

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

На правах рукописи

Миронкин Владимир Олегович

Явные формулы для
распределений характеристик
итераций случайных
отображений

Специальность 05.13.19 — «Методы и системы защиты информации,
информационная безопасность»

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук
Зубков Андрей Михайлович

Москва — 2021

Оглавление

Введение	4
1 Итерации равновероятного случайного отображения	27
1.1 Теоретико-вероятностная модель	27
1.2 Отрезок аperiodичности вершины в графе отображения f^k . . .	33
1.3 Множество образов при отображении f^k	45
1.4 Слои и циклические вершины в графе отображения f^k	53
1.5 Инцидентность вершин одной компоненте связности в графе отображения f^k	62
1.6 Прообразы вершин и коллизии в графе отображения f^k	73
1.7 Выводы	78
2 Композиция независимых равновероятных случайных отображений	80
2.1 Теоретико-вероятностная модель	80
2.2 Отрезок аperiodичности вершины в графе отображения $f_{[k]}$. . .	81
2.3 Слои и циклические вершины в графе отображения $f_{[k]}$	92
2.4 Множество образов и коллизии в графе отображения $f_{[k]}$	105
2.5 Инцидентность вершин одной компоненте связности в графе отображения $f_{[k]}$	110

2.6	Прообразы вершин в графе отображения $f_{[k]}$	118
2.7	Выводы	120
Заключение		122
Список сокращений и условных обозначений		124
Список литературы		125

Введение

Актуальность темы исследования. Развитие раздела теории вероятностей, связанного с исследованием случайных отображений и их модификаций, обусловлено активным применением алгоритмических методов защиты информации (например, конечных автоматов [31, 32], алгоритмов преобразования данных [79], алгоритмов хеширования и генерации псевдослучайных последовательностей [3, 30]) (далее — АМЗИ) при решении широкого спектра задач информационной безопасности, а также необходимостью стандартизации отечественных разработок в части, связанной с генерацией производных ключей и псевдослучайных последовательностей. Согласно пп. 17, 18 Доктрины информационной безопасности Российской Федерации [5], утвержденной Указом президента Российской Федерации № 646 от 5 декабря 2016 года, указанные направления исследований приобретают особую значимость и актуальность.

На сегодняшний день наиболее изученными математическими объектами, используемыми при моделировании АМЗИ и описании режимов их функционирования, являются равновероятные случайные отображения [12–14, 41, 43, 72]. В тоже время интенсивное развитие методов синтеза АМЗИ привело к тому, что равновероятные случайные отображения стало невозможно рассматривать как адекватные модели ряда современных АМЗИ, имеющих итерационную структуру. В связи с этим возникла естественная потребность в разра-

ботке и обосновании новых теоретико-вероятностных моделей, построенных как на равновероятных, так и на неравновероятных случайных отображениях, с перспективой их дальнейшего использования при создании и исследовании АМЗИ. Примерами подобных неравновероятных отображений, рассматриваемых в качестве моделей современных АМЗИ, являются итерации одного равновероятного случайного отображения [7, 17–24, 26, 29] и композиции нескольких независимых равновероятных случайных отображений [9, 10, 25].

Наряду с моделированием процесса работы итерационных АМЗИ, указанные классы отображений могут быть использованы при решении уравнений с однонаправленными функциями [8, 73, 75, 81–83], а также при решении целого ряда задач, возникающих в рамках анализа методов балансировки времени-памяти-данных, применяемых для обращения однонаправленных функций и построения радужных таблиц [35].

Степень разработанности темы исследования. Итерации одного и композиция нескольких случайных отображений представляют собой обобщение случайных отображений — математических объектов, широко используемых при решении задач информационной безопасности, и подробно изученных видными российскими и зарубежными учеными, в частности, В. Н. Сачковым [40–43], Б. А. Севастьяновым [44, 45], В. Е. Степановым [48–50], А. М. Зубковым [6], В. Ф. Колчиным [12–14], В. Г. Михайловым [30–32], В. Г. Проскуриным [38, 39], А. Л. Якимивым [56, 57], А. Одлыжко (A. Odlyzko), Ф. Флажолле (P. Flajolet) [71], Д. Олдосом (D. Aldous), Д. Питманом (J. Pitman) [59–63], Х. Рубином (H. Rubin), Б. Харрисом (B. Harris) [72], Р. Ситгрейвесом (R. Sitgreaves) [84] и др.

В работах указанных специалистов получен целый спектр результатов, описывающих особенности строения графа случайного отображения, выписаны асимптотические и точные выражения для его характеристик, в том

числе подробно изучена цикловая структура как самого отображения, так и ряда производных конструкций, построенных на его основе (автоматные отображения, регистры сдвига и т.д.).

В частности, в работе Х. Рубина и Р. Ситгрейвеса [84], опубликованной в 1954 году, для множества всех n^n отображений $\Omega = \{f: S \rightarrow S\}$ с заданным на нем равновероятным распределением, где S — произвольное конечное множество, $|S| = n$, $n \in \mathbb{N}$, получены точные выражения для локальных вероятностей общего числа N_f циклических вершин, размера C_f случайной компоненты связности и общего числа M_f компонент связности в графе G_f равновероятного случайного отображения f (см. определения в § 1.1):

$$\begin{aligned}\mathbf{P}\{N_f = j\} &= \frac{(n-1)!j}{(n-j)!n^j}, \\ \mathbf{P}\{C_f = j\} &= \frac{(n-1)!}{(n-j)!(j-1)!} \frac{j^j (n-j)^{n-j}}{n^n} \sum_{i=1}^j \frac{(j-1)!}{(j-i)!j^i}, \\ \mathbf{P}\{M_f = j\} &= \sum_{i=1}^n \frac{(n-1)!j}{(n-j)!n^j} \alpha\{i, j\},\end{aligned}$$

где $j \in \{1, \dots, n\}$, а $\alpha\{i, j\}$ — коэффициент при z^i в разложении $\frac{\Gamma(z+j)}{\Gamma(z)j!}$ в степенной ряд. В свою очередь, В. Ф. Колчиным в [12] выписаны и асимптотические формулы для указанных распределений.

В тех же условиях в [64, 72, 84] для длины $\tau_f(x)$ отрезка апериодичности произвольной фиксированной вершины $x \in S$ и длины $\beta_f(x)$ цикла компоненты связности графа G_f , содержащей вершину $x \in S$ (см. определения в § 1.1), получены совместные и маргинальные распределения

$$\begin{aligned}\mathbf{P}\{\tau_f(x) = k, \beta_f(x) = j\} &= \frac{(n-1)!}{(n-k)!n^k}, \quad 1 \leq j \leq k \leq n, \\ \mathbf{P}\{\beta_f(x) = j\} &= \sum_{k=j}^n \frac{(n-1)!}{(n-k)!n^k}, \quad j \in \{1, 2, \dots, n\},\end{aligned}$$

$$\mathbf{P}\{\tau_f(x) = k\} = \frac{(n-1)!k}{(n-k)!n^k}, \quad k \in \{1, 2, \dots, n\}.$$

Позднее в представленной на международной конференции «Workshop on the Theory and Application of Cryptographic Techniques» (Бельгия, апрель 1989 г.) работе [71] была выписана асимптотика при $n \rightarrow \infty$ для средних значений случайных величин N_f , M_f , $|T_f|$ и $|f(S)|$, где T_f — множество вершин в графе G_f , не имеющих прообразов, а $f(S)$ — образ множества S при действии случайного отображения f :

$$\begin{aligned} \mathbf{E}N_f &\sim \sqrt{\frac{\pi n}{2}}, & \mathbf{E}M_f &\sim \frac{\ln n}{2}, \\ \mathbf{E}|T_f| &\sim e^{-1}n, & \mathbf{E}|f(S)| &\sim (1 - e^{-1})n. \end{aligned}$$

В том числе для композиции независимых равновероятных случайных отображений $f_1, \dots, f_k$ множества S в себя, где $k \in \mathbb{N}$ — произвольное, авторами было получено асимптотическое равенство при $n \rightarrow \infty$, $k = \text{const} > 0$ для среднего значения случайной величины $|f_k(\dots(f_1(x))\dots)(S)|$:

$$\mathbf{E}|f_k(\dots(f_1(x))\dots)(S)| \sim (1 - \tau_k)n,$$

где $\tau_0 = 0$, $\tau_{k+1} = e^{-1+\tau_k}$.

Для распределения случайной величины, равной мощности t -го слоя $H_f^{(t)} = \{x \in S: \alpha_f(x) = t\}$ в графе G_f , для произвольного $t > 0$ [69] и $t = o(\sqrt{n})$ при $n \rightarrow \infty$ [80] доказана сходимость при $n \rightarrow \infty$ к распределению Рэлея [4] с модой 1:

$$\mathbf{P}\left\{\frac{|H_f^{(t)}|}{\sqrt{n}} \leq z\right\} \rightarrow 1 - e^{-\frac{z^2}{2}}, \quad z \geq 0,$$

позволившая получить асимптотики для численных характеристик случайной величины $|H_f^{(t)}|$ в области типичных значений при $n \rightarrow \infty$:

$$\mathbf{E}|H_f^{(t)}| \sim \sqrt{\frac{\pi n}{2}} \quad \text{и} \quad \mathbf{D}|H_f^{(t)}| \sim \left(2 - \frac{\pi}{2}\right)n.$$

Кроме того, в [69] для числа $\nu_f(r)$ вершин кратности r (т.е. вершин в графе G_f , имеющих в точности r прообразов) доказана локальная сходимость при $n \rightarrow \infty$ к стандартному нормальному закону для произвольного фиксированного $r \geq 0$:

$$\mathbf{P} \left\{ \frac{\nu_f(r) - n\mu_r}{\sigma_r \sqrt{n}} \leq x \right\} \rightarrow \Phi(x),$$

где $\mu_r = \frac{1}{er!}$, $\sigma_r^2 = \mu_r + \left(1 + (r-1)^2\right) \mu_r^2$, а в [66] указанный результат обобщен на случай отличного от константы функционала $r = r(n)$. Так, в частности, в случае $r(n) \sim \lambda n^{\frac{2}{3}}$, где $\lambda > 0$, при $n \rightarrow \infty$ распределение случайной величины $\nu_f(r)$ сходится к пуассоновскому распределению $\Pi(\lambda)$, а в случае $r(n) = o(n)$ при $n \rightarrow \infty$ — к стандартному нормальному распределению $\mathcal{N}(0, 1)$.

На X Всероссийском симпозиуме по прикладной и промышленной математике (Санкт-Петербург, май 2009 г.) в рамках доклада А. М. Зубкова и П. В. Халипова «Вероятность попадания нескольких точек в одну компоненту связности случайного отображения», посвященного исследованию строения компонент связности графа G_f , для произвольных вершин $x_1, \dots, x_k \in S$, где $k \geq 2$, сформулирован следующий результат:

$$\lim_{n \rightarrow \infty} \mathbf{P}\{x_1, \dots, x_k \in \mathcal{K}_f(x_1)\} = \frac{(2k-2)!!}{(2k-1)!!},$$

где $\mathcal{K}_f(x_1)$ — компонента связности графа G_f , содержащая вершину x_1 .

В [68] выписано приближение среднего числа компонент связности графа G_f , включающих по крайней мере s -ю часть от общего числа вершин и имеющих циклы длины, не превосходящей $tn^{\frac{1}{2}}$, где $0 \leq s, t \leq 1$:

$$\mathbf{E}X_n(s, t) \approx \frac{1}{\sqrt{2\pi}} \int_t^1 \int_0^s \frac{e^{-\frac{y^2}{2x}}}{\sqrt{x^3(1-x)}} dy dx.$$

Отдельную группу формируют результаты исследований различного рода модификаций равновероятных случайных отображений. Так, использование кратных итераций равновероятного случайного отображения позволило

оптимизировать двухэтапный метод М. Хеллмана [73] решения уравнений вида $g(x) = a$, где $g: S \rightarrow S$ — произвольная однонаправленная функция [36], а $|S| = n$. В частности, в [35] получены оценки временной сложности оперативного этапа метода Хеллмана с использованием радужных таблиц (RM-метод) и маркеров цепочек (RMM-метод), а также рассчитана средняя временная сложность полной обработки одной такой таблицы.

В свою очередь, в [8] изучалась модель построения радужной таблицы на основе композиции независимых равновероятных случайных отображений $f_1, \dots, f_k$ множества S в себя, где $k \in \mathbb{N}$. Для произвольного $S_0 \subseteq S$, $|S_0| = m \leq n$ и соответствующих последовательностей множеств

$$S_k = f_k(f_{k-1}(\dots(f_1(S_0))\dots)), \quad \Psi_k = S_1 \cup \dots \cup S_k, \quad k = 1, 2, \dots,$$

описан способ точного вычисления распределений случайных величин $\varphi_k = |S_k|$ и $\zeta_k = |\Psi_k|$ с использованием аппарата цепей Маркова. В том числе получены верхние и нижние оценки для некоторых условных характеристик:

$$\begin{aligned} \frac{m}{n} - C_m^2 \frac{k}{n^2} &\leq \mathbf{P}\{x \in S_k \mid \varphi_0 = m\} < \frac{m}{n} - C_m^2 \frac{k}{n^2} + \frac{m^3 k^2}{4n^3}, \\ \frac{mk}{n} - C_{k+1}^2 \frac{3m^2}{2n^2} &< \mathbf{P}\{x \in \Psi_k \mid \varphi_0 = m\} < \frac{mk}{n} - C_m^2 C_{k+1}^2 \frac{1}{n^2} + \frac{m^3 (k+1)^3}{12n^3}, \\ m - C_m^2 \frac{k}{n} &\leq \mathbf{E}\{\varphi_k \mid \varphi_0 = m\} < n - C_m^2 \frac{k}{n} + \frac{m^3 k^2}{4n^2}, \\ mk - C_{k+1}^2 \frac{3m^2}{2n} &< \mathbf{E}\{\zeta_k \mid \varphi_0 = m\} < mk - C_m^2 C_{k+1}^2 \frac{1}{n} + \frac{m^3 (k+1)^3}{12n^2}, \\ \mathbf{D}\{\varphi_k \mid \varphi_0 = m\} &< \frac{km^3}{n} \left(1 + \frac{(m+2)k}{4mn}\right). \end{aligned}$$

А. М. Зубковым и А. А. Серовым в [9] доказана асимптотическая нормальность случайной величины φ_k при $l, m, k, n \rightarrow \infty : l = O(n^{\frac{1}{4}})$, $m = o(l)$, $k = 2n \left(\frac{1}{m} - \frac{1}{l}\right) + (1 + o(1)) x \frac{2n}{\sqrt{3}} \sqrt{\frac{1}{m^3} - \frac{1}{l^3}}$, где $x \in \mathbb{R}$:

$$\mathbf{P} \left\{ \varphi_k \leq \frac{n}{n/l + k/2} \right\} \rightarrow \Phi(x),$$

что соответствует полученному с использованием эвристических рассуждений приближению [74]:

$$\frac{\varphi_k}{n} \approx \frac{1}{n/\varphi_0 + k/2},$$

а также выписаны точные формулы для следующих условных распределений:

$$\mathbf{P}\{\varphi_k = m \mid \varphi_0 = m\} = \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right)^k,$$

$$\mathbf{P}\{\varphi_k = m - 1 \mid \varphi_0 = m\} = \frac{m}{2} \left(1 - \left(1 - \frac{m-1}{n}\right)^k\right) \prod_{i=1}^{m-2} \left(1 - \frac{i}{n}\right)^k,$$

$$\mathbf{P}\{\varphi_k = m - a \mid \varphi_{k-1} = m\} = \sum_{2 \leq j_1 < j_2 < \dots < j_a \leq m} \prod_{i=1}^{m-a-1} \left(1 - \frac{i}{n}\right)^a \prod_{v=1}^a \frac{j_v - v}{n}.$$

Позднее в [10] ими же получены двусторонние неравенства для $\mathbf{E}\{\varphi_k \mid \varphi_0 = m\}$, в которых разность между верхней и нижней оценками имеет порядок $o(m)$ при $m, k, n \rightarrow \infty$: $mk = o(n)$.

Задачи, связанные с оценкой скорости сжатия исходного множества S при действии композиции отображений и имеющие особое практическое значение при моделировании алгоритмов выработки производных ключей, решались в [11, 70]. Так, в частности, для

$$\tau_n = \min\{t \in \mathbb{N} : |f_t(\dots(f_1(S))\dots)| = 1\},$$

где $f_1, \dots, f_k$ — независимые равновероятные случайные отображения множества S в себя, доказана сходимость распределения случайной величины $\zeta = \frac{1}{n}\tau_n$ при $n \rightarrow \infty$ к распределению суммы $\xi = \sum_{j=1}^{\infty} \xi_j$, где случайные величины $\xi_1, \xi_2, \dots$ независимы и

$$\mathbf{P}\{\xi_j \leq x\} = 1 - e^{-xC_{j+1}^2}, \quad x \geq 0, \quad j = 1, 2, \dots,$$

а для случайной величины ξ выполняется равенство (см. [65, 67, 76]):

$$\mathbf{E}\xi = \sum_{j=1}^{\infty} \frac{2}{j(j+1)} = 2.$$

Другая модификация итераций отображений, построенная на основе одного равновероятного случайного отображения $f: S \rightarrow S$ и последовательности $R_1, R_2, \dots$ случайных независимых биективных отображений множества S в себя, рассматривалась в [81]. Для подмножества $S_0 \subset S$, $|S_0| = m$, и последовательности его образов

$$S_k = R_k(f(\dots(R_1(f(S_0)))\dots)), \quad k = 1, 2, \dots,$$

и случайного множества

$$\tilde{\Psi}_k = S_1 \cup \dots \cup S_k, \quad k = 1, 2, \dots,$$

с использованием эвристических рассуждений получена приближенная формула

$$\mathbf{P}\{x \in S_0 \cup \tilde{\Psi}_k\} \approx 1 - \prod_{i=1}^k \left(1 - \frac{n_i}{n}\right),$$

где $n_1 = m$, $n_{i+1} = n \left(1 - e^{-\frac{n_i}{n}}\right)$ при $i \geq 1$.

В [73] М. Хеллманом для равновероятного случайного отображения $f: S \rightarrow S$, множества $S_0 \subset S$, $|S_0| = m$, и случайного множества

$$\Phi_k = f(S_0) \cup f^2(S_0) \cup \dots \cup f^k(S_0)$$

получена двусторонняя оценка

$$\frac{1}{n} \sum_{i=1}^m \sum_{j=1}^k \left(1 - \frac{ik}{n}\right)^j \leq \mathbf{P}\{x \in \Phi_k\} \leq \frac{mk}{n},$$

справедливая для произвольного $x \in S$. В частности, автор показал, что при $mk^2 \approx n$ и $m, k \geq 1$ левая часть этого неравенства близка к $0,80 \frac{mk}{n}$. Позднее в [77] была найдена более точная нижняя оценка

$$\frac{1}{n} \sum_{i=1}^m \sum_{j=1}^k \left(1 - \frac{ik}{n}\right)^j \geq \frac{mk}{n} \int_0^1 \frac{1 - e^{-x}}{x} kx \approx 0,796599 \frac{mk}{n},$$

а в [75] с помощью перехода к аппроксимирующим дифференциальным уравнениям — приближенная формула

$$\mathbf{P}\{x \in \Phi_k\} \approx 2 \left(1 - \frac{1}{\tau^2}\right) \frac{e^{\frac{k}{\tau}} - e^{-\frac{k}{\tau}}}{(\tau + 1) e^{\frac{k}{\tau}} + (\tau - 1) e^{-\frac{k}{\tau}}},$$

где $\tau = \sqrt{\frac{2n}{m}}$.

Наконец, в [46] изучались последовательности независимых пар зависимых равновероятных случайных отображений $(f_1, g_1), (f_2, g_2), \dots$ множества S в себя, удовлетворяющих условиям

$$\mathbf{P}\{f_k(x) = g_k(x) = y\} = \frac{\alpha}{n},$$

$$\mathbf{P}\{f_k(x) = y, g_k(x) = z\} = \frac{1 - \alpha}{n(n - 1)}$$

для любых $y, z \in S$, $y \neq z$, где $\frac{1}{n} \leq \alpha < 1$.

Так, для множеств

$$S_k = f_k(\dots(f_1(S_0))\dots), \quad T_k = g_k(\dots(g_1(S_0))\dots)$$

при любых $1 \leq k, m \leq n$ выписаны двусторонние оценки

$$L(k, n) \leq \mathbf{P}\{x \in S_k \cap T_k \mid |S_0| = m\} < L(k, n) + U(k, n),$$

где при $\lambda_1 = 1 - \frac{1}{n}$, $\lambda_2 = \alpha - \frac{1}{n}$, $\lambda_3 = (1 - \frac{2}{n})(\alpha - \frac{1}{n})$

$$L(k, n) = \frac{m}{n} \frac{1 + n(1 - \alpha)(2 - \lambda_2^t)}{n(1 - \lambda_2)} - \frac{m(m - 1)}{n} \left(1 - \lambda_1^t + \frac{1 - \lambda_2^t}{n(1 - \lambda_2)}\right),$$

$$\begin{aligned} U(k, n) = & \frac{m(m - 1)}{n^2} \left(\frac{(m - 2)k^2}{2n} + \frac{m(1 - \lambda_1^k)}{1 - \lambda_2} \right) + \\ & + \frac{m(m - 1)}{n^2} \left(\frac{\lambda_2(\lambda_1^k m - \lambda_3^k(m - 2))}{(n(1 - \alpha) + 2\lambda_2)(1 - \lambda_2)} + \frac{n(\lambda_2^k - \lambda_3^k)(1 - \alpha)}{1 - \lambda_2} \right). \end{aligned}$$

Цель исследования. Построение и исследование адекватных математических моделей современных итерационных АМЗИ, основанных на итерациях одного или нескольких независимых равновероятных случайных отображений конечного множества в себя, с перспективой их дальнейшего использования при создании новых и совершенствовании действующих АМЗИ.

Задачи исследования.

- Исследование структуры графа G_{f^k} , где f^k — k -кратная итерация равновероятного случайного отображения $f: S \rightarrow S$, в том числе множеств циклических, висячих вершин, прообразов произвольных вершин, слоев и образа $f^k(S)$, $k \in \mathbb{N}$.

Вывод точных выражений и неравенств для вероятностей инцидентности вершин перечисленным выше множествам, вероятностей коллизий, а также для распределений основных характеристик графа G_{f^k} : длин отрезков аперiodичности, подходов, циклов и т. д.

- Исследование структуры графа $G_{f_{[k]}}$, где $f_{[k]}$ — композиция k независимых равновероятных случайных отображений $f_i: S \rightarrow S$, $i = 1, \dots, k$, в том числе множеств циклических, висячих вершин, прообразов произвольных вершин, слоев и образа $f_{[k]}(S)$, $k \in \mathbb{N}$.

Вывод точных выражений и неравенств для вероятностей инцидентности вершин перечисленным выше множествам, вероятностей коллизий, а также для распределений основных характеристик графа $G_{f_{[k]}}$: длин отрезков аперiodичности, подходов, циклов и т. д.

Область исследования. Содержание диссертации соответствует паспорту специальности 05.13.19 («Методы и системы защиты информации, информационная безопасность») в части п. 1 «Теория и методология обеспечения информационной безопасности и защиты информации», п. 9 «Модели и

методы оценки защищенности информации и информационной безопасности объекта» и п. 13 «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

Научная новизна. Построены новые математические модели, основанные на неравновероятных случайных отображениях: кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, позволяющие адекватно описывать современные итерационные АМЗИ. Получены явные формулы для распределений вероятностных характеристик указанных моделей.

Теоретическая значимость. Полученные в диссертации явные формулы для распределений вероятностных характеристик моделей, основанных на кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, могут быть использованы при синтезе и анализе современных итерационных АМЗИ, предназначенных для преобразования и хеширования данных, выработки производных ключей и генерации псевдослучайных последовательностей, а также при обосновании их теоретической стойкости.

Практическая значимость. Полученные в диссертации явные формулы для распределений вероятностных характеристик моделей, основанных на кратной итерации равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых случайных отображений конечного множества в себя, находят свое применение при обосновании выбора параметров итерационных АМЗИ, используемых при выработке производных ключей, существенно влияющих на безопасность обрабатываемой

с их использованием информации.

Практическая значимость диссертации подтверждена двумя актами о внедрении. Результаты диссертации использованы в деятельности ПФ ФГУП «НТЦ «Атлас» в рамках сертификационных исследований создаваемых средств защиты информации, а также в деятельности ООО «КРИПТО-ПРО» при выборе параметров, ограничивающих количество преобразований одного ключа с использованием механизма «CryptoPro Key Meshing».

Результаты первой главы учтены при синтезе и анализе усовершенствованного механизма периодической смены ключа АСРКМ, вошедшего в документ Росстандарта Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» и используемого в настоящее время в продуктах компаний-разработчиков средств защиты информации в качестве одного из основных методов защиты информации в части преобразования ключей.

Методология и методы исследования. Настоящие исследования базируются на известных теоретических положениях дискретной математики, теории вероятностей, теории графов, математического и комбинаторного анализа. В качестве методологической базы использовались источники [6, 12–14, 30, 38–43, 48–52, 71, 72, 84].

Положения, выносимые на защиту. На защиту выносятся: обоснование актуальности, научная новизна, теоретическая и практическая значимость работы, а также следующие положения, которые подтверждаются результатами исследования, представленными в Заключение диссертации.

1. Для графа k -кратной итерации равновероятного случайного отображения конечного множества S в себя, $k \in \mathbb{N}$:

- а) формулы и неравенства для распределений длины отрезка апериодичности и высоты произвольной фиксированной вершины (§ 1.2, § 1.4);
 - б) формулы и неравенства для вероятностей инцидентности вершин множеству циклических вершин и одной компоненте связности (§ 1.4, § 1.5);
 - в) формулы для вероятностей инцидентности вершин слоям и множеству прообразов произвольной фиксированной вершины (§ 1.4, § 1.6);
 - г) формула для вероятности появления коллизии (§ 1.6).
2. Для графа композиции k независимых равновероятных случайных отображений конечного множества S в себя, $k \in \mathbb{N}$:
- а) точные, предельные формулы, а также неравенства для распределений длины отрезка апериодичности и высоты произвольной фиксированной вершины (§ 2.2);
 - б) формулы и неравенства для вероятностей инцидентности вершин слоям и множеству циклических вершин (§ 2.3);
 - в) формулы для вероятностей появления коллизии и инцидентности вершин образу исходного множества вершин (§ 2.4);
 - г) формулы для вероятностей инцидентности вершин одной компоненте связности и множеству прообразов произвольной фиксированной вершины (§ 2.5, § 2.6).

Достоверность результатов исследования. Достоверность полученных результатов обеспечивается строгими математическими доказательствами утверждений и подтверждается их согласованностью с данными, полученными в ходе вычислительных экспериментов. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Апробация результатов исследования. Основные результаты диссертации опубликованы в 8 работах в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность» и входящих в списки Scopus или RSCI WoS:

1. Зубков А. М., МIRONKIN В. О., “Распределение длины отрезка апериодичности в графе k -кратной итерации случайного равновероятного отображения”, *Математические вопросы криптографии*, **8**:4 (2017), 63-74.
2. МIRONKIN В. О., Михайлов В. Г., “О множестве образов k -кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **9**:3 (2018), 99-108.
3. МIRONKIN В. О., “Об оценках распределения длины отрезка апериодичности в графе k -кратной итерации равновероятного случайного отображения”, *Прикладная дискретная математика*, **42** (2018), 6-17.
4. МIRONKIN В. О., “Слои в графе k -кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **10**:1 (2019), 73-82.
5. МIRONKIN В. О., “Распределение длины отрезка апериодичности в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **10**:3 (2019), 89-99.
6. МIRONKIN В. О., “Коллизии и инцидентность вершин компонентам в графе k -кратной итерации равновероятного случайного отображения”, *Дискретная математика*, **31**:4 (2019), 38-52.

7. Миронкин В. О., “Слои в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **11:1** (2020), 101-114.
8. Миронкин В. О., “Об образах и прообразах в графе композиции независимых равновероятных случайных отображений”, *Прикладная дискретная математика*, **49** (2020), 5-17.

Результаты диссертации были доложены на следующих семинарах, всероссийских конференциях и симпозиумах:

1. XV Всероссийский Симпозиум по прикладной и промышленной математике (весенняя сессия) (Кисловодск, 1 мая — 8 мая 2014 г.).
2. XVII научно-практическая конференция «РусКрипто'2015» (Московская область, Солнечногорский район, 17 марта — 20 марта 2015 г.).
3. Научный семинар «Математические методы криптографического анализа» МГУ имени М.В. Ломоносова (Москва, 6 апреля 2015 г.).
4. XVI Всероссийский Симпозиум по прикладной и промышленной математике (летняя сессия) (Челябинск, 21 июня — 27 июня 2015 г.).
5. XVI Всероссийский Симпозиум по прикладной и промышленной математике (осенняя сессия)¹ (Сочи, 27 сентября — 4 октября 2015 г.).
6. XVII Всероссийский Симпозиум по прикладной и промышленной математике (весенняя сессия) (Кисловодск, 1 мая — 8 мая 2016 г.).

Структура и объём диссертации. Диссертация состоит из введения, двух глав, разделенных на параграфы, заключения, списка сокращений и

¹Доклад отмечен медалью и грамотой за III место в III Общероссийском открытом конкурсе «Отмеченная работа молодого исследователя в области прикладной и промышленной математики» в 2015 году.

условных обозначений, а также списка литературы, включающего 84 наименования. Текст диссертации изложен на 134 страницах с 8 рисунками.

В первой главе диссертации исследована структура графа k -кратной итерации одного равновероятного случайного отображения конечного множества в себя, $k \in \mathbb{N}$. В частности, для множества $S = \{1, \dots, n\}$, $n > 1$, и вероятностного пространства $(\Omega, \mathcal{F}, \mathbf{P})$, 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 $\mathbf{P}(f) = \frac{1}{n^n} \quad \forall f \in \Omega$ (соотношение (1.1), см. § 1.1), получены результаты, описывающие теоретико-вероятностные свойства и характеристики графа G_{f^k} , которые могут быть использованы при моделировании и исследовании итерационных АМЗИ типа «CryptoPro Key Meshing».

Для длины $\tau_{f^k}(x)$ отрезка аperiodичности $\mathcal{R}_{f^k}(x)$, начинающегося в вершине $x \in S$ графа G_{f^k} , доказан следующий результат.

Теорема 1.1. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P}\{\tau_{f^k}(x) = z\} = \sum_{m \in Q_1^n(k, z)} \frac{(n)_m}{n^{m+1}} + \sum_{m \in \tilde{Q}_1^n(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{(n)_{r+v}}{n^{r+v+1}},$$

где $r = m + \left(z - \frac{m}{(m, k)} - 1\right)k$, а $Q_1^n(k, z)$ и $\tilde{Q}_1^n(k, z)$ определяются соотношениями (1.7), (1.8) в § 1.2.

Здесь и далее по тексту $]z[= \min\{n \in \mathbb{Z}: n \geq z\}$, $[z] = \max\{n \in \mathbb{Z}: n \leq z\}$, а $(n)_k = n(n-1)\dots(n-k+1)$ — k -я факториальная степень числа n .

Через F_k обозначим функцию распределения случайной величины $\tau_{f^k}(x)$ для произвольной фиксированной вершины $x \in S$.

Теорема 1.2. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$, $kz \leq n$, справедливы равенства

$$F_k(z) = \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=0}^{\left(z - \frac{m}{(m, k)}\right)k} \frac{(n)_{m+t}}{n^{m+t+1}}$$

и

$$F_k(z) = \frac{1}{n} \sum_{u=1}^k \sum_{j=0}^{\left[\frac{(k, u)z-u}{k}\right]} S\left(kj + u, \left(z - \frac{kj + u}{(u, k)}\right)k\right),$$

где $S(m, W) = \sum_{t=0}^W \frac{(n)_{m+t}}{n^{m+t}}$, а $\tilde{Q}_1^n(k, z)$ определяется соотношением (1.8) в § 1.2.

Теорема 1.4. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P}\{x \in f^k(S)\} = \sum_{l=1}^n \frac{(n)_l}{n^{l+1}} + \sum_{t=1}^{n-1} \sum_{l=t+1}^n \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l, m}^{(k)},$$

где величины $B_{n-l, m}^{(k)}$ удовлетворяют равенствам (1.22) и (1.23) в § 1.3.

Через T_{f^k} обозначим множество висячих вершин в графе G_{f^k} .

Следствие 1.4. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P}\{x \in T_{f^k}\} = 1 - \sum_{l=1}^n \frac{(n)_l}{n^{l+1}} - \sum_{t=1}^{n-1} \sum_{l=t+1}^n \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l, m}^{(k)}.$$

Через $C_l(G_{f^k})$ обозначим множество циклических вершин графа G_{f^k} , лежащих на циклах длины $l \in \{1, \dots, n\}$.

Теорема 1.5. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \{x \in C_l(G_{f^k})\} = \sum_{m \in Q_1^n(k, l)} \frac{(n)_m}{n^{m+1}},$$

где $Q_1^n(k, l)$ определяется соотношением (1.7) в § 1.2.

Для произвольных $l \in \{1, \dots, n\}$, $t \in \{0, \dots, n-l\}$ определим множество вершин $H_{f^k}^{(t, l)} = \{x \in S: \alpha_{f^k}(x) = t, \beta_{f^k}(x) = l\}$.

Теорема 1.7. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ и $t \in \{1, \dots, n-l\}$ справедливо равенство

$$\mathbf{P} \{x \in H_{f^k}^{(t, l)}\} = \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-tk+s}(k, l)} \frac{(n)_{m+tk-s}}{n^{m+tk-s+1}},$$

где $Q_1^n(k, l)$ определяется соотношением (1.7) в § 1.2.

Для произвольного фиксированного $x \in S$ через $\mathcal{K}_{f^k}(x)$ обозначим компоненту связности графа G_{f^k} , содержащую x .

Теорема 1.10. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} = \sum_{m=1}^n \sum_{v=m}^n \sum_{s=0}^{n-v} \frac{\left(\frac{v}{(m, k)} \left[-\omega_{m, v, s} \right] (n-2)_{v+s-2} \right)}{n^{v+s}},$$

где $\omega_{m, v, s} = \begin{cases} 1, & \text{если } s = 0, \\ \Delta_{(m, k)}^{s, v} & \text{в противном случае,} \end{cases}$ а $\Delta_{(m, k)}^{s, v}$ определяется соотношением (1.56) в § 1.5.

Следствие 1.8. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо двустороннее неравенство

$$\frac{1}{3k} < \lim_{n \rightarrow \infty} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} \leq \frac{2}{3}.$$

Теорема 1.12. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \{y \in (f^k)^{-1}(x)\} = \sum_{m \in \overline{Q}_2^n(k,1)} \frac{(n-2)_{m-2}}{n^m} + \sum_{t=1}^{n-1} \sum_{m=t+1}^n \frac{(n-2)_{m-2}}{n^m},$$

где $\overline{Q}_2^n(k,1) = \{2, \dots, n\} \setminus Q_2^n(k,1)$ определяется соотношением (1.7) в § 1.2.

Теорема 1.13. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{f^k(x) = f^k(y)\} = & \sum_{t=1}^k \sum_{s=0}^{n-1} \sum_{m=t+1}^{n-s} \frac{(1 + \delta_{s,0})(n-2)_{m+s-2}}{n^{m+s}} + \\ & + \sum_{t=1}^k \sum_{m=t+1}^n \sum_{i=0}^{t-1} \sum_{j=\delta_{i,0}}^{\left[\frac{k-t}{m-t}\right]} \frac{(n-2)_{m+i+jm-2}}{n^{m+i+jm}}, \end{aligned}$$

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

Во второй главе диссертации исследована структура графа композиции k независимых равновероятных случайных отображений конечного множества в себя, $k \in \mathbb{N}$. Для вероятностного пространства $(\Omega, \mathcal{F}, \mathbf{P})$ и независимых случайных отображений $f_1, \dots, f_k$, имеющих распределение (1.1) на $\mathfrak{S}$, получены следующие результаты, описывающие теоретико-вероятностные свойства и характеристики графа $G_{f_{[k]}}$.

Через $F_{[k]}$ обозначим функцию распределения случайной величины $\tau_{f_{[k]}}(x)$ для произвольной фиксированной вершины $x \in S$.

Теорема 2.1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{0, 1, \dots, n\}$ справедливо равенство

$$F_{[k]}(z) = 1 - \left(1 - \frac{z}{n}\right) \left(\frac{\binom{n}{z}}{n^z}\right)^k.$$

Следствие 2.2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$, где $|S| = n$, и любого $u \geq 0$ справедливо равенство

$$\lim_{n \rightarrow \infty} \mathbf{P} \left\{ \tau_{f_{[k]}}(x) > u\sqrt{2n} \right\} = e^{-ku^2}.$$

Следствие 2.3. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} = \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right) \left(1 - \frac{z-1}{n}\right)^k\right) \left(\frac{\binom{n}{z-1}}{n^{z-1}}\right)^k.$$

Через $C(G_{f_{[k]}})$ обозначим множество циклических вершин графа $G_{f_{[k]}}$, а через $C_l(G_{f_{[k]}})$ — множество вершин графа $G_{f_{[k]}}$, лежащих на циклах длины $l \in \{1, \dots, n\}$.

Теорема 2.2. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $l \in \{1, \dots, n\}$ справедливы равенства

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

Через $\lambda_{f_{[k]}}$ обозначим случайную величину, равную общему количеству циклических вершин в графе $G_{f_{[k]}}$.

Следствие 2.6. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого $l \in \{1, \dots, n\}$

$$e^{-k(1+\frac{l}{n})\frac{l(l-1)}{2n}} \leq \mathbf{E}\lambda_{f_{[k]}}(l) \leq e^{-k\frac{l(l-1)}{2n}}, \quad \mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{\pi n}{2k}}.$$

Если при этом $n \rightarrow \infty$, то $\mathbf{E}\lambda_{f_{[k]}} = (1 + o(1)) \sqrt{\frac{\pi n}{2k}}$.

Теорема 2.4. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любых $t \in \{1, \dots, n-1\}$, $l \in \{1, \dots, n-t\}$

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

Для произвольных $k \in \mathbb{N}$, $m, s_1, \dots, s_k \in \mathbb{N}$, $n \geq m \geq s_1 \geq \dots \geq s_k$, и произвольных фиксированных различных вершин $y_1, \dots, y_m \in S$ определим событие

$$D_{s_1, \dots, s_k}^{\{k\}}(y_1, \dots, y_m) = \bigcap_{i=1}^k \left\{ |\{f_{[i]}(y_1), \dots, f_{[i]}(y_m)\}| = s_i \right\}.$$

Лемма 2.1. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых $m, s_1, \dots, s_k \in \mathbb{N}$, $n \geq m \geq s_1 \geq \dots \geq s_k$, и любых фиксированных различных $y_1, \dots, y_m \in S$ справедливо равенство

$$\mathbf{P} \left\{ D_{s_1, \dots, s_k}^{\{k\}}(y_1, \dots, y_m) \right\} = q(m, s_1) \prod_{i=1}^{k-1} q(s_i, s_{i+1}),$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$.

Теорема 2.5. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\mathbf{P} \{f_{[k]}(x) = f_{[k]}(y)\} = \sum_{\substack{s_1, \dots, s_{k-1}: \\ 2 \geq s_1 \geq \dots \geq s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}),$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$.

Теорема 2.6. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{x \in f_{[k]}(S)\} &= \frac{1}{n} \sum_{l=1}^n \left(\frac{(n)_l}{n^l}\right)^k + \\ &+ \sum_{l=1}^{n-2} \sum_{t=1}^{n-l-1} \sum_{m=1}^{n-t-l} (-1)^{m-1} C_{n-1}^m \sum_{\substack{s_1, \dots, s_{k-1}: \\ m \geq s_1 \geq \dots \geq s_{k-1}}} \frac{q(m, s_1)}{n^{s_{k-1}}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}) V_{s_1, \dots, s_{k-1}}^{\{k, m\}}, \end{aligned}$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$, а $V_{s_1, \dots, s_{k-1}}^{\{k, m\}}$ определяется соотношением (2.37) в § 2.4.

Теорема 2.7. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \setminus S'$ и любых $r \in \{1, \dots, n-1\}$, $S' \subseteq S$, $|S'| = r$, и $z \in \{1, \dots, n\}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{\tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \emptyset\} &= \\ &= \left(1 - \left(1 - \frac{z}{n}\right) \left(1 - \frac{z-1}{n}\right)^{k-1}\right) \left(\frac{(n)_{z-1}}{n^{z-1}}\right)^{k-1} \frac{(n)_{r+z}}{n^{z-1} (n)_{r+1}}. \end{aligned}$$

Теорема 2.8. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых

фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\mathbf{P} \{y \in \mathcal{K}_{f_{[k]}}(x)\} = 1 - \sum_{z=0}^{n-2} \left(1 - \left(1 - \frac{z+1}{n}\right) \left(1 - \frac{z}{n}\right)^{k-1}\right) \left(\frac{(n)_z}{n^z}\right)^k \frac{C_{n-z}^2}{C_n^2} + \\ + \sum_{z=1}^{n-1} \sum_{u=0}^{n-z-1} \chi_k(z, u),$$

где $\chi_k(z, u)$ определяется соотношением (2.40) в § 2.5.

Теорема 2.9. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $r \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \{y \in (f_{[k]})^{-r}(x)\} = \frac{1}{n} \left(1 - \frac{1}{n-1} \sum_{z \in Q_r \setminus \{1\}} \left(\frac{(n)_z}{n^z}\right)^k\right),$$

где Q_r определяется соотношением (2.52) в § 2.6.

Личный вклад автора. Результаты, представленные в главах 1, 2 настоящей диссертации, получены автором самостоятельно. Соавторам работ [7, 29] (соответственно, А. М. Зубкову и В. Г. Михайлову) принадлежат постановки задач и общее руководство исследованиями. Утверждения, доказанные другими специалистами, содержат ссылки на оригинальные работы и приводятся без доказательства.

Благодарности. Автор выражает искреннюю благодарность научному руководителю доктору физико-математических наук, старшему научному сотруднику Зубкову Андрею Михайловичу за постановку задач и внимание к работе. Автор благодарит доктора физико-математических наук, ведущего научного сотрудника отдела дискретной математики Математического института им. В. А. Стеклова Российской академии наук Михайлова Владимира Гавриловича за проявленный интерес к работе и научное сотрудничество.

1 Итерации равновероятного случайного отображения

Настоящая глава посвящена исследованию вероятностных характеристик и свойств графа k -кратной итерации равновероятного случайного отображения конечного множества в себя, $k \in \mathbb{N}$, находящих свое применение в рамках решения синтезных задач АМЗИ с итерационной структурой.

1.1 Теоретико-вероятностная модель

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:

$$\mathbf{P}(f) = \frac{1}{n^n} \quad \forall f \in \Omega. \quad (1.1)$$

Указанное вероятностное пространство будем называть *вероятностным пространством случайных равновероятных отображений*.

Каждое такое отображение $f: S \rightarrow S$ однозначно определяется набором значений $f(1), \dots, f(n)$, и, как следствие, распределение (1.1) индуцирует

распределение случайных величин $f(1), \dots, f(n)$. В частности, имеет место следующий критерий.

Предложение 1.1. *[12] Случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) тогда и только тогда, когда случайные величины $f(1), \dots, f(n)$ независимы и каждая из них имеет равновероятное распределение на множестве S .*

Из предложения 1.1, в частности, следует, что для последовательности $x_1, x_2 = f(x_1), x_3 = f^2(x_2), \dots$ и попарно различных $a_1, \dots, a_i \in S$, где $i \in \{1, \dots, n-1\}$, а также произвольного $a_{i+1} \in S$ выполняется равенство

$$\mathbf{P}(f(x_i) = a_{i+1} \mid x_1 = a_1, \dots, x_i = a_i) = \frac{1}{n}.$$

При этом в случае реализации события $\{f(x_i) = a_j\}$, где $j \in \{1, \dots, i\}$, для очередной итерации отображения f справедливо

$$\mathbf{P}(f(x_{i+1}) = f(a_j) \mid x_1 = a_1, \dots, x_i = a_i, x_{i+1} = a_j) = 1.$$

Таким образом, траектория в графе G_f , начинающаяся в произвольной вершине из S , формируется случайно и равновероятно до момента попадания в уже пройденную вершину, после чего она становится детерминированной и заикливается. Так, в частности, из [40–42, 48, 49] хорошо известно, что цикловая структура графа случайного отображения представляет собой объединение циклов с подходами, что существенно используется, например, при анализе хеш-функций. При моделировании АМЗИ с использованием модификации случайного равновероятного отображения возникает аналогичная задача описания цикловой структуры графа соответствующего преобразования и оценки ее влияния на теоретическую стойкость [36] АМЗИ в целом.

В настоящей главе в качестве объекта исследования будем рассматривать граф модификации равновероятного случайного отображения $f: S \rightarrow S$,

представляющей его k -кратную итерацию, где $k \in \mathbb{N}$.

При изложении результатов будем использовать следующие определения для характеристик графа отображения (в определениях отображение f будем считать детерминированным).

Определение 1.1. *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 1.2. *Компонентой связности $\mathcal{K}_f(x)$ графа G_f , содержащей вершину $x \in S$, называется множество вершин*

$$\{y \in S : f^l(y) = f^k(x) \text{ для некоторых } k, l \geq 0\}.$$

Определение 1.3. *Вершина $x \in S$ называется циклической вершиной графа G_f , если существует такое $b \geq 1$, что $f^b(x) = x$.*

Для произвольного $x \in S$ множество циклических вершин компоненты связности $\mathcal{K}_f(x)$ обозначим $C_f(x)$ (или, что то же самое, сам цикл), а через $\beta_f(x)$ обозначим случайную величину, равную длине (числу вершин) цикла $C_f(x)$ в графе G_f .

Возвращаясь к вопросу о строении графа G_f , следует отметить, что из каждой его вершины выходит в точности одно ребро. Таким образом, из любой вершины $x_1 \in S$ графа G_f выходит траектория, порожденная последовательным применением отображения f :

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

и заканчивающаяся бесконечным прохождением по циклу $C_f(x_1)$.

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

Определение 1.4. *Подходом $\mathcal{P}_f(x)$, начинающимся в вершине $x \in S$ графа G_f , называется отрезок выходящей из x траектории от x до ее первого попадания в циклическую вершину.*

В рамках определения 1.4 будем считать, что соответствующая циклическая вершина не принадлежит подходу $\mathcal{P}_f(x)$.

Через $\alpha_f(x)$ обозначим случайную величину, равную длине подхода $\mathcal{P}_f(x)$ и будем называть ее *высотой вершины x* в графе G_f :

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

Определение 1.5. *Отрезком аперiodичности $\mathcal{R}_f(x)$, начинающимся в вершине $x \in S$ графа G_f , называется отрезок выходящей из x траектории от x до ее первого самопересечения.*

Через $\tau_f(x)$ обозначим случайную величину, равную длине отрезка аперiodичности $\mathcal{R}_f(x)$:

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

Согласно определениям 1.4, 1.5 для произвольного $x \in S$ выполняется соотношение

$$\tau_f(x) = \alpha_f(x) + \beta_f(x).$$

Замечание 1.1. Распределения случайных величин $\tau_f(x)$, $\alpha_f(x)$, $\beta_f(x)$ зависят от n . Однако во избежание загромождения формул данный факт в тексте диссертации отражаться не будет.

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

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

Будем считать, что f^0 — тождественное отображение множества S в себя.

Заметим, что Ω_k является собственным подмножеством Ω при любом $k > 1$, и что если случайное отображение f имеет равновероятное распределение (1.1), то распределение f^k не является равновероятным ни на Ω , ни на Ω_k .

Замечание 1.2. Величины $\tau_{f^k}(x)$, $\alpha_{f^k}(x)$, $\beta_{f^k}(x)$, определенные для отображения f^k , $k \in \mathbb{N}$, могут быть явно выражены через соответствующие величины $\tau_f(x)$, $\alpha_f(x)$, $\beta_f(x)$. Так, например, для произвольного $x \in S$ длины подходов $\alpha_f(x)$ и $\alpha_{f^k}(x)$ связаны следующим соотношением:

$$\alpha_{f^k}(x) = \left\lceil \frac{\alpha_f(x)}{k} \right\rceil, \quad (1.2)$$

где $\lceil z \rceil = \min \{n \in \mathbb{Z} : n \geq z\}$.

Действительно, пусть $\alpha_f(x) = t \in \{0, 1, \dots, n-1\}$. Тогда, в соответствии с определением 1.4, подход $\mathcal{P}_f(x)$ определяется начальным отрезком длины t траектории

$$x_1 = x, x_2 = f(x), \dots, x_t = f^{t-1}(x), \dots, \quad (1.3)$$

где каждая из первых t вершин не является циклической в графе G_f , а не вошедшие в $\mathcal{P}_f(x)$ вершины $x_{t+1} = f^t(x)$, $x_{t+2} = f^{t+1}(x)$, ... уже являются циклическими.

При этом в $\mathcal{P}_{f^k}(x)$, состоящий из $\alpha_{f^k}(x)$ вершин, попадет каждая k -я вершина указанного отрезка, начиная с x_1 . А именно, в случае $k|t$

$$\mathcal{P}_{f^k}(x) = x_1, x_k, \dots, x_t,$$

и подход состоит из $\frac{t}{k}$ вершин, а в случае $k \nmid t$

$$\mathcal{P}_{f^k}(x) = x_1, x_k, \dots, x_{\lceil \frac{t}{k} \rceil k},$$

где $[z] = \max \{n \in \mathbb{Z} : n \leq z\}$, и подход состоит из $\left[\frac{t}{k}\right] + 1 = \left]\frac{t}{k}\right[$ вершин соответственно, что, в конечном итоге, и доказывает (1.2).

Дополнительно отметим, что часть траектории (1.3), начинающаяся в вершине $x_{t+1} = f^t(x)$, образует $C_f(x)$ и состоит в точности из $\beta_{f^k}(x) = |C_{f^k}(x)|$ вершин.

Нетрудно проверить, что при этом для $\beta_{f^k}(x)$ выполняется соотношение

$$\beta_{f^k}(x) = \frac{\beta_f(x)}{(\beta_f(x), k)}, \quad (1.4)$$

где $(\beta_f(x), k)$ — наибольший общий делитель $\beta_f(x)$ и k .

Действительно, пусть вершины из $C_f(x)$ формируют в графе G_f траекторию $x_1, \dots, x_m$, где $\beta_f(x) = m \in \{1, \dots, n\}$, а $x_1 = x$. На основе этой траектории построим бесконечную периодическую последовательность

$$x_1, \dots, x_m, x_1, \dots, x_m, \dots \quad (1.5)$$

и выделим в ней каждую k -ю вершину, начиная с первой. Очевидно, что первое совпадение среди выделенных вершин произойдет при выделении $[m, k]$ -й вершины последовательности (1.5), где $[m, k]$ — наименьшее общее кратное чисел m и k . При этом последовательность, построенная из выделенных вершин, будет иметь период

$$\frac{[m, k]}{k} = \frac{m}{(m, k)},$$

равный длине цикла, содержащего вершину x , в графе G_{f^k} . Что и требовалось доказать.

В итоге, для произвольного $k \in \mathbb{N}$ из (1.2) и (1.4) вытекает равенство

$$\tau_{f^k}(x) = \frac{\beta_f(x)}{(\beta_f(x), k)} + \left] \frac{\alpha_f(x)}{k} \right[. \quad (1.6)$$

Далее перейдем к более подробному изучению определенных в настоящем параграфе характеристик графов G_{f^k} , когда f имеет равновероятное распределение на Ω , а $k \in \mathbb{N}$ фиксировано.

1.2 Отрезок апериодичности вершины в графе отображения f^k

Одной из характеристик итерационных алгоритмов выработки производных ключей на основе долговременных данных, как правило, хранящихся в секрете [21, 37], существенно влияющих на теоретическую стойкость как самих алгоритмов, так и использующих сформированные ключи АМЗИ, является число тактов работы до момента формирования ранее выработанного ключа. При этом результаты отдельных тактов работы указанных алгоритмов могут использоваться как последовательно (например, как в американском стандарте в банковской отрасли ANSI X9.17 [16]), что соответствует модели равновероятного случайного отображения конечного множества в себя, так и с некоторым фиксированным шагом $k > 1$. Последнее, в свою очередь, описывается моделью k -кратной итерации равновероятного случайного отображения конечного множества в себя.

В качестве примера на рис. 1.1 изображена функциональная схема алгоритма «CryptoPro Key Meshing» [21, 58] выработки последовательности производных 256-битных ключей $k_1, k_2 \dots$ на основе долговременного секретного ключа $k_0 \in V_{256}$ и некоторой открытой информации $C = C_1 || C_2 || C_3 || C_4 \in V_{256}$ с использованием блочного алгоритма зашифрования ГОСТ 28147-89 [47], где $\varphi_{C_i} : V_{256} \rightarrow V_{256}$ — функция зашифрования на ключе, равном C_i , $i = 1, 2, 3, 4$, а символ $||$ обозначает конкатенацию векторов.

Рассмотрим обобщение математической модели алгоритмов выработки производных ключей типа «CryptoPro Key Meshing» на случай, когда результаты отдельных тактов их работы могут быть использованы с произвольным фиксированным периодом $k \in \mathbb{N}$.

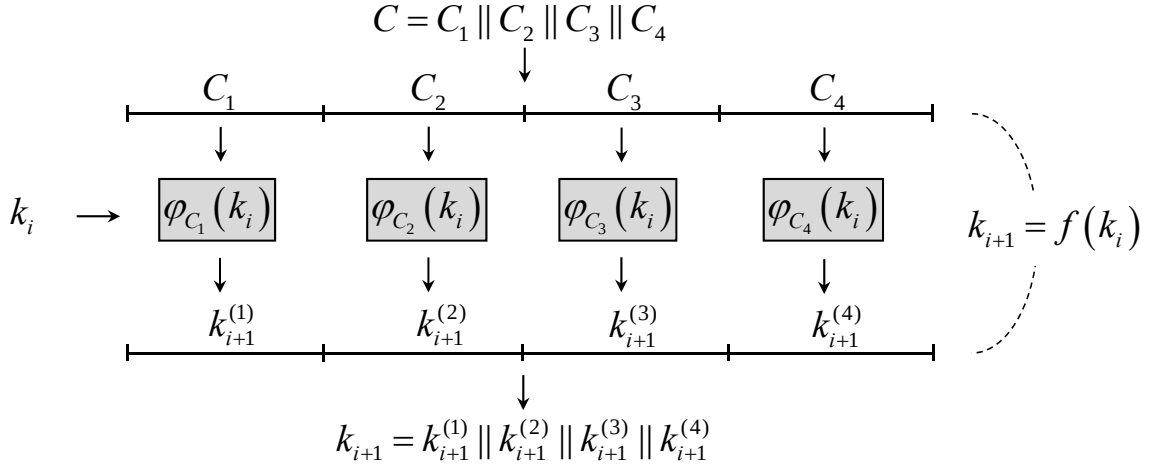


Рис. 1.1: Схема одного такта работы алгоритма «CryptoPro Key Meshing»

Итак, для произвольных $i = 1, 2$ и $k, l, j \in \mathbb{N}$, $j \geq i$, введем обозначения

$$Q_i^j(k, l) = \{m \in \mathbb{N} : i \leq m \leq j, \frac{m}{(m, k)} = l\}, \quad (1.7)$$

$$\tilde{Q}_i^j(k, l) = \{m \in \mathbb{N} : i \leq m \leq j, \frac{m}{(m, k)} < l\}. \quad (1.8)$$

Замечание 1.3. Мощность множества $Q_i^j(k, l)$ не превосходит количества делителей p числа k , для которых $pl \leq j$. В частности, для простого k множество $Q_i^j(k, l)$ состоит не более чем из 2 элементов.

Здесь и далее по тексту для любых $i_0, i_1 \in \mathbb{Z} : i_0 > i_1$ положим $\sum_{j=i_0}^{i_1} (\dots) \equiv 0$, $\prod_{j=i_0}^{i_1} (\dots) \equiv 1$.

Теорема 1.1. [7] Пусть случайное отображение $f : S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \{ \tau_{f^k}(x) = z \} = \sum_{m \in Q_1^n(k, z)} \frac{(n)_m}{n^{m+1}} + \sum_{m \in \tilde{Q}_1^n(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{(n)_{r+v}}{n^{r+v+1}}, \quad (1.9)$$

где $r = m + \left(z - \frac{m}{(m, k)} - 1 \right) k$, а $Q_1^n(k, z)$ и $\tilde{Q}_1^n(k, z)$ определяются соотношениями (1.7), (1.8).

Доказательство. Зафиксируем $x \in S$ и для произвольного $k \in \mathbb{N}$ рассмотрим событие $\{\tau_{f^k}(x) = z\}$. Обозначим через m длину цикла $C_f(x)$, где $m \leq n$. Тогда, в соответствии с (1.4), число циклических вершин на отрезке аperiodичности длины z в графе G_{f^k} , лежащих на указанном цикле, равно $\frac{m}{(m,k)}$, а число вершин, не лежащих на нем, равно $z - \frac{m}{(m,k)}$ (если данная разность неотрицательна). При этом, если $\frac{m}{(m,k)} < z$, то высота $\alpha_f(x)$ вершины x в графе G_f может принимать любое из значений $\min\left(\left(z - \frac{m}{(m,k)}\right)k - v, n - m\right)$, где $v \in \{0, \dots, k-1\}$, если же $\frac{m}{(m,k)} = z$, то $\alpha_f(x) = 0$ (см. рис. 1.2).

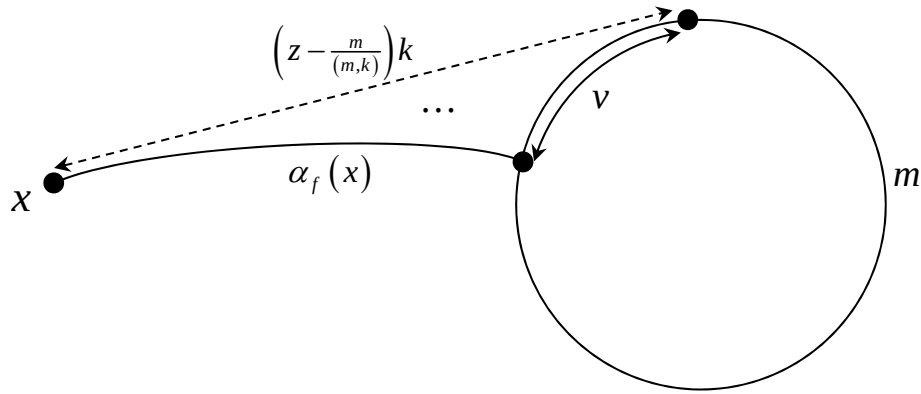


Рис. 1.2: Расположение вершины x в компоненте $\mathcal{K}_f(x)$

С использованием обозначений (1.7), (1.8) запишем равенство событий

$$\begin{aligned} \{\tau_{f^k}(x) = z\} &= \bigcup_{s=1}^z \{\alpha_{f^k}(x) = z - s, \beta_{f^k}(x) = s\} = \\ &= \left(\bigcup_{m \in Q_1^n(k, z)} \left\{ \begin{array}{l} \alpha_f(x)=0, \\ \beta_f(x)=m \end{array} \right\} \right) \cup \left(\bigcup_{m \in \tilde{Q}_1^n(k, z)} \bigcup_{t=(z-\frac{m}{(m,k)}-1)k+1}^{\min((z-\frac{m}{(m,k)})k, n-m)} \left\{ \begin{array}{l} \alpha_f(x)=t, \\ \beta_f(x)=m \end{array} \right\} \right). \end{aligned}$$

Заметим, что события под знаками объединения несовместны, и что при фиксированных z , m и t соответствующие им вероятности равны $\frac{1}{n} \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n}\right)$. Поэтому, положив $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$, для вероятности

искомого события получаем

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z \} &= \\ &= \frac{1}{n} \sum_{m \in Q_1^n(k, z)} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right) + \frac{1}{n} \sum_{m \in \tilde{Q}_1^n(k, z)} \sum_{v=1}^{\min(k, n-r)} \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n} \right), \end{aligned}$$

откуда с учетом очевидного соотношения $\prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right) = \frac{(n)_m}{n^m}$, где $(n)_m = n(n-1)\dots(n-m+1)$ — m -я факториальная степень числа n , вытекает утверждение теоремы. Теорема доказана. $\square$

Из теоремы 1.1, в частности, следует, что при достаточно больших значениях $k \in \mathbb{N}$ цикловая структура графа отображения f^k вырождается в совокупность циклов с подходами длин, не превосходящих 1.

Следствие 1.1. [7] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$, $kz \leq n$, справедливо равенство

$$\mathbf{P} \{ \tau_{f^k}(x) = z \} = \sum_{m \in Q_1^n(k, z)} \frac{(n)_m}{n^{m+1}} + \sum_{m \in \tilde{Q}_1^n(k, z)} \sum_{v=1}^k \frac{(n)_{r+v}}{n^{r+v+1}}, \quad (1.10)$$

где $r = m + \left(z - \frac{m}{(m, k)} - 1 \right) k$, а $Q_1^n(k, z)$ и $\tilde{Q}_1^n(k, z)$ определяются соотношениями (1.7), (1.8).

Доказательство. В условиях настоящего следствия справедлива цепочка соотношений

$$\begin{aligned} n - r - k &= n - m - \left(z - \frac{m}{(m, k)} - 1 \right) k = \\ &= n - kz + m \left(\frac{k}{(m, k)} - 1 \right) \geq n - kz \geq 0, \end{aligned}$$

в соответствии с которой $\min(k, n-r) = k$. В результате искомое выражение вытекает из (1.9). Следствие доказано. $\square$

Нетрудно показать, что выражение (1.10) для $z \in \{1, \dots, n\}$ и простых значений k таких, что $1 < k \leq n$ и $kz \leq n$, может быть представлено в следующем виде:

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z \} = & I \{ z \geq 1 \} \left(\frac{(n)_{zk}}{n^{zk+1}} + (z-1) \sum_{v=1}^k \frac{(n)_{(z-1)k+v}}{n^{(z-1)k+v+1}} \right) + \\ & + I \{ z \pmod k > 0 \} \frac{(n)_z}{n^{z+1}} + \sum_{m=1}^{z-1} I \{ m \pmod k > 0 \} \sum_{v=1}^k \frac{(n)_{m+(z-m-1)k+v}}{n^{m+(z-m-1)k+v+1}}, \end{aligned}$$

где $I \{ A \}$ — индикатор события A .

Так, в качестве примера на рис. 1.3, 1.4 представлена зависимость величины $\mathbf{P} \{ \tau_{f^k}(x) = z \}$ от значений $z \in \{1, \dots, [\frac{n}{k}]\}$ при $n = 256$, $k = 2$ и $k = 7$ соответственно.

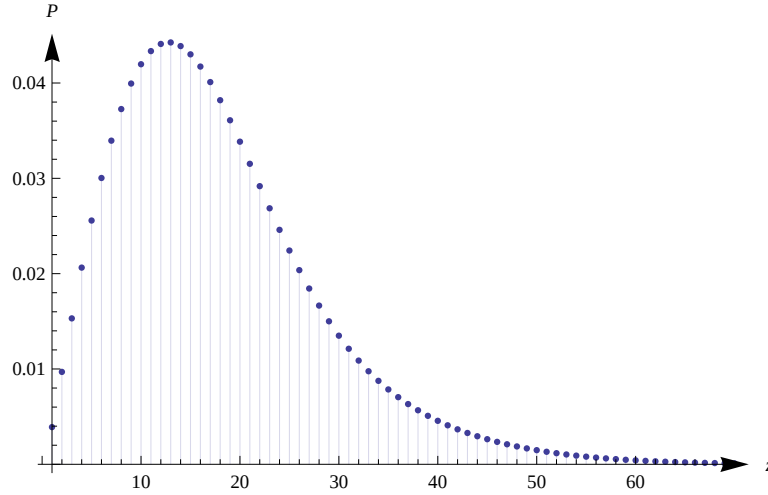


Рис. 1.3: Зависимость $\mathbf{P} \{ \tau_{f^2}(x) = z \}$ от величины z

В свою очередь, для $z \in \{1, \dots, n\}$ и таких простых k , что $k > n$, выражение (1.9) имеет еще более компактную форму:

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = 1 \} &= \frac{1}{n}, \\ \mathbf{P} \{ \tau_{f^k}(x) = z \} &= \frac{(n)_z}{n^{z+1}} + \sum_{v=1}^{n-z+1} \frac{(n)_{z+v-1}}{n^{z+v}}, \quad z = 2, \dots, n, \end{aligned}$$

и, что существенно, не зависит от величины k .

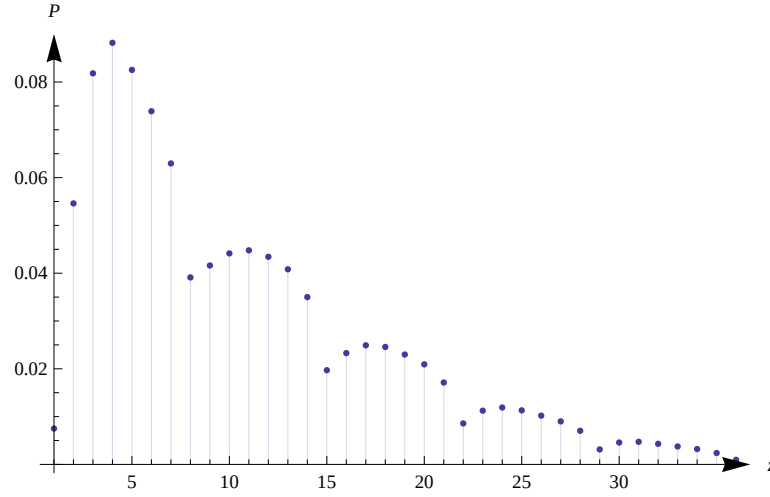


Рис. 1.4: Зависимость $\mathbf{P} \{ \tau_{fk}(x) = z \}$ от величины z

Замечание 1.4. Для итерационных алгоритмов выработки производных ключей типа «CryptoPro Key Meshing», выходами которых являются результаты отдельных тактов, взятых с произвольным фиксированным периодом $k \in \mathbb{N}$, распределение (1.9) случайной величины $\tau_{fk}(x)$ задает распределение периода неповторного использования производных ключей, сформированных на основе некоторого долговременного ключа, соответствующего $x \in S$.

Следует также отметить, что при $kz \leq n$ формула (1.10) позволяет получить оценки величины $\mathbf{P} \{ \tau_{fk}(x) = z \}$, эффективно вычисляемые (без привлечения высокопроизводительных ЭВМ) для используемых на практике значений n , превышающих 2^{64} [33].

Сформулируем результат, приведенный А. М. Зубковым в рамках университетского курса лекций по теории вероятностей и существенно используемый при получении указанных оценок.

Лемма 1.1. Для произвольных $n \in \mathbb{N}$, $m \in \{1, \dots, n\}$ справедливо двустороннее неравенство

$$e^{-\left(1 + \frac{m}{n}\right) \frac{m(m-1)}{2n}} \leq \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right) \leq e^{-\frac{m(m-1)}{2n}}. \quad (1.11)$$

Следствие 1.2. [23] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$, $kz \leq n$, справедливы следующие неравенства:

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z \} &> \frac{1}{n} \sum_{m \in Q_1^n(k, z)} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} + \\ &+ \sum_{m \in \tilde{Q}_1^n(k, z)} e^{-(1+\frac{r}{n})\frac{r^2}{2n}} \left(\frac{1}{r+k} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{r+k}{n} \right)^k \right), \end{aligned}$$

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z \} &< \frac{1}{n} \sum_{m \in Q_1^n(k, z)} e^{-\frac{(m-1)^2}{2n}} + \\ &+ \sum_{m \in \tilde{Q}_1^n(k, z)} e^{-\frac{(r-1)^2}{2n}} \left(\frac{1}{r} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{r}{n} \right)^k \right), \end{aligned}$$

где $r = m + \left(z - \frac{m}{(m, k)} - 1 \right) k$, а $Q_1^n(k, z)$ и $\tilde{Q}_1^n(k, z)$ определяются соотношениями (1.7), (1.8).

Доказательство. Выражение (1.10) может быть представлено в эквивалентном виде (см., например, [7], с. 66):

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z \} &= \\ &= \frac{1}{n} \sum_{m \in Q_1^n(k, z)} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right) + \frac{1}{n} \sum_{m \in \tilde{Q}_1^n(k, z)} \sum_{v=1}^k \prod_{i=1}^{m + \left(z - \frac{m}{(m, k)} - 1 \right) k + v - 1} \left(1 - \frac{i}{n} \right). \quad (1.12) \end{aligned}$$

Рассмотрим отдельно второе слагаемое в (1.12) и преобразуем сумму вида $\sum_{v=1}^k \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n} \right)$, где $r \geq 1$, следующим образом:

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

Вместе с этим при условии $0 < \frac{r}{n} < \frac{r+k}{n} \leq 1$ справедливы оценки сверху и снизу:

$$\sum_{w=0}^{k-1} \prod_{j=0}^w \left(1 - \frac{r+j}{n}\right) < \sum_{w=0}^{k-1} \left(1 - \frac{r}{n}\right)^{w+1} = \frac{n-r}{r} \left(1 - \left(1 - \frac{r}{n}\right)^k\right), \quad (1.13)$$

$$\begin{aligned} \sum_{w=0}^{k-1} \prod_{j=0}^w \left(1 - \frac{r+j}{n}\right) &> \\ &> \sum_{w=0}^{k-1} \left(1 - \frac{r+k}{n}\right)^{w+1} = \left(\frac{n}{r+k} - 1\right) \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right). \end{aligned} \quad (1.14)$$

Тогда с учётом (1.13), (1.14) и двустороннего неравенства

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

вытекающего из (1.11) и справедливого для $1 \leq r \leq n$, получаем

$$\begin{aligned} \left(\frac{n}{r+k} - 1\right) e^{-(1+\frac{r}{n})\frac{r^2}{2n}} \left(1 - \left(1 - \frac{r+k}{n}\right)^k\right) &< \\ &< \sum_{v=1}^k \prod_{i=1}^{r+v-1} \left(1 - \frac{i}{n}\right) < \frac{n-r}{r} e^{-\frac{(r-1)^2}{2n}} \left(1 - \left(1 - \frac{r}{n}\right)^k\right). \end{aligned} \quad (1.15)$$

Положим $r = m + \left(z - \frac{m}{(m,k)} - 1\right)k$. Тогда из ограничений $\frac{m}{(m,k)} < z$ и $m \geq 1$ на суммирование во втором слагаемом в (1.12) следует, что $r \geq 1$.

Поэтому из условия $kz \leq n$ получаем цепочку неравенств

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

Таким образом, $0 < \frac{r}{n} < \frac{r+k}{n} \leq 1$, и следовательно, неравенство (1.15) выполняется для искомой вероятности. Следствие доказано. $\square$

Через $\nu_{fk}(z)$ обозначим случайную величину, равную числу вершин в графе G_{fk} , для которых длина отрезка аperiodичности равна $z \in \{1, \dots, n\}$.

Замечание 1.5. В силу равноправия вершин из S математическое ожидание $\nu_{f^k}(z)$ определяется равенством $\mathbf{E}\nu_{f^k}(z) = n\mathbf{P}\{\tau_{f^k}(x) = z\}$.

Далее через F_k обозначим функцию распределения случайной величины $\tau_{f^k}(x)$ для произвольной фиксированной вершины $x \in S$ (в силу равноправия вершин из S зависимость от x отражать не будем).

Теорема 1.2. [7] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$, $kz \leq n$, справедливы равенства

$$F_k(z) = \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=0}^{\left(z - \frac{m}{(m, k)}\right)k} \frac{(n)_{m+t}}{n^{m+t+1}}, \quad (1.16)$$

и

$$F_k(z) = \frac{1}{n} \sum_{u=1}^k \sum_{j=0}^{\left[\frac{(k, u)z - u}{k}\right]} S\left(kj + u, \left(z - \frac{kj + u}{(u, k)}\right)k\right), \quad (1.17)$$

где $S(m, W) = \sum_{t=0}^W \frac{(n)_{m+t}}{n^{m+t}}$, а $\tilde{Q}_1^n(k, z)$ определяется соотношением (1.8).

Доказательство. Для произвольных фиксированных $x \in S$, $k \in \mathbb{N}$ и $z \in \{1, \dots, n\}$ таких, что $kz \leq n$, справедливо равенство событий

$$\{\tau_{f^k}(x) \leq z\} = \bigcup_{u=1}^z \{\alpha_{f^k}(x) \leq z - u, \beta_{f^k}(x) = u\}.$$

Перепишем его с использованием случайных величин $\alpha_f(x)$ и $\beta_f(x)$.

Учитывая соотношение

$$\{\beta_{f^k}(x) = u\} = \bigcup_{m \in Q_1^n(k, u)} \{\beta_f(x) = m\}$$

и тот факт, что при фиксированном значении m длина $\beta_{f^k}(x)$ соответствующей

щего цикла в графе G_{fk} равна $u = \frac{m}{(m,k)}$, получаем цепочку равенств

$$\begin{aligned}
\{\tau_{fk}(x) \leq z\} &= \bigcup_{u=1}^z \bigcup_{m \in Q_1^n(k,u)} \left\{ \alpha_{fk}(x) \leq z - \frac{m}{(m,k)}, \beta_f(x) = m \right\} = \\
&= \bigcup_{m \in \tilde{Q}_1^n(k,z+1)} \left\{ \alpha_{fk}(x) \leq z - \frac{m}{(m,k)}, \beta_f(x) = m \right\} = \\
&= \bigcup_{m \in \tilde{Q}_1^n(k,z+1)} \left\{ \alpha_f(x) \leq \left(z - \frac{m}{(m,k)} \right) k, \beta_f(x) = m \right\} = \\
&= \bigcup_{m \in \tilde{Q}_1^n(k,z+1)} \bigcup_{t=0}^{\left(z - \frac{m}{(m,k)} \right) k} \{ \alpha_f(x) = t, \beta_f(x) = m \},
\end{aligned}$$

где события, стоящие под знаком последнего объединения, несовместны, и соответствующие им вероятности равны $\frac{1}{n} \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n} \right)$. Отсюда, очевидно, следует равенство (1.16).

Чтобы доказать справедливость формулы (1.17), положим при $m \geq 1$, $W \geq 0$

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

тогда формулу (1.16) можно переписать в виде

$$F_k(z) = \frac{1}{n} \sum_{m \in \tilde{Q}_1^n(k,z+1)} S \left(m, \left(z - \frac{m}{(m,k)} \right) k \right).$$

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

$$F_k(z) = \frac{1}{n} \sum_{u=1}^k \sum_{j=0}^{\left[\frac{(k,u)z-u}{k} \right]} S \left(kj + u, \left(z - \frac{kj+u}{(u,k)} \right) k \right).$$

Теорема доказана. □

Замечание 1.6. Нетрудно показать, что в отсутствии ограничения $kz \leq n$ формула (1.16) принимает следующий вид:

$$F_k(z) = \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=0}^{\min\left(\left(z - \frac{m}{(m,k)}\right)k, n-m\right)} \frac{(n)_{m+t}}{n^{m+t+1}}. \quad (1.18)$$

В свою очередь, из (1.18) и равенства

$$\mathbf{E}\xi = \sum_{z=0}^{\infty} \mathbf{P}\{\xi > z\} \quad (1.19)$$

для математического ожидания случайной величины ξ , принимающей натуральные значения (см., например, [15], с. 11), вытекает формула для $\mathbf{E}\tau_{f^k}(x)$, где x — произвольная вершина из S :

$$\mathbf{E}\tau_{f^k}(x) = \sum_{z=0}^{n-1} \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=0}^{\min\left(\left(z - \frac{m}{(m,k)}\right)k, n-m\right)} \frac{(n)_{m+t}}{n^{m+t+1}}.$$

Следствие 1.3. [23] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$, $kz \leq n$, справедливо двустороннее неравенство

$$\begin{aligned} \sum_{m \in \tilde{Q}_1^n(k, z+1)} e^{-(1+\frac{m}{n})\frac{m^2}{2n}} \left(\frac{1}{n} + \left(\frac{1}{m+r} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{m+r}{n} \right)^r \right) \right) < \\ < F_k(z) < \sum_{m \in \tilde{Q}_1^n(k, z+1)} e^{-\frac{(m-1)^2}{2n}} \left(\frac{1}{n} + \frac{n-m}{mn} \left(1 - \left(1 - \frac{m}{n} \right)^r \right) \right), \end{aligned}$$

где $r = \left(z - \frac{m}{(m,k)} \right) k$, а $\tilde{Q}_1^n(k, z)$ определяется соотношением (1.8).

Доказательство. Выделим в (1.16) слагаемые, соответствующие значению $t = 0$. Тогда, положив $r = \left(z - \frac{m}{(m,k)} \right) k$, можно записать

$$F_k(z) = \frac{1}{n} \sum_{m \in \tilde{Q}_1^n(k, z+1)} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right) + \frac{1}{n} \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=1}^r \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n} \right).$$

Представим сумму $\sum_{t=1}^r \prod_{i=1}^{m+t-1} \left(1 - \frac{i}{n}\right)$, где $m \geq 1$, в следующем виде:

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

При этом справедлива цепочка неравенств $0 < \frac{m}{n} < \frac{m+r}{n} \leq 1$. Действительно,

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

Тогда имеют место оценки

$$\sum_{w=0}^{r-1} \prod_{j=0}^w \left(1 - \frac{m+j}{n}\right) < \left(\frac{n}{m} - 1\right) \left(1 - \left(1 - \frac{m}{n}\right)^r\right),$$

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

Рассуждая далее как и при доказательстве следствия 1.2, получаем искомое выражение. Следствие доказано. $\square$

Замечание 1.7. Выражение (1.17) также позволяет получать явные двусторонние оценки для функции распределения случайной величины $\tau_{fk}(x)$. Наметим способ вывода таких оценок.

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

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

Учитывая неравенства

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

находим, что при $1 \leq m \leq \frac{n}{2}$

$$\begin{aligned}
S(m, W) &\leq \sum_{t=0}^W e^{-\frac{(m+t)(m+t-1)}{2n}} = \sum_{t=m}^{m+W} e^{-\frac{t(t-1)}{2n}} < \\
&< \int_{m-1}^{m+W} e^{-\frac{x(x-1)}{2n}} dx = \int_{m-1}^{m+W} e^{-\frac{(x-1/2)^2}{2n} + \frac{1}{8n}} dx = \\
&= \sqrt{2\pi n} e^{\frac{1}{8n}} \left(\Phi\left(\frac{m+W-1/2}{\sqrt{n}}\right) - \Phi\left(\frac{m-1-1/2}{\sqrt{n}}\right) \right), \quad (1.20)
\end{aligned}$$

где $\Phi(x)$ — функция стандартного нормального распределения, и при $c = \sqrt{1 + \frac{2(m+W)}{3n}}$.

$$\begin{aligned}
S(m, W) &\geq \sum_{t=0}^W e^{-\left(1 + \frac{2(m+t)}{3n}\right) \frac{(m+t)(m+t-1)}{2n}} > \\
&> \sum_{t=0}^W e^{-c^2 \frac{(m+t)(m+t-1)}{2n}} > \int_m^{m+W} e^{-\frac{(x-1/2)^2}{2n/c^2} + \frac{c^2}{8n}} dx = \\
&= \frac{\sqrt{2\pi n}}{c} e^{\frac{c^2}{8n}} \left(\Phi\left(\frac{(m+W+1/2)c}{\sqrt{n}}\right) - \Phi\left(\frac{m-1/2}{\sqrt{n}} c\right) \right). \quad (1.21)
\end{aligned}$$

Далее суммы двусторонних оценок (1.20) и (1.21) значений $S(m, W)$, входящих в (1.17), можно получить с помощью равенства

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

1.3 Множество образов при отображении f^k

Один из наиболее значимых этапов синтеза АМЗИ рассматриваемого типа, в частности, хеш-функций и алгоритмов выработки производных ключей, заключается в оценке степени сжатия исходного множества в процессе работы АМЗИ. В ряде случаев значение указанной характеристики позволяет сделать выводы о наличии или отсутствии потенциальных уязвимостей

разрабатываемого АМЗИ, а также оценить его теоретическую стойкость относительно некоторых методов опробования [1, 2, 36].

В свою очередь, для алгоритмов выработки производных ключей, как правило, решается и обратная задача, заключающаяся в описании потенциально возможного множества ключей, сформированного к заданному такту работы соответствующего алгоритма. Так, в частности, информация об указанном множестве может быть использована в рамках анализа возможных последствий компрометации текущего производного (сеансового) ключа (см., например, гл. 10 в [54]).

Итак, для случайного отображения $f: S \rightarrow S$, имеющего распределение (1.1) на Ω , положим $S(r) = \{1, \dots, r\} \subset S$, где $1 \leq r < n$, и для произвольного $y \in S(r)$ рассмотрим следующее событие:

$$F_y^{(k)}(r) = \{y, f(y), \dots, f^{k-1}(y) \in S(r) \text{ различны; } f^k(y) = r+1\}.$$

Для произвольного $m \in \{1, \dots, r\}$ определим величины

$$B_{r,m}^{(k)} = \sum_{1 \leq y_1 < \dots < y_m \leq r} \mathbf{P} \left\{ \bigcap_{i=1}^m F_{y_i}^{(k)}(r) \right\} = C_r^m P_{r,m}^{(k)}, \quad (1.22)$$

где $P_{r,m}^{(k)} = \mathbf{P} \left\{ \bigcap_{i=1}^m F_i^{(k)}(r) \right\}$ в силу равноправия всех вершин из S . При этом событие $\left\{ \bigcap_{i=1}^m F_i^{(k)}(r) \right\}$ означает, что в течение первых $k-1$ итераций отображение f не позволяет заикливиться образам вершин $1, \dots, m$ и не выводит их из множества $S(r)$, а на k -м шаге отображение f переводит их в одну и ту же вершину $r+1$.

Из (1.22) легко вывести, что

$$P_{r,m}^{(1)} = \frac{1}{n^m}, \quad B_{r,m}^{(1)} = \frac{C_r^m}{n^m}. \quad (1.23)$$

Лемма 1.2. [29] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда величины $P_{r,m}^{(k)}$, определенные формулами (1.22)

и (1.23), при $m = 1, \dots, r$ удовлетворяют соотношениям

$$P_{r,m}^{(k)} = \sum_{s=1}^m a_{r,m,s} P_{r-m,s}^{(k-1)}, \quad k \geq 2, \quad (1.24)$$

где числа $a_{r,m,s}$ определяются равенствами

$$a_{r,m,s} = C_{r-m}^s \left(\frac{s}{n}\right)^m \sum_{t=0}^s C_s^t (-1)^t \left(1 - \frac{t}{s}\right)^m. \quad (1.25)$$

Доказательство. Пусть $m = 1$. Тогда согласно (1.22) имеет место равенство

$$P_{r,1}^{(k)} = \mathbf{P} \left\{ F_1^{(k)}(r) \right\} = \frac{(r-1)(r-2) \dots (r-k+1)}{n^k} = \frac{(r-1)_{k-1}}{n^k},$$

соответствующее (1.23) и (1.24).

Пусть $m \geq 2$. Для равномерного случайного отображения $f: S \rightarrow S$ совместное распределение значений $f(1), \dots, f(m)$ соответствует равномерной схеме независимого размещения m частиц по n ячейкам с номерами $1, \dots, m, m+1, \dots, n$.

Через $G_m(r)$ обозначим событие, заключающееся в том, что в результате размещения все m частиц попали в ячейки с номерами из множества $S(r) \setminus \{1, \dots, m\} = \{m+1, \dots, r\}$, а через $\mu(m, n)$ — случайную величину, равную числу занятых ячеек.

Для значений $f(1), \dots, f(m)$ рассмотрим полную группу событий $H_s = \{\mu(m, n) = s\}$, $s = 1, 2, \dots, m$, соответствующих тому, что после применения отображения f к вершинам $1, \dots, m$ соответствующие m траекторий в графе G_f склеились ровно в s траекторий (см. рис. 1.5).

Таким образом, по формуле полной вероятности (см., например, [55], с. 46) получаем рекуррентное соотношение:

$$P_{r,m}^{(k)} = \sum_{s=1}^m \mathbf{P} \{G_m(r) \cap \{\mu(m, n) = s\}\} P_{r-m,s}^{(k-1)}. \quad (1.26)$$

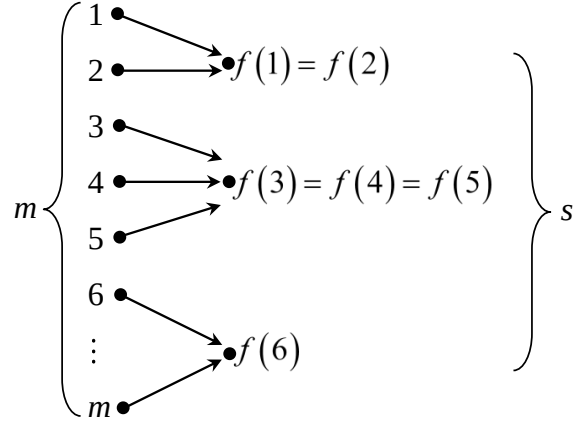


Рис. 1.5: Пример склеивания траекторий в графе G_f

При каждом фиксированном $s \in \{1, \dots, m\}$ представим вероятность, стоящую под знаком суммирования в (1.26), в следующем виде:

$$\mathbf{P}\{G_m(r) \cap \{\mu(m, n) = s\}\} = \mathbf{P}\{\mu(m, n) = s \mid G_m(r)\} \mathbf{P}\{G_m(r)\}.$$

При этом

$$\mathbf{P}\{G_m(r)\} = \left(\frac{r-m}{n}\right)^m, \quad (1.27)$$

$$\begin{aligned} \mathbf{P}\{\mu(m, n) = s \mid G_m(r)\} &= \mathbf{P}\{\mu(m, r-m) = s\} = \\ &= \mathbf{P}\{\mu(m, r') = s\} = \mathbf{P}\{\mu_0(m, r') = r' - s\}, \end{aligned} \quad (1.28)$$

где $r' = r - m$, а $\mu_0(m, r') = r' - \mu(m, r')$ — число пустых ячеек при равномерном размещении m частиц по r' ячейкам.

Согласно формулам для распределения величины $\mu_0(m, r')$ (см. [14], формулы (1), (2) на с. 10)

$$\mathbf{P}\{\mu_0(m, r') = r' - s\} = C_{r'}^s \left(\frac{s}{r'}\right)^m \sum_{t=0}^s C_s^t (-1)^t \left(1 - \frac{t}{s}\right)^m. \quad (1.29)$$

Из (1.27) — (1.29) вытекает формула

$$\mathbf{P}\{G_m(r) \cap \{\mu(m, n) = s\}\} = C_{r-m}^s \left(\frac{s}{n}\right)^m \sum_{t=0}^s C_s^t (-1)^t \left(1 - \frac{t}{s}\right)^m.$$

В свою очередь, из нее и (1.26) следуют (1.24) и (1.25). Лемма доказана. $\square$

Через $f^k(S)$ обозначим образ множества S при действии отображения f^k , $k \geq 1$.

Теорема 1.3. [29] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P}\{x \in f^k(S)\} = \sum_{l=1}^n \frac{(n)_l}{n^{l+1}} + \sum_{t=1}^{n-1} \sum_{l=t+1}^n \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l,m}^{(k)}, \quad (1.30)$$

где величины $B_{n-l,m}^{(k)}$ удовлетворяют равенствам (1.22) и (1.23).

Доказательство. Для произвольной фиксированной вершины $x \in S$ рассмотрим событие

$$E_{t,l}(x) = \{\alpha_f(x) = t, \beta_f(x) = l\},$$

которое может быть представлено в виде объединения попарно несовместных событий:

$$E_{t,l}(x) = \bigcup_{T_{t,l}} \{f(x) = x_1, \dots, f^{t+l}(x) = x_{t+l}\},$$

где

$$T_{t,l} = \{(x_1, \dots, x_{t+l}) :$$

$$x_1, \dots, x_{t+l} \in S \setminus \{x\}, x_{t+l} = x_t, |\{x_1, \dots, x_{t+l}\}| = t + l - 1\}.$$

Здесь и далее t и l указывают соответственно высоту вершины x и длину цикла, на подходе к которому лежит x . Очевидно, что

$$\{x \in f^k(S)\} = \{x \in C(G_{f^k})\} \cup \bigcup_{t=1}^{n-1} \bigcup_{l=1}^{n-t} \{\{x \in f^k(S)\} \cap E_{t,l}(x)\}. \quad (1.31)$$

В силу несовместности событий, указанных в правой части (1.31), и равенства $C(G_{f^k}) = C(G_f)$ получаем

$$\begin{aligned} \mathbf{P}\{x \in f^k(S)\} &= \\ &= \mathbf{P}\{x \in C(G_f)\} + \sum_{t=1}^{n-1} \sum_{l=1}^{n-t} \mathbf{P}\{\{x \in f^k(S)\} \cap E_{t,l}(x)\}. \end{aligned} \quad (1.32)$$

Для первого слагаемого в (1.32) выполнено равенство

$$\mathbf{P}\{x \in C(G_f)\} = \sum_{l=1}^n \frac{(n)_l}{n^{l+1}}, \quad (1.33)$$

вытекающее, например, из формулы (3.1) на с. 1047 в [72].

Теперь вычислим вероятности, стоящие под знаками суммирования в правой части (1.32). При фиксированных значениях $t \in \{1, \dots, n-1\}$, $l \in \{1, \dots, n-t\}$ имеет место соотношение

$$\begin{aligned} \{x \in f^k(S)\} \cap E_{t,l}(x) &= \\ &= \bigcup_{T_{t,l}} \bigcup_{y \in S'} \left\{ \tilde{F}_{x,y}^{(k)}(S'); f(x) = x_1, \dots, f^{t+l}(x) = x_{t+l} \right\}, \end{aligned} \quad (1.34)$$

где $S' = S \setminus \{x, x_1, \dots, x_{t+l-1}\}$ и для произвольного $M \subseteq S$

$$\tilde{F}_{x,y}^{(k)}(M) = \{y, f(y), \dots, f^{k-1}(y) \in M \text{ различны; } f^k(y) = x\}.$$

Из несовместности событий $\{f(x) = x_1, \dots, f^{t+l}(x) = x_{t+l}\}$, входящих в правую часть равенства (1.34), получаем, что

$$\begin{aligned} \mathbf{P}\{\{x \in f^k(S)\} \cap E_{t,l}(x)\} &= \\ &= \sum_{T_{t,l}} \mathbf{P}\left\{ \bigcup_{y \in S'} \left\{ \tilde{F}_{x,y}^{(k)}(S'); f(x) = x_1, \dots, f^{t+l}(x) = x_{t+l} \right\} \right\}, \end{aligned} \quad (1.35)$$

Заметим, что все слагаемые суммы в (1.35) одинаковые по величине. Рассмотрим слагаемое, отвечающее $(x_1, \dots, x_{t+l}) = v$, где

$$v = (n-t-l+2, n-t-l+3, \dots, n-l+1, \dots, n, n-l+1) \in T_{t,l}.$$

В этом случае $S' = \{1, \dots, r\}$, где $r = n - t - l$, $x_0 = r + 1$. Умножим это слагаемое на общее число слагаемых $|T_{t,l}| = (n - 1)_{t+l-1}$ и силу независимости в совокупности случайных величин $f(x)$, $x \in S$, получим

$$\begin{aligned} \mathbf{P} \{ \{x \in f^k(S)\} \cap E_{t,l}(x) \} &= \\ &= (n - 1)_{t+l-1} \mathbf{P} \left\{ \bigcup_{y \in S'} \tilde{F}_{x,y}^{(k)}(S') \right\} \mathbf{P} \{ (f(x), \dots, f^{t+l}(x)) = v \} = \\ &= \frac{(n - 1)_{t+l-1}}{n^{t+l}} \mathbf{P} \left\{ \bigcup_{y \in S(r)} F_y^{(k)}(r) \right\}. \end{aligned} \quad (1.36)$$

По формуле включения-исключения (см., например, [41], с. 23)

$$\mathbf{P} \left\{ \bigcup_{y \in S(r)} F_y^{(k)}(r) \right\} = \sum_{m=1}^r (-1)^{m-1} B_{r,m}^{(k)}, \quad (1.37)$$

где величины $B_{r,m}^{(k)}$ определяются соотношениями (1.22), (1.23). Таким образом, из (1.36) и (1.37) следует, что

$$\mathbf{P} \{ \{x \in f^k(S)\} \cap E_{t,l}(x) \} = \frac{(n - 1)_{t+l-1}}{n^{t+l}} \sum_{m=1}^r (-1)^{m-1} B_{r,m}^{(k)}. \quad (1.38)$$

Подставив (1.38) и (1.33) в (1.32), получим искомое выражение (1.30). Теорема доказана. $\square$

Замечание 1.8. В силу равноправия всех $x \in S$ и равенства

$$|f^k(S)| = \sum_{x \in S} I \{x \in f^k(S)\}$$

имеет место цепочка соотношений

$$\mathbf{E} |f^k(S)| = \mathbf{E} \sum_{x \in S} I \{x \in f^k(S)\} = n \mathbf{P} \{x \in f^k(S)\}.$$

Замечание 1.9. В случае, когда величина k превышает максимум длин подходов в графе G_{f^k} , что заведомо выполняется при $k \geq n - 1$, выполняется равенство $f^k(S) = C(G_f)$.

Определение 1.6. Вершина $x \in S$ в графе G_f называется *висячей вершиной*, если не существует $y \in S$: $f(y) = x$.

Через T_{f^k} обозначим множество висячих вершин в графе G_{f^k} , $k \in \mathbb{N}$.

Из определения 1.6 следует, что T_{f^k} соответствует множеству ключей, которые не могут быть сформированы в процессе работы итерационного алгоритма рассматриваемого типа, для моделирования которого используется случайное отображение f^k .

При $k = 1$ множество T_f изучалось, например, в [71]. Рассмотрим общий случай $k \geq 1$. Вычислим вероятность попадания произвольной вершины x графа G_{f^k} в множество T_{f^k} . Заметим, что для любого $f: S \rightarrow S$

$$S = f^k(S) \cup T_{f^k}, \quad f^k(S) \cap T_{f^k} = \emptyset.$$

Поэтому для произвольного фиксированного $x \in S$ выполняется соотношение

$$\mathbf{P}\{x \in T_{f^k}\} = 1 - \mathbf{P}\{x \in f^k(S)\},$$

позволяющее применить теорему 1.3 для вычисления $\mathbf{P}\{x \in T_{f^k}\}$.

Следствие 1.4. Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P}\{x \in T_{f^k}\} = 1 - \sum_{l=1}^n \frac{(n)_l}{n^{l+1}} - \sum_{t=1}^{n-1} \sum_{l=t+1}^n \frac{(n-1)_{l-1}}{n^l} \sum_{m=1}^{n-l} (-1)^{m-1} B_{n-l,m}^{(k)},$$

где величины $B_{n-l,m}^{(k)}$ удовлетворяют равенствам (1.22) и (1.23).

Замечание 1.10. В силу равноправия всех $x \in S$ имеет место цепочка равенств

$$\mathbf{E} |T_{f^k}| = n\mathbf{P}\{x \in T_{f^k}\} = n - n\mathbf{P}\{x \in f^k(S)\}.$$

Замечание 1.11. При $k \geq n - 1$ множеству T_{f^k} принадлежат все вершины графа G_f , лежащие на подходах к циклам.

1.4 Слои и циклические вершины в графе отображения f^k

Классификация элементов формируемого ключевого множества на основе количественных характеристик используемого для моделирования работы АМЗИ отображения представляет собой отдельный этап как синтеза, так и анализа соответствующего АМЗИ. В некоторых случаях подобная классификация позволяет задать на исходном множестве ключей отношение эквивалентности, существенно используемое для оценки теоретической стойкости анализируемого итерационного алгоритма выработки производных ключей.

Так, в качестве классифицирующей характеристики будем рассматривать значение высоты $\alpha_{f^k}(x)$ отдельно взятой произвольной вершины x в графе G_{f^k} , $k \in \mathbb{N}$.

Определение 1.7. Для произвольного $t \in \{0, \dots, n - 1\}$ назовём t -м *слоем* в графе G_f множество вершин $H_f^{(t)} = \{x \in S : \alpha_f(x) = t\}$.

Определение 1.8. 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 $H_f^{(t,l)} = \{x \in S : \alpha_f(x) = t, \beta_f(x) = l\}$.

Из определений 1.7 и 1.8 для отображения f^k при $t = 0$ вытекают равенства множеств $H_{f^k}^{(0)} = C(G_{f^k})$ и $H_{f^k}^{(0,l)} = C_l(G_{f^k})$.

В частности, в случае $k = 1$ множества вершин $H_{f^k}^{(0)}$ и $H_{f^k}^{(0,l)}$ подробно изучены в работах [6, 32, 41].

Теорема 1.4. [24] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \{x \in C_l(G_{f^k})\} = \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}}, \quad (1.39)$$

где $Q_1^n(k, l)$ определяется соотношением (1.7).

Доказательство. Зафиксируем вершину $x \in S$ и обозначим через m длину цикла компоненты $\mathcal{K}_f(x)$ графа G_f , содержащей вершину x , где $m \leq n$. Тогда соответствующая компонента содержит цикл длины $l = \frac{m}{(m,k)}$. Используя обозначение (1.7), для произвольных $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ запишем равенство событий

$$\{x \in C_l(G_{f^k})\} = \bigcup_{m \in Q_1^n(k,l)} \left\{ \begin{array}{l} \alpha_f(x) = 0, \\ \beta_f(x) = m \end{array} \right\}. \quad (1.40)$$

Заметим, что события, стоящие под знаком объединения в (1.40), несовместны, и что при фиксированных l и m вероятности соответствующих событий равны $\frac{(n)_m}{n^{m+1}}$. Поэтому, переходя в (1.40) к вероятностям, получаем

$$\mathbf{P} \{x \in C_l(G_{f^k})\} = \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}},$$

что соответствует утверждению теоремы. Теорема доказана. $\square$

Следствие 1.5. [24] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ справедлива двусторонняя оценка

$$\frac{1}{n} \sum_{m \in Q_1^n(k,l)} e^{-(1+\frac{m}{n})\frac{m(m-1)}{2n}} \leq \mathbf{P} \{x \in C_l(G_{f^k})\} \leq \frac{1}{n} \sum_{m \in Q_1^n(k,l)} e^{-\frac{(m-1)^2}{2n}},$$

где $Q_1^n(k, z)$ определяется соотношением (1.7).

Доказательство. С учетом двустороннего неравенства, вытекающего из (1.11):

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

справедливого для $1 \leq m \leq n$, получаем искомую оценку. Следствие доказано. $\square$

Важно отметить, что при переходе от графа G_f к графу G_{f^k} , $k > 1$, множество циклических вершин остается неизменным. При этом из (1.39) для произвольного фиксированного $x \in S$ и любого $k \in \mathbb{N}$ следует равенство

$$\mathbf{P} \{x \in C(G_{f^k})\} = \sum_{l=1}^n \sum_{m \in Q_1^n(k, l)} \frac{(n)_m}{n^{m+1}}. \quad (1.41)$$

С учетом справедливого для произвольного $k \in \mathbb{N}$ соотношения

$$\{1, \dots, n\} = \bigcup_{l=1}^n Q_1^n(k, l)$$

формула (1.41) может быть записана в следующем виде:

$$\mathbf{P} \{x \in C(G_{f^k})\} = \sum_{l=1}^n \frac{(n)_l}{n^{l+1}},$$

где правая часть равенства не зависит от k . Таким образом, для произвольного $k \in \mathbb{N}$

$$\mathbf{P} \{x \in H_{f^k}^{(0)}\} = \mathbf{P} \{x \in H_f^{(0)}\} = \sum_{l=1}^n \frac{(n)_l}{n^{l+1}}.$$

При этом распределение случайной величины λ_f , равной общему количеству циклических вершин в графе G_f , также не зависит от k . С учетом хорошо известного выражения

$$\mathbf{P} \{\lambda_f = j\} = \frac{j(n)_j}{n^{j+1}}, \quad (1.42)$$

справедливого для любого $j \in \{1, \dots, n\}$ (см., например, [84], формула (3.8) на с. 6), для произвольного $k \in \mathbb{N}$ получаем цепочку равенств

$$\mathbf{P} \{ \lambda_{f^k} = j \} = \mathbf{P} \{ \lambda_f = j \} = \frac{j(n)_j}{n^{j+1}}.$$

Вместе с тем отметим, что распределение числа циклических вершин по компонентам графа G_{f^k} уже существенно зависит от величины k . Поэтому в общем случае для произвольных $k \in \mathbb{N}$, $x \in S$ и $l \in \{1, \dots, n\}$ величины

$$\mathbf{P} \{ x \in H_{f^{k-i}}^{(0,l)} \} \quad \text{и} \quad \mathbf{P} \{ x \in H_{f^{k-j}}^{(0,l)} \}, \quad \text{где } i, j \in \{0, 1, \dots, k\}, \quad i \neq j,$$

не совпадают. Это объясняется тем, что при переходе от отображения f к отображению f^k каждый цикл графа G_f длины $m \in \{1, \dots, n\}$ распадается на (m, k) отдельных циклов графа G_{f^k} длины $\frac{m}{(m,k)}$ (см. рис. 1.6)

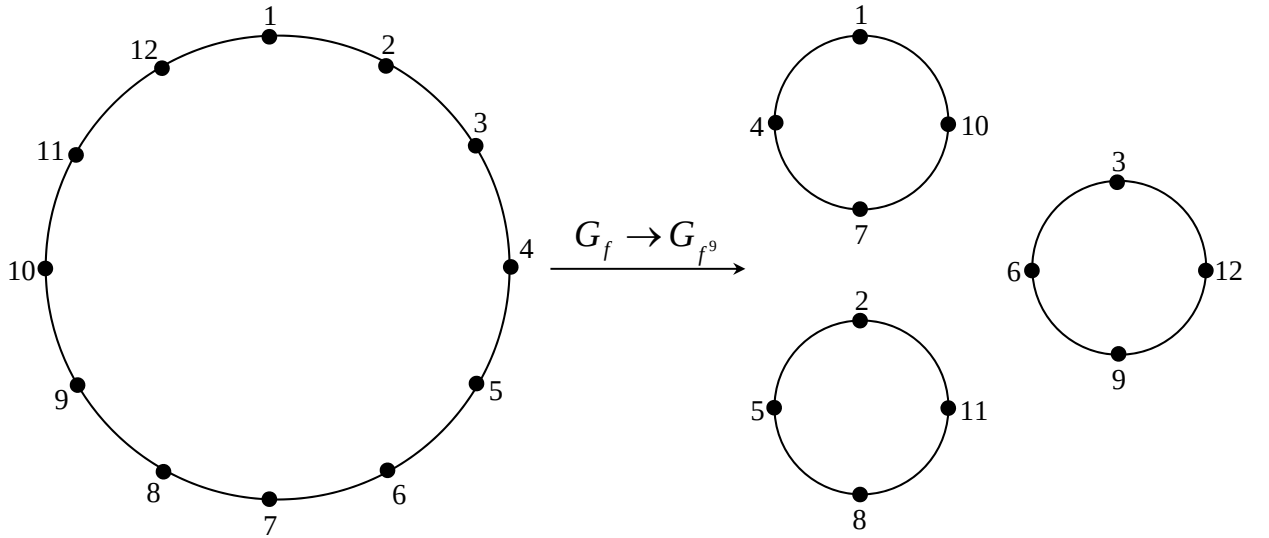


Рис. 1.6: Распад отдельного цикла при переходе от G_f к G_{f^9}

Через $\lambda_{f^k}(l)$ обозначим случайную величину, равную числу вершин в графе G_{f^k} , лежащих на циклах длины $l \in \{1, \dots, n\}$.

Замечание 1.12. Теорема 1.4 позволяет выписать выражения для $\mathbf{E}\lambda_{f^k}(l)$, $\mathbf{E}\lambda_{f^k}$. Действительно, так как

$$\lambda_{f^k}(l) = \sum_{x \in S} I\{x \in C_l(G_{f^k})\}, \quad \lambda_{f^k} = \sum_{x \in S} I\{x \in C(G_{f^k})\},$$

то в силу равноправия всех $x \in S$

$$\mathbf{E}\lambda_{f^k}(l) = \mathbf{E} \sum_{x \in S} I\{x \in C_l(G_{f^k})\} = n\mathbf{P}\{x \in C_l(G_{f^k})\} = \sum_{m \in Q_1^n(k, l)} \frac{(n)_m}{n^m},$$

$$\mathbf{E}\lambda_{f^k} = n\mathbf{P}\{x \in C(G_{f^k})\} = \sum_{l=1}^n \frac{(n)_l}{n^l}.$$

Далее для $k \in \mathbb{N}$ и произвольных фиксированных вершин $x, y \in S$, $x \neq y$, вычислим совместную вероятность их попадания на циклы фиксированных длин в графе G_{f^k} .

Теорема 1.5. [24] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $k \in \mathbb{N}$ и $l_1, l_2 \in \{1, \dots, n\}$, $l_1 + l_2 \leq n(1 + \delta_{l_1, l_2})$, справедливо равенство

$$\begin{aligned} & \mathbf{P}\{x \in C_{l_1}(G_{f^k}), y \in C_{l_2}(G_{f^k})\} = \\ & = \delta_{l_1, l_2} \sum_{m \in Q_1^n(k, l_1)} \frac{(m-1)(n-2)_{m-2}}{n^m} + \sum_{m_1 \in Q_1^n(k, l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k, l_2)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}}, \end{aligned}$$

где $\delta_{l_1, l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2, \end{cases}$ — символ Кронекера, а $Q_1^n(k, l)$ определяется соотношением (1.7).

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

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

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

$$\mathbf{P} \left\{ x, y \in C_l (G_{f^k}) \right\} = \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l (G_{f^k}) \\ I_{x,y} = 1 \end{array} \right\} + \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l (G_{f^k}) \\ I_{x,y} = 0 \end{array} \right\}. \quad (1.43)$$

Вычислим первое слагаемое в правой части (1.43). Зафиксируем вершину $x \in S$. При этом для произвольной фиксированной вершины $y \in S, y \neq x$, существует в точности $m - 1$ вариантов расположения на содержащем x цикле длины $m \in Q_1^n(k, l)$ в графе G_f . Тогда, рассуждая как и в теореме 1.4 (с учетом не одной фиксированной вершины x , а уже двух вершин x, y), получаем цепочку равенств

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l (G_{f^k}) \\ I_{x,y} = 1 \end{array} \right\} &= \\ &= \sum_{m \in Q_2^n(k, l)} \frac{m-1}{n^m} \prod_{i=2}^{m-1} (n-i) = \sum_{m \in Q_1^n(k, l)} \frac{(m-1)(n-2)_{m-2}}{n^m}. \end{aligned} \quad (1.44)$$

Для случая, когда вершины x, y лежат на различных циклах длин $m_1, m_2 \in \{1, \dots, n\}, m_1 + m_2 \leq n$, в графе G_f , имеем

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l (G_{f^k}) \\ I_{x,y} = 0 \end{array} \right\} &= \sum_{m_1 \in Q_1^n(k, l)} \sum_{m_2 \in Q_1^{n-m_1}(k, l)} \frac{1}{n^{m_1+m_2}} \prod_{i=2}^{m_1+m_2-1} (n-i) = \\ &= \sum_{m_1 \in Q_1^n(k, l)} \sum_{m_2 \in Q_1^{n-m_1}(k, l)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}}. \end{aligned} \quad (1.45)$$

Подставив (1.44) и (1.45) в равенство (1.43), получим выражение для искомой вероятности в случае $l_1 = l_2 = l$.

Пусть теперь $l_1 \neq l_2$. В этом случае вершины x, y могут лежать только на разных циклах в графе G_{f^k} , а следовательно, и в графе G_f . Поэтому

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{c} x \in C_{l_1}(G_{f^k}), y \in C_{l_2}(G_{f^k}) \\ l_1 \neq l_2 \end{array} \right\} = \\ = \sum_{m_1 \in Q_1^n(k, l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k, l_2)} \frac{(n-2)_{m_1+m_2-2}}{n^{m_1+m_2}}. \end{aligned} \quad (1.46)$$

Объединяя выражения (1.43) и (1.46) с использованием символа Кронекера, приходим к утверждению теоремы. Теорема доказана. $\square$

Поскольку для произвольного фиксированного $l \in \{1, \dots, n\}$ множества вершин $H_{f^k}^{(t,l)}$ в графе G_{f^k} имеют принципиально различную структуру при $t = 0$ и $t \neq 0$, сформулируем ряд утверждений, описывающих множества $H_{f^k}^{(t,l)}$ для $t \in \{1, \dots, n-1\}$.

Теорема 1.6. [24] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $l \in \{1, \dots, n\}$ и $t \in \{1, \dots, n-l\}$ справедливо равенство

$$\mathbf{P} \left\{ x \in H_{f^k}^{(t,l)} \right\} = \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-tk+s}(k,l)} \frac{(n)_{m+tk-s}}{n^{m+tk-s+1}}, \quad (1.47)$$

где $Q_1^n(k, l)$ определяется соотношением (1.7).

Доказательство. Покажем, что для произвольных $k \in \mathbb{N}$ и $x \in S$ случайная величина $\alpha_{f^k}(x)$ удовлетворяет соотношению

$$\alpha_{f^k}(x) = \left\lfloor \frac{\alpha_f(x) + k - 1}{k} \right\rfloor. \quad (1.48)$$

Для этого докажем эквивалентность (1.48) и (1.2). Пусть $\alpha_{f^k}(x) = s \in \{0, \dots, n-1\}$. Разделим s на k с остатком:

$$s = pk + q, \quad p \geq 0, \quad q \in \{0, 1, \dots, k-1\}.$$

Тогда в случае $q = 0$ выражение (1.48) представляется в следующем виде:

$$s = p + 1 + \left[-\frac{1}{k} \right] = p.$$

При этом правая часть (1.2) также равна p .

В случае же $q \in \{1, \dots, k-1\}$ из (1.48) получаем

$$\alpha_{f^k}(x) = p + 1 + \left[\frac{q-1}{k} \right] = p + 1,$$

и правая часть (1.2) принимает значение $p + \left] \frac{q}{k} \right[= p + 1$, что и доказывает справедливость (1.48).

В соответствии с равенством (1.48) при $l \in \{1, \dots, n\}$ и $t \in \{1, \dots, n-l\}$ событие $\{x \in H_{f^k}^{(t,l)}\}$ может быть выражено через события $\{x \in H_f^{(j,m)}\}$ при подходящих значениях m , где $j \in \overline{(t-1)k+1, tk}$:

$$\begin{aligned} \{x \in H_{f^k}^{(t,l)}\} &= \\ &= \bigcup_{m \in Q_1^{n-tk}(k,l)} \{x \in H_f^{(tk,m)}\} \cup \bigcup_{m \in Q_1^{n-tk+1}(k,l)} \{x \in H_f^{(tk-1,m)}\} \cup \dots \\ &\quad \dots \cup \bigcup_{m \in Q_1^{n-(t-1)k+1}(k,l)} \{x \in H_f^{((t-1)k+1,m)}\} = \\ &= \bigcup_{s=0}^{k-1} \bigcup_{m \in Q_1^{n-tk+s}(k,l)} \{x \in H_f^{(tk-s,m)}\}, \quad (1.49) \end{aligned}$$

где под знаками объединения стоят несовместные события.

Далее, учитывая справедливое для произвольных $v \in \{1, \dots, n\}$ и $u \in \{1, \dots, n-v\}$ равенство

$$\mathbf{P} \{x \in H_f^{(u,v)}\} = \frac{(n)_{u+v}}{n^{u+v+1}}$$

(см., например, [72], формула (3.1) на с. 1047) и переходя в (1.49) к вероятностям событий, получаем искомое утверждение. Теорема доказана. $\square$

Замечание 1.13. В силу равноправия всех $x \in S$ выполняется соотношение $\mathbf{E} \left| H_{f^k}^{(t,l)} \right| = n \mathbf{P} \left\{ x \in H_{f^k}^{(t,l)} \right\}$.

Через $\tilde{F}_k$ обозначим функцию распределения случайной величины $\alpha_{f^k}(x)$ для произвольной фиксированной вершины $x \in S$ (в силу равноправия вершин из S зависимость от x отражать не будем).

Следствие 1.6. [24] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого фиксированного $x \in S$ и любых $k \in \mathbb{N}$, $z \in \{1, \dots, n-1\}$ справедливы равенства

$$\mathbf{P} \left\{ x \in H_{f^k}^{(z)} \right\} = \sum_{l=1}^{n-z} \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-zk+s}(k,l)} \frac{(n)_{m+zk-s}}{n^{m+zk-s+1}},$$

$$\tilde{F}_k(z) = \sum_{l=1}^n \sum_{m \in Q_1^n(k,l)} \frac{(n)_m}{n^{m+1}} + \sum_{u=1}^z \sum_{l=1}^{n-u} \sum_{s=0}^{k-1} \sum_{m \in Q_1^{n-uk+s}(k,l)} \frac{(n)_{m+uk-s}}{n^{m+uk-s+1}},$$

где $Q_1^n(k, l)$ определяется соотношением (1.7).

Доказательство. 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 $l_1 \neq l_2$, а также выражения (1.47) вытекают искомые соотношения для $\mathbf{P} \left\{ x \in H_{f^k}^{(z)} \right\}$ и $\tilde{F}_k(z)$. Следствие доказано. $\square$

Замечание 1.14. Разбиение исходного множества вершин S вида

$$S = \bigcup_{u=1}^n \left[\bigcup_{t=0}^{u-1} H_{f^k}^{(t,u-t)} \right]$$

позволяет классифицировать производные ключи, вырабатываемые с использованием итерационного АМЗИ рассматриваемого типа, по величине $\mathbf{P} \left\{ x \in H_{f^k}^{(t,u-t)} \right\}$ — вероятности их неповторного формирования за u тактов работы алгоритма на основе произвольного фиксированного долговременного ключа, соответствующего вершине $x \in S$, $u \in \{1, \dots, n\}$, $t \in \{0, 1, \dots, u-1\}$.

1.5 Инцидентность вершин одной компоненте связности в графе отображения f^k

В настоящем параграфе изучаются характеристики графа G_{f^k} , описывающие особенности взаимного расположения вершин и в ряде случаев влияющие на теоретическую стойкость итерационных АМЗИ.

В частности, пересечение отрезков апериодичности нескольких фиксированных вершин, соответствующих долговременным ключам, в графе отображения, используемого для моделирования работы итерационного АМЗИ, приводит к повторному использованию производных ключей, а также может существенно ухудшить последствия возможной компрометации ключей.

Так, например, при использовании различных долговременных ключей $x_1, x_2, \dots, x_d \in S$, $d > 1$, для формирования производной ключевой информации на основе АМЗИ, описываемого случайным отображением f^k , в случае $\mathcal{R}_{f^k}(x_i) \cap \mathcal{R}_{f^k}(x_j) \neq \emptyset$, где $1 \leq i < j \leq d$, компрометация хотя бы одного ключа, выработанного на основе долговременного ключа x_i , приводит к компрометации части ключей, сформированных с использованием ключа x_j , в силу гарантированного дублирования ключевой информации, соответствующей циклическим вершинам компоненты $\mathcal{K}_{f^k}(x_i)$. При этом минимальное число скомпрометированных ключей составляет $\beta_{f^k}(x_i)$.

Кроме того, если исходная ключевая система содержит слабые ключи [36] $y_1, y_2, \dots, y_t$, $t \geq 1$, то в целях обеспечения теоретической стойкости использующего их алгоритма защиты информации на указанные отрезки апериодичности накладывается естественное ограничение

$$\{y_1, y_2, \dots, y_t\} \cap \left(\bigcup_{i=1}^d \mathcal{R}_{f^k}(x_i) \right) = \emptyset. \quad (1.50)$$

Замечание 1.15. В качестве $\{y_1, y_2, \dots, y_t\}$, $t \geq 1$, можно рассматривать не только слабые ключи, но и ключи, выработанные итерационным алгоритмом к текущему (анализируемому) моменту времени.

Рассмотрим случай $t = d = 1$. Тогда событие (1.50) принимает вид $\{y \notin \mathcal{R}_{f^k}(x)\}$. Вычислим вероятность этого события для произвольных фиксированных вершин $x, y \in S$, $x \neq y$.

Теорема 1.7. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $k \in \mathbb{N}$, $z \in \{2, \dots, n\}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) = z; y \in \mathcal{R}_{f^k}(x) \} = \\ = (z-1) \left[\sum_{m \in Q_2^n(k, z)} \frac{(n-2)_{m-2}}{n^m} + \sum_{m \in \tilde{Q}_1^{n-1}(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{(n-2)_{r+v-2}}{n^{r+v}} \right], \end{aligned}$$

где $r = m + \left(z - \frac{m}{(m, k)} - 1 \right) k$, а $Q_2^n(k, z)$ и $\tilde{Q}_1^{n-1}(k, z)$ определяются соотношениями (1.7), (1.8).

Доказательство. Зафиксируем произвольную пару вершин $x, y \in S$, $x \neq y$, и для любого $z \in \{2, \dots, n\}$ рассмотрим более широкое событие

$$\{ \tau_{f^k}(x) = z; y \in \mathcal{R}_f(x) \},$$

для наступления которого в случае $x \in C(G_f)$ и $\beta_f(x) = m$, где $m \in \{2, \dots, n\}$, существует в точности $m-1$ вариантов прохождения случайной траектории $\mathcal{R}_f(x)$ через вершину y , а в случае $\alpha_f(x) = t$, где $t \in \{1, 2, \dots, n-m\}$, $m \in \{1, \dots, n-1\}$, существует $m+t-1$ вариантов.

Повторяя рассуждения теоремы 1.1 (с учетом расположения вершины y на $\mathcal{R}_f(x)$) и обозначая $r = m + \left(z - \frac{m}{(m, k)} - 1 \right) k$, по формуле полной вероятности получаем следующую цепочку равенств:

$$\begin{aligned}
\mathbf{P} \{ \tau_{f^k}(x) = z; y \in \mathcal{R}_f(x) \} &= \mathbf{P} \{ x \in C_z(G_{f^k}); y \in C_f(x) \} + \\
&+ \mathbf{P} \{ \tau_{f^k}(x) = z; x \notin C(G_f); y \in \mathcal{R}_f(x) \} = \sum_{m \in Q_2^n(k, z)} \frac{m-1}{n^2} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n} \right) + \\
&+ \sum_{m \in \tilde{Q}_1^{n-1}(k, z)} \sum_{t = \left(z - \frac{m}{(m, k)} - 1 \right)k + 1}^{\min\left(\left(z - \frac{m}{(m, k)}\right)k, n-m\right)} \frac{m+t-1}{n^2} \prod_{i=2}^{m+t-1} \left(1 - \frac{i}{n} \right) = \\
&= \sum_{m \in Q_2^n(k, z)} \frac{(m-1)(n-2)_{m-2}}{n^m} + \sum_{m \in \tilde{Q}_1^{n-1}(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{(r+v-1)(n-2)_{r+v-2}}{n^{r+v}}.
\end{aligned} \tag{1.51}$$

Далее следует учесть, что доли вершин y , лежащих на соответствующих траекториях длины m в графе G_f (для первой группы слагаемых в (1.51)) и длины $r+v$ (для второй группы слагаемых), при которых $y \in \mathcal{R}_{f^k}(x)$, составляют $\frac{z-1}{m-1}$ и $\frac{z-1}{r+v-1}$ соответственно. Таким образом, из (1.51) следует

$$\begin{aligned}
\mathbf{P} \{ \tau_{f^k}(x) = z; y \in \mathcal{R}_{f^k}(x) \cap \mathcal{R}_f(x) \} &= \\
&= \sum_{m \in Q_2^n(k, z)} \frac{z-1}{m-1} \cdot \frac{(m-1)(n-2)_{m-2}}{n^m} + \\
&+ \sum_{m \in \tilde{Q}_1^{n-1}(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{z-1}{r+v-1} \cdot \frac{(r+v-1)(n-2)_{r+v-2}}{n^{r+v}} = \\
&= (z-1) \left[\sum_{m \in Q_2^n(k, z)} \frac{(n-2)_{m-2}}{n^m} + \sum_{m \in \tilde{Q}_1^{n-1}(k, z)} \sum_{v=1}^{\min(k, n-r)} \frac{(n-2)_{r+v-2}}{n^{r+v}} \right],
\end{aligned}$$

откуда с использованием соотношения

$$\mathbf{P} \{ \tau_{f^k}(x) = z; y \in \mathcal{R}_{f^k}(x) \} = \mathbf{P} \{ \tau_{f^k}(x) = z; y \in \mathcal{R}_{f^k}(x) \cap \mathcal{R}_f(x) \}.$$

приходим к утверждению теоремы. Теорема доказана. $\square$

Теорема 1.8. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $k \in \mathbb{N}$, $z \in \{2, \dots, n\}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) \leq z; y \in \mathcal{R}_{f^k}(x) \} = \\ = \sum_{m \in \tilde{Q}_1^n(k, z+1)} \sum_{t=m}^{\min(r, n)} \frac{\left(\left\lfloor \frac{t-m}{k} \right\rfloor + \frac{m}{(m, k)} - 1 \right) (n-2)_{t-2}}{n^t}, \end{aligned} \quad (1.52)$$

где $r = m + \left(z - \frac{m}{(m, k)} \right) k$, а $\tilde{Q}_1^n(k, z)$ определяется соотношением (1.8).

Доказательство. Для произвольной фиксированной пары вершин $x, y \in S$, $x \neq y$, с учетом (1.16) и (1.44) находим, что

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) \leq z; y \in \mathcal{R}_f(x) \} &= \mathbf{P} \{ \tau_{f^k}(x) \leq z; x \in C(G_f); y \in C_f(x) \} + \\ &+ \mathbf{P} \{ \tau_{f^k}(x) \leq z; x \notin C(G_f); y \in \mathcal{R}_f(x) \} = \sum_{m \in \tilde{Q}_2^n(k, z+1)} \frac{m-1}{n^2} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n} \right) + \\ &+ \sum_{m \in \tilde{Q}_1^{n-1}(k, z+1)} \sum_{t=1}^{\min(r, n)-m} \frac{t+m-1}{n^2} \prod_{i=2}^{t+m-1} \left(1 - \frac{i}{n} \right) = \\ &= \sum_{m \in \tilde{Q}_2^n(k, z+1)} \frac{(m-1)(n-2)_{m-2}}{n^m} + \\ &+ \sum_{m \in \tilde{Q}_1^{n-1}(k, z+1)} \sum_{t=1}^{\min(r, n)-m} \frac{(t+m-1)(n-2)_{t+m-2}}{n^{t+m}}. \end{aligned} \quad (1.53)$$

При этом из равенства (1.6) следует, что при фиксированном $m \in \tilde{Q}_2^n(k, z+1)$ (для первой группы слагаемых в (1.53)), а также при такой фиксированной паре (m, t) (для второй группы слагаемых), что $m \in \tilde{Q}_1^{n-1}(k, z+1)$ и $t \in \{1, \dots, \min(r, n) - m\}$, доля вершин $y \in \mathcal{R}_f(x)$, для которых $y \in \mathcal{R}_{f^k}(x)$, составляет $\frac{\frac{m}{(m, k)} - 1}{m-1}$ и $\frac{\left\lfloor \frac{t}{k} \right\rfloor + \frac{m}{(m, k)} - 1}{t+m-1}$ соответственно. Таким

образом, из (1.53) вытекает выражение

$$\begin{aligned} \mathbf{P} \{ \tau_{f^k}(x) \leq z; y \in \mathcal{R}_{f^k}(x) \} &= \sum_{m \in \tilde{Q}_2^n(k, z+1)} \frac{\left(\frac{m}{(m, k)} - 1 \right) (n-2)_{m-2}}{n^m} + \\ &+ \sum_{m \in \tilde{Q}_1^{n-1}(k, z+1)} \sum_{t=1}^{\min(r, n)-m} \frac{\left(\left\lfloor \frac{t}{k} \right\rfloor + \frac{m}{(m, k)} - 1 \right) (n-2)_{t+m-2}}{n^{t+m}}, \end{aligned}$$

из которого путем объединения первой и второй групп слагаемых получаем искомую формулу. Теорема доказана. $\square$

Замечание 1.16. Выражения для $\mathbf{P} \{ \tau_{f^k}(x) = z \}$ и $\mathbf{P} \{ \tau_{f^k}(x) \leq z \}$, полученные в § 1.2 (формулы (1.9) и (1.18) соответственно), а также результаты теорем 1.7, 1.8 позволяют выписать формулы для величин

$$\mathbf{P} \{ \tau_{f^k}(x) = z; y \notin \mathcal{R}_{f^k}(x) \}, \quad \mathbf{P} \{ \tau_{f^k}(x) \leq z; y \notin \mathcal{R}_{f^k}(x) \}.$$

Следствие 1.7. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \{ y \notin \mathcal{R}_{f^k}(x) \} = 1 - \sum_{m=1}^n \sum_{t=m}^n \frac{\left(\left\lfloor \frac{t-m}{k} \right\rfloor + \frac{m}{(m, k)} - 1 \right) (n-2)_{t-2}}{n^t}.$$

Доказательство. Искомая вероятность может быть представлена в следующем виде:

$$\begin{aligned} \mathbf{P} \{ y \notin \mathcal{R}_f(x) \} &= \\ &= 1 - \mathbf{P} \{ y \in \mathcal{R}_f(x) \} = 1 - \mathbf{P} \{ \tau_f(x) \leq n; y \in \mathcal{R}_f(x) \}. \end{aligned} \quad (1.54)$$

Поэтому для вывода формулы достаточно подставить выражение (1.52) в (1.54) и учесть, что в случае $z = n$ предел и множество суммирования слагаемых в (1.52) принимают вид

$$\min(r, n) = \min\left(\left(n - \frac{m}{(m, k)}\right)k, n - m\right) + m = n,$$

$$\tilde{Q}_1^n(k, n+1) = \{1, \dots, n\}.$$

Следствие доказано. $\square$

Перейдем к оценке вероятности попадания вершин из S в одну компоненту связности графа G_{f^k} , $k \in \mathbb{N}$. Как было указано во введении, в случае $k = 1$ для произвольных фиксированных различных вершин $x_1, x_2, \dots, x_d \in S$, $d > 1$, имеет место асимптотическое равенство при $n \rightarrow \infty$

$$\mathbf{P}\{x_1, x_2, \dots, x_d \in \mathcal{K}_f(x_1)\} = \frac{(2d-2)!!}{(2d-1)!!} + o(1). \quad (1.55)$$

Следует отметить, что $\mathbf{P}\{x_1, x_2, \dots, x_d \in \mathcal{K}_{f^k}(x_1)\}$ также позволяет оценить возможность компрометации производных ключей, вырабатываемых с использованием АМЗИ, описываемого случайным отображением $f^k: S \rightarrow S$, поскольку событие $\{x_1, x_2, \dots, x_d \in \mathcal{K}_{f^k}(x_1)\}$ совпадает с упомянутым в начале настоящего параграфа событием $\left\{\bigcap_{i=1}^d \mathcal{R}_{f^k}(x_i) \neq \emptyset\right\}$.

Пусть далее $d = 2$. Для произвольной пары вершин $x, y \in S$, $x \neq y$, вычислим $\mathbf{P}\{y \in \mathcal{K}_{f^k}(x)\}$.

Для любых $m \in \mathbb{N}$ и $s, t \in \mathbb{N} \cup \{0\}$ обозначим

$$\Delta_m^{s,t} = \begin{cases} 1, & s_{\bmod m} \geq t_{\bmod m} > 0, \\ 0 & \text{в противном случае,} \end{cases} \quad (1.56)$$

здесь и далее используется обозначение $s_{\bmod m} = s - m\left[\frac{s}{m}\right]$ для наименьшего неотрицательного вычета s по модулю m .

Теорема 1.9. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} = \sum_{m=1}^n \sum_{v=m}^n \sum_{s=0}^{n-v} \frac{\left(\left\lfloor \frac{v}{(m,k)} \right\rfloor - \omega_{m,v,s} \right) (n-2)_{v+s-2}}{n^{v+s}}, \quad (1.57)$$

$$\text{где } \omega_{m,v,s} = \begin{cases} 1, & \text{если } s = 0, \\ \Delta_{(m,k)}^{s,v} & \text{в противном случае.} \end{cases}$$

Доказательство. Зафиксируем произвольную пару вершин $x, y \in S$, $x \neq y$. Тогда по формуле полной вероятности

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} &= \\ &= \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \in C_f(x)\} + \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \notin C_f(x)\}. \end{aligned} \quad (1.58)$$

Вычислим первое слагаемое в (1.58). Зафиксируем длину $m \in \{1, \dots, n\}$ цикла $C_f(x)$. Заметим, что существует в точности $\frac{m}{(m,k)} - 1$ вариантов расположения вершины $y \in S$, $y \neq x$, на цикле $C_f(x)$, при которых наступает событие $\{y \in \mathcal{K}_{f^k}(x)\}$. Вероятность каждого такого варианта составляет $\frac{1}{n^2} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n}\right)$.

Если же $\alpha_f(y) = s \in \{1, \dots, n-m\}$, то для каждого такого фиксированного s существует ровно $\frac{m}{(m,k)}$ вариантов для вхождения подхода $\mathcal{P}_f(y)$ в цикл $C_f(x)$, при которых также наступает событие $\{y \in \mathcal{K}_{f^k}(x)\}$, а вероятность каждого из них равна $\frac{1}{n^2} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right)$. Таким образом,

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \in C_f(x)\} &= \\ &= \sum_{m=2}^n \frac{\frac{m}{(m,k)} - 1}{n^2} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n}\right) + \sum_{m=1}^n \sum_{s=1}^{n-m} \frac{\frac{m}{(m,k)}}{n^2} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right). \end{aligned} \quad (1.59)$$

Рассмотрим второе слагаемое в (1.58). В этом случае, помимо значения m , зафиксируем длину $t > 0$ подхода вершины x . Если $y \in \mathcal{R}_f(x)$, то существует $\left\lfloor \frac{t+m}{(m,k)} \right\rfloor - 1$ вариантов (исключается вершина x) расположения $y \in S$,

$y \neq x$, на отрезке аperiodичности $\mathcal{R}_f(x)$, при которых наступает событие $\{y \in \mathcal{K}_{f^k}(x)\}$. Вероятность каждого такого варианта равна $\frac{1}{n^2} \prod_{i=2}^{m+t-1} \left(1 - \frac{i}{n}\right)$.

Пусть теперь $s = \min \{w \in \mathbb{N} \cup \{0\} : f^w(y) \in \mathcal{R}_f(x)\} > 0$. Тогда для всех t , кратных (m, k) , существует ровно $\left\lfloor \frac{t+m}{(m,k)} \right\rfloor$ вариантов для вхождения траектории, начинающейся в вершине y , в отрезок аperiodичности $\mathcal{R}_f(x)$, при которых наступает событие $\{y \in \mathcal{K}_{f^k}(x)\}$. Если же $(m, k) \nmid t$, то для $s_{\text{mod}}(m, k) < t_{\text{mod}}(m, k)$ число таких вариантов составляет $\left\lfloor \frac{t+m}{(m,k)} \right\rfloor$, а для $s_{\text{mod}}(m, k) \geq t_{\text{mod}}(m, k)$ — соответственно $\left\lfloor \frac{t+m}{(m,k)} \right\rfloor - 1$. Вероятность каждого такого вхождения равна $\frac{1}{n^2} \prod_{i=2}^{m+s+t-1} \left(1 - \frac{i}{n}\right)$. Следовательно,

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \notin C_f(x)\} &= \sum_{m=1}^n \sum_{t=1}^{n-m} \frac{\left\lfloor \frac{t+m}{(m,k)} \right\rfloor - 1}{n^2} \prod_{i=2}^{m+t-1} \left(1 - \frac{i}{n}\right) + \\ &+ \sum_{m=1}^n \sum_{t=1}^{n-m} \sum_{s=1}^{n-m-t} \frac{\left\lfloor \frac{t+m}{(m,k)} \right\rfloor - \Delta_{(m,k)}^{s,t}}{n^2} \prod_{i=2}^{m+t+s-1} \left(1 - \frac{i}{n}\right). \quad (1.60) \end{aligned}$$

Подставив (1.59) и (1.60) в (1.58) и преобразовав полученное выражение с использованием замены переменной $t = v - m$, с учетом равенства $\Delta_{(m,k)}^{s,v} = \Delta_{(m,k)}^{s,t}$ приходим к искомому результату. Теорема доказана. $\square$

Так, в частности, из (1.57) при $k = 1$ следует выражение для равновероятного случайного отображения $f: S \rightarrow S$:

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_f(x)\} &= \\ &= \frac{1}{n(n-1)} \left(\sum_{m=1}^n \sum_{v=m-1}^{n-1} v \frac{(n)_{v+1}}{n^{v+1}} + \sum_{m=1}^n \sum_{v=m}^n \sum_{s=1}^{n-v} v \frac{(n)_{v+s}}{n^{v+s}} \right) = \\ &= \sum_{z=1}^n \frac{z(z-1)}{n(n-1)} \frac{(n)_z}{n^z} + \sum_{z=1}^n \sum_{u=1}^{n-z} \frac{z^2}{n(n-1)} \frac{(n)_{z+u}}{n^{z+u}}. \quad (1.61) \end{aligned}$$

Замечание 1.17. Теорема 1.9 позволяет вычислить среднюю мощность компоненты связности произвольной фиксированной вершины $x \in S$ в графе

G_{f^k} . Действительно, из соотношения

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} &= \sum_{r=2}^n \mathbf{P} \{|\mathcal{K}_{f^k}(x)| = r\} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x) \mid |\mathcal{K}_{f^k}(x)| = r\} = \\ &= \sum_{r=2}^n \frac{r-1}{n-1} \mathbf{P} \{|\mathcal{K}_{f^k}(x)| = r\} = \frac{1}{n-1} \mathbf{E} (|\mathcal{K}_{f^k}(x)| - 1) \end{aligned}$$

следует итоговое равенство

$$\mathbf{E} |\mathcal{K}_{f^k}(x)| = (n-1) \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} + 1.$$

Замечание 1.18. В силу равноправия вершин из S среднее число пар $(x, y) \in S^2$, $x \neq y$, сохраняющих инцидентность одной компоненте связности при переходе от графа G_f к графу G_{f^k} , определяется равенством $C_n^2 \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\}$.

Следствие 1.8. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо двустороннее неравенство

$$\frac{1}{3k} < \lim_{n \rightarrow \infty} \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} \leq \frac{2}{3}.$$

Доказательство. Из соотношения (1.59) и очевидного неравенства $\frac{m}{2k} < \frac{m}{(m,k)}$, справедливого для произвольных $m \in \{1, \dots, n\}$ и $k \in \mathbb{N}$, получаем

$$\frac{1}{2k} \mathbf{P} \{y \in \mathcal{K}_f(x), x \in C_f(x)\} < \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \in C_f(x)\}. \quad (1.62)$$

В свою очередь, из определения величины $\Delta_{(m,k)}^{s,t}$ и соотношения $\frac{t+m}{(m,k)} \geq 1$, справедливого для произвольных $m \in \{1, \dots, n\}$, $t \in \{0, \dots, n-m\}$, $s \in \{0, \dots, n-m-t\}$ и $k \in \mathbb{N}$, следует неравенство

$$\frac{t+m}{2k} < \left[\frac{t+m}{(m,k)} \right] - \Delta_{(m,k)}^{s,t},$$

из которого получаем

$$\frac{1}{2k} \mathbf{P} \{y \in \mathcal{K}_f(x), x \notin C_f(x)\} < \mathbf{P} \{y \in \mathcal{K}_{f^k}(x), x \notin C_f(x)\},$$

и следовательно, с учетом (1.62) для произвольного $k \in \mathbb{N}$ можем записать двустороннюю оценку

$$\frac{1}{2k} \mathbf{P} \{y \in \mathcal{K}_f(x)\} < \mathbf{P} \{y \in \mathcal{K}_{f^k}(x)\} \leq \mathbf{P} \{y \in \mathcal{K}_f(x)\}.$$

Таким образом, переходя к пределу в полученном неравенстве при $n \rightarrow \infty$, с использованием формулы $\lim_{n \rightarrow \infty} \mathbf{P} \{y \in \mathcal{K}_f(x)\} = \frac{2}{3}$ (частный случай (1.55) при $d = 2$) получаем искомый результат. Следствие доказано. $\square$

Отметим еще одну особенность формирования множества производных ключей на основе АМЗИ рассматриваемого типа. Использование не всех последовательно вырабатываемых ключей, а лишь отобранных с некоторым фиксированным периодом $k > 1$, позволяет уменьшить вероятность дублирования ключевой информации (сформированной на основе различных долговременных ключей). Указанный эффект обусловлен возможным увеличением числа компонент связности при переходе от графа G_f к графу G_{f^k} за счет распада некоторых компонент графа G_f . Исключение составляет случай, когда граф G_{f^k} уже является связным, и, как следствие, любой набор вершин из S сохраняет инцидентность единственной компоненте.

Обозначим через η_f случайную величину, равную числу компонент связности в графе G_f .

Теорема 1.10. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \{\eta_{f^k} = 1\} = \sum_{j \in D_k} \frac{(n)_j}{n^{j+1}},$$

где $D_k = \{j \in \{1, \dots, n\} : (k, j) = 1\}$.

Доказательство. По формуле полной вероятности

$$\mathbf{P} \{ \eta_{f^k} = 1 \} = \sum_{j=1}^n \mathbf{P} \{ \eta_{f^k} = 1 \mid \lambda_f = j \} \mathbf{P} \{ \lambda_f = j \}. \quad (1.63)$$

Рассмотрим выражение, стоящее под знаком суммирования в (1.63). При фиксированном $j \in \{1, \dots, n\}$ величину $\mathbf{P} \{ \eta_{f^k} = 1 \mid \lambda_f = j \}$ можно интерпретировать как вероятность того, что k -кратная итерация равновероятной случайной подстановки $\pi \in S_j$ содержит ровно 1 цикл. При этом выполняется равенство

$$\mathbf{P} \{ \eta_f = 1 \mid \lambda_f = j \} = \frac{1}{j},$$

справедливое для любого $j \in \{1, \dots, n\}$ (см. [84], с. 7). Далее учитывая, что для произвольных $j \in \{1, \dots, n\}$ и $k \in \mathbb{N}$ таких, что $(k, j) = 1$,

$$\mathbf{P} \{ \eta_{f^k} = 1 \mid \lambda_f = j \} = \mathbf{P} \{ \eta_f = 1 \mid \lambda_f = j \},$$

можем записать

$$\mathbf{P} \{ \eta_{f^k} = 1 \mid \lambda_f = j \} = \begin{cases} \frac{1}{j}, & \text{если } (k, j) = 1, \\ 0 & \text{в противном случае.} \end{cases}$$

В итоге, подставив (1.42) в (1.63), получим искомый результат. Теорема доказана. $\square$

Следствие 1.9. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любого $k \in \mathbb{N}$ справедливы следующие оценки:

$$\frac{1}{n} \sum_{j \in D_k} e^{-\left(1 + \frac{j}{n}\right) \frac{j(j-1)}{2n}} \leq \mathbf{P} \{ \eta_{f^k} = 1 \} \leq \frac{1}{n} \sum_{j \in D_k} e^{-\frac{j(j-1)}{2n}},$$

Доказательство. Искомое неравенство вытекает из (1.11). Следствие доказано. $\square$

1.6 Прообразы вершин и коллизии в графе отображения f^k

Неотъемлемой составляющей анализа хеш-функций, а также АМЗИ, построенных на их основе, является исследование вопросов, связанных с поиском коллизий и описанием множества прообразов произвольного элемента, сформированного при действии соответствующего отображения [34]. Указанная проблематика тесно связана, в том числе с вопросами оптимизации методов балансировки времени-памяти-данных [35].

Через $(f^k)^{-1}(x)$ обозначим множество непосредственных прообразов произвольной вершины $x \in S$ в графе G_{f^k} , $k \geq 1$.

Отметим, что для любого $k \in \mathbb{N}$, в случае $y = x$, выполняется равенство событий

$$\left\{x \in (f^k)^{-1}(x)\right\} = \left\{x \in C_1(G_{f^k})\right\},$$

откуда с учетом (1.39)

$$\mathbf{P}\left\{x \in (f^k)^{-1}(x)\right\} = \sum_{m \in Q_1^n(k,1)} \frac{(n)_m}{n^{m+1}}.$$

В частности, для простого $k \in \mathbb{N}$ получаем выражение

$$\mathbf{P}\left\{x \in (f^k)^{-1}(x)\right\} = \frac{1}{n} \left(1 + \frac{(n)_k}{n^k}\right),$$

вырождающееся при $k > n$ в равенство $\mathbf{P}\left\{x \in (f^k)^{-1}(x)\right\} = \frac{1}{n}$.

В свою очередь, для случая $y \neq x$ имеет место следующий результат.

Теорема 1.11. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и

любого $k \in \mathbb{N}$ справедливо равенство

$$\mathbf{P} \left\{ y \in (f^k)^{-1}(x) \right\} = \sum_{m \in \overline{Q}_2^n(k,1)} \frac{(n-2)_{m-2}}{n^m} + \sum_{t=1}^{n-1} \sum_{m=t+1}^n \frac{(n-2)_{m-2}}{n^m},$$

где $\overline{Q}_2^n(k,1) = \{2, \dots, n\} \setminus Q_2^n(k,1)$, а $Q_2^n(k,1)$ определяется соотношением (1.7).

Доказательство. Для произвольных фиксированных вершин $x, y \in S$, $x \neq y$, по формуле полной вероятности имеем

$$\begin{aligned} \mathbf{P} \left\{ y \in (f^k)^{-1}(x) \right\} &= \\ &= \mathbf{P} \left\{ f^k(y) = x, x \in C_f(x) \right\} + \mathbf{P} \left\{ f^k(y) = x, x \notin C_f(x) \right\}. \end{aligned} \quad (1.64)$$

Рассмотрим первое слагаемое в (1.64). На цикле $C_f(x)$ с фиксированной длиной $m \in \{2, \dots, n\}$ в случае $m \nmid k$ существует единственный вариант расположения вершины $y \in S$, $y \neq x$, при котором наступает событие $\left\{ y \in (f^k)^{-1}(x) \right\}$, и его вероятность составляет $\frac{1}{n^2} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n}\right)$. В случае $m \mid k$ таких вариантов не существует.

Если же $\alpha_f(y) = s \in \{1, \dots, k\}$, то для любого $\beta_f(x) = m \in \{1, \dots, n-s\}$ существует единственный вариант вхождения траектории, начинающейся в вершине y , в цикл $C_f(x)$, при котором наступает событие $\left\{ y \in (f^k)^{-1}(x) \right\}$, и его вероятность равна $\frac{1}{n^2} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right)$.

Объединив указанные случаи, приходим к выражению для первого слагаемого в (1.64)

$$\begin{aligned} \mathbf{P} \left\{ f^k(y) = x, x \in C_f(x) \right\} &= \\ &= \frac{1}{n^2} \sum_{m \in \overline{Q}_2^n(k,1)} \prod_{i=2}^{m-1} \left(1 - \frac{i}{n}\right) + \frac{1}{n^2} \sum_{s=1}^k \sum_{m=1}^{n-s} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right), \end{aligned} \quad (1.65)$$

где $\overline{Q}_2^n(k,1) = \{2, \dots, n\} \setminus Q_2^n(k,1)$.

Перейдем к вычислению второго слагаемого в (1.64). Запишем равенство

$$\{f^k(y) = x, x \notin C_f(x)\} = \bigcup_{t=1}^{n-k-1} \bigcup_{m=1}^{n-k-t} \{\alpha_f(x) = t, \beta_f(x) = m, f^k(y) = x\},$$

где под знаками объединения стоят несовместные события, и при фиксированных t, m вероятность соответствующего события равна $\frac{1}{n^2} \prod_{i=2}^{t+m+k-1} (1 - \frac{i}{n})$. Тогда, переходя к вероятностям, получаем

$$\begin{aligned} \mathbf{P} \{f^k(y) = x, x \notin C_f(x)\} &= \\ &= \frac{1}{n^2} \sum_{t=1}^{n-k-1} \sum_{m=1}^{n-k-t} \prod_{i=2}^{t+m+k-1} \left(1 - \frac{i}{n}\right) = \frac{1}{n^2} \sum_{t=k+1}^{n-1} \sum_{m=1}^{n-t} \prod_{i=2}^{t+m-1} \left(1 - \frac{i}{n}\right). \end{aligned} \quad (1.66)$$

В итоге, подставив (1.65) и (1.66) в (1.64), приходим к искомому выражению. Теорема доказана. $\square$

Замечание 1.19. В силу равноправия вершин из S для произвольной фиксированной вершины $x \in S$ справедливо

$$\begin{aligned} \mathbf{E} \left| (f^k)^{-1}(x) \right| &= \mathbf{E} \sum_{y \in S} I \{y \in (f^k)^{-1}(x)\} = \\ &= (n-1) \mathbf{P} \{y \in (f^k)^{-1}(x)\} + \mathbf{P} \{x \in (f^k)^{-1}(x)\}. \end{aligned}$$

Определение 1.9. Коллизией в графе отображения G_f называется произвольная пара вершин $x, y \in S$, $x \neq y$, для которых $f(x) = f(y)$.

Теорема 1.12. [26] Пусть случайное отображение $f: S \rightarrow S$ имеет распределение (1.1) на Ω . Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $k \in \mathbb{N}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{f^k(x) = f^k(y)\} &= \sum_{t=1}^k \sum_{s=0}^{n-1} \sum_{m=t+1}^{n-s} \frac{(1 + \delta_{s,0})(n-2)_{m+s-2}}{n^{m+s}} + \\ &\quad + \sum_{t=1}^k \sum_{m=t+1}^n \sum_{i=0}^{t-1} \sum_{j=\delta_{i,0}}^{\left\lfloor \frac{k-t}{m-t} \right\rfloor} \frac{(n-2)_{m+i+jm-2}}{n^{m+i+jm}}, \end{aligned}$$

$$\text{где } \delta_{i,j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases} \quad - \text{ символ Кронекера.}$$

Доказательство. Зафиксируем произвольные $x, y \in S$, $x \neq y$. По формуле полной вероятности

$$\begin{aligned} \mathbf{P} \{f^k(x) = f^k(y)\} &= \mathbf{P} \{f^k(x) = f^k(y), x \in C_f(x)\} + \\ &+ \mathbf{P} \{f^k(x) = f^k(y), x \notin C_f(x)\}. \end{aligned} \quad (1.67)$$

Рассмотрим первое слагаемое в (1.67). Заметим, что в случае $x \in C_f(x)$ событие $\{f^k(x) = f^k(y)\}$ может наступить только при $\alpha_f(y) = s \in \{1, \dots, k\}$. При этом для любого $\beta_f(x) = m \in \{1, \dots, n - s\}$ существует единственный вариант вхождения траектории, начинающейся в вершине y , в цикл $C_f(x)$, и его вероятность составляет $\frac{1}{n^2} \prod_{i=2}^{m+s-1} (1 - \frac{i}{n})$. Таким образом,

$$\mathbf{P} \{f^k(x) = f^k(y), x \in C_f(x)\} = \frac{1}{n^2} \sum_{s=1}^k \sum_{m=1}^{n-s} \prod_{i=2}^{m+s-1} \left(1 - \frac{i}{n}\right). \quad (1.68)$$

Вычислим второе слагаемое в (1.67). Запишем равенство событий

$$\begin{aligned} \{f^k(x) = f^k(y), x \notin C_f(x)\} &= \\ &= \{f^k(x) = f^k(y), \alpha_f(x) > k\} \cup \{f^k(x) = f^k(y), 1 \leq \alpha_f(x) \leq k\} \end{aligned}$$

и рассмотрим отдельно события, стоящие в его правой части.

Пусть $\alpha_f(x) = t \in \{k+1, \dots, n-1\}$. В этом случае имеем $s = \min \{w \in \mathbb{N} \cup \{0\} : f^w(y) \in \mathcal{R}_f(x)\} \in \{1, \dots, k\}$. При этом для произвольного $\beta_f(x) = m \in \{1, \dots, n - s - t\}$ существует единственный вариант вхождения траектории, начинающейся в вершине y , в отрезок апериодичности $\mathcal{R}_f(x)$, при котором наступает событие $\{f^k(x) = f^k(y)\}$, и его вероятность составляет $\frac{1}{n^2} \prod_{i=2}^{m+s+t-1} (1 - \frac{i}{n})$.

Пусть теперь $\alpha_f(x) = t \in \{1, \dots, k\}$. Тогда для произвольного фиксированного $s \in \{0, \dots, k\}$ существует единственный вариант вхождения траектории, начинающейся в вершине y , в цикл $C_f(x)$ длины m , при котором выполняется равенство $f^k(x) = f^k(y)$. Вероятность каждого такого вхождения также равна $\frac{1}{n^2} \prod_{i=2}^{m+s+t-1} \left(1 - \frac{i}{n}\right)$.

При этом же условии определим множество M вариантов расположения вершины y , при которых начинающаяся в ней траектория входит в подход $\mathcal{P}_f(x) = x, f(x), \dots, f^{t-1}(x)$, и выполняется равенство $f^k(x) = f^k(y)$. Указанное множество определяют две группы вершин $y \in S \setminus \{x\}$:

- вершины y , для которых выполняются равенства $\alpha_f(y) = t$ и $\mathcal{P}_f(y) = y, \dots, f^{i-1}(y), f^i(x), \dots, f^{t-1}(x)$, $i = 1, \dots, t-1$, а также вершины $z \in S \setminus \{x, y\}$ такие, что $f^{jm}(z) = y$, $j = 1, \dots, \left[\frac{k-t}{m}\right]$.
- вершины y , для которых $\mathcal{P}_f(y)$ полностью содержит $\mathcal{P}_f(x)$ и $f^{jm}(y) = x$, $j = 1, \dots, \left[\frac{k-t}{m}\right]$.

Таким образом, указанное множество M имеет вид

$$M = \left\{ y \in S \setminus \{x\} : f^{i+jm}(y) = f^i(x), i = 0, \dots, t-1, j = \delta_{i,0}, \dots, \left[\frac{k-t}{m}\right] \right\},$$

а вероятность каждого варианта расположения y равна $\frac{1}{n^2} \prod_{i=2}^{m+t+i+jm-1} \left(1 - \frac{i}{n}\right)$.

Следовательно,

$$\begin{aligned} \mathbf{P} \{f^k(x) = f^k(y), x \notin C_f(x)\} &= \frac{1}{n^2} \sum_{t=k+1}^{n-1} \sum_{s=1}^k \sum_{m=1}^{n-t-s} \prod_{i=2}^{m+t+s-1} \left(1 - \frac{i}{n}\right) + \\ &+ \frac{1}{n^2} \sum_{t=1}^k \sum_{s=0}^k \sum_{m=1}^{n-t-s} \prod_{i=2}^{m+t+s-1} \left(1 - \frac{i}{n}\right) + \\ &+ \frac{1}{n^2} \sum_{t=1}^k \sum_{m=1}^{n-t} \sum_{i=0}^{t-1} \sum_{j=\delta_{i,0}}^{\left[\frac{k-t}{m}\right]} \prod_{i=2}^{m+t+i+jm-1} \left(1 - \frac{i}{n}\right). \quad (1.69) \end{aligned}$$

В результате, подставив выражения (1.68) и (1.69) в (1.67) и проведя элементарные преобразования, получим искомую формулу. Теорема доказана. $\square$

Замечание 1.20. В силу равноправия вершин из S среднее число коллизий в графе G_{f^k} определяется величиной $C_n^2 \mathbf{P} \{f^k(x) = f^k(y)\}$.

1.7 Выводы

В главе 1 диссертации получены точные выражения, а также неравенства для распределения, математического ожидания длины отрезка аperiodичности и числа вершин с отрезком аperiodичности заданной длины в графе k -кратной итерации равновероятного случайного отображения конечного множества в себя. Найдены математические ожидания мощности образа исходного множества вершин при действии случайного отображения f^k , а также мощности множества вершин, не имеющих прообразов. Получены явные формулы для вероятностей инцидентности указанным множествам фиксированной вершины из S . Описаны особенности формирования циклов и компонент при переходе от исходного графа G_f к графу G_{f^k} , $k > 1$, влияющие на теоретическую стойкость соответствующих итерационных АМЗИ. Вычислены вероятности появления коллизии, попадания произвольной фиксированной вершины в множество прообразов другой произвольной фиксированной вершины, а также инцидентности любых двух фиксированных вершин одной компоненте связности в графе G_{f^k} .

Приведенные результаты главы 1 диссертации могут быть использованы при синтезе и анализе современных итерационных АМЗИ типа «CryptoPro Key Meshing» (например, функций сжатия, хеш-функций, регистров сдвига [31, 32], алгоритмов выработки производных ключей и генерации псевдо-

случайных последовательностей [30]), а также обосновании выбора используемых в них параметров, существенно влияющих на теоретическую стойкость АМЗИ в целом.

Формулы для распределений отдельных случайных величин, заданных на множестве вершин графа G_{f^k} и описанных в настоящей главе, в ряде случаев могут использоваться при построении критериев проверки статистических гипотез о видах распределений последовательностей, формируемых с использованием итерационных АМЗИ.

2 Композиция независимых равновероятных случайных отображений

Настоящая глава посвящена исследованию вероятностных характеристик и свойств графа композиции независимых равновероятных случайных отображений конечного множества в себя — объекта, находящего свое применение при моделировании и обосновании теоретической стойкости итерационных АМЗИ, использующих либо различные преобразования, либо источники случайности, определяющие реализуемое преобразование в каждый такт работы.

2.1 Теоретико-вероятностная модель

Итерационные алгоритмы «CryptoPro Key Meshing» [21, 58] для повышения теоретической стойкости (например, для исключения корреляции между тактами работы) могут быть модифицированы за счет применения разных преобразований и разных случайных элементов (раундовых ключей, векторов инициализации) в каждый отдельный такт их работы. В таком случае k -кратная итерация одного и того же равновероятного случайного отображения уже не является адекватной моделью, и имеет смысл рассматривать ком-

позиции равновероятных случайных отображений [9, 10, 46, 70], точнее описывающие процесс функционирования подобных модификаций АМЗИ.

Рассмотрим конечное множество $S = \{1, \dots, n\}$, $n > 1$, и определенное в главе 1 вероятностное пространство случайных равновероятных отображений, в котором вероятностная мера задается соотношением (1.1).

Далее для произвольного $k \in \mathbb{N}$ рассмотрим последовательность независимых отображений $f_1, \dots, f_k$, имеющих распределение (1.1) на $\mathfrak{S}$, и через $f_{[k]}$ обозначим композицию отображений $f_k(\dots(f_1(x))\dots)$, $x \in S$. При этом под $f_{[0]}$ будем понимать тождественное отображение.

Отметим, что если случайные отображения $f_1, \dots, f_k$ имеют равновероятное распределение (1.1), то распределение $f_{[k]}$ при $k > 1$ не является равновероятным на $\mathfrak{S}$, так как $|S| \geq |f_{[1]}(S)| \geq |f_{[2]}(S)| \geq \dots$ и с положительной вероятностью указанные неравенства являются строгими (см. [71], с. 8).

В настоящей главе изучаются вероятностные характеристики и свойства графов $G_{f_{[k]}}$, когда $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$, а $k \in \mathbb{N}$ фиксировано.

2.2 Отрезок апериодичности вершины в графе отображения $f_{[k]}$

В графе случайного отображения $f_{[k]}$, $k \in \mathbb{N}$, начинающаяся в произвольной вершине $x_1 \in S$ траектория определяется соотношением

$$x_{i+1} = f_{[k]}(x_i), i = 1, 2, \dots$$

Как уже отмечалось в § 1.2, вопросы, связанные с описанием момента ее первого заикливания, представляют особый интерес для ряда задач информационной безопасности, в том числе для оценки среднего числа сообщений,

которые могут быть зашифрованы на последовательности ключей, выработанных с использованием итерационного АМЗИ.

Через $F_{[k]}$ обозначим функцию распределения случайной величины $\tau_{f_{[k]}}(x)$ для произвольной фиксированной вершины $x \in S$ (в силу равноправия вершин из S зависимость от x отражать не будем).

Теорема 2.1. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{0, 1, \dots, n\}$ справедливо равенство

$$F_{[k]}(z) = 1 - \left(1 - \frac{z}{n}\right) \left(\frac{\binom{n}{z}}{n^z}\right)^k. \quad (2.1)$$

Доказательство. В случае $z = 0$ очевидно равенство $F_k(0) = 0$. При этом правая часть выражения (2.1) также обращается в нуль.

Пусть далее $z \in \{1, \dots, n\}$. Для фиксированных $k \in \mathbb{N}$ и $x \in S$ рассмотрим итерационную процедуру формирования последовательности вершин $x, f_{[1]}(x), \dots, f_{[k]}(x), f_{[1]}(f_{[k]}(x)), \dots, f_{[1]}^2(x), f_{[1]}(f_{[k]}^2(x)), \dots$ (см. рис. 2.1).

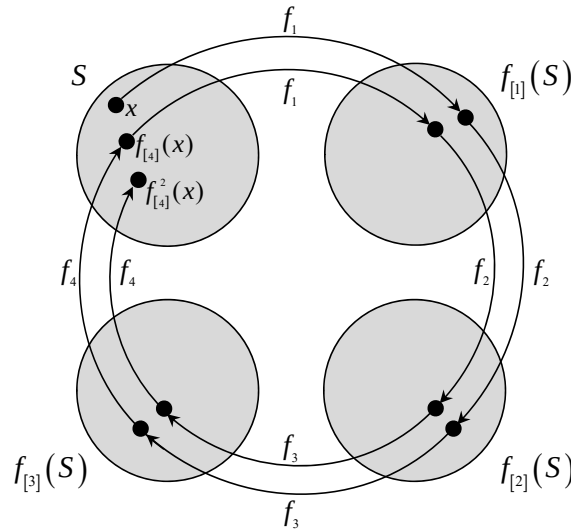


Рис. 2.1: Схема формирования компоненты $\mathcal{K}_{f_{[4]}}(x)$

Заметим, что процесс заикливания траектории в графе $G_{f_{[k]}}$, начинающийся в вершине x , существенно зависит от величины z .

Пусть $z = 1$. В этом случае в множествах $f_{[i]}(S)$, $i = 1, \dots, k-1$, формируется ровно по одной вершине, и заикливание траектории в $G_{f_{[k]}}$ за 1 шаг возможно только при условии $f_k(\dots(f_1(x))\dots) = x$, что выполняется с вероятностью $\frac{1}{n}$. Следовательно, $\mathbf{P}\{\tau_{f_{[k]}}(x) > 1\} = 1 - \frac{1}{n}$.

Пусть $z > 1$. Тогда событие $\{\tau_{f_{[k]}}(x) > z\}$ наступает тогда и только тогда, когда при любом $m = 1, \dots, k$ вершины $f_{[m]}^j(x)$, $j = 0, 1, \dots, z-1$, различны и $f_{[k]}^z(x) \notin \bigcup_{i=0}^{z-1} \{f_{[k]}^i(x)\}$. Таким образом, искомое событие $\{\tau_{f_{[k]}}(x) > z\}$ может быть представлено в следующем виде:

$$\{\tau_{f_{[k]}}(x) > z\} = \bigcap_{u=1}^{k-1} \bigcap_{\substack{i,j=0 \\ i < j}}^{z-1} \bigcap_{\substack{s,l=0 \\ s < l}}^z \left\{ \begin{array}{l} f_{[u]}^i(f_{[k]}^j(x)) \neq f_{[u]}^j(f_{[k]}^i(x)) \\ f_{[k]}^s(x) \neq f_{[k]}^l(x) \end{array} \right\},$$

В силу независимости отображений $f_1, \dots, f_k$, переходя к вероятностям, получаем цепочку равенств

$$\begin{aligned} \mathbf{P}\{\tau_{f_{[k]}}(x) > z\} &= \prod_{i=1}^z \left(1 - \frac{i}{n}\right) \left(\prod_{i=1}^{z-1} \left(1 - \frac{i}{n}\right)\right)^{k-1} = \\ &= \left(1 - \frac{z}{n}\right) \prod_{i=1}^{z-1} \left(1 - \frac{i}{n}\right)^k = \left(1 - \frac{z}{n}\right) \left(\frac{(n)_z}{n^z}\right)^k. \end{aligned} \quad (2.2)$$

Отсюда и из соотношения $F_{[k]}(z) = 1 - \mathbf{P}\{\tau_{f_{[k]}}(x) > z\}$ следует искомый результат. Теорема доказана. $\square$

Следствие 2.1. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ справедливо равенство

$$\mathbf{E}\tau_{f_{[k]}}(x) = \sum_{z=0}^{n-1} \left(1 - \frac{z}{n}\right) \left(\frac{(n)_z}{n^z}\right)^k.$$

Доказательство. Искомое равенство вытекает из (1.19) и соотношения (2.1):

$$\mathbf{E}\tau_{f_{[k]}}(x) = \sum_{z=0}^{\infty} \mathbf{P}\{\tau_{f_{[k]}}(x) > z\} = \sum_{z=0}^{n-1} \left(1 - \frac{z}{n}\right) \left(\frac{\binom{n}{z}}{n^z}\right)^k.$$

Следствие доказано. $\square$

Теорема 2.1 позволяет выписать асимптотику распределения случайной величины $\tau_{f_{[k]}}(x)$ при $n \rightarrow \infty$ для любого фиксированного $x \in S$.

Следствие 2.2. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$, где $|S| = n$, и любого $u \geq 0$ справедливо равенство

$$\lim_{n \rightarrow \infty} \mathbf{P}\left\{\tau_{f_{[k]}}(x) > u\sqrt{2n}\right\} = e^{-ku^2}.$$

Доказательство. С учетом леммы 1.1 для произвольного $m \in \{0, 1, \dots, n\}$ выполняется двойное неравенство

$$e^{-(1+\frac{m}{n})\frac{m(m-1)}{2n}} \leq \frac{\binom{n}{m}}{n^m} = \prod_{i=1}^{m-1} \left(1 - \frac{i}{n}\right) \leq e^{-\frac{m(m-1)}{2n}}. \quad (2.3)$$

Из него и формулы (2.2) получаем двустороннюю оценку

$$\left(1 - \frac{m}{n}\right) e^{-k(1+\frac{m}{n})\frac{m(m-1)}{2n}} \leq \mathbf{P}\{\tau_{f_{[k]}}(x) > m\} \leq \left(1 - \frac{m}{n}\right) e^{-k\frac{m(m-1)}{2n}}. \quad (2.4)$$

В итоге, полагая $m = u\sqrt{2n}$ и переходя в (2.4) к пределу при $n \rightarrow \infty$, приходим к утверждению следствия. Следствие доказано. $\square$

Замечание 2.1. Согласно следствию 2.2 для произвольного $x \in S$, не зависящего от $f_1, \dots, f_k$, распределение случайной величины $\frac{\tau_{f_{[k]}}(x)}{\sqrt{2n}}$ при $n \rightarrow \infty$ сходится к распределению Рэлея [4] с модой $\sigma = \frac{1}{\sqrt{2k}}$. Таким образом, в области типичных значений случайная величина $\tau_{f_{[k]}}(x)$ характеризуется асимптотическими математическим ожиданием $\sqrt{\frac{\pi n}{2k}}$ и дисперсией $\frac{2n}{k} \left(1 - \frac{\pi}{4}\right)$.

Следствие 2.3. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{1, \dots, n\}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{ \tau_{f_{[k]}}(x) = z \} &= \\ &= \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^k \right) \left(\frac{\binom{n}{z-1}}{n^{z-1}} \right)^k. \end{aligned} \quad (2.5)$$

Доказательство. С учетом (2.1) для искомой локальной вероятности выполняется цепочка равенств

$$\begin{aligned} \mathbf{P} \{ \tau_{f_{[k]}}(x) = z \} &= F_k(z) - F_k(z-1) = \\ &= 1 - \left(1 - \frac{z}{n} \right) \prod_{i=1}^{z-1} \left(1 - \frac{i}{n} \right)^k - \left(1 - \left(1 - \frac{z-1}{n} \right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right)^k \right) = \\ &= \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^k \right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right)^k. \end{aligned}$$

Следствие доказано. $\square$

Перейдем к более детальному рассмотрению события $\{ \tau_{f_{[k]}}(x) = z \}$, где $x \in S$ — произвольная вершина и $z \in \{1, \dots, n\}$. Отметим, что для равновероятного случайного отображения $f: S \rightarrow S$ реализация любой фиксированной траектории в графе G_f , начинающейся в вершине x и имеющей длину z , которая влечет за собой наступление события $\{ \tau_f(x) = z \}$, имеет одинаковую вероятность, равную $\frac{1}{n^z}$. Выясним, являются ли равновероятными реализации соответствующих траекторий в графе $G_{f_{[k]}}$ для произвольных фиксированных значений $k \in \mathbb{N}$ и $z \in \{1, \dots, n\}$.

Очевидно, что при $z = 1$ и любом фиксированном $k \in \mathbb{N}$ такая реализация в графе $G_{f_{[k]}}$ единственная, и это цикл длины 1, вероятность которого равна $\frac{1}{n}$. Данный случай является несодержательным, и поэтому будем рассматривать траектории длины $z \in \{2, \dots, n\}$.

Итак, зафиксируем любые $z - 1$ вершин $x_1, \dots, x_{z-1} \in S \setminus \{x\}$. Тогда для произвольного $k \in \mathbb{N}$ выполняется равенство

$$\begin{aligned} \{\mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x\} = \\ = \left\{ \bigcap_{u=1}^{k-1} \bigcap_{\substack{i,j=0 \\ i < j}}^{z-1} \left\{ \begin{aligned} &f_{[u]}(f_{[k]}^i(x)) \neq f_{[u]}(f_{[k]}^j(x)) \\ &f_{[k]}(x) = x_1, \dots, f_{[k]}^{z-1}(x) = x_{z-1}, f_{[k]}^z(x) = x \end{aligned} \right\} \right\}, \end{aligned}$$

где отрезок аperiodичности $\mathcal{R}_{f_{[k]}}(x)$ представляет собой цикл длины z . Далее, переходя к вероятностям указанных событий, с учетом независимости отображений $f_1, \dots, f_k$ получаем выражение

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x \} = \\ = \frac{1}{n^z} \left(\prod_{i=1}^{z-1} \left(1 - \frac{i}{n} \right) \right)^{k-1} = \frac{1}{n^z} \left(\frac{(n)_z}{n^z} \right)^{k-1}. \quad (2.6) \end{aligned}$$

В случае, когда рассматриваемая вершина x формирует фиксированный подход $x, x_1, \dots, x_{m-1}$ длины $m \in \{1, \dots, z-1\}$ к циклу $x_m, \dots, x_{z-1}, x_m$ длины $z - m$, имеет место следующее равенство событий:

$$\begin{aligned} \{\mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x_m\} = \\ = \left\{ \bigcap_{u=1}^{k-1} \bigcap_{\substack{i,j=0 \\ i < j}}^{z-1} \left\{ \begin{aligned} &f_{[u]}(f_{[k]}^i(x)) \neq f_{[u]}(f_{[k]}^j(x)) \\ &f_{[k]}(x) = x_1, \dots, f_{[k]}^{z-1}(x) = x_{z-1}, f_{[k]}^z(x) = x_m \end{aligned} \right\} \right\} \cup \\ \cup \left\{ \bigcap_{u=1}^{k-1} \bigcap_{\substack{i,j=0 \\ i < j}}^{z-2} \left\{ \begin{aligned} &f_{[u]}(f_{[k]}^i(x)) \neq f_{[u]}(f_{[k]}^j(x)) \\ &f_{[k]}(x) = x_1, \dots, f_{[k]}^{z-1}(x) = x_{z-1} \\ &f_{[1]}(f_{[k]}^{z-1}(x)) = f_{[1]}(f_{[k]}^{m-1}(x)) \end{aligned} \right\} \right\} \cup \end{aligned}$$

$$\bigcup \left\{ \bigcap_{d=1}^{k-2} \bigcap_{u=1}^d \bigcap_{v=d+1}^{k-1} \bigcap_{\substack{i,j=0 \\ i < j}}^{z-1} \bigcap_{\substack{s,l=0 \\ s < l}}^{z-2} \left\{ \begin{array}{l} f_{[u]} \left(f_{[k]}^i(x) \right) \neq f_{[u]} \left(f_{[k]}^j(x) \right) \\ f_{[v]} \left(f_{[k]}^s(x) \right) \neq f_{[v]} \left(f_{[k]}^l(x) \right) \\ f_{[k]}(x) = x_1, \dots, f_{[k]}^{z-1}(x) = x_{z-1} \\ f_{[d+1]} \left(f_{[k]}^{z-1}(x) \right) = f_{[d+1]} \left(f_{[k]}^{m-1}(x) \right) \end{array} \right\} \right\}$$

и, соответственно,

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x_m \} &= \frac{1}{n^z} \left(\prod_{i=1}^{z-1} \left(1 - \frac{i}{n} \right) \right)^{k-1} + \\ &+ \frac{1}{n^z} \left(\prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right) \right)^{k-1} + \frac{1}{n^z} \sum_{d=1}^{k-2} \left(1 - \frac{z-1}{n} \right)^d \left(\prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right) \right)^{k-1} = \\ &= \frac{1}{n^z} \left(\prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right) \right)^{k-1} \sum_{d=0}^{k-1} \left(1 - \frac{z-1}{n} \right)^d = \\ &= \frac{1}{n^{z-1} (z-1)} \left(\frac{(n)_{z-1}}{n^{z-1}} \right)^{k-1} \left(1 - \left(1 - \frac{z-1}{n} \right)^k \right). \quad (2.7) \end{aligned}$$

Формулы (2.6), (2.7) позволяют сделать вывод о том, что для произвольных $k \in \mathbb{N}$, $z \in \{2, \dots, n\}$ и любых фиксированных $z-1$ вершин $x_1, \dots, x_{z-1} \in S \setminus \{x\}$ вероятность того, что реализация траектории длины z в графе $G_{f_{[k]}}$, $k > 1$, начинающейся в вершине x , сформирует цикл, меньше вероятности формирования любого фиксированного подхода к циклу на величину

$$\frac{1}{n^{z-1} (z-1)} \left(\frac{(n)_{z-1}}{n^{z-1}} \right)^{k-1} \left(1 - \left(1 - \frac{z-1}{n} \right)^{k-1} \right).$$

При этом каждая из $(z-1)$ -й возможных траекторий, представляющих собой подход к циклу, имеет одинаковую вероятность (2.7).

Замечание 2.2. В общем случае сформулировать аналогичный вывод для графа G_{f^k} , $k > 1$, не представляется возможным в силу существенной зависимости структуры указанного графа от соотношения k и z , в частности,

наличия у них общих делителей. Так, например, при $n > 4$, $z = 2$ и $k = 2$ для вероятности того, что отрезок апериодичности, начинающийся в произвольной вершине $x \in S$, проходящий через фиксированную вершину $x_1 \in S \setminus \{x\}$ и имеющий длину 2, совпадет с циклом, имеем

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f^2}(x) = x, x_1, x \} = \\ = \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, x_1, y_2, x \} = \frac{1}{n^2} \left(1 - \frac{2}{n} \right) \left(1 - \frac{3}{n} \right), \end{aligned}$$

а для вероятности совпасть с подходом:

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f^2}(x) = x, x_1, x_1 \} = \\ \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, x_1, y_2, x_1 \} + \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, x_1, x_1 \} = \\ = \frac{1}{n^2} \left(1 - \frac{2}{n} \right) \left(1 - \frac{3}{n} \right) + \frac{1}{n^2} \left(1 - \frac{2}{n} \right), \end{aligned}$$

где $y_1, y_2 \in S \setminus \{x, x_1\}$ — произвольные различные вершины. В данном случае вероятность совпадения с циклом меньше вероятности совпадения с подходом в графе G_{f^2} . Вместе с тем, при $z = 2$ и $k = 3$

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f^2}(x) = x, x_1, x \} = \\ = \mathbf{P} \{ \mathcal{R}_f(x) = x, x_1, x \} + \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, y_2, x_1, y_3, y_4, x \} = \\ = \frac{1}{n^2} + \frac{1}{n^2} \left(1 - \frac{2}{n} \right) \left(1 - \frac{3}{n} \right) \left(1 - \frac{4}{n} \right) \left(1 - \frac{5}{n} \right), \end{aligned}$$

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f^2}(x) = x, x_1, x_1 \} = \\ \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, y_2, x_1, x_1 \} + \mathbf{P} \{ \mathcal{R}_f(x) = x, y_1, y_2, x_1, y_3, y_4, x_1 \} = \\ = \frac{1}{n^2} \left(1 - \frac{2}{n} \right) \left(1 - \frac{3}{n} \right) + \frac{1}{n^2} \left(1 - \frac{2}{n} \right) \left(1 - \frac{3}{n} \right) \left(1 - \frac{4}{n} \right) \left(1 - \frac{5}{n} \right), \end{aligned}$$

где $y_1, y_2, y_3, y_4 \in S \setminus \{x, x_1\}$ — произвольные различные вершины. Здесь уже вероятность совпадения с циклом длины 2 в графе G_{f^3} больше вероятности совпадения с указанным выше подходом.

Далее для произвольных $k \in \mathbb{N}$, $z \in \{1, \dots, n\}$ и произвольных вершин $x_1, \dots, x_z \in S$ определим событие $R_{(x_1, \dots, x_z)}^{[k]}$, заключающееся в том, что фиксированная траектория $x_1, \dots, x_z$ в графе $G_{f_{[k]}}$ представляет собой отрезок апериодичности $\mathcal{R}_{f_{[k]}}(x)$ длины z . Тогда с учетом (2.6) и (2.7) справедливо равенство

$$\begin{aligned} \mathbf{P} \left\{ R_{(x, x_1, \dots, x_{z-1})}^{[k]} \right\} &= \mathbf{P} \left\{ \mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x \right\} + \\ &+ (z-1) \mathbf{P} \left\{ \mathcal{R}_{f_{[k]}}(x) = x, x_1, \dots, x_{z-1}, x_m \right\} = \frac{z}{n^z} \left(\prod_{i=1}^{z-1} \left(1 - \frac{i}{n} \right) \right)^{k-1} + \\ &+ \frac{1}{n^{z-1}} \left(\prod_{i=1}^{z-2} \left(1 - \frac{i}{n} \right) \right)^{k-1} \left(1 - \left(1 - \frac{z-1}{n} \right)^{k-1} \right) = \\ &= \frac{1}{n^{z-1}} \left(\frac{(n)_{z-1}}{n^{z-1}} \right)^{k-1} \left(1 - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^{k-1} \right). \quad (2.8) \end{aligned}$$

Замечание 2.3. Формула (2.8) может быть использована для вычисления $\mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\}$. Действительно, в силу равноправия вершин из S справедливо соотношение

$$\mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} = (n-1)_{z-1} \mathbf{P} \left\{ R_{(x, x_1, \dots, x_{z-1})}^{[k]} \right\}.$$

Перейдем к выводу оценочных выражений, допускающих эффективное вычисление $\mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\}$ при больших значениях параметра n .

Следствие 2.4. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $z \in \{1, \dots, n\}$ справедливы неравенства

$$\begin{aligned} \mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} &\geq \\ &\geq \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^k \right) e^{-k \left(1 + \frac{z}{n} \right) \frac{(z-1)(z-2)}{2n}}, \quad (2.9) \end{aligned}$$

$$\begin{aligned} \mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} &\leq \\ &\leq \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^k \right) e^{-k \frac{(z-1)(z-2)}{2n}}. \end{aligned} \quad (2.10)$$

Если при этом $z > 1$ и $kz \leq n$, то

$$\begin{aligned} \mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} &> \\ &> \left(1 - \frac{z-1}{n} \right) \left(\frac{k(z-1)}{n} - C_k^2 \frac{(z-1)^2}{n^2} \right) e^{-k \left(1 + \frac{z}{n} \right) \frac{(z-1)(z-2)}{2n}}, \\ \mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z \right\} &\leq \frac{1}{n} \left(1 + k(z-1) \left(1 - \frac{z}{n} \right) \right) e^{-k \frac{(z-1)(z-2)}{2n}}. \end{aligned}$$

Доказательство. С учетом двойного неравенства (2.3) и формулы (2.5) получаем искомые оценки (2.9) и (2.10).

Далее рассмотрим справедливое при $-1 < x < 1$ неравенство

$$1 - kx \leq (1 - x)^k \leq 1 - kx + C_k^2 x^2, \quad (2.11)$$

вытекающее из соотношения

$$(1 - x)^k = 1 - kx + C_k^2 x^2 - C_k^3 x^3 + \dots,$$

где $-1 < x < 1$ (см., например, [53], с. 63). В условиях настоящего следствия и левая, и правая части данного неравенства являются содержательными для $x = \frac{z-1}{n}$. Согласно (2.11) имеет место цепочка соотношений

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

откуда следует оценка снизу для $\mathbf{P} \{ \tau_{f_{[k]}}(x) = z \}$.

С другой стороны, из (2.11) получаем

$$\begin{aligned} 1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right) \left(1 - \frac{z-1}{n}\right)^k &\leq \\ &\leq 1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right) \left(1 - \frac{k(z-1)}{n}\right) = \\ &= \frac{1}{n} + \frac{k(z-1)}{n} - \frac{kz(z-1)}{n^2} = \frac{1}{n} \left(1 + k(z-1) \left(1 - \frac{z}{n}\right)\right), \end{aligned}$$

и поэтому

$$\mathbf{P} \{ \tau_{f_{[k]}}(x) = z \} \leq \frac{1}{n} \left(1 + k(z-1) \left(1 - \frac{z}{n}\right)\right) e^{-k \frac{(z-1)(z-2)}{2n}}.$$

Следствие доказано. $\square$

Через $\nu_{f_{[k]}}(z)$ обозначим случайную величину, равную числу вершин в графе $G_{f_{[k]}}$, для которых длина отрезка аperiodичности равна $z \in \{1, \dots, n\}$.

Следствие 2.5. [25] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого $z \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{E} \nu_{f_{[k]}}(z) = n \left(1 - \frac{z-1}{n} - \left(1 - \frac{z}{n}\right) \left(1 - \frac{z-1}{n}\right)^k\right) \left(\frac{(n)_{z-1}}{n^{z-1}}\right)^k.$$

Доказательство. Зафиксируем $z \in \{1, \dots, n\}$ и представим случайную величину $\nu_{f_{[k]}}(z)$ в виде суммы индикаторов:

$$\nu_{f_{[k]}}(z) = \sum_{x \in S} I \{ \tau_{f_{[k]}}(x) = z \}.$$

Тогда в силу равноправия всех вершин множества S

$$\mathbf{E} \nu_{f_{[k]}}(z) = \sum_{x \in S} \mathbf{P} \{ \tau_{f_{[k]}}(x) = z \} = n \mathbf{P} \{ \tau_{f_{[k]}}(x) = z \},$$

откуда с учетом равенства (2.5) получим искомое выражение. Следствие доказано. $\square$

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

Так же как и в модели k -кратной итерации равновероятного случайного отображения конечного множества в себя, структуры множеств $H_{f_{[k]}}^{(t)}$ и $H_{f_{[k]}}^{(t,l)}$ (см. определения 1.7 и 1.8) в графе $G_{f_{[k]}}$ при $t = 0$ и $t > 0$ различны.

В случае $t = 0$ рассматриваемые множества совпадают с множествами $C(G_{f_{[k]}})$ и $C_l(G_{f_{[k]}})$ соответственно. Перейдем к описанию их вероятностных свойств.

Теорема 2.2. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любого $l \in \{1, \dots, n\}$ справедливы равенства

$$\mathbf{P} \{x \in C_l(G_{f_{[k]}})\} = \frac{1}{n} \left(\frac{(n)_l}{n^l} \right)^k, \quad (2.12)$$

$$\mathbf{P} \{x \in C(G_{f_{[k]}})\} = \frac{1}{n} \sum_{l=1}^n \left(\frac{(n)_l}{n^l} \right)^k. \quad (2.13)$$

Доказательство. Зафиксируем $x \in S$. Тогда для произвольного $k \in \mathbb{N}$ 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. рис. 2.1, с. 80) событие $\{x \in C_l(G_{f_{[k]}})\}$ наступает 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 $f_1, \dots, f_k$

$$\mathbf{P} \{x \in C_l(G_{f_{[k]}})\} = \frac{1}{n} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n} \right)^k. \quad (2.14)$$

Второе утверждение теоремы получаем с использованием (2.14) и формулы полной вероятности. Теорема доказана. $\square$

Через $\lambda_{f_{[k]}}(l)$ обозначим случайную величину, равную числу вершин в графе $G_{f_{[k]}}$, лежащих на циклах длины $l \in \{1, \dots, n\}$, а через $\lambda_{f_{[k]}}$ — равную общему числу циклических вершин в графе $G_{f_{[k]}}$.

Теорема 2.2 позволяет выписать равенства для средних значений

$$\mathbf{E}\lambda_{f_{[k]}}(l) = \left(\frac{(n)_l}{n^l}\right)^k, \quad \mathbf{E}\lambda_{f_{[k]}} = \sum_{l=1}^n \left(\frac{(n)_l}{n^l}\right)^k. \quad (2.15)$$

Следствие 2.6. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого $l \in \{1, \dots, n\}$

$$e^{-k(1+\frac{l}{n})\frac{l(l-1)}{2n}} \leq \mathbf{E}\lambda_{f_{[k]}}(l) \leq e^{-k\frac{l(l-1)}{2n}}, \quad (2.16)$$

$$\mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{\pi n}{2k}}. \quad (2.17)$$

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

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

Доказательство. Оценки (2.16) следуют из (2.12) и неравенства (1.11).

Перейдем к доказательству (2.17). 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 (2.15) и (2.16) получаем

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

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:

$$\mathbf{E}\lambda_{f_{[k]}} < 1 + \sqrt{\frac{n}{k}} \int_0^\infty e^{-\frac{z^2}{2}} dz = 1 + \sqrt{\frac{n}{k}} \frac{\sqrt{2\pi}}{2} = 1 + \sqrt{\frac{\pi n}{2k}}. \quad (2.18)$$

С другой стороны, из (1.11) следует, что при $1 \leq l \leq n^{\frac{7}{12}}$

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

Тогда, применяя неравенство

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

получаем цепочку соотношений при $n \rightarrow \infty$

$$\begin{aligned} \mathbf{E} \lambda_{f_{[k]}} &> \sum_{l=1}^{\lfloor n^{7/12} \rfloor} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right)^k > \sum_{l=1}^{\lfloor n^{7/12} \rfloor} e^{-k \frac{l^2}{2n} \left(1 + n^{-\frac{5}{12}}\right)} > \\ &> \int_1^{n^{7/12}} e^{-k \frac{x^2}{2n} \left(1 + n^{-\frac{5}{12}}\right)} dx = (1 + o(1)) \sqrt{\frac{\pi n}{2k \left(1 + n^{-\frac{5}{12}}\right)}} = (1 + o(1)) \sqrt{\frac{\pi n}{2k}}, \end{aligned}$$

откуда с учетом (2.18) получаем $\mathbf{E} \lambda_{f_{[k]}} = (1 + o(1)) \sqrt{\frac{\pi n}{2k}}$ при $n \rightarrow \infty$. Следствие доказано. $\square$

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

Теорема 2.3. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $l_1, l_2 \in \mathbb{N}$, $l_1 + l_2 \leq n(1 + \delta_{l_1, l_2})$, справедливо равенство

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

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

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

$$I_{x,y} = \begin{cases} 1, & \text{если } x, y \text{ — на одном цикле графа } G_{f[k]}, \\ 0 & \text{в противном случае.} \end{cases} \quad (2.19)$$

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

$$\begin{aligned} \mathbf{P} \{x, y \in C_l (G_{f[k]})\} &= \\ &= \mathbf{P} \left\{ \begin{matrix} x, y \in C_l (G_{f[k]}) \\ I_{x,y} = 1 \end{matrix} \right\} + \mathbf{P} \left\{ \begin{matrix} x, y \in C_l (G_{f[k]}) \\ I_{x,y} = 0 \end{matrix} \right\}. \end{aligned} \quad (2.20)$$

Вычислим первое слагаемое в правой части (2.20). Для произвольной фиксированной 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 2.2 с учетом дополнительной фиксированной вершины y , получаем равенство

$$\begin{aligned} \mathbf{P} \left\{ \begin{matrix} x, y \in C_l (G_{f[k]}) \\ I_{x,y} = 1 \end{matrix} \right\} &= \frac{l-1}{n^2} \prod_{i=2}^{l-1} \left(1 - \frac{i}{n}\right) \cdot \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right)^{k-1} = \\ &= \frac{l-1}{n(n-1)} \prod_{i=1}^{l-1} \left(1 - \frac{i}{n}\right)^k. \end{aligned} \quad (2.21)$$

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

$$\mathbf{P} \left\{ \begin{matrix} x, y \in C_l (G_{f[k]}) \\ I_{x,y} = 0 \end{matrix} \right\} = \frac{1}{n(n-1)} \prod_{i=1}^{2l-1} \left(1 - \frac{i}{n}\right)^k. \quad (2.22)$$

Подставив (2.21) и (2.22) в равенство (2.20), 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

$$\mathbf{P} \left\{ \begin{array}{c} x \in C_{l_1}(G_{f_{[k]}}), y \in C_{l_2}(G_{f_{[k]}}) \\ l_1 \neq l_2 \end{array} \right\} = \frac{1}{n(n-1)} \prod_{i=1}^{l_1+l_2-1} \left(1 - \frac{i}{n}\right)^k. \quad (2.23)$$

Объединив выражения (2.20) и (2.23) с использованием символа Кронекера, получим утверждение теоремы. Теорема доказана. $\square$

Замечание 2.4. Как отмечалось в § 1.4, при итерировании одного случайного отображения множество циклических вершин остается неизменным, а вероятность попадания вершины во множество циклических вершин не зависит от количества итераций. Таким образом, для произвольных $d, k \in \mathbb{N}$ в графе $G_{f_{[k]}^d}$ выполняется равенство

$$C(G_{f_{[k]}^d}) = C(G_{f_{[k]}}).$$

При этом с учетом теоремы 2.2

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

В свою очередь, при фиксированном $k \in \mathbb{N}$ распределение числа циклических вершин по компонентам графа $G_{f_{[k]}^d}$ зависит от величины $d \in \mathbb{N}$.

Следствие 2.7. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любых $d \in \mathbb{N}$, $l \in \{1, \dots, n\}$ справедливо равенство

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

где $Q_1^n(d, l)$ определяется соотношением (1.7).

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 (2.12) следует искомый результат. Следствие доказано. $\square$

Следствие 2.8. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $d \in \mathbb{N}$ и $l_1, l_2 \in \{1, \dots, n\}$, $l_1 + l_2 \leq n(1 + \delta_{l_1, l_2})$, справедливо равенство

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

где δ_{l_1, l_2} — символ Кронекера, а $Q_1^n(d, l)$ определяется соотношением (1.7).

Доказательство. Рассмотрим случай $l_1 = l_2 = l$. Используя обозначения (2.19), для произвольных фиксированных $x, y \in S$ по формуле полной вероятности имеем

$$\begin{aligned} \mathbf{P} \left\{x, y \in C_l \left(G_{f_{[k]}^d}\right)\right\} &= \\ &= \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l \left(G_{f_{[k]}^d}\right) \\ I_{x, y} = 1 \end{array} \right\} + \mathbf{P} \left\{ \begin{array}{c} x, y \in C_l \left(G_{f_{[k]}^d}\right) \\ I_{x, y} = 0 \end{array} \right\}. \quad (2.24) \end{aligned}$$

Вычислим первое слагаемое в правой части (2.24). Для произвольной фиксированной вершины $y \in S$, $y \neq x$, существует в точности $m - 1$ вариантов ее расположения на содержащем x цикле длины $m \in Q_2^n(d, l)$ в графе $G_{f_{[k]}}$. Тогда

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 1 \end{array} \right\} &= \\ &= \sum_{m \in Q_2^n(d, l)} \frac{m-1}{n(n-1)} \prod_{i=1}^{m-1} \left(1 - \frac{i}{n} \right)^k = \sum_{m \in Q_1^n(d, l)} \frac{m-1}{n(n-1)} \left(\frac{(n)_m}{n^m} \right)^k. \end{aligned} \quad (2.25)$$

Если вершины x, y лежат на циклах различных длин $m_1, m_2 \in \{1, \dots, n\}$, $m_1 \in Q_1^n(d, l)$, $m_2 \in Q_1^{n-m_1}(d, l)$, в графе $G_{f_{[k]}}$, то

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x, y \in C_l \left(G_{f_{[k]}}^d \right) \\ I_{x,y} = 0 \end{array} \right\} &= \\ &= \sum_{m_1 \in Q_1^n(d, l)} \sum_{m_2 \in Q_1^{n-m_1}(d, l)} \frac{1}{n(n-1)} \prod_{i=1}^{m_1+m_2-1} \left(1 - \frac{i}{n} \right)^k = \\ &= \frac{1}{n(n-1)} \sum_{m_1 \in Q_1^n(d, l)} \sum_{m_2 \in Q_1^{n-m_1}(d, l)} \left(\frac{(n)_{m_1+m_2}}{n^{m_1+m_2}} \right)^k. \end{aligned} \quad (2.26)$$

Подставив (2.25) и (2.26) в (2.24), 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

$$\begin{aligned} \mathbf{P} \left\{ \begin{array}{l} x \in C_{l_1} \left(G_{f_{[k]}}^d \right), y \in C_{l_2} \left(G_{f_{[k]}}^d \right) \\ l_1 \neq l_2 \end{array} \right\} &= \\ &= \frac{1}{n(n-1)} \sum_{m_1 \in Q_1^n(d, l_1)} \sum_{m_2 \in Q_1^{n-m_1}(d, l_2)} \left(\frac{(n)_{m_1+m_2}}{n^{m_1+m_2}} \right)^k. \end{aligned} \quad (2.27)$$

Объединяя выражения (2.24) и (2.27), получаем искомую формулу. Следствие доказано. $\square$

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

Теорема 2.4. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любых $t \in \{1, \dots, n-1\}$, $l \in \{1, \dots, n-t\}$

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\} &= \\ &= \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) \left(\frac{\binom{n}{t+l-1}}{n^{t+l-1}} \right)^k. \end{aligned} \quad (2.28)$$

Доказательство. Зафиксируем $x \in S$ и для произвольного $k \in \mathbb{N}$ рассмотрим указанную выше 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. рис. 2.1). Событие $\left\{ x \in H_{f_{[k]}}^{(t,l)} \right\}$ наступает 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 $f_{[k]}^{t+l}(x) = f_{[k]}^t(x)$, иными словами, существует такое $j \in \{1, \dots, k\}$, что $f_{[i]}(f_{[k]}^{t+l-1}(x)) \notin \left\{ f_{[i]}(f_{[k]}^m(x)), m = 0, \dots, t+l-2 \right\}$ 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

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

$$\cap \left\{ \bigcup_{j=1}^k \left\{ \min \left\{ m \neq t-1 : f_{[j]} \left(f_{[k]}^m(x) \right) = f_{[j]} \left(f_{[k]}^{t-1}(x) \right) \right\} = t+l-1, \right. \right. \\ \left. \left. f_{[j-1]} \left(f_{[k]}^{t+l-1}(x) \right) \neq f_{[j-1]} \left(f_{[k]}^{t-1}(x) \right) \right\} \right\},$$

где под знаком объединения стоят несовместные события. Поэтому, переходя к вероятностям, с учетом независимости отображений $f_1, \dots, f_k$ получаем

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

откуда следует искомая формула. Теорема доказана. $\square$

Замечание 2.5. Для среднего значения мощности множества $H_{f_{[k]}}^{(t,l)}$ в графе $G_{f_{[k]}}$ в силу равноправия всех вершин $x \in S$ справедливо

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

Следствие 2.9. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ и любых $t \in \{1, \dots, n-1\}$, $l \in \{1, \dots, n-t\}$ справедливы неравенства

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(t,l)} \right\} &\geq \\ &\geq \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) e^{-k \left(1 + \frac{t+l}{n} \right) \frac{(t+l-1)(t+l-2)}{2n}}, \quad (2.29) \end{aligned}$$

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \right\} &\leq \\ &\leq \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) e^{-k \frac{(t+l-1)(t+l-2)}{2n}}. \end{aligned} \quad (2.30)$$

Если при этом $t+l \leq \frac{n}{k}$, то

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \right\} &> \left(\frac{k}{n} - \frac{k(t+l-1)}{n^2} \right) \left(1 - \frac{k(t+l)}{2n} \right) e^{-k \left(1 + \frac{t+l}{n} \right) \frac{(t+l-1)(t+l-2)}{2n}}, \\ \mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \right\} &< \left(\frac{k}{n} - \frac{k(t+l-1)}{n^2} \right) e^{-k \frac{(t+l-1)(t+l-2)}{2n}}. \end{aligned}$$

Доказательство. Из неравенства (1.11) и формулы (2.28), очевидным образом, вытекают оценки (2.29) и (2.30).

Далее рассмотрим двустороннее неравенство (2.11), справедливое, в том числе, для $0 < x = \frac{t+l-1}{n} < 1$. Заметим, что его левая часть является содержательной в условиях настоящего следствия, так как $kx = \frac{k(t+l-1)}{n} < 1$ а следовательно, содержательна и его правая часть, поскольку $\frac{(k-1)x}{2} < kx < 1$.

Таким образом, имеет место цепочка неравенств

$$\begin{aligned} &\left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) > \\ &> \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(\frac{k(t+l-1)}{n} - \frac{k(k-1)(t+l-1)^2}{2n^2} \right) > \\ &> \left(\frac{k}{n} - \frac{k(t+l-1)}{n^2} \right) \left(1 - \frac{k(t+l)}{2n} \right), \end{aligned}$$

откуда следует оценка снизу для $\mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \right\}$. С другой стороны,

$$\begin{aligned} &\left(\frac{1}{t+l-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{t+l-1}{n} \right)^k \right) < \\ &< \left(\frac{1}{t+l-1} - \frac{1}{n} \right) \frac{k(t+l-1)}{n} = \frac{k}{n} - \frac{k(t+l-1)}{n^2}, \end{aligned}$$

и поэтому

$$\mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \right\} < \left(\frac{k}{n} - \frac{k(t+l-1)}{n^2} \right) e^{-k \frac{(t+l-1)(t+l-2)}{2n}}.$$

Следствие доказано. $\square$

Отметим, что классификация вершин по слоям графа $G_{f[k]}$ является более информативной, чем классификация вершин по величине их отрезков апериодичности, и может быть использована для расчета теоретических оценок вероятности повторного использования производных ключей.

Действительно, выполнение условия $\tau_{f[k]}(x) \neq \tau_{f[k]}(y)$ для произвольных различных фиксированных вершин $x, y \in S$ не исключает факт повторного использования производных ключей, сформированных на основе долговременных ключей, соответствующих вершинам x и y . В частности, при попадании обеих вершин в одну компоненту связности, минимальное число совпавших ключей составляет $\beta_{f[k]}(x)$. В свою очередь, выполнение условия $\left\{ x \in H_{f[k]}^{(t_1, l_1)}, y \in H_{f[k]}^{(t_2, l_2)} \right\}$, где $l_1 \neq l_2$, полностью исключает повтор ключей, хотя при этом может иметь место равенство $t_1 + l_1 = t_2 + l_2$, а следовательно, и совпадение длин отрезков апериодичности $\tau_{f[k]}(x) = \tau_{f[k]}(y)$.

Замечание 2.6. Указанные выводы справедливы и для графа G_{f^k} , $k \in \mathbb{N}$.

Через $\tilde{F}_{[k]}$ обозначим функцию распределения случайной величины $\alpha_{f[k]}(x)$ для произвольной фиксированной вершины $x \in S$ (в силу равноправия вершин из S зависимость от x отражать не будем).

Следствие 2.10. [27] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ выполняются равенства

$$\mathbf{P} \left\{ x \in H_{f[k]}^{(z)} \right\} = \sum_{l=z}^{n-1} \left(\frac{1}{l} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{l}{n} \right)^k \right) \left(\frac{(n)_l}{n^l} \right)^k, \quad (2.31)$$

где $z \in \{1, \dots, n-1\}$,

$$\begin{aligned} \tilde{F}_{[k]}(z) = \frac{1}{n} \sum_{l=1}^n \left(\frac{(n)_l}{n^l} \right)^k + \\ + \sum_{s=1}^z \sum_{l=s}^{n-1} \left(\frac{1}{l} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{l}{n} \right)^k \right) \left(\frac{(n)_l}{n^l} \right)^k, \end{aligned} \quad (2.32)$$

где $z \in \{0, \dots, n-1\}$.

Доказательство. Из соотношения $H_{f_{[k]}}^{(z)} = \bigcup_{l=1}^{n-z} H_{f_{[k]}}^{(z,l)}$, где $H_{f_{[k]}}^{(z,l_1)} \cap H_{f_{[k]}}^{(z,l_2)} = \emptyset$ при $l_1 \neq l_2$, справедливого для произвольного $z \in \{1, \dots, n-1\}$, следует

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

откуда с учетом равенства (2.28) получаем искомое выражение (2.31).

Второе утверждение следствия вытекает из равенства событий

$$\left\{ \alpha_{f_{[k]}}(x) \leq z \right\} = \left\{ x \in C(G_{f_{[k]}}) \right\} \cup \left(\bigcup_{s=1}^z \left\{ x \in H_{f_{[k]}}^{(s)} \right\} \right)$$

и формул (2.13) и (2.31). Следствие доказано. $\square$

Следствие 2.10 позволяет получить некоторое представление об общем строении графа $G_{f_{[k]}}$, $k \in \mathbb{N}$. А именно, для произвольного фиксированного $x \in S$ из выражения (2.31) следует, что вероятность $\mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z)} \right\}$ монотонно убывает с ростом $z \in \{1, \dots, n-1\}$:

$$\begin{aligned} \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z-1)} \right\} - \mathbf{P} \left\{ x \in H_{f_{[k]}}^{(z)} \right\} = \\ = \sum_{l=z-1}^{n-1} \left(\frac{1}{l} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{l}{n} \right)^k \right) \left(\frac{(n)_l}{n^l} \right)^k - \\ - \sum_{l=z}^{n-1} \left(\frac{1}{l} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{l}{n} \right)^k \right) \left(\frac{(n)_l}{n^l} \right)^k = \\ = \left(\frac{1}{z-1} - \frac{1}{n} \right) \left(1 - \left(1 - \frac{z-1}{n} \right)^k \right) \left(\frac{(n)_{z-1}}{n^{z-1}} \right)^k > 0. \end{aligned}$$

Таким образом, для фиксированного $k \in \mathbb{N}$ в графе $G_{f[k]}$ вершины с большей вероятностью сосредотачиваются вблизи циклов. При этом с ростом значения k эта плотность возрастает. Так, в качестве примера на рисунке 2.2 проиллюстрирована скорость убывания величины $\mathbf{P} \left\{ x \in H_{f[k]}^{(z)} \right\}$ с ростом z для значений $k = 1, 2, 4, 16$ и $n = 512$.

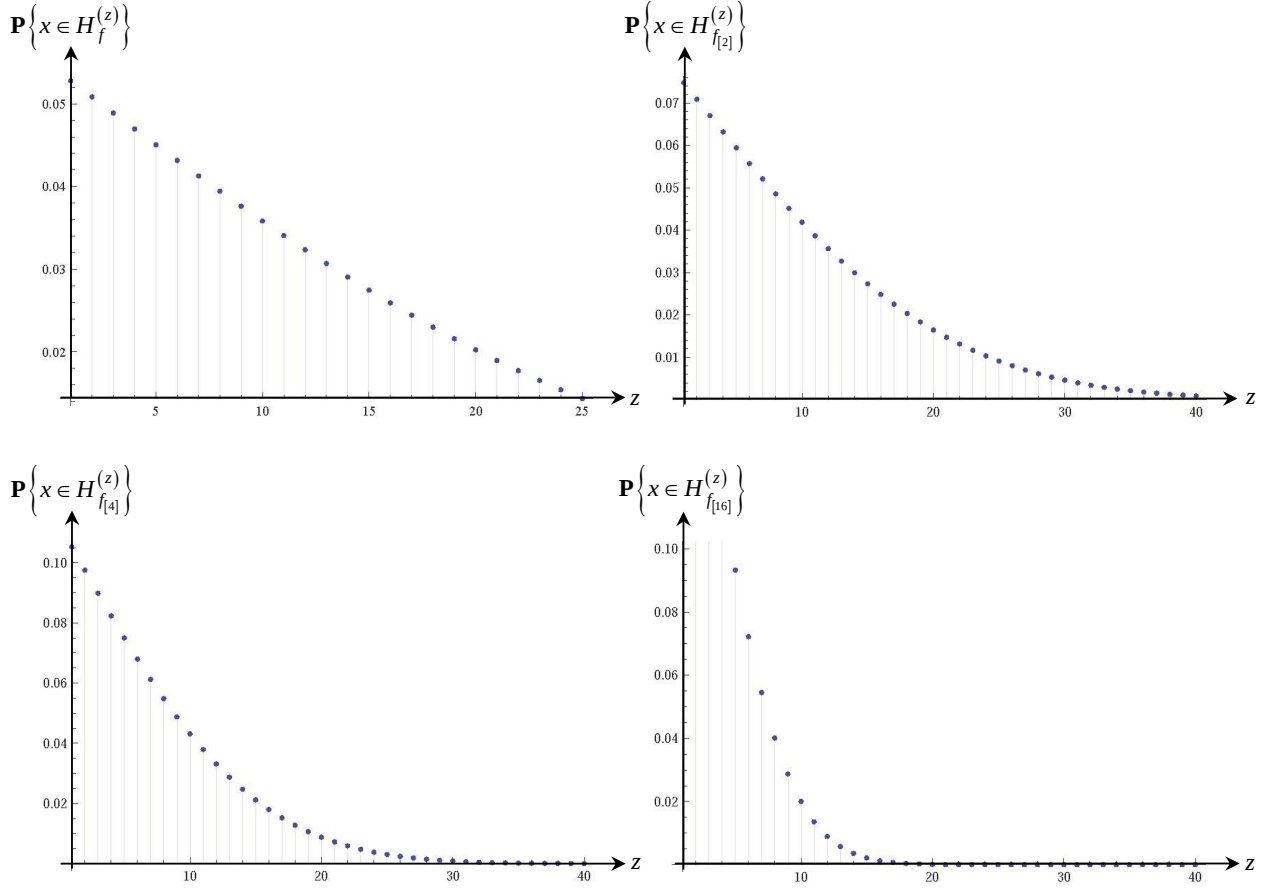


Рис. 2.2: Зависимость $\mathbf{P} \left\{ x \in H_{f[k]}^{(z)} \right\}$ от z при $k = 1, 2, 4, 16$

Замечание 2.7. Для произвольного фиксированного $x \in S$ следствие 2.10 позволяет выписать выражения для $\mathbf{E}\alpha_{f[k]}(x)$, как с помощью (2.13) и (2.31):

$\mathbf{E}\alpha_{f[k]}(x) = \sum_{z=0}^{n-1} z \mathbf{P} \left\{ x \in H_{f[k]}^{(z)} \right\}$, так и с помощью (2.32):

$$\mathbf{E}\alpha_{f[k]}(x) = \sum_{z=0}^{n-2} \mathbf{P} \left\{ \alpha_{f[k]}(x) > z \right\} = \sum_{z=0}^{n-2} \left(1 - \tilde{F}_{[k]}(z) \right) = n - \sum_{z=0}^{n-1} \tilde{F}_{[k]}(z).$$

2.4 Множество образов и коллизии в графе отображения $f_{[k]}$

В рамках исследования вероятностных характеристик множества $f_{[k]}(S)$, $k \in \mathbb{N}$, А.М. Зубковым и А.А. Серовым в [10] получены оценки математического ожидания мощности образа подмножества $S_0 \subset S$ при композиции независимых равновероятных случайных отображений конечного множества в себя. Результаты, приведенные в § 2.3 настоящей диссертации, позволяют выписать точные формулы для ряда вероятностных характеристик образа $f_{[k]}(S)$ исходного множества S , в том числе, для математического ожидания его мощности.

Для произвольных $k \in \mathbb{N}$, $m, s_1, \dots, s_k \in \mathbb{N}$, $n \geq m \geq s_1 \geq \dots \geq s_k$, и произвольных фиксированных различных вершин $y_1, \dots, y_m \in S$ рассмотрим следующее событие:

$$D_{s_1, \dots, s_k}^{\{k\}}(y_1, \dots, y_m) = \bigcap_{i=1}^k \{|\{f_{[i]}(y_1), \dots, f_{[i]}(y_m)\}| = s_i\}.$$

Лемма 2.1. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых $m, s_1, \dots, s_k \in \mathbb{N}$, $n \geq m \geq s_1 \geq \dots \geq s_k$, и любых фиксированных различных $y_1, \dots, y_m \in S$ справедливо равенство

$$\mathbf{P} \left\{ D_{s_1, \dots, s_k}^{\{k\}}(y_1, \dots, y_m) \right\} = q(m, s_1) \prod_{i=1}^{k-1} q(s_i, s_{i+1}),$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$.

Доказательство. Для произвольных $i \in \{1, \dots, k\}$, $a \in \{1, \dots, m\}$ и $b \in \{1, \dots, a\}$ определим событие

$$D^{(i)}(a, b) = \{|\{f_i(1), \dots, f_i(a)\}| = b\},$$

вероятность которого, согласно формуле (2) на с. 10 в [14], равна

$$\begin{aligned} q^{(i)}(a, b) &= \mathbf{P} \left\{ D^{(i)}(a, b) \right\} = \mathbf{P} \left\{ \mu_0(a, n) = n - b \right\} = \\ &= C_n^{n-b} \left(\frac{b}{n} \right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b} \right)^a, \quad (2.32) \end{aligned}$$

где случайная величина $\mu_0(a, n)$ — число пустых ячеек в схеме равновероятных размещений, в которой a частиц независимо друг от друга размещаются в n ячейках.

Поскольку из полученного выражения следует, что $q^{(i)}(a, b)$ не зависят от i , верхний индекс в обозначении $q^{(i)}(a, b)$ опустим.

С учетом (2.32) в силу независимости отображений $f_1, \dots, f_k$ для произвольного $m \in \mathbb{N}$, произвольных фиксированных различных вершин $y_1, \dots, y_m \in S$ и произвольного набора $(s_1, \dots, s_k)$ такого, что $n \geq m \geq s_1 \geq \dots \geq s_k$, получаем искомое равенство

$$\mathbf{P} \left\{ D_{s_1, \dots, s_k}^{\{k\}}(y_1, \dots, y_m) \right\} = q(m, s_1) \prod_{i=1}^{k-1} q(s_i, s_{i+1}).$$

Лемма доказана. □

Лемма 2.1 позволяет вычислить вероятность формирования произвольными фиксированными вершинами $x, y \in S$, $x \neq y$, коллизии в графе $G_{f_{[k]}}$.

Теорема 2.5. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\mathbf{P} \left\{ f_{[k]}(x) = f_{[k]}(y) \right\} = \sum_{\substack{s_1, \dots, s_{k-1}: \\ 2 \geq s_1 \geq \dots \geq s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}),$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n} \right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b} \right)^a$.

Доказательство. Для произвольных фиксированных $x, y \in S$, $x \neq y$, в соответствии с результатом леммы 2.1, имеет место цепочка соотношений

$$\begin{aligned} \mathbf{P} \{f_{[k]}(x) = f_{[k]}(y)\} &= \sum_{\substack{s_1, \dots, s_{k-1}: \\ 2 \geq s_1 \geq \dots \geq s_{k-1}}} \mathbf{P} \left\{ D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(x, y) \right\} = \\ &= \sum_{\substack{s_1, \dots, s_{k-1}: \\ 2 \geq s_1 \geq \dots \geq s_{k-1}}} q(2, s_1) q(s_{k-1}, 1) \prod_{i=1}^{k-2} q(s_i, s_{i+1}) = \\ &= \sum_{\substack{s_1, \dots, s_{k-1}: \\ 2 \geq s_1 \geq \dots \geq s_{k-1}}} \frac{q(2, s_1)}{n^{s_{k-1}-1}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}). \end{aligned}$$

Теорема доказана. □

Замечание 2.8. В силу равноправия вершин из S среднее число коллизий в графе $G_{f_{[k]}}$ определяется величиной $C_n^2 \mathbf{P} \{f_{[k]}(x) = f_{[k]}(y)\}$.

Теорема 2.6. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{x \in f_{[k]}(S)\} &= \frac{1}{n} \sum_{l=1}^n \left(\frac{\binom{n}{l}}{n^l} \right)^k + \\ &+ \sum_{l=1}^{n-2} \sum_{t=1}^{n-l-1} \sum_{m=1}^{n-t-l} (-1)^{m-1} C_{n-1}^m \sum_{\substack{s_1, \dots, s_{k-1}: \\ m \geq s_1 \geq \dots \geq s_{k-1}}} \frac{q(m, s_1)}{n^{s_{k-1}}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}) V_{s_1, \dots, s_{k-1}}^{\{k, m\}}, \end{aligned}$$

где $q(a, b) = C_n^{n-b} \left(\frac{b}{n}\right)^a \sum_{l=0}^b C_b^l (-1)^l \left(1 - \frac{l}{b}\right)^a$, $V_{s_1, \dots, s_{k-1}}^{\{k, m\}}$ определяется соотношением (2.37).

Доказательство. Заметим, что произвольная фиксированная вершина $x \in S$ лежит в множестве $f_{[k]}(S)$ в случаях, когда она либо является циклической в графе $G_{f_{[k]}}$, либо лежит на подходах к циклу и при этом не является висячей.

Таким образом, выполняется равенство

$$\begin{aligned} \{x \in f_{[k]}(S)\} = \\ = \{x \in C(G_{f_{[k]}})\} \cup \bigcup_{l=1}^{n-2} \bigcup_{t=1}^{n-l-1} \left\{x \in H_{f_{[k]}}^{(t,l)}, \left|(f_{[k]})^{-1}(x)\right| \geq 1\right\}, \end{aligned}$$

где под знаком объединения стоят несовместные события. Тогда, переходя в указанном равенстве к вероятностям, получаем

$$\begin{aligned} \mathbf{P}\{x \in f_{[k]}(S)\} = \mathbf{P}\{x \in C(G_{f_{[k]}})\} + \\ + \sum_{l=1}^{n-2} \sum_{t=1}^{n-l-1} \mathbf{P}\left\{x \in H_{f_{[k]}}^{(t,l)}, \left|(f_{[k]})^{-1}(x)\right| \geq 1\right\}. \quad (2.33) \end{aligned}$$

Первое слагаемое в правой части (2.33) определяется выражением (2.13). Рассмотрим отдельно величины, стоящие под знаками суммирования в (2.33), при фиксированных $l \in \{1, \dots, n-2\}$, $t \in \{1, \dots, n-l-1\}$. По формуле включения-исключения в силу равноправия всех вершин $y \in S \setminus \{x\}$

$$\begin{aligned} \mathbf{P}\left\{x \in H_{f_{[k]}}^{(t,l)}, \left|(f_{[k]})^{-1}(x)\right| \geq 1\right\} = \\ = \mathbf{P}\left\{\bigcup_{y \in S \setminus \{x\}} \left\{x \in H_{f_{[k]}}^{(t,l)}, y \in (f_{[k]})^{-1}(x)\right\}\right\} = \\ = \sum_{m=1}^{n-t-l} (-1)^{m-1} C_{n-1}^m \mathbf{P}\left\{\begin{array}{l} x \in H_{f_{[k]}}^{(t,l)}, f_{[k]}(y_1) = \dots = f_{[k]}(y_m) = x, \\ y_1, \dots, y_m \in S \setminus \{x\} \text{ — различные} \end{array}\right\}. \quad (2.34) \end{aligned}$$

Теперь рассмотрим вероятность, стоящую под знаком суммирования в правой части (2.34), при фиксированном значении $m \in \{1, \dots, n-l-t\}$. Для произвольных фиксированных различных $y_1, \dots, y_m \in S \setminus \{x\}$ по формуле

полной вероятности имеем

$$\begin{aligned}
\mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)}, f_{[k]}(y_1) = \dots = f_{[k]}(y_m) = x \right\} &= \\
&= \sum_{\substack{s_1, \dots, s_{k-1} : \\ m \geq s_1 \geq \dots \geq s_{k-1}}} \mathbf{P} \left\{ D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(y_1, \dots, y_m), f_{[k]}(y_1) = x, x \in H_{f[k]}^{(t,l)} \right\} = \\
&= \sum_{\substack{s_1, \dots, s_{k-1} : \\ m \geq s_1 \geq \dots \geq s_{k-1}}} \mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \mid D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(y_1, \dots, y_m), f_{[k]}(y_1) = x \right\} \times \\
&\quad \times \mathbf{P} \left\{ D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(y_1, \dots, y_m), f_{[k]}(y_1) = x \right\}. \quad (2.35)
\end{aligned}$$

При этом в силу независимости отображений $f_1, \dots, f_k$ с учетом леммы 2.1

$$\begin{aligned}
\mathbf{P} \left\{ D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(y_1, \dots, y_m), f_{[k]}(y_1) = x \right\} &= \\
&= \frac{1}{n^{s_{k-1}}} \mathbf{P} \left\{ D_{s_1, \dots, s_{k-1}}^{\{k-1\}}(y_1, \dots, y_m) \right\} = \frac{q(m, s_1)}{n^{s_{k-1}}} \prod_{i=1}^{k-2} q(s_i, s_{i+1}). \quad (2.36)
\end{aligned}$$

Далее заметим, что вычисление условной вероятности, стоящей под знаком суммирования в правой части (2.35), проводится аналогично вычислениям, представленным в теореме 2.4, с поправкой на наличие дополнительных $s_1, \dots, s_{k-1}, m$ вершин во множествах $f_{[1]}(S), \dots, f_{[k]}(S)$ соответственно. Таким образом,

$$\begin{aligned}
V_{s_1, \dots, s_{k-1}}^{\{k, m\}} &= \mathbf{P} \left\{ x \in H_{f[k]}^{(t,l)} \mid D_{s_1, \dots, s_{k-1}, 1}^{\{k\}}(y_1, \dots, y_m), f_{[k]}(y_1) = x \right\} = \\
&= \frac{1}{n} \prod_{i=m+1}^{t+l+m-1} \left(1 - \frac{i}{n} \right) \cdot \prod_{i=1}^{k-1} \prod_{j=s_i+1}^{t+l+s_i-2} \left(1 - \frac{j}{n} \right) \cdot \sum_{v=0}^{k-1} \prod_{u=1}^v \left(1 - \frac{t+l+s_u-1}{n} \right). \quad (2.37)
\end{aligned}$$

Подставив (2.36) и (2.37) в (2.35), а затем полученный результат — в (2.34) и далее в (2.33), получим искомую формулу. Теорема доказана. $\square$

Следствие 2.11. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда

$$\mathbf{E} |f_{[k]}(S)| = n \mathbf{P} \{x \in f_{[k]}(S)\}.$$

Замечание 2.9. Из равенства $S = T_{f_{[k]}} \cup f_{[k]}(S)$, где $T_{f_{[k]}} \cap f_{[k]}(S) = \emptyset$, вытекает выражение для вероятности попадания произвольной вершины $x \in S$ во множество висячих вершин в графе $G_{f_{[k]}}$:

$$\mathbf{P}\{x \in T_{f_{[k]}}\} = 1 - \mathbf{P}\{x \in f_{[k]}(S)\}.$$

При этом в силу равноправия вершин из S выполняется следующее соотношение для среднего числа висячих вершин в графе $G_{f_{[k]}}$:

$$\mathbf{E} |T_{f_{[k]}}| = n \mathbf{P}\{x \in T_{f_{[k]}}\} = n - n \mathbf{P}\{x \in f_{[k]}(S)\}.$$

2.5 Инцидентность вершин одной компоненте связности в графе отображения $f_{[k]}$

Для вычисления вероятности попадания вершин из S в одну компоненту связности графа $G_{f_{[k]}}$ докажем ряд вспомогательных утверждений.

Выделим в исходном множестве S некоторое подмножество вершин $S' = \{y_1, \dots, y_r\} \subseteq S$, где $r < n$. Для данного множества вычислим вероятность события, заключающегося в том, что отрезок аперiodичности $\mathcal{R}_{f_{[k]}}(x)$ произвольной вершины $x \in S \setminus S'$ не проходит через вершины множества S' .

Теорема 2.7. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \setminus S'$ и любых $r \in \{1, \dots, n-1\}$, $S' \subseteq S$, $|S'| = r$, и $z \in \{1, \dots, n\}$ справедливо равенство

$$\begin{aligned} \mathbf{P} \{ \tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \emptyset \} = \\ = \left(1 - \left(1 - \frac{z}{n} \right) \left(1 - \frac{z-1}{n} \right)^{k-1} \right) \left(\frac{(n)_{z-1}}{n^{z-1}} \right)^{k-1} \frac{(n)_{r+z}}{n^{z-1} (n)_{r+1}}. \end{aligned} \quad (2.36)$$

Доказательство. Зафиксируем множество $S' = \{y_1, \dots, y_r\} \subseteq S$ и произвольную вершину $x \in S \setminus S'$. Тогда для любых различных фиксированных вершин $x_1, \dots, x_{z-1} \in S \setminus \{S' \cup \{x\}\}$ справедливо равенство

$$\mathbf{P} \{ \tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' = \emptyset \} = (n - r - 1)_{z-1} \mathbf{P} \left\{ R_{(x, x_1, \dots, x_{z-1})}^{[k]} \right\}, \quad (2.37)$$

где $(n - r - 1)_{z-1}$ — число всех возможных траекторий $x_1, \dots, x_{z-1}$, составленных из различных вершин множества $S \setminus \{S' \cup \{x\}\}$.

Подставив (2.8) в (2.37), получим искомое выражение. Теорема доказана. $\square$

Замечание 2.10. Из формул (2.5) и (2.36) вытекает выражение для величины $\mathbf{P} \{ \tau_{f_{[k]}}(x) = z, \mathcal{R}_{f_{[k]}}(x) \cap S' \neq \emptyset \}$.

Следствие 2.12. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любого фиксированного $x \in S \setminus S'$ и любых $r \in \{1, \dots, n-1\}$, $S' \subseteq S$, $|S'| = r$, справедливо равенство

$$\begin{aligned} \mathbf{P} \{ \mathcal{R}_{f_{[k]}}(x) \cap S' = \emptyset \} = \\ = \sum_{z=0}^{n-r-1} \left(1 - \left(1 - \frac{z+1}{n} \right) \left(1 - \frac{z}{n} \right)^{k-1} \right) \left(\frac{(n)_z}{n^z} \right)^{k-1} \frac{(n)_{r+z+1}}{n^z (n)_{r+1}}. \end{aligned} \quad (2.38)$$

Отметим, что формулы (2.36) и (2.38) могут быть использованы для оценки среднего числа сообщений, которые могут быть зашифрованы при помощи последовательности ключей, представляющей собой неповторную выборку

элементов ключевого множества, при наличии дополнительной информации о слабых или ранее выработанных ключах.

Далее для случая $r = 1$ вычислим вероятность того, что вершина $y = y_1 \in S$, соответствующая некоторому ключу, попадет в компоненту связности $\mathcal{K}_{f_{[k]}}(x)$, где $x \in S \setminus \{y\}$ — произвольная фиксированная вершина.

Теорема 2.8. Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, справедливо равенство

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f_{[k]}}(x)\} = \\ = 1 - \sum_{z=0}^{n-2} \left(1 - \left(1 - \frac{z+1}{n}\right) \left(1 - \frac{z}{n}\right)^{k-1}\right) \left(\frac{(n)_z}{n^z}\right)^k \frac{C_{n-z}^2}{C_n^2} + \\ + \sum_{z=1}^{n-1} \sum_{u=0}^{n-z-1} \chi_k(z, u), \quad (2.39) \end{aligned}$$

где

$$\begin{aligned} \chi_k(z, u) = \left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k \left(\sum_{t=1}^k \frac{z^2}{n(n-1)} \left(1 - \frac{z+u}{n}\right)^t + \right. \\ + \sum_{s=2}^k \sum_{t=1}^{s-1} \frac{z(z-1)}{n(n-1)} \left(1 - \frac{z+u-1}{n}\right)^{s-k} \left(1 - \frac{z+u}{n}\right)^t + \\ \left. + \sum_{t=1}^{k-1} \sum_{s=1}^t \frac{(z-1)^2}{n(n-1)} \left(1 - \frac{z+u-1}{n}\right)^{t-k} \left(1 - \frac{z+u}{n}\right)^s\right). \quad (2.40) \end{aligned}$$

Доказательство. Для произвольной фиксированной пары вершин $x, y \in S$, $x \neq y$, выполняется равенство событий

$$\begin{aligned} \{y \in \mathcal{K}_{f_{[k]}}(x)\} = \{y \in \mathcal{R}_{f_{[k]}}(x)\} \cup \\ \cup \bigcup_{z=1}^{n-1} \bigcup_{u=0}^{n-z-1} \left\{ \tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x) \right\}, \end{aligned}$$

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

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{K}_{f_{[k]}}(x)\} &= \mathbf{P} \{y \in \mathcal{R}_{f_{[k]}}(x)\} + \\ &+ \sum_{z=1}^{n-1} \sum_{u=0}^{n-z-1} \mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x) \right\}. \end{aligned} \quad (2.41)$$

Выражение для первого слагаемого в (2.41) следует из (2.38) при $r = 1$:

$$\begin{aligned} \mathbf{P} \{y \in \mathcal{R}_{f_{[k]}}(x)\} &= 1 - \mathbf{P} \{y \notin \mathcal{R}_{f_{[k]}}(x)\} = \\ &= 1 - \sum_{z=0}^{n-2} \left(1 - \left(1 - \frac{z+1}{n} \right) \left(1 - \frac{z}{n} \right)^{k-1} \right) \left(\frac{(n)_z}{n^z} \right)^k \frac{C_{n-z}^2}{C_n^2}. \end{aligned} \quad (2.42)$$

Вычислим вероятность, стоящую под знаками суммирования в (2.41) при фиксированных значениях $z \in \{1, \dots, n-1\}$ и $u \in \{0, \dots, n-z-1\}$. Для произвольного $s \in \{1, \dots, k\}$ и указанных значений z, u определим события

$$\begin{aligned} A_{z,s}^{\{x\}} &= \\ &= \left\{ \min_{j \in \{1, \dots, k\}} \left\{ j: f_{[j]} \left(f_{[k]}^{z-1}(x) \right) \in \left\{ f_{[j]} \left(f_{[k]}^m(x) \right), m = 0, \dots, z-2 \right\} \right\} = s \right\}, \\ B_{u,s}^{\{x,y\}} &= \\ &= \left\{ \min_{j \in \{1, \dots, k\}} \left\{ j: f_{[j]} \left(f_{[k]}^u(y) \right) \in \left\{ \begin{array}{c} f_{[i]} \left(f_{[k]}^m(x) \right), m = 0, \dots, z-1, \\ i = 1, \dots, k \end{array} \right\} \right\} = s \right\}. \end{aligned}$$

Так, событие $A_{z,s}^{\{x\}}$ заключается в том, что траектория, начинающаяся в вершине x , зацикливается на z -м шаге итерационной процедуры формирования вершин в графе $G_{f_{[k]}}$ при действии отображения $f_{[s]}$, а событие $B_{u,s}^{\{x,y\}}$ — в том, что траектория, начинающаяся в вершине $y \notin \mathcal{R}_{f_{[k]}}(x)$, входит в отрезок апериодичности $\mathcal{R}_{f_{[k]}}(x)$ длины z на $(u+1)$ -м шаге соответствующей процедуры при действии отображения $f_{[s]}$.

С учетом введенных обозначений справедливо равенство

$$\left\{ \tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x) \right\} = \\ = \bigcup_{s=1}^k \bigcup_{t=1}^k \left\{ \tau_{f_{[k]}}(x) = z, A_{z,s}^{\{x\}}, B_{u,t}^{\{x,y\}}, \right. \\ \left. f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x) \right\}.$$

Вычислим вероятность $p_{z,u,s,t}$ события, стоящего под знаками объединения, при фиксированных значениях $s \in \{1, \dots, k\}$, $t \in \{1, \dots, k\}$.

В случае $s = t = k$:

$$p_{z,u,k,k} = \\ = \frac{z}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-1} \left(1 - \frac{i}{n}\right)^{k-1} \times \frac{z}{n} \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=z}^{z+u} \left(1 - \frac{i}{n}\right)^{k-1} = \\ = \frac{z^2}{n^2} \prod_{i=2}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z+u} \left(1 - \frac{i}{n}\right)^{k-1} = \frac{z^2}{n(n-1)} \left(\frac{(n)_{z+u+1}}{n^{z+u+1}} \right)^k, \quad (2.43)$$

где произведение, стоящее до знака « $\times$ » в правой части первого равенства, соответствует вероятности формирования отрезка аперидичности $\mathcal{R}_{f_{[k]}}(x)$ длины z при действии отображения $f_{[k]}$, а произведение, стоящее после знака « $\times$ », — вероятности вхождения траектории, начинающейся в вершине $y \notin \mathcal{R}_{f_{[k]}}(x)$, в отрезок аперидичности $\mathcal{R}_{f_{[k]}}(x)$ на $(u+1)$ -м шаге итерационной процедуры формирования вершин в графе $G_{f_{[k]}}$ при действии отображения $f_{[k]}$. Для остальных случаев будем записывать выражения в таком же порядке.

В случае $s = k, t < k$:

$$p_{z,u,k,t} = \frac{z}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-1} \left(1 - \frac{i}{n}\right)^{k-1} \times \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \cdot \\ \cdot \frac{z}{n} \prod_{i=z}^{z+u-1} \left(1 - \frac{i}{n}\right)^{k-1} \left(1 - \frac{z+u}{n}\right)^{t-1} = \frac{z^2}{n(n-1)} \left(\frac{(n)_{z+u}}{n^{z+u}} \right)^k \left(1 - \frac{z+u}{n}\right)^t. \quad (2.44)$$

В случае $s < k$, $t = k$:

$$\begin{aligned}
p_{z,u,s,k} &= \frac{z-1}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n}\right)^{k-1} \left(1 - \frac{z-1}{n}\right)^{s-1} \times \\
&\quad \times \frac{z}{n} \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=z}^{z+u} \left(1 - \frac{i}{n}\right)^{s-1} \prod_{i=z-1}^{z+u-1} \left(1 - \frac{i}{n}\right)^{k-s} = \\
&= \frac{z(z-1)}{n(n-1)} \left(\frac{(n)_{z+u}}{n^{z+u}}\right)^k \left(1 - \frac{z+u}{n}\right)^s. \quad (2.45)
\end{aligned}$$

В случае $t < s < k$:

$$\begin{aligned}
p_{z,u,s,t} &= \frac{z-1}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n}\right)^{k-1} \left(1 - \frac{z-1}{n}\right)^{s-1} \times \\
&\quad \times \frac{z}{n} \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=z}^{z+u} \left(1 - \frac{i}{n}\right)^{t-1} \prod_{i=z}^{z+u-1} \left(1 - \frac{i}{n}\right)^{s-t} \prod_{i=z-1}^{z+u-2} \left(1 - \frac{i}{n}\right)^{k-s} = \\
&= \frac{z(z-1)}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}}\right)^k \left(1 - \frac{z+u-1}{n}\right)^s \left(1 - \frac{z+u}{n}\right)^t. \quad (2.46)
\end{aligned}$$

В случае $s < t < k$:

$$\begin{aligned}
p_{z,u,s,t} &= \frac{z-1}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n}\right)^{k-1} \left(1 - \frac{z-1}{n}\right)^{s-1} \times \\
&\quad \times \frac{z-1}{n} \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=z}^{z+u} \left(1 - \frac{i}{n}\right)^{s-1} \prod_{i=z-1}^{z+u-1} \left(1 - \frac{i}{n}\right)^{t-s} \prod_{i=z-1}^{z+u-2} \left(1 - \frac{i}{n}\right)^{k-t} = \\
&= \frac{(z-1)^2}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}}\right)^k \left(1 - \frac{z+u-1}{n}\right)^t \left(1 - \frac{z+u}{n}\right)^s. \quad (2.47)
\end{aligned}$$

В случае $t = s < k$:

$$\begin{aligned}
p_{z,u,s,t} &= \frac{z-1}{n} \prod_{i=2}^z \left(1 - \frac{i}{n}\right) \prod_{i=1}^{z-2} \left(1 - \frac{i}{n}\right)^{k-1} \left(1 - \frac{z-1}{n}\right)^{s-1} \times \\
&\quad \times \frac{z-1}{n} \prod_{i=z+1}^{z+u} \left(1 - \frac{i}{n}\right) \prod_{i=z}^{z+u} \left(1 - \frac{i}{n}\right)^{t-1} \prod_{i=z-1}^{z+u-2} \left(1 - \frac{i}{n}\right)^{k-t} = \\
&= \frac{(z-1)^2}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}}\right)^k \left(1 - \frac{z+u-1}{n}\right)^t \left(1 - \frac{z+u}{n}\right)^t. \quad (2.48)
\end{aligned}$$

Таким образом, для вероятности, стоящей под знаками суммирования в (2.41) и равной сумме (2.43) — (2.48), получаем равенство

$$\begin{aligned}
\mathbf{P} \left\{ \tau_{f_{[k]}}(x) = z, f_{[k]}^u(y) \notin \mathcal{R}_{f_{[k]}}(x), f_{[k]}^{u+1}(y) \in \mathcal{R}_{f_{[k]}}(x) \right\} = \\
= \frac{z^2}{n(n-1)} \left(\frac{(n)_{z+u+1}}{n^{z+u+1}} \right)^k + \sum_{t=1}^{k-1} \frac{z^2}{n(n-1)} \left(\frac{(n)_{z+u}}{n^{z+u}} \right)^k \left(1 - \frac{z+u}{n} \right)^t + \\
+ \sum_{s=1}^{k-1} \frac{z(z-1)}{n(n-1)} \left(\frac{(n)_{z+u}}{n^{z+u}} \right)^k \left(1 - \frac{z+u}{n} \right)^s + \\
+ \sum_{s=2}^{k-1} \sum_{t=1}^{s-1} \frac{z(z-1)}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}} \right)^k \left(1 - \frac{z+u-1}{n} \right)^s \left(1 - \frac{z+u}{n} \right)^t + \\
+ \sum_{t=2}^{k-1} \sum_{s=1}^{t-1} \frac{(z-1)^2}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}} \right)^k \left(1 - \frac{z+u-1}{n} \right)^t \left(1 - \frac{z+u}{n} \right)^s + \\
+ \sum_{t=1}^{k-1} \frac{(z-1)^2}{n(n-1)} \left(\frac{(n)_{z+u-1}}{n^{z+u-1}} \right)^k \left(1 - \frac{z+u-1}{n} \right)^t \left(1 - \frac{z+u}{n} \right)^t. \quad (2.49)
\end{aligned}$$

Сгруппировав слагаемые в (2.49) и затем подставив результат в (2.41), получим с учетом (2.42) искомое выражение. Теорема доказана. $\square$

Замечание 2.11. При $k = 1$ выражение (2.39) принимает вид

$$\mathbf{P} \{y \in \mathcal{K}_f(x)\} = 1 - \sum_{z=1}^{n-1} \frac{z}{n-1} \frac{(n)_{z+1}}{n^{z+1}} + \sum_{z=1}^{n-1} \sum_{u=1}^{n-z} \frac{z^2}{n(n-1)} \frac{(n)_{z+u}}{n^{z+u}} \quad (2.50)$$

и совпадает с (1.61). Действительно, для доказательства указанного факта достаточно показать, что выполняется равенство

$$\sum_{z=1}^n \frac{z(z-1)}{n(n-1)} \frac{(n)_z}{n^z} = 1 - \sum_{z=1}^{n-1} \frac{z}{n-1} \frac{(n)_{z+1}}{n^{z+1}}. \quad (2.51)$$

Левую часть равенства (2.51) с использованием соотношений

$$\mathbf{P} \{ \tau_f(x) = z \} = \frac{z}{n} \frac{(n)_z}{n^z}, \quad \mathbf{P} \{ \tau_f(x) > z \} = \frac{(n)_{z+1}}{n^{z+1}},$$

$$\mathbf{E}\tau_f(x) = \sum_{z=1}^n z \mathbf{P}\{\tau_f(x) = z\} = \sum_{z=0}^{n-1} \mathbf{P}\{\tau_f(x) > z\}$$

преобразуем следующим образом:

$$\begin{aligned} \sum_{z=1}^n \frac{z(z-1)}{n(n-1)} \frac{(n)_z}{n^z} &= \sum_{z=1}^n \frac{z^2}{n(n-1)} \frac{(n)_z}{n^z} - \sum_{z=1}^n \frac{z}{n(n-1)} \frac{(n)_z}{n^z} = \\ &= \frac{1}{n-1} \sum_{z=1}^n z \mathbf{P}\{\tau_f(x) = z\} - \frac{1}{n-1} \sum_{z=1}^n \mathbf{P}\{\tau_f(x) = z\} = \\ &= \frac{1}{n-1} \sum_{z=0}^{n-1} \frac{(n)_{z+1}}{n^{z+1}} - \frac{1}{n-1} = \frac{1}{n-1} \sum_{z=1}^{n-1} \frac{(n)_{z+1}}{n^{z+1}}. \end{aligned}$$

В свою очередь, правая часть (2.51), в соответствии с формулой

$$1 = \sum_{z=1}^n \mathbf{P}\{\tau_f(x) = z\} = \sum_{z=1}^n \frac{z}{n} \frac{(n)_z}{n^z},$$

представляется в виде

$$\begin{aligned} 1 - \sum_{z=1}^{n-1} \frac{z}{n-1} \frac{(n)_{z+1}}{n^{z+1}} &= \sum_{z=1}^n \frac{z}{n} \frac{(n)_z}{n^z} - \sum_{z=1}^{n-1} \frac{z}{n-1} \frac{(n)_{z+1}}{n^{z+1}} = \\ &= \sum_{z=0}^{n-1} \frac{z+1}{n} \frac{(n)_{z+1}}{n^{z+1}} - \sum_{z=0}^{n-1} \frac{z}{n-1} \frac{(n)_{z+1}}{n^{z+1}} = \sum_{z=0}^{n-2} \frac{n-z-1}{n(n-1)} \frac{(n)_{z+1}}{n^{z+1}} = \\ &= \frac{1}{n-1} \sum_{z=0}^{n-2} \frac{(n)_{z+2}}{n^{z+2}} = \frac{1}{n-1} \sum_{z=1}^{n-1} \frac{(n)_{z+1}}{n^{z+1}}, \end{aligned}$$

что, в конечном итоге, и доказывает равенство выражений (1.61) и (2.50).

Замечание 2.12. Для средней мощности компоненты связности произвольной фиксированной вершины $x \in S$ в графе $G_{f[k]}$ справедливо равенство

$$\mathbf{E}|\mathcal{K}_{f[k]}(x)| = (n-1) \mathbf{P}\{y \in \mathcal{K}_{f[k]}(x)\} + 1.$$

2.6 Прообразы вершин в графе отображения

$$f_{[k]}$$

Для произвольного фиксированного $x \in S$ и произвольного $r \in \mathbb{N}$ через $(f_{[k]})^{-r}(x)$ обозначим множество $\{y \in S: f_{[k]}^r(y) = x\}$.

Дополнительно для любых $j, r \in \mathbb{N}$ определим

$$Q_r = \{m \in \mathbb{N}: m|r\}. \quad (2.52)$$

Заметим, что для произвольного фиксированного $x \in S$ вероятность события $\{y \in (f_{[k]})^{-r}(x)\}$ зависит от выбора $y \in S$, а именно, от выполнения и невыполнения условия $y = x$. Так, в частности, в случае $y = x$ выполняется равенство

$$\{x \in (f_{[k]})^{-r}(x)\} = \bigcup_{m \in Q_r} \{x \in C_m(G_{f_{[k]}})\},$$

где под знаком объединения стоят несовместные события, и поэтому переходя к вероятностям, с учетом (2.12) получаем

$$\mathbf{P} \{x \in (f_{[k]})^{-r}(x)\} = \frac{1}{n} \sum_{m \in Q_r} \left(\frac{(n)_m}{n^m} \right)^k.$$

В случае $y \neq x$ справедлив следующий результат.

Теорема 2.9. [28] Пусть $k \in \mathbb{N}$ — произвольное, случайные отображения $f_1, \dots, f_k$ независимы и имеют распределение (1.1) на $\mathfrak{S}$. Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любого $r \in \{1, \dots, n\}$ справедливо равенство

$$\mathbf{P} \{y \in (f_{[k]})^{-r}(x)\} = \frac{1}{n} \left(1 - \frac{1}{n-1} \sum_{z \in Q_r \setminus \{1\}} \left(\frac{(n)_z}{n^z} \right)^k \right),$$

где Q_r определяется соотношением (2.52).

Доказательство. Для произвольных фиксированных $x, y \in S$, $x \neq y$, по формуле полной вероятности

$$\begin{aligned} \mathbf{P} \left\{ y \in (f_{[k]})^{-r}(x) \right\} &= \sum_{z \in Q_r \setminus \{1\}} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x \right\} + \\ &+ \sum_{z \in \overline{Q}_r} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x \right\} + \\ &+ \sum_{z=r+1}^n \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x \right\}, \quad (2.53) \end{aligned}$$

где $\overline{Q}_r = \{1, \dots, r\} \setminus Q_r$.

Заметим, что в случае $z \in Q_r \setminus \{1\}$

$$\mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x, y \in C(G_{f_{[k]}}) \right\} = 0.$$

Тогда для величин, стоящих под первым знаком суммирования в (2.53), имеем

$$\begin{aligned} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x \right\} &= \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x, y \notin C(G_{f_{[k]}}) \right\} = \\ &= \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, y \notin C(G_{f_{[k]}}) \right\} \mathbf{P} \left\{ f_{[k]}^r(y) = x \mid \tau_{f_{[k]}}(y) = z, y \notin C(G_{f_{[k]}}) \right\} = \\ &= (\mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\} - \mathbf{P} \left\{ y \in C_z(G_{f_{[k]}}) \right\}) \frac{(n-2)_{z-2}(z-1)}{(n-1)_{z-1}(z-1)} = \\ &= \frac{1}{n-1} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\} - \frac{1}{n-1} \mathbf{P} \left\{ y \in C_z(G_{f_{[k]}}) \right\}. \quad (2.54) \end{aligned}$$

В случае $z \in \overline{Q}_r \cup \{r+1, \dots, n\}$ на расположение вершины $y \in \mathcal{K}_{f_{[k]}}(x)$ никаких дополнительных ограничений не накладывается, и поэтому

$$\begin{aligned} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z, f_{[k]}^r(y) = x \right\} &= \\ &= \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\} \mathbf{P} \left\{ f_{[k]}^r(y) = x \mid \tau_{f_{[k]}}(y) = z \right\} = \\ &= \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\} \frac{(n-2)_{z-2}}{(n-1)_{z-1}} = \frac{1}{n-1} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\}. \quad (2.55) \end{aligned}$$

Подставив выражения (2.54) и (2.55) в (2.53), с учетом равенств (2.1) и (2.12) получим искомую формулу

$$\begin{aligned}
\mathbf{P} \left\{ y \in (f_{[k]})^{-r}(x) \right\} &= \\
&= \frac{1}{n-1} \left(\sum_{z=2}^n \mathbf{P} \left\{ \tau_{f_{[k]}}(y) = z \right\} - \sum_{z \in Q_r \setminus \{1\}} \mathbf{P} \left\{ y \in C_z(G_{f_{[k]}}) \right\} \right) = \\
&= \frac{1}{n-1} \mathbf{P} \left\{ \tau_{f_{[k]}}(y) > 1 \right\} - \frac{1}{n-1} \sum_{z \in Q_r \setminus \{1\}} \mathbf{P} \left\{ y \in C_z(G_{f_{[k]}}) \right\} = \\
&= \frac{1}{n} \left(1 - \frac{1}{n-1} \sum_{z \in Q_r \setminus \{1\}} \left(\frac{(n)_z}{n^z} \right)^k \right).
\end{aligned}$$

Теорема доказана. $\square$

Замечание 2.13. Для среднего числа прообразов произвольной фиксированной вершины $x \in S$ в графе $G_{f_{[k]}}$ в силу равноправия вершин из S справедлива цепочка соотношений

$$\begin{aligned}
\mathbf{E} \left| (f_{[k]})^{-r}(x) \right| &= \mathbf{E} \sum_{y \in S} I \left\{ y \in (f_{[k]})^{-r}(x) \right\} = \\
&= (n-1) \mathbf{P} \left\{ y \in (f_{[k]})^{-r}(x) \right\} + \mathbf{P} \left\{ x \in (f_{[k]})^{-r}(x) \right\}.
\end{aligned}$$

2.7 Выводы

В главе 2 диссертации найдено точное распределение длины отрезка аперидичности случайной вершины в графе k -кратной итерации независимых равновероятных отображений конечного множества в себя, доказано, что распределение его нормированной длины сходится к распределению Рэлея с модой $\sigma = \frac{1}{\sqrt{2k}}$, установлен ряд неравенств для связанных с отрезком аперидичности локальных вероятностей. Оценено среднее число циклических

вершин в графе $G_{f_{[k]}}$. Изучено множество слоев и получен ряд оценок для вероятности инцидентности произвольной фиксированной вершины заданному слою графа $G_{f_{[k]}}$. Найдены математические ожидания числа элементов образа исходного множества вершин при действии случайного отображения $f_{[k]}$, а также числа вершин, не имеющих прообразы. Получены явные формулы для вероятностей инцидентности указанным множествам фиксированной вершины. Выписаны формулы для распределения длины отрезка аперидичности произвольной фиксированной вершины, не проходящего через заданное множество вершин, вероятностей инцидентности любых двух фиксированных вершин одной компоненте связности и попадания произвольной фиксированной вершины в множество прообразов другой произвольной фиксированной вершины в графе $G_{f_{[k]}}$. Вычислена вероятность формирования коллизии произвольной парой фиксированных вершин в графе $G_{f_{[k]}}$.

Результаты настоящей главы описывают строение и вероятностные свойства графа $G_{f_{[k]}}$, $k \in \mathbb{N}$, существенно используемые в рамках синтеза и анализа итерационных АМЗИ в части формирования ключей, в принцип функционирования которых заложено применение различных преобразований или источника случайности в каждый отдельный такт их работы.

Заключение

Исследования, проведенные в рамках настоящей диссертации, направлены на развитие математического аппарата, позволяющего адекватно описывать современные итерационные АМЗИ, а также обосновывать выбор значений параметров соответствующих алгоритмов, гарантирующих защиту обрабатываемой с их использованием информации.

В диссертации исследованы структуры графов кратной итерации одного равновероятного случайного отображения конечного множества в себя и композиции нескольких независимых равновероятных случайных отображений конечного множества в себя, а также их вероятностные характеристики и свойства, которые могут быть использованы при моделировании и обосновании теоретической стойкости итерационных АМЗИ при выработке производных ключей.

Перспективными направлениями дальнейших исследований модификаций равновероятных случайных отображений конечного множества в себя в области защиты информации являются:

- исследование свойств и характеристик кратной итерации композиции нескольких равновероятных случайных отображений как объекта моделирования алгоритмов выработки производных ключей, использующих различные преобразования, определяемые некоторым источником случайности в каждый такт их работы, и реализующих последовательность

производных ключей на основе тактов, отобранных с некоторым фиксированным периодом,

- построение и исследование математических моделей итерационных древовидных режимов работы хеш-функций, построенных на основе случайных отображений и обеспечивающих эффективную обработку больших объемов данных, а также допускающих реализацию в распределенных вычислительных системах и сетях,
- исследования, связанные с оценкой качества псевдослучайных последовательностей, формируемых с использованием итерационных АМЗИ, в том числе построение соответствующих статистических критериев.

Список сокращений и условных обозначений

$\mathbb{N}$	множество натуральных чисел;
$\mathbb{Z}$	множество целых чисел;
$f: S \rightarrow S$	отображение множества S в множество S ;
$f(x) \sim g(x), x \rightarrow x_0$	эквивалентные функции $f(x)$ и $g(x)$ при $x \rightarrow x_0$;
$g(x) = o(f(x)), x \rightarrow x_0$	бесконечная малость $g(x)$ относительно $f(x)$ при $x \rightarrow x_0$;
S^m	m -я декартова степень множества S , $m \in \mathbb{N}$;
$ S $	мощность множества S ;
$X \cup Y$	объединение множеств X и Y ;
$X \cap Y$	пересечение множеств X и Y ;
V_n	множество двоичных векторов длины $n \in \mathbb{N}$;
$a b$	конкатенация векторов a и b произвольной длины;
$[z]$	наибольшее целое число, меньшее или равное z ;
$]z[$	наименьшее целое число, большее или равное z ;
$(x)_k$	k -я факториальная степень $x \in \mathbb{R}$, $k \in \mathbb{N} \cup \{0\}$;
E	символ математического ожидания;
D	символ дисперсии.

Список литературы

1. Арбеков И. М., “Критерии секретности ключа”, *Математические вопросы криптографии*, **7:1** (2016), 39-56.
2. Arbekov I. M., “Lower bounds for the practical secrecy of a key”, *Математические вопросы криптографии*, **8:2** (2017), 29-38.
3. Богданов Д. С., Миронкин В. О., “О коллизиях отображений, построенных на основе случайной подстановки”, *Обозрение прикладной и промышленной математики*, **25:1** (2018), 64-66.
4. Вадзинский Р. Н., *Справочник по вероятностным распределениям*, СПб. : Наука, 2001, 295 с.
5. “Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента РФ № 646 от 5 декабря 2016 года”.
6. Зубков А. М., “Вычисление распределений характеристик чисел компонент и циклических точек случайного отображения”, *Математические вопросы криптографии*, **1:2** (2010), 5-18.
7. Зубков А. М., Миронкин В. О., “Распределение длины отрезка апериодичности в графе k-кратной итерации случайного равновероятного отображения”, *Математические вопросы криптографии*, **8:4** (2017), 63-74.

8. Зубков А. М., Серов А. А., “Совокупность образов подмножества конечного множества при итерациях случайных отображений”, *Дискретная математика*, **26**:4 (2014), 43-50.
9. Зубков А. М., Серов А. А., “Предельная теорема для мощности образа подмножества при композиции случайных отображений”, *Дискретная математика*, **29**:1 (2017), 17-26.
10. Зубков А. М., Серов А. А., “Оценки среднего размера образа подмножества при композиции случайных отображений”, *Дискретная математика*, **30**:2 (2018), 27-36.
11. Зубков А. М., Шибанов О. К., “Время до объединения всех частиц при равновероятных размещениях по последовательности слоев ячеек”, *Матем. заметки*, **85**:3 (2009), 373-381.
12. Колчин В. Ф., *Случайные отображения*, М.: Наука, 1984, 208 с.
13. Колчин В. Ф., *Случайные графы (2-е изд.)*, М.: ФИЗМАТЛИТ, 2004, 256 с.
14. Колчин В. Ф., Севастьянов Б. А., Чистяков В. П., *Случайные размещения*, М.: Наука, 1976, 224 с.
15. Лагутин М. Б., *Наглядная математическая статистика: учебное пособие (2-е изд.)*, М.: БИНОМ. Лаборатория знаний, 2009, 472 с.
16. Лось А. Б., Нестеренко А. Ю., Рожков М. И., *Криптографические методы защиты информации: учебник для академического бакалавриата*, М.: Издательство Юрайт, 2018, 473 с.
17. Миронкин В. О., “Исследование свойств и характеристик степени случайного отображения”, *Обзорные прикладной и промышленной математики*

ки, **21**:1 (2014), 70-73.

18. Миронкин В. О., “Вероятностные характеристики слоев в графе случайного отображения”, *Обзорные прикладной и промышленной математики*, **22**:1 (2015), 80-82.
19. Миронкин В. О., “Вероятность коллизии двух случайных точек для степени случайного отображения”, *Обзорные прикладной и промышленной математики*, **22**:4 (2015), 403-409.
20. Миронкин В. О., “Совместная вероятность длин отрезков апериодичности двух вершин в графе степени случайного отображения”, *Обзорные прикладной и промышленной математики*, **22**:4 (2015), 482-484.
21. Миронкин В. О., “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”, *Проблемы информационной безопасности. Компьютерные системы*, 2015, № 4, 140-146.
22. Миронкин В. О., “Об особенностях строения графа степени случайного отображения”, *Обзорные прикладной и промышленной математики*, **23**:1 (2016), 57-62.
23. Миронкин В. О., “Об оценках распределения длины отрезка апериодичности в графе k-кратной итерации равновероятного случайного отображения”, *Прикладная дискретная математика*, **42** (2018), 6-17.
24. Миронкин В. О., “Слои в графе k-кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **10**:1 (2019), 73-82.

25. Миронкин В. О., “Распределение длины отрезка аperiodичности в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **10**:3 (2019), 89-99.
26. Миронкин В. О., “Коллизии и инцидентность вершин компонентам в графе k -кратной итерации равновероятного случайного отображения”, *Дискретная математика*, **31**:4 (2019), 38-52.
27. Миронкин В. О., “Слои в графе композиции независимых равновероятных случайных отображений”, *Математические вопросы криптографии*, **11**:1 (2020), 101-114.
28. Миронкин В. О., “Об образах и прообразах в графе композиции независимых равновероятных случайных отображений”, *Прикладная дискретная математика*, **49** (2020), 5-17.
29. Миронкин В. О., Михайлов В. Г., “О множестве образов k -кратной итерации равновероятного случайного отображения”, *Математические вопросы криптографии*, **9**:3 (2018), 99-108.
30. Михайлов В. Г., “О повторяемости состояний датчика псевдослучайных чисел при его многократном использовании”, *Теор. вероятн. и её примен.*, **40**:4 (1995), 786-797.
31. Михайлов В. Г., “Исследование комбинаторно-вероятностной модели автоматов из регистров с неравномерным движением”, *Труды по дискретной математике*, 2002, 139-149.
32. Михайлов В. Г., “Исследование числа циклических точек автомата из регистров с неравномерным движением”, *Труды по дискретной математике*, 2002, 167-172.

33. *Национальный стандарт Российской Федерации. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры*, Стандартинформ, 2016, 15 с.
34. Пильщиков Д. В., “Асимптотическое поведение мощности полного прообраза случайного множества при итерациях отображений конечного множества”, *Математические вопросы криптографии*, **8:1** (2017), 95-106.
35. Пильщиков Д. В., “Исследование сложности метода радужных таблиц с маркерами цепочек”, *Математические вопросы криптографии*, **8:4** (2017), 99-116.
36. Погорелов Б. А., Сачков В. Н., *Словарь криптографических терминов*, М.: МЦНМО, 2006, 94 с.
37. Попов В., Курепкин И., Леонтьев С., *Дополнительные криптографические алгоритмы для применения с алгоритмами ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94*, 2006, 30 <https://tools.ietf.org/html/rfc4357> с.
38. Проскурин Г. В., “О распределении числа вершин в слоях случайного отображения”, *Теор. вероятн. и её примен.*, **18:4** (1973), 846-852.
39. Проскурин Г. В., “Предельные распределения числа циклических точек устойчивого случайного отображения”, *Дискретная математика*, **6:2** (1994), 74-87.
40. Сачков В. Н., “Случайные отображения ограниченной высоты”, *Теор. вероятн. и её примен.*, **18:1** (1973), 122-132.
41. Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.

42. Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, М.: Наука. Гл. ред. физ.-мат. лит., 1982, 384 с.
43. Сачков В. Н., *Курс комбинаторного анализа*, Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
44. Севастьянов Б. А., “Некоторые классы случайных отображений конечных множеств и неоднородные ветвящиеся процессы”, *Дискретная математика*, **16**:1 (2004), 9-13.
45. Севастьянов Б. А., “Сходимость по распределению случайных отображений конечных множеств к ветвящимся процессам”, *Дискретная математика*, **17**:1 (2005), 18-21.
46. Серов А. А., “Образы конечного множества при итерациях двух случайных зависимых отображений”, *Дискретная математика*, **27**:4 (2015), 133-140.
47. *Стандарт криптографической защиты данных, ГОСТ 28147-89*, Гос. комитет СССР по стандартизации, 1989.
48. Степанов В. Е., “О распределении числа вершин в слоях случайного дерева”, *Теор. вероятн. и её примен.*, **14**:1 (1969), 64-77.
49. Степанов В. Е., “Предельные распределения некоторых характеристик случайных отображений”, *Теор. вероятн. и её примен.*, **14**:4 (1969), 639-653.
50. Степанов В. Е., “Случайные отображения с одним притягивающим центром”, *Теория вероятн. и её примен.*, **16**:1 (1971), 148-156.

51. Тимашёв А. Н., “Предельные теоремы для совместного распределения объемов компонент в случайном отображении с известным числом компонент”, *Дискретная математика*, **23**:1 (2011), 21-27.
52. Тимашёв А. Н., “Асимптотические разложения для распределения числа компонент в случайных отображениях и разбиениях”, *Дискретная математика*, **23**:2 (2011), 66-75.
53. Феллер В., *Введение в теорию вероятностей и ее приложения. Том 1 (2-е изд.)*, М.: Мир, 1963, 498 с.
54. Фомичев В. М., *Дискретная математика и криптология. Курс лекций*, М.: Диалог-МИФИ, 2003, 400 с.
55. Чистяков В. П., *Курс теории вероятностей (7-е изд.)*, М.: Дрофа, 2007, 253 с.
56. Якимив А. Л., “О числе циклических точек случайного A -отображения”, *Дискретная математика*, **25**:3 (2013), 116-127.
57. Якимив А. Л., “Предельная теорема для логарифма порядка случайного A -отображения”, *Дискретная математика*, **29**:1 (2017), 136-155.
58. Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., Smyshlyaev 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.
59. Aldous D., Pitman J., “Invariance principles for non-uniform random mappings and trees”, *Asymptotic combinatorics with applications to mathematical physics*, **77** (2002), 113-147.

60. Aldous D., Pitman J., “The asymptotic distribution of the diameter of a random mapping”, *Comptes Rendus Mathematique*, **334**:11 (2002), 1021-1024.
61. Aldous D., Pitman J., “Two recursive decompositions of Brownian bridge related to the asymptotics of random mappings”, *Comptes Rendus Math. Technical Report 595, Dept. Statistics, U.C. Berkeley*, 2002.
62. Aldous D., Miermont G., Pitman J., “Brownian bridge asymptotics for random p-mappings”, *Electronic Journal of Probability*, **9** (2004), 37-56.
63. Aldous D., Miermont G., Pitman J., “Weak convergence of random p-mappings and the exploration process of inhomogeneous continuum random trees”, *Probability Theory and Related Fields*, **133**:1 (2005), 1-17.
64. Arney J., Bender E. A., “Random mappings with constraints on coalescence and number of origins”, *Pacific journal of mathematics*, **103**:2 (1982), 269-294.
65. Avoine G., Junod P., Oechslin P., “Characterization and improvement of time-memory trade-off based on perfect tables”, *Trans. Inf. Syst. Secur.*, **11**:17 (2008), 1-17.
66. Baron G., Drmota M., Mutafchiev L., “Predecessors in Random Mappings”, *Combinatorics, Probability and Computing*, **5** (1996), 317-335.
67. Dalal A., Schmutz E., “Compositions of random functions on a finite set”, *Electr. J. Comb.*, **9**:R26 (2002), 1-7.
68. DeLaurentis J. M., “Components and cycles of a random function”, *Lecture Notes in Computer Science*, **293** (1988), 231-242.

69. Drmota M., Soria M., “Images and preimages in a random mapping”, *SIAM Journal on Discrete Mathematics*, **10** (1996), 246-269.
70. Fill J. A., “On compositions of random functions on a finite Set”, 2002 <http://www.mts.jhu.edu/~fill/>, 1-15.
71. Flajolet P., Odlyzko A., “Random Mapping Statistics”, *Lect. Notes Comput. Sci.* **434**, 1989, 329-354.
72. Harris B., “Probability distributions related to random mapping”, *Ann. Math. Statist.*, **31**:4 (1960), 1045-1062.
73. Hellman M. E., “A cryptanalytic time-memory trade-off”, *IEEE Trans. Inf. Theory*, 1980, 401-406.
74. Hong J., “The cost of false alarms in Hellman and rainbow tradeoffs”, *Designs, Codes and Cryptography*, **57**:3 (2010), 293-327.
75. Hong J., Ma D., “Success probability of the Hellman trade-off”, *Inf. Process. Lett.*, **109**:7 (2009), 347-351.
76. Kingman J. F. C., “The coalescent”, *Stoch. Proc. Appl.*, **13** (1982), 235-248.
77. Kusuda K., Matsumoto T., “Optimization of time-memory trade-off cryptanalysis and its application to DES, FEAL-32, and Skipjack”, *IEICE Trans. on Fundamentals*, **1**:E-79A (1996), 35-48.
78. McSweeney J. K., Pittel B. G., “Expected coalescence time for a nonuniform allocation process”, *Adv. Appl. Probab.*, **40**:4 (2008), 1002-1032.
79. Minaud B., Seurin Y., “The iterated random permutation problem with applications to cascade encryption”, *Links Among Impossible Differential, Integral and Zero Correlation Linear Cryptanalysis*, 2015, 351-367.

80. Mutafovchiov L., “The limit distribution of the number of nodes in low strata of a random mapping”, *Statist. Probab. Lett.*, **7** (1989), 247-251.
81. Oechslin P., “Making a faster cryptanalytic time-memory trade-off”, *Lect. Notes Comput. Sci.*, **2729** (2003), 617-630.
82. 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.
83. 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.
84. Rubin H., Sitgreaves R., *Probability distributions related to random transformations of a finite set*, Tech. Rept. №19A, Applied Mathematics and Statistics Laboratory, Stanford University, 1954, 50 pp.