} \mu(i) \right) + 2 \mathbf{E} \left(\frac{1}{3} \mu^{[3]}(j) + \mu^{[2]}(j) + \frac{1}{3} \mu(j) \right). \end{aligned}$$

Обозначим $\mathbf{E} \mu^{[2]}(1) = B$, $\mathbf{E} \mu^{[3]}(1) = C$. Хорошо известны [10] равенства

$$\mathbf{E} \mu(k) = 1, \quad \mathbf{E} \mu^{[2]}(k) = Bk, \quad \mathbf{E} \mu^{[3]}(k) = \frac{3}{2} B^2 k^{[2]} + Ck.$$

С их помощью получаем оценки

$$\mathbf{E} \left(\frac{1}{3} \mu^{[3]}(k) + \mu^{[2]}(k) + \frac{1}{3} \mu(k) \right) \leq \frac{1}{2} (B^2 k^{[2]} + (C+B)k + 1),$$

$$\mathbf{E} \mu(i) \mu^{[2]}(j) \leq B^2 (i^2 + j^2) + (C+B)(i+j) + 2.$$

Применяя их, находим:

$$\frac{1}{m_s t_s} \widehat{q}_{0,s}(i_s, j_s) \leq \frac{t_s m_s}{N_s} \left(S_{1,s} + S_{2,s} + \frac{1}{t_s^2} \right),$$

$$S_{1,s} = (\mathbf{E} \mu_s^{[2]}(1))^2 \left(\left(\frac{i_s}{t_s} \right)^2 + \left(\frac{j_s}{t_s} \right)^2 \right),$$

$$S_{2,s} = \frac{\mathbf{E} \mu_s^{[3]}(1) + \mathbf{E} \mu_s^{[2]}(1)}{t_s} \left(\frac{i_s}{t_s} + \frac{j_s}{t_s} \right).$$

В условиях теоремы

$$\frac{t_s m_s}{N_s} \rightarrow 0, \quad S_{1,s} \rightarrow x_0^2 + x_1^2, \quad S_{2,s} \rightarrow 0 \quad \text{при} \quad s \rightarrow \infty.$$

Следовательно,

$$\frac{1}{m_s t_s} \widehat{q}_{0,s}(i_s, j_s) \rightarrow 0, \quad s \rightarrow \infty.$$

Теорема доказана. □

Для формулировки теоремы 2 введем следующие функции:

$$f_0(y, z) = \frac{y + \sqrt{z} \operatorname{th} \sqrt{z}}{1 + y \frac{\operatorname{th} \sqrt{z}}{\sqrt{z}}} \quad \text{при} \quad z > 0, \quad f_0(y, 0) = \frac{y}{1+y},$$

$$f_1(x, y, z) = \frac{1}{x} f_0(yx, zx^2) \quad \text{при} \quad x > 0, \quad f_1(0, y, z) = y,$$

$$f_{A,B}(x, y, z) = \frac{2}{B} f_1\left(x, y \frac{B}{2} + \frac{A}{2}, z \frac{B}{2} + \left(\frac{A}{2}\right)^2\right) - \frac{A}{B},$$

$$\widetilde{f}_{A,B}(x, y, z) = \frac{\partial f_{A,B}(x, y, z)}{\partial y}.$$

Далее будем полагать, что для каждого натурального s заданы параметры $N_s, m_s, i_s, j_s, t_s, t_{1,s}$, процесс Гальтона–Ватсона $\mu_{\Theta,s}$, $\mu_{\Theta,s}(0) = 1$, $\mathbf{E} \mu_{\Theta,s}(1) = 1 - 1/t_s$, и формулой (8) определены величины $\widehat{q}_{\Theta,s}(i_s, j_s)$.

Теорема 2. Пусть при $s \rightarrow \infty$ выполняются соотношения

$$N_s, m_s, t_s, i_s, j_s, t_{1,s} \rightarrow \infty,$$

$$\frac{m_s t_s^2}{2N_s} \rightarrow \alpha, \quad \frac{i_s}{t_s} \rightarrow x_0, \quad \frac{j_s}{t_s} \rightarrow x_1, \quad \frac{t_{1,s}}{t_s} \rightarrow x_2, \quad x_1 < x_2,$$

$$\mathbf{E} \mu_{\Theta,s}^{[2]}(1) \rightarrow 1, \quad \mathbf{E} \mu_{\Theta,s}^{[3]}(1) < R < \infty.$$

Тогда

$$t_s \frac{\widehat{q}_{\Theta,s}(i_s, j_s)}{N_s} \rightarrow \gamma_2(\alpha, x_0, x_1, x_2) \quad \text{при } s \rightarrow \infty,$$

где

$$\begin{aligned} \gamma_2(\alpha, x_0, x_1, x_2) = & e^{-x_0} - I\{x_0 < x_1\} \gamma_{2,1}(\alpha, x_0, x_1, x_2) - \\ & - I\{x_1 < x_0 \leq x_2\} \gamma_{2,2}(\alpha, x_0, x_1, x_2) - \\ & - I\{x_2 < x_0\} \gamma_{2,3}(\alpha, x_0, x_1, x_2), \end{aligned}$$

$$\gamma_{2,1}(\alpha, x_0, x_1, x_2) = \widetilde{f}_{1,1}(x_0, f_{1,1}(x_1 - x_0, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0), 0),$$

$$\begin{aligned} \gamma_{2,2}(\alpha, x_0, x_1, x_2) = & \widetilde{f}_{1,1}(x_0 - x_1, f_{1,1}(x_2 - x_0, 0, 2\alpha), 2\alpha) \times \\ & \times \widetilde{f}_{1,1}(x_1, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0), \end{aligned}$$

$$\begin{aligned} \gamma_{2,3}(\alpha, x_0, x_1, x_2) = & \widetilde{f}_{1,1}(x_0 - x_2, 0, 0) \cdot \widetilde{f}_{1,1}(x_2 - x_1, 0, 2\alpha) \times \\ & \times \widetilde{f}_{1,1}(x_1, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0). \end{aligned}$$

Доказательство. Справедливо представление

$$\begin{aligned} \widehat{q}_{\Theta,s}(i_s, j_s) \frac{t_s}{N_s} &= \mathbf{E} \mu_{\Theta,s}(i_s) \left(1 - \left(1 - \frac{m_s}{N_s} \right)^{v_{\Theta,s}(j_s)} \right) = \\ &= \left(1 - \frac{1}{t_s} \right)^{t_s \frac{i_s}{t_s}} - \mathbf{E} \mu_{\Theta,s}(i_s) \left(1 - \frac{m_s t_s^2}{N_s} \frac{1}{t_s^2} \right)^{v_{\Theta,s}(j_s)}. \end{aligned}$$

Для доказательства теоремы достаточно заметить, что существуют пределы уменьшаемого и вычитаемого. В самом деле,

$$\left(1 - \frac{1}{t_s} \right)^{t_s \frac{i_s}{t_s}} \rightarrow e^{-x_0}, \quad s \rightarrow \infty.$$

Из [9, теорема 2, пп. 1–3] следует, что если выполнены условия теоремы и $s \rightarrow \infty$, то:

1) при $x_0 < x_1$

$$\mathbf{E} \mu_{\Theta,s}(i_s) \left(1 - \frac{m_s t_s^2}{N_s} \frac{1}{t_s^2}\right)^{v_{\Theta,s}(j_s)} \rightarrow \tilde{f}_{1,1}(x_0, f_{1,1}(x_1 - x_0, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0), 0),$$

2) при $x_1 < x_0 < x_2$

$$\mathbf{E} \mu_{\Theta,s}(i_s) \left(1 - \frac{m_s t_s^2}{N_s} \frac{1}{t_s^2}\right)^{v_{\Theta,s}(j_s)} \rightarrow \tilde{f}_{1,1}(x_0 - x_1, f_{1,1}(x_2 - x_0, 0, 2\alpha), 2\alpha) \cdot \tilde{f}_{1,1}(x_1, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0),$$

3) при $x_2 < x_0$

$$\mathbf{E} \mu_{\Theta,s}(i_s) \left(1 - \frac{m_s t_s^2}{N_s} \frac{1}{t_s^2}\right)^{v_{\Theta,s}(j_s)} \rightarrow \tilde{f}_{1,1}(x_0 - x_2, 0, 0) \cdot \tilde{f}_{1,1}(x_2 - x_1, 0, 2\alpha) \cdot \tilde{f}_{1,1}(x_1, f_{1,1}(x_2 - x_1, 0, 2\alpha), 0).$$

Теорема доказана. $\square$

Полученные результаты при достаточно больших значениях параметров хорошо соответствуют экспериментальным данным, что говорит об адекватности использованных в работе вероятностных предположений.

Список литературы

- [1] Avoine G., Junod P., Oechslin P., “Characterization and improvement of time-memory trade-off based on perfect tables”, *Trans. Inf. Syst. Secur.*, **11**:17 (July 2008), 1–17.
- [2] Borst J., Preneel B., Vandewalle J., “On the time-memory tradeoff between exhaustive key search and table precomputation”, *Symp. Inf. Theory in the Benelux* (1998), 111–118.
- [3] Hellman M. E., “A cryptanalytic time-memory trade off”, *IEEE Trans. Inf. Theory*, **IT-26** (1980), 401–406.
- [4] Hong J., “The cost of false alarms in Hellman and rainbow tradeoffs”, *Des., Codes and Cryptogr.*, **57**:3 (2010), 293–327.
- [5] Oechslin P., “Making a faster cryptanalytic time-memory trade-off”, *CRYPTO’03, Lect. Notes Comput. Sci.*, **2729**, 2003, 617–630.
- [6] Standaert F.X., Rouvroy G., Quisquater J.J., Legat J.D., “A time-memory tradeoff using distinguished points: New analysis & FPGA results”, *CHES 2002, Lect. Notes Comput. Sci.*, **2523**, 2002, 593–609.
- [7] Hoch Y. Z., *Security analysis of generic iterated hash functions*, Ph.D. Thesis, Weizmann Inst. of Sci., 2009.
- [8] Hong J., Moon S., “A comparison of cryptanalytic tradeoff algorithms”, *J. Cryptology*, **26** (2013), 559–637.
- [9] Pilshchikov D. V., “On the limiting mean values in probabilistic models of time-memory-data tradeoff methods”, *Mathematical Aspects of Cryptography*, **6**:2 (2015), 59–65.
- [10] Севастьянов Б. А., *Ветвящиеся процессы*, М.: Наука, 1971.