МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Научный журнал

2023 № 62

Зарегистрирован в Федеральной службе по надзору
в сфере связи и массовых коммуникаций

Свидетельство о регистрации ПИ № ФС 77-33762 от 16 октября 2008 г.

Подписной индекс в объединённом каталоге «Пресса России» 38696

УЧРЕДИТЕЛЬ
Томский государственный университет

Адрес редакции и издателя: 634050, г. Томск, пр. Ленина, 36
E-mail: pank@mail.tsu.ru

В журнале публикуются результаты фундаментальных и прикладных научных исследований отечественных и зарубежных ученых, включая студентов и аспирантов, в области дискретной математики и её приложений в криптографии, компьютерной безопасности, кибернетике, информатике, программировании, теории надёжности, интеллектуальных системах.

Периодичность выхода журнала: 4 номера в год.

Редактор *Н. И. Шидловская*
Редактор-переводчик *Т. В. Бутузова*
Верстка *И. А. Панкратовой*

Подписано к печати 05.12.2023. Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 14,6. Тираж 300 экз.
Заказ № 5695. Цена свободная. Дата выхода в свет 13.12.2023.

Отпечатано на оборудовании
Издательства Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

CONTENTS

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.212.2 DOI 10.17223/20710410/62/1

О РАСПРЕДЕЛЕНИИ ДЛИН ЦИКЛОВ В ГРАФЕ k-КРАТНОЙ ИТЕРАЦИИ РАВНОВЕРОЯТНОЙ СЛУЧАЙНОЙ ПОДСТАНОВКИ

В. О. Миронкин

МИРЭА — Российский технологический университет, г. Москва, Россия

E-mail: mironkin.v@mail.ru

Изучается влияние процесса итерирования на структуру графа G_π исходной равновероятной случайной подстановки $\pi\colon S \to S$. Выписаны точные формулы для распределения длины $\beta_\pi(x)$ цикла $\mathcal{K}_\pi(x)$, содержащего произвольную фиксированную вершину $x \in S$. Получено выражение для математического ожидания случайной величины $\lambda_{\pi^k}(l)$, равной числу вершин в графе G_{π^k}, лежащих на циклах длины $l \in \{1, \ldots, |S|\}$. Для $k \in \mathbb{N}$ и произвольных фиксированных вершин $x, y \in S$, $x \neq y$, вычислена совместная вероятность их попадания на циклы фиксированных длин в графе G_{π^k}.

Ключевые слова: *равновероятная случайная подстановка, итерация подстановки, граф подстановки, распределение длин циклов, неподвижные точки.*

ON THE DISTRIBUTION OF CYCLE LENGTHS IN THE GRAPH OF k-MULTIPLE ITERATION OF THE UNIFORM RANDOM SUBSTITUTION

V. O. Mironkin

MIREA — Russian Technological University, Moscow, Russia

The influence of the iteration process on the structure of the graph G_π of the uniform random substitution $\pi\colon S \to S$ is studied. Exact formulas are written out for the distribution of the length $\beta_\pi(x)$ of the cycle $\mathcal{K}_\pi(x)$ containing an arbitrary fixed vertex $x \in S$. An expression is written for the mathematical expectation of a random variable $\lambda_{\pi^k}(l)$ equal to the number of vertices in the graph G_{π^k} lying on cycles of length $l \in \{1, \ldots, |S|\}$. For $k \in \mathbb{N}$ and arbitrary fixed vertices $x, y \in S$, $x \neq y$, the joint probability of their falling on cycles of fixed lengths in the graph G_{π^k} is calculated.

Keywords: *uniform random substitution, iteration of a substitution, graph of a substitution, distribution of cycle lengths, fixed points.*

Введение

Наряду с равновероятными случайными отображениями конечного множества в себя [1–4] особую практическую роль при синтезе и анализе алгоритмических методов

защиты информации (далее — АМЗИ) играют равновероятные случайные подстановки — биективные отображения конечного множества в себя. Так, в частности, класс указанных отображений представляет собой основной математический инструментарий, используемый при моделировании алгоритмов блочного шифрования, которые, как правило, имеют итерационную структуру. Такое построение АМЗИ нацелено на повышение их криптографического качества. При этом может возникнуть естественный вопрос о целесообразности дополнительного итерирования уже отдельных блоков АМЗИ, например блока подстановок. Как подобная модификация скажется на криптографическом качестве АМЗИ в целом? Для того чтобы ответить на этом вопрос, требуются знания о свойствах и характеристиках итераций упомянутых блоков.

В работе изучаются вероятностные свойства и характеристики одной модификации класса равновероятных случайных подстановок, состоящего из их кратных итераций.

Следует отметить, что результаты исследований равновероятных случайных отображений [5, 6] не могут быть в явном виде распространены на указанные математические объекты из-за неравновероятности распределения случайных подстановок на множестве всех отображений некоторого конечного множества в себя.

1. Теоретико-вероятностная модель

Рассмотрим конечное множество $S = \{1, \ldots, n\}$, $n > 1$, и вероятностное пространство $(\Omega, \mathcal{F}, \mathbf{P})$, в котором пространством элементарных исходов Ω является множество S_n всех $n!$ биективных отображений $\pi\colon S \to S$, алгеброй событий $\mathcal{F}$ — множество всех подмножеств Ω, а вероятностная мера $\mathbf{P}$, соответствующая равновероятным случайным отображениям, задана следующим образом:

$$\mathsf{P}[\pi] = \frac{1}{n!}, \quad \pi \in \Omega. \tag{1}$$

Определение 1. *Графом подстановки* $\pi \in \Omega$ называется ориентированный граф $G_\pi = (S, E_\pi)$ с множеством вершин S и множеством ориентированных рёбер $E_\pi = \{(x, \pi(x))\colon x \in S\} \subset S^2$.

Определение 2. *Циклом* $\mathcal{K}_\pi(x)$ графа G_π, содержащим вершину $x \in S$, называется множество вершин

$$\{y \in S\colon \pi^u(y) = \pi^v(x) \text{ для некоторых } u, v \geqslant 0\}.$$

Здесь $\pi^0(y) = y$ и $\pi^u(y) = \underbrace{\pi(\ldots(\pi}_{u}(y)\ldots)$ в случае $u > 0$.

Через $\beta_\pi(x)$ обозначим длину цикла $\mathcal{K}_\pi(x)$, а через $C_l(G_\pi)$ — множество вершин графа G_π, лежащих на циклах длины $l \in \{1, \ldots, n\}$.

Замечание 1. Распределение случайной величины $\beta_\pi(x)$ зависит от n. Однако во избежание загромождения формул данный факт в тексте отражать не будем.

2. Вспомогательные результаты

Для произвольных $k, l, i, j \in \mathbb{N}$, $i \leqslant j$, введём обозначение

$$Q_i^j(k, l) = \left\{m \in \mathbb{N} : i \leqslant m \leqslant j,\ \frac{m}{(m, k)} = l\right\}, \tag{2}$$

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

Далее для произвольного $u \in \mathbb{N}$, $u > 1$, будем использовать следующее представление:

$$u = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}, \tag{3}$$

где $p_1 = 2 < p_2 < \ldots < p_t$ — последовательные простые числа; $a_t > 0$; $a_i \geqslant 0$, $i = 1, \dots, t-1$. При этом через Δ_u будем обозначать множество номеров ненулевых элементов последовательности $a_1, \dots, a_t$, а через $\overline{\Delta_u} = \{1, \dots, t\} \setminus \Delta_u$ — множество номеров нулевых элементов. Кроме того, для произвольных $n \in \mathbb{N}$, $n > 1$, $r \in \mathbb{N}$ и $D \in \mathbb{R}$ через $W_{\{i_1,\dots,i_r\}}^{(\{a_{i_1},\dots,a_{i_r}\})}(n, D)$ будем обозначать множество решений из $(\mathbb{N} \cup \{0\})^r$ системы линейных неравенств

$$\begin{cases} x_1 \log_n p_{i_1} + x_2 \log_n p_{i_2} + \ldots + x_r \log_n p_{i_r} \leqslant D, \\ x_j \leqslant a_{i_j}, \ j = 1, \dots, r, \end{cases}$$

где $i_1 < \ldots < i_r$. Здесь и далее положим $\prod\limits_{i \in \varnothing} (\ldots) \equiv 1$, $\sum\limits_{i \in \varnothing} (\ldots) \equiv 0$.

Утверждение 1. Пусть $n \in \mathbb{N}$, $n > 1$. Тогда для любых $k = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t} \in \mathbb{N}$ и $l = p_1^{b_1} p_2^{b_2} \dots p_s^{b_s} \in \{1, \dots, n\}$, представленных в виде (3), справедливо равенство

$$|Q_1^n(k, l)| = \left| W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i \colon i \in \Delta_k \cap \overline{\Delta_l}\})} \left(n, 1 - \sum_{i \in \Delta_l} (a_i + b_i) \log_n p_i \right) \right|. \tag{4}$$

Доказательство. Зафиксируем $m \in \{1, \dots, n\}$ и запишем его в следующем виде:

$$m = \prod_{i \in \left(\Delta_m \cap \Delta_k \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{c_i},$$

где $c_i > 0$ в соответствии с (3). Тогда в условиях утверждения равенство $\dfrac{m}{(m,k)} = l$ имеет вид

$$\frac{m}{(m,k)} = \prod_{i \in (\Delta_m \cap \Delta_k \cap \overline{\Delta_l})} p_i^{c_i - \min(c_i, a_i)} \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{c_i - \min(c_i, a_i)} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)} p_i^{c_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{c_i} =$$

$$= \prod_{i \in (\Delta_m \cap \Delta_k \cap \Delta_l)} p_i^{b_i} \prod_{i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)} p_i^{b_i}.$$

При этом для произвольного фиксированного $i \in \Delta_m$

$$c_i - \min(c_i, a_i) = \begin{cases} 0, & c_i \leqslant a_i, \\ c_i - a_i & \text{в противном случае.} \end{cases}$$

В частности, при условии $m \in \{1, \dots, n\}$ выполняется следующее:

1) для $i \in \left(\Delta_m \cap \Delta_k \cap \overline{\Delta_l}\right)$ уравнение

$$c_i - \min(c_i, a_i) = 0 \tag{5}$$

относительно c_i имеет в точности $a_i + 1$ различных решений вида $c_i = 0, \dots, a_i$;

2) для $i \in (\Delta_m \cap \Delta_k \cap \Delta_l)$ уравнение

$$c_i - \min(c_i, a_i) = b_i \neq 0 \tag{6}$$

имеет единственное решение вида $c_i = a_i + b_i$;

3) для $i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \overline{\Delta_l}\right)$ уравнение (5) имеет единственное решение $c_i = 0$;

4) для $i \in \left(\Delta_m \cap \overline{\Delta_k} \cap \Delta_l\right)$ уравнение (6) имеет единственное решение $c_i = b_i$.

Таким образом, число различных m, удовлетворяющих (2), совпадает с мощностью множества $W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i:\, i \in \Delta_k \cap \overline{\Delta_l}\})}\left(n, 1 - \sum\limits_{i \in \Delta_l} (a_i + b_i) \log_n p_i\right)$. ■

Следствие 1. Пусть в условиях утверждения 1 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$|Q_1^n(k,l)| = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1). \tag{7}$$

В частности, если k — простое, то

$$|Q_1^n(k,l)| = \begin{cases} 2, & (k,l) = 1, \\ 1, & (k,l) \neq 1. \end{cases} \tag{8}$$

3. Распределение длин циклов в графе G_{π^k}

Прежде чем перейти к описанию распределения случайной величины β_{π^k}, $k > 1$, выясним, как процесс итерирования произвольной подстановки $\pi \in S_n$ влияет на структуру её графа G_π.

Отметим, что распределение числа вершин по циклам графа G_{π^k}, $k > 1$, сформированного на основе графа G_π, определяется величиной k, а именно: каждый цикл графа G_π длины $m \in \{1, \ldots, n\}$ распадается на (m,k) отдельных циклов графа G_{π^k} длины $\dfrac{m}{(m,k)}$ (рис. 1).

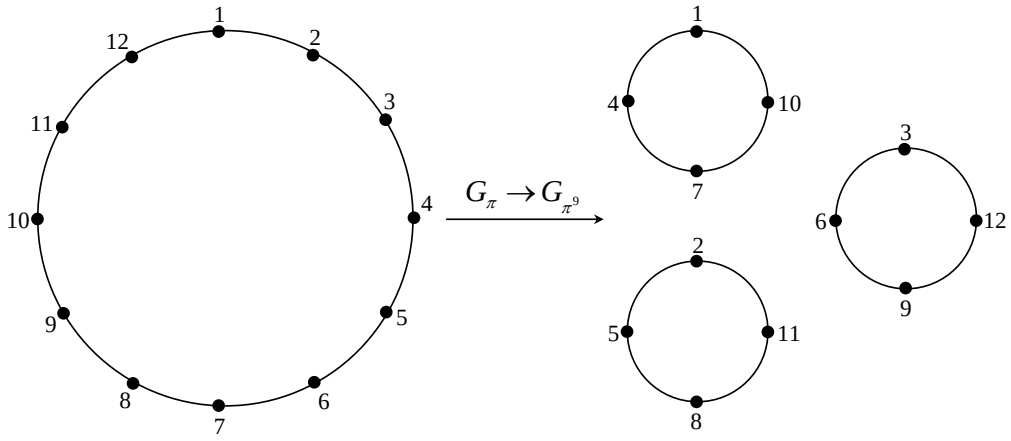


Рис. 1. Распад цикла при 9-кратном итерировании равновероятной случайной подстановки π

Этот факт позволяет выписать точную формулу для локальной вероятности $\mathsf{P}\left[\beta_{\pi^k}(x) = l\right]$ с использованием распределения случайной величины β_π.

Утверждение 2. Пусть $n \in \mathbb{N}$, $n > 1$ и случайная подстановка $\pi\colon S \to S$ имеет распределение (1). Тогда для любого фиксированного $x \in S$, любых $k = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t} \in \in \mathbb{N}$ и $l = p_1^{b_1} p_2^{b_2} \ldots p_s^{b_s} \in \{1, \ldots, n\}$, представленных в виде (3), справедливо равенство

$$\mathsf{P}\left[\beta_{\pi^k}(x) = l\right] = \frac{1}{n} \left| W_{\Delta_k \cap \overline{\Delta_l}}^{(\{a_i:\, i \in \Delta_k \cap \overline{\Delta_l}\})}\left(n, 1 - \sum_{i \in \Delta_l} (a_i + b_i) \log_n p_i\right) \right|.$$

Доказательство. Зафиксируем вершину $x \in S$ и обозначим через m длину цикла $\mathcal{K}_\pi(x)$, где $m \leqslant n$. Тогда для произвольного $k \in \mathbb{N}$ соответствующий цикл $\mathcal{K}_{\pi^k}(x)$ имеет длину $l = \dfrac{m}{(m,k)}$. Используя обозначение (2), запишем равенство событий

$$[\beta_{\pi^k}(x) = l] = \bigcup_{m \in Q_n(k,l)} [\beta_\pi(x) = m]. \tag{9}$$

Заметим, что события, стоящие под знаком объединения в (9), несовместны и что величина

$$\mathsf{P}[\beta_\pi(x) = m] = \left(1 - \frac{1}{n}\right)\left(1 - \frac{1}{n-1}\right)\ldots\left(1 - \frac{1}{n-m+2}\right)\frac{1}{n-m+1} = \frac{1}{n}$$

не зависит от m.

Поэтому, переходя в (9) к вероятностям, получаем

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \sum_{m \in Q_n(k,l)} \mathsf{P}[\beta_\pi(x) = m] = \frac{|Q_1^n(k,l)|}{n}, \tag{10}$$

что с учётом (4) даёт искомый результат. ■

Следствие 2. Пусть в условиях утверждения 2 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \frac{1}{n} \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1). \tag{11}$$

В частности, если k — простое, то

$$\mathsf{P}[\beta_{\pi^k}(x) = l] = \begin{cases} 2/n, & (k,l) = 1, \\ 1/n, & (k,l) \neq 1. \end{cases}$$

Доказательство. Искомые выражения естественным образом следуют из (10) и соотношений (7) и (8). ■

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

Следствие 3. Пусть в условиях утверждения 2 выполнено неравенство $kl \leqslant n$. Тогда справедлива формула

$$\mathbf{E}\lambda_{\pi^k}(l) = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1).$$

Доказательство. Действительно, так как $\lambda_{\pi^k}(l) = \sum\limits_{x \in S} I\{x \in C_l(G_{\pi^k})\}$, где $I\{A\}$ — индикатор события A, то в силу равноправия всех $x \in S$ и с учётом (11) получаем цепочку соотношений

$$\mathbf{E}\lambda_{\pi^k}(l) = \mathbf{E}\sum_{x \in S} I\{x \in C_l(G_{\pi^k})\} = n\,\mathsf{P}[x \in C_l(G_{\pi^k})] = n\,\mathsf{P}[\beta_{\pi^k}(x) = l] = \prod_{i \in \left(\Delta_k \cap \overline{\Delta_l}\right)} (a_i + 1).$$

Следствие доказано. ■

В результатах следствий 2 и 3 выделим частный случай, представляющий особый интерес для анализа криптографических примитивов (например, s-боксов), используемых в составе алгоритмов блочного шифрования.

Определение 3. Неподвижной точкой подстановки $\pi\colon S \to S$ называется элемент $x \in S$, для которого $\pi(x) = x$.

С учётом введённых обозначений множество неподвижных точек k-кратной итерации произвольной подстановки $\pi\colon S \to S$ совпадает с $C_1(G_{\pi^k})$.

Следствие 4. Пусть в условиях утверждения 2 число k — простое и выполнено неравенство $k \leqslant n$. Тогда справедливы формулы

$$\mathsf{P}\left[x \in C_1(G_{\pi^k})\right] = \frac{2}{n},$$
$$\mathbf{E}\lambda_{\pi^k}(1) = 2.$$

Замечание 2. Результаты следствий 3 и 4 могут найти применение в рамках статистической проверки гипотезы о равновероятности распределения подстановок. Действительно, имея реализацию $\pi_1, \pi_2, \ldots, \pi_N$ выборки объёма $N \in \mathbb{N}$ из некоторого неизвестного распределения, заданного на измеримом пространстве $(\Omega, \mathcal{F})$, можно для произвольного $k > 1$ сформировать и работать с набором производных реализаций

$$\pi_1, \ldots, \pi_N,\ \pi_1^2, \ldots, \pi_N^2,\ \ldots,\ \pi_1^k, \ldots, \pi_N^k,$$

получив при этом вместо одной оценки $\overline{X}_1$ величины $\mathbf{E}\lambda_\pi(l)$, $l \in \{1, \ldots, n\}$, набор из k оценок $\overline{X}_1, \ldots, \overline{X}_k$ величин $\mathbf{E}\lambda_\pi(l), \ldots, \mathbf{E}\lambda_{\pi^k}(l)$ соответственно.

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_{π^k}.

Утверждение 3. Пусть $n \in \mathbb{N}$, $n > 1$ и случайная подстановка $\pi\colon S \to S$ имеет распределение (1). Тогда для любых фиксированных $x, y \in S$, $x \neq y$, и любых $k \in \mathbb{N}$ и $l_1, l_2 \in \{1, \ldots, n\}$, $l_1 + l_2 \leqslant n(1 + \delta_{l_1,l_2})$, справедливо равенство

$$\mathsf{P}\left[x \in C_{l_1}(G_{\pi^k}), y \in C_{l_2}(G_{\pi^k})\right] = \delta_{l_1,l_2} \sum_{m \in Q_1^n(k,l_1)} \frac{m-1}{n(n-1)} + \sum_{m_1 \in Q_1^n(k,l_1)} \sum_{m_2 \in Q_1^{n-m_1}(k,l_2)} \frac{1}{n(n-1)},$$

где $\delta_{l_1,l_2} = \begin{cases} 1, & l_1 = l_2, \\ 0, & l_1 \neq l_2 \end{cases}$ — символ Кронекера; $Q_1^n(k,l)$ определяется соотношением (2).

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

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

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

$$\mathsf{P}\left[x, y \in C_l(G_{\pi^k})\right] = \mathsf{P}\left[x, y \in C_l(G_{\pi^k}), I_{x,y} = 1\right] + \mathsf{P}\left[x, y \in C_l(G_{\pi^k}), I_{x,y} = 0\right]. \tag{12}$$

Вычислим первое слагаемое в правой части (12). Зафиксируем вершину $x \in S$. Для произвольной фиксированной вершины $y \in S$, $y \neq x$, существует в точности $m-1$ вариантов расположения на содержащем x цикле длины $m \in Q_n(k,l)$ в графе G_π.

Тогда получаем следующую цепочку равенств:

$$\begin{gathered}\mathsf{P}\left[x,y\in C_l(G_{\pi^k}),I_{x,y}=1\right]=\\ =\sum_{m\in Q_2^n(k,l)}\frac{1}{n}\left(1-\frac{1}{n-1}\right)\left(1-\frac{1}{n-2}\right)\ldots\left(1-\frac{1}{n-m+2}\right)\frac{1}{n-m+1}+\\ +\sum_{m\in Q_2^n(k,l)}\left(1-\frac{2}{n}\right)\frac{1}{n-1}\left(1-\frac{1}{n-2}\right)\ldots\left(1-\frac{1}{n-m+2}\right)\frac{1}{n-m+1}+\ldots+\\ +\sum_{m\in Q_2^n(k,l)}\left(1-\frac{2}{n}\right)\left(1-\frac{2}{n-1}\right)\ldots\left(1-\frac{2}{n-m+3}\right)\frac{1}{n-m+2}\frac{1}{n-m+1}=\\ =\sum_{m\in Q_1^n(k,l)}\frac{m-1}{n\,(n-1)}.\end{gathered}\tag{13}$$

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

$$\begin{gathered}\mathsf{P}\left[x,y\in C_l(G_{\pi^k}),I_{x,y}=0\right]=\sum_{m_1\in Q_1^n(k,l)}\prod_{i=0}^{m_1-2}\left(1-\frac{2}{n-i}\right)\frac{1}{n-m_1+1}\times\\ \times\sum_{m_2\in Q_1^{n-m_1}(k,l)}\prod_{i=m_1}^{m_1+m_2-2}\left(1-\frac{1}{n-i}\right)\frac{1}{n-m_1-m_2+1}=\\ =\sum_{m_1\in Q_1^n(k,l)}\sum_{m_2\in Q_1^{n-m_1}(k,l)}\frac{1}{n\,(n-1)}.\end{gathered}\tag{14}$$

Подставив (13) и (14) в равенство (12), 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_{π^k}, а следовательно, и в графе G_π. Поэтому

$$\mathsf{P}\left[x\in C_{l_1}(G_{\pi^k}),y\in C_{l_2}(G_{\pi^k}),l_1\neq l_2\right]=\sum_{m_1\in Q_1^n(k,l_1)}\sum_{m_2\in Q_1^{n-m_1}(k,l_2)}\frac{1}{n(n-1)}.\tag{15}$$

Объединяя выражения (12) и (15) с использованием символа Кронекера, приходим к искомому выражению. ■

Заключение

Полученные результаты позволяют описывать строение и некоторые вероятностные свойства графа G_{π^k}, $k\geqslant 1$, используемые при синтезе и анализе АМЗИ. Кроме того, точные распределения исследованных случайных величин расширяют возможности статистической проверки гипотезы о согласии распределения анализируемых подстановок с равновероятным.

ЛИТЕРАТУРА

1. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984. 208 с.
2. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978. 288 с.
3. *Flajolet P. and Odlyzko A.* Random mapping statistics // LNCS. 1989. V. 434. P. 329–354.
4. *Harris B.* Probability distributions related to random mapping // Ann. Math. Statist. 1960. V. 31. No. 4. P. 1045–1062.

5. *Миронкин В. О.* Слои в графе k-кратной итерации равновероятного случайного отображения // Математические вопросы криптографии. 2019. Т. 10. № 1. С. 73–82.
6. *Миронкин В. О.* Слои в графе композиции независимых равновероятных случайных отображений // Математические вопросы криптографии. 2020. Т. 11. № 1. С. 101–114.

REFERENCES

1. *Kolchin V. F.* Sluchaynie otobrazeniya [Random Mappings]. Moscow, Nauka Publ., 1984. (in Russian)
2. *Sachkov V. N.* Veroyatnostnie metodi v kombinatornom analize [Probabilistic Methods in Combinatorial Analysis]. Moscow, Nauka Publ., 1978. (in Russian)
3. *Flajolet P. and Odlyzko A.* Random mapping statistics. LNCS, 1989, vol. 434, pp. 329–354.
4. *Harris B.* Probability distributions related to random mapping. Ann. Math. Statist., 1960, vol. 31, no. 4, pp. 1045–1062.
5. *Mironkin V. O.* Sloi v grafe k-kratnoy iteratsii ravnoveroyatnogo sluchaynogo otobrazheniya [On the layers in the graph of k-fold iteration of uniform random mapping]. Mat. Vopr. Kriptogr., 2019, vol. 10, no. 1, pp. 73–82. (in Russian)
6. *Mironkin V. O.* Sloi v grafe kompozitsii nezavisimykh ravnoveroyatnykh sluchaynykh otobrazheniy [Layers in a graph of the composition of independent uniform random mappings]. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 1, pp. 101–114. (in Russian)

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/20710410/62/2

ON BLINDNESS OF SEVERAL ELGAMAL-TYPE BLIND SIGNATURES

A. A. Babueva*, L. R. Akhmetzyanova*, E. K. Alekseev*, O. G. Taraskin**

*CryptoPro, Moscow, Russia
**Waves, Moscow, Russia

E-mail: babueva@cryptopro.ru, lah@cryptopro.ru, alekseev@cryptopro.ru, tog.postquant@gmail.com

Blind signature schemes are the essential element of many e-cash and e-voting systems. Anonymity in such systems is ensured through the blindness property of the signature schemes. We discuss the blindness property and analyze several ElGamal-type blind signature schemes regarding this property. We present effective attacks violating blindness on three schemes.

Keywords: *blind signature scheme, blindness, ElGamal-type blind signature.*

О СВОЙСТВЕ НЕОТСЛЕЖИВАЕМОСТИ НЕСКОЛЬКИХ СХЕМ ПОДПИСИ ВСЛЕПУЮ НА ОСНОВЕ УРАВНЕНИЯ ЭЛЬ-ГАМАЛЯ

А. А. Бабуева*, Л. Р. Ахметзянова*, Е. К. Алексеев*, О. Г. Тараскин**

*КриптоПро, г. Москва, Россия
**Waves, г. Москва, Россия

Схемы подписи вслепую являются неотъемлемым элементом большого количества систем электронных платежей и систем дистанционного электронного голосования. Анонимность в таких системах обеспечивается за счёт свойства неотслеживаемости схем подписи вслепую. Настоящая работа посвящена анализу некоторых схем подписи вслепую на основе уравнения Эль-Гамаля с точки зрения обеспечения свойства неотслеживаемости. Построены атаки, нарушающие свойство неотслеживаемости, на три схемы подписи вслепую указанного типа.

Ключевые слова: *схема подписи вслепую, свойство неотслеживаемости, схема подписи вслепую типа Эль-Гамаля.*

1. Introduction

The blind signature mechanism was originally proposed by Chaum in 1982 in [1] for e-cash systems. Signature issuing protocol is the interactive protocol that runs between two parties: a Signer and a Requester. As the result, the Requester receives the signature for a message without the Signer receiving any information about the message or the signature value. The application of blind signature schemes includes electronic voting systems, anonymous e-cash systems, direct anonymous attestation, anonymous credentials, etc.

Blind signature schemes should provide two security properties: unforgeability and blindness. The first one is standard for all signature schemes and ensures that a valid signature can be generated only during the interaction with the secret signing key holder. The second property is more specific for this class of signature schemes and provides that a Signer learns no additional information during the protocol execution. However, the way to determine this information is not obvious. Intuitively, it seems that the message to be signed should be hidden from the Signer, but it turns out that this is not enough.

In the paper, we discuss the blindness property and analyze several blind signature schemes based on ElGamal equation (ElGamal-type blind signature schemes) regarding this property. We present attacks violating blindness on schemes introduced in [2–4]. It seems that one of them [3] was broken due to a misunderstanding of blindness property.

2. Blindness property

Before we talk about blindness, let us recall the definition of a blind signature scheme. It is determined by three algorithms:

— $(sk, pk) \leftarrow \texttt{KeyGen}()$: a key generation algorithm that outputs a secret key sk and a public key pk;
— $(b, \sigma) \leftarrow \langle \text{Signer}(sk), \text{Requester}(pk, m) \rangle$: an interactive signing protocol that is run between a Signer with a secret key sk and a Requester with a public key pk and a message m; the Signer outputs $b = 1$, if the interaction completes successfully, and $b = 0$ otherwise, while the Requester outputs a signature σ, if it terminates correctly, and a fail indicator $\perp$ otherwise;
— $b \leftarrow \text{Verify}(pk, m, \sigma)$: a (deterministic) verification algorithm that takes a public key pk, a message m, and a signature σ, and returns 1 if σ is valid on m under pk and 0 otherwise.

Blindness. Informally, the blind signature scheme provides blindness if there is no way to link a (message, signature) pair to the certain execution of the signing protocol. In other words, the blindness is broken if the particular protocol execution for some fixed message leads to fixing the signature value in an unambiguous way or at least to significant narrowing the set of possible signature values. It means that for each protocol transcription and message there exists only the small set of valid signature values (and hence, blinding factors values) that could be produced during such protocol execution.

For a deeper understanding, we consider the example of using blind signature schemes in e-voting systems. Suppose, that the authenticated voter performs a blind signature protocol with the Registrar and receives a signature for his ballot (the ballot acts as the message in this scenario). Note that in this case the transcription of the protocol is tied to a specific person, his full name and personal information. After receiving the signature, the voter sends a signed ballot to the ballot box anonymously. Thus, if one can link the protocol transcription to the (message, signature) pair, then he can link the ballot to the specific person and violate anonymity.

Towards formalizing. Let describe the regular blindness security notion introduced in [5, 6]. An adversary acts as a malicious Signer and is powered to run the signing protocol with the Requester twice. It is assumed that the Requester behaves correctly (according to the protocol). After two successful interactions the Requester outputs two (message, signature) pairs simultaneously. If at least one of the interactions failed, the Requester outputs fail indicator.

The adversary's task (threat) is to link the transcription to the corresponding (message, signature) pair with a probability of success significantly greater than 1/2. A strong and a weak attacks may be also distinguished by the following criteria [7]:

— by key generation way (weak attack — the adversary generates key pair according to the protocol, strong — in the malicious way);
— by the method of choosing messages, the signature for which the adversary should distinguish (weak attack — the messages are chosen by the Requester, strong — by the adversary).

Note that regular blindness assumes that all interactions terminates successfully. However, extended security notions, that allow an adversary to initiate aborts, were also introduced: a-posteriori blindness [8], selective-failure blindness [9]. The latter notion was also extended to the multiple interaction case [10]. A-posteriori blindness originally considers blindness of multiple executions between the Signer and the Requester, and guarantees unlinkability of execution with (message, signature) pairs only for non-aborted sessions. An adversary is powered to control the distribution on the signed messages, but not to choose them. However, a-posteriori blindness does not imply ordinary blindness and vice versa [8]. Selective-failure blindness guarantees that adversary could not force Requester to abort the signing protocol because of a certain property of the Requester message, which would disclose some information about the message to the adversary. Selective-failure blindness is a strictly stronger notion than regular blindness [10].

3. Broken schemes

This section presents three ElGamal-type blind signature schemes that do not provide blindness and the corresponding attacks. To address specific schemes, we name them by the authors' initials and the date of paper publication.

All considered schemes are based on the elliptic curve discrete logarithm problem. If p is a prime number, then the set $\mathbb{Z}_p$ is a finite field with characteristic p. We assume the canonic representation of the elements in $\mathbb{Z}_p$ as a natural number in the set $\{0, \ldots, p-1\}$. We define $\mathbb{Z}_p^*$ as the set $\mathbb{Z}_p$ without zero element. We denote the group of points of elliptic curve over the field $\mathbb{Z}_p$ by $\mathbb{G}$, the order of the prime subgroup of $\mathbb{G}$ by q and elliptic curve point of order q by P. For simplicity, we assume that $p < q$. A key generation algorithm `KeyGen` in all schemes involves picking random d from $\mathbb{Z}_q^*$ (secret signing key) and defining $Q = dP$ (public verifying key). We denote by H the hash function that maps binary strings to elements from $\mathbb{Z}_q$ and assume that all field operations are performed modulo q.

To avoid trivial attacks, we assume that during the signing protocol both the Signer and the Requester check that field elements are nonzero, points belong to the used elliptic curve and are not equal to the zero point. Moreover, the Requester should always check that the values obtained from the Signer are valid for its query. If one of these checks fails, the participant should abort the protocol with fail indicator.

All the proposed attacks are applied in the weak security model:

— key pair is generated correctly;
— Requester chooses the messages for signing on its own;
— an adversary does not need to know secret signing key;
— an adversary does not need to initiate aborts on the Requester side.

In fact, all these attacks may be performed by any external observer, not only the Signer.

3.1. GYP16 schemes

Four blind signature schemes, based on ECDSA, GDSA, KCDSA, and DSTU schemes, were proposed in [2] in 2016. We present the definition of ECDSA-based scheme and attack on it. The attacks on other schemes are constructed similarly.

Scheme description. The signing protocol is defined at Fig. 1.

The signing protocol

Signer(d, Q)		**Requester**(Q, m)
$k \leftarrow_{\$} \mathbb{Z}_q^*$		
$R \leftarrow kP$		
	$\xrightarrow{R}$	
		$\alpha \leftarrow_{\$} \mathbb{Z}_q^*$
		$R' \leftarrow \alpha R$
		$r \leftarrow R.x \bmod q$
		$r' \leftarrow R'.x \bmod q$
		$e' \leftarrow H(m)$
		$e \leftarrow r(r')^{-1}e'$ (1)
	$\xleftarrow{e}$	
$r \leftarrow R.x \bmod q$		
$s \leftarrow k^{-1}(dr + e)$		
	$\xrightarrow{s}$	
		$s' \leftarrow s\alpha^{-1}r'r^{-1}$
		$\sigma \leftarrow (r', s')$

Fig. 1. GYP16 scheme: the signing protocol

The verification procedure for the message m and the signature (r, s) assumes computing point $R = s^{-1}(rQ + eP)$, where $e = H(m)$, and verifying the equality $R.x \bmod q = r$.

Attack. We show that for fixed protocol transcription and message there exists only the small set of valid signature values that could be produced during the given protocol execution. Indeed, if the protocol transcription (R, e, s) and message m are fixed, then the $r = R.x \bmod q$ and $e' = H(m)$ values are also fixed. The line (1) allows to define the r' component of the signature unambiguously as $r' = re^{-1}e'$ and thus R' point is fixed up to sign. For each possible value R', there exists the unique α such that $R' = \alpha R$. But the α values are chosen uniformly at random, so the probability to choose α, such that $(\alpha R).x \bmod q = re^{-1}e'$, during several protocol executions is negligible. Therefore, with overwhelming probability there exist only one signature with r' component satisfied the condition in line (1).

Hence, the line (1) provides the criteria to break the blindness property. The exact transcription (R, e, s) corresponds to the certain message m with signature (r', s') iff the

following condition holds:

$$e = r(r')^{-1}e',$$

where $e' = H(m)$.

3.2. R00 scheme

Two blind signature schemes based on Schnorr and ElGamal (specifically, GOST) signatures were proposed in [3] in 2000. Both of them are vulnerable to the same attack. Let us show it on the GOST-based blind signature example.

Further, we assume that elliptic curve points can be represented as binary strings (corresponding to their coordinates) and therefore may be passed as input to the hash function H.

Scheme description. The signing protocol is defined at Fig. 2.

The signing protocol

Signer(d, Q)		**Requester**(Q, m)	
$k \leftarrow_{\$} \mathbb{Z}_q^*$			
$R \leftarrow kP$			
$r \leftarrow H(R)$			
	$\xrightarrow{R}$		
		$\alpha \leftarrow_{\$} \mathbb{Z}_q^*$	
		$R' \leftarrow \alpha R$	(1)
		$r' \leftarrow H(R')$	(2)
		$r \leftarrow H(R)$	
		$\beta \leftarrow r'r^{-1}$	(3)
		$e' \leftarrow H(m)$	
		$e \leftarrow \alpha\beta^{-1}e'$	(4)
	$\xleftarrow{e}$		
$s \leftarrow ke + dr$			
	$\xrightarrow{s}$		
		$s' \leftarrow s\beta$	
		$\sigma \leftarrow (R', s')$	

Fig. 2. R00 scheme: the signing protocol

The verification procedure for the message m and the signature (R, s) assumes verifying the equality $sP = H(R)Q + eR$, where $e = H(m)$.

Attack. Similar to the previous scheme, we show that for a fixed protocol transcription and message there are only few valid signatures that could be produced during the given protocol execution. Indeed, if the protocol transcription (R, e, s) and message m are fixed, then the $r = H(R)$ and $e' = H(m)$ values are also fixed. Consider the line (4) of the protocol

keeping in mind the relations from lines (1)–(3):

$$e = \alpha\beta^{-1}e' = \alpha(r'r^{-1})^{-1}e' = \alpha(r')^{-1}re' = \alpha H(\alpha R)^{-1}re'.$$

The equation $e = \alpha H(\alpha R)^{-1}re'$ for α has only few roots. However, α values are chosen uniformly at random, so the probability to choose α, that satisfies the equation above, during several protocol executions is negligible. Therefore, with overwhelming probability there exists only one signature with $R' = \alpha R$ component for which α satisfies the condition in line (4).

Hence, the criteria for breaking blindness can be constructed from the lines (1)–(4). The exact transcription (R, e, s) corresponds to the certain message m with hash-value e' and signature (R', s') iff the following condition holds:

$$\alpha R = R',$$

where $\alpha = e(e')^{-1}H(R')H(R)^{-1}$.

The attack on Schnorr-based blind signature [3] is defined using the same considerations.

Blindness understanding. The attack seems to become possible due to misunderstanding of blindness property. The authors of [3] considered blindness as the resistance to the attacks that lead to the disclosure of message m after the protocol execution. However, blindness property is much wider. Indeed, the protocol transcription may leak information about the signature value that also may violate blindness.

3.3. TNHV18 scheme

The similar attack is applicable to the aggregate blind signature scheme that was proposed in 2018 in [4] (more precisely, two cases of Signing protocol differring on the Requester side were proposed). It is also GOST-based scheme. Without loss of generality, we omit the aggregation property and present the description of the scheme in the case of a single Signer. Indeed, the following attack does not need the secret key knowledge and can be performed by anyone who can view the set of protocol transcriptions and the set of generated (message, signature) pairs.

Scheme description. The signing protocol is defined at Fig. 3.

The verification procedure for message m and signature (r, s) in both cases assumes computing point $R = e^{-1}sP - e^{-1}rQ$, where $e = H(m)$, and verifying the equality $R.x = r \bmod q$.

Attack. Consider the first case of the scheme. As usual, we show that for a fixed protocol transcription and message there are only few valid signatures that could be produced during the given protocol execution. If the protocol transcription (R, r, e, s) and message m are fixed, then the $e' = H(m)$ value is also fixed. Consider the line (4) of the protocol keeping in mind the relations from lines (1)–(3):

$$r = r'\beta^{-1}\alpha = (R'.x \bmod q)\beta^{-1}e(e')^{-1} = ((\beta R + \alpha P).x \bmod q)\beta^{-1}e(e')^{-1} = \\ = ((\beta R + e(e')^{-1}P).x \bmod q)\beta^{-1}e(e')^{-1}.$$

The equation

$$r = ((\beta R + e(e')^{-1}P).x \bmod q)\beta^{-1}e(e')^{-1}$$

for β has only few roots. However, β values are chosen uniformly at random, so the probability to choose β, such that the equation above is satisfied, during several protocol executions is negligible. Therefore, with overwhelming probability there is only one signature

The signing protocol

Signer(d, Q)		**Requester**(Q, m)		
		Case 1	Case 2	
$k \leftarrow\!\!\$\ \mathbb{Z}_q^*$				
$R \leftarrow kP$				
	R $\longrightarrow$			
		$\alpha, \beta \leftarrow\!\!\$\ \mathbb{Z}_q^*$	$\alpha, \beta \leftarrow\!\!\$\ \mathbb{Z}_q^*$	
		$e' \leftarrow H(m)$	$e' \leftarrow H(m)$	
		$e \leftarrow \alpha e'$	$e \leftarrow \beta e'$	(1)
		$R' \leftarrow \beta R + \alpha P$	$R' \leftarrow \alpha^{-1} R + P + Q$	(2)
		$r' \leftarrow R'.x \bmod q$	$r' \leftarrow R'.x \bmod q$	(3)
		$r \leftarrow r'\beta^{-1}\alpha$	$r \leftarrow \alpha\beta(r' + e')$	(4)
	r, e $\longleftarrow$			
$s \leftarrow ke + dr$				
	s $\longrightarrow$			
		$s' \leftarrow \beta\alpha^{-1}s + \alpha e'$	$s' \leftarrow \beta^{-1}\alpha^{-1}s + e'$	
		$\sigma \leftarrow (r', s')$	$\sigma \leftarrow (r', s')$	

Fif. 3. TNHV18 scheme: the signing protocol

with r' component equal to $(\beta R + e(e')^{-1}P).x \bmod q$, for which β satisfies the condition in line (4).

Hence, lines (1)–(4) provide the following criteria for breaking blindness. The exact transcription (R, r, e, s) corresponds to the certain message m with hash-value e' and signature (r', s') iff the following condition holds:

$$R'.x \bmod q = r',$$

where $R' = \beta R + \alpha P$, $\alpha = e(e')^{-1}$, $\beta = r'r^{-1}\alpha$.

The attack on the second case of the scheme is justified similarly. The exact transcription (R, r, e, s) corresponds to the certain message m with hash-value e' and signature (r', s') iff the following condition holds:

$$R'.x \bmod q = r',$$

where $R' = \alpha^{-1}R + P + Q$, $\alpha = r\beta^{-1}(r' + e')^{-1}$, $\beta = e(e')^{-1}$.

REFERENCES

1. *Chaum D.* Blind signatures for untraceable payments. D. Chaum, R. L. Rivest, and A. T. Sherman (eds.). Advances in Cryptology. Boston, MA, Springer, 1983, pp. 199–203.
2. *Gorbenko I., Yesina M., and Ponomar V.* Anonymous electronic signature method. Third Intern. Conf. PIC S&T, Kharkiv, Ukraine, 2016, pp. 47–50.

3. *Rostovtsev A. G.* Podpis' "vslepuyu" na ellipticheskoy krivoy dlya elektronnykh deneg [Blind signature on elliptic curve for e-cash]. Information Security Problems. Computer Systems, 2000, no. 1, pp. 40–45. (in Russian)
4. *Tan D. N., Nam H. N., Hieu M. N., and Van H. N.* New blind muti-signature schemes based on ECDLP. IJECE, 2018, vol. 8, no. 2, pp. 1074–1083.
5. *Juels A., Luby M., and Ostrovsky R.* Security of blind digital signatures. LNCS, 1997, vol. 1294, pp. 150–164.
6. *Pointcheval D. and Stern J.* Security arguments for digital signatures and blind signatures. J. Cryptology, 2000, vol. 13, no. 3, pp. 361–396.
7. *Okamoto T.* Efficient blind and partially blind signatures without random oracles. LNCS, 2006, vol. 3876, pp. 80–99.
8. *Hazay C., Katz J., Koo C. Y., and Lindell Y.* Concurrently-secure blind signatures without random oracles or setup assumptions. LNCS, 2007, vol. 4392, pp. 323–341.
9. *Camenisch J., Neven G., and Shelat A.* Simulatable adaptive oblivious transfer. LNCS, 2007, vol. 4515, pp. 573–590.
10. *Fischlin M. and Schroder D.* Security of blind signatures under aborts. LNCS, 2009, vol. 5443, pp. 297–316.

УДК 519.7 DOI 10.17223/20710410/62/3

ON THE NUMBER OF ℓ-SUITABLE BOOLEAN FUNCTIONS IN CONSTRUCTIONS OF FILTER AND COMBINING MODELS OF STREAM CIPHERS[1]

T. A. Bonich*, M. A. Panferov**, N. N. Tokareva*

*Novosibirsk State University, Novosibirsk, Russia,
**Sobolev Institute of Mathematics, Novosibirsk, Russia

E-mail: t.bonich@g.nsu.ru, m.panferov@g.nsu.ru, crypto1127@mail.ru

It is well known that every stream cipher is based on a good pseudorandom generator. For cryptographic purposes, we are interested in generating pseudorandom sequences with the maximum possible period. A feedback register is one of the most known cryptographic primitives that is used to construct stream ciphers. We consider periodic properties of pseudorandom sequences produced by filter and combiner generators (two known schemes of stream generators based on feedback registers). We analyze functions in these schemes that lead to output sequences of period at least a given number ℓ. We call such functions ℓ-suitable and count the exact number of them for an arbitrary n.

Keywords: *stream cipher, filter generator, combiner generator, Boolean function.*

О ЧИСЛЕ ℓ-ПОДХОДЯЩИХ БУЛЕВЫХ ФУНКЦИЙ В КОНСТРУКЦИЯХ ФИЛЬТРУЮЩЕЙ И КОМБИНИРУЮЩЕЙ МОДЕЛЕЙ ПОТОЧНЫХ ШИФРОВ

Т. А. Бонич*, М. А. Панферов**, Н. Н. Токарева*

*Новосибирский государственный университет, г. Новосибирск, Россия,
**Институт математики им. С. Л. Соболева, г. Новосибирск, Россия

Известно, что любой поточный шифр основан на хорошем генераторе псевдослучайных чисел. В криптографических целях изучаются различные способы генерации псевдослучайных последовательностей с максимально возможным периодом. Регистр сдвига с обратной связью — один из криптографических примитивов, который используется для построения поточных шифров. В работе изучаются периодические свойства псевдослучайных последовательностей, создаваемых фильтрующим и комбинирующим генераторами (известными схемами поточных генераторов на основе регистров сдвига с обратной связью). В этих схемах анализируются функции, которые приводят к выходным последовательностям с периодом не менее заданного числа ℓ. Мы называем такие функции ℓ-подходящими и подсчитываем их точное количество для произвольного n.

Ключевые слова: *поточный шифр, фильтрующий генератор, комбинирующий генератор, булева функция.*

[1]The work is supported by the Mathematical Center in Akademgorodok under the agreement No. 075-15-2022-282 with the Ministry of Science and Higher Education of the Russian Federation.

1. Introduction

Symmetric ciphers are usually divided into block and stream ciphers. Stream ciphers are considered as more fast but not as secure as block ciphers. One of the most known cryptographic primitives that is used to construct stream ciphers is a feedback shift register (FSR). There are many attacks and defenses on such ciphers and countermeasures against them, see, for instance, [1, 2].

The task of studying feedback registers leads to the problem of studying a pseudorandom sequence (gamma) generated by a feedback register [3]. Cryptographers who develop various pseudorandom number generators study the resulting gamma for the presence of the necessary properties. For example, it should have a large period, high linear complexity, and a uniform bit distribution [4]. It is often important that the sequence be reproducible [5]. Only if gamma has the required properties it can be considered for use in cryptographic applications [6]. An important property of the generated sequence is the randomness. There should be independence of values, unpredictability and uniform distribution [7]. Before using a pseudorandom sequence, it is necessary to evaluate its randomness. There are many different statistical tests for this, for example, NIST, Diehard, ENT test [8].

The properties of the pseudorandom sequence generated by FSR are well studied in the case when f is a linear function (LFSR). If f is nonlinear (see [9, 10]), there are too many open questions related to pseudorandom sequences that all are connected to analysis of nonlinear recurrent sequences, for example, see [11] for further review. That is why some nonlinear combinations of LFSRs are usually considered, for instance, filter and combining models of stream generators [6].

Let us recall a few definitions. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A *Boolean function in n variables* is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$. A *vector of values* for a given Boolean function f is the vector $\big(f(x^{(1)}), \ldots, f(x^{(2^n)})\big)$, where $x^{(1)}, \ldots, x^{(2^n)}$ are binary vectors in $\mathbb{F}_2^n$ that are lexicographically ordered. Any Boolean function f can be represented uniquely in its *algebraic normal form* (*ANF*): $f(x_1, \ldots, x_n) = \bigoplus\limits_{I \in \mathcal{P}(N)} a_I \Big(\prod\limits_{i \in I} x_i \Big)$, where $\mathcal{P}(N)$ is a power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2$. For a Boolean function f, the number of variables in the longest item of its ANF is called *the algebraic degree* of the function. If algebraic degree of f is not more than 1, then f is called *affine*. A function is called *linear* if it is affine and $f(0) = 0$. If algebraic degree of a function f is more than 1, then f is called *nonlinear*.

A feedback shift register consists of two parts: a binary block $x = (x_1, \ldots, x_n)$ of length n and a feedback function f, where f is a Boolean function in n variables. First, we fill the block x with constants, it is the *initial state* of the register. During the encryption process the register is changing its state using the feedback function. *Gamma* is a pseudorandom sequence generated by FSR. For functioning of the FSR the time is considered to be divided into clock cycles. On each clock cycle, the value $f(x)$ is calculated first, then the register state $x = (x_1, \ldots, x_{n-1}, x_n)$ goes to the state $x' = (x_2, \ldots, x_n, f(x))$, while the bit x_1 will be written as the first bit of the generated gamma. A *period* is a length of repeating part of gamma. If f is linear, we have LFSR. Similarly, *nonlinear feedback shift register* (NFSR) uses nonlinear Boolean function as a feedback function. It is known that LFSR can be also specified by a feedback polynomial. It is a polynomial of degree n defining bits to be summed. If $f(x_1, \ldots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n$, then the corresponding feedback polynomial is defined as $p(z) = a_1 z^n + a_2 z^{n-1} + \ldots + a_n z + 1$, where $a_i \in \mathbb{F}_2$, $i = 1, \ldots, n$. If $p(z)$ is a *primitive polynomial*, i.e., the primitive element of the field $\mathrm{GF}(2^n)$ is its root,

then the period of a pseudorandom sequence generated by LFSR is maximal, i.e., is equal to $2^n - 1$. As a result, primitive polynomials are mainly used in LSFRs.

There are many stream ciphers based on LFSR and NFSR. One of them is Grain, developed in 2004 [12]. It is constructed by combining model based on two shift registers, one with linear feedback and one with nonlinear feedback, and a nonlinear output function. Both linear and nonlinear shift register sizes are 80 bits. Another one is A5/1 cipher from GSM standard [13]. It has three LSFRs of lengths 19, 22 and 23 bits with irregular clocking. The registers are clocked in a stop/go fashion using a majority rule. The output is the sum of the last bits of the three registers. We could also mention the Gollmann cascade [14]. This cipher is representative of epy combining model. It consists of a series of LFSRs that are clock-controlled by the previous LFSR. If all the LFSRs have the same length n, the linear complexity of a system with k LFSRs is equal to $n(2^n - 1)^{k-1}$. Other examples of ciphers that are based on LFSR and NFSR are Geffe generator, Jennings generator, and Beth — Piper Stop-and-Go generator.

In this paper, we analyze pseudorandom sequences produced by filter and combiner generators. Namely, we study functions in these schemes that lead to pseudorandom sequences with a period not less than a given ℓ. We call such functions *ℓ-suitable* and count the exact number of them for an arbitrary n.

This paper is a modified continuation of the previous one [15].

2. The analysis of gamma for linear feedback shift register generators

2.1. Filter generators

The filter generator consists of a single LFSR of length n and uses a primitive polynomial to change states. A Boolean function $h(x_1, \ldots, x_n)$ applied to the current state generates a pseudorandom sequence (gamma). Let us note that the number of all possible functions $h(x_1, \ldots, x_n)$ is equal to 2^{2^n}. The work of the filter generator is shown in [16].

Let gamma be defined as $\gamma = (y_1, y_2, \ldots, y_{2^n-1})$, where $y_1 = h(x_1, \ldots, x_n)$, $y_2 = h(x_2, \ldots, x_n, f(x_1, \ldots, x_n))$, etc., and $f(x_1, \ldots, x_n)$ is the feedback function. Since the number of all nonzero states is equal to $2^n - 1$, the maximum possible value of the gamma period is also $2^n - 1$. We would like to determine all ℓ-suitable Boolean functions h in n variables. Functions which lead to gammas with a period less than a given ℓ we would call *ℓ-unsuitable*. Note that the number of such functions does not depend on a linear feedback function. But whether the function is ℓ-suitable or not for the given generator, depends on the feedback function. When we count the number of ℓ-suitable functions h, we do not consider a specific set of states. We say that there is a certain number of different states used by the generator (all sets that are generated by primitive polynomials fit this definition). Next, we study which pseudorandom sequences have the period not less than a given ℓ. We analyze the number of ℓ-unsuitable functions and the number of ℓ-suitable functions. Thus, our reasonings do not affect the specific order of the states. Therefore, there will be the exact calculated number of ℓ-suitable functions h for any set of states used by the generator.

Let us provide some examples of ℓ-suitable and ℓ-unsuitable functions. Let $n = 4$ be the length of a shift register, $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2$ be a feedback function, and $p(z) = z^4 + z^3 + 1$ be a corresponding primitive polynomial. Let $h_1(x_1, x_2, x_3, x_4) = x_2x_1 \oplus x_3x_1 \oplus x_3x_2 \oplus x_4x_1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$ and $h_2(x_1, x_2, x_3, x_4) = x_4x_2x_1 \oplus x_2x_1 \oplus x_3x_2 \oplus x_3 \oplus 1$ be Boolean functions in n variables. We present generated gamma for these functions in the Table.

States	0001	0010	0100	1001	0011	0110	1101	1010
$h_1(x_1, x_2, x_3, x_4)$	1	0	0	1	0	0	1	0
$h_2(x_1, x_2, x_3, x_4)$	1	0	1	1	0	1	1	0

States	0101	1011	0111	1111	1110	1100	1000	0001
$h_1(x_1, x_2, x_3, x_4)$	0	1	0	0	1	0	0	1
$h_2(x_1, x_2, x_3, x_4)$	1	0	1	1	0	0	1	1

Note that h_1 and h_2 generate the gamma with periods 3 and 15. If $\ell = 15$, i.e., we need a gamma with maximum period, then h_1 is an ℓ-unsuitable function, h_2 is a ℓ-suitable function.

To begin with, we show the calculation of the number of ℓ-unsuitable sequences. The number of aperiodic Boolean sequences has been studied in [17], we present our calculations of the number U_ℓ of sequences with a period less than ℓ (ℓ-unsuitable sequences).

Lemma 1. Let $\ell = q_1^{\omega_1} q_2^{\omega_2} \dots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of ℓ-unsuitable sequences is equal to

$$U_\ell = \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \dots + \beta_k + 1} 2^{q_1^{\omega_1 - \beta_1} \dots q_k^{\omega_k - \beta_k}} \right), \text{ where } \beta = (\beta_1, \dots, \beta_k).$$

Proof. We can count the number of ℓ-unsuitable sequences of length ℓ only. Consider sequences of length $\ell = q_1^{\omega_1} q_2^{\omega_2} \dots q_k^{\omega_k}$ with a period less than ℓ. Let A_i be a set of sequences that can be divided on q_i identical subsequences, $i = 1, \dots, k$. Then $A_i \cap A_j$ is a set of sequences that can be divided on $q_{i \cdot j}$ identical subsequences, where $i \neq j$, $i, j = 1, \dots, k$. Then $A_i \cup A_j$ is a set of sequences that can be divided on q_i or q_j identical subsequences, where $i \neq j$, $i, j = 1, \dots, k$. Hence, all ℓ-unsuitable sequences belong to the set $\bigcup\limits_{i=1}^{k} A_i$, and $U_\ell = |\bigcup\limits_{i=1}^{k} A_i|$. When a sequence is divided into q_i identical subsequences, the length of the subsequence is equal to $q_1^{\omega_1} q_2^{\omega_2} \dots q_i^{\omega_i - 1} \dots q_k^{\omega_k}$. Since the elements of the subsequences are in $\{0, 1\}$, then

$$|A_i| = 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_k^{\omega_k}},$$

$$|A_i \cap A_j| = 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_{(j-1)}^{\omega_{(j-1)}} q_j^{\omega_j - 1} q_{(j+1)}^{\omega_{(j+1)}} \dots q_k^{\omega_k}},$$

$$\dots$$

$$\Big| \bigcap_{i=1}^{k} A_i \Big| = 2^{q_1^{\omega_1 - 1} q_2^{\omega_2 - 1} \dots q_k^{\omega_k - 1}}.$$

Therefore, we can compute $|\bigcup\limits_{i=1}^{k} A_i|$ using the inclusion-exclusion principle:

$$\Big| \bigcup_{i=1}^{k} A_i \Big| = \sum_{i=1}^{k} |A_i| - \sum_{1 \leqslant i < j \leqslant k} |A_i \cap A_j| + \sum_{1 \leqslant i < j < t \leqslant k} |A_i \cap A_j \cap A_t| - \dots$$

$$+ (-1)^{k-1} |A_1 \cap A_2 \cap \dots \cap A_k| = \sum_{i=1}^{k} 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_k^{\omega_k}} -$$

$$- \sum_{1 \leqslant i < j \leqslant k} 2^{q_1^{\omega_1} q_2^{\omega_2} \dots q_{(i-1)}^{\omega_{(i-1)}} q_i^{\omega_i - 1} q_{(i+1)}^{\omega_{(i+1)}} \dots q_{(j-1)}^{\omega_{(j-1)}} q_j^{\omega_j - 1} q_{(j+1)}^{\omega_{(j+1)}} \dots q_k^{\omega_k}} +$$

$$\ldots + (-1)^{k-1} 2^{q_1^{\omega_1-1} q_2^{\omega_2-1} \ldots q_k^{\omega_k-1}} = \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \cdots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right),$$

where $\beta = (\beta_1, \ldots, \beta_k)$. ■

Let us prove the main result for filter generators.

Theorem 1. Let $n \in \mathbb{N}$ and ℓ is a divisor of $2^n - 1$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of ℓ-suitable Boolean functions in n variables for the filter generator with LFSR based on a primitive polynomial of degree n is equal to

$$2^{2^n} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \ldots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right), \text{ where } \beta = (\beta_1, \ldots, \beta_k).$$

Proof. From Lemma 1 we know the number U_ℓ of ℓ-unsuitable sequences of the length $2^n - 1$. We can write all states of the register one by one and from one state we get the second one as the next state. Consider the vector of values of a Boolean function h that generates our gamma. Since there is no zero state in the set of states (it generates the cycle of length 1), function h can take any value (0 or 1) on zero vector. That is why there are exactly two Boolean functions that generate the same sequence.

Hence, the number of ℓ-unsuitable functions is equal to $2\,U_\ell$. Then, the number of ℓ-suitable functions is $2^{2^n} - 2\,U_\ell$. ■

Similarly, we propose to count the number of Boolean functions in n variables leading to gammas with period exactly equal to ℓ.

Theorem 2. Let $n \in \mathbb{N}$ and ℓ is a divisor of $2^n - 1$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$. Then the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with LFSR based on a primitive polynomial of degree n is equal to

$$2^{\ell+1} - 2 \sum_{\beta \in \mathbb{F}_2^k, \beta \neq 0} \left((-1)^{\beta_1 + \ldots + \beta_k + 1} 2^{q_1^{\omega_1-\beta_1} \ldots q_k^{\omega_k-\beta_k}} \right), \text{ where } \beta = (\beta_1, \ldots, \beta_k).$$

Proof. To calculate the number of functions that lead to gammas with a period exactly equal to ℓ, we take the number of functions that lead to gammas with a period not greater than ℓ and subtract the number of functions that lead to gammas with a period less than ℓ.

The number of functions that lead to gammas with a period not greater than ℓ is equal to $2^{\ell+1}$. The remaining arguments are similar to those given in the proof of Theorem 1. ■

2.2. Combining model

Combiner generators use several LFSRs. Each register has its own length n_i and uses its own primitive polynomial for changing states. A Boolean function $h(X_1, \ldots, X_m)$ generates a pseudorandom sequence gamma, where X_i is a bit string of register i. The work of the combiner generator is shown in [16].

Since we do not use zero state in LFSR, the total number of states does not exceed $N = (2^{n_1} - 1)(2^{n_2} - 1) \ldots (2^{n_m} - 1)$. In this case, the maximum is reached when $(n_i, n_j) = 1$ for all $i, j \in \{1, \ldots, m\}$, $i \neq j$, and if all LFSRs have primitive feedback polynomials. Then a Boolean function can generate a gamma with a period ranging from 1 to N.

We consider a more general model of a combiner generator. This generalized combining model is used in ciphers such as Grain [12]. Note that the classical combining model does not allow to describe a number of modern stream ciphers based on the more complicated operating with bits from different registers.

Theorem 3. Let $n, m, n_1, \ldots, n_m \in \mathbb{N}$, $\sum\limits_{i=1}^{m} n_i = n$, and ℓ is a divisor of $(2^{n_1}-1)\ldots\times$ $\times(2^{n_m}-1)$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$, $k \in \mathbb{N}$. Then the number of ℓ-suitable Boolean functions in n variables for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$ all based on primitive polynomials is equal to

$$2^{2^n} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^k, \beta\neq 0} \left((-1)^{\beta_1+\ldots+\beta_k+1} 2^{q_1^{\omega_1-\beta_1}\ldots q_k^{\omega_k-\beta_k}}\right),$$

where $\beta = (\beta_1, \ldots, \beta_k)$.

Proof. Number of ℓ-unsuitable sequences for the combiner generators is equal to U_ℓ, in view of Lemma 1. Since we use only $(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)$ states and the total number of states is equal to $2^{n_1}\,2^{n_2}\ldots 2^{n_m} = 2^n$, then we have $2^n - (2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)$ states, where our function can be equal to 0 or 1. Therefore, for one of these states we have two functions. Thus, the number of ℓ-unsuitable Boolean functions in n variables for the combiner generators equals $2^{2^n-(2^{n_1}-1)(2^{n_2}-1)\ldots(2^{n_m}-1)}\,U_\ell$. Then, the number of ℓ-suitable functions is equal to $2^{2^n} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)}\,U_\ell$. ■

Similarly, we propose to count the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$.

Theorem 4. Let $n, m, n_1, \ldots, n_m \in \mathbb{N}$, $\sum\limits_{i=1}^{m} n_i = n$, and ℓ is a divisor of $(2^{n_1}-1)\ldots\times$ $\times(2^{n_m}-1)$, $\ell = q_1^{\omega_1} q_2^{\omega_2} \ldots q_k^{\omega_k}$, where q_i are pairwise distinct prime numbers, $\omega_i \in \mathbb{N}$, $k \in \mathbb{N}$. Then the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the combiner generator with LFSRs of lengths $n_1, \ldots, n_m$ all based on primitive polynomials is equal to

$$2^{\ell+(2^n-(2^{n_1}-1)\ldots(2^{n_m}-1))} - 2^{2^n-(2^{n_1}-1)\ldots(2^{n_m}-1)} \sum_{\beta\in\mathbb{F}_2^k, \beta\neq 0} ((-1)^{\beta_1+\ldots+\beta_k+1} 2^{q_1^{\omega_1-\beta_1}\ldots q_k^{\omega_k-\beta_k}}),$$

where $\beta = (\beta_1, \ldots, \beta_k)$.

Proof. The proof is similar to that of Theorem 2 with the remark that the number of functions that lead to gammas with a period not greater than ℓ is equal to $2^{\ell+(2^n-(2^{n_1}-1)\ldots(2^{n_m}-1))}$. ■

3. Functions for models with nonlinear registers

A nonlinear feedback shift register (NFSR) consists of two parts: a binary vector $x = (x_1, \ldots, x_n)$ of length n and a nonlinear state function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ in n variables.

Similarly to the linear case, let us consider the filter generator. We assume that NFSR passes over all 2^n states, i.e., it has the maximum possible period.

Theorem 5. Let $n \in \mathbb{N}$ and $\ell = 2^t$, $t \leqslant n$. Then the number of ℓ-suitable Boolean functions in n variables for the filter generator with NFSR of the maximum possible period is equal to $2^{2^n} - 2^{2^{t-1}}$.

Proof. The number of ℓ-unsuitable sequences for the filter generator with NFSR is equal to $2^{2^{t-1}}$. Since we use all the states then the number of ℓ-unsuitable sequences is equal to the number of ℓ-unsuitable Boolean functions. Hence, the number of ℓ-unsuitable Boolean functions in n variables for the filter generator with NFSR is equal to $2^{2^{t-1}}$. Therefore, the number of ℓ-suitable functions is $2^{2^n} - 2^{2^{t-1}}$. ■

Similarly, we propose to count the number of Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with NFSR.

Theorem 6. Let $n \in \mathbb{N}$ and $\ell = 2^t$, where $t \leqslant n$. Then the number of ℓ-suitable Boolean functions in n variables that lead to gammas with period exactly equal to ℓ for the filter generator with NFSR of the maximum possible period is equal to $2^\ell - 2^{2^{t-1}}$.

Proof. To calculate the number of functions that lead to gammas with period exactly equal to ℓ, we take the number of functions that lead to gammas with a period not greater than ℓ (i.e., 2^ℓ) and subtract the number of functions that lead to gammas with a period less than ℓ (i.e., $2^{2^{t-1}}$). ■

There is another question related to NFSRs: how to determine for which nonlinear feedback functions NFSR of length n generates gamma with the maximum possible period 2^n? This question is still open.

REFERENCES

1. *Golić J. D.* On the security of nonlinear filter generators. LNCS, 1996, vol. 1039, pp. 173–188.
2. *Courtois N. T. and Meier W.* Algebraic attacks on stream ciphers with linear feedback. LNCS, 2003, vol. 2656, pp. 345–359.
3. *Salhab O., Jweihan N., Jodeh M. A., et al.* Survey paper: Pseudo random number generators and security tests. J. Theor. Appl. Inform. Technology, 2018, vol. 96, pp. 1951–1970.
4. *Hamza R.* A novel pseudo random sequence generator for image-cryptographic applications. J. Inform. Security Appl., 2017, vol. 35, pp. 119–127.
5. *Goresky M. and Klapper A.* Algebraic Shift Register Sequences. Cambridge, Cambridge University Press, 2012. 496 p.
6. *Menezes A. J., Van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. Boca Raton, CRC Press, 1996. 780 p.
7. *Márton K., Suciu A., Săcărea C., and Cret O.* Generation and testing of random numbers for cryptographic applications. Proc. Romanian Academy, 2012, vol. 13, pp. 368–377.
8. *Parvees M. Y. M., Samath J. A., and Bose B. P.* Cryptographically secure diffusion sequences — an attempt to prove sequences are random. Advances in Big Data and Cloud Computing. Advances in Intelligent Systems and Computing, 2019, vol. 750, pp. 433–442.
9. *Key E. L.* An analysis of the structures and complexity of nonlinear binary sequence generators. IEEE Trans. Inform. Theory, 1976, vol. 22, pp. 732–736.
10. *Gorodilova A. A.* Ot kriptoanaliza shifra k kriptograficheskomu svoystvu bulevoy funktsii [From cryptanalysis to cryptographic property of a Boolean function]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 16–44. (in Russian)
11. *Gluhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra [Algebra]. Moscow, Gelios ARV Publ., 2003. 336 p. (in Russian)
12. *Hell M., Johansson T., and Meier W.* Grain: A stream cipher for constrained environments. Intern. J. Wireless Mobile Computing, 2007, vol. 2, no. 1, pp. 86–93.
13. *Canteaut A.* A5/1. Encyclopedia of Cryptography and Security, Boston, Springer, 2011, pp. 1–2.
14. *Gollmann D.* Kaskadenschaltungen taktgesteuerter Schieberegister als Pseudozufallszahlengeneratoren. PhD thesis, Johannes Kepler Universität Linz, Wien, 1986. (in German)
15. *Bonich T. A., Panferov M. A., and Tokareva N. N.* On the number of unsuitable Boolean functions in constructions of filter and combining models of stream ciphers. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2020, vol. 13, pp. 78–80.

16. *Carlet C.* Boolean functions for cryptography and error-correcting codes. Y. Crama and P. L. Hammer (eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge, Cambridge University Press, 2010, pp. 257–397.
17. *Golomb S. W.* Shift Register Sequences. San Francisco, Holden-Day, 1967.

УДК 519.7 DOI 10.17223/20710410/62/4

MATHEMATICAL PROBLEMS AND SOLUTIONS OF THE NINTH INTERNATIONAL OLYMPIAD IN CRYPTOGRAPHY NSUCRYPTO[1]

V. A. Idrisova[2], N. N. Tokareva[2], A. A. Gorodilova[2], I. I. Beterov[3], T. A. Bonich[2], E. A. Ishchukova[4], N. A. Kolomeec[2], A. V. Kutsenko[2], E. S. Malygina[5], I. A. Pankratova[6], M. A. Pudovkina[7], A. N. Udovenko[8]

[2] *Novosibirsk State University, Novosibirsk, Russia*
[3] *Rzhanov Institute of Semiconductor Physics, Novosibirsk, Russia*
[4] *Southern Federal University, Taganrog, Russia*
[5] *HSE, Moscow, Russia*
[6] *Tomsk State University, Tomsk, Russia*
[7] *National Research Nuclear University MEPhI, Moscow, Russia*
[8] *CryptoExperts, Paris, France*

E-mail: vvitkup@yandex.ru, crypto1127@mail.ru, gorodilova@math.nsc.ru, beterov@isp.nsc.ru, t.bonich@g.nsu.ru, uaishukova@sfedu.ru, kolomeec@math.nsc.ru, alexandrkutsenko@bk.ru, emalygina@hse.ru, pank@mail.tsu.ru, maricap@rambler.ru, aleksei.udovenko1@gmail.com

Every year the International Olympiad in Cryptography Non-Stop University CRYPTO (NSUCRYPTO) offers mathematical problems for university and school students and, moreover, for professionals in the area of cryptography and computer science. The main goal of NSUCRYPTO is to draw attention of students and young researchers to modern cryptography and raise awareness about open problems in the field. We present problems of NSUCRYPTO'22 and their solutions. There are 16 problems on the following topics: ciphers, cryptosystems, protocols, e-money and cryptocurrencies, hash functions, matrices, quantum computing, S-boxes, etc. They vary from easy mathematical tasks that could be solved by school students to open problems that deserve separate discussion and study. So, in this paper, we consider several open problems on three-pass protocols, public and private keys pairs, modifications of discrete logarithm problem, cryptographic permutations, and quantum circuits.

Keywords: *cryptography, ciphers, protocols, number theory, S-boxes, quantum circuits, matrices, hash functions, interpolation, cryptocurrencies, postquantum cryptosystems, Olympiad, NSUCRYPTO.*

[1] The work of the first, second, third, fifth, seventh and eighth authors was supported by the Mathematical Center in Akademgorodok under the agreement No. 075-15-2022-282 with the Ministry of Science and Higher Education of the Russian Federation. The work of the ninth author was supported by the Kovalevskaya North-West Centre of Mathematical Research under the agreement No. 075-02-2023-934 with the Ministry of Science and Higher Education of the Russian Federation. The work is also supported by Novosibirsk State University and Kryptonite.

МАТЕМАТИЧЕСКИЕ ПРОБЛЕМЫ И РЕШЕНИЯ ДЕВЯТОЙ МЕЖДУНАРОДНОЙ ОЛИМПИАДЫ ПО КРИПТОГРАФИИ NSUCRYPTO

В. А. Идрисова[2], Н. Н. Токарева[2], А. А. Городилова[2], И. И. Бетеров[3], Т. А. Бонич[2], Е. А. Ищукова[4], Н. А. Коломеец[2], А. В. Куценко[2], Е. С. Малыгина[5], И. А. Панкратова[6], М. А. Пудовкина[7], А. Н. Удовенко[8]

[2]*Новосибирский государственный университет, г. Новосибирск, Россия*
[3]*Институт физики полупроводников СО РАН, г. Новосибирск, Россия*
[4]*Южный федеральный университет, г. Таганрог, Россия*
[5]*МИЭМ НИУ ВШЭ, г. Москва, Россия*
[6]*Томский государственный университет, г. Томск, Россия*
[7]*Национальный исследовательский ядерный университет «МИФИ», г. Москва, Россия*
[8]*CryptoExperts, г. Париж, Франция*

Ежегодно Международная олимпиада по криптографии Non-Stop University CRYPTO (NSUCRYPTO) предлагает математические задачи для студентов университетов и школ, а также для профессионалов в области криптографии и информатики. Основная цель NSUCRYPTO — привлечь внимание студентов и молодых исследователей к современной криптографии, в частности к её открытым проблемам. Мы рассматриваем задачи NSUCRYPTO'22 и их решения. Приводятся 16 задач по следующим темам: шифры, криптосистемы, протоколы, электронные деньги и криптовалюты, хэш-функции, матрицы, квантовые вычисления, S-блоки и т. д. Задачи варьируются от простых математических задач, которые могут быть решены школьниками, до открытых задач, заслуживающих отдельного обсуждения и исследования. Рассматриваются несколько открытых задач по трёхпроходным протоколам, парам открытых и закрытых ключей, модификациям задачи дискретного логарифмирования, криптографическим перестановкам и квантовым схемам.

Ключевые слова: *криптография, шифры, протоколы, теория чисел, S-блоки, квантовые схемы, матрицы, хэш-функции, интерполяция, криптовалюты, постквантовые криптосистемы, олимпиада, NSUCRYPTO.*

1. Introduction

Non-Stop University CRYPTO (**NSUCRYPTO**) is the unique international competition for professionals, school and university students, providing various problems on theoretical and practical aspects of modern cryptography [1]. The main goal of the olympiad is to draw attention of young researchers not only to competetive fascinating tasks, but also to sophisticated and tough scientific problems at the intersection of mathematics and cryptography. That is why each year there are several open problems in the list of tasks that require rigorous studying and, if solved, deserve a separate publication. Since NSUCRYPTO holds via the Internet, everybody can easily take part in it. Rules of the Olympiad, the archive of problems, solutions and mach more can be found on the official website [2].

The first Olympiad was held in 2014, since then more than 3000 students and specialists from almost 70 countries took part in it. The Program committee now is including 22 members from cryptographic groups all over the world. Main organizers and partners are Cryptographic Center (Novosibirsk), Mathematical Center in Akademgorodok,

Novosibirsk State University, KU Leuven, Tomsk State University, Belarusian State University, Kovalevskaya North-West Center of Mathematical Research, and Kryptonite.

This year, 37 participants in the first round and 27 teams in the second round from 14 countries have become the winners (see the list [3]). We proposed 16 problems to participants and 5 of them were entirely open or included some open questions. Totally, there were 623 particpants from 36 countries.

Following the results of each Olympiad, we also publish scientific papers with detailed solutions and some analysis of the solutions proposed by the participants, including advances on unsolved ones [4–11].

2. An overview of open problems

One of the main characteristic of the Olympiad is that unsolved scientific problems are proposed to the participants in addition to problems with known solutions. All 31 open problems that have been offered since the first NSUCRYPTO can be found in [12]. Some of these problems have been of great interest to cryptographers and mathematicians for many years. These are such problems as "APN permutation" (2014), "Big Fermat numbers" (2016), "Boolean hidden shift and quantum computings" (2017), "Disjunct Matrices" (2018), and others.

Despite the fact that it is noted that the problem is open and therefore requires a lot of work to advance it, some of the problems we proposed have been solved or partially solved by our participants during the Olympiad. For example, problems "Algebraic immunity" (2015), "Sylvester matrices" (2018), "Miller — Rabin revisited" (2020) were solved completely. Also, partial solutions were suggested for problems "Curl27" (2019), "Bases" (2020), "Quantum error correction" (2021), and "s-Boolean sharing" (2021).

Moreover, some researchers continue to work on solutions even after the Olympiad was over. For example, the authors of [13] proposed a complete solution for the problem "Orthogonal arrays" (2018). Partial solutions for another open problem, "A secret sharing" (2014), were presented in [14, 15], and a recursive algorithm for finding the solution was proposed in [16].

This year, two open problems have been solved during the Olympiad. These are problems "Public keys for e-coins" (Problem 4.10) and "Quantum entanglement" (Problem 4.16).

3. Problem structure of the Olympiad

There were 16 problems stated during the Olympiad, some of them were included in both rounds (Tables 1 and 2). Section A of the first round consisted of six problems, while Section B of the first round consisted of eight problems. The second round was composed of eleven problems; five of them included unsolved questions (awarded special prizes).

Table 1

Problems of the first round

No.	Problem title	Max score
1	Numbers and points	4
2	Wallets	4
3	A long-awaited event	4
4	Hidden primes	4
5	Face-to-face	4
6	Crypto locks	4 + open problem

Section A

No.	Problem title	Max score
1	Numbers and points	4
2	Hidden primes	4
3	Face-to-face	4
4	Matrix and reduction	4
5	Reversing a gate	6
6	Bob's symbol	8
7	Crypto locks	4 + open problem
8	Public keys for e-coins	Open problem

Section B

Table 2

Problems of the second round

No.	Problem title	Max score
1	CP problem	Open problem
2	Interpolation with errors	8
3	HAS01	8
4	Weaknesses of the PHIGFS	8
5	Super dependent S-box	6 + open problem
6	Quantum entanglement	6 + open problem
7	Numbers and points	4
8	Bob's symbol	8
9	Crypto locks	4 + open problem
10	Public keys for e-coins	Open problem
11	A long-awaited event	4

4. Problems and their solutions

In this section, we formulate all the problems of 2022 year Olympiad and present their detailed solutions, in some particular cases we also pay attention to solutions proposed by the participants.

4.1. Problem "Numbers and points"

Formulation

Decrypt the message in Fig. 1.

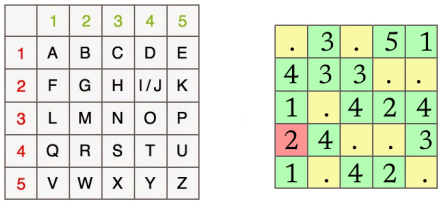


Fig. 1. The illustration for the problem "Numbers and points"

Solution

There is a board made up of numbers and dots on the right half of Fig. 1. One cell is highlighted in red. The path along which the sensible plaintext is encrypted begins with it (Fig. 2). The ciphertext has a "number – number – dot" pattern. The ciphertext is the following:

21 . 42 . 24 . 15 . 33 . 14 .

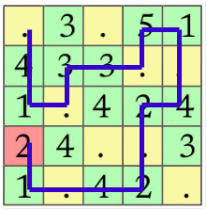


Fig. 2. The path along which the sensible plaintext is encrypted

The table in the left half of Fig. 1 refers to the Polybius square. Each letter is represented by its coordinates in the grid. Comparing the numbers from the ciphertext with the coordinates of the letters in the Polybius square, we get:

F . R. (I/J) . E . N . D .

Picking I from (I/J), we get the sensible plaintext **FRIEND**.

The problem looked simple but there was only one complete solution proposed by the team of Robin Jadoul (Belgium), Esrever Yu (Taiwan) and Jack Pope (United Kingdom).

4.2. Problem "Wallets"

Formulation

Bob has a wallet with 2022 NSUcoins. He decided to open a lot of new wallets and spread his NSUcoins among them. The platform that operates his wallets can distribute content of any wallet between 2 newly generated ones, charging 1 NSUcoin commission and removing the initial wallet.

He created a lot of new wallets, but suddenly noticed that all of his wallets contain exactly 8 NSUcoins each. Bob called the platform and told that there might be a mistake. How did he notice that?

Solution

Suppose that there were n such operations, so we had $n+1$ wallets. Since 1 NSUcoin is charged for each operation, the total commission is equal to n. Therefore, we have $2022-n = 8(n+1)$ and $2014 = 9n$, but that is impossible since n is a natural number. The most accurate and detailed solution was sent by Egor Desyatkov (Russia).

4.3. Problem "A long-awaited event"

Formulation

Bob received from Alice the secret message

`L78V8LC7GBEYEE`

informing him about some important event.

It is known that Alice used an alphabet with 37 characters from `A` to `Z`, from `0` to `9` and a space. The character encoding is shown in Table 3.

Table 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	SPACE	
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	

For the encryption, Alice used a function f such that $f(x) = ax^2 + bx + c \bmod 37$ for some integers a, b, c and f satisfies the property

$$f(x-y) - 2f(x)f(y) + f(1+xy) = 1 \pmod{37} \quad \text{for any integers } x, y.$$

Decrypt the message that Bob received.

Solution

Let $y = 0$:

$$f(x) - 2f(x)f(0) + f(1) = 1 \pmod{37},$$
$$f(x)(1 - 2f(0)) = 1 - f(1) \pmod{37}.$$

Since f is not a constant function, we have that both sides of the equation above are zeros, so $f(0) = 19 \pmod{37}$ and $f(1) = 1 \pmod{37}$. From this we obtain that $c = 19$. Let $y = -1$:

$$f(1 + x) + f(1 - x) = 1 + 2f(x)f(-1) \pmod{37}.$$

By replacing $x \mapsto (-x)$ we get

$$f(1 - x) + f(1 + x) = 1 + 2f(-x)f(-1) \pmod{37}.$$

Left sides of the last two expressions are equal, therefore $f(x) = f(-x) \pmod{37}$ that is f is even function, provided $f(-1) \neq 0 \pmod{37}$. We can check the last condition by putting $x = 0$, $y = 1$ to the initial relation on f, that yields $f(-1) = 1 \neq 0 \pmod{37}$. Therefore, $f(x) = f(-x) \pmod{37}$ for any integer x, hence $b = 0$.

From $f(1) = 1 \pmod{37}$ we reveal the value of the coeffecient a that is equal to 19. Thus, we have $f(x) = 19\left(x^2 + 1\right) \pmod{37}$, then for recovering of the plaintext we use the inverse expression $x = \pm\sqrt{2f(x) + 36} \pmod{37}$ and for every symbol of the ciphertext we choose the appropriate variant of the corresponding symbol of the plaintext:

$$\text{L78V8LC7GBEYEE} \hookrightarrow \text{NSUCRYPTO 2022}.$$

The only correct solution was sent by William Zhang (United Kingdom).

4.4. Problem "Hidden primes"

Formulation

The Olympiad team rented an office at the Business Center, 1-342 room, on 1691th street for NSUCRYPTO-2022 competition for 0 nsucoins (good deal!). Mary from the team wanted to create a task for the competition and she needed to pick up three numbers for this task. She used to find an inspiration in numbers around her and various equations with them. After some procedure, she found three prime numbers! It is interesting that when Mary added the smallest number to the largest one and divided the sum by the third number, the result was also the prime number.

Can you guess these numbers she found?

Solution

We may assume from the problem statement that Mary used some numbers around her and some equations with them in order to find these three numbers. We may also get from the description that she used only one procedure to find these hidden numbers.

So all three numbers are connected by some procedure and the numbers around Mary are used, from phrase "various equations" we can assume that there exists some equation with these numbers as coefficients. There were 5 numbers around Mary: 1, −342, 1691, −2022 and 0.

In addition, analyzing the picture (Fig. 3), you can see the curve, cubes with 4 letters: a, b, c, d and the cube with 0. The curve resembles a graph of a cubic function and the

letters on the cubes look like coefficients of a cubic function. The cube with 0 gives a hint for the use of a cubic equation.

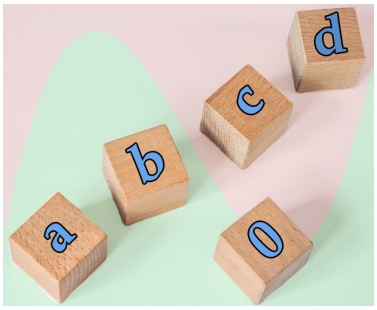


Fig. 3. The illustration for the problem "Hidden primes"

Let us substitute the numbers from the problem statement into the cubic equation. Solving the equation $x^3 - 342x^2 + 1691x - 2022 = 0$ we find the roots 2, 3, 337. All three numbers are prime and satisfy the condition from the statement: $(2 + 337)/3 = 113$, where 113 is also a prime number.

Best solutions were proposed independently by Konstantin Romanov (Russia), Vasiliy Kadykov (Russia) and Sergey Zabolotskiy (Russia).

4.5. Problem "Face-to-face"

Formulation

Alice picked a new pin code (4 pairwise distinct digits from $\{1, 2, \ldots, 9\}$) for her credit card such that all digits have the same parity and are arranged in increasing order. Bob and Charlie wanted to guess her pin code. Alice said that she can give each of them a hint but face-to-face only.

Bob alone came to Alice and she told him that the sum of her pin code digits is equal to the number of light bulbs in the living room chandelier. Bob replied that he didn't have enough information yet to guess the code and left. After that, Charlie alone came to Alice and she told him that if we find the product of all pin code digits and then sum up digits of those product, this result number would be equal to the amount of books on the shelf. Charlie also replied that he didn't have enough information to guess the code yet and left.

Unfortunately, Eve was eavesdropping in the next apartment and, after Charlie had left, she immediately found out Alice pin code despite that she had never seen those chandelier and bookshelf. Could you find the pin code too?

Solution

Let P be the pin code. Since all the digits of P have the same parity and are arranged in increasing order, we have only six options (Table 4).

Table 4

Pin code P	The sum of digits	The product of digits	The sum of product digits
1357	16	105	6
1359	18	135	9
1379	20	189	18
1579	22	315	9
2468	20	384	15
3579	24	945	18

Since Bob could not guess the code, the sum of digits must allow at least two options for the code, so we have $P \in \{1379, 2468\}$. Since Charlie could not guess the code either, we have the same problem for the sum of product digits and it follows that $P \in \{1359, 1579, 1379, 3579\}$. Therefore, the pin code is equal to 1379.

The best solutions to this problem were sent by Henning Seidler (Germany), Himanshu Sheoran (India) and Phuong Hoa Nguyen (France).

4.6. Problem "Crypto locks"

Formulation

Alice and Bob are wondering about the creation of a new version for the Shamir three-pass protocol. They have several ideas about it.

The Shamir three-pass protocol was developed more than 40 years ago. Recall it. Let p be a big prime number. Let Alice take two secret numbers c_A and d_A such that $c_A d_A = 1 \pmod{(p-1)}$. Bob takes numbers c_B and d_B with the same property. If Alice wants to send a secret message m to Bob, where m is an integer number, $1 < m < p-1$, then she calculates $x_1 = m^{c_A} \bmod p$ and sends it to Bob. Then Bob computes $x_2 = x_1^{c_B} \bmod p$ and forwards it back to Alice. On the third step, Alice founds $x_3 = x_2^{d_A} \bmod p$ and sends it to Bob. Finally, Bob recovers m as $x_3^{d_B} \bmod p$ according to Fermat's Little theorem.

It is possible to think about action of c_A and d_A over the message as about locking and unlocking, see Fig. 4.

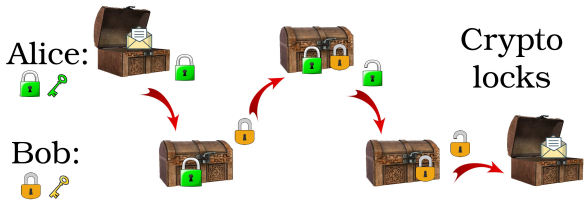


Fig. 4. The illustration for the problem "Crypto locks"

Alice and Bob decided to change the scheme by using symmetric encryption and decryption procedures instead of locking and unlocking with c_A, c_B, d_A, and d_B.

Q1 Propose some simple symmetric ciphers that would be possible to use in such scheme. What properties for them are required? Should Alice and Bob use the same cipher (with different own keys) or not?

Q2 **Problem for a special prize!** Could you find such symmetric ciphers that make the modified scheme to be secure as before? Please, give your reasons and proofs.

Solution

Q1 Assume that Alice and Bob use functions Enc_A, Dec_A and Enc_B, Dec_B for encryption and decryption, respectively. Suppose that Alice wants to send the message m, then the three-pass protocol will look as follows:

- Alice calculates $\mathrm{Enc}_A(m, k_A)$, where k_A is her secret key, and sends it to Bob.
- Bob computes $\mathrm{Enc}_B(\mathrm{Enc}_A(m, k_A), k_B)$, where k_B is his secret key, and forwards it to Alice.
- Finally, Alice computes $\mathrm{Dec}_A(\mathrm{Enc}_B(\mathrm{Enc}_A(m, k_A), k_B), k_A)$ and sends it to Bob.

For Bob to recover m, the following property must be true:

$$\mathrm{Dec}_B(\mathrm{Dec}_A(\mathrm{Enc}_B(\mathrm{Enc}_A(m, k_A), k_B), k_A), k_B) = m.$$

The most common approach was to use encryption functions that commute with each other. In that case, if Alice wants to send a secret message m to Bob, then she calculates $x = m \circ k_A$ and sends it to Bob. Then Bob computes $x_2 = x \circ k_B$ and forwards it back to Alice. On the third step, Alice finds $x_3 = x_2 \circ k_A^{-1}$ and sends it to Bob. Finally, the commutative property of operation $\circ$ allows Bob to recover m as $x_3 \circ k_B^{-1}$.

Remark 1. Note that if Eve can intercept all three messages, then she can obtain m if she could compute x_2^{-1}, since $x \circ x_3 \circ x_2^{-1} = m$. As a result, all schemes that use ciphers with only XOR operation (the most common suggestion by the participants) have this weakness.

Regarding **Q2**, one interesting idea found by a few participants is to use the product of matrices for encryption and decryption, with the additional condition that the matrix M associated with the message m is singular. That additional condition appears as a countermeasure against the attack described in Remark 1. However, such schemes require additional security analysis.

Another interesting idea suggested by the team of Himanshu Sheoran, Gyumin Roh and Yo Iida (India, South Korea, Japan) was to base the scheme on permutations that commute with each other. Note that a three-pass cryptographic protocol with a similar idea was presented in [17].

4.7. Problem "Matrix and reduction"

Formulation

Alice used an alphabet with 30 characters from `A` to `Z` and `0`, `1`, «`,`», «`!`». The character encoding is shown in Table 5.

Table 5

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
P	Q	R	S	T	U	V	W	X	Y	Z	0	1	,	!
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Encryption. The plaintext is divided into consequent subwords of length 4 that are encrypted independently via the same encryption (2×2)-matrix F with elements from $\mathbb{Z}_{30}$. For example, let the j-th subword be `WORD` and the encryption matrix F be equal to

$$F = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix}.$$

The matrix that corresponds to `WORD` is denoted by P_j and the matrix that corresponds to the encryption result of `WORD` is C_j and is calculated as follows:

$$C_j = F \cdot P_j = \begin{pmatrix} 11 & 9 \\ 11 & 10 \end{pmatrix} \begin{pmatrix} 22 & 17 \\ 14 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 4 \\ 22 & 7 \end{pmatrix} \pmod{30},$$

that is, the j-th subword of the ciphertext is `IWEH`.

Eve has intercepted a ciphertext that was transmitted from Alice to Bob:

`CYPHXWQE!WNKHZOZ`

Also, she knows that the third subword of the plaintext is `FORW`. Will Eve be able to restore the original message?

Solution

The third word of the plaintext is `FORW`:

$$P = \texttt{FORW} = \begin{pmatrix} 5 & 17 \\ 14 & 22 \end{pmatrix} \pmod{30}.$$

The ciphertext corresponding to it is

$$C = \texttt{!WNK} = \begin{pmatrix} 29 & 13 \\ 22 & 10 \end{pmatrix} \pmod{30}.$$

Since $C_3 = F \cdot P_3$, where F is the encryption matrix, the matrix for the decryption could have the following form:

$$D = P_3 \cdot C_3^{-1}.$$

But $\det(C_3) = 4 \pmod{30}$ and $\gcd(4, 30) \neq 1$, that is, such matrix does not exist modulo 30. So we will consider the following calculations by reduction modulo 15.

Let $\overline{P_3} = P_3 \pmod{15}$, $\overline{C_3} = C \pmod{15}$, and $\overline{F} = F \pmod{15}$. We have

$$\overline{F}^{-1} = \overline{P_3}\left(\overline{C_3}\right)^{-1} = \begin{pmatrix} 9 & 2 \\ 4 & 9 \end{pmatrix} \pmod{15},$$

consequently,

$$D = \begin{pmatrix} 9 & 2 \\ 4 & 9 \end{pmatrix} + 15\,F_0 \pmod{30},$$

where F_0 is 2×2 binary matrix. We have $D \cdot C_3 = P_3$, or

$$\overline{F}^{-1} \begin{pmatrix} 29 & 13 \\ 22 & 10 \end{pmatrix} + 15\,F_0 \begin{pmatrix} 29 & 13 \\ 22 & 10 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 14 & 22 \end{pmatrix} \pmod{30}.$$

Finally, we obtain

$$\begin{pmatrix} 5 & 17 \\ 14 & 22 \end{pmatrix} = F_0 \begin{pmatrix} 15 & 15 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 14 & 22 \end{pmatrix} \pmod{30}.$$

If we set $F_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then it is clear that only the values $a = c = 0$ and $b = 1$, $d = 0$ give us the answer `GOODLUCKFORWIN!!`.

Best solutions for this problem were sent by Pieter Senden (Belgium) and by Sergey Zabolotskiy (Russia).

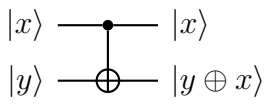
4.8. Problem "Reversing a gate"

Formulation

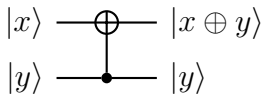
Daniel continues to study quantum circuits. A controlled NOT (CNOT) gate is the most complex quantum gate from the universal set of gates required for quantum computation. This gate acts on two qubits and makes the following transformation:

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle.$$

This gate is clearly asymmetric. The first qubit is considered as the control qubit, and the second is the target qubit. CNOT is described by the following quantum circuit ($x, y \in \mathbb{F}_2$):



The problem. Help Daniel to design a circuit in a special way that reverses CNOT gate:



It makes the following procedure: $|00\rangle \to |00\rangle$, $|01\rangle \to |11\rangle$, $|10\rangle \to |10\rangle$, $|11\rangle \to |01\rangle$. To do this, you should modify the original CNOT gate without re-ordering the qubits but by adding some single-qubit gates from the following (Table 6).

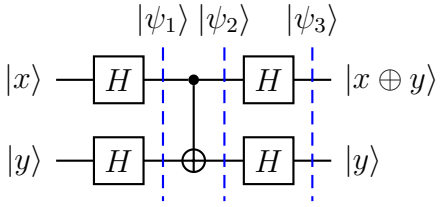
Table 6

Pauli-X gate	$\|x\rangle$ — X — $\|x \oplus 1\rangle$	Acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
Pauli-Z gate	$\|x\rangle$ — Z — $(-1)^x \|x\rangle$	Acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$
Hadamard gate	$\|x\rangle$ — H — $\frac{\|0\rangle + (-1)^x \|1\rangle}{\sqrt{2}}$	Acts on a single qubit in the state $\|x\rangle$, $x \in \{0,1\}$

Remark 2. Let us briefly formulate the key points of quantum circuits. A qubit is a two-level quantum mechanical system whose state $|\psi\rangle$ is the superposition of basis quantum states $|0\rangle$ and $|1\rangle$. The superposition is written as $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, where α_0 and α_1 are complex numbers, called amplitudes, that possess $|\alpha_0|^2 + |\alpha_1|^2 = 1$. The amplitudes α_0 and α_1 have the following physical meaning: after the measurement of a qubit which has the state $|\psi\rangle$, it will be observed in the state $|0\rangle$ with probability $|\alpha_0|^2$ and in the state $|1\rangle$ with probability $|\alpha_1|^2$. In order to operate with multi-qubit systems, we consider the bilinear operation $\otimes : |x\rangle, |y\rangle \to |x\rangle \otimes |y\rangle$ on $x, y \in \{0,1\}$ which is defined on pairs $|x\rangle, |y\rangle$ and, by bilinearity, is expanded on the space of all linear combinations of $|0\rangle$ and $|1\rangle$. When we have two qubits in states $|\psi\rangle$ and $|\varphi\rangle$ correspondingly, the state of the whole system of these two qubits is $|\psi\rangle \otimes |\varphi\rangle$. In general, for two qubits we have $|\psi\rangle = \alpha_{00}|0\rangle \otimes |0\rangle + \alpha_{01} |0\rangle \otimes |1\rangle + + \alpha_{10} |1\rangle \otimes |0\rangle + \alpha_{11} |1\rangle \otimes |1\rangle$. The physical meaning of complex numbers α_{ij} is the same as for one qubit, so we have the essential restriction $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. We use more brief notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$. In order to verify your circuits, you can use different quantum circuit simulators, for example, see [18].

Solution

The desired circuit has the following form for any $x, y \in \mathbb{F}_2$:



Indeed, with initial state $|x\rangle |y\rangle$ we have

$$|\psi_1\rangle = \left(\frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + (-1)^y |1\rangle}{\sqrt{2}}\right) = \\ = \frac{|00\rangle + (-1)^y |01\rangle + (-1)^x |10\rangle + (-1)^{x \oplus y} |11\rangle}{2},$$

$$|\psi_2\rangle = \frac{|00\rangle + (-1)^y |01\rangle + (-1)^x |11\rangle + (-1)^{x\oplus y} |10\rangle}{2} =$$
$$= \left(\frac{|0\rangle + (-1)^{x\oplus y} |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + (-1)^y |1\rangle}{\sqrt{2}}\right),$$
$$|\psi_3\rangle = |x \oplus y\rangle\,|y\rangle\,.$$

Best solutions were sent by Daniel Popescu (Romania), by Yo Iida (Japan) and by David Marton (Hungary).

4.9. Problem "Bob's symbol"

Formulation

Bob learned the Goldwasser — Micali cryptosystem at university. Now he is thinking about functions over finite fields that are similar to Jacobi symbol.

He chose a function $B_n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (Bob's symbol) defined as follows for any $a \in \mathbb{F}_{2^n}$:

$$B_n(a) = \begin{cases} 1, & \text{if } a = x^2 + x \text{ for some } x \in \mathbb{F}_{2^n}, \\ 0, & \text{otherwise.} \end{cases}$$

Bob knows that finite fields may have some subfields. Indeed, it is well known that $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^n}$ if and only if $k \mid n$. Bob wants to exclude the elements of subfields. In other words, he considers the restriction of B_n to the set

$$\widehat{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \setminus \bigcup_{k|n,\, k\neq n} \mathbb{F}_{2^k}.$$

Here, by $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ we mean the removal from $\mathbb{F}_{2^n}$ the elements forming the field of order 2^k.

Finally, Bob is interested in the sets

$$B_n^0 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 0\} \quad \text{and} \quad B_n^1 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 1\}.$$

Q1 Help Bob to find $|B_n^0|/|B_n^1|$ if n is odd.
Q2 Help Bob to find $|B_n^0|$ and $|B_n^1|$ for an arbitrary n.

Solution

Let us define

$$B(\mathbb{F}_{2^n}) = \{x \in \mathbb{F}_{2^n} : B_n(x) = 0\}, \text{ i.e., } B_n^0 = \widehat{\mathbb{F}}_{2^n} \cap B(\mathbb{F}_{2^n}).$$

First we prove the following lemma.

Lemma 1. Let $k \mid n$. Then

$$|\mathbb{F}_{2^k} \cap B(\mathbb{F}_{2^n})| = \begin{cases} \frac{1}{2}|\mathbb{F}_{2^k}|, & \text{if } n/k \text{ is odd,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let us consider the function $G(x) = x^2 + x = x(x+1)$, where $x \in \mathbb{F}_{2^k}$. First, $G(x) = G(x+1)$. Secondly, $x^2 + x + a$, $a \in \mathbb{F}_{2^k}$, has at most 2 roots. It means that G is a two-to-one function. Therefore, there are exactly 2^{k-1} distinct a such that $x^2 + x \neq a$ for any $x \in \mathbb{F}_{2^k}$.

Next, for any such a the polynomial $x^2 + x + a$ is irreducible over $\mathbb{F}_{2^k}$. It means that it has a root q in the quadratic extension $\mathbb{F}_{2^{2k}}$ of $\mathbb{F}_{2^k}$, i.e., $a = q^2 + q$. If n/k is even, $\mathbb{F}_{2^{2k}}$ is a subfield of $\mathbb{F}_{2^n}$, i.e., $q \in \mathbb{F}_{2^n}$. Thus, $|\mathbb{F}_{2^k} \cap B(\mathbb{F}_{2^n})| = 0$. If n/k is odd, then $\mathbb{F}_{2^{2k}}$ is not a subfield of $\mathbb{F}_{2^n}$. Moreover, $\mathbb{F}_{2^{2k}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^k}$. It means that any root q does not belong to $\mathbb{F}_{2^n}$, i.e., $|\mathbb{F}_{2^k} \cap B(\mathbb{F}_{2^n})| = 2^{k-1}$. ■

Now we are ready to answer the questions. Let $n = m2^t$, where m is odd. We define

$$f_t(d) = |\widehat{\mathbb{F}}_{2^{d2^t}} \cap B(\mathbb{F}_{2^n})| \quad \text{and} \quad g_t(d) = \frac{1}{2}2^{d2^t},$$

where $d \mid m$. This means that $|B_n^0| = |B_{m2^t}^0| = f_t(m)$. At the same time, the definition of $\widehat{\mathbb{F}}_{2^n}$ gives us that

$$\sum_{d|n} |\widehat{\mathbb{F}}_{2^d} \cap B(\mathbb{F}_{2^n})| = |\mathbb{F}_{2^n} \cap B(\mathbb{F}_{2^n})|.$$

According to Lemma 1 and the denotations above,

$$\sum_{d|n} |\widehat{\mathbb{F}}_{2^d} \cap B(\mathbb{F}_{2^n})| = \sum_{d|m} |\widehat{\mathbb{F}}_{2^{d2^t}} \cap B(\mathbb{F}_{2^n})| = \sum_{d|m} f_t(d),$$

$$|\mathbb{F}_{2^n} \cap B(\mathbb{F}_{2^n})| = |\mathbb{F}_{2^{m2^t}} \cap B(\mathbb{F}_{2^n})| = \frac{1}{2}|\mathbb{F}_{2^{m2^t}}| = g_t(m).$$

Hence,

$$g_t(m) = \sum_{d|m} f_t(d) \text{ holds for any integers } m \geqslant 1 \text{ and } t \geqslant 0.$$

According to the Möbius inversion formula,

$$f_t(m) = \sum_{d|m} \mu(d) g_t(m/d) = \frac{1}{2} \sum_{d|m} \mu(d) 2^{(m/d)2^t}.$$

Recall that $\mu(d) = 0$ if d is not square-free (there is an integer $u \geqslant 2$ such that $u^2 \mid d$); otherwise, it is equal to 1 (-1) if d has an even (odd) number of prime factors. As a result,

$$|B_n^0| = \frac{1}{2} \sum_{d|m} \mu(d) 2^{n/d}.$$

Also, $|B_n^1| = |\widehat{\mathbb{F}}_{2^n}| - |B_n^0|$. We need only to note that $|\widehat{\mathbb{F}}_{2^n}| = \sum_{d|n} \mu(d) 2^{n/d}$. This can be easily proven just using $2^n = |\mathbb{F}_{2^n}| = \sum_{d|n} |\widehat{\mathbb{F}}_{2^d}|$ together with the Möbius inversion formula. Finally, we can see that $|B_n^0| = |B_n^1| = \frac{1}{2}|\widehat{\mathbb{F}}_{2^n}|$ for odd n, which means that the answer for Q1 is 1. In fact, it directly follows from Lemma 1 and the definition of $\widehat{\mathbb{F}}_{2^n}$.

Many teams provided the correct answers in the second round using similar ideas: Himanshu Sheoran, Gyumin Roh, Yo Iida (India), Mikhail Kudinov, Denis Nabokov, Alexey Zelenetskiy (Russia), Stepan Davydov, Anastasiia Chichaeva, Kirill Tsaregorodtsev (Russia), Mikhail Borodin, Vitaly Kiryukhin, Andrey Rybkin (Russia), Kristina Geut, Sergey Titov, Dmitry Ananichev (Russia), Pham Minh, Dung Truong Viet (Vietnam), and Alexander Belov (Russia).

4.10. Problem "Public keys for e-coins"

Formulation

Alice has n electronic coins that she would like to spend via some public service S (bank). The service applies some asymmetric algorithm of encryption $E(\cdot)$ and decryption $D(\cdot)$ in its work. Namely, for the pair of public and private keys (PK, SK) and for any message m it holds: if $c = E(m, PK)$, then $m = D(c, SK)$, and visa versa: if $c' = E(m, SK)$, then $m = D(c', PK)$.

To spend her money, Alice generates a sequence of public and private key pairs $(PK_1, SK_1), \ldots, (PK_n, SK_n)$ and sends the sequence of public keys $PK_1, \ldots, PK_n$ to the service S. By doing so, she authorizes the service S to control her n coins.

If Alice would like to spend a coin with number i in the shop of Bob, she just gives the secret key SK_i to Bob and informs him about the number i. To get the coin with number i, Bob sends three parameters to the service S: number i, some non secret message m, and its electronic signature $c' = E(m, SK_i)$. The service S checks whether the signature c' corresponds to the message m, i.e., does it hold the equality $m = D(c', PK_i)$. If it is so, the service accepts the signature, gives the coin number i to Bob and marks it as "spent".

Problem for a special prize! Propose a *modification of this scheme* related to generation of public and private key pairs. Namely, is it possible for Alice not to send the sequence of public keys $PK_1, \ldots PK_n$ to the service S, but send only some initial information enough for generating all necessary public keys on the service's side? Suppose that Alice sends to the service S only some initial key PK (denote it also as PK_0), some function f and a set of parameters T such that $PK_{i+1} = f(PK_i, T)$ for all $i \geqslant 0$. Propose your variant of this function f and the set T. Also think what asymmetric cryptosystem could be used in such a scheme.

Requirements to the solution. Knowing PK, f, and T, it is impossible to find any private key SK_i, where $i = 1, \ldots, n$. It should be impossible to recover SK_i even if the secret keys $SK_1, \ldots, SK_{i-1}$ are also known, or even if all other secret keys are known (more strong condition).

Solution

The problem was solved by two teams and partially solved by four teams.

One of the best partial solutions was proposed by the team of Viet-Sang Nguyen, NhatLinh Le Tan, and Phuong Hoa Nguyen from France. It is described in the BIP32 document [19].The main idea is to consider SK_i as the sequence of numbers additively related to each other: $SK_i = SK_0 + \rho_i$, where $\rho_i = \mathrm{HMAC}_T(PK_0 \| i)$. Public keys can be easily generated by the server S. This approach is compatible with ElGamal type signature schemes, but requires additional security analysis [20].The main disadvantage of the scheme is described by the authors: server S should keep the point PK_0 in secret, as well as Bob should do with SK_i. The problem is that if there is some data leakage, then all coins of Alice will be lost. So the potential complicity of the server and Bob forms a crucial danger for Alice.

The remaining partial solutions use the interesting idea of generating a private key from a public key.

An original attempt to solve the problem was proposed by two teams: Alexander Bakharev, Rinchin Zapanov, and Denis Bykov (Russia); Himanshu Sheoran (India), Gyumin Roh (South Korea), and Yo Iida (Japan). They applied RSA-like techniques and considered private keys as $SK_i = PK_i^{-1} \bmod \phi(n)$, where $n = pq$ and prime numbers p, q are known to Alice only, as well as $\phi(n)$. In the solution of A. Bakharev et al., public keys are formed as

the consecutive prime numbers: PK_{i+1} is the next prime number after PK_i. In the solution of H. Sheoran et al., public keys are formed using a hash function. But the security of this schemes is still under the question.

A very nice partial solution was proposed by Robin Jadoul (Belgium), Esrever Yu (Taiwan), and Jack Pope (United Kingdom). The authors describe an identity-based signature scheme with message recovery based on the RSA hardness assumption. The main idea is to generate public keys from the corresponding master keys by application of hash-to-field functions (four functions are used).

We have accepted two complete solutions.

One of them was proposed by the team of G. Teseleanu, P. Cotan, and L. Constantin-Sebastian from the Institute of Mathematics of the Romanian Academy. On the first round the partial solution was proposed by G. Teseleanu. Private and public keys are connected as $(SK_i)^2 = PK_i \bmod N$, while public keys are generated via HMAC function: $PK_i = \mathrm{HMAC}_T(i)$. The authors also provide a signature scheme that uses keys of this type. Only Alice can produce private keys because she knows the prime factors p and q, where $N = pq$.

Another accepted solution was proposed by Ivan Ioganson, Zhan-Mishel Dakuo and Andrei Golovanov from Saint Petersburg ITMO University (Russia). It uses the ideas of an ID-based signature scheme. Public and private keys are generated from the corresponding master keys PK_0 and SK_0. The principles of Diffie — Hellman protocol on finite groups are applied. Namely, private keys are generated as $SK_i = SK_0 * H(i)$, where H is hash-to-field function, whereas public keys used by the server are combinations of $PK_0 = SK_0 * P$ and numbers i, where P is a generator element of the group. It is difficult to recover SK_i by information from the server and from $SK_1, \ldots, SK_{i-1}, SK_{i+1}, \ldots, SK_n$ if the hash-to-field function H is of a good cryptographic quality.

It is nice to mention the paper of A. Babueva and S. Kyazhin [20] that appeared after the Olympiad, in which the authors continued solving the problem.

4.11. Problem "CP Problem"

Formulation

Let $\mathbb{G} = \langle g \rangle$ be a group of prime order q, κ is the bit length of q. Let us consider two known modifications of the discrete logarithm problem over $\mathbb{G}$, namely, s-DLOG problem and ℓ-OMDL problem. Both of them are believed to be difficult.

s-DLOG problem (with parameter $s \in \mathbb{N}$)

Unknown values:	x is chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values:	$g^x, g^{x^2}, \ldots, g^{x^s}$.
Access to oracles:	no.
The task:	to find x.

ℓ-OMDL (One-More Discrete Log) problem (with parameter $\ell \in \mathbb{N}$)

Unknown values:	$x_1, x_2, \ldots, x_{\ell+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values:	$g^{x_1}, g^{x_2}, \ldots, g^{x_{\ell+1}}$.
Access to oracles:	at most ℓ queries to O_1 that on input $y \in \mathbb{G}$ returns x such that $g^x = y$.
The task:	to find $x_1, x_2, \ldots, x_{\ell+1}$.

Consider another problem that is close to the s-DLOG and ℓ-OMDL problems:

(k,t)-CP (Chaum—Pedersen) problem (with parameters $k, t \in \mathbb{N}$)

Unknown values:	$x_1, x_2, \ldots, x_{t+1}$ are chosen uniformly at random from $\mathbb{Z}_q^*$.
Known values:	$g^{x_1}, g^{x_2}, \ldots, g^{x_{t+1}}$.
Access to oracles:	at most k queries to O_1 that on input $(i, z) \in \{1, \ldots, t+1\} \times \mathbb{G}$ returns z^{x_i}, and at most t queries to O_2 that on input $(\alpha_1, \ldots, \alpha_{t+1}) \in \mathbb{Z}_q^{t+1}$ returns $\alpha_1 x_1 + \ldots + \alpha_{t+1} x_{t+1}$.
The task:	to find $x_1, x_2, \ldots, x_{t+1}$.

It is easy to see that if there exists a polynomial (by κ) algorithm that solves the s-DLOG problem, then there exists a polynomial algorithm that solves the $(s-1,t)$-CP problem for any $t \in \mathbb{N}$.

Problem for a special prize! Prove or disprove the following conjecture: if there exists a polynomial algorithm that solves (k,t)-CP problem, then there exists a polynomial algorithm that solves at least one of the s-DLOG and ℓ-OMDL problems, where k, t, s, ℓ are upper bounded by polynomial of κ.

Solution

Unfortunately, there were no any advances on solving this problem among participants, so this conjecture is still open.

4.12. Problem "Interpolation with Errors"

Formulation

Let $n = 2022$ and let $\mathbb{Z}_n$ be the ring of integers modulo n. Given $x_i, y_i \in \mathbb{Z}_n$ for $i \in \{1, \ldots, 324\}$, find monic polynomials

$$f(x) = x^{16} + \alpha_{15} x^{15} + \ldots + \alpha_1 x + \alpha_0,$$
$$g(x) = x^{16} + \beta_{15} x^{15} + \ldots + \beta_1 x + \beta_0$$

of degree $d = 16$ and coefficients from $\mathbb{Z}_n$ such that the relation

$$y_i = \frac{f(x_i)}{g(x_i)} = \frac{x_i^{16} + \alpha_{15} x_i^{15} + \ldots + \alpha_1 x_i + \alpha_0}{x_i^{16} + \beta_{15} x_i^{15} + \ldots + \beta_1 x_i + \beta_0}$$

holds for at least 90 of the indices $i \in \{1, \ldots, 324\}$.

Note. The coefficients $\beta_0, \ldots, \beta_{15}$ are such that the denominator of the above fraction is invertible for all possible values of $x_i \in \mathbb{Z}_n$. It can be assumed that they are sampled uniformly at random from all such sets of values. Furthermore, the positions and error values can be also assumed to be sampled uniformly at random.

The attachment (see [21]) contains a CSV file with 324 triplets (i, x_i, y_i).

Solution

First, note that $n = 2022 = 2 \cdot 3 \cdot 337$. Therefore, the problem can be solved for moduli 2, 3, 337 independently, and then recovered using the Chinese Remainder Theorem (CRT). Furthermore, for moduli 2 and 3, there are only a few possible polynomials (in view of the relations $x^2 = x \pmod 2$ and $x^3 = x \pmod 3$). The best candidate polynomial modulo 6 (ignoring equivalent forms) satisfies m out of 324 values x_i, y_i, while the next best one does only 109. Note that the expected value is $90 + (324 - 90)/6 = 129$ (90 correct ones and $1/6$ wrong pairs satisfying the relation modulo 6 by chance), so that it is safe to assume that the best one is correct. We can now consider the problem modulo 337, where we know that

the 90 correct pairs must be among those m correct pairs observed modulo 6. Denote the set of those m remaining indices by I.

Note that the relation can be rewritten as $y_i \cdot g(x_i) - f(x_i) = 0$, or, more explicitly,

$$\left(y_i \sum_{j=0}^{15} \beta_i x_i^j\right) - \left(\sum_{j=0}^{15} \alpha_i x_i^j\right) + \left(y_i x_i^d - x_i^d\right) = 0. \tag{1}$$

The target problem can now be formulated as the problem of decoding a linear code over the finite field GF(337). Indeed, let the generator matrix G be given by columns

$$\left(-1,\ -x_i,\ -x_i^2,\ \ldots,\ -x_i^{15},\ y_i,\ y_i x_i,\ y_i x_i^2,\ \ldots,\ y_i x_i^{15}\right)$$

for all chosen indexes $i \in I$, let the target vector v be given by

$$v = \left(y_i x_i^d - x_i^d\right)_{i \in I},$$

and consider the "solution" vector

$$s = (\alpha_0, \ldots, \alpha_{15}, \beta_0, \ldots, \beta_{15}).$$

It is easy to verify that the codeword $s \cdot G$ differs from $-v$ in at most $\mathsf{m} - 90$ places, i.e., has at most 35 errors. Indeed, the vector $s \cdot G$ computes the contribution of the first two clauses of equation (1), whereas v defines the third clause, and the three clauses sum to zero on correct data pairs. Note that G defines a $[\mathsf{m}, 32]$-code, i.e., a 32-dimensional code of length m. A random such code has expected minimum distance about 82 (given by the Gilbert — Varshamov bound), so that the solution (with the error 35 less than half of the distance) should likely be unique (modulo 337).

A very basic yet efficient method for linear code decoding is the so-called "pooled Gauss" method: choosing $k = 32$ random coordinates of the code and assuming that they are error-free, allowing to recover full codeword by solving a linear system. Alternatively, `SageMath` includes an implementation of the Lee — Brickell method, which is slightly faster. The decoding should take less than 30 minutes using the basic method.

Remark 3. Due to the equivalent polynomial fractions modulo 2 and modulo 3, the overall solution is not unique (but there are only a few candidates).

4.13. Problem "HAS01"

Formulation

Bob is a beginner cryptographer. He read an article about the new hash function HAS01 [22]. Bob decided to implement the HAS01 function in order to use it for checking the integrity of messages being forwarded. However, he was inattentive and made a mistake during the implementation. In the function f_1, he did not notice the sign «'» in the variable a and used the following set of formulas:

For $i = 0, \ldots, 7$
  For $j = 0, \ldots, 6$
  $a_{(i+1) \bmod 8,j} := \mathrm{SBox}(((a_{i,j} \oplus a_{(i+1) \bmod 8,j}) \ll 3) \oplus ((a_{i,j+1} \oplus a_{(i+1) \bmod 8,j+1}) \gg 5))$;
$a_{(i+1) \bmod 8,7} := \mathrm{SBox}(((a_{i,7} \oplus a_{(i+1) \bmod 8,7}) \ll 3) \oplus ((a_{i,0} \oplus a_{(i+1) \bmod 8,0}) \gg 5) \oplus 7)$.

Q1 Prove that Bob's version of the hash function is cryptographically weak.

Q2 Find a collision to the following message (given in hexadecimal format):
`3165203938203362203236203437203163203738203865 20`.

The test set value for the original HAS01 hash function is given in [23].

The test set value for Bob's implementation is given in [24].

Solution

Q1. In the case when Bob makes a mistake and uses formulas with recursion, it turns out that for each first byte of the string $(a_{00}, a_{10}, a_{20}, a_{30}, a_{40}, a_{50}, a_{60}, a_{70})$, the most significant three bits do not affect the formation of the digest. Therefore, the function is not collision resistant, making it easy to pick up a number of different values that produce the same hash value.

Q2. According to the formulas, the most significant three bits for the first byte of each string do not affect the formation of the hash value. However, the original message fills only the first three rows of the original matrix. Therefore, changing the upper three bits in bytes a_{00}, a_{10}, a_{20} will allow you to get the same hash values. Therefore, for a given value `3165203938203362203236203437203163203738203865 20`, you can get $2^9 - 1 = 511$ collisions.

For example:

`3165203938203362203236203437203163203738203865 20;`
`F165203938203362203236203437203163203738203865 20;`
`F16520393820336 2E03236203437203163203738203865 20;`
`3165203938203362203236203437203 1E3203738203865 20;`

and so on.

It should be noted that most of the participants who tried to solve this problem were able to get the correct answer and identify the collision. Separately, it is worth noting that the team of Mikhail Borodin, Vitaly Kiryukhin and Andrey Rybkin (Russia) not only answered the questions of the task correctly, but also considered the issues of a possible vulnerability for the HAS01-512 algorithm.

4.14. Problem "Weaknesses of the PHIGFS"

Formulation

A young cryptographer Philip designs a family of lightweight block ciphers based on a 4-line type-2 Generalized Feistel scheme (GFS) with better diffusion effect.

Its block is divided into four m-bit subblocks, $m \geqslant 1$. For better diffusion effect, Philip decides to use a (4×4)-matrix A over $\mathbb{F}_{2^m}$ instead of a standard subblocks shift register in each round. The family $\mathrm{PHIGFS}_\ell(A, b)$ is parameterized by a non-linear permutation $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, the matrix A and the number of rounds $\ell \geqslant 1$. The one-round keyed transformation of $\mathrm{PHIGFS}_\ell(A, b)$ is a permutation g_k on $\mathbb{F}_{2^m}^4$ defined as

$$g_k(x_3, x_2, x_1, x_0) = A\,(x_3, x_2 \oplus b(x_3 \oplus k_1), x_1, x_0 \oplus b(x_1 \oplus k_0))^{\mathrm{T}},$$

where $x_0, x_1, x_2, x_3 \in \mathbb{F}_{2^m}$, $k = (k_1, k_0)$ is a $2m$-bit round key, $k_0, k_1 \in \mathbb{F}_{2^m}$.

The ℓ-round encryption function $f_{k^{(1)},\ldots,k^{(\ell)}}\colon \mathbb{F}_{2^m}^4 \to \mathbb{F}_{2^m}^4$ under a key $(k^{(1)}, \ldots, k^{(\ell)}) \in \mathbb{F}_{2^m}^\ell$ is given by

$$f_{k^{(1)},\ldots,k^{(\ell)}}(\mathbf{x}) = g_{k^{(\ell)}} \ldots g_{k^{(1)}}(\mathbf{x}) \quad \text{for all} \quad \mathbf{x} \in \mathbb{F}_{2^m}^4.$$

For effective implementation and security, Philip chooses two binary matrices A', A'' with the maximum branch number among all binary matrices of size 4:

$$A' = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \; A'' = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

For approval, he shows the cipher to his friend Antony who claims that A', A'' are bad choices because ciphers $\mathrm{PHIGFS}_\ell(A', b)$ and $\mathrm{PHIGFS}_\ell(A'', b)$ are insecure against distinguisher attacks for all $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, $\ell \geqslant 1$.

Help Philip to analyze the cipher $\mathrm{PHIGFS}_\ell(A, b)$. Namely, for any $b\colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ and any $\ell \geqslant 1$, show that $\mathrm{PHIGFS}_\ell(A, b)$ has

a) ℓ-round differential sets with probability 1,

b) ℓ-round impossible differential sets

for the following cases: **Q1**: $A = A'$ and **Q2**: $A = A''$. In each case, construct these nontrivial differential sets and prove the corresponding property.

Remark 4. Let us recall the following definitions.

— Let $\delta, \varepsilon \in \mathbb{F}_{2^n}$ be fixed nonzero input and output differences. The *differential probability* of $s\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

$$p_{\delta,\varepsilon}(s) = 2^{-n} \cdot \left|\{\alpha \in \mathbb{F}_{2^n} : s(\alpha \oplus \delta) \oplus s(\alpha) = \varepsilon\}\right|.$$

— If $s\colon \mathbb{F}_{2^n} \times K \to \mathbb{F}_{2^n}$ depends on a key space K, then the *differential probability* of s is defined as

$$p_{\delta,\varepsilon}(s) = |K|^{-1} \sum_{k \in K} p_{\delta,\varepsilon}(s_k),$$

where $s(x, k) = s_k(x)$, $x \in \mathbb{F}_{2^n}$, $k \in K$. In this case, the pair (δ, ε) represents a differential denoted by $\delta \to^s \varepsilon$.

— Let $\Omega, \Delta \subseteq \mathbb{F}_{2^n} \backslash \{0\}$ and Ω, Δ are nonempty. If $p_{\delta,\varepsilon}(s) = 0$ for any $\delta \in \Omega,\ \varepsilon \in \Delta$, then (Ω, Δ) are *impossible differential sets*. But if

$$\sum_{\delta \in \Omega, \varepsilon \in \Delta} p_{\delta,\varepsilon}(s) = 1,$$

then (Ω, Δ) are *differential sets with probability* 1. We call (Ω, Δ) trivial (impossible) differential sets if $\Omega \in \{\varnothing, \mathbb{F}_{2^n} \backslash \{0\}\}$ or $\Delta \in \{\varnothing, \mathbb{F}_{2^n} \backslash \{0\}\}$.

— For the l-round encryption function f, we will sometimes write $\delta \to_l \varepsilon$ to emphasize the number of rounds l instead of $\delta \to^f \varepsilon$.

— For $\delta \in \mathbb{F}_{2^m}, b : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, we denote

$$\Delta_\delta(b) = \{b(\alpha \oplus \delta) \oplus b(\alpha) : \alpha \in \mathbb{F}_{2^m}\}.$$

Solution

Note that g_k consists of a transformation $v_k : \mathbb{F}_{2^m}^4 \to \mathbb{F}_{2^m}^4$ and the matrix A over $\mathbb{F}_{2^m}$, where

$$v_k(x_3, x_2, x_1, x_0) = (x_3, x_2 \oplus b(x_3 \oplus k_1), x_1, x_0 \oplus b(x_1 \oplus k_0)),$$
$$g_k(\mathbf{x}) = A(v_k(\mathbf{x}))^{\mathrm{T}}, \mathbf{x} \in \mathbb{F}_{2^m}^4.$$

Q1. $A = A'$.

Let $\varepsilon \in \mathbb{F}_{2^m}$, $W(\varepsilon) = \{(\alpha_3, \alpha_2, \alpha_1, \alpha_0) \in \mathbb{F}_{2^m}^4 : \alpha_3 \oplus \alpha_1 = \varepsilon\} \setminus \{(0, 0, 0, 0)\}$.

Theorem 1. Let l be any positive integer, $\varepsilon \in \mathbb{F}_{2^m}$. Then l-round differential sets $W(\varepsilon) \to_l W(\varepsilon)$ of the $\mathrm{PHIGFS}_l(A', b)$ hold with probability 1.

Proof. For any $(x_3, x_2, x_1, x_0) \in \mathbb{F}_{2^m}^4$ we have the following equality:

$$A'(x_3, x_2, x_1, x_0)^{\mathrm{T}} = (x_3 \oplus x_2 \oplus x_0, x_3 \oplus x_1 \oplus x_0, x_2 \oplus x_1 \oplus x_0, x_3 \oplus x_2 \oplus x_1)^{\mathrm{T}}.$$

Let us consider any nonzero $(\delta, \lambda, \omega) \in \mathbb{F}_{2^m}^3$ and any round key $k \in \mathbb{F}_{2^m}^2$. Note that v_k maps a difference $(\delta, \lambda, \delta \oplus \varepsilon, \omega) \in W(\varepsilon)$ to a difference $(\delta, \lambda^{(1)}, \delta \oplus \varepsilon, \omega^{(1)}) \in W(\varepsilon)$ for any

$$\lambda^{(1)} \in \Delta_\delta(b) \oplus \lambda, \quad \omega^{(1)} \in \Delta_{\delta \oplus \varepsilon}(b) \oplus \omega.$$

Then $A'\left(\delta, \lambda^{(1)}, \delta \oplus \varepsilon, \omega^{(1)}\right) = \left(\omega^{(1)} \oplus \delta \oplus \lambda^{(1)}, \omega^{(1)} \oplus \varepsilon, \omega^{(1)} \oplus \delta \oplus \lambda^{(1)} \oplus \varepsilon, \lambda^{(1)} \oplus \varepsilon\right)$. Thus, g_k maps the difference $(\delta, \lambda, \delta \oplus \varepsilon, \omega) \in W(\varepsilon)$ to the difference $\left(\delta^{(1)}, \lambda^{(2)}, \delta^{(1)} \oplus \varepsilon, \omega^{(2)}\right) \in$ $\in W(\varepsilon)$, where $\delta^{(1)} = \lambda^{(1)} \oplus \delta \oplus \omega^{(1)}$, $\lambda^{(2)} = \omega^{(1)} \oplus \varepsilon$, $\omega^{(2)} = \lambda^{(1)} \oplus \varepsilon$. Therefore,

$$\mathsf{P}\left[W(\varepsilon) \to^g W(\varepsilon)\right] = 1.$$

By induction on the number of rounds l, we get $\mathsf{P}[W(\varepsilon) \to_l W(\varepsilon)] = 1$. ■

Corollary 1. For any number of rounds $l \geqslant 1$, $(W(\varepsilon), W(\delta))$ are a pair of impossible l-round differential sets for any different $\varepsilon, \delta \in \mathbb{F}_{2^m}$.

Q2. $A = A''$.

Let $W = \{(0, \delta, \delta, \theta) : (\delta, \theta) \in \mathbb{F}_{2^m}^2 \setminus \{(0,0)\}\}$.

Theorem 2. Let l be any positive integer, $\varepsilon \in \mathbb{F}_{2^m}$. Then l-round differential sets $W \to_l W$ of the $\mathrm{PHIGFS}_l(A'', b)$ holds with probability 1.

Proof. For any $(x_3, x_2, x_1, x_0) \in \mathbb{F}_{2^m}^4$, we have

$$A''(x_3, x_2, x_1, x_0)^{\mathrm{T}} = (x_3 \oplus x_2 \oplus x_1, x_3 \oplus x_2 \oplus x_0, x_3 \oplus x_1 \oplus x_0, x_2 \oplus x_1 \oplus x_0)^{\mathrm{T}}.$$

Let us consider any nonzero $(\delta, \theta) \in \mathbb{F}_{2^m}^2$ and any round key $k \in \mathbb{F}_{2^m}^2$. Note that v_k maps a difference $(0, \delta, \delta, \theta) \in W$ to a difference $\left(0, \delta, \delta, \theta^{(1)}\right) \in W$ for any $\theta^{(1)} \in \Delta_\delta(b) \oplus \gamma$. Then

$$A''\left(0, \delta, \delta, \theta^{(1)}\right) = \left(0, \theta^{(1)} \oplus \delta, \theta^{(1)} \oplus \delta, \theta^{(1)}\right).$$

Thus, g_k maps the difference $(0, \delta, \delta, \theta) \in W$ to the difference $\left(0, \delta^{(1)}, \delta^{(1)}, \theta^{(1)}\right) \in W$, where $\delta^{(1)} = \theta^{(1)} \oplus \delta$. Therefore,

$$\mathsf{P}\left[W \to^g W\right] = 1.$$

By induction on the number of rounds l, we get $\mathsf{P}[W \to_l W] = 1$. ■

Corollary 2. For any number of rounds $l \geqslant 1$, (W, W') are a pair of impossible l-round differential sets for any $W' \subseteq \mathbb{F}_{2^m}^4 \setminus (W \cup \{0\})$.

We would like to mention the solution of Gabriel Tulba-Lecu, Ioan Dragomir and Mircea-Costin Preoteasa (Romania).

4.15. Problem "Super dependent S-box"

Formulation

Harry wants to find a super dependent S-box for his new cipher. He decided to use a permutation that is strictly connected with every of its variables. He tries to estimate the number of such permutations.

A vectorial Boolean function $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$, where $x \in \mathbb{F}_2^n$, is a *permutation* on $\mathbb{F}_2^n$ if it is a one-to-one mapping on the set $\mathbb{F}_2^n$. Its coordinate function $f_k(x)$

(that is a Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) *essentially depends* on the variable x_j if there exist values $b_1, b_2, \ldots, b_{j-1}, b_{j+1}, \ldots, b_n \in \mathbb{F}_2$ such that

$$f_k(b_1, b_2, \ldots, b_{j-1}, 0, b_{j+1}, \ldots, b_n) \neq f_k(b_1, b_2, \ldots, b_{j-1}, 1, b_{j+1}, \ldots, b_n).$$

In other words, the essential dependence on the variable x_j of a function f means the presence of x_j in the algebraic normal form of f (the unique representation of a function in the basis of binary operations AND, XOR, and constants 0 and 1).

An example. Let $n = 3$. Then the Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_3$ essentially depends on all its variables; but $g(x_1, x_2, x_3) = x_1x_2 \oplus x_2 \oplus 1$ essentially depends only on x_1 and x_2.

The problem. Find the number of permutations on $\mathbb{F}_2^n$ such that all their coordinate functions essentially depend on all n variables, namely

Q1 Solve the problem for $n = 2, 3$.

Q2 **Problem for a special prize!** Solve the problem for arbitrary n.

Solution

Let us denote the number of super-dependent S-boxes in n variables by $S(n)$. We can represent F as $F(x) = (f_1(x), \ldots, f_n(x))$, where $x \in \mathbb{F}_2^n$ and $f_1, \ldots, f_n$ are Boolean functions in n variables (i.e., functions of the form $\mathbb{F}_2^n \to \mathbb{F}_2$). Recall that F is a permutation if and only if any its component function $b_1f_1(x) \oplus \ldots \oplus b_nf_n(x)$, $b \in \mathbb{F}_2^n \setminus \{0\}$, is balanced (i.e., it takes zero and one in the same number of arguments).

The most of solutions provided by the participants contain an answer for Q1. As a rule, an exhaustive search was used. The correct answer for Q1 is the following: $S(2) = 0$ and $S(3) = 24576$. At the same time, some progress has been made on Q2. A short description of these results is bellow.

The team of Mikhail Kudinov, Denis Nabokov and Alexey Zelenetskiy (Russia) used the inclusion-exclusion principle and provided lower and upper bounds for $S(n)$. Their ideas were the following. Let $H(k)$ be the set of functions $f : \mathbb{F}_2^k \to \mathbb{F}_2$ that essentially depend on all its variables $x_1, \ldots, x_k$. Then,

$$|H(n)| = \mathrm{C}_{2^n}^{2^{n-1}} - \sum_{k=0}^{n-1} \mathrm{C}_n^k |H(k)|,$$

where C_n^k is a binomial coefficient. Next, let us define for any $i \in \{1, \ldots, n\}$ the sets

$$A_i = \{\text{a permutation } F(x) = (f_1(x), \ldots, f_n(x)) \text{ on } \mathbb{F}_2^n : f_i \notin H(n)\}.$$

It means that the number of super-dependent S-boxes is the following:

$$S(n) = 2^n! - |A_1 \cup \ldots \cup A_n|.$$

It is not difficult to see that $|A_{i_1} \cap \ldots \cap A_{i_k}| = |A_1 \cap \ldots \cap A_k|$ for any $1 \leqslant k \leqslant n$ and any k-element set $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$. The inclusion-exclusion principle gives us that

$$S(n) = 2^n! + \sum_{k=1}^{n} (-1)^k \mathrm{C}_n^k |A_1 \cap \ldots \cap A_k|.$$

The cardinalities of intersections can be calculated in the following way:

$$|A_1 \cap \ldots \cap A_k| = 2^n! \frac{d(n,k)}{\prod\limits_{i=0}^{k-1} \left(\mathrm{C}_{2^{n-i}}^{2^{n-i-1}}\right)^{2^i}},$$

where $d(n,k)$ is the number of tuples $(f_1,\ldots,f_k)$ consisting of Boolean functions in n variables such that $f_1,\ldots,f_k \notin H(n)$ and $b_1f_1 \oplus \ldots \oplus b_kf_k$ is balanced for any $b \in \mathbb{F}_2^k \setminus \{0\}$. It is not easy to calculate $d(n,k)$. However, there is a trivial estimation $d(n,k) \geqslant \mathrm{C}_{2^{n-1}}^{2^{n-2}}$. Also,

$$|A_1| = 2^n! \frac{\mathrm{C}_{2^n}^{2^{n-1}} - |H(n)|}{\mathrm{C}_{2^n}^{2^{n-1}}}.$$

This can be used to estimate $S(n)$:

$$2^n! - n|A_1| \leqslant S(n) \leqslant 2^n! - |A_1|.$$

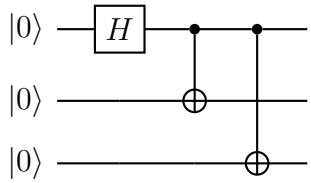
The team of Stepan Davydov, Anastasiia Chichaeva, and Kirill Tsaregorodtsev (Russia) proposed interesting ideas as well. They noticed that $2^n \mid S(n)$, implemented Monte-Carlo simulations for $n = 4$ and $n = 5$, and showed that $\lim\limits_{n\to\infty} \dfrac{S(n)}{2^n!} = 1$. Also, the team pointed out a subclass of super-dependent S-boxes such that even component functions of its representatives essentially depend on all its variables.

The team of Mikhail Borodin, Vitaly Kiryukhin and Andrey Rybkin (Russia) calculated that $S(4) = 19344102217728 = 24 \cdot 16 \cdot 50375266192$. They used that the addition to a super-dependent S-box in n variables of any binary vector from $\mathbb{F}_2^n$ and rearranging its output bits provided a super-dependent S-box as well. In other words, $(n! \cdot 2^n) \mid S(n)$ holds. Note that some other participants mentioned such kind of classifications (for instance, in the solution above). However, the team exploited this fact most successfully.

4.16. Problem "Quantum entanglement"

Formulation

The Nobel Prize in Physics in 2022 was awarded to researchers who experimentally investigated quantum *entanglement*. One of their studies was devoted to a Greenberger — Horne — Zeilinger state $|GHZ\rangle = \dfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, which is an entangled state of three qubits. This state can be created using the following quantum circuit:



After the measurement, the probability to find the system described by $|GHZ\rangle$ in the state $|000\rangle$ or in the state $|111\rangle$ is equal to $1/2$.

When we make measurements in quantum physics, we are able to make *post-selection*. For example, if we post-select the events when the first qubit was in state $|0\rangle$, the second and the third qubits will also be found in the state $|0\rangle$ for sure, this is actually what entanglement means. We also see that the post-selection destroys entanglement of two remaining qubits.

Q1 But what will happen, if we post-select the events when the 1st qubit is in the Hadamard state $|+\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$? How can we perform this kind of post-selection if the result of each measurement of a qubit state can be only 0 or 1 and we can only post-select these events? Will the two remaining qubits be entangled after post-selection? Design the circuit which will provide an answer.

Q2 **Problem for a special prize!** There are two different classes of three-qubit entanglement. One of them is

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle),$$

and the other is

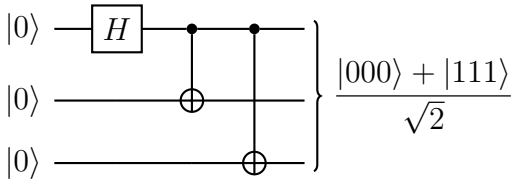
$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle).$$

Discuss the possible ideas how the difference between these states can be found with the usage of post-selection and measurement. Don't forget that you need to verify entanglement for both types of states!

Remark 5. For details about quantum circuits, see Remark 2. Additionally, we can measure qubit, initially given in the state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$, in other basis, for example Hadamard basis $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. In order to do this, we consider the state in the form $|\psi\rangle = \alpha'_0 |+\rangle + \alpha'_1 |-\rangle$, where complex amplitudes α'_0, α'_1 have the same physical meaning as α_0 and α_1. Then we can calculate the probability that the qubit will be in the state $|+\rangle$ or $|-\rangle$ after the measurement and consider the process of post-selection in this case. Recall that for two qubits we use notation $|a\rangle \otimes |b\rangle \equiv |ab\rangle$. By induction, this process is expanded on the case of three qubits and more. Mathematically, the entanglement of n-qubits state means that we can not consider this state in the form $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, where $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are some states of m and $n-m$ qubits, correspondingly.

Solution

Q1. The circuit for creation of the Greenberger — Horne — Zeilinger state $|GHZ\rangle$ is the following:

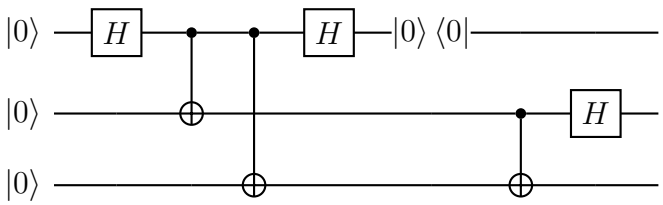


First, we need to post-select events when the first qubit is in the Hadamard state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. For this purpose, we make an Hadamard gate prior to the measurement of the first qubit. After this we perform a post-selection.

The state $|GHZ\rangle$ can be written as

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} = |+\rangle \frac{(|00\rangle + |11\rangle)}{2\sqrt{2}} + |-\rangle \frac{(|00\rangle - |11\rangle)}{2\sqrt{2}},$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. It means that if we select the first qubit in the state $|+\rangle$, the other qubits will be in the entangled Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. This state can be detected using a CNOT gate followed by the Hadamard gate. The whole circuit is



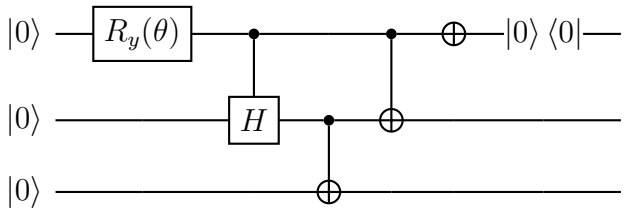
Q2. This question that supposed to be the open problem was solved during the Olympiad by the team of Viet-Sang Nguyen, Nhat Linh LE Tan and Phuong Hoa Nguyen (France). Here we provide the solution.

If we measure any qubit of the state $|GHZ\rangle$ and know the result of the measurement, we immediately know the state of two rest qubits. Thus, the state of the whole system of 3 qubits is an entangled one. But the state of two rest qubits after the measurement of any qubit is separable.

When we measure the first qubit of the state $|W\rangle$, the result is 0 with probability 2/3 and 1 with probability 1/3. When the state of the first qubit is measured 1, the system collapses to a separable state $|00\rangle$ hence it is not entangled anymore. However, when the state of the first qubit is measured 0, the remaining two qubits become the maximally entangled state of two qubits. Given the measurement of one qubit as $|1\rangle$, we can deduce the information about the other two because there is correlation in the information between qubits. Thus, $|W\rangle$ is an entangled quantum state of three qubits.

Unlike $|GHZ\rangle$, measuring one qubit in $|W\rangle$ creates an entangle state of two remaining qubit with probability 2/3. While being in $|GHZ\rangle$, the system collapses to a separable state after measurement of any qubit.

The post-selection procedure for the state $|GHZ\rangle$ was discussed in the question **Q1**, so the same technique can be applied for the state $|W\rangle$. This state contains residual entanglement after measurement of a qubit, we can post-selection the third qubit in the state $|0\rangle$ to attain the Bell state of the remaining qubits:



Here, $R_y(\theta)$ gate is a single-qubit rotation through angle $\theta = 2\arccos(1/\sqrt{3})$ (radians) around the y-axis.

The state $|W\rangle$ has the following representation:

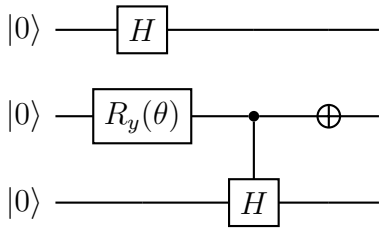
$$|W\rangle = \frac{1}{\sqrt{3}}\big(\,|001\rangle + |010\rangle + |100\rangle\,\big) = \frac{1}{\sqrt{6}}\big(\,|00+\rangle + |01+\rangle + |10+\rangle - |00-\rangle + |01-\rangle + |10-\rangle\,\big).$$

If we can post-select the state $|+\rangle$ for the third qubit, we have

$$\frac{1}{\sqrt{3}}\big(\,|00+\rangle + |01+\rangle + |10+\rangle\,\big) = \frac{1}{\sqrt{3}}\big(\,|00\rangle + |01\rangle + |10\rangle\,\big) \otimes |+\rangle\,,$$

which is equivalent to a circuit with two entangled qubits similar to $|W\rangle$ and an independent qubit in the state $|+\rangle$. There is a correlation between two rest qubits in this system: if we measure 1 in one qubit, the other must be 0. Hence, we have an entanglement between two qubits.

The circuit for the system with third qubit in the state $|+\rangle$ and two entangled qubits:



In conclusion, when measuring one qubit of the state $|W\rangle$, the state of the other two qubits are still entangled. But after the measurement of any qubit of the state $|GHZ\rangle$, the states of the remaining qubits become known. When post measuring Hadamard $|+\rangle$ state, both $|W\rangle$ and $|GHZ\rangle$ states return outcome equivalent to a separate qubit in the state $|+\rangle$ and an entangled state of two qubits.

We also would like to mention participants who made a progress in solution, that is the team of Gabriel Tulba-Lecu, Mircea-Costin Preoteasa, and Ioan Dragomir (Romania), the team of Mikhail Kudinov, Denis Nabokov, and Alexey Zelenetskiy (Russia), the team of Himanshu Sheoran, Gyumin Roh, and Yo Iida (India, South Korea, Japan), and the team of Donat Akos Koller, Csaba Kiss, and Marton Marits (Hungary).

5. Acknowledgement

The authors are grateful to Andrey Nelyubin, Yuliya Maksimlyuk, Irina Khilchuk, Darya Zyubina, Valeria Kochetkova, and Sergey Kyazhin for useful discussions and various help.

REFERENCES

1. `https://nsucrypto.nsu.ru/`.
2. `https://nsucrypto.nsu.ru/outline/`.
3. `https://nsucrypto.nsu.ru/archive/2021/total_results/\#data`.
4. *Agievich S., Gorodilova A., Kolomeec N., et al.* Problems, solutions and experience of the first international student's Olympiad in cryptography. Prikladnaya Diskretnaya Matematika, 2015, no. 3(29), pp. 41–62.
5. *Agievich S., Gorodilova A., Idrisova V., et al.* Mathematical problems of the second international student's Olympiad in cryptography. Cryptologia, 2017, vol. 41, no. 6, pp. 534–565.
6. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems from the Third International Students' Olympiad in Cryptography., Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 34–58.
7. *Gorodilova A., Agievich S., Carlet C., et al.* Problems and solutions of the Fourth International Students' Olympiad in Cryptography (NSUCRYPTO). Cryptologia, 2019, vol. 43, no. 2, pp. 138–174.
8. *Gorodilova A., Agievich S., Carlet C., et al.* The Fifth International Students' Olympiad in Cryptography — NSUCRYPTO: problems and their solutions. Cryptologia, 2020, vol. 44, no. 3, pp. 223–256.
9. *Gorodilova A., Tokareva N., Agievich S., et al.* On the Sixth International Olympiad in Cryptography NSUCRYPTO. J. Appl. Industr. Math., 2020, vol. 14, no. 4, pp. 623–647.
10. *Gorodilova A. A., Tokareva N. N., Agievich S. V., et al.* The Seventh International Olympiad in Cryptography: problems and solutions. Siberian Electronic Math. Reports, 2021, vol. 18, no. 2, pp. A4–A29.
11. *Gorodilova A. A., Tokareva N. N., Agievich S. V., et al.* An overview of the Eight International Olympiad in Cryptography "Non-Stop University CRYPTO". Siberian Electronic Math. Reports, 2022, vol. 19, no. 1, pp. A9–A37.
12. `https://nsucrypto.nsu.ru/unsolved-problems/`.
13. *Kiss R. and Nagy G. P.* On the nonexistence of certain orthogonal arrays of strength four. Prikladnaya Diskretnaya Matematika, 2021, no. 52, pp. 65–68.
14. *Geut K. L., Kirienko K. A., Sadkov P. O., et al.* O yavnykh konstruktsiyakh dlya resheniya zadachi "A secret sharing" [On explicit constructions for solving the problem "A secret sharing"]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2017, no. 10, pp. 68–70. (in Russian)

15. *Geut K. L. and Titov S. S.* O blokirovke dvumernykh affinnykh mnogoobraziy [On the blocking of two-dimensional affine varieties]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 7–10. (in Russian)
16. *Ayat S. M. and Ghahramani M.* A recursive algorithm for solving "A secret sharing" problem. Cryptologia, 2019, vol. 43, no. 6, pp. 497–503.
17. *Shcherba A., Faure E., and Lavdanska O.* Three-pass cryptographic protocol based on permutations. IEEE 2nd Intern. Conf. ATIT, Kyiv, Ukraine, 2020, pp. 281–284.
18. `https://algassert.com/quirk`.
19. *Wuille P.* Hierarchical Deterministic Wallets. `https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki`.
20. *Babueva A. A. and Kyazhin S. N.* Public keys for e-coins: partially solved problem using signature with rerandomizable keys. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2023, no. 16, pp. 110–114.
21. `https://nsucrypto.nsu.ru/media/MediaFile/data_round2.txt`.
22. *Kapalova N., Dyusenbayev. D., and Sakan K.* A new hashing algorithm — HAS01: development, cryptographic properties and inclusion in graduate studies. Global J. Engineering Education, 2022, vol. 24, no. 2, pp. 155–164.
23. `https://nsucrypto.nsu.ru/media/MediaFile/test_vector.txt`.
24. `https://nsucrypto.nsu.ru/media/MediaFile/test_vector2.txt`.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94 DOI 10.17223/20710410/62/5

МОДЕЛЬ И МЕТРИКИ ОСВЕДОМЛЁННОСТИ В КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЧАСТЬ 2. ФАКТИЧЕСКАЯ ОСВЕДОМЛЁННОСТЬ

Н. А. Гайдамакин

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия

E-mail: n.a.gaidamakin@urfu.ru

Фактическая осведомлённость пользователей в конфиденциальной информации рассматривается как владение соответствующей информацией, характеризующееся степенью восприятия (усвоения) и возможности использования информации («извлечения» из памяти). В рамках субъектно-объектного класса моделей управления доступом в компьютерных системах произведена формализация понятия осведомлённости как результата доступов пользователей к объектам, содержащим конфиденциальную информацию. Доступ к объекту (по чтению), имеющий временны́е рамки (продолжительность), формирует осведомлённость пользователя в конфиденциальной информации соответствующего объекта, величина которой пропорциональна объёму конфиденциальной информации объекта, индексу сложности (читабельности) текста объекта, продолжительности доступа и, кроме того, зависит от индивидуальных способностей пользователя в восприятии (скорости чтения) и освоении (понимании, обработке) информации. При этом объём конфиденциальной информации объекта определяется как величина, пропорциональная количеству слов в тексте объекта и коэффициенту информативности объекта. С течением времени по кривой забывания Г. Эббингауза осведомлённость пользователя в конфиденциальной информации уменьшается. Степень снижения осведомлённости зависит от индивидуальных особенностей пользователя и уровня конфиденциальности информации. Последующие доступы к объекту могут восстанавливать степень осведомлённости в зависимости от продолжительности доступов и времени, прошедшего с предыдущего доступа. Рассматриваются вид и параметры функции уменьшения/восстановления осведомлённости с течением времени и в зависимости от истории доступов. Осведомлённость пользователя во всей конфиденциальной информации, содержащейся (обрабатывающейся) в компьютерной системе, складывается из осведомлённости по всем объектам доступа с учётом синергетического эффекта, который может быть как положительным (знание о системе объектов больше суммы знаний об объектах), так и отрицательным. Характер и особенности фактической осведомлённости пользователей в конфиденциальной информации иллюстрируются на примерах при различных параметрах объектов доступа, истории доступов и индивидуальных особенностей пользователей.

Ключевые слова: *конфиденциальная информация, осведомлённость, фактическая осведомлённость, модель осведомлённости, метрики осведомлённости, информативность объекта доступа, сложность текста объекта доступа, понимание текста объекта доступа, продолжительность доступа, кривая забывания информации, история доступов, эффект синергии в осведомлённости.*

THE MODEL AND METRICS OF AWARENESS IN CONFIDENTIAL INFORMATION. PART 2. ACTUAL AWARENESS

N. A. Gaydamakin

Ural Federal University named after the First President of Russia B. N. Yeltsin, Ekaternburg, Russia

The actual awareness of users in confidential information is considered as the possession of relevant information, characterized by the degree of perception (assimilation) and the possibility of using information ("extraction" from memory). Within the subject-object class of access control models in computer systems, the concept of awareness is formalized as a result of user access to objects containing confidential information. Access to the object (by reading), having a time frame (duration), forms the user's awareness of the confidential information of the corresponding object, the value of which is proportional to the volume of confidential information of the object, the index of complexity (readability) of the text of the object, the duration of access and and also depends on the user's individual ability to perceive (reading speed) and master (understanding, processing) information. At the same time, the volume of confidential information of an object is defined as a value proportional to the number of words in the text and the coefficient of informativeness of the object. Over time, according to the Ebbinghaus forgetting curve, the user's awareness of sensitive information decreases. The degree of decrease in awareness depends on the individual characteristics of the user and the level of confidentiality of the information. Subsequent accesses to the object can restore the degree of awareness depending on the duration of the accesses and the time elapsed since the previous access. The type and parameters of the function of reducing/restoring awareness over time and depending on the access history are considered. The user's awareness of all confidential information contained (processed) in a computer system consists of awareness of all access objects, taking into account the synergetic effect, which can be either positive (knowledge about the system of objects is greater than the sum of knowledge about objects) or negative. The nature and features of users' actual awareness in confidential information are illustrated by examples with various parameters of access objects, access history and individual characteristics of users.

Keywords: *confidential information, awareness, actual awareness, awareness model, awareness metrics, informativeness of the access object, complexity of the access object text, understanding of the access object text, duration of access, information forgetting curve, access history, synergy effect in awareness.*

Введение

Как отмечено в [1], *осведомлённость* пользователей в конфиденциальной информации рассматривается в качестве синонима *владения* информацией, т. е. как знание сведений, сообщений, данных, составляющих информацию. Соответственно *фактическая осведомлённость* (Actual Awareness) пользователей в конфиденциальной информации

является результатом осуществления доступов к объектам компьютерной системы, содержащим конфиденциальную информацию.

Вместе с тем известные субъектно-объектные модели управления доступом в компьютерных системах [2, 3] не затрагивают результативную сторону процессов доступа, поскольку неявно полагается, что субъект-пользователь, осуществив доступ к объекту (по чтению), априори обладает соответствующей информацией и впоследствии в любой момент времени может её использовать. Интуитивно ясно, что это не совсем так. В процессе доступа можно успеть прочесть только часть текста (файла, объекта) и в результате обладать только частью информации, содержащейся в объекте доступа. Можно прочесть весь текст объекта (текстовый файл), но ничего не понять или понять только часть информации.

Таким образом, требует формализации процедурно-результативная и темпорально-целевая сторона процесса доступа к информации в компьютерных системах, включая доступ к конфиденциальной информации.

Целевая сторона понятия «осведомлённость» исследовалась в сфере феноменологической социологии [4, 5], где один из подходов трактует «*осведомлённость*» как *состояние, в котором субъект осведомлён о некоторой информации* (*владеет некоторой информацией*) *и эта информация непосредственно доступна для использования в направлении широкого спектра поведенческих действий*. Иначе говоря, осведомлённость, разделяемая в некоторых подходах по феноменологической социологии на «явную» и «неявную» («скрытую»), рассматривается в контексте способности индивидуума к эффективному применению имеющихся у него знаний и сведений, что предполагает, в первую очередь, способность «извлечь из памяти» информацию в последующие моменты времени.

В сфере обучения и психологии исследовались процессы восприятия (усвоения) информации, подаваемой в той или иной форме (пирамида Дейла) — устной (через слушание), текстовой (через чтение) и т. д. [6], и были получены эмпирические данные и соотношения по степени усвоения, сохранения и воспроизведения информации [7–13].

Тем не менее в рамках отмеченных формальных моделей управления доступом в компьютерных системах как в отношении результативности доступа к объектам, содержащим конфиденциальную информацию, так и в отношении способности к эффективному использованию информации в дальнейшем не рассматриваются временны́е аспекты, связанные с изменениями с течением времени актуальности, в том числе конфиденциальности информации, с изменениями способности индивидуума к эффективному «извлечению» и использованию информации, которой он обладает (забывание информации), а также то, что можно именовать временно́й диссипацией (деградацией) информации [14].

Наконец, понятие «осведомлённость» широко используется в сфере управления знаниями персонала организации (knowledge management), включая понятие осведомлённости персонала в вопросах информационной безопасности [15–18].

Целью данной работы является рассмотрение формализованной и процедурно-аналитической составляющей (фактической) осведомлённости пользователей в конфиденциальной информации, содержащейся в компьютерных системах.

1. Исходные положения

Будем основываться на субъектно-объектной формализации компьютерной системы, рассматривая её как совокупность *объектов* доступа $o \in O$, содержащих конфиденциальную информацию (файлы, каталоги, базы данных и/или их таблицы-

строки/записи-поля), и *субъектов* доступа $s \in S$ (выполняющиеся по командам *пользователей* $u \in U$ компьютерные программы).

Также будем предполагать, что в компьютерной системе действует дискретное время, в каждый момент t_k которого пользователи $u \in U$ осуществляют *доступы* субъектов $s \in S$ к объектам $o \in O$. Под доступом будем понимать имеющий временны́е рамки процесс воздействия субъекта $s \in S$ на объект $o \in O$, в результате которого формируется *поток информации* — однонаправленный, т. е. от объекта к субъекту или от субъекта (через субъект) к объекту, либо двунаправленный, т. е. одновременно от субъекта к объекту и от объекта к субъекту.

В контексте анализа осведомлённости, как и в [1], ограничимся рассмотрением только доступов вида «Чтение» (Read) к объектам, содержащим текстовую информацию, и будем использовать *детерминистскую* трактовку понятия *информационного потока* как процесса изменения слова, характеризующего объект-приемник информационного потока в зависимости от слова, характеризующего объект-источник информационного потока. Иначе говоря, объект доступа в теоретико-информационном смысле рассматривается как слово некоторого языка [19].

Под «*фактической осведомлённостью в конфиденциальной информации*» будем понимать величину, характеризующую в количественной (интервальной) шкале степень владения пользователем $u \in U$ конфиденциальной информацией, находящейся в компьютерной системе.

Под *владением* пользователем $u \in U$ конфиденциальной информацией будем понимать её знание, т. е. *ознакомленность* с ней, и её понимание, а также способность к её эффективному использованию, включая количественную (объём информации) и качественную (степень конфиденциальности и извлекаемости) стороны.

Таким образом, быть осведомлённым в конфиденциальной информации означает знать информацию, т. е. её воспринять и понять, переработать и интегрировать с ранее усвоенной информацией, и, кроме того, быть способным её извлечь из памяти и использовать в тех или иных целях.

Степень владения конфиденциальной информацией (величину осведомлённости) в интервальной шкале ограничим диапазоном $[0, 1]$, где 1 — максимальная, т. е. 100-процентная осведомлённость во всей конфиденциальной информации (абсолютно полное владение информацией), обрабатывающейся в компьютерной системе.

2. Объём конфиденциальной информации, информативность, сложность и конфиденциальность информации объектов доступа

Как уже отмечалось, в теоретико-информационном смысле при детерминистском подходе объект доступа рассматривается как слово некоторого языка в определённом алфавите [19]. В случае конечного алфавита объём информации, реализуемый информационным потоком в результате доступа, характеризуется количеством слов, представляющих объект. Исходя из этого, понятие «*объём* (*конфиденциальной*) *информации объекта* o_n» можно определить как величину, пропорциональную количеству слов $Q(o_n, t_m)$, содержащихся в момент времени t_m в тексте объекта o_n:

$$V(o_n, t_m) = Q(o_n, t_m)\, \theta(o_n, t_m), \tag{1}$$

где $\theta(o_n, t_m)$ — изменяющийся в диапазоне $[0, 1]$ коэффициент информативности объекта o_n в момент времени t_m.

Введение коэффициента информативности $\theta(o_n, t_m)$ обусловлено тем, что языком письменной речи одну и ту же информацию можно выразить по-разному, с разной

ясностью, чёткостью, полнотой, «понятностью» и, следовательно, с различным словесным объёмом. Будем считать, что существует вещественно-значная функция, выражающая данное свойство объектов в числовом диапазоне $[0, 1]$.

В процессе восприятия (чтения) текстовой информации, её усвоения важным фактором является т. н. «*читабельность*» («*понятность*», «*трудность*») текста, во многих источниках отождествляемая с понятием *сложности* текста. Многочисленные исследования, обзор которых можно найти в [20], определили ряд критериев сложности текста, к которым относятся, прежде всего, количественно-статистические параметры (средняя буквенная или слоговая длина слов, среднее количество слов в предложениях, доля сложносочинённых предложений, количество специальных терминов), а также ряд других грамматических и семантико-тематических критериев (повествовательность изложения, конкретность/абстрактность слов и выражений, среднее значение словесного расстояния между связанными элементами предложений и др.). Предложены эмпирические соотношения для определения «индекса читабельности» (*индекса сложности*) текста, на основе которых разработаны специальные программные средства для автоматизированного вычисления индекса читабельности, в том числе для текстов на русском языке [20].

Будем считать, что существует вещественно-значная функция $\varphi(o_n, t_m)$, которая для каждого объекта доступа o_n в любой момент времени t_m ставит в соответствие количественное значение его индекса сложности. Диапазон значений индекса сложности объекта $\varphi(o_n, t_m)$ определим так, чтобы его среднее значение для группы однородно-тематических текстов (например, тексты финансово-экономической, кадровой, проектно-конструкторской и т. д. тематики) равнялось 1.

Конфиденциальность информации объектов доступа будем понимать как такое свойство соответствующей информации, когда может возникнуть какой-либо ущерб при свободном обороте этой информации, т. е. в результате доступа к ней (соответственно осведомлённости в ней) неопределённого круга лиц.

Отметим, что не все объекты доступа содержат конфиденциальную информацию и/или не вся информация объекта является конфиденциальной. Однако ввиду существенных трудностей формализации вопросов семантического анализа и разделения информации объекта доступа на конфиденциальную и неконфиденциальную части будем считать, что весь объём информации объекта доступа, определяемый по соотношению (1), в том числе с учётом информативности объекта доступа, характеризует конфиденциальную информацию, содержащуюся в объекте.

Также отметим, что из понятия конфиденциальности следует её различная степень — в зависимости от величины ущерба при свободном обороте соответствующей информации. В большинстве случаев степень конфиденциальности информации ввиду существенных сложностей в определении количественных значений ущерба выражается величиной в качественных (порядково-вербальных) шкалах («высокая», «средняя», «низкая»). Тем не менее будем считать, что существует вещественно-значная функция $f_{\text{conf}}(o_n, t_m)$, которая каждому объекту $o_n \in O$ компьютерной системы в каждый момент времени t_m ставит в соответствие некоторую величину конфиденциальности $\mathcal{K} = f_{\text{conf}}(o_n, t_m)$ в диапазоне $[0, 1]$.

3. Осведомлённость в конфиденциальной информации пользователя в результате однократного доступа к объекту

Из рассмотренных выше определений и формализаций следует, что количество информации, которую получает субъект s (управляющий им пользователь u) в резуль-

тате доступа к объекту o определяется словесным объёмом соответствующего объекта (например, файла).

Однако здравый смысл говорит, что это не всегда так, поскольку, как уже отмечалось, в результате доступа можно ознакомиться только с частью информации или понять только часть информации объекта.

Разрешение этой проблемы представляется на основе введения темпорального аспекта в определение и характеристики доступа, т. е. временны́х рамок, и результативных аспектов последовательности доступов в понятие владения информацией.

Сделаем следующие предположения.

Положение 1. Пользователи $u_l \in U$, осуществляя в моменты времени t_m доступы к объектам $o_n \in O$ продолжительностью Δt_{mn}, формируют или повышают степень владения информацией, заключённой в соответствующих объектах.

Таким образом, атрибутами доступа, помимо идентификаторов субъекта и объекта, вида доступа (чтение, запись, редактирование), являются начало и окончание (длительность) доступа.

Положение 2. *Приращение осведомлённости* в конфиденциальной информации $\mathcal{A}_\Delta(u_l, o_n, t_m, \Delta t_{mn})$ пользователя u_l в результате доступа к объекту o_n в момент времени t_m продолжительностью Δt_{mn} определяется:

— объёмом $V(o_n, t_k)$ конфиденциальной информации, содержащейся в момент времени t_m в объекте o_n;
— продолжительностью Δt_{mn} доступа пользователя u_l к объекту o_n в момент времени t_m;
— величиной $f_{\text{conf}}(o_n, t_m)$ конфиденциальности информации, содержащейся в момент времени t_m в объекте o_n;
— сложностью $\varphi(o_n, t_m)$ текста объекта доступа o_n в момент времени t_m;
— индивидуальными особенностями (способностями) пользователя u_l в отношении скорости восприятия информации (скорости чтения);
— индивидуальными особенностями (способностями) пользователями u_l в отношении степени понимания воспринятой *информации*, т. е. её переработки и интегрирования с ранее усвоенной информацией.

Диапазон значений функции приращения осведомлённости $\mathcal{A}_\Delta(u_l, o_n, t_m, \Delta t_{mn})$ ограничим отрезком $[0, 1]$, полагая под значением 1 максимальную осведомлённость в конфиденциальной информации, имеющейся в объекте.

Исходя из положения 2, приращение осведомлённости $\mathcal{A}_\Delta(u_l, o_n, \Delta t_{mn})$ пользователя u_l в конфиденциальной информации объекта o_n в результате доступа в момент времени t_m продолжительностью Δt_{mn} будем определять на основе соотношения

$$\mathcal{A}_\Delta(u_l, o_n, t_m, \Delta t_{mn}) = \left(\frac{\overline{\vartheta} \beta_l \Delta t_{mn}}{Q(o_n, t_m)} \theta(o_n, t_m) \varphi(o_n, t_m) \left(1 - \chi_{mn}\right) \gamma_l \right)_{|1}, \qquad (2)$$

где:

— $\overline{\vartheta}$ — средняя скорость чтения текста, равная по некоторым данным 200 слов в минуту [21];
— β_l — коэффициент индивидуальной способности пользователя u_l в отношении скорости чтения текста относительно среднего значения, принимающий по некоторым данным значения в диапазоне от 0,3 до 1,88;
— χ_{mn} — доля времени закрытия текста объекта o_n на экране программой типа «Заставка» от момента времени t_m до момента времени $t_m + \Delta t_{mn}$ (для многостранич-

ных текстов, для которых требуется «пролистывание» текста на экране компьютера, в величину χ_{mn} можно добавлять долю времени «неактивности пользователя»);

— γ_l — коэффициент индивидуальной способности пользователя u_l в отношении понимания прочитанного текста в диапазоне от 0 до 1, среднее значение которого по некоторым данным равно 0,52 (52 %) (имеется в виду коэффициент понимания текста служебных документов. В отношении сложных учебных, технических, научных текстов можно использовать с известными оговорками (без учёта влияния иллюстраций, мультимедиа и т. д.) данные пирамиды Дейла [6], согласно которым объём усвоения однократно прочитанного текста обучаемыми в среднем составляет 10 %);

— $(x)_{|1}$ обозначает функцию

$$(x)_{|1} = \begin{cases} x, & \text{если } x < 1, \\ 1, & \text{если } x \geqslant 1. \end{cases}$$

Значение $\mathcal{A}_\Delta(u_l, o_n, t_m, \Delta t_{mn}) = 1$ означает 100-процентную осведомлённость пользователя u_l в конфиденциальной информации, содержащейся в тексте объекта o_n.

Параметры β_l и γ_l, характеризующие индивидуальные особенности пользователей в отношении восприятия и усвоения воспринятой информации, могут оцениваться на основе аналитико-тестовых процедур, подобных процедурам определения профессиональной квалификации сотрудников организаций.

Выражение (2) задаёт приращение осведомлённости пользователя в результате однократного доступа к объекту.

4. Осведомлённость пользователя в конфиденциальной информации объекта в результате последовательности доступов

Сделаем следующие очевидные предположения.

Положение 3. Осведомлённость пользователя u_l в конфиденциальной информации объекта o_n с течением времени имеет тенденцию к снижению, при этом осведомлённость в более конфиденциальной информации снижается в меньшей степени.

Положение 4. Последующие доступы пользователя u_l к объекту o_n после доступа в момент времени t_m могут повышать (возобновлять, восстанавливать) осведомлённость пользователя в соответствующей информации.

Действительно, если осведомлённость пользователя в информации объекта o_n не достигла 1, то пользователь может её повысить в результате повторного и последующего доступов. При этом с течением времени соответствующая информация может забываться, воспроизводиться («извлекаться» из памяти) в меньшем объёме, с худшим качеством (с худшим пониманием) и в результате степень владения пользователем соответствующей информацией будет снижаться. Очевидно, что более важная, т. е. более конфиденциальная информация обрабатывается и хранится в сознании пользователя более тщательно и, следовательно, степень владения такой информацией снижается медленнее, чем менее конфиденциальной информацией.

В результате, основываясь на положениях 3 и 4, величину $\mathcal{A}(u_l, o_n, t_k)$ осведомлённости пользователя u_l в конфиденциальной информации, содержащейся в объекте o_n в момент времени t_k после последнего доступа к этому объекту в момент времени t_m, можно определять на основе следующего итеративного соотношения:

$$\mathcal{A}(u_l, o_n, t_k) = \left(\mathcal{A}(u_l, o_n,\ t_m) f_{\text{Forg}}(u_l, o_n, t_k, t_m) + \mathcal{A}_\Delta(u_l, o_n, t_k, \Delta t_{nk})\right)_{|1}, \qquad (3)$$

где $f_{\text{Forg}}(u_l, o_n, t_k, t_m)$ — функция «забывания» информации (доля остаточной в памяти информации от первоначальной) и, следовательно, снижения к моменту времени t_k степени владения пользователем u_l информацией объекта o_n с момента предыдущего ознакомления с ней в момент времени t_m, $m < k$.

Начало исследованиям процессов сохранения информации в памяти положили работы Г. Эббингауза (см. [7, 13]), который определил «кривую забывания» (*Forgetting Curve*), выражающуюся в разных интерпретациях эмпирически определённой функцией вида

$$f_{\text{Forg}}(u_l, o_n, t_k, t_m) = \frac{a}{a + b\log(t_k - t_m)},$$

где a и b — параметры «забывания», эмпирические средние значения которых при усреднении для различных индивидуумов (пользователей), т. е. без учёта их индивидуальных особенностей, равны 1,84 и 1,25 соответственно.

Следует отметить, что значения параметров a и b, экспериментально найденные Эббингаузом, относятся к способности обучаемых через определённое время воспроизводить слогословесную информацию (трёхбуквенные слоги, лишенные ассоциативной связи). Многочисленные последующие исследования подтвердили результаты Эббингауза, при этом были исследованы вопросы влияния на запоминание, сохранение и воспроизведение информации ассоциативных связей в элементах информации, структурных и ритмичных характеристик, эмоциональной окраски информации. Были предложены и другие виды функций кривых забывания [7–13, 22], характер поведения которых в общем виде сходен с кривой Г. Эббингауза.

В контексте анализа осведомлённости в конфиденциальной информации необходимо анализировать способность пользователей воспроизводить не словесно-речевую форму прочитанного текста, а усвоенное в результате предыдущего чтения смысловое содержание, т. е. основные смысловые составляющие текста и их параметры. Скорость забывания смысловых составляющих информации существенно медленнее и по данным многих исследователей [10, 13, 22] может характеризоваться функцией экспоненциального вида

$$f_{\text{Forg}}(u_l, o_n, t_k, t_m) \approx e^{-\lambda_l(t_k - t_m)}, \tag{4}$$

где λ_l — параметр скорости забывания информации l-м пользователем, среднее значение которого в отношении забывания (объёма воспроизведения) смысловых элементов текста характеризуется величиной, которую на основе аппроксимации функции (4) по методу наименьших квадратов экспериментальными данными, приведёнными в [23, 24], можно определить равной $5{,}36 \cdot 10^{-06}$ мин$^{-1}$.

Индивидуальное значение параметра скорости забывания информации l-м пользователем λ_l, как и параметры β_l и γ_l, может определяться на основе специальных аналитико-тестовых процедур.

В соответствии с положением 3, функция (4) должна учитывать влияние на скорость забывания уровня конфиденциальности информации. Этого можно достичь, введя в соотношение (4) функцию $f_{\text{conf\_}v}(o_n, t_m)$ как некий коэффициент пропорциональности степени забывания информации от уровня конфиденциальности:

$$f_{\text{Forg}}(u_l, o_n, t_k, t_m) = f_{\text{conf\_}v}(o_n, t_m)e^{-\lambda_l(t_k - t_m)}. \tag{5}$$

Здесь $f_{\text{conf\_}v}(o_n, t_m)$ — функция со значениями в диапазоне от 0 до 1, определяющая степень влияния на скорость забывания уровня конфиденциальности информации.

При этом, ввиду неопределённости факторов, определяющих вид функции $f_{\text{conf\_}v}(o_n, t_m)$, будем считать её тождественной функции $f_{\text{conf}}(o_n, t_m)$. Иначе говоря,

при самом высоком уровне конфиденциальности информации объекта o_n значение $f_{\text{conf}\_v}(o_n, t_{i-1}) = 1$, т. е. максимально медленное забывание соответствующей информации; при уровнях конфиденциальности, меньших максимального, $f_{\text{conf}\_v}(o_n, t_{i-1}) < 1$ и забывание происходит быстрее.

Пример 1. На рис. 1 для иллюстрации характера функции (3) приведены расчёты величины осведомлённости пользователя в конфиденциальной информации $\mathcal{A}(u_l, o_1, t_k)$, содержащейся в объекте o_1, объём которого составляет 3000 слов (порядка 10 страниц текста) с неизменяющимися по времени уровнем конфиденциальности «Средний» (0,809 от максимального), уровне информативности $\theta = 0{,}5$, индексе сложности текста $\varphi = 1$, при полном задействовании времени доступов ($\chi_{m1} = 0$). Об эвристиках перевода показаний порядково-вербальной шкалы конфиденциальности в количественную см. [1].

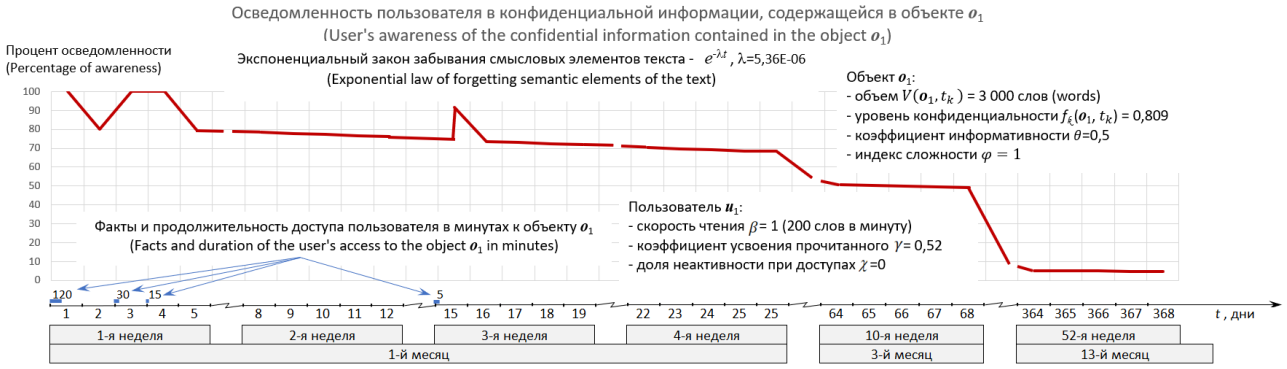


Рис. 1. Пример для иллюстрации осведомлённости пользователя в конфиденциальной информации, содержащейся в объекте, в результате определённой истории доступов

Как видно из рис.1, пользователь u_1 в первый рабочий день в течение двух часов имел доступ к объекту o_1, что позволило ему несколько раз его прочесть (напомним, средняя скорость чтения текста составляет 200 слов в минуту), как говорят, «полностью отработать», и в результате с учётом в среднем 52-процентной усвояемости прочитанного один раз текста получить полное представление о содержании (о смысле и деталях) информации объекта. В следующий рабочий день у пользователя u_1 доступа к объекту o_1 не было, и в результате процессов забывания информации, в том числе с учётом влияния на скорость забывания уровня конфиденциальности, степень владения конфиденциальной информацией соответствующего объекта у пользователя снизилась до 80 %. В третий и четвёртый рабочие дни пользователь u_1 вновь осуществлял доступы к объекту o_1 в течение 30 и 15 мин соответственно, что позволило ему повысить уровень владения соответствующей информацией вновь до 100 %.

В последующие два рабочих дня первой недели и всю вторую неделю доступа пользователя u_1 к объекту o_1 не было, шёл процесс забывания информации по экспоненциальному закону (сначала очень быстро, затем медленнее), в результате чего уровень владения конфиденциальной информацией объекта к началу третьей рабочей недели снизился до 75 % (график на рис. 1 отражает величину осведомлённости с шагом по времени в один день, поэтому имеет вид ломаной линии). В первый рабочий день третьей недели пользователь u_1 имел непродолжительный (5-минутный) доступ к объекту o_1 (видимо, чтобы вспомнить или уточнить какие-либо аспекты информации), что позволило повысить уровень владения до 91,6 %, т. е. из-за кратковременности доступа не до 100 %. Далее ввиду отсутствия у пользователя u_1 в последующее время

доступов к объекту o_1 шёл процесс экспоненциального снижения уровня владения соответствующей информацией и к концу года степень осведомлённости пользователя в конфиденциальной информации объекта o_1 составила всего 4,8 %.

5. Осведомлённость пользователя во всей конфиденциальной информации в результате последовательности доступов к объектам компьютерной системы

Сделаем следующие предположения.

Положение 5. Осведомлённость пользователя в конфиденциальной информации по некоторой системе объектов складывается из осведомлённости в конфиденциальной информации по отдельным объектам, её составляющим.

Положение 6. Осведомлённость пользователя в конфиденциальной информации некоторой системы объектов в целом характеризуется синергетическим эффектом, который в зависимости от особенностей пользователя и конфиденциальности информации по соответствующим объектам, сложности системы и характера взаимосвязей объектов, её составляющих, может быть как положительным, так и отрицательным.

Положительный эффект синергии в осведомлённости заключается в формировании нового знания о системе объектов на основе обработки, агрегирования и обобщения знаний по отдельным объектам. Иначе говоря, знание о системе больше суммы знаний о составляющих её объектах.

Отрицательный эффект синергии заключается в том, что знание о системе ухудшается (уменьшается, «запутывается») в результате неспособности индивидуума переработать, обобщить, интегрировать знание по отдельным объектам системы в целое, т. е. знание о системе в целом меньше суммы знаний о составляющих её объектах.

Исходя из положений 5 и 6, осведомлённость $\mathcal{A}(u_l, t_k)$ пользователя u_l во всей конфиденциальной информации, содержащейся в компьютерной системе в момент времени t_k, будем определять как аддитивно-мультипликативную функцию осведомлённости по объектам, содержащим конфиденциальную информацию, по отношению ко всему объёму конфиденциальной информации:

$$\mathcal{A}(u_l, t_k) = \left(\mathcal{E}(u_l, t_k, O) \sum_{n=1}^{N_{t_k}} \mathcal{A}_{\mathbf{N}}(u_l, o_n, t_k) \right)_{|1} . \tag{6}$$

Здесь:

- $\mathcal{E}(u_l, t_k, O)$ — функция эффекта синергии в осведомлённости по системе объектов в целом в зависимости от осведомлённости по каждому отдельному объекту, значениями которой являются положительные числа как больше 1 (положительный эффект синергии), так и меньше 1 (отрицательный эффект синергии);
- O — множество объектов доступа компьютерной системы с отношениями (с их взаимосвязями, содержанием и т. д.);
- N_{t_k} — количество объектов с конфиденциальной информацией в момент времени t_k;
- $\mathcal{A}_{\mathbf{N}}(u_l, o_n, t_k)$ — величина осведомлённости пользователя u_l в момент времени t_k в конфиденциальной информации объекта o_n, вычисляемая с нормированием по отношению к объёму всей конфиденциальной информации, обрабатываемой в компьютерной системе в соответствующие моменты времени, с учётом степени конфиденциальности информации объектов доступа:

$$\mathcal{A}_{\mathbf{N}}(u_l, o_n, t_k) = (\mathcal{A}_{\mathbf{N}}(u_l, o_n, t_m) f_{\mathrm{Forg}}(u_l, o_n, t_k, t_m) + \mathcal{A}_{\mathbf{N}_\Delta}(u_l, o_n, t_k, \Delta t_{nk}))_{|1} ,$$

где t_m — момент времени последнего доступа пользователя u_l к объекту o_n;

— $\mathcal{A}_{\mathbf{N}_\Delta}(u_l, o_n, t_k, \Delta t_{nk})$ — нормированное приращение осведомлённости пользователя u_l в конфиденциальной информации объекта o_n в результате доступа в момент времени t_k продолжительностью Δt_{nk}, которое, в свою очередь, определяется следующим соотношением:

$$\mathcal{A}_{\mathbf{N}_\Delta}(u_l, o_n, t_k, \Delta t_{nk}) = \left(f_{\mathcal{K}}(o_n, t_k) \frac{\overline{\vartheta}\beta_l \Delta t_{nk}}{\sum\limits_{j=1}^{N_{t_k}} V(o_j, t_k)} \theta(o_n, t_k)\varphi(o_n, t_k)(1 - \chi_{kn})\ \gamma_l \right)_{|1}. \quad (7)$$

Ввиду сложности природы эффекта синергии определение вида функция $\mathcal{E}(u_l, t_k, O)$ представляет отдельное направление исследований. В практических приложениях можно принять $\mathcal{E}(u_l, t_k, O) = 1$.

Пример 2. На рис. 2 для иллюстрации характера поведения величины $\mathcal{A}(u_l, t_k)$ приведены результаты расчёта осведомлённости пользователя в конфиденциальной информации, обрабатываемой в компьютерной системе, включающей три объекта, параметры которых (объём, конфиденциальность, информативность) представлены на рисунке.

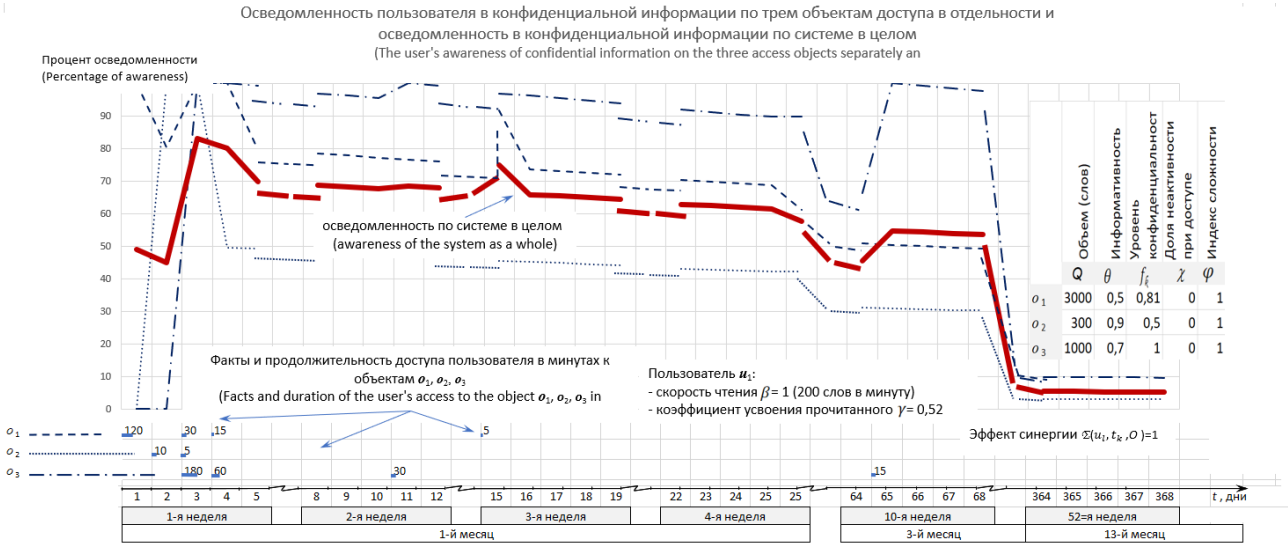


Рис. 2. Иллюстрация осведомлённости пользователя о конфиденциальной информации в компьютерной системе, включающей три объекта, в результате определённой последовательности (истории) доступов

Как видно из рис. 2, пользователь u_1 осуществлял серию доступов к 10-страничному объекту o_1 со средним уровнем конфиденциальности, коэффициентами информативности и сложности по фактам и продолжительности доступов аналогично данным рис. 1.

К небольшому (одностраничному) объекту o_2 с низким уровнем конфиденциальности, но с высоким уровнем информативности, пользователь u_1 во второй и третий рабочий день осуществил 10-минутный и 5-минутный доступы соответственно, что с учётом небольшого объёма информации объекта обеспечило ему 100-процентную осведомлённость в соответствующей конфиденциальной информации. Больше доступов к объекту o_2 не было и шёл процесс экспоненциального снижения осведомлённости.

При этом вклад осведомлённости в соответствующей информации в «общую копилку» осведомлённости ввиду небольшого объёма и невысокого уровня конфиденциальности объекта o_2 являлся незначительным.

К объекту o_3, самому конфиденциальному ($f_{\text{conf}}(o_3, t_k) = 1$) и довольно объёмному ($Q(o_3, t_k) = 1000$ слов — 3–4 страницы текста) с высокой степенью информативности ($\theta(o_3, t_k) = 0{,}7$), пользователь u_1 осуществлял продолжительные доступы (180 и 60 мин) в третий и четвёртый рабочие дни, что обеспечило ему 100-процентную осведомлённость в соответствующей конфиденциальной информации. При этом снижение степени владения (осведомлённости) до следующего доступа на 11-й рабочий день ввиду высокой степени конфиденциальности соответствующей информации происходило существенно медленнее, чем по объектам o_1 и o_2. Последующие доступы пользователя к объекту o_3 продолжительностью 30 минут (в 11-й рабочий день) и 15 минут (через два месяца в 65-й рабочий день) ввиду высоких остаточного уровня осведомлённости и величины продолжительности доступа по отношению к объёму объекта позволяли восстанавливать осведомлённость до 100 %.

Как видно из рис. 2, характер изменения осведомлённости пользователя u_1 по всей конфиденциальной информации системы с учётом времени доступа, объёма, информативности и конфиденциальности объектов определялся в основном доступами к объектам o_1 и o_3. При этом вклад в общую осведомлённость доступов к объекту o_3 был примерно равным вкладу от доступов к существенно более объёмному, но менее конфиденциальному и менее информативному объекту o_1.

Рассмотренные примеры расчётов и анализа осведомлённости в конфиденциальной информации демонстрируют результаты, отражающие интуитивные качественные представления о содержании понятия «осведомлённость» и характере её изменений.

Следует отметить, что как и в случае с анализом потенциальной осведомлённости, дополнительные возможности анализа фактической осведомлённости предоставляет тематико-иерархическое управление доступом [25, 26]. В таких системах конфиденциальная информация объектов доступа помечается (индексируется) мультирубриками [27], которые являются совокупностью рубрик-тематик $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$, организованных в иерархический тематический рубрикатор $T_{\text{TH}} = \{r, \tau_1, \tau_2, \ldots, \tau_K\}$, где r — корень дерева (вся тематика), отражающего иерархическую структуру рубрикатора. Управление доступом осуществляется на основе сравнения мультирубрик объектов доступа и тематических полномочий субъектов доступа (пользователей), которые выражаются также совокупностью разрешённых рубрик-тематик (разрешённой мультирубрикой). В результате появляется возможность анализировать фактическую осведомлённость пользователей не только в целом по всей конфиденциальной информации системы, но и осведомлённость в конфиденциальной информации по определённой рубрике-тематике или по некоторой тематической мультирубрике $\mathcal{T}_i^{(m)}$ — $\mathcal{A}(u_l, \mathcal{T}_i^{(m)}, t_k)$. С этой целью в соотношениях (2), (7) необходимо ввести в качестве дополнительного сомножителя двоичную функцию $\delta\left(\mathcal{T}^{(m)}(o_n, t_k), \mathcal{T}_i^{(m)}\right)$, равную 1, если тематика (мультирубрика) объекта доступа $\mathcal{T}^{(m)}(o_n, t_k)$ шире (охватывает) анализируемую тематику (мультирубрику) конфиденциальной информации $\mathcal{T}_i^{(m)}$, и 0 в противном случае.

Заключение

Как и в случае с «потенциальной осведомлённостью» [1], представленные понятие и величины фактической осведомлённости пользователей в конфиденциальной ин-

формации $\mathcal{A}_\Delta(u_l, o_n, \Delta t_{mn})$, $\mathcal{A}(u_l, o_n, t_k)$ и $\mathcal{A}(u_l, t_k)$ могут составить базис специального программного обеспечения в процессах мониторинга информационной безопасности компьютерных систем. Анализируя значения осведомлённости пользователей в конфиденциальной информации отдельных объектов или по всей совокупности объектов, администраторы компьютерных систем могут формировать на этой основе обоснованные решения в контексте обеспечения информационной безопасности.

Также следует отметить, что, как и в отношении технических аспектов анализа потенциальной осведомлённости, основные параметры для вычисления величин $\mathcal{A}_\Delta(u_l, o_n, \Delta t_{mn})$, $\mathcal{A}(u_l, o_n, t_k)$ и $\mathcal{A}(u_l, t_k)$ либо автоматически определяются в современных офисных системах работы с документами и электронного документооборота (объём информации в словах, история и продолжительность доступов), либо могут определяться на основе регламентации процедур делопроизводства.

Отдельных специальных исследований требуют вид функций «кривых забывания» в контексте владения конфиденциальной информацией и связанные с ними параметры восприятия, усвоения конфиденциальных данных, в том числе вопросов «старения» информации [14], а также вопросов, связанных с эффектом синергии осведомлённости по системе объектов доступа. Направлениями развития представленного подхода может быть рассмотрение осведомлённости и соответствующих параметров $\theta(o_n, t_k)$, $\varphi(o_n, t_k)$, β_l, γ_l, λ_l, $\mathcal{E}(u_l, t_k, O)$ как случайных величин с распределениями вероятностей, требующими теоретических и экспериментальных исследований, или как величин, являющихся элементами нечётких множеств [28, 29].

Вместе с тем представленные данные по соответствующим функциям и параметрам можно рассматривать в качестве «первого приближения» для использования в практических системах.

ЛИТЕРАТУРА

1. *Гайдамакин Н. А.* Модель и метрики осведомленности в конфиденциальной информации. Часть 1. Потенциальная осведомленность // Прикладная дискретная математика. 2023. № 61. С. 86–103.
2. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия — Телеком, 2020. 352 с.
3. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
4. *Chalmers D.* The Conscious Mind: In Search of a Fundamental Theory. Oxford: Oxford University Press,1996. 225 p.
5. *Шютц А.* Смысловая структура повседневного мира: очерки по феноменологической социологии. М.: Институт Фонда «Общественное мнение», 2003. 336 с.
6. *Lee S. J. and Reeves T. C.* Edgar Dale: A significant contributor to the field of educational technology // Educational Technology. 2007. V. 47. No. 6. P. 56–59.
7. Хрестоматия по общей психологии. Психология памяти / под ред. Ю. Б. Гиппенрейтер, В. Я. Романова. М.: Изд-во МГУ, 1979. 272 с.
8. *Аткинсон Р.* Человеческая память и процесс обучения. М.: Прогресс, 1980. 527 с.
9. *Зинченко Т. П.* Память в экспериментальной и когнитивной психологии. СПб.: Питер, 2002. 320 с.
10. *Ланге В. Г.* О скорости забывания // Вопросы психологии. 1983. № 4. С. 142–145.
11. *Wickelgren W. A.* Trace resistance and the decay of longterm memory // J. Math. Psychology. 1972. No. 9. P. 418–455.

12. *Wickelgren W. A.* Single-trace fragility theory of memory dynamics // Memory Cognition. 1974. V. 2(4). P. 775–780.
13. http://www.ideationizing.com/2009/06/brief-history-of-mathematical.html — A Brief History of the Mathematical Definition of Forgetting Curves. 2023.
14. *Ефимов А. Н.* Информация: ценность, старение, рассеяние. М.: Знание, 1978. 64 с.
15. ГОСТ Р 53894-2016. Менеджмент знаний. Термины и определения. М.: Стандартинформ, 2020. 24 с.
16. ГОСТ Р ИСО/МЭК 27002. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М.: Стандартинформ, 2021. 74 с.
17. Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, 2003.
18. *Астахова Л. В., Ульянов Н. Л.* Модель политики управления осведомленностью сотрудников организации в области информационной безопасности // Материалы 67-й науч. конф. ЮУрГУ, Челябинск, 14–17 апреля 2015 г. С. 678–682.
19. *Грушо А. А., Применко Е. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности. М.: Академия, 2009. 272 с.
20. *Солнышкина С. И., Киселъников А. С.* Сложность текста: этапы изучения в отечественном прикладном языкознании // Вестник Томского госуниверситета. Филология. 2015. № 6(38). С. 86–99.
21. *Чмыхова Е. В., Давыдов Д. Г., Лаврова Т. П.* Экспериментальное исследование факторов скорости чтения // Психология обучения. 2014. № 9. С. 26–36.
22. *Буймов А. Г.* Закономерности поведения кривых забывания // Доклады ТУСУРа. 2017. Т. 20. № 4. С. 138–141.
23. *Thalheimer W.* How Much Do People Forget? http://www.work-learning.com/catalog.html. 2023
24. *Шардаков М. Н.* Усвоение и сохранение в обучении. Учёные записки Ленингр. гос. пед. ин-та им. А. И. Герцена. 1940. Т. 36. 195 с.
25. *Гайдамакин Н. А.* Модель тематического разграничения доступа к информации при иерархической структуре классификатора в автоматизированных системах управления // Автоматика и телемеханика. 2003. № 3. С. 177–189.
26. *Гайдамакин Н. А.* Многоуровневое тематико-иерархическое управление доступом (MLTHS-система) // Прикладная дискретная математика. 2018. № 39. С. 42–57.
27. *Гайдамакин Н. А., Баранский В. А.* Алгебра мультирубрик на корневых деревьях иерархических тематических классификаторов // Сиб. электрон. матем. изв. 2017. Т. 14. С. 1030–1040.
28. Нечеткие множества в моделях управления и искусственного интеллекта / под ред. Д. А. Поспелова. М.: Наука, 1986. 312 с.
29. *Пегат А.* Нечеткое моделирование и управление: пер. с англ. 2-е изд. М.: БИНОМ. Лаборатория знаний, 2013. 798 с.

REFERENCES

1. *Gaydamakin N. A.* Model' i metriki osvedomlennosti v konfidentsial'noy informatsii. Chast' 1. Potentsial'naya osvedomlennost' [The model and metrics of awareness in confidential information. Part 1. Potential awareness]. Prikladnaya Diskretnaya Matematika, 2023, no. 61, pp. 86–103. (in Russian)

2. *Devyanin P. N.* Modeli bezopasnosti kompyuternykh sistem. Upravleniye dostupom i informatsionnymi potokami [Security models of computer systems. Access and information flow management]. Moscow, Goryachaya liniya — Telekom, 2020. 352 p. (in Russian)
3. *Gaydamakin N. A.* Razgranichenie dostupa k informatsii v komp'yuternykh sistemakh. [Differentiation of access to information in computer systems]. Ekaterinburg, UrFU Publ., 2003. 328 p. (in Russian)
4. *Chalmers D.* The Conscious Mind: In Search of a Fundamental Theory. Oxford, Oxford University Press, 1996. 225 p.
5. *Schutz A.* The Phenomenology of the Social World. Northwestern University Press, 1972. 255 p.
6. *Lee S. J. and Reeves T. C.* Edgar Dale: A significant contributor to the field of educational technology. Educational Technology, 2007, vol. 47, no. 6, pp. 56–59.
7. Khrestomatiya po obshchey psikhologii. Psikhologiya pamyati [Common Psychology reader. Memory Psychology]. Yu. B. Gippenreyter and V. Ya. Romanov (eds), Moscow, MSU Publ., 1979. 272 p. (in Russian)
8. *Atkinson R.* Chelovecheskaya pamyat' i protsess obucheniya [Human Memory and Learning Process]. Moscow, Progress Publ., 1980. 527 p. (in Russian)
9. *Zinchenko T. P.* Pamyat' v eksperimental'noy i kognitivnoy psikhologii [Memory in experimental and cogitative psychology]. Saint-Petersburg, Piter, 2002. 320 p. (in Russian)
10. *Lange V. G.* O skorosti zabyvaniya [About forgetting speed]. Voprosy Psikhologii, 1983, no. 4, pp. 142–145. (in Russian)
11. *Wickelgren W. A.* Trace resistance and the decay of longterm memory. J. Math. Psychology, 1972, no. 9, pp. 418–455.
12. *Wickelgren W. A.* Single-trace fragility theory of memory dynamics. Memory Cognition, 1974, vol. 2(4), pp. 775–780.
13. `http://www.ideationizing.com/2009/06/brief-history-of-mathematical.html` — A Brief History of the Mathematical Definition of Forgetting Curves, 2023.
14. *Efimov A. N.* Informatsiya: tsennost', starenie, rasseyanie [Information: Price, Consenescence, Diffusion]. Moscow, Znanie, 1978. 64 p.
15. GOST R 53894-2016. Menedzhment znaniy. Terminy i opredeleniya [Knowledge Management. Terms and Definitions]. Moscow, Standartinform, 2020. 24 p.(in Russian).
16. GOST R ISO/MEK 27002. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil menedzhmenta informatsionnoy bezopasnosti [Information Technology. Methods and Means of Ensuring Security. Information Security Management Norms and Rules]. Moscow, Standartinform, 2021. 74 p. (in Russian)
17. Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, 2003.
18. *Astakhova L. V. and Ul'yanov N. L.* Model' politiki upravleniya osvedomlennost'yu sotrudnikov organizatsii v oblasti informatsionnoy bezopasnosti [Model of control policy of awareness of the organization staff in the field of information security]. Proc.67th Conf. SUSU, Chelyabinsk, April 14–17, 2015, p. 678–682. (in Russian)
19. *Grusho A. A., Primenko E. A., and Timonina E. E.* Teoreticheskie osnovy komp'yuternoy bezopasnosti [Theoretical foundations of computer security]. Moscow, Akademiya Publ., 2009. 272 p. (in Russian)
20. *Solnyshkina S. I. and Kisel'nikov A. S.* Slozhnost' teksta: etapy izucheniya v otechestvennom prikladnom yazykoznanii [Text difficulty: learning stages in pratical homeland glossology]. Vestnik TSU. Filologiya, 2015, no. 6(38), pp. 86–99. (in Russian)

21. *Chmykhova E. V., Davydov D. G., and Lavrova T. P.* Eksperimental'noe issledovanie faktorov skorosti chteniya [Reading speed factors experimental study]. Psikhologiya Obucheniya, 2014, no. 9, pp. 26–36. (in Russian)
22. *Buymov A. G.* Zakonomernosti povedeniya krivykh zabyvaniya [Forgetting curves action patterns]. Doklady TUSURa, 2017, vol. 20, no. 4, pp. 138–141. (in Russian)
23. How Much Do People Forget? `http://www.work-learning.com/catalog.html`, 2023.
24. *Shardakov M. N.* Usvoenie i sokhranenie v obuchenii [Adoption and Saving in Learning]. Scientific Notes of the Leningrad State Pedagogical University named after Herzen, 1940, vol. 36. 195 s. (in Russian)
25. *Gaydamakin N. A.* A model of thematic differentiation of access to information for the hierarchical classifier in automatic control systems. Autom. Remote Control, 2003, vol. 64, no. 3, pp. 505–516.
26. *Gaydamakin N. A.* Mnogourovnevoe tematiko-ierarkhicheskoe upravlenie dostupom (MLTHS-sistema) [Multilevel thematic-hierarchical access control (MLTHS-system)]. Prikladnaya Diskretnaya Matematika, 2018, no. 39, pp. 42–57. (in Russian)
27. *Gaydamakin N. A. and Baranskiy V. A.* Algebra mul'tirubrik na kornevykh derev'yakh ierarkhicheskikh tematicheskikh klassifikatorov [Algebra of multirubric on root trees of hierarchical thematic classifiers]. Siberian Electronic Math. Reports, 2017, vol. 14, pp. 1030–1040. (in Russian)
28. Nechetkie mnozhestva v modelyakh upravleniya i iskusstvennogo intellekta [Illegible sets in artificial intelligence handling models]. D. A. Pospelov (ed.), Moscow, Nauka, 1986. 312 p. (in Russian)
29. *Piegat A.* Fuzzy Modeling and Control. Berlin; Heidelberg, Springer Verlag, 2001. 728 p.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718.7 DOI 10.17223/20710410/62/6

КОРОТКИЕ ПРОВЕРЯЮЩИЕ ТЕСТЫ ДЛЯ КОНТАКТНЫХ СХЕМ ПРИ ПРОИЗВОЛЬНЫХ СЛАБО СВЯЗНЫХ НЕИСПРАВНОСТЯХ КОНТАКТОВ

К. А. Попков

Институт прикладной математики им. М. В. Келдыша РАН, г. Москва, Россия

E-mail: kirill-formulist@mail.ru

Доказано, что для любого натурального k любую булеву функцию можно реализовать двухполюсной контактной схемой, k-неизбыточной и допускающей k-проверяющий тест длины не более 3 относительно произвольных связных неисправностей контактов в группах, где каждая группа состоит из одного замыкающего и одного размыкающего контакта. Установлено, что если булева функция не является самодвойственной, то оценку можно понизить до 2.

Ключевые слова: *контактная схема, связные неисправности контактов, проверяющий тест, булева функция.*

SHORT FAULT DETECTION TESTS FOR CONTACT CIRCUITS UNDER ARBITRARY WEAKLY CONNECTED FAULTS OF CONTACTS

K. A. Popkov

Keldysh Institute of Applied Mathematics, Moscow, Russia

We prove that for any natural k, any Boolean function can be implemented by a two-pole contact circuit that is k-irredundant and allows a k-fault detection test of length no more than 3 relative to arbitrary connected faults of contacts in groups, where each group consists of one closing and one opening contact. We establish that if the Boolean function is not self-dual, then this bound can be lowered to 2.

Keywords: *contact circuit, connected faults of contacts, fault detection test, Boolean function.*

Введение

Рассматривается задача синтеза легкотестируемых двухполюсных контактных схем [1], реализующих заданные булевы функции (слово «двухполюсная» в дальнейшем будем опускать). Логический подход к тестированию контактных схем предложен И. А. Чегис и С. В. Яблонским в [2]. Представим, что имеется контактная схема S, реализующая булеву функцию $f(\tilde{x}^n)$, где $\tilde{x}^n = (x_1, \ldots, x_n)$. Под воздействием некоторого источника неисправностей один или несколько контактов схемы S могут перейти

в неисправное состояние. В качестве неисправностей контактов обычно рассматриваются их обрывы и (короткие) замыкания. При обрыве контакта проводимость между его концами становится тождественно нулевой, а при замыкании — тождественно единичной. В результате схема S вместо исходной функции $f(\tilde{x}^n)$ станет реализовывать некоторую булеву функцию $g(\tilde{x}^n)$, вообще говоря, отличную от f. Все такие функции $g(\tilde{x}^n)$, получающиеся при всевозможных допустимых для рассматриваемой задачи неисправностях в схеме S, называются *функциями неисправности* данной схемы.

Введём следующие определения [3–5]. *Проверяющим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что для любой отличной от $f(\tilde{x}^n)$ функции неисправности $g(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\sigma}$, на котором $f(\tilde{\sigma}) \neq g(\tilde{\sigma})$. *Диагностическим тестом* для схемы S называется такое множество T наборов значений переменных $x_1, \ldots, x_n$, что T является проверяющим тестом и, кроме того, для любых двух различных функций неисправности $g_1(\tilde{x}^n)$ и $g_2(\tilde{x}^n)$ схемы S в T найдётся набор $\tilde{\pi}$, на котором $g_1(\tilde{\pi}) \neq g_2(\tilde{\pi})$. Число наборов в T называется *длиной* теста. В качестве тривиального диагностического (и проверяющего) теста длины 2^n для схемы S всегда можно взять множество, состоящее из всех двоичных n-разрядных наборов. Тест называется *полным*, если в схеме могут быть неисправны сколько угодно контактов, и *единичным*, если в схеме может быть неисправен только один контакт. Единичные тесты обычно рассматривают для *неизбыточных схем* [5, с. 110–111], в которых любая допустимая неисправность любого одного контакта приводит к функции неисправности, отличной от функции, реализуемой данной схемой; такие функции неисправности называют *нетривиальными*. Если в схеме допускаются только обрывы контактов (или только их замыкания), то говорят о *тестах размыкания* (соответственно о *тестах замыкания*).

В работах [6–16] получены различные, в том числе окончательные результаты о возможностях построения легкотестируемых контактных схем, реализующих заданные булевы функции. Упомянем только один результат, который удобно сравнить с нижеследующей теоремой 4. В [9, теорема 2] доказано, что для любого натурального $n \geqslant 2$ существует булева функция от n переменных, которую нельзя реализовать контактной схемой, неизбыточной и допускающей единичный проверяющий тест длины менее $n + 2$ относительно обрывов и замыканий контактов.

Назовём проверяющий (диагностический) тест для контактной схемы *k-проверяющим* (*k-диагностическим*), если в схеме может произойти не более k неисправностей, где $k \in \mathbb{N}$. Будем рассматривать такие тесты только для *k-неизбыточных схем*, в которых любые не менее одной и не более k допустимых неисправностей приводят к нетривиальной функции неисправности.

В настоящей работе в качестве неисправностей в контактных схемах рассмотрим связные неисправности контактов в группах, как это сделано Н. П. Редькиным в [17, 18]. Пусть зафиксированы целые неотрицательные числа a и b, удовлетворяющие условиям $a + b \geqslant 2$ и $a \geqslant b$. Будем считать, что в рассматриваемых схемах все контакты разбиваются на группы связанных между собой контактов. Каждая группа содержит $a + b$ контактов, отвечающих одной и той же переменной, и разбивается на два блока из a контактов (первый блок) и b контактов (второй блок), причём внутри каждого блока все контакты одинаковы (т. е. либо все замыкающие, либо все размыкающие), а в разных блоках контакты противоположны. Предполагается, что обрыв (замыкание) любого контакта из одного из блоков влечёт за собой обрыв (соответственно замыкание) всех остальных контактов из этого блока и замыкание (соответственно обрыв) всех контактов из другого блока. Таким образом, каждая контактная группа

подвержена только двум видам неисправностей: обрыву всех контактов из первого блока и одновременному замыканию всех контактов из второго блока, либо замыканию всех контактов из первого блока и одновременному обрыву всех контактов из второго блока. Мотивировка рассмотрения именно таких неисправностей с физической точки зрения даётся в [17, с. 42–43]. Контактные схемы, удовлетворяющие указанным условиям, будем называть (a, b)-*схемами*. Общее число неисправностей в (a, b)-схеме будем считать равным числу неисправных контактных групп (а не неисправных контактов).

Пусть множество T является k-проверяющим тестом для некоторой (a, b)-схемы S. Введём следующие обозначения: $D^{k\text{-П}}_{a,b}(T)$ — длина теста T; $D^{k\text{-П}}_{a,b}(S) = \min D^{k\text{-П}}_{a,b}(T)$, где минимум берётся по всем k-проверяющим тестам T для схемы S; $D^{k\text{-П}}_{a,b}(f) = \min D^{k\text{-П}}_{a,b}(S)$, где минимум берётся по всем k-неизбыточным (a, b)-схемам S, реализующим функцию f; $D^{k\text{-П}}_{a,b}(n) = \max D^{k\text{-П}}_{a,b}(f)$, где максимум берётся по всем булевым функциям f от n переменных. Функция $D^{k\text{-П}}_{a,b}(n)$ называется *функцией Шеннона* длины k-проверяющего теста. По аналогии с функциями $D^{k\text{-П}}_{a,b}$ можно ввести функции $D^{k\text{-Д}}_{a,b}$, $D^{\text{ПП}}_{a,b}$ и $D^{\text{ПД}}_{a,b}$ для соответственно k-диагностического, полного проверяющего и полного диагностического тестов, зависящие от T, S, f и n (в определениях функций $D^{\text{ПП}}_{a,b}(f)$ и $D^{\text{ПД}}_{a,b}(f)$ не предполагается неизбыточности схем). Если в первом блоке каждой контактной группы допустимы как обрыв, так и замыкание всех контактов (соответственно допустим только обрыв всех контактов, допустимо только замыкание всех контактов), то в конце верхнего индекса буквы D через точку с запятой будем ставить 01 (соответственно 0, 1); в первом из указанных трёх случаев связные неисправности контактов будем считать *произвольными*, а во втором и третьем случаях — *однотипными*. Основной целью исследований является нахождение оценок (в идеале — точных значений) величин $D_{a,b}(f)$ и $D_{a,b}(n)$ с разными верхними индексами при различных a, b, f и n.

В [17] установлено, что если $a + b \geqslant 3$, а t — натуральное число, то $2n - 2t - 1 \leqslant D^{\text{ПП};\,01}_{a,b}(n) \leqslant 2n$ при $n = 2^t + t + 1$; $2n - 2t - 2 \leqslant D^{\text{ПП};\,01}_{a,b}(n) \leqslant 2n$ при $2^t + t + 1 < n \leqslant 2^{t+1} + t + 1$. В [18] при $a + b \geqslant 3$ доказано неравенство $D^{1\text{-Д};\,01}_{a,b}(n) \leqslant 4n$, а при $a + b = 2$ получены оценки $D^{1\text{-П};\,01}_{a,b}(n) \leqslant 2^{\lceil n/2 \rceil} + 2^{\lfloor n/2 \rfloor} + n$, $D^{\text{ПП};\,1}_{a,b}(n) \leqslant 2n$ и $D^{\text{ПП};\,0}_{a,b}(n) \leqslant 2n$. Вслед за работой [18], связные неисправности контактов в случае $a + b = 2$ будем считать *слабо связными*.

1. Покрывающие и ключевые множества

Двоичный n-разрядный набор $\tilde{\sigma}$ будем называть (i, α)-*набором*, если его i-я (слева) компонента равна α.

Двоичный n-разрядный набор $\tilde{\sigma}$ будем называть β-*набором* булевой функции $f(\tilde{x}^n)$, если $f(\tilde{\sigma}) = \beta$.

Множество M (некоторых) β-наборов булевой функции $f(\tilde{x}^n)$, где $n \geqslant 1$ и $\beta \in \{0, 1\}$, назовём β-*покрывающим* для этой функции, если для любых $i \in \{1, \ldots, n\}$, $\alpha \in \{0, 1\}$ в M найдётся (i, α)-набор.

Множество M (некоторых) β-наборов булевой функции $f(\tilde{x}^n)$, где $n \geqslant 1$ и $\beta \in \{0, 1\}$, назовём β-*ключевым* для этой функции, если для любых $i \in \{1, \ldots, n\}$, $\alpha \in \{0, 1\}$, таких, что существует хотя бы один (i, α)-набор, являющийся β-набором функции $f(\tilde{x}^n)$, в M найдётся (i, α)-набор.

В качестве β-ключевого множества для функции $f(\tilde{x}^n)$ всегда можно взять множество всех её β-наборов.

Очевидно, что любое β-покрывающее множество является β-ключевым. Обратное, вообще говоря, неверно: например, для функции $f(x_1, x_2) = x_1 \& x_2$ множество $\{(1,1)\}$ является 1-ключевым, но не 1-покрывающим (более того, для этой функции не существует ни одного 1-покрывающего множества).

Сформулируем два полученных ранее результата.

Теорема 1 [11, теорема 1]. Пусть M — 1-ключевое множество для булевой функции $f(\tilde{x}^n)$, $n \geqslant 1$. Тогда эту функцию для любого $k \in \mathbb{N}$ можно реализовать контактной схемой, k-неизбыточной относительно обрывов контактов, для которой множество M является k-проверяющим тестом размыкания.

Теорема 2 [16, теорема 1]. Пусть M — 0-ключевое множество для булевой функции $f(\tilde{x}^n)$, $n \geqslant 1$. Тогда эту функцию для любого $k \in \mathbb{N}$ можно реализовать контактной схемой, k-неизбыточной относительно замыканий контактов, для которой множество M является k-проверяющим тестом замыкания.

В формулировках теорем 1 и 2 общее число неисправностей в контактных схемах считается равным числу неисправных контактов.

Булева функция $f(\tilde{x}^n)$ называется *самодвойственной*, если $\overline{f}(\overline{x}_1, \ldots, \overline{x}_n) = f(\tilde{x}^n)$.

Утверждение 1. Для любой несамодвойственной булевой функции $f(\tilde{x}^n)$, $n \geqslant 1$, существует β-покрывающее множество мощности 2 хотя бы для одного $\beta \in \{0,1\}$.

Доказательство. Существуют такие $\sigma_1, \ldots, \sigma_n \in \{0,1\}$, что $f(\sigma_1, \ldots, \sigma_n) = f(\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$, так как функция $f(\tilde{x}^n)$ несамодвойственная. Тогда множество

$$\{(\sigma_1, \ldots, \sigma_n), (\overline{\sigma}_1, \ldots, \overline{\sigma}_n)\}$$

является β-покрывающим для этой функции при $\beta = f(\sigma_1, \ldots, \sigma_n)$. ■

Утверждение 2. Для любой самодвойственной булевой функции $f(\tilde{x}^n)$, существенно зависящей по крайней мере от трёх переменных, существует β-покрывающее множество мощности 3 для каждого $\beta \in \{0,1\}$.

Доказательство. Функция f неконстантная, поэтому существуют два двоичных n-разрядных набора, различающихся только в одном разряде, на которых она принимает различные значения. Обозначим эти наборы через $(\sigma_1, \ldots, \sigma_n)$ и $(\sigma_1, \ldots, \sigma_{r-1}, \overline{\sigma}_r, \sigma_{r+1}, \ldots, \sigma_n)$, где $r \in \{1, \ldots, n\}$; тогда $f(\sigma_1, \ldots, \sigma_n) = \overline{f}(\sigma_1, \ldots, \sigma_{r-1}, \overline{\sigma}_r, \sigma_{r+1}, \ldots, \sigma_n)$. Функция $f(\tilde{x}^n)$ самодвойственная, поэтому $f(\sigma_1, \ldots, \sigma_n) = \overline{f}(\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$. Из последних двух соотношений вытекает, что $f(\overline{\sigma}_1, \ldots, \overline{\sigma}_n) = f(\sigma_1, \ldots, \sigma_{r-1}, \overline{\sigma}_r, \sigma_{r+1}, \ldots, \sigma_n)$. Положим $\gamma = f(\overline{\sigma}_1, \ldots, \overline{\sigma}_n)$.

Если для любых $\pi_1, \ldots, \pi_{r-1}, \pi_{r+1}, \ldots, \pi_n \in \{0,1\}$ выполняется равенство $f(\pi_1, \ldots, \pi_{r-1}, \sigma_r, \pi_{r+1}, \ldots, \pi_n) = \overline{\gamma}$, то $f(\overline{\pi}_1, \ldots, \overline{\pi}_{r-1}, \overline{\sigma}_r, \overline{\pi}_{r+1}, \ldots, \overline{\pi}_n) = \gamma$ для любых $\pi_1, \ldots, \pi_{r-1}, \pi_{r+1}, \ldots, \pi_n \in \{0,1\}$ в силу самодвойственности функции f, а тогда легко проверить, что $f(\tilde{x}^n) = x_r \oplus \sigma_r \oplus \overline{\gamma}$. Получаем, что функция f существенно зависит только от переменной x_r, однако это противоречит условию утверждения 2. Поэтому существуют такие $\pi_1, \ldots, \pi_{r-1}, \pi_{r+1}, \ldots, \pi_n \in \{0,1\}$, что $f(\pi_1, \ldots, \pi_{r-1}, \sigma_r, \pi_{r+1}, \ldots, \pi_n) = \gamma$. В таком случае множество

$$M = \{(\overline{\sigma}_1, \ldots, \overline{\sigma}_n), (\sigma_1, \ldots, \sigma_{r-1}, \overline{\sigma}_r, \sigma_{r+1}, \ldots, \sigma_n), (\pi_1, \ldots, \pi_{r-1}, \sigma_r, \pi_{r+1}, \ldots, \pi_n)\}$$

является γ-покрывающим для функции $f(\tilde{x}^n)$. Действительно, на каждом наборе из этого множества, как показано выше, функция f принимает значение γ; для любых $i \in \{1, \ldots, n\} \setminus \{r\}$, $\alpha \in \{0,1\}$ один из наборов $(\overline{\sigma}_1, \ldots, \overline{\sigma}_n), (\sigma_1, \ldots, \sigma_{r-1}, \overline{\sigma}_r, \sigma_{r+1}, \ldots, \sigma_n)$

является (i,α)-набором, а для $i = r$ и любого $\alpha \in \{0,1\}$ один из наборов $(\overline{\sigma}_1,\dots,\overline{\sigma}_n),(\pi_1,\dots,\pi_{r-1},\sigma_r,\pi_{r+1},\dots,\pi_n)$ является (i,α)-набором. Множество

$$\{(\sigma_1,\dots,\sigma_n),(\overline{\sigma}_1,\dots,\overline{\sigma}_{r-1},\sigma_r,\overline{\sigma}_{r+1},\dots,\overline{\sigma}_n),(\overline{\pi}_1,\dots,\overline{\pi}_{r-1},\overline{\sigma}_r,\overline{\pi}_{r+1},\dots,\overline{\pi}_n)\},$$

состоящее из наборов, противоположных наборам из M, является $\overline{\gamma}$-покрывающим для функции $f(\tilde{x}^n)$. Действительно, на каждом наборе из этого множества функция f в силу самодвойственности принимает значение $\overline{\gamma}$; для любых $i \in \{1,\dots,n\}\backslash\{r\}$, $\alpha \in \{0,1\}$ один из наборов $(\sigma_1,\dots,\sigma_n),(\overline{\sigma}_1,\dots,\overline{\sigma}_{r-1},\sigma_r,\overline{\sigma}_{r+1},\dots,\overline{\sigma}_n)$ является (i,α)-набором, а для $i = r$ и любого $\alpha \in \{0,1\}$ один из наборов $(\sigma_1,\dots,\sigma_n),(\overline{\pi}_1,\dots,\overline{\pi}_{r-1},\overline{\sigma}_r,\overline{\pi}_{r+1},\dots,\overline{\pi}_n)$ является (i,α)-набором. ■

2. Формулировки и доказательства основных результатов

Введём обозначение

$$\alpha^\beta = \begin{cases} \alpha, & \text{если } \beta = 1, \\ \overline{\alpha}, & \text{если } \beta = 0, \end{cases}$$

где $\alpha \in \{0,1\}$.

Далее для краткости всюду вместо «замыкающий (размыкающий) контакт, отвечающий переменной x_i», $i = 1,\dots,n$, будем говорить «контакт x_i» (соответственно «контакт $\overline{x}_i$»).

Теорема 3. Пусть M — β-покрывающее множество для булевой функции $f(\tilde{x}^n)$, где $\beta \in \{0,1\}$ и $n \geqslant 1$. Тогда эту функцию для любого $k \in \mathbb{N}$ можно реализовать k-неизбыточной $(1,1)$-схемой, для которой множество M является k-проверяющим тестом относительно произвольных связных неисправностей контактов.

Доказательство. Зафиксируем натуральное k. Рассмотрим два случая.

1. Пусть $\beta = 1$. Из теоремы 1 и того факта, что любое β-покрывающее множество является β-ключевым, следует, что функцию $f(\tilde{x}^n)$ можно реализовать контактной схемой S, k-неизбыточной относительно обрывов контактов, для которой множество M является k-проверяющим тестом размыкания. Построим контактные схемы $A_1,\dots,A_n$ по аналогии с тем, как это сделано в [17, с. 44]. Пусть i — произвольный индекс из множества $\{1,\dots,n\}$. Схема A_i представляет собой параллельное соединение двух несамопересекающихся цепей C_i^1 и C_i^0 из контактов. Цепь C_i^1 содержит только контакты x_i, а цепь C_i^0 — только контакты $\overline{x}_i$. Для каждого контакта x_i, содержащегося в схеме S, в цепи C_i^0 содержится свой контакт $\overline{x}_i$, который образует с ним контактную группу; будем считать эту группу *основной*. Для каждого контакта $\overline{x}_i$, содержащегося в схеме S, в цепи C_i^1 содержится свой контакт x_i, который образует с ним контактную группу; её также будем считать *основной*. Если хотя бы в одной из цепей C_i^1, C_i^0 к настоящему моменту содержится не более k контактов, добавим к каждой из них одинаковое число контактов, чтобы как в цепи C_i^1, так и в цепи C_i^0 содержалось не менее $k+1$ контактов; при этом к цепи C_i^1 будем добавлять только контакты x_i, а к цепи C_i^0 — только контакты $\overline{x}_i$, и все добавляемые контакты разобьём на группы из двух связанных между собой контактов x_i и $\overline{x}_i$, которые будем считать *дополнительными* группами. В итоге каждый контакт цепи C_i^1 имеет тип x_i и образует контактную группу с каким-то контактом $\overline{x}_i$, содержащимся либо в схеме S, либо в цепи C_i^0, а каждый контакт цепи C_i^0 имеет тип $\overline{x}_i$ и образует контактную группу с каким-то контактом x_i, содержащимся либо в схеме S, либо в цепи C_i^1.

Соединим все контактные схемы $S, A_1,\dots,A_n$ последовательно; обозначим полученную контактную схему через S^* (рис. 1). В ней все контакты разделены на группы

связанных между собой контактов, каждая из которых состоит из одного замыкающего и одного размыкающего контакта переменной x_i для некоторого $i \in \{1, \ldots, n\}$. Таким образом, схема S^* является $(1,1)$-схемой. При отсутствии неисправностей в этой схеме подсхема A_i, очевидно, реализует функцию $x_i \vee \overline{x}_i \equiv 1$ для $i = 1, \ldots, n$, поэтому схема S^* реализует функцию $f(\tilde{x}^n)\&\underbrace{1\&\ldots\&1}_{n} = f(\tilde{x}^n)$. Докажем, что данная схема k-неизбыточна и допускает k-проверяющий тест M относительно произвольных связных неисправностей контактов. Предположим, что в схеме S^* оказались неисправными не менее одной и не более k контактных групп. Согласно определению $(1,1)$-схемы, в каждой неисправной контактной группе один контакт оборван и один замкнут. Рассмотрим два подслучая.

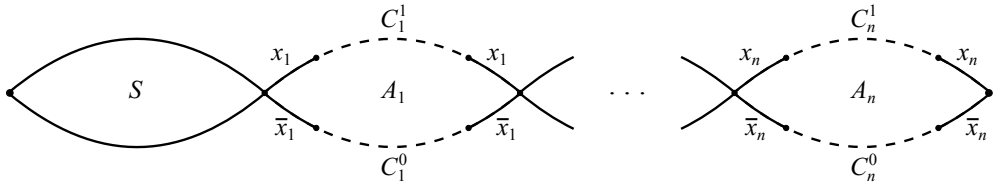


Рис. 1. Схема S^* в случае 1

1.1. Существует такое $i \in \{1, \ldots, n\}$, что в подсхеме A_i хотя бы один контакт оборван. Пусть это контакт x_i^α, где $\alpha \in \{0, 1\}$. Тогда функция проводимости цепи C_i^α, состоящей из контактов x_i^α, равна тождественному нулю. В цепи $C_i^{\overline{\alpha}}$, состоящей из контактов $x_i^{\overline{\alpha}}$, по построению содержится не менее $k+1$ контактов. Если хотя бы один из них оборван, то функция проводимости цепи $C_i^{\overline{\alpha}}$ также равна тождественному нулю. В противном случае замкнуто в указанной цепи может быть не более k контактов, поскольку всего в схеме S^* неисправно не более k контактных групп. Таким образом, хотя бы один контакт в цепи $C_i^{\overline{\alpha}}$ исправен и функция её проводимости равна $x_i^{\overline{\alpha}}$. Следовательно, функция проводимости подсхемы A_i равна либо $0 \vee 0 = 0$, либо $0 \vee x_i^{\overline{\alpha}} = x_i^{\overline{\alpha}}$. Множество M является 1-покрывающим для функции $f(\tilde{x}^n)$, поэтому в нём найдётся такой (i, α)-набор $\tilde{\sigma}$, что $f(\tilde{\sigma}) = 1$. На этом наборе подсхема A_i не проводит и схема S^* выдаст значение 0, отличное от $f(\tilde{\sigma})$; тем самым неисправность схемы будет обнаружена.

1.2. Ни в одной из подсхем $A_1, \ldots, A_n$ ни один контакт не оборван. Тогда в подсхеме S ни один контакт не замкнут (в противном случае контакт, образующий группу с произвольным замкнутым контактом x_i^α подсхемы S, по построению содержался бы в цепи $C_i^{\overline{\alpha}}$ подсхемы A_i и был бы оборван), а все дополнительные контактные группы в схеме S^* исправны. Значит, неисправны не менее одной и не более k основных контактных групп в данной схеме, и при этом тот контакт каждой неисправной группы, который содержится в подсхеме S, оборван. Множество M является k-проверяющим тестом размыкания для k-неизбыточной схемы S, поэтому хотя бы на одном наборе $\tilde{\sigma}$ из M подсхема S выдаст значение, отличное от «правильного», т. е. от $f(\tilde{\sigma})$. Из описания подслучая 1.2 вытекает также, что для любых $i \in \{1, \ldots, n\}$, $\alpha \in \{0, 1\}$ функция проводимости цепи C_i^α равна либо x_i^α, либо 1, поэтому для любого $i \in \{1, \ldots, n\}$ функция проводимости подсхемы A_i равна либо $x_i^\alpha \vee x_i^{\overline{\alpha}}$, либо $1 \vee x_i^{\overline{\alpha}}$, либо $x_i^\alpha \vee 1$, либо $1 \vee 1$, т. е. равна тождественной единице. Следовательно, функция, реализуемая схемой S^*, совпадает с функцией проводимости подсхемы S, и на наборе $\tilde{\sigma}$ схема S^* выдаст значение, отличное от $f(\tilde{\sigma})$; тем самым неисправность схемы будет обнаружена.

Из приведённых рассуждений следует, что схема S^* является k-неизбыточной и допускает k-проверяющий тест M относительно произвольных связных неисправностей контактов. Случай 1 разобран.

2. Пусть $\beta = 0$. Из теоремы 2 и того факта, что любое β-покрывающее множество является β-ключевым, следует, что функцию $f(\tilde{x}^n)$ можно реализовать контактной схемой S, k-неизбыточной относительно замыканий контактов, для которой множество M является k-проверяющим тестом замыкания. Построим контактные схемы $B_1^1, \ldots, B_n^1, B_1^0, \ldots, B_n^0$ по аналогии с тем, как это сделано в [17, с. 45] (в [17] они обозначаются через $B_1, \ldots, B_n, B_1', \ldots, B_n'$ соответственно). Рассмотрим произвольные $i \in \{1, \ldots, n\}$ и $\alpha \in \{0, 1\}$. Схема B_i^α представляет собой пучок из контактов x_i^α, т. е. параллельное соединение некоторого числа контактов x_i^α. Для каждого контакта $x_i^{\overline{\alpha}}$, содержащегося в схеме S, в схеме B_i^α содержится свой контакт x_i^α, который образует с ним контактную группу; будем считать эту группу *основной*. Если хотя бы в одной из схем B_i^1, B_i^0 к настоящему моменту содержится не более k контактов, добавим к каждой из них одинаковое число контактов, чтобы как в схеме B_i^1, так и в схеме B_i^0 содержалось не менее $k+1$ контактов и каждая из схем B_i^1, B_i^0 по-прежнему представляла собой пучок из контактов; при этом к схеме B_i^1 будем добавлять только контакты x_i, а к схеме B_i^0 — только контакты $\overline{x}_i$, и все добавляемые контакты разобьём на группы из двух связанных между собой контактов x_i и $\overline{x}_i$, которые будем считать *дополнительными* группами. В итоге каждый контакт схемы B_i^1 имеет тип x_i и образует контактную группу с каким-то контактом $\overline{x}_i$, содержащимся в одной из схем S, B_i^0, а каждый контакт схемы B_i^0 имеет тип $\overline{x}_i$ и образует контактную группу с каким-то контактом x_i, содержащимся в одной из схем S, B_i^1. Соединим контактные схемы B_i^1 и B_i^0 последовательно и обозначим полученную схему через B_i.

Теперь все контактные схемы $S, B_1, \ldots, B_n$ соединим параллельно и обозначим итоговую контактную схему через S^* (рис. 2). В ней все контакты разделены на группы связанных между собой контактов, каждая из которых состоит из одного замыкающего и одного размыкающего контакта переменной x_i для некоторого $i \in \{1, \ldots, n\}$. Таким образом, схема S^* является $(1,1)$-схемой. При отсутствии неисправностей в этой схеме подсхема B_i, очевидно, реализует функцию $x_i \& \overline{x}_i \equiv 0$ для $i = 1, \ldots, n$, поэтому схема S^* реализует функцию $f(\tilde{x}^n) \vee \underbrace{0 \vee \ldots \vee 0}_{n} = f(\tilde{x}^n)$. Докажем, что данная схема k-неизбыточна и допускает k-проверяющий тест M относительно произвольных связных неисправностей контактов. Предположим, что в схеме S^* оказались неисправными не менее одной и не более k контактных групп. Отметим, что в каждой неисправной контактной группе один контакт оборван и один замкнут. Рассмотрим два подслучая.

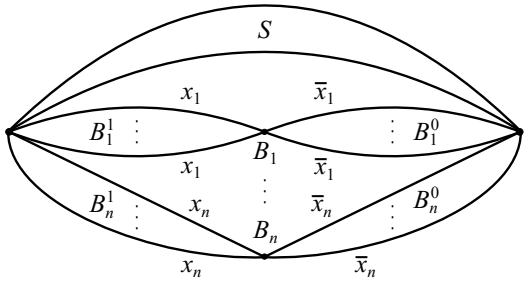


Рис. 2. Схема S^* в случае 2

2.1. Существует такое $i \in \{1, \ldots, n\}$, что в подсхеме B_i хотя бы один контакт замкнут. Пусть это контакт x_i^α, где $\alpha \in \{0, 1\}$. Тогда функция проводимости подсхемы B_i^α, состоящей из контактов x_i^α, равна тождественной единице. В подсхеме $B_i^{\overline{\alpha}}$, состоящей из контактов $x_i^{\overline{\alpha}}$, по построению содержится не менее $k+1$ контактов. Если хотя бы один из них замкнут, то функция проводимости подсхемы $B_i^{\overline{\alpha}}$ также равна тождественной единице. В противном случае оборвано в указанной подсхеме может быть не более k контактов, поскольку всего в схеме S^* неисправно не более k контактных групп. Таким образом, хотя бы один контакт в подсхеме $B_i^{\overline{\alpha}}$ исправен и функция её проводимости равна $x_i^{\overline{\alpha}}$. Следовательно, функция проводимости подсхемы B_i равна либо $1 \vee 1 = 1$, либо $1 \vee x_i^{\overline{\alpha}} = x_i^{\overline{\alpha}}$. Множество M является 0-покрывающим для функции $f(\tilde{x}^n)$, поэтому в нём найдётся такой $(i, \overline{\alpha})$-набор $\tilde{\sigma}$, что $f(\tilde{\sigma}) = 0$. На этом наборе подсхема B_i проводит и схема S^* выдаст значение 1, отличное от $f(\tilde{\sigma})$; тем самым неисправность схемы будет обнаружена.

2.2. Ни в одной из подсхем $B_1, \ldots, B_n$ ни один контакт не замкнут. Тогда в подсхеме S ни один контакт не оборван (в противном случае контакт, образующий группу с произвольным оборванным контактом x_i^α подсхемы S, по построению содержался бы в подсхеме $B_i^{\overline{\alpha}}$, а значит, в подсхеме B_i, и был бы замкнут), а все дополнительные контактные группы в схеме S^* исправны. Значит, неисправны не менее одной и не более k основных контактных групп в данной схеме, и при этом тот контакт каждой неисправной группы, который содержится в подсхеме S, замкнут. Множество M является k-проверяющим тестом замыкания для k-неизбыточной схемы S, поэтому хотя бы на одном наборе $\tilde{\sigma}$ из M подсхема S выдаст значение, отличное от «правильного», т. е. от $f(\tilde{\sigma})$. Из описания подслучая 2.2 вытекает также, что для любых $i \in \{1, \ldots, n\}$, $\alpha \in \{0, 1\}$ функция проводимости подсхемы B_i^α равна либо x_i^α, либо 0, поэтому для любого $i \in \{1, \ldots, n\}$ функция проводимости подсхемы B_i равна либо $x_i^\alpha \& x_i^{\overline{\alpha}}$, либо $0 \& x_i^{\overline{\alpha}}$, либо $x_i^\alpha \& 0$, либо $0 \& 0$, т. е. равна тождественному нулю. Следовательно, функция, реализуемая схемой S^*, совпадает с функцией проводимости подсхемы S, и на наборе $\tilde{\sigma}$ схема S^* выдаст значение, отличное от $f(\tilde{\sigma})$; тем самым неисправность схемы будет обнаружена.

Из приведённых рассуждений следует, что схема S^* является k-неизбыточной и допускает k-проверяющий тест M относительно произвольных связных неисправностей контактов. Случай 2 разобран. ■

Теорема 4. Пусть $f(\tilde{x}^n)$ — булева функция и $k \in \mathbb{N}$. Тогда

$$\begin{cases} D_{1,1}^{k\text{-П};\,01}(f) = 0, & \text{если } f \equiv 0 \text{ или } f \equiv 1, \\ D_{1,1}^{k\text{-П};\,01}(f) \in \{2, 3\}, & \text{если } f \text{ — самодвойственная функция, существенно зависящая} \\ & \text{по крайней мере от трёх переменных,} \\ D_{1,1}^{k\text{-П};\,01}(f) = 2 & \text{в остальных случаях.} \end{cases}$$

Доказательство. Если $f \equiv 0$ или $f \equiv 1$, то функцию f можно реализовать $(1, 1)$-схемой, не содержащей ни одного контакта. У такой схемы нет ни одной функции неисправности, поэтому она k-неизбыточна и допускает k-проверяющий тест $\varnothing$ длины 0 (относительно произвольных связных неисправностей контактов), откуда следует, что $D_{1,1}^{k\text{-П};\,01}(f) = 0$. Далее будем считать, что функция f отлична от констант. Докажем неравенство $D_{1,1}^{k\text{-П};\,01}(f) \geqslant 2$.

Пусть S — произвольная k-неизбыточная $(1, 1)$-схема, реализующая функцию $f(\tilde{x}^n)$, и T — произвольный k-проверяющий тест для схемы S. В этой схеме содержится

хотя бы одна контактная группа, состоящая из контактов x_i и $\overline{x}_i$ для некоторого $i \in \{1, \ldots, n\}$. Если i-я компонента каждого набора из множества T равна нулю (единице), то в случае отсутствия неисправностей в схеме S при подаче вместо набора переменных $(x_1, \ldots, x_n)$ произвольного набора $\tilde{\sigma}$ из T все контакты x_i в этой схеме будут иметь нулевую (соответственно единичную) проводимость, а все контакты $\overline{x}_i$ — единичную (нулевую) проводимость, поэтому обрыв (замыкание) контакта x_i и замыкание (обрыв) контакта $\overline{x}_i$ из рассматриваемой группы никак не отразятся на значении, выдаваемой схемой на наборе $\tilde{\sigma}$. Однако это противоречит тому, что схема S является k-неизбыточной и допускает k-проверяющий тест T. Значит, в T входят хотя бы один $(i, 1)$-набор и хотя бы один $(i, 0)$-набор. Таким образом, любой k-проверяющий тест для схемы S содержит по крайней мере два набора, откуда следует, что $D_{1,1}^{k\text{-П};\,01}(S) \geqslant 2$, а с учётом произвольности выбора схемы S — что $D_{1,1}^{k\text{-П};\,01}(f) \geqslant 2$.

Если $f(\tilde{x}^n)$ — самодвойственная функция, существенно зависящая по крайней мере от трёх переменных, то в силу утверждения 2 и теоремы 3 эту функцию можно реализовать k-неизбыточной $(1, 1)$-схемой, допускающей k-проверяющий тест длины 3; отсюда $D_{1,1}^{k\text{-П};\,01}(f) \leqslant 3$ и $D_{1,1}^{k\text{-П};\,01}(f) \in \{2, 3\}$. Если $f(\tilde{x}^n)$ — несамодвойственная функция, то в силу утверждения 1 и теоремы 3 данную функцию можно реализовать k-неизбыточной $(1, 1)$-схемой, допускающей k-проверяющий тест длины 2; отсюда $D_{1,1}^{k\text{-П};\,01}(f) \leqslant 2$ и $D_{1,1}^{k\text{-П};\,01}(f) = 2$. Пусть, наконец, $f(\tilde{x}^n)$ — самодвойственная функция, существенно зависящая менее чем от трёх переменных. Тогда это обязательно функция вида x_i^α для некоторых $i \in \{1, \ldots, n\}$ и $\alpha \in \{0, 1\}$ (как известно, ни одна булева функция, существенно зависящая ровно от двух переменных, не является самодвойственной). Реализуем её $(1, 1)$-схемой, содержащей ровно три вершины и ровно два контакта, образующих группу: контакт x_i^α между полюсами схемы и контакт $x_i^{\overline{\alpha}}$ между одним из полюсов схемы и её вершиной, отличной от полюсов. При обрыве контакта x_i^α и замыкании контакта $x_i^{\overline{\alpha}}$ схема станет реализовывать тождественный нуль, а при замыкании контакта x_i^α и обрыве контакта $x_i^{\overline{\alpha}}$ — тождественную единицу. Константу 0 (константу 1) можно отличить от функции $f(\tilde{x}^n) = x_i^\alpha$ на любом (i, α)-наборе (соответственно $(i, \overline{\alpha})$-наборе), поэтому рассматриваемая схема k-неизбыточна и допускает k-проверяющий тест длины 2. Отсюда следует, что $D_{1,1}^{k\text{-П};\,01}(f) \leqslant 2$ и $D_{1,1}^{k\text{-П};\,01}(f) = 2$. ■

Следствие 1. Пусть $n \in \mathbb{N} \cup \{0\}$ и $k \in \mathbb{N}$. Тогда

$$\begin{cases} D_{1,1}^{k\text{-П};\,01}(n) = 0, & \text{если } n = 0, \\ D_{1,1}^{k\text{-П};\,01}(n) = 2, & \text{если } n = 1 \text{ или } n = 2, \\ D_{1,1}^{k\text{-П};\,01}(n) \in \{2, 3\}, & \text{если } n \geqslant 3. \end{cases}$$

Заключение

Сравним полученные результаты с результатами работ [9, 18]. В [18], в частности, доказано неравенство $D_{a,b}^{1\text{-П};\,01}(n) \leqslant 2^{\lceil n/2 \rceil} + 2^{\lfloor n/2 \rfloor} + n$ при $a + b = 2$. Следствие 1 показывает, что в случае $a = b = 1$, $n \geqslant 3$ верхнюю оценку $2^{\lceil n/2 \rceil} + 2^{\lfloor n/2 \rfloor} + n$ можно понизить до 3 и затем для любого $k \in \mathbb{N}$ распространить на величину $D_{1,1}^{k\text{-П};\,01}(n)$. В [9, теорема 2] установлено, что для любого натурального $n \geqslant 2$ существует булева функция от n переменных, которую нельзя реализовать контактной схемой, неизбыточной и допускающей единичный проверяющий тест длины менее $n + 2$ относительно произвольных неисправностей контактов, т. е. обрывов и замыканий контактов. Теорема 4 демонстрирует, что если разбить все контакты на пары противоположных контактов и связать между собой обрыв одного контакта и замыкание другого контакта в паре,

то, напротив, любую булеву функцию для любого $k \in \mathbb{N}$ можно реализовать контактной схемой, k-неизбыточной и допускающей k-проверяющий тест длины не более 3 относительно произвольных связных неисправностей контактов.

ЛИТЕРАТУРА

1. *Лупанов О. Б.* Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984. 138 с.
2. *Чегис И. А., Яблонский С. В.* Логические способы контроля работы электрических схем // Труды МИАН. 1958. Т. 51. С. 270–360.
3. *Яблонский С. В.* Надёжность и контроль управляющих систем // Материалы Всесоюзного семинара по дискретной математике и её приложениям (Москва, 31 января–2 февраля 1984 г.). М.: Изд-во МГУ, 1986. С. 7–12.
4. *Яблонский С. В.* Некоторые вопросы надёжности и контроля управляющих систем // Математические вопросы кибернетики. 1988. Вып. 1. С. 5–25.
5. *Редькин Н. П.* Надёжность и диагностика схем. М.: Изд-во МГУ, 1992. 192 с.
6. *Мадатян Х. А.* Полный тест для бесповторных контактных схем // Проблемы кибернетики. Вып. 23. М.: Наука, 1970. С. 103–118.
7. *Редькин Н. П.* О полных проверяющих тестах для контактных схем // Методы дискретного анализа в исследовании экстремальных структур. Вып. 39. Новосибирск: ИМ СО АН СССР, 1983. С. 80–87.
8. *Редькин Н. П.* О проверяющих тестах замыкания и размыкания // Методы дискретного анализа в оптимизации управляющих систем. Вып. 40. Новосибирск: ИМ СО АН СССР, 1983. С. 87–99.
9. *Романов Д. С., Романова Е. Ю.* О единичных проверяющих тестах константной длины для обобщённых итеративных контактных схем // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. 2015. № 3. С. 42–50.
10. *Попков К. А.* О проверяющих тестах размыкания для контактных схем // Дискретная математика. 2017. Т. 29. Вып. 4. С. 66–86.
11. *Попков К. А.* О диагностических тестах размыкания для контактных схем // Дискретная математика. 2019. Т. 31. Вып. 2. С. 124–143.
12. *Попков К. А.* Короткие единичные проверяющие тесты для контактных схем при обрывах и замыканиях контактов // Интеллектуальные системы. Теория и приложения. 2019. Т. 23. Вып. 3. С. 97–130.
13. *Редькин Н. П.* О диагностических тестах для контактных схем // Вестник Московского университета. Серия 1. Математика. Механика. 2019. № 2. С. 35–37.
14. *Попков К. А.* О полных диагностических тестах для контактных схем при обрывах и/или замыканиях контактов // Изв. вузов. Поволжский регион. Физико-математические науки. 2019. № 3 (51). С. 3–24.
15. *Попков К. А.* Короткие тесты замыкания для контактных схем // Математические заметки. 2020. Т. 107. Вып. 4. С. 591–603.
16. *Попков К. А.* Оценки функций Шеннона длин тестов замыкания для контактных схем // Дискретная математика. 2020. Т. 32. Вып. 3. С. 49–67.
17. *Редькин Н. П.* Об одной математической модели неисправностей контактных схем // Вестник Московского университета. Серия 1. Математика. Механика. 1993. № 1. С. 42–49.
18. *Редькин Н. П.* Единичные тесты для связных неисправностей контактных схем // Вестник Московского университета. Серия 1. Математика. Механика. 1993. № 2. С. 20–27.

REFERENCES

1. *Lupanov O. B.* Asimptoticheskie otsenki slozhnosti upravlyayushchikh sistem. [Asymptotic Bounds of the Complexity of Control Systems]. Moscow, MSU Publ., 1984. 138 p. (in Russian)
2. *Chegis I. A. and Yablonskiy S. V.* Logicheskie sposoby kontrolya raboty elektricheskikh skhem [Logical ways of monitoring the operation of electrical circuits]. Trudy MIAN, 1958, vol. 51, pp. 270–360. (in Russian)
3. *Yablonskiy S. V.* Nadezhnost' i kontrol' upravlyayushchikh sistem [Reliability and verification of control systems]. Materialy Vsesoyuznogo seminara po diskretnoy matematike i ee prilozheniyam (Moscow, 31 Jan.–2 Feb. 1984). Moscow, MSU Publ., 1986, pp. 7–12. (in Russian)
4. *Yablonskiy S. V.* Nekotorye voprosy nadezhnosti i kontrolya upravlyayushchikh sistem [Some questions of reliability and verification of control systems]. Matematicheskie Voprosy Kibernetiki, 1988, iss. 1, pp. 5–25. (in Russian)
5. *Red'kin N. P.* Nadezhnost' i diagnostika skhem [Circuits Reliability and Diagnostics]. Moscow, MSU Publ., 1992. 192 p. (in Russian)
6. *Madatyan Kh. A.* Polnyy test dlya bespovtornykh kontaktnykh skhem [Complete test for non-repetitive contact circuits]. Problemy Kibernetiki, iss. 23. Moscow, Nauka Publ., 1970, pp. 103–118. (in Russian)
7. *Red'kin N. P.* O polnykh proveryayushchikh testakh dlya kontaktnykh skhem [On complete fault detection tests for contact circuits]. Metody Diskretnogo Analiza v Issledovanii Ekstremal'nykh Struktur, iss. 39. Novosibirsk, Math. Inst. Sib. Br. USSR Acad. Sci., 1983, pp. 80–87. (in Russian)
8. *Red'kin N. P.* O proveryayushchikh testakh zamykaniya i razmykaniya [On fault detection tests of closure and opening]. Metody Diskretnogo Analiza v Optimizatsii Upravlyayushchikh Sistem, iss. 40. Novosibirsk, Math. Inst. Sib. Br. USSR Acad. Sci., 1983, pp. 87–99. (in Russian)
9. *Romanov D. S. and Romanova E. Y.* Single fault detection tests for generalized iterative switching circuits. Moscow Univ. Comput. Math. Cybern., 2015, vol. 39, no. 3, pp. 144–152.
10. *Popkov K. A.* On fault detection tests of contact break for contact circuits. Discrete Math. Appl., 2018, vol. 28, no. 6, pp. 369–383.
11. *Popkov K. A.* On diagnostic tests of contact break for contact circuits. Discrete Math. Appl., 2020, vol. 30, no. 2, pp. 103–116.
12. *Popkov K. A.* Korotkie edinichnye proveryayushchie testy dlya kontaktnykh skhem pri obryvakh i zamykaniyakh kontaktov [Short single fault detection tests for contact circuits under breaks and closures of contacts]. Intellektual'nyye Sistemy. Teoriya i Prilozheniya, 2019, vol. 23, no. 3, pp. 97–130. (in Russian)
13. *Red'kin N. P.* Diagnostic tests for contact circuits. Moscow Univ. Math. Bull., 2019, vol. 74, no. 2, pp. 62–64.
14. *Popkov K. A.* O polnykh diagnosticheskikh testakh dlya kontaktnykh skhem pri obryvakh i/ili zamykaniyakh kontaktov [On complete diagnostic tests for contact circuits under breaks and/or closures of contacts]. Izvestiya Vysshikh Uchebnykh Zavedeniy. Povolzhskiy Region. Fiziko-matematicheskiye nauki, 2019, no. 3 (51), pp. 3–24. (in Russian)
15. *Popkov K. A.* Short tests of closures for contact circuits. Math. Notes, 2020, vol. 107, no. 4, pp. 653–662.
16. *Popkov K. A.* Bounds on Shannon functions of lengths of contact closure tests for contact circuits. Discrete Math. Appl., 2021, vol. 31, no. 3, pp. 165–178.

17. *Red'kin N. P.* Ob odnoy matematicheskoy modeli neispravnostey kontaktnykh skhem [On one mathematical model of faults of contact circuits]. Vestnik Moskovskogo Universiteta. Ser. 1. Matematika. Mekhanika, 1993, no. 1, pp. 42–49. (in Russian)

18. *Red'kin N. P.* Edinichnye testy dlya svyaznykh neispravnostey kontaktnykh skhem [Single tests for connected faults of contact circuits]. Vestnik Moskovskogo Universiteta. Ser. 1. Matematika. Mekhanika, 1993, no. 2, pp. 20–27. (in Russian)

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.725 DOI 10.17223/20710410/62/7

АЛГЕБРОГЕОМЕТРИЧЕСКИЕ КОДЫ И ИХ ДЕКОДИРОВАНИЕ НА ОСНОВЕ ПАР, ИСПРАВЛЯЮЩИХ ОШИБКИ[1]

Е. С. Малыгина*, А. А. Кунинец**, В. Л. Раточка**, А. Г. Дупленко**, Д. Я. Нейман**

*МИЭМ НИУ ВШЭ, г. Москва, Россия

**Балтийский федеральный университет им. И. Канта, г. Калининград, Россия

E-mail: emalygina@hse.ru, artkuninets@yandex.ru, willenst@gmail.com, dvplenko@mail.ru, reterior@yandex.ru

Рассматриваются теоретические основы алгебраических кривых и их функциональных полей, необходимые для построения алгеброгеометрических (АГ) кодов, а также пар, исправляющих ошибки, с целью их дальнейшего применения для декодирования кодов. Приведены теория, необходимая для обоснования корректности работы алгоритма декодирования АГ-кодов на основе пар, исправляющих ошибки, и сам алгоритм декодирования. Рассмотрены примеры построения АГ-кодов, ассоциированных с эллиптической кривой, эрмитовой кривой и квартикой Клейна, и явно заданы пары, исправляющие ошибки, для построенных кодов.

Ключевые слова: *алгеброгеометрический код, функциональное поле, дивизор, исправляющие ошибки пары, декодирование алгеброгеометрического кода, эллиптическая кривая, эрмитова кривая, квартика Клейна.*

ALGEBRAIC-GEOMETRY CODES AND DECODING BY ERROR-CORRECTING PAIRS

E. S. Malygina*, A. A. Kuninets**, V. L. Ratochka**, A. G. Duplenko**, D. Y. Neiman**

*HSE, Moscow, Russia

**Immanuel Kant Baltic Federal University, Kaliningrad, Russia

We consider the basic theory of algebraic curves and their function fields necessary for constructing algebraic geometry codes and a pair of codes forming an error-correction pair which is used in a precomputation step of the decoding algorithm for the algebraic geometry codes. Also, we consider the decoding algorithm and give the necessary theory to prove its correctness. As a result, we consider elliptic curves, Hermitian curves and Klein quartics and construct the algebraic geometry codes associated with these families of curves, and also explicitly define the error-correcting pairs for the resulting codes.

Keywords: *algebraic geometry code, function field, divisor, error-correcting pair, decoding of algebraic geometry code, elliptic curve, Hermitian curve, Klein quartic.*

[1]Обзор подготовлен в рамках Программы фундаментальных исследований НИУ ВШЭ; работа второго автора поддержана грантом Российского научного фонда № 22-41-0441.

Введение

В начале 70-х годов XX века российский математик В. Д. Гоппа установил связь между алгебраическими кривыми над конечными полями и кодами, исправляющими ошибки, предложив построить код, используя либо рациональные функции, либо дифференциальные формы на кривых [1]. Считалось, что построенный код обладал хорошими характеристиками, если отношение числа рациональных точек кривой к её роду достаточно велико. Новая связь позволила глубже изучить асимптотику кодов. Так, в то время для анализа параметров $[n, k, d]$-кода $\mathcal{C}$, где n — длина, k — размерность, d — минимальное расстояние, наилучшей нижней границей являлась граница Варшамова — Гилберта

$$R \geqslant 1 - H(\delta),$$

где $R = k/n$ — относительная скорость; $\delta = d/n$ — асимптотическое относительное минимальное расстояние кода $\mathcal{C}$; $H(x) = -(x \log_q x + (1-x)\log_q(1-x))$ — функция энтропии при условии, что код $\mathcal{C}$ определён над конечным полем $\mathbb{F}_q$.

Вскоре после результатов Гоппы в 1982 г. М. Цфасман, С. Влэдуц и Т. Цинк сопоставили последовательности кривых с последовательностями асимптотически хороших кодов, рассматривая модулярные кривые и кривые Шимуры [2]. Они доказали существование последовательностей кодов над конечным полем $\mathbb{F}_q$, где $q = p^2$ или $q = p^4$ для простого p, параметры которых удовлетворяли границе

$$R \geqslant 1 - \delta - \frac{1}{\sqrt{q} - 1}.$$

Для $q \geqslant 49$ граница Цфасмана — Влэдуца — Цинка лучше, чем граница Варшамова — Гилберта, поскольку гарантируемое ею значение относительной скорости больше. Независимо Я. Ихара доказал аналогичный результат [3] для любого конечного поля $\mathbb{F}_q$, где q — квадрат простого числа, а именно:

$$R \geqslant 1 - \delta - A(q)^{-1}.$$

Здесь $A(q) = \limsup\limits_{g \to +\infty} \frac{\max |C(\mathbb{F}_q)|}{g(C)} = \sqrt{q} - 1$; $|C(\mathbb{F}_q)|$ — число $\mathbb{F}_q$-рациональных точек алгебраической кривой C; $g(C)$ — её род.

Полученный Цфасманом, Влэдуцем и Цинком результат стал основополагающим для интенсивного исследования как кривых с большим числом точек, так и ассоциированных с ними АГ-кодов. Так, например, А. Гарсия и Х. Штихтенот получили оптимальные последовательности кривых, для которых отношение числа точек к роду достигает границы Дринфельда — Влэдуца [4]. Ещё одно направление исследований АГ-кодов касается разработки полиномиальных алгоритмов декодирования, исправляющих до половины конструктивного расстояния и даже более ошибок.

Отметим, что многие свойства АГ-коды унаследовали из свойств обобщённых кодов Рида — Соломона, которые, в свою очередь, можно рассматривать как АГ-коды на проективной прямой. Однако ещё одной мотивацией исследовать коды, ассоциированные с кривыми больших родов, стал следующий факт: длина кода Рида — Соломона, определённого над заданным конечным полем $\mathbb{F}_q$, не превышает $q+1$, в то время как можно построить АГ-код произвольной длины над заданным фиксированным полем $\mathbb{F}_q$. Кроме того, к интересным свойствам АГ-кодов, которые делают их пригодными для очень широкого спектра приложений, можно отнести следующие. Во-первых, АГ-коды

можно построить явно, во-вторых, для АГ-кодов существуют эффективные алгоритмы декодирования, в-третьих, для большинства семейств АГ-кодов минимальное расстояние находится достаточно близко к своей верхней границе — границе Синглтона, в-четвёртых, дуальный к АГ-коду код также является АГ-кодом, в-пятых, квадрат АГ-кода содержится в исходном АГ-коде, а зачастую совпадает с ним. АГ-коды находят своё применение в таких прикладных областях, как криптография с открытым ключом, теория алгебраической сложности, разделение секрета, а в последнее время и в постквантовой криптографии.

Целью настоящего обзора является представление базовой теории функциональных полей, позволяющей описать как теоретическое, так и практическое построение АГ-кодов, а также обзор алгоритма декодирования на основе пар, исправляющих ошибки. Рассмотрены три семейства кривых — эллиптические и эрмитовы кривые, а также квартика Клейна, для которых построены АГ-коды. Для самих кодов построены пары, исправляющие ошибки, необходимые для входных параметров алгоритма декодирования.

1. Предварительные сведения из теории алгебраических кривых

Будем считать, что $\mathbb{F}_q$ — конечное поле, содержащее q элементов; $\mathbb{A}^n$ — аффинное пространство над $\mathbb{F}_q$ размерности n.

Определение 1. *n-Мерное проективное пространство над конечным полем $\mathbb{F}_q$*, которое будем обозначать $\mathbb{P}^n(\mathbb{F}_q)$ или кратко $\mathbb{P}^n$, состоит из классов эквивалентности $(n+1)$-наборов, обозначаемых $P = (x_1 : \ldots : x_{n+1})$, где $x_i \in \mathbb{F}_q$. При этом отношение эквивалентности задано следующим образом:

$$(x_1 : \ldots : x_{n+1}) \sim (y_1 : \ldots : y_{n+1}) \Leftrightarrow x_i = \lambda y_i \text{ для } i = 1, \ldots, n+1 \text{ и некоторого } \lambda \in \mathbb{F}_q^*.$$

Такой класс эквивалентности P называется *точкой проективного пространства* $\mathbb{P}^n$, а $(n+1)$-набор, определяющий точку P, называется её *однородными координатами*.

Отметим, что существует естественное вложение $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$, такое, что $(x_1, \ldots, x_n) \mapsto$ $\mapsto (x_1 : \ldots : x_n : 1)$. Точки из $\mathbb{P}^n$, для которых $x_{n+1} = 0$, называются *бесконечно удалёнными точками*.

Определение 2. Многочлен $f \in \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ называется *однородным многочленом* степени d, если для любого набора $(x_1, \ldots, x_{n+1}) \in \mathbb{F}_q^{n+1}$ и любого $\lambda \in \mathbb{F}_q^*$ имеет место соотношение

$$f(\lambda x_1, \ldots, \lambda x_{n+1}) = \lambda^d f(x_1, \ldots, x_{n+1}).$$

Если многочлен является однородным, то его множество нулей (корней) определено корректно.

Определение 3. Пусть $S \subseteq \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ — множество однородных многочленов. *Множество нулей многочленов, ассоциированных с S*, обозначим как

$$Z(S) = \{P \in \mathbb{P}^n : f(P) = 0 \text{ для всех } f \in S\}.$$

Подмножество $Y \subseteq \mathbb{P}^n$ назовём *проективным алгебраическим множеством*, если существует множество $S \subseteq \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ однородных многочленов, такое, что $Y = Z(S)$.

Идеалом алгебраического множества Y называется идеал $I(Y)$, порождённый множеством однородных многочленов $f \in \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ так, что $f(P) = 0$ для всех $P \in Y$.

Определение 4. *Проективным многообразием* будем называть неприводимое замкнутое (в смысле топологии Зарисского [5]) подмножество в $\mathbb{P}^n$.

Определение 5. Пусть Y — алгебраическое множество. Определим *координатное кольцо* для Y как фактор-кольцо $\mathbb{F}_q[Y] = \mathbb{F}_q[X_1, \ldots, X_{n+1}]/I(Y)$.

Рассмотрим однородные многочлены $f, g \in \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ одинаковой степени, причём $g \notin I(Y)$, и будем считать, что Y — некоторое многообразие. Дробь $f/g \in \mathbb{F}_q[X_1, \ldots, X_{n+1}]$ называется *рациональной функцией на* Y. Элементы f/g и f'/g' определяют одну и ту же рациональную функцию, если $(fg' - f'g)(P) = 0$ для всех $P \in Y$.

Определение 6. *Полем функций* $\mathbb{F}_q(Y)$ многообразия Y называется поле рациональных функций на Y. Размерность Y над $\mathbb{F}_q$ определяется как степень трансцендентности $\mathbb{F}_q(Y)$.

Таким образом, *проективную кривую, определённую над полем* $\mathbb{F}_q$, можно определить как многообразие размерности один над $\mathbb{F}_q$. Приведём наглядный пример.

Пример 1. В аффинной плоскости над конечным полем $\mathbb{F}_q$ рассмотрим многообразие $\mathcal{X}$, определённое однородным многочленом $Y^2Z - X^3 - Z^3$ степени 3. Обозначим $x = X/Z$ и $y = Y/Z$. Поле функций $\mathbb{F}_q(\mathcal{X})$ состоит их элементов вида f/g, где $f, g \in \mathbb{F}_q[x, y]$. Поскольку y удовлетворяет уравнению $y^2 = x^3 + 1$, то степень трансцендентности $\mathbb{F}_q(\mathcal{X})$ над $\mathbb{F}_q$ равна 1. Таким образом, многообразие $\mathcal{X}$ является кривой.

Поскольку при построении АГ-кода мы используем кривую, определённую над конечным полем, то под проективной кривой $\mathcal{X}/\mathbb{F}_q$ над конечным полем будем понимать проективную кривую $\mathcal{X} \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$, определяемую однородным многочленом с коэффициентами в $\mathbb{F}_q$, где $\overline{\mathbb{F}}_q$ — алгебраическое замыкание $\mathbb{F}_q$. При этом поле рациональных функций кривой $\mathcal{X}$ с коэффициентами из $\mathbb{F}_q$ будем обозначать $\mathbb{F}_q(\mathcal{X})$, оно является полем функций кривой $\mathcal{X}/\mathbb{F}_q$ или её функциональным полем. Множество точек кривой, имеющих координаты в $\mathbb{F}_q$, обозначается $\mathcal{X}(\mathbb{F}_q)$. Такие точки называются $\mathbb{F}_q$-*рациональными* точками кривой $\mathcal{X}$.

2. Предварительные сведения из теории функциональных полей

Существует альтернативное определение функционального поля без непосредственной привязки к кривой.

Определение 7. *Алгебраическим функциональным полем* $F/\mathbb{F}_q$ *от одной переменной* называется расширение F поля $\mathbb{F}_q$, такое, что F является конечным алгебраическим расширением поля $\mathbb{F}_q(x)$ для некоторого элемента $x \in F$, являющегося трансцендентным над $\mathbb{F}_q$.

В действительности любое функциональное поле F от n переменных представляет собой поле дробей $\mathrm{Frac}\big(\mathbb{F}_q[x_1, x_2, \ldots, x_n]/f(x_1, x_2, \ldots, x_n)\big)$, числители и знаменатели которых являются многочленами от переменных $x_1, x_2, \ldots, x_n$ с коэффициентами в $\mathbb{F}_q$ с учётом редукции по модулю $f(x_1, x_2, \ldots, x_n)$, где $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ — абсолютно неприводимый многочлен.

Согласно сказанному, далее будем ассоциировать с любой кривой $\mathcal{X}/\mathbb{F}_q$, заданной многочленом $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$, её поле функций (функциональное поле) $F = \mathbb{F}_q(\mathcal{X})$ и дадим ряд базовых определений теории функциональных полей, необходимых для построения математических объектов, которые нужны для определения и построения АГ-кода.

Определение 8. Определим *дискретное нормирование функциональъного поля* $F/\mathbb{F}_q$ как функцию

$$v : F \to \mathbb{Z} \cup \{\infty\},$$

обладающую следующими свойствами:

— $v(x) = \infty \Leftrightarrow x = 0$;
— $v(xy) = v(x) + v(y)$ для всех $x, y \in F$;
— $v(x + y) \geqslant \min\{v(x), v(y)\}$ для всех $x, y \in F$;
— существует $x \in F$, такой, что $v(x) = 1$;
— $v(\alpha) = 0$ для всех $\alpha \in F^*$.

Определение 9. *Кольцом нормирования* функционального поля $F/\mathbb{F}_q$ называется кольцо $\mathcal{O} \subseteq F$, такое, что $\mathbb{F}_q \subsetneqq \mathcal{O} \subsetneqq F$ и для всякого $f \in F$ либо $f \in \mathcal{O}$, либо $f^{-1} \in \mathcal{O}$.

Отметим, что *точкой* функционального поля $F/\mathbb{F}_q$ является максимальный идеал некоторого кольца нормирования $\mathcal{O}$ этого поля. Таким образом, если $\mathcal{O}$ — кольцо нормирования поля $F/\mathbb{F}_q$ и P — его максимальный идеал, то $\mathcal{O}$ единственным образом определяется с помощью P, а именно: $\mathcal{O} = \{f \in F : f^{-1} \notin P\}$. Поэтому далее вместо $\mathcal{O}$ будем писать $\mathcal{O}_P$, а все точки функционального поля $F/\mathbb{F}_q$ будем обозначать $\mathbb{P}_F$.

Согласно свойствам, максимальный идеал P кольца нормирования $\mathcal{O}_P$ является главным, т. е. $P = t_p\mathcal{O}_P$. При этом элемент t_P называется *локальным* или *униформизующим параметром.*

С каждой точкой $P \in \mathbb{P}_F$ ассоциируем дискретное нормирование следущим образом. Всякий элемент $f \in F$ имеет единственное представление $f = t_P^n u$, где $u \in \mathcal{O}_P^\times = \mathcal{O}_P \setminus \{0\}$ и $n \in \mathbb{Z}$. Определим действие дискретного нормирования на элементы функционального поля F следующим образом:

$$v_P(f) = n \quad \text{и} \quad v_P(0) = \infty.$$

Функция v_P удовлетворяет всем свойствам определения 8.

Определение 10. Будем говорить, что точка P является *нулём* функции f тогда и только тогда, когда $v_P(f) > 0$, и является *полюсом* функции f тогда и только тогда, когда $v_P(f) < 0$.

Определение 11. Множество точек $\mathbb{P}_F$ порождает абелеву группу $\mathcal{D}_F$, называемую *группой дивизоров* поля $F/\mathbb{F}_q$. Элемент группы $\mathcal{D}_F$ называется *дивизором* функционального поля $F/\mathbb{F}_q$ и представляет собой формальную сумму точек

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

где $n_P \in \mathbb{Z}$ и почти все $n_P = 0$.

Носителем дивизора D является множество

$$\operatorname{supp}(D) = \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Для точки $P \in \mathbb{P}_F$ и дивизора D определим *нормирование дивизора в точке* P как $v_P(D) = n_P$. Таким образом, мы можем перезаписать дивизор следующим образом:

$$D = \sum_{P \in \operatorname{supp}(D)} v_P(D)\, P.$$

Отметим, что в группе $\mathcal{D}_F$ определено частичное упорядочивание. Будем считать, что $D_1 \leqslant D_2$ тогда и только тогда, когда $v_P(D_1) \leqslant v_P(D_2)$ для всех $P \in \mathbb{P}_F$.

Определим также *степень дивизора*

$$\deg(D) = \sum_{P \in \mathbb{P}_F} v_P(D) \deg(P),$$

где $\deg(P) = [\mathcal{O}_P/P : \mathbb{F}_q]$ — степень расширения поля $\mathcal{O}_P/P$ над $\mathbb{F}_q$, которое изоморфно некоторому конечному полю, являющемуся расширением поля $\mathbb{F}_q$. Точки степени 1 функционального поля $F/\mathbb{F}_q$ соответствуют $\mathbb{F}_q$-рациональным точкам кривой $\mathcal{X}/\mathbb{F}_q$.

Определение 12. Пусть $f \in F \setminus \{0\}$. Обозначим через Z (через N) множество нулей (полюсов) f в $\mathbb{P}_F$. Тогда для функции f определим её
дивизор нулей:

$$(f)_0 = \sum_{P \in Z} v_P(f)\, P;$$

дивизор полюсов:

$$(f)_\infty = \sum_{P \in N} (-v_P(f))\, P;$$

главный дивизор:

$$(f) = (f)_0 - (f)_\infty.$$

Главную роль в определении АГ-кода играет пространство Римана — Роха:

Определение 13. *Пространством Римана — Роха, ассоциированным с дивизором* $D \in \mathcal{D}_F$, называется множество функций вида

$$\mathscr{L}(D) = \{f \in F : (f) \geqslant -D\} \cup \{0\}.$$

Отметим, что $\mathscr{L}(D)$ является конечномерным векторным пространством над $\mathbb{F}_q$, а целое число $\dim(D) = \dim \mathscr{L}(D)$ называется *размерностью дивизора* D.

В силу изоморфизма $\mathbb{F}_q(\mathcal{X}) \cong F/\mathbb{F}_q$ род алгебраической кривой совпадает с родом её поля функций.

Определение 14. *Род функционального поля* F/K определён как

$$g = \max\{\deg(D) - \dim(D) + 1 : D \in \mathcal{D}_F\}.$$

3. АГ-коды

Покажем, как задаётся код, ассоциированный с функциональным полем алгебраической кривой. Такие коды, как уже сказано, называются геометрическими кодами Гоппы или АГ-кодами.

Зафиксируем следующие обозначения:

— $F/\mathbb{F}_p$ — алгебраическое функциональное поле рода g;
— $P_1, P_2, \ldots, P_n$ — попарно различные точки поля $F/\mathbb{F}_p$ степени один;
— $D = P_1 + \ldots + P_n$ — дивизор $\mathcal{D}_F$;
— $G \in \mathcal{D}_F$ — такой дивизор в $\mathcal{D}_F$, что $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \varnothing$.

Определение 15. АГ-код $\mathcal{C}_{\mathscr{L}}(D, G)$, ассоциированный с дивизорами D и G, определён следующим образом:

$$\mathcal{C}_{\mathscr{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathscr{L}(G)\} \subseteq \mathbb{F}_p^n.$$

Отметим, что всякий код $\mathcal{C}_{\mathscr{L}}(D,G)$ можно охарактеризовать параметрами $[n,k,d]$, где n — длина кода (число точек в записи дивизор D); k — размерность кода (размерность пространства Римана — Роха $\mathscr{L}(G)$ или $\dim(G)$); d — минимальное расстояние кода (минимальное число отличных от нуля позиций в кодовых словах).

Согласно [6, Theorem 2.2.2], АГ-код $\mathcal{C}_{\mathscr{L}}(D,G)$ является $[n,k,d]$-кодом, чьи параметры удовлетворяют следующим условиям:

$$k = \dim(G) - \dim(G-D), \quad d \geqslant n - \deg(G). \tag{1}$$

Утверждение 1 [6, Corollary 2.2.3]. Если $\deg(G) < n$, то:
- $\mathcal{C}_{\mathscr{L}}(D,G)$ является $[n,k,d]$-кодом, где $d \geqslant n-\deg(G)$ и $k = \dim(G) \geqslant \deg(G)+1-g$;
- если в дополнение $\deg(G) > 2g-2$, то $k = \deg(G)+1-g$;
- если $\{f_1,\ldots,f_k\}$ — базис пространства $\mathscr{L}(G)$, то матрица

$$\mathbf{G} = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{pmatrix} \in \mathbb{F}_p^{k\times n}$$

является порождающей матрицей кода $\mathcal{C}_{\mathscr{L}}(D,G)$.

Из общей теории кодирования отметим, что $\mathcal{C}_{\mathscr{L}}(D,G) = \{x\mathbf{G} : x \in \mathbb{F}_p^k\}$ и проверочная матрица кода $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$ удовлетворяет условию $\mathbf{H}c^{\mathrm{T}} = 0$, где $c \in \mathcal{C}_{\mathscr{L}}(D,G)$.

Важным объектом в теории кодирования является понятие дуального кода к коду $\mathcal{C}_{\mathscr{L}}(D,G)$. В действительности его структура сложнее, нежели $\mathcal{C}_{\mathscr{L}}(D,G)$, поскольку сопряжена с пространством дифференциалов. Для более детального ознакомления стоит обратиться к [6]. Здесь мы постараемся упростить понимание дуального АГ-кода, не вдаваясь в такие понятия, как пространство дифференциалов, дифференциальный дивизор, адели и вычеты, а опираясь исключительно на свойство дуальности.

Далее дуальный код будем обозначать как

$$\mathcal{C}_{\mathscr{L}}(D,G)^{\perp} = \{x \in \mathbb{F}_p^n : \langle x,c\rangle = 0 \text{ для всех } c \in \mathcal{C}_{\mathscr{L}}(D,G)\},$$

где $\langle x,c\rangle = \sum\limits_{i=1}^{n} x_1c_1 + \ldots, x_nc_n$. Очевидно, что тогда проверочная матрица $\mathbf{H}$ кода $\mathcal{C}_{\mathscr{L}}(D,G)$ является порождающей матрицей кода $\mathcal{C}_{\mathscr{L}}(D,G)^{\perp}$. Соответственно, представляя порождающую матрицу в систематической форме $\mathbf{G} = (I_k|A)$, где I_k — единичная матрица размерности $k\times k$ и $A \in \mathbb{F}_p^{k\times(n-k)}$, мы без труда можем привести проверочную матрицу к систематическому виду $\mathbf{H} = (-A^{\mathrm{T}}|I_{n-k})$, где I_{n-k} — единичная матрица размерности $(n-k)\times(n-k)$, и как следствие построить дуальный код. Кроме того, будем считать, что код $\mathcal{C}$ является самодуальным, если $\mathcal{C} = \mathcal{C}^{\perp}$.

Согласно [6, Theorem 2.2.7], если $2g-2 < \deg(G) < n$, то АГ-код $\mathcal{C}_{\mathscr{L}}(D,G)^{\perp}$ является $[n,k',d']$-кодом, чьи параметры удовлетворяют следующим условиям:

$$k' = n+g-1-\deg(G),\ d' \geqslant \deg(G) - (2g-2).$$

Чем больше минимальное расстояние кода, тем большее число ошибок можно исправить. К сожалению, в отличие от длины и размерности кода, которые можно вычислить явно, в общем случае минимальное расстояние имеет лишь нижнюю границу (как указано выше) и верхнюю границу — границу Синглтона:

$$d \leqslant n+1-k.$$

Очевидно, что меньшая размерность даёт более высокую верхнюю границу для минимального расстояния кода. Однако одним из необходимых свойств кода является его относительно высокая размерность, поскольку для заданного кодового слова $[n, k, d]$-кода лишь k координат содержат фактическую информацию. Другие $n - k$ координат используются для создания избыточности и возможности исправления ошибок. Если k велико, то значение k/n, отвечающее за скорость передачи информации, также высоко, что означает эффективность используемого кода. Учитывая верхнюю границу Синглтона, мы можем не получить большого значения минимального расстояния, однако всегда существует компромисс между скоростью передачи информации и способностью кода исправлять ошибки.

Как показано выше, минимальные расстояния кодов $\mathcal{C}_{\mathscr{L}}(D, G)$ и $\mathcal{C}_{\mathscr{L}}(D, G)^{\perp}$ имеют нижние границы

$$\delta = n - \deg(G) \quad \text{и} \quad \delta' = \deg(G) - 2g + 2,$$

которые называются *конструктивным минимальным расстоянием* соответствующего кода и обеспечивают исправление по крайней мере $\lfloor (\delta(\delta') - 1)/2 \rfloor$ ошибок. В общем случае рассматриваемые коды могу исправить не больше $\lfloor (d(d') - 1)/2 \rfloor$ ошибок, где d и d' — минимальные расстояния кодов $\mathcal{C}_{\mathscr{L}}(D, G)$ и $\mathcal{C}_{\mathscr{L}}(D, G)^{\perp}$ соответственно.

4. Декодирование на основе пар, исправляющих ошибки

Одно из важнейших условий применимости того или иного класса кодов в криптографии — существование эффективного алгоритма декодирования для него. Разумеется, декодировать АГ-коды возможно, используя все базовые алгоритмы, справедливые для линейных кодов, однако условию эффективности они не удовлетворяют. Существует ряд модификаций алгоритма декодирования Берлекэмпа — Мэсси для АГ-кодов. В [7] описывается списочный алгоритм декодирования, работающий за полиномиальное время для любого АГ-кода $\mathcal{C}$ с параметрами $[n, k, d]$ при $\mathrm{wt}(e) < n - \sqrt{n(n-d)}$, где $\mathrm{wt}(\cdot)$ обозначает вес вектора. Однако наиболее эффективным для АГ-кодов в настоящее время является алгоритм декодирования на основе пар, исправляющих ошибки. Он представляет также большой интерес с криптографической точки зрения, поскольку в [8] предложена атака на произвольный АГ-код, в основе которой лежат пары, исправляющие ошибки. Сложность детерминированной атаки равна $\mathcal{O}(n^4 log(n))$, однако применение вероятностного подхода позволяет уменьшить сложность до $\mathcal{O}(n^{3+\epsilon}\log(n))$. Таким образом, пары, исправляющие ошибки, играют важную роль в криптоанализе примитивов, построенных с использованием АГ-кодов.

4.1. Пары, исправляющие ошибки

Идея использовать пару линейных кодов для декодирования появилась ещё в 90-х годах XX века и предложена в [9]. Введём ряд обозначений.

Определение 16. Пусть $a, b \in \mathbb{F}_q^n$. *Произведение Шура двух векторов* определяется как произведение их соответствующих координат, а именно:

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n),$$
$$(a_1, \ldots, a_n)^i = (a_1^i, \ldots, a_n^i).$$

Аналогично определению 16, введём определение произведения Шура для двух множеств. Пусть $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q^n$, тогда их произведение Шура определяется следующим образом:

$$\mathcal{A} * \mathcal{B} = \{a * b : a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

Определение 17. Пусть $\mathcal{C} \in \mathbb{F}_q^n$ — линейный код. Тогда пара линейных кодов $(\mathcal{A}, \mathcal{B})$, где $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q^n$, называется *парой, исправляющей t ошибок*, для кода $\mathcal{C}$, если выполняются следующие условия:

1) $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$;
2) $k(\mathcal{A}) > t$;
3) $d(\mathcal{B}^\perp) > t$;
4) $d(\mathcal{A}) + d(\mathcal{C}) > n$.

Здесь $k(\cdot)$ и $d(\cdot)$ — размерность и минимальное расстояние соответствующего кода.

Замечание 1. Пункт 4 в определении 17 может быть заменён эквивалентными утверждениями:

— $d(\mathcal{A}^\perp) > 1$;
— $d(\mathcal{A}) > n - 2t$.

В обозначениях определения 17 $d(\mathcal{C}) \geqslant 2t + 1$. На практике вместо условия 1 часто ищут коды $\mathcal{A}, \mathcal{B}$, такие, что $\mathcal{A} * \mathcal{C} \subset \mathcal{B}^\perp$. Это позволяет сократить вычисления для условия 3.

В [10, 11] описаны условия существования кодов $\mathcal{A}$ и $\mathcal{B}$, составляющих пару, исправляющую t ошибок; в [11] приведены также примеры существования пар для нескольких семейств кодов.

Утверждение 2. Пусть F — функциональное поле рода g; $D = P_1 + \ldots + P_n$ — дивизор, носитель которого состоит из точек степени один поля F; G, H — дивизоры, такие, что $\deg(G) \geqslant 2g$, $\deg(H) \geqslant 2g + 1$ и $\operatorname{supp}(D) \cap \{\operatorname{supp}(G), \operatorname{supp}(H)\} = \varnothing$. Тогда

$$\mathcal{C}_{\mathscr{L}}(D, G) * \mathcal{C}_{\mathscr{L}}(D, H) = \mathcal{C}_{\mathscr{L}}(D, G + H).$$

Из утверждения 2 следует, что пара $(\mathcal{A}, \mathcal{B})$, где $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H)$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}(D, G - H)$, $\deg(G) > \deg(H) \geqslant t + g$, $\deg(G - H) > t + 2g - 2$, является парой, исправляющей t ошибок, для кода $\mathcal{C}_{\mathscr{L}}(D, G)^\perp$.

Если для АГ-кода $\mathcal{C}_{\mathscr{L}}(D, G)$ выполняется условие $n > \deg(G) > 2g - 2$, то конструктивное расстояние дуального к нему кода $\delta(\mathcal{C}_{\mathscr{L}}(D, G))^\perp = \deg(G) + 2 - 2g$ и всегда найдётся пара кодов $(\mathcal{A}, \mathcal{B})$, исправляющая $\lfloor (\delta - g - 1)/2 \rfloor$ ошибок.

Рассмотрим размерность кода $\mathcal{A} * \mathcal{B}$, для этого введём понятие стабилизатора.

Определение 18. Пусть $\mathcal{C} \subseteq \mathbb{F}_q^n$. *Стабилизатор кода* $\mathcal{C}$ определяется следующим образом:

$$\operatorname{stab}(\mathcal{C}) = \left\{ x \in \mathbb{F}_q^n : \forall c \in \mathcal{C} (x * c \in \mathcal{C}) \right\}.$$

Теорема 1 [12, Theorem 2.11]. Пусть $\mathcal{A}, \mathcal{B}$ — линейные коды. Тогда

$$k(\mathcal{A} * \mathcal{B}) \geqslant k(\mathcal{A}) + k(\mathcal{B}) - k(\operatorname{stab}(\mathcal{A} * \mathcal{B})).$$

Линейный код имеет стабилизатор, размерность которого превосходит 1, тогда и только тогда, когда код является прямой суммой двух подкодов $\mathcal{C}_{\mathscr{L}}(D, G)$ и $\mathcal{C}_{\mathscr{L}}(D, G')$ с непересекающимися носителями дивизоров G и G' или порождающая матрица кода имеет нулевой столбец. В противном случае $k(\mathcal{A} * \mathcal{B}) \geqslant k(\mathcal{A}) + k(\mathcal{B}) - 1$.

4.2. Алгоритм декодирования

Далее рассмотрим алгоритм декодирования, предложенный в [9]. Введём ряд обозначений.

Определение 19. Пусть $\mathfrak{I} = \{j_1, \ldots, j_s\} \subset \{1, \ldots, n\}$, $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ и $\mathcal{A} \subseteq \mathbb{F}_q^n$. Тогда:

1) $x_{\mathfrak{I}} = (x_{j_1}, \ldots, x_{j_s})$;
2) $Z(x) = \{i \in \{1, \ldots, n\} : x_i = 0\}$;
3) $Z(\mathcal{A}) = \{i \in \{1, \ldots, n\} : a_i = 0$ для всех$a \in \mathcal{A}\}$;
4) $\mathcal{A}(\mathfrak{I}) = \{a \in \mathcal{A} : a_{\mathfrak{I}} = 0\}$.

Пусть $\mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код с параметрами $[n, k, d]$, $y = c + e$ — принятый вектор, $I_e = \{i : e_i \neq 0\} = \operatorname{supp}(e)$, $(\mathcal{A}, \mathcal{B})$ — пара, исправляющая t ошибок, для кода $\mathcal{C}_{\mathscr{L}}(D, G)$.

Алгоритм декодирования можно разделить на две части:

1) поиск множества $\mathfrak{I} \supseteq I_e$, где $|I_e| = \operatorname{wt}(e) \leqslant t$;
2) восстановление ненулевых позиций вектора ошибки e.

На первом шаге необходимо найти множество, равное или содержащее в себе позиции ошибок в полученном слове. Сложность этой процедуры заключается в незнании элементов множества I_e. Для нахождения $\mathfrak{I}$ используют пару кодов $(\mathcal{A}, \mathcal{B})$.

Утверждение 3 [9, Theorem 2.14]. Если $k(\mathcal{A}) > t$ и $|I_e| \leqslant t$, то $\mathcal{A}(I_e) \neq \varnothing$.

Рассмотрим множество $M = \{a \in \mathcal{A} : \langle a * y, b\rangle = 0$ для всех $b \in \mathcal{B}\}$, являющееся ядром отображения ϕ: $a \mapsto (b \mapsto \langle a * y, b\rangle)$.

Утверждение 4 [9, Proposition 2.9]. Пусть $y = c + e$ — принятый вектор, $I_e = \operatorname{supp}(e)$, $\mathcal{C} \subseteq \mathbb{F}_q^n$ — линейный код. Если $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^{\perp}$, то

1) $\mathcal{A}(I_e) \subseteq M \subseteq \mathcal{A}$;
2) если $d(\mathcal{B}^{\perp}) > t$, то $\mathcal{A}(I_e) = M$.

Если пара линейных кодов $(\mathcal{A}, \mathcal{B})$ удовлетворяет свойствам 1 и 2 определения 17, то множество $Z(M)$ не является тривиальным и содержит I_e. Разумеется, на практике не обязательно брать в качестве $\mathfrak{I}$ именно $Z(M)$. Это не оптимально ввиду большой вычислительной сложности.

Замечание 2. Пусть $a \in M$ и $M = \mathcal{A}(I_e)$. Тогда $I_e \subseteq Z(a)$. Следовательно, в качестве множества $\mathfrak{I}$ можно использовать $\mathfrak{I} = Z(a)$.

Замечание 3. Нахождение множества $M = \{a \in \mathcal{A} : \langle a * y, b\rangle = 0$ для всех $b \in \mathcal{B}\}$ сводится к вычислению левого ядра матрицы, составленной из образов базисных векторов кода $\mathcal{A}$, полученных применением отображения ϕ: $a \mapsto (b \mapsto \langle a * y, b\rangle)$, что эквивалентно вычислению правого ядра матрицы линейного отображения ϕ.

На втором шаге необходимо решить систему уравнений. Пусть $\mathbf{H}$ — проверочная матрица, имеющая n столбцов, $\mathfrak{I} = Z(a)$ — множество, вычисленное на шаге 1. Тогда $\mathbf{H}_{\mathfrak{I}}$ — подматрица, чьи столбцы проиндексированы элементами множества $\mathfrak{I}$, и ненулевые позиции вектора e можно найти, решив следующую систему:

$$\mathbf{H}_{\mathfrak{I}} u^{\mathrm{T}} = \mathbf{H} y^{\mathrm{T}}. \tag{2}$$

Отметим, что решение системы (2) в общем случае не единственно.

Теорема 2. Пусть для пары кодов $(\mathcal{A}, \mathcal{B})$ выполняются условия утверждения 4. Если $d(\mathcal{A}) + d(\mathcal{C}) > n$, $k(\mathcal{A}) > t$ и $\mathfrak{I} = Z(a)$, то $|\mathfrak{I}| < d(\mathcal{C})$ и существует не более одного решения системы (2).

Доказательство. Пусть $I_e \subseteq \mathfrak{I} = Z(a), a \in M$, $|I_e| = t$ и $y = c + e$ — полученный вектор. Определим отображение

$$R_{\mathfrak{I}} : \begin{cases} \mathbb{F}_q^t \to \mathbb{F}_q^n, \\ R_{\mathfrak{I}}(x_{\mathfrak{I}}) = (x_1, \ldots, x_n) \in \mathbb{F}_p^n, x_i = 0, \text{если } i \notin \mathfrak{I}, \text{ и } x_i = x_{\mathfrak{I}_i}, \text{если } i \in \mathfrak{I}. \end{cases}$$

Очевидно, что $\mathbf{H}_\mathfrak{J} e_\mathfrak{J}^{\mathrm{T}} = \mathbf{H} \cdot R_\mathfrak{J}(e_\mathfrak{J})^{\mathrm{T}} = \mathbf{H}e^{\mathrm{T}} = \mathbf{H}y^{\mathrm{T}}$. Таким образом, система (2) имеет решение $e_\mathfrak{J}^{\mathrm{T}}$.

Теперь докажем единственность решения при $d(\mathcal{A}) + d(\mathcal{C}) > n$ и $k(\mathcal{A}) > t$. Если нашлось ещё одно решение системы, например $x_\mathfrak{J}^{\mathrm{T}}$, то

$$\mathbf{H}\left(R_\mathfrak{J}(x_\mathfrak{J})\right)^{\mathrm{T}} = \mathbf{H}_\mathfrak{J} x_\mathfrak{J}^{\mathrm{T}} = \mathbf{H}\left(R_\mathfrak{J}(e_\mathfrak{J})\right)^{\mathrm{T}} = \mathbf{H}e^{T} = \mathbf{H}y^{\mathrm{T}}.$$

Следовательно, $\mathbf{H}\left(R_\mathfrak{J}(x_\mathfrak{J}) - e\right)^{\mathrm{T}} = 0$, а также

$$\mathrm{wt}(R_\mathfrak{J}(x_\mathfrak{J}) - e) \leqslant |Z(a)| \leqslant n - d(\mathcal{A}) < d(\mathcal{C}).$$

Получили $R_\mathfrak{J}(x_\mathfrak{J}) - e = 0$, и, таким образом, нетривиальное решение системы единственно. ■

Описанные шаги можно представить в виде алгоритма 1..

Алгоритм 1. Декодирование

Вход: $\mathcal{C}_\mathscr{L}(D, G)$ — АГ-код, $(\mathcal{A}, \mathcal{B})$ — пара, исправляющая t ошибок, $y = c + e$ — полученный вектор с ошибкой.

Выход: $e_\mathfrak{J}$, c.

1: Вычислить $M = \{a \in \mathcal{A} : \langle a * y, b\rangle = 0 \text{ для всех } b \in \mathcal{B}\}$.
2: **Если** $M = \varnothing$, **то**
3: перейти на шаг 11.
4: Положить $a := \mathrm{random}(x)$, $x \in M$.
5: Вычислить $\mathfrak{J} = Z(a)$.
6: Построить матрицу $\mathbf{H}_\mathfrak{J}$.
7: Решить систему уравнений $\mathbf{H}_\mathfrak{J} u^{\mathrm{T}} = \mathbf{H}y^{\mathrm{T}}$ относительно u.
8: **Если** $\mathrm{wt}(u) > t$, **то**
9: перейти на шаг 11.
10: **Вернуть** $e_\mathfrak{J} = u$, $c = y - R_\mathfrak{J}(e_\mathfrak{J})$.
11: **Вернуть** «В полученном векторе более t ошибок.»

Замечание 4. На шагах 1 и 2 необходимо вычислить ядро M отображения ϕ, а также $Z(a)$, где $a \in M$. Далее решается система из максимум n уравнений с n неизвестными. Таким образом, сложность алгоритма равна $\mathcal{O}(n^3)$.

5. Примеры

Рассмотрим ряд примеров построения АГ-кодов, ассоциированных с эллиптической и эрмитовой кривыми, а также с квартикой Клейна. Для каждого построенного кода найдём соответствующую пару, исправляющую ошибки.

5.1. АГ-коды на эллиптических кривых

Определение 20. Алгебраическое функциональное поле $F/\mathbb{F}_q$ называется *эллиптическим*, если выполняются следующие условия:

1) $g(F/\mathbb{F}_q) = 1$;
2) существует дивизор $A \in \mathcal{D}_F$, такой, что $\deg(A) = 1$.

Отметим некоторые факты, касающиеся эллиптических кривых и их функциональных полей. На протяжении всего п. 5.1 под $F = \mathbb{F}_q(x, y)$ будем подразумевать эллиптическое функциональное поле. В зависимости от характеристики базового поля, уравнение функционального поля эллиптической кривой может быть задано следующим образом:

— если $\mathrm{char}\,(\mathbb{F}_q) \neq 2$, то существуют $x, y \in F$, такие, что $F = \mathbb{F}_q(x, y)$ и

$$y^2 = f(x),$$

где $f(x) \in \mathbb{F}_q[x]$ — свободный от квадратов многочлен и $\deg(f) = 3$;

— если $\mathrm{char}\,(\mathbb{F}_q) = 2$, то существуют $x, y \in F$, такие, что $F = \mathbb{F}_q(x, y)$ и

$$y^2 + y = f(x), \quad \text{где } f(x) \in \mathbb{F}_q[x] \text{ и } \deg f = 3,$$

или

$$y^2 + y = x + \frac{1}{ax + b}, \quad \text{где } a, b \in \mathbb{F}_q \text{ и } a \neq 0.$$

Отметим, что $[n, k]$-код, ассоциированный с эллиптическим функциональным полем, является MDS-кодом (достигает границы Синглтона) тогда и только тогда, когда для любого подмножества точек $\{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\} \subseteq \mathrm{supp}(G)$ дивизор вида $P_{i_1} + P_{i_2} + \ldots + P_{i_k} - kP_\infty$ не является главным. Согласно границе Хассе — Вейля, максимальное количество рациональных точек эллиптической кривой $\mathcal{X}$, или точек степени один функционального поля, равно $q + 1 + 2\sqrt{q}$. Таким образом, рассмотрение кривых с числом точек, достигающим границы Хассе — Вейля, позволяет максимально увеличить длину кодового слова.

Исходя из уравнения эллиптического функционального поля, для функций $x, y \in \in \mathbb{F}_q(\mathcal{X})$ можно вычислить соответствующие нормирования

$$-v_{P_\infty}(x) = 2, \quad -v_{P_\infty}(y) = 3 \quad \text{и} \quad -v_{P_\infty}(x^\lambda y^\gamma) = 2\lambda + 3\gamma$$

для некоторых $\lambda, \gamma \in \mathbb{Z}^{>0}$. Соответственно базис пространства Римана — Роха $\mathcal{L}(\alpha P_\infty)$, $\alpha \in \mathbb{Z}^{>0}$, ассоциированного с дивизором, кратным бесконечно удалённой точке, состоит из функций $f = x^\lambda y^\gamma$, где $\lambda \in \mathbb{N}$, $\gamma \in \{0, 1\}$, $2\lambda + 3\gamma \leqslant \alpha$, и имеет вид

$$\{1, x, y, x^2, xy, x^3, x^2y, x^4, x^3y, \ldots\}.$$

Пример 2. Пусть $F = \mathbb{F}_q(x, y)$ — эллиптическое функциональное поле с уравнением $y^2 = x^3 + 7x + 4$ и $q = 17$. Отметим, что $g(F) = 1$. Построим АГ-код, ассоциированный с заданной эллиптической кривой, и найдём пару, исправляющую ошибки, для построенного кода.

Зададим дивизор $D = P_1 + P_2 + \ldots + P_{12}$, где P_i — точки степени один поля F для $i = 1, \ldots, 12$:

$$P_1 = (0, 15),\ P_2 = (0, 2),\ P_3 = (3, 16),\ P_4 = (3, 1),\ P_5 = (15, 13),\ P_6 = (15, 4),$$
$$P_7 = (11, 16),\ P_8 = (11, 1),\ P_9 = (16, 9),\ P_{10} = (16, 8),\ P_{11} = (2, 14),\ P_{12} = (2, 3).$$

Зададим дивизор $G = m \cdot P_\infty$, где P_∞ — полюс функций x и y, и пусть $m = 5$.

Вычислим базис пространства Римана — Роха $\mathscr{L}(G) = \mathscr{L}(5P_\infty)$, необходимый для построения АГ-кода $C_{\mathscr{L}}(D, G)$. Для этого рассмотрим дискретные нормирования функций, являющихся претендентами на базис $\mathscr{L}(G)$, значения которых в точке P_∞ не должны превышать $m = 5$ (табл. 1).

Таблица 1

Значения нормирования	Базис $\mathscr{L}(G)$
$\nu_\infty(1) = 0$	1
$\nu_\infty(x) = 2$	x
$\nu_\infty(y) = 3$	y
$\nu_\infty(x^2) = 4$	x^2
$\nu_\infty(xy) = 5$	xy
$\nu_\infty(x^3) = 6$	—

Запишем порождающую и проверочную матрицы кода $C_{\mathscr{L}}(D, G)$:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 8 & 10 & 0 & 8 & 14 & 8 & 16 \\ 0 & 1 & 0 & 0 & 0 & 9 & 1 & 11 & 4 & 15 & 4 & 13 \\ 0 & 0 & 1 & 0 & 0 & 14 & 7 & 9 & 2 & 16 & 1 & 16 \\ 0 & 0 & 0 & 1 & 0 & 3 & 15 & 13 & 7 & 10 & 12 & 14 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 14 & 14 & 10 & 10 \end{bmatrix},$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 11 & 12 & 4 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 14 & 9 & 8 & 13 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 & 11 & 10 & 0 & 7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 6 & 15 & 8 & 16 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 5 & 13 & 12 & 6 & 14 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 5 & 8 & 0 & 15 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 16 & 11 & 6 & 10 & 7 \end{bmatrix}.$$

Код $\mathcal{C}_{\mathscr{L}}(D, G)$, ассоциированный с определённой выше эллиптической кривой, имеет параметры $[12, 5, 7]$, а его дуальный код $\mathcal{C}_{\mathscr{L}}(D, G)^\perp$ — параметры $[12, 7, 5]$.

Для построения пары, исправляющей ошибки, для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ необходимо определить вспомогательный дивизор

$$H = (t + g)\, P_\infty = 3\, P_\infty,$$

где $t = \lfloor (n - \deg(G) - 1 - g)/2 \rfloor$. Тогда для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ парой, исправляющей $t = 2$ ошибок, является пара кодов $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H)$ и $\mathcal{B} = \mathcal{C}^{\perp}_{\mathscr{L}}(D, G+H)$ с параметрами $[12, 3, 9]$ и $[12, 4, 8]$ соответственно.

5.2. АГ-коды на эрмитовых кривых

Определение 21. Функциональное поле $F = \mathbb{F}_{q^2}(x, y)$, определённое уравнением эрмитовой кривой

$$y^q + y = x^{q+1},$$

будем называть *эрмитовым* функциональным полем.

Отметим некоторые факты, касающиеся эрмитовых функциональных полей. На протяжении всего п. 5.2 под $F = \mathbb{F}_{q^2}(x, y)$ будем подразумевать эрмитово функциональное поле, для которого справедливо:

— $g(F) = q(q-1)/2$;

— F имеет $q^3 + 1$ точек степени один над полем $\mathbb{F}_{q^2}$ следующего вида:

1) бесконечно удалённая точка Q_∞ — общий полюс функций x и y;
2) для каждого $\alpha \in \mathbb{F}_{q^2}$ существует q элементов $\beta \in \mathbb{F}_{q^2}$, таких, что $\beta^q + \beta = \alpha^{q+1}$; и для всех таких пар (α, β) существует единственная точка $P_{\alpha,\beta}$ степени один, где $x(P_{\alpha,\beta}) = \alpha$ и $y(P_{\alpha,\beta}) = \beta$;

— для некоторого $r \geqslant 0$ функции вида $x^i y^j$, где $0 \leqslant i, 0 \leqslant j \leqslant q-1$ и $iq + j(q+1) \leqslant r$, образуют базис пространства Римана — Роха $\mathscr{L}(rQ_\infty)$.

Определение 22. Для $r \in \mathbb{Z}$ определим *эрмитов АГ-код*

$$\mathcal{C}_r = \mathcal{C}_{\mathscr{L}}(D, rQ_\infty), \quad D = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta},$$

где дивизор D является суммой всех точек первой степени (кроме точки Q_∞) эрмитова функционального поля $F/\mathbb{F}_{q^2}$.

Семейство эрмитовых кодов представляет особый интерес, поскольку в определённых случаях наряду с длиной и размерностью можно явно вычислить минимальное расстояние таких кодов. Над полем $\mathbb{F}_{q^2}$ эрмитов код имеет длину $n = q^3$.

Для некоторого $r \leqslant s$ имеем $\mathcal{C}_r \subseteq \mathcal{C}_s$. Это включение следует из включения соответствующих пространст Римана — Роха $\mathscr{L}(D, rQ_\infty) \subseteq \mathscr{L}(D, sQ_\infty)$. Если $r \leqslant 0$, то $\mathscr{L}(rQ_\infty) = 0$ и $\mathcal{C}_r = 0$. Если $r > q^3 + q^2 - q - 2 = q^3 + (2g-2)$, то, учитывая (1), имеем

$$k(\mathcal{C}_r) = \dim(rQ_\infty) - \dim(rQ_\infty - D) = (r + 1 - g) - (r - q^3 + 1 - g) = q^3 = n$$

и, следовательно, $\mathcal{C}_r = F_{q^2}^n$. Согласно [6], для $0 \leqslant r \leqslant q^3 + q^2 - q - 2$ справедливо следующее

Утверждение 5. Пусть $\mathcal{C}_r$ — эрмитов код и $0 \leqslant r \leqslant q^3 + q^2 - q - 2$. Тогда:

— Дуальным к коду $\mathcal{C}_r$ является

$$\mathcal{C}_r{}^\perp = \mathcal{C}_{q^3+q^2-q-2-r}.$$

Код $\mathcal{C}_r$ является самодуальным, если $r = (q^3 + q^2 - q - 2)/2$ (что, на самом деле, возможно только в случае, если q является степенью 2).

— Размерность $\mathcal{C}_r$ определяется следующим образом:

$$k(\mathcal{C}_r) = \begin{cases} |I(r)|, & 0 \leqslant r \leqslant q^3, \\ q^3 - |I(s)|, & q^3 \leqslant r \leqslant q^3 + q^2 - q - 2, \end{cases}$$

где $s = q^3 + q^2 - q - 2 - r$ и $I(r) = \{0 \leqslant n \leqslant r : \exists z \in F \left((z)_\infty = nQ_\infty\right)\}$.
Для $q^2 - q - 2 \leqslant r \leqslant q^3$ имеем

$$k(C_r) = r + 1 - q(q-1)/2.$$

— Минимальное расстояние d кода $\mathcal{C}_r$ удовлетворяет неравенству

$$d(\mathcal{C}_r) \geqslant q^3 - r.$$

Если $0 \leqslant r \leqslant q^3$ и $r, (r^3 - r)$ являются полюсными числами для точки Q_∞ (т. е. существуют функции $f, f' \in F$, такие, что $(f)_\infty = rQ_\infty$ и $(f')_\infty = (r^3 - r)Q_\infty$), то

$$d(\mathcal{C}_r) = q^3 - r.$$

Пример 3. Пусть $F = \mathbb{F}_{q^2}(x, y)$ — функциональное поле эрмитовой кривой с уравнением $y^3 + y = x^4$ и $q = 3$. Зададим дивизор $D = P_1 + P_2 + \ldots + P_{27}$, где P_i — точки первой степени для $i = 1, \ldots, 27$:

$$\begin{array}{lllllll} P_1 = (0,0), & P_2 = (0,a^6), & P_3 = (0,a^2), & P_4 = (a,a^5), & P_5 = (a,a^7), & P_6 = (a,1), \\ P_7 = (a^2,2), & P_8 = (a^2,a), & P_9 = (a^2,a^3), & P_{10} = (a^3,a^5), & P_{11} = (a^3,a^7), & P_{12} = (a^3,1), \\ P_{13} = (2,2), & P_{14} = (2,a), & P_{15} = (2,a^3), & P_{16} = (a^5,a^5), & P_{17} = (a^5,a^7), & P_{18} = (a^5,1), \\ P_{19} = (a^6,2), & P_{20} = (a^6,a), & P_{21} = (a^6,a^3), & P_{22} = (a^7,a^5), & P_{23} = (a^7,a^7), & P_{24} = (a^7,1), \\ P_{25} = (1,2), & P_{26} = (1,a), & P_{27} = (1,a^3). & & & \end{array}$$

Здесь a — корень примитивного над $\mathbb{F}_q$ многочлена $f(x) = x^2 + 2x + 2$.

Зададим дивизор $G = r \cdot Q_\infty$, где Q_∞ — общий полюс функций x и y поля F и $r = 17$.

Вычислим базис пространства Римана — Роха $\mathscr{L}(G) = \mathscr{L}(17Q_\infty)$, необходимый для построения АГ-кода $\mathcal{C}_\mathscr{L}(D, G)$. Для этого рассмотрим дискретные нормирования функций, являющихся претендентами на базис $\mathscr{L}(G)$, в точке Q_∞, значения которых не должны превышать $r = 17$ (табл. 2).

Таблица 2

Значения нормирования	Базис $\mathscr{L}(G)$
$\nu_\infty(1) = 0$	1
$\nu_\infty(x) = 3$	x
$\nu_\infty(y) = 4$	y
$\nu_\infty(x^2) = 6$	x^2
$\nu_\infty(xy) = 7$	xy
$\nu_\infty(y^2) = 8$	y^2
$\nu_\infty(x^3) = 9$	x^3
$\nu_\infty(x^2y) = 10$	x^2y
$\nu_\infty(xy^2) = 11$	xy^2
$\nu_\infty(x^4) = 12$	x^4
$\nu_\infty(x^3y) = 13$	x^3y
$\nu_\infty(x^2y^2) = 14$	x^2y^2
$\nu_\infty(x^5) = 15$	x^5
$\nu_\infty(x^4y) = 16$	x^4y
$\nu_\infty(x^3y^2) = 17$	x^3y^2
$\nu_\infty(x^6) = 18$	—

Запишем порождающую и проверочную матрицы кода $\mathcal{C}_\mathscr{L}(D, G)$:

$$\mathbf{G} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & 1 & a & a^5 & a & a^7 & 2 & a^3 & 0 & a^3 & a^5 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & a^2 & 0 & 2 & a^3 & a^6 & 0 & 0 & a^5 & 2 & a^6 & a^3 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 & a^3 & a^5 & a^5 & a^2 & a^2 & a^6 & 0 & 1 & a^7 & a^5 & a \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^6 & 0 & 2 & a^3 & 2 & a^3 & 0 & a & a^6 & a & a^7 & 0 & a^7 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^6 & 0 & a & a & a & 0 & a & 1 & a^3 & a^5 & a^7 & a^5 & a^6 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^6 & 0 & a^3 & 2 & 0 & a^3 & 2 & 1 & 2 & a^7 & a^5 & a^3 & a \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^5 & 0 & 1 & a^5 & a^7 & a & 0 & a^6 & a & a & a^6 & a^2 & a^5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & a^5 & 0 & a & a^2 & a^5 & a^6 & a & 0 & 1 & a^2 & a^6 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & a^5 & 0 & a^6 & 2 & a^3 & a^3 & a & a & a^3 & a^2 & 2 & 2 & a^6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a^7 & 0 & 0 & a^7 & 1 & a^5 & a^6 & 2 & a^2 & a & a^2 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & a^7 & 0 & 1 & a^2 & a^6 & a^7 & a^7 & a & a^3 & a^6 & a^5 & a & a^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & a^7 & 0 & 2 & a & a^7 & 0 & 1 & a & a^5 & a^5 & a & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & a^2 & a^6 & a^2 & a & a^7 & a & a^6 & 1 & a^6 & a^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & a^6 & a^2 & a^7 & a & a^2 & a^7 & 0 & a^3 & 1 & a^7 & a^5 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & a^3 & a^3 & a^3 & a & a & a
\end{bmatrix},$$

$$\mathbf{H} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & a^6 & 0 & a^2 & a & 2 & 0 & 0 & a^6 & a^6 & 1 & a^5 & a^2 & 2 & a \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & a^5 & a^3 & a^7 & a^5 & a^5 & 2 & 0 & a^5 & a^7 & a^2 & a & a & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & a^7 & a & a^3 & 1 & 1 & a^7 & 0 & a & a & a^7 & a^3 & 0 & a^7 & a^2 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^7 & 0 & a^7 & 2 & 1 & a^2 & 0 & a^2 & a^5 & a^5 & a^3 & a^7 & a^2 & 2 & a^2 & a^3 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & a^7 & 0 & 1 & a & a^6 & a^7 & a^2 & 0 & 2 & a^6 & a^3 & 0 & a^5 & a^5 & a^5 & a^3 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & a^7 & 0 & a^5 & a^3 & 2 & 2 & a^2 & a^5 & a^7 & a^6 & a & a & a^3 & 1 & a^6 & a^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & a^3 & 0 & 0 & 1 & a^3 & 1 & a & a^2 & 1 & a^7 & a & 0 & 0 & a^5 & 1 & a^6 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & a^3 & 0 & a & a^3 & a & a^2 & a^2 & a^7 & a & 2 & 2 & 1 & a & a^7 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & a^3 & 0 & a^5 & a^2 & a^2 & 0 & a^3 & a^7 & a^3 & a^3 & 1 & a^7 & 0 & a^7 & a & a^3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & a^7 & a^3 & a & 1 & a^6 & a^3 & 1 & a^2 & a & a^5 & 0 & a^3 & 2 & a \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & a^3 & a^7 & a^6 & 1 & a & a & 0 & a^5 & a^3 & a^2 & 1 & a & 2 & a^3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & a^2 & a^2 & a^2 & 1 & 1 & 1 & a^7 & a^7 & a^7 & a^2 & a^2 & a^2
\end{bmatrix}.$$

Код $\mathcal{C}_{\mathscr{L}}(D, G)$, ассоциированный с определённой выше эрмитовой кривой, имеет параметры $[27, 15, 10]$, а его дуальный код $\mathcal{C}_{\mathscr{L}}(D, G)^{\perp}$ — параметры $[27, 12, 13]$.

Для построения пары, исправляющей ошибки, для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ необходимо определить вспомогательный дивизор:

$$H = (t + g)\, Q_\infty = 6\, Q_\infty,$$

где $t = \lfloor (n - \deg(G) - 1 - g)/2 \rfloor$. В нашем случае $g = 3$ и $t = 3$. Тогда для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ парой, исправляющей $t = 3$ ошибки, является пара кодов $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H)$ и $\mathcal{B} = \mathcal{C}^{\perp}_{\mathscr{L}}(D, G + H)$ с параметрами $[27, 4, 21]$ и $[27, 6, 19]$ соответственно.

Для построения пары, исправляющей ошибки, для кода $\mathcal{C}^{\perp}_{\mathscr{L}}(D, G)$ необходимо, чтобы $t = \lfloor (\deg(G) - 3g + 1)/2 \rfloor$. Определим вспомогательный дивизор

$$H' = (t + g)\, Q_\infty = 7\, Q_\infty.$$

Тогда для кода $\mathcal{C}^{\perp}_{\mathscr{L}}(D, G)$ пару, исправляющую 4 ошибки, составляют коды $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H')$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}(D, G - H')$ с параметрами $[27, 5, 20]$ и $[27, 8, 17]$ соответственно.

5.3. АГ-коды на квартике Клейна

Предположим, что $\mathrm{char}\,(\mathbb{F}_q) \neq 7$. Рассмотрим функциональное поле $F = \mathbb{F}_q(z, y)$ квартики Клейна, заданное уравнением

$$z^3 + y^3 z + y = 0. \tag{3}$$

После умножения (3) на y^6, полагая $x = -y^2 z$, можем записать $F = \mathbb{F}_q(x, y)$, где

$$y^7 = \frac{x^3}{1 - x}.$$

Так как $\mathrm{char}\,(\mathbb{F}_q) \neq 7$, функциональное поле квартики Клейна F не является рациональным. Дадим пару определений, чтобы записать основные свойства этого функционального поля.

Определение 23. Пусть $F'/\mathbb{F}_q$ — алгебраическое расширение функционального поля $F/\mathbb{F}_q$.

— Говорят, что *точка $P' \in \mathbb{P}_{F'}$ лежит над точкой $P \in \mathbb{P}_F$*, если $P \subseteq P'$.

— Пусть точка $P' \in \mathbb{P}_{F'}$ лежит над точкой $P \in \mathbb{P}_F$. При этом нормирования в рассматриваемых точках связаны следующим соотношением:

$$v_{p'}(x) = e \cdot v_P(x) \quad \text{для всех } x \in F.$$

Если $e > 1$, то говорят, что *точка P разветвляется.*

Перечислим свойства функционального поля квартики Клейна:

1) $g(F) = 3$;
2) ровно три точки поля $\mathbb{F}_q(x)$ являются точками ветвления в $F/\mathbb{F}_q$, а именно: полюс P_∞ и нуль P_1 функции x, а также нуль P_2 функции $x-1$. Обозначим через Q_∞, Q_1, Q_2 точки, лежащие над P_∞, P_1, P_2 соответственно;
3) точки Q_∞, Q_1 и Q_2 являются точками степени один;
4) отображение
$$\phi : \begin{cases} x \longmapsto \dfrac{x-1}{x}, \\ \\ y \longmapsto \dfrac{-x}{y^3} \end{cases}$$
является автоморфизмом порядка 3 поля $F/\mathbb{F}_q$, который циклично порождает точки Q_∞, Q_1, Q_2, т. е. $\phi(\phi(Q_\infty)) = \phi(Q_1) = Q_2$.

Рассмотрим некоторый подкласс АГ-кодов, ассоциированных с квартикой Клейна, а именно коды, для которых дивизор G определён следующим образом:

$$G = k_0 Q_\infty + k_1 Q_1 + k_2 Q_2 > 0,$$

где $k_i \in \mathbb{N}_0 \setminus \{1,2,3,4\}$, $i = 0,1,2$ ($\mathbb{N}_0 = \{0,1,2,\ldots\}$), и будем считать, что $\deg(G) \geqslant 5$. Тогда по теореме Римана — Роха $\dim(G) = \deg(G) - 2$. Согласно [13], определим базис пространства Римана — Роха $\mathcal{L}(G)$.

Лемма 1. Если $G = k_0 Q_\infty + k_1 Q_1 + k_2 Q_2 > 0$, где $k_i \in \mathbb{N}_0 \setminus \{1,2,3,4\}$, то базис пространства Римана — Роха $\mathcal{L}(G)$ состоит из степеней и произведений следующих элементов:

$$w_1 = \frac{x}{y^2}, \qquad w_2 = \frac{x}{y}, \qquad w_3 = x,$$
$$z_1 = \phi(w_1) = \frac{-1}{y}, \qquad z_2 = \phi(w_2) = \frac{x}{y^4}, \qquad z_3 = \phi(w_3) = \frac{x-1}{x},$$
$$v_1 = \phi^2(w_1) = \frac{y^3}{x}, \qquad v_2 = \phi^2(w_2) = \frac{-y^5}{x^2}, \qquad v_3 = \phi^2(w_3) = \frac{1}{1-x}.$$

Для $k_1 = k_2 = 0$, $k_0 \geqslant 5$:

$$\mathcal{L}(k_0 Q_\infty) = \langle w_1^{\beta_1} w_2^{\beta_2} w_3^{\beta_3} | \beta_i \geqslant 0, 3\beta_1 + 5\beta_2 + 7\beta_3 \leqslant k_0 \rangle.$$

Для $k_2 = 0$, $k_0 \geqslant k_1 \geqslant 5$:

$$\begin{aligned} \mathcal{L}(k_0 Q_\infty + k_1 Q_1) = \langle & w_1^{\beta_1} w_2^{\beta_2} w_3^{\beta_3} | \beta_i \geqslant 0, 3\beta_1 + 5\beta_2 + 7\beta_3 \leqslant k_0, \\ & z_1^{\gamma_1} z_2^{\gamma_2} z_3^{\gamma_1} \quad | \gamma_i \geqslant 0, 3\gamma_1 + 5\gamma_2 + 7\gamma_3 \leqslant k_1, \\ & w_1 z_1, (w_1 z_1)^2, w_1 (w_1 z_1) \rangle. \end{aligned}$$

Для $k_1 = 0$, $k_0 \geqslant k_2 \geqslant 5$:

$$\begin{aligned} \mathcal{L}(k_0 Q_\infty + k_2 Q_2) = \langle & w_1^{\beta_1} w_2^{\beta_2} w_3^{\beta_3} | \beta_i \geqslant 0, 3\beta_1 + 5\beta_2 + 7\beta_3 \leqslant k_0, \\ & v_1^{\gamma_1} v_2^{\gamma_2} v_3^{\gamma_1} \quad | \gamma_i \geqslant 0, 3\gamma_1 + 5\gamma_2 + 7\gamma_3 \leqslant k_2, \\ & w_1 v_1, (w_1 v_1)^2, w_1 (w_1 v_1) \rangle. \end{aligned}$$

Для $k_0 \geqslant k_i \geqslant 5$, $i = 1, 2$:

$$\begin{aligned}\mathcal{L}(k_0Q_\infty + k_1Q_1 + k_2Q_2) = \langle & w_1^{\beta_1}w_2^{\beta_2}w_3^{\beta_3} | \beta_i \geqslant 0, 3\beta_1 + 5\beta_2 + 7\beta_3 \leqslant k_0, \\ & v_1^{\gamma_1}v_2^{\gamma_2}v_3^{\gamma_1} \quad | \gamma_i \geqslant 0, 3\gamma_1 + 5\gamma_2 + 7\gamma_3 \leqslant k_1, \\ & z_1^{\delta_1}z_2^{\delta_2}z_3^{\delta_1} \quad | \delta_i \geqslant 0, 3\delta_1 + 5\delta_2 + 7\delta_3 \leqslant k_2, \\ & w_1z_1, (w_1z_1)^2, v_1z_1, (v_1z_1)^2, w_1v_1, (w_1v_1)^2\rangle.\end{aligned}$$

Главные дивизоры элементов, участвующих в построении базиса $\mathcal{L}(G)$, имеют вид

$$\begin{aligned}&(w_1) = \left(\frac{x}{y^2}\right) = 2Q_2 + Q_1 - 3Q_\infty, (w_2) = \left(\frac{x}{y}\right) = Q_2 + 4Q_1 - 5Q_\infty, (w_3) = (x) = 7Q_1 - 7Q_\infty, \\ &(v_1) = \left(\frac{y^3}{x}\right) = 2Q_1 + Q_\infty - 3Q_2, \ (v_2) = \left(\frac{-y^5}{x^2}\right) = Q_1 + 4Q_\infty - 5Q_2, (v_3) = \left(\frac{1}{1-x}\right) = 7Q_\infty - 7Q_2, \\ &(z_1) = \left(\frac{-1}{y}\right) = 2Q_\infty + Q_2 - 3Q_1, (z_2) = \left(\frac{x}{y^4}\right) = Q_\infty + 4Q_2 - 5Q_1, (z_3) = \left(\frac{x-1}{x}\right) = 7Q_2 - 7Q_1.\end{aligned}$$

Пример 4. Пусть $F = \mathbb{F}_{q^2}(x, y)$ — функциональное поле квартики Клейна с уравнением $x^3y + y^3 + x = 0$ и $q = 5$.

Зададим дивизор $D = P_1 + P_2 + \ldots + P_{25}$, где P_i — точки степени один поля F для $i = 1, \ldots, 25$:

$$\begin{array}{lllll} P_1 = (0,0), & P_2 = (1,0), & P_3 = (a^4, a), & P_4 = (a^{23}, a^3), & P_5 = (a^9, a^4), \\ P_6 = (a^{20}, a^5), & P_7 = (4,2), & P_8 = (3,2), & P_9 = (a^{16}, a^8), & P_{10} = (a^7, 4), \\ P_{11} = (a^{11}, 4), & P_{12} = (3,4), & P_{13} = (a, a^{13}), & P_{14} = (a^2, a^{13}), & P_{15} = (a^{11}, a^{13}), \\ P_{16} = (a^7, a^{14}), & P_{17} = (a^{19}, a^{15}), & P_{18} = (a^8, a^{16}), & P_{19} = (a^5, a^{17}), & P_{20} = (a^7, a^{17}), \\ P_{21} = (a^{10}, a^{17}), & P_{22} = (4, a^{19}), & P_{23} = (a^{21}, a^{20}), & P_{24} = (a^{11}, a^{22}), & P_{25} = (4, a^{23}). \end{array}$$

Здесь a — один из корней примитивного многочлена $f(x) = x^2 + 4x + 2$ над $\mathbb{F}_q$.

Зададим дивизор $G = m\,Q_\infty$, где $m = 13$. Вычислим базис пространства Римана — Роха

$$\mathscr{L}(G) = \mathscr{L}(13Q_\infty) = \langle w_1^{\beta_1}w_2^{\beta_2}w_3^{\beta_3} | \beta_i \geqslant 0, 3\beta_1 + 5\beta_2 + 7\beta_3 \leqslant 13\rangle,$$

необходимый для построения АГ-кода $C_{\mathscr{L}}(D, G)$. Для этого рассмотрим дискретные нормирования функций, являющихся претендентами на базис $\mathscr{L}(G)$, в точке Q_∞ (табл. 3).

Запишем порождающую и проверочную матрицы кода $\mathcal{C}_{\mathscr{L}}(D, G)$:

$$\mathbf{G} = \left[\begin{array}{cccccccccccccccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&a^{23}&a^{10}&a^{20}&a^{20}&a^3&a^{14}&a^4&a^{10}&a^{11}&a^{23}&a^{11}&a^3&a^{14}&a^{53} \\ 0&1&0&0&0&0&0&0&0&0&0&0&a^2&a^7&a^7&0&a&a^{15}&a^{22}&a^{21}&a&a^9&a^2&a^5&a^{11}&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&a^{14}&3&a^{22}&a^{14}&a^{16}&a^2&a^{13}&a^{17}&a^7&a^3&a^9&a^{17}&a^5&a^{19} \\ 0&0&0&1&0&0&0&0&0&0&0&0&a^9&a^7&a^{17}&a^3&3&a^{14}&a^5&a^{20}&a^{11}&a^8&a^{22}&a^{13}&1&a \\ 0&0&0&0&1&0&0&0&0&0&0&0&a^2&a^{20}&a^{22}&a^4&4&a^{10}&a^{22}&a^{15}&4&a^3&a^{23}&a^9&a^{14}&a^{14} \\ 0&0&0&0&0&1&0&0&0&0&0&0&a^{20}&a^9&a^{22}&a^{17}&a^{13}&0&a^{22}&a^9&a^5&a^{19}&4&a^{15}&a&a^{11} \\ 0&0&0&0&0&0&1&0&0&0&0&0&a^{15}&a^4&2&a^{22}&a^{13}&a^2&a^{21}&1&a^4&a^9&a^{10}&a^{19}&a^9&a^{15} \\ 0&0&0&0&0&0&0&1&0&0&0&0&a^{23}&a^7&a^{10}&a^4&3&a^5&a^{17}&a^{16}&a^{21}&a^{20}&a^{11}&4&2&3 \\ 0&0&0&0&0&0&0&0&1&0&0&0&a^{20}&a^4&a^{16}&a^4&a^{10}&a^{16}&0&a&4&a^{16}&a^{19}&1&a^3&a^{11} \\ 0&0&0&0&0&0&0&0&0&1&0&0&a^{11}&a^{16}&a^{21}&a^{20}&a^{19}&a^{21}&a^{13}&3&a^{20}&a^{20}&a^{14}&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0&a^{21}&a^4&a^4&a^{11}&a^8&a^{15}&2&a^7&3&3&a^{17}&4&a^8&a^2 \end{array}\right],$$

$$\mathbf{H} = \left[\begin{array}{cccccccccccccc|cccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^9 & a^{15} & a^8 & 1 & a^{11} & a^4 & 2 & a^{19} & a^{15} & a^{21} & a^{11} \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^5 & a^9 & a^5 & a^{23} & a^3 & a^{20} & a^9 & a^{13} & a^{22} & a^{23} & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^{17} & 2 & a^{11} & a^{13} & a^{20} & a^{19} & a & a^{19} & a^5 & 0 & a^9 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^{14} & a^{23} & a^{13} & a^{22} & a^8 & a^2 & a^{19} & 2 & a^{14} & a^{13} & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^{16} & a^7 & a^3 & a^9 & a^{11} & a^{17} & a^8 & a^{21} & 2 & a^5 & a^2 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^5 & 0 & a^9 & a^{19} & a^{10} & a^3 & a^{23} & 0 & a^{22} & a^{23} & a^{23} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & a^7 & a^{13} & a^{22} & a^{17} & a^8 & a^7 & a^4 & a^{19} & a^{19} & a^{23} & a^{16} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & a^{14} & a^{23} & a^{10} & 4 & a^2 & 4 & 0 & a^5 & a^2 & a^{19} & a \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & a^2 & a^{20} & a^{16} & a & a^2 & a^{15} & a^3 & a^{20} & a^5 & a^{16} & a^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & a^{10} & 4 & a^9 & a^{15} & a^7 & a^7 & a^{13} & a^2 & a^8 & a^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & a^{10} & a^{22} & 3 & a^4 & a^{22} & a^3 & a^{21} & a & a^8 & a^{11} & 3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & a & a^3 & a^5 & 2 & a^{20} & a^7 & a^4 & 0 & a^{13} & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & a^{10} & a^{15} & a^4 & a^9 & a^4 & a^7 & a^{22} & a^{17} & 3 & a^7 & a^7 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & a^{10} & a^3 & a & a^7 & a^2 & a^{19} & 4 & a^{11} & a^8 & 0
\end{array}\right].$$

Таблица 3

Значения нормирования	Базис $\mathscr{L}(G)$	$w_1^{\beta_1} w_2^{\beta_2} w_3^{\beta_3}$
$\nu_\infty(1) = 0$	1	$w_1^0 w_2^0 w_3^0$
$\nu_\infty\left(\frac{x}{y^2}\right) = 3$	$\frac{x}{y^2}$	$w_1^1 w_2^0 w_3^0$
$\nu_\infty\left(\frac{x}{y}\right) = 5$	$\frac{x}{y}$	$w_1^0 w_2^1 w_3^0$
$\nu_\infty\left(\frac{x^2}{y^4}\right) = 6$	$\frac{x^2}{y^4}$	$w_1^2 w_2^0 w_3^0$
$\nu_\infty(x) = 7$	x	$w_1^0 w_2^0 w_3^1$
$\nu_\infty\left(\frac{x^2}{y^3}\right) = 8$	$\frac{x^2}{y^3}$	$w_1^1 w_2^1 w_3^0$
$\nu_\infty\left(\frac{x^3}{y^6}\right) = 9$	$\frac{x^3}{y^6}$	$w_1^3 w_2^0 w_3^0$
$\nu_\infty\left(\frac{x^2}{y^2}\right) = 10$	$\frac{x^2}{y^2}$	$w_1^0 w_2^2 w_3^0$
$\nu_\infty\left(\frac{x^3}{y^5}\right) = 11$	$\frac{x^3}{y^5}$	$w_1^2 w_2^1 w_3^0$
$\nu_\infty\left(\frac{x^2}{y}\right) = 12$	$\frac{x^2}{y}$	$w_1^0 w_2^1 w_3^1$
$\nu_\infty\left(\frac{x^3}{y^4}\right) = 13$	$\frac{x^3}{y^4}$	$w_1^1 w_2^2 w_3^0$
$\nu_\infty\left(x^4\right) = 14$	—	—

Код $\mathcal{C}_{\mathscr{L}}(D, G)$, ассоциированный с определённой выше квартикой Клейна, имеет параметры $[25, 11, 12]$, а его дуальный код $\mathcal{C}_{\mathscr{L}}(D, G)^\perp$ — параметры $[25, 14, 9]$.

Для построения пары, исправляющей ошибки, для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ необходимо, чтобы $m > t+g$, где $t = \lfloor (n - \deg(G) - 1 - g)/2 \rfloor$. В нашем случае $g = 3$ и $t = 4$. Определим вспомогательный дивизор:

$$H = (t + g)\, Q_\infty = 7\, Q_\infty.$$

Тогда для кода $\mathcal{C}_{\mathscr{L}}(D, G)$ парами, исправляющими 4 ошибки, являются:

— $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H)$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}^{\perp}(D, G + H)$ с параметрами $[25, 5, 18]$ и $[25, 7, 16]$ соответственно;
— $\mathcal{A} = \mathcal{C}_{\mathscr{L}}^{\perp}(D, H)$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}(D, H - G)$ с параметрами $[25, 5, 18]$ и $[25, 7, 16]$ соответственно.

Для построения пары, исправляющей ошибки для кода $\mathcal{C}_{\mathscr{L}}^{\perp}(D, G)$, необходимо, чтобы $t = \lfloor(\deg(G) - 3g + 1)/2\rfloor$. В нашем случае $g = 3$ и $t = 2$. Определим вспомогательный дивизор

$$H' = (t + g)\, Q_\infty = (2 + 3)\, Q_\infty.$$

Тогда для кода $\mathcal{C}_{\mathscr{L}}^{\perp}(D, G)$ пару, исправляющую две ошибки, составляют коды $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H')$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}(D, G - H')$ с параметрами $[25, 3, 20]$ и $[25, 6, 17]$ соответственно.

5.4. Пример декодирования АГ-кода на эллиптической кривой

Рассмотрим АГ-код на эллиптической кривой, построенный в п. 5.1.

Пусть $F = \mathbb{F}_q(x, y)$ — эллиптическое функциональное поле с уравнением $y^2 = x^3 + 7x + 4$ и $q = 17$. Запишем порождающую и проверочную матрицы $[12, 5, 7]$-кода $C_{\mathscr{L}}(D, G)$, где $G = 5P_\infty$:

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 8 & 10 & 0 & 8 & 14 & 8 & 16 \\ 0 & 1 & 0 & 0 & 0 & 9 & 1 & 11 & 4 & 15 & 4 & 13 \\ 0 & 0 & 1 & 0 & 0 & 14 & 7 & 9 & 2 & 16 & 1 & 16 \\ 0 & 0 & 0 & 1 & 0 & 3 & 15 & 13 & 7 & 10 & 12 & 14 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 14 & 14 & 10 & 10 \end{bmatrix},$$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 11 & 12 & 4 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 6 & 14 & 9 & 8 & 13 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 & 11 & 10 & 0 & 7 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 5 & 6 & 15 & 8 & 16 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 5 & 13 & 12 & 6 & 14 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 5 & 8 & 0 & 15 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 16 & 11 & 6 & 10 & 7 \end{bmatrix}.$$

В п. 5.1 получены также коды $\mathcal{A} = \mathcal{C}_{\mathscr{L}}(D, H)$ и $\mathcal{B} = \mathcal{C}_{\mathscr{L}}^{\perp}(D, G + H)$ с параметрами $[12, 3, 9]$ и $[12, 4, 8]$, составляющие пару, исправляющую $t = 2$ ошибки для кода $C_{\mathscr{L}}(D, G)$. Запишем порождающие матрицы соответствующих кодов:

$$\mathbf{G}_{\mathcal{A}} = \begin{bmatrix} 1 & 0 & 0 & 8 & 2 & 0 & 15 & 6 & 7 & 3 & 5 & 12 \\ 0 & 1 & 0 & 9 & 11 & 13 & 5 & 14 & 0 & 4 & 1 & 11 \\ 0 & 0 & 1 & 1 & 5 & 5 & 15 & 15 & 11 & 11 & 12 & 12 \end{bmatrix},$$

$$\mathbf{G}_{\mathcal{B}} = \begin{bmatrix} 1 & 0 & 0 & 16 & 0 & 3 & 12 & 4 & 8 & 1 & 8 & 15 \\ 0 & 1 & 0 & 16 & 0 & 3 & 0 & 16 & 15 & 11 & 11 & 12 \\ 0 & 0 & 1 & 16 & 0 & 0 & 5 & 12 & 9 & 8 & 8 & 9 \\ 0 & 0 & 0 & 0 & 1 & 16 & 3 & 14 & 4 & 13 & 4 & 13 \end{bmatrix}.$$

Пусть $y = \begin{pmatrix} \mathit{2} & 13 & 15 & \mathit{14} & 8 & 1 & 8 & 6 & 12 & 7 & 2 & 6 \end{pmatrix}$ — вектор из кода $C_{\mathscr{L}}(D, G)$, содержащий две ошибки (позиции ошибок выделены курсивом). Пункт 1 алгоритма 1. заключается в нахождении ядра $M = \{a \in \mathcal{A} : \langle a * y, b\rangle = 0 \text{ для всех } b \in \mathcal{B}\}$ отображения $\phi : a \mapsto (b \mapsto \langle a * y, b\rangle)$. Как упомянуто в замечании 2, можно ограничиться нахождением одного вектора из ядра, что и продемонстрировано далее. Пусть $\overrightarrow{b_i} \in \mathbf{G}_{\mathcal{B}}$, вычислим матрицу, столбцы которой составляют значения $y * \overrightarrow{b_i}$:

$$\mathbf{G}_\phi = \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 13 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 3 & 3 & 3 & 0 \\ 0 & 0 & 0 & 8 \\ 3 & 3 & 0 & 16 \\ 11 & 0 & 6 & 7 \\ 7 & 11 & 4 & 16 \\ 11 & 10 & 6 & 14 \\ 7 & 9 & 5 & 6 \\ 16 & 5 & 16 & 8 \\ 5 & 4 & 3 & 10 \end{bmatrix}.$$

Необходимо найти один вектор $a \in \mathcal{A} \mid \langle a, y * b \rangle = 0$, для этого подействуем отображением ϕ на все базисные векторы $\overrightarrow{a_i} \in \mathbf{G}_\mathcal{A}$. Из полученных образов составим матрицу:

$$\mathbf{G}_{\phi(\mathcal{A})} = \begin{bmatrix} 12 & 5 & 5 & 0 \\ 12 & 12 & 12 & 0 \\ 7 & 7 & 7 & 0 \end{bmatrix} \sim \begin{bmatrix} 12 & 5 & 5 \\ 12 & 12 & 12 \\ 7 & 7 & 7 \end{bmatrix}.$$

Найдя левое ядро матрицы $\mathbf{G}_{\phi(\mathcal{A})}$ и выбрав случайный вектор из ядра, получим соответствующие коэффициенты в линейном разложении вектора a, образ которого равен нулевому вектору:

$$x \cdot \mathbf{G}_{\phi(\mathcal{A})} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix},$$
$$x \in \mathrm{Span}_{\mathbb{F}_q}\{(0,1,8)\}, \quad M = \mathrm{Span}_{\mathbb{F}_q}\{(0 \cdot \overrightarrow{a_0} + \overrightarrow{a_1} + 8\overrightarrow{a_2})\},$$
$$a = 0 \cdot \overrightarrow{a_0} + 1 \cdot \overrightarrow{a_1} + 8 \cdot \overrightarrow{a_2} \mid \phi(a) = 0 \; \forall b \in \mathcal{B},$$
$$a = \begin{pmatrix} 0 & 1 & 8 & 0 & 0 & 2 & 6 & 15 & 3 & 7 & 12 & 5 \end{pmatrix}.$$

Очевидно, что $I_e \subseteq \mathfrak{I} = Z(a) = \{0, 3, 4\}$. Перейдём к шагу 6 и построим проверочную матрицу $H_\mathfrak{I}$:

$$\mathbf{H}_\mathfrak{I} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Решив систему уравнений $\mathbf{H}_\mathfrak{I} u^{\mathrm{T}} = \mathbf{H} y^{\mathrm{T}}$ относительно u, получим

$$e_\mathfrak{I} = u = \begin{pmatrix} 7 & 10 & 0 \end{pmatrix} \to R(e_\mathfrak{I}) = \begin{pmatrix} 7 & 0 & 0 & 10 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Окончательно в результате процедуры декодирования имеем

$$y - R(e_\mathfrak{I}) = (\ 2\ 13\ 15\ 14\ 8\ 1\ 8\ 6\ 12\ 7\ 2\ 6\ ) - (\ 7\ 0\ 0\ 10\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ) =$$
$$= (\ 12\ 13\ 15\ 4\ 8\ 1\ 8\ 6\ 12\ 7\ 2\ 6\ ) = c \in C_\mathscr{L}(D, G).$$

ЛИТЕРАТУРА

1. *Гонна В. Д.* Коды, ассоциированные с дивизорами // Проблемы передачи информации. 1977. Т. 13. № 1. С. 33–39.
2. *Tsfasman M. A., Vlădutx S. G., and Zink Th.* Modular curves, Shimura curves and Goppa codes, better than Varshamov — Gilbert bound // Math. Nachr. 1982. V. 109. P. 21–28.
3. *Ihara Y.* Some remarks on the number of rational points of algebraic curves over finite fields // J. Fac. Sci. Univ. Tokyo. Sect. IA Math. 1981. V. 28. P. 721–724.
4. *Garcia A. and Stichtenoth H.* A tower of Artin — Schreier extensions of function fields attaining the Drinfeld — Vladut bound // Inventiones Mathematicae. 1995. V. 121. P. 211–222.
5. *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. М.: Мир, 2000. 687 с.
6. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
7. *Guruswami V. and Sudan M.* Improved decoding of Reed — Solomon and algebraic geometry codes // IEEE Trans. Inform. Theory. 1999. V. 45. P. 1757–1768.
8. *Couvreur A., Márquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes // IEEE Trans. Inform. Theory. 2017. V. 63. P. 5404–5418.
9. *Pellikaan R.* On decoding by error location and dependent sets of error positions // Discrete Math. 1992. V. 106–107. P. 113–121.
10. *Márquez-Corbella I. and Pellikaan R.* Error-correcting pairs: a new approach to code-based cryptography // 20th Conf. ACA 2014, Jul 2014, New York, USA. `https://hal.science/hal-01088433/document`.
11. *Pellikaan R.* On the existence of error-correcting pairs // Statistical Planning Inference. 1996. V. 51. P. 229–242.
12. *Couvreur A., Panaccione I.* Power Error Locating Pairs. `https://arxiv.org/abs/1907.11658v3`.
13. *Wesemeyer S.* On the automorphism group of various Goppa codes // IEEE Trans. Inform. Theory. 1998. V. 44. No. 2. P. 630–643.

REFERENCES

1. *Goppa V. D.* Kody, assotsiirovannye s divizorami [Codes associated with divisors]. Problemy Peredachi Informatsii, 1977, vol. 13, no. 1, pp. 33–39. (in Russian)
2. *Tsfasman M. A., Vlădutx S. G., and Zink Th.* Modular curves, Shimura curves and Goppa codes, better than Varshamov — Gilbert bound. Math. Nachr., 1982, vol. 109, pp. 21–28.
3. *Ihara Y.* Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo, Sect. IA Math., 1981, vol. 28, pp. 721–724.
4. *Garcia A. and Stichtenoth H.* A tower of Artin — Schreier extensions of function fields attaining the Drinfeld — Vladut bound. Inventiones Mathematicae, 1995, vol. 121, pp. 211–222.
5. *Cox D., Little J., and O'Shea D.* Ideals, Varieties and Algorithms. Springer Verlag, 1992.
6. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
7. *Guruswami V. and Sudan M.* Improved decoding of Reed — Solomon and algebraic geometry codes. IEEE Trans. Inform. Theory, 1999, vol. 45, pp. 1757–1768.
8. *Couvreur A., Márquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. IEEE Trans. Inform. Theory, 2017. vol. 63, pp. 5404–5418.

9. *Pellikaan R.* On decoding by error location and dependent sets of error positions. Discrete Math., 1992, vol. 106–107, pp. 113–121.
10. *Márquez-Corbella I. and Pellikaan R.* Error-correcting pairs: a new approach to code-based cryptography. 20th Conf. ACA 2014, Jul 2014, New York, USA. https://hal.science/hal-01088433/document.
11. *Pellikaan R.* On the existence of error-correcting pairs. Statistical Planning Inference, 1996, vol. 51, pp. 229–242.
12. *Couvreur A. and Panaccione I.* Power Error Locating Pairs. https://arxiv.org/abs/1907.11658v3.
13. *Wesemeyer S.* On the automorphism group of various Goppa codes. IEEE Trans. Inform. Theory, 1998, vol. 44, no. 2, pp. 630–643.

УДК 519.725 DOI 10.17223/20710410/62/8

WEIGHT DISTRIBUTION OF LOW-DENSITY PERIODIC RANDOM ERRORS AND THEIR CORRECTING CODES WITH ERROR DECODING PROBABILITY

L. Haokip, P.K. Das

Tezpur University, Tezpur, India

E-mail: h_letminthang@yahoo.com, pankaj4thapril@yahoo.co.in

We present weight distribution of low-density periodic random errors in the space of all q-ary n-tuples along with the average Hamming weight of the error set. We also provide necessary and sufficient conditions for the existence of linear codes correcting such error pattern. Examples of such codes are given. Finally, probability of decoding error of such codes over a binary symmetric channel is derived.

Keywords: *parity-check matrix, syndromes, periodic random error, error decoding probability.*

ВЕСОВОЕ РАСПРЕДЕЛЕНИЕ ПЕРИОДИЧЕСКИХ СЛУЧАЙНЫХ ОШИБОК МАЛОЙ ПЛОТНОСТИ И ИХ КОРРЕКТИРУЮЩИЕ КОДЫ С ВЕРОЯТНОСТЬЮ ОШИБКИ ДЕКОДИРОВАНИЯ

Л. Хаокип, П.К. Дас

Университет Тезпур, г. Тезпур, Индия

Изучается весовое распределение периодических случайных ошибок малой плотности в пространстве всех q-арных n-кортежей и среднее число таких ошибок на блок длины n. Приведены необходимые и достаточные условия существования и примеры линейных кодов, исправляющих такие ошибки. Вычислена вероятность ошибки декодирования таких кодов для двоичного симметричного канала связи.

Ключевые слова: *матрица проверки чётности, синдромы, периодическая случайная ошибка, вероятность ошибки декодирования.*

1. Introduction

Periodic random error is one type of errors which occurs in electronic control unit like power lines, inverters, car electric, compact disc, CD ROM. This was observed by N. Lange in 1994 [1]. This error pattern behaves in such a way that any b consecutive components are disturbed after a gap of some fixed positions repeatedly. Linear codes capable of detecting and correcting such errors along with their Hamming weight distribution and decoding error probability are studied in [2, 3]. A periodic random error can be defined as follows.

Definition 1. An s-periodic random error of length b is an n-tuple whose nonzero components are confined to distinct sets of b consecutive positions such that the sets are separated by s positions.

In 1963, Wyner [4] observed that for low intensity disturbances, only a few components within a burst [5] get disturbed, and he introduced the concept of low-density burst.

We extend this idea to periodic random errors whose intensity is low and define low-density periodic random error as below.

Definition 2. Low-density periodic random error is an s-periodic random error of length b such that each sets of b consecutive components separated by s zeros contains at most w, $w \leqslant b$, nonzero components.

Let $\xi_{(s,b|w),n,q}$ denote the set of all low-density periodic random errors in the space of n-tuples over $\mathrm{GF}(q)$. For example, the following vectors are some members of $\xi_{(3,2|1),10,2}$:

$$0000001000, 0000010000, 0100000000, 0100001000, 0100010000,$$
$$1000000000, 1000001000, 1000010000, 0000000100, 0010000000,$$
$$0010000100, 0010001000, 0100000100, 0000000010, 0001000000,$$
$$0001000010, 0001000100, 0010000010, 0000000001, 0000100000.$$

In this paper, we study the Hamming weight distribution of the vectors of $\xi_{(s,b|w),n,q}$. Then we study the existence of linear codes correcting the errors from the set $\xi_{(s,b|w),n,q}$. We denote a linear code that corrects low-density periodic random errors from the set $\xi_{(s,b|w),n,q}$ by $\mathrm{LDP}_{(s,b|w),n,q}$RC-code. We further study the probability of decoding error for the errors set $\xi_{(s,b|w),n,q}$ over a binary symmetric channel. Throughout the paper, we consider $n = \lambda(b+s)+l$, where $0 \leqslant l < s+b$ and $\lambda \in \mathbb{N}$.

The organization of remaining part of the paper is as follows. Section 2 gives the Hamming weight distribution of the vectors of $\xi_{(s,b|w),n,q}$ along with examples. Average Hamming weight of the vectors of $\xi_{(s,b|w),n,q}$ is derived. In Section 3, we obtain necessary and sufficient conditions for existence of a $\mathrm{LDP}_{(s,b|w),n,q}$RC-code followed by three examples. Finally, we provide the probability of decoding error for the errors of $\xi_{(s,b|w),n,q}$ over a binary symmetric channel.

2. Hamming weight distribution of vectors of $\xi_{(s,b|w),n,q}$

In this section, we give the Hamming weight distribution of vectors of $\xi_{(s,b|w),n,q}$ and average Hamming weight of a vector from the set $\xi_{(s,b|w),n,q}$.

Here $n = \lambda(b+s)+l$, where $0 \leqslant l < s+b$, then the maximum Hamming weight $w_{\max}$ of a vector of $\xi_{(s,b|w),n,q}$ is given by

$$w_{\max} = \begin{cases} w\lambda, & \text{when} \quad l = 0, \\ w\lambda + \min\{l, w\}, & \text{when} \quad 1 \leqslant l < b, \\ w\,(\lambda+1)\,, & \text{when} \quad b \leqslant l < s+b. \end{cases}$$

We first state the following lemma from [6].

Lemma 1 [6]. If λ_i denotes the number of sets of non-zero positions and m_i the maximum number of nonzero positions in a vector of $\xi_{(s,b|w),n,q}$ that starts from i^{th} position, then

$$\lambda_i = \left\lceil \frac{n-i+1}{s+b} \right\rceil \text{ and } m_i = \left\lfloor \frac{n-i+1}{s+b} \right\rfloor b + \gamma\big((n-i+1) \bmod (b+s)\big),$$

where $\lfloor x \rfloor$ means the greatest integer $\leqslant x$, $\lceil x \rceil$ means the smallest integer $\geqslant x$, and

$$\gamma(r) = \begin{cases} r, & \text{if} \quad 0 \leqslant r \leqslant b, \\ b, & \text{if} \quad b < r < b+s. \end{cases}$$

Next, we give the following Lemma to derive weight distribution of vectors of $\xi_{(s,b|w),n,q}$.

Lemma 2. Let p_i be the number of common nonzero positions of the errors of $\xi_{(s,b|w),n,q}$ that starts from the i^{th} $(i = s+2, \ldots, s+b)$ position with an error vector of $\xi_{(s,b|w),n,q}$ that starts from the 1^{st} position. Then p_i is given by

(1) when $l = 0$ and $b-1 \leqslant l \leqslant s+b$: $\quad p_i = (i-s-1)\beta_i$, and

(2) when $1 \leqslant l < b-1$: $\quad p_i = \begin{cases} (i-s-1)\beta_{i-1} & \text{for} \quad i = s+2, \\ (i-s-1)\beta_{i-1} + l & \text{for} \quad i = s+3, s+4, \ldots, s+b, \end{cases}$

where $\beta_i = \left\lceil \dfrac{n-i-b+1}{s+b} \right\rceil$.

Proof.

C a s e 1 : $l = 0$ and $b-1 \leqslant l \leqslant s+b$.

The common nonzero positions of the error pattern of $\xi_{(s,b|w),n,q}$ that starts from the $(s+2)^{\text{th}}$ position with the error pattern that starts from the 1^{st} position are $s+b+1$, $2(s+b)+1$, …, $\beta_{s+1}(s+b)+1$, where $\beta_{s+1} = \left\lceil \dfrac{n-(s+1)-b+1}{s+b} \right\rceil$. This number of common nonzero position is given by β_{s+1}.

The common nonzero positions of the error pattern of $\xi_{(s,b|w),n,q}$ that starts from the $(s+3)^{\text{th}}$ position with the error pattern that starts from the 1^{st} position are $s+b+1$, $s+b+2$, $2(s+b)+1$, $2(s+b)+2$, …, $\beta_{s+2}(s+b)+1$, $\beta_{s+2}(s+b)+2$, where $\beta_{s+3} = \left\lceil \dfrac{n-(s+3)-b+1}{s+b} \right\rceil$. This number of common nonzero position is given by $2\beta_{s+2}$.

Continuing this, the common nonzero positions of the error pattern of $\xi_{(s,b|w),n,q}$ that starts from the $(s+b)^{\text{th}}$ position with the error pattern that starts from the 1^{st} position are $s+b+1$, $s+b+2$, …, $s+b+(b-1)$, $2(s+b)+1$, $2(s+b)+2$, …, $2(s+b)+(b-1)$, …, $\beta_{s+b-1}(s+b)+1$, $\beta_{s+b-1}(s+b)+2$, …, $\beta_{s+b-1}(s+b)+(b-1)$, where $\beta_{s+b-1} = \left\lceil \dfrac{n-(s+b-1)-b+1}{s+b} \right\rceil$. This number of common nonzero position is given by $(b-1)\beta_{s+b-1}$.

Thus $p_i = (i-s-1)\beta_{i-1}$ for $i = s+2, s+3, \ldots, s+b$, where $\beta_i = \left\lceil \dfrac{n-i-b+1}{s+b} \right\rceil$.

C a s e 2 : $1 \leqslant l < b-1$.

The common nonzero positions of the error pattern of $\xi_{(s,b|w),n,q}$ that starts from the $(s+2)^{\text{th}}$ position with the error pattern that starts from the 1^{st} position are $s+b+1$, $2(s+b)+1$, …, $\beta_{s+1}(s+b)+1$, where $\beta_{s+1} = \left\lceil \dfrac{n-(s+2)-b+1}{s+b} \right\rceil$. This number of common nonzero position is given by β_{s+1}.

If the error pattern starts from the $(s+3)^{\text{th}}$ position, the common nonzero positions with the error pattern that starts from the 1^{st} position, excluding the last set of nonzero positions, are $s+b+1$, $s+b+2$, $2(s+b)+1$, $2(s+b)+2$, …, $\beta_{s+2}(s+b)+1$, $\beta_{s+2}(s+b)+2$, where $\beta_{s+2} = \left\lceil \dfrac{n-(s+2)-b+1}{s+b} \right\rceil$.

The common positions with the last set are $\lambda_{s+3}(s+b)+1$, $\lambda_{s+3}(s+b)+2$, …, $\lambda_{s+3}(s+b)+l$ (λ_i are given by Lemma 1), whose number is l. Therefore, the total number of common nonzero positions is given by $2\beta_{s+2}+l$.

Continuing this, if the error pattern starts from the $(s+b)^{\text{th}}$ position, the common nonzero positions with the error pattern that starts from the 1^{st} position, excluding the last set of nonzero positions, are $s+b+1$, $s+b+2$, …, $s+b+(b-1)$, $2(s+b)+1$, $2(s+b)+2$,

$\ldots$, $2(s+b)+(b-1)$, $\ldots$, $\beta_{s+b-1}(s+b)+1$, $\beta_{s+b-1}(s+b)+2$, $\ldots$, $\beta_{s+b-1}(s+b)+(b-1)$, where $\beta_{s+b-1}=\left\lceil\dfrac{n-(s+b-1)-b+1}{s+b}\right\rceil$.

The last set has common positions $\lambda_{s+b}(s+b)+1$, $\lambda_{s+b}(s+b)+2$, $\ldots$, $\lambda_{s+b}(s+b)+l$, whose number is l. This number of common nonzero position is given by $(b-1)\beta_{s+b-1}+l$. Thus $p_i=\begin{cases}(i-s-1)\beta_{i-1} & \text{for} \quad i=s+2,\\ (i-s-1)\beta_{i-1}+l & \text{for} \quad i=s+3,s+4,\ldots,s+b.\end{cases}$

Lemma 2 is proven. ■

Theorem 1. Let $R^n_{s,b|w}(j)$ be the total number of vectors of $\xi_{(s,b|w),n,q}$, whose Hamming weight is j. Then:

For $j=1$:

$$R^n_{s,b|w}(1)=\sum_{i=1}^{s+1}\left[\binom{m_i}{1}-\binom{k_{i-1}}{1}\right](q-1)+\sum_{i=s+2}^{s+b}\left[\binom{m_i}{1}-\binom{k_{i-1}}{1}-\binom{\beta_{i-1}}{1}\right](q-1).$$

For $2\leqslant j\leqslant w$:

$$R^n_{s,b|w}(j)=\sum_{i=1}^{s+1}\left[\binom{m_i}{j}-\binom{k_{i-1}}{j}\right](q-1)^j+\sum_{i=s+2}^{s+b}\left[\binom{m_i}{j}-\binom{k_{i-1}}{j}-\binom{p_i}{j}+\binom{p_{i-1}}{j}\right](q-1)^j.$$

For $w+1\leqslant j\leqslant w_{\max}-1$:

$$R^n_{s,b|w}(j)=\sum_{i=1}^{s+1}\left[\binom{m_i}{j}-\binom{k_{i-1}}{j}-\binom{(b-w)\beta_{i-1}}{1}\binom{m_i-b}{j-w-1}\right](q-1)^j+$$
$$+\sum_{i=s+2}^{s+b}\left[\binom{m_i}{j}-\binom{k_{i-1}}{j}-\binom{p_i}{j}+\binom{p_{i-1}}{j}-\binom{(b-w)\beta_{i-1}}{1}\binom{m_i-b}{j-w-1}\right](q-1)^j.$$

For $j=w_{\max}$:

$$R^n_{s,b|w}(w_{\max})=\begin{cases}\Big[(s+1)b^\lambda+b^{\lambda-1}-s-1\Big](q-1)^{w_{\max}}, & \text{when} \quad l=0,\\ b^\lambda(q-1)^{w_{\max}}, & \text{when} \quad 1\leqslant l<b,\\ \Big[(l-b+1)b^{\lambda+1}+b^\lambda-l+b-1\Big](q-1)^{w_{\max}}, & \text{when} \quad b\leqslant l<s+b,\end{cases}$$

where $p_{s+1}=1$, $k_0=0$, $k_i=m_{i+1}-\beta_i$, β_i, m_i, and p_i are given by Lemmas 1, 2.

Proof.

C a s e 1 : $j=1$.

The number of error patterns of weight 1 that start from the i^{th} positions, where $i=1,2,\ldots,s+1$, is given by $\binom{m_i}{1}(q-1)$. But in the calculation $\binom{m_{i+1}}{1}(q-1)$, number of already counted nonzero components in $\binom{m_i}{1}(q-1)$ is $k_i=m_{i+1}-\beta_i$ for $i=1,2,3,\ldots,s+1$, where $\beta_i=\left\lceil\dfrac{n-i-b+1}{s+b}\right\rceil$ represents the total number of complete sets of b consecutive positions in which the nonzero elements of the error pattern start from the i^{th} position. Therefore, the total number of the errors having weight 1 is $\sum\limits_{i=1}^{s+1}\left[\binom{m_i}{1}-\binom{k_{i-1}}{1}\right](q-1)^1$ with $k_0=0$.

For error patterns whose starting position is $i = s+2, \ldots, s+b$, all the weight 1 vectors are already present in the first position (i.e., the b^{th} positions of each set of nonzero positions except the last set which may be less than b components). The number of these nonzero components is given by β_{i-1}. Thus, $\binom{\beta_{i-1}}{1}$, number of weight 1, need to be subtracted from each starting position of the error pattern. So, the number of weight 1 in these positions is given by the quantity $\binom{m_i}{1} - \binom{k_{i-1}}{1} - \binom{\beta_{i-1}}{1}$. We have

$$R^n_{s,b|w}(1) = \sum_{i=1}^{s+1} \left[\binom{m_i}{1} - \binom{k_{i-1}}{1} \right] (q-1) + \sum_{i=s+2}^{s+b} \left[\binom{m_i}{1} - \binom{k_{i-1}}{1} - \binom{\beta_{i-1}}{1} \right] (q-1).$$

C a s e 2 : $2 \leqslant j \leqslant w$.

As above, the total number of the errors having weight j that start from the i^{th} positions, where $i = 1, 2, \ldots, s+1$, is the quantity $\sum_{i=1}^{s+1} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} \right] (q-1)^j$ with $k_0 = 0$.

But, for error patterns that start from positions $i = s+2, \ldots, s+b$, there are some more common vectors with the already counted error vectors that starts from the 1^{st} position.

By Lemma 2, p_i denotes the number of common nonzero components that start from the i^{th} $(i = s+2, \ldots, s+b)$ position which are already present in the errors that start from the first position; $\binom{p_i}{j}(q-1)^j$ gives the number of vectors of weight j in the i^{th} $(i = s+2, \ldots, s+b)$ positions which are already counted in the error pattern that start from the first position. This includes some vectors which are deleted by the term $\binom{k_{i-1}}{j}(q-1)^j$, thus the term $\binom{p_{i-1}}{j}(q-1)^j$ is added to include such already deleted error vectors, here $p_{s+1} = 1$. So the exact number of common vectors that need to be excluded is $\left[\binom{p_i}{j} - \binom{p_{i-1}}{j} \right] (q-1)^j$. Therefore, we have

$$R^n_{s,b|w}(j) = \sum_{i=1}^{s+1} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} \right] (q-1)^j + \sum_{i=s+2}^{s+b} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} - \binom{p_i}{j} + \binom{p_{i-1}}{j} \right] (q-1)^j.$$

C a s e 3: $w+1 \leqslant j \leqslant w_{\max} - 1$.

In this case, we can also similarly calculate the total number of all error vectors having weight j and starting from the i^{th} position, where $i = 1, 2, \ldots, s+1$, after deleting the common vectors as the quantity

$$\sum_{i=1}^{s+1} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} - \binom{(b-w)\beta_{i-1}}{1} \binom{m_i - b}{j-w-1} \right] (q-1)^j \quad \text{with } k_0 = 0.$$

Again, for error vectors having weight j starting from $(s+2)^{\text{th}}$ to $(s+b)^{\text{th}}$ positions, there are some more common vectors which we have calculated, as in the previous case: $\left[\binom{p_i}{j} - \binom{p_{i-1}}{j} \right] (q-1)^j$. Therefore,

$$R^n_{s,b|w}(j) = \sum_{i=1}^{s+1} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} - \binom{(b-w)\beta_{i-1}}{1} \binom{m_i - b}{j-w-1} \right] (q-1)^j +$$
$$+ \sum_{i=s+2}^{s+b} \left[\binom{m_i}{j} - \binom{k_{i-1}}{j} - \binom{(b-w)\beta_{i-1}}{1} \binom{m_i - b}{j-w-1} - \binom{p_i}{j} + \binom{p_{i-1}}{j} \right] (q-1)^j.$$

C a s e 4 : $j = w_{\max}$.

In this case, the number of error vectors with weight j is calculated, and different formulas are found for $l = 0$, $1 \leqslant l < b$, and $b \leqslant l < s + b$:

$$R^n_{s,b|w}(w_{\max}) = \begin{cases} \left[(s+1)b^\lambda + b^{\lambda-1} - s - 1\right](q-1)^{w_{\max}}, & \text{when} \quad l = 0, \\ b^\lambda (q-1)^{w_{\max}}, & \text{when} \quad 1 \leqslant l < b, \\ \left[(l-b+1)b^{\lambda+1} + b^\lambda - l + b - 1\right](q-1)^{w_{\max}}, & \text{when} \quad b \leqslant l < s+b. \end{cases}$$

Theorem 1 is proven. ■

Remark 1. The values of m_i and p_i in [3] are given by

$$m_i = \begin{cases} b\lambda & \text{for} \quad 1 \leqslant i \leqslant s+1, \\ b\lambda + s - i + 1 & \text{for} \quad s+2 \leqslant i \leqslant s+b, \end{cases} \qquad \text{if} \quad l = 0,$$

$$m_i = \begin{cases} b\lambda + l - i + 1 & \text{for} \quad 1 \leqslant i \leqslant l, \\ b\lambda & \text{for} \quad l+1 \leqslant i \leqslant s+l+1, \\ b\lambda + s + l - i + 1 & \text{for} \quad s+l+2 \leqslant i \leqslant s+b, \end{cases} \qquad \text{if} \quad 1 \leqslant l < b,$$

$$m_i = \begin{cases} b(\lambda+1) & \text{for} \quad 1 \leqslant i \leqslant l-b+1, \\ b(\lambda+1) + (l-b-i+1) & \text{for} \quad l-b+1 < i \leqslant l, \\ b\lambda & \text{for} \quad 1+l \leqslant i \leqslant s+b, \end{cases} \qquad \text{if} \quad b \leqslant l < s+b,$$

$$p_i = i\beta_{i+s}, \qquad \text{if} \quad l = 0 \quad \text{or} \quad b \leqslant l < s+b,$$

$$p_i = \begin{cases} i\beta_{i+s} & \text{for} \quad 1 \leqslant i \leqslant l, \\ i(p_1 - 1) + l & \text{for} \quad l+1 \leqslant i \leqslant b-1, \end{cases} \qquad \text{if} \quad 1 \leqslant l < b.$$

In this paper, we consider the simplified form for m_i and p_i in Lemma 1 and Theorem 1, and for $b = w$ we get

$$w_{\max} = \begin{cases} b\lambda, & \text{when} \quad l = 0, \\ b\lambda + l, & \text{when} \quad 1 \leqslant l < b, \\ b\,(\lambda+1)\,, & \text{when} \quad b \leqslant l < s+b, \end{cases} \qquad \text{and} \quad \binom{(b-w)\beta_{i-1}}{1}\binom{m_i - b}{j-w-1} = 0.$$

Then Theorem 1 coincides with Lemma 3.1 [3].

Example 1. Considering $q = 3$, $n = 11$, $s = 3$, $b = 2$, and $w = 1$ in Theorem 1, we have $\lambda = 2$, $l = 11 \bmod 5 = 1$, $m_1 = 5$, $m_2 = \cdots = m_5 = 4$, $p_{s+1} = 1$, $p_{s+2} = 2$, $\beta_0 = \beta_1 = \cdots = \beta_4 = 2$. Then

$$R^{11}_{3,2|1}(1) = \left[\binom{5}{1} - \binom{0}{1}\right](3-1)^1 + \left[\binom{4}{1} - \binom{2}{1}\right](3-1)^1 +$$
$$+ \left[\binom{4}{1} - \binom{2}{1}\right](3-1)^1 + \left[\binom{4}{1} - \binom{2}{1}\right](3-1)^1 + \left[\binom{4}{1} - \binom{2}{1} - \binom{2}{1}\right](3-1)^1 =$$
$$= 5 \cdot 2 + 2 \cdot 3 \cdot 2 + 0 = 22;$$
$$R^{11}_{3,2|2}(2) = \left[\binom{5}{2} - \binom{0}{2} - \binom{(3-2)\cdot 2}{1}\binom{3}{2-1-1}\right](3-1)^2 +$$
$$+ \left[\binom{4}{2} - \binom{2}{2} - \binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right](3-1)^2 +$$

$$+\left[\binom{4}{2}-\binom{2}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right](3-1)^2+$$
$$+\left[\binom{4}{2}-\binom{2}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right](3-1)^2+$$
$$+\left[\binom{4}{2}-\binom{2}{2}-\binom{2}{2}+\binom{1}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right](3-1)^2=76;$$
$$R^{11}_{3,2|3}(3)=2^2(3-1)^3=32.$$

Here the maximum weight is $w_{\max}=3$. This example can be verified by using Example 4 in the next section.

Example 2. Considering $q=2$, $n=12$, $s=3$, $b=2$, and $w=1$ in Theorem 1, we have $\lambda=2$, $l=12 \bmod 5=2$, $m_1=6$, $m_2=5$, $m_3=\cdots=m_5=4$, $p_{s+1}=1$, $p_{s+2}=2$, $\beta_0=\beta_1=\cdots=\beta_4=2$. Then

$$R^{11}_{3,2|1}(1)=\left[\binom{6}{1}-\binom{0}{1}\right]+\left[\binom{5}{1}-\binom{3}{1}\right]+\left[\binom{4}{1}-\binom{2}{1}\right]+\left[\binom{4}{1}-\binom{2}{1}\right]+$$
$$+\left[\binom{4}{1}-\binom{2}{1}-\binom{2}{1}\right]=6+2\cdot 3+0=12;$$
$$R^{11}_{3,2|2}(2)=\left[\binom{6}{2}-\binom{0}{2}-\binom{(3-2)\cdot 3}{1}\binom{4}{2-1-1}\right]+$$
$$+\left[\binom{5}{2}-\binom{3}{2}-\binom{(3-2)\cdot 2}{1}\binom{3}{2-1-1}\right]+\left[\binom{4}{2}-\binom{2}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right]+$$
$$+\left[\binom{4}{2}-\binom{2}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right]+$$
$$+\left[\binom{4}{2}-\binom{2}{2}-\binom{2}{2}+\binom{1}{2}-\binom{(3-2)\cdot 2}{1}\binom{2}{2-1-1}\right]=12+5+3\cdot 2+2=25;$$
$$R^{11}_{3,2|3}(3)=(2-2+1)\,2^3+2^2-2+2-1=11.$$

Here the maximum weight is $w_{\max}=3$.

Example 3. Taking $q=2$, $n=14$, $s=4$, $b=3$, and $w=2$ in Theorem 1, we have $\lambda=2$, $l=14 \bmod 7=0$, $m_1=m_2=\cdots=m_5=6$, $m_6=5$, $m_7=4$, $p_{s+1}=1$, $p_{s+2}=1$, $p_{s+3}=2$, $\beta_0=\beta_1=\cdots=\beta_4=2$, $\beta_5=\beta_6=1$. Then

$$R^{14}_{4,3|1}(1)=\left[\binom{6}{1}-\binom{0}{1}\right]+\left[\binom{6}{1}-\binom{4}{1}\right]+\left[\binom{6}{1}-\binom{4}{1}\right]+\left[\binom{6}{1}-\binom{4}{1}\right]+$$
$$+\left[\binom{6}{1}-\binom{4}{1}\right]+\left[\binom{6}{1}-\binom{4}{1}\right]+$$
$$+\left[\binom{5}{1}-\binom{3}{1}-\binom{2}{1}\right]+\left[\binom{4}{1}-\binom{2}{1}-\binom{1}{1}\right]=6+4\cdot 2+0=14;$$
$$R^{14}_{4,3|2}(2)=\left[\binom{6}{2}-\binom{0}{2}\right]+\left[\binom{6}{2}-\binom{4}{2}\right]+$$
$$+\left[\binom{6}{2}-\binom{4}{2}\right]+\left[\binom{6}{2}-\binom{4}{2}\right]+\left[\binom{6}{2}-\binom{4}{2}\right]+$$
$$+\left[\binom{5}{2}-\binom{4}{2}-\binom{1}{2}+\binom{1}{2}\right]+\left[\binom{4}{2}-\binom{3}{2}-\binom{2}{2}+\binom{1}{2}\right]=15+9\cdot 4+4+2=57;$$

$$R^{14}_{4,3|3}(3) = \left[\binom{6}{3} - \binom{0}{3} - \binom{(3-2)\cdot 2}{1}\binom{4}{3-2-1}\right] +$$
$$+\left[\binom{6}{3} - \binom{4}{3} - \binom{(3-2)\cdot 2}{1}\binom{4}{3-2-1}\right] + \left[\binom{6}{3} - \binom{4}{3} - \binom{(3-2)\cdot 2}{1}\binom{4}{3-2-1}\right] +$$
$$+\left[\binom{6}{3} - \binom{4}{3} - \binom{(3-2)\cdot 2}{1}\binom{4}{3-2-1}\right] +$$
$$+\left[\binom{5}{3} - \binom{4}{3} - \binom{1}{3} + \binom{1}{3} - \binom{(3-2)\cdot 1}{1}\binom{2}{3-2-1}\right] +$$
$$+\left[\binom{4}{3} - \binom{3}{3} - \binom{2}{3} + \binom{1}{3} - \binom{(3-2)\cdot 1}{1}\binom{1}{3-2-1}\right] =$$
$$= (20-2) + (20-4-2)\cdot 4 + (10-4-1) + (4-1-1) = 81;$$
$$R^{14}_{4,3|4}(4) = (4+1)\cdot 3^2 + 3^{2-1} - 4 - 1 = 43.$$

Here the maximum weight is $w_{\max} = 4$.

Theorem 2. The average weight of a vector of the set $\xi_{(s,b|w),n,q}$ is

$$\sum_{j=1}^{w_{\max}} jR^n_{s,b|w}(j) \Big/ \sum_{j=1}^{w_{\max}} R^n_{s,b|w}(j),$$

where $R^n_{s,b|w}(j)$ is given by Theorem 1.

Proof. By Theorem 1, the number of vectors of $\xi_{(s,b|w),n,q}$ having Hamming weight j is $R^n_{s,b|w}(j)$, and the total weight of all vectors of $\xi_{(s,b|w),n,q}$ is given by $\sum\limits_{j=1}^{w_{\max}} jR^n_{s,b|w}(j)$. The ratio gives the required average weight. ■

3. Existence of LDP$_{(s,b|w),n,q}$RC-codes

In this section, we obtain necessary and sufficient conditions for the existence of q-ary LDP$_{(s,b|w),n,q}$RC-codes. We also derive an upper bound on the number of codewords for such a code. We also construct examples based on the results.

Theorem 3. Every (n,k) LDP$_{(s,b|w),n,q}$RC-code satisfies

$$n - k \geqslant \log_q \left[1 + \sum_{j=1}^{w_{\max}} R^n_{s,b|w}(j)\right], \text{ where } R^n_{s,b|w}(j) \text{ is given by Theorem 1.}$$

Proof. By Theorem 1, the number of error vectors of $\xi_{(s,b|w),n,q}$ including the zero vector is $1 + |\xi_{(s,b|w),n,q}| = 1 + \sum\limits_{j=1}^{w_{\max}} R^n_{s,b|w}(j)$. As the maximum available coset is q^{n-k} and LDP$_{(s,b|w),n,q}$RC-code corrects all such errors, we have

$$q^{n-k} \geqslant 1 + \sum_{j=1}^{w_{\max}} R^n_{s,b|w}(j) \implies n - k \geqslant \log_q \left[1 + \sum_{j=1}^{w_{\max}} R^n_{s,b|w}(j)\right].$$

Theorem 3 is proven. ■

Remark 2. The maximum number of codewords of an (n,k) LDP$_{(s,b|w),n,q}$RC-code is

$$M \leqslant \frac{q^n}{1 + \sum\limits_{j=1}^{w_{\max}} R^n_{s,b|w}(j)}.$$

In the following theorem, we apply the well known technique used in Varshamov — Gilbert — Sacks bound (see [7] and [8, Theorem 4.7]).

Theorem 4. For existence of an (n, k) $\mathrm{LDP}_{(s,b|w),n,q}$RC-code, the following condition is sufficient:

$$q^{n-k} > \sum_{j=0}^{w-1} \binom{b-1}{j}(q-1)^j \left(\sum_{j=0}^{w} \binom{b-1}{j}(q-1)^j \right)^{\lambda-1} \sum_{j=0}^{\min\{w,g\}} \binom{g}{j}(q-1)^j \left(1 + \sum_{j=1}^{w_{\max}} R_{s,b|w}^{n-b}(j) \right), \tag{1}$$

where $g = \gamma(l)$ and $R_{s,b|w}^{n-b}(j)$ is given by Theorem 1. Here $\sum\limits_{j=0}^{\min\{w,g\}} \binom{g}{j}(q-1)^j = 1$ for $g = 0$.

Proof. The proof is done by constructing an appropriate $(n-k) \times n$ parity-check matrix H of the code. Suppose that the first $n-1$ columns $h_1, h_2, h_3, \ldots, h_{n-1}$ are added suitably to H. Then any (nonzero) column h_n is added to H provided that it is not a linear combination of at most $w-1$ columns among the immediately preceding $b-1$ columns together with at most w columns from each set of previous b consecutive columns which are at gap of s columns (the last set may contain less than b columns), along with a linear combination of at most w columns from each set of b consecutive columns which are at gap of s columns confined to the first $n-b$ columns (the last set may contain less than b columns). This can be written as

$$\begin{aligned} h_n \neq & \left(\sum_{i=1}^{b-1} a_{i1} h_{n-i} + \sum_{i=0}^{b-1} b_{i1} h_{n-(s+b)-i} + \sum_{i=0}^{b-1} b_{i2} h_{n-2(s+b)-i} + \ldots + \sum_{i=0}^{g-1} b_{i\lambda} h_{n-\lambda(s+b)-i} \right) + \\ & + \left(\sum_{i=0}^{b-1} \alpha_{i1} h_{j'-i} + \sum_{i=0}^{b-1} \beta_{i1} h_{j'-(s+b)-i} + \sum_{i=0}^{b-1} \beta_{i2} h_{j'-2(s+b)-i} + \ldots + \sum_{i=0}^{g'-1} \beta_{i\lambda'} h_{j'-\lambda'(s+b)-i} \right), \end{aligned} \tag{2}$$

where $a_{ij}, b_{ij}, \alpha_{ij}, \beta_{ij} \in \mathrm{GF}(q)$ such that the number of nonzero a_{ij} is at most $w-1$, and that of b_{ij}, α_{ij}, β_{ij} is at most w; $j' \leqslant n-b$; $g = \gamma\big(n \bmod (s+b)\big) = \gamma(l)$, $g' = \gamma\big((n-b-j'+1) \bmod (s+b)\big)$, and $\lambda' = \left\lfloor \dfrac{n-b}{s+b} \right\rfloor$.

The number of coefficients a_{i1} is $\sum\limits_{j=0}^{w-1} \binom{b-1}{j}(q-1)^j$.

The number of coefficients b_{ij} is $\left(\sum\limits_{j=0}^{w} \binom{b-1}{j}(q-1)^j \right)^{\lambda-1} \sum\limits_{j=0}^{\min\{w,g\}} \binom{g}{j}(q-1)^j$. So the number of all possible linear combinations in the first bracket of the right-hand side (2) is

$$\sum_{j=0}^{w-1} \binom{b-1}{j}(q-1)^j \left(\sum_{j=0}^{w} \binom{b-1}{j}(q-1)^j \right)^{\lambda-1} \sum_{j=0}^{\min\{w,g\}} \binom{g}{j}(q-1)^j.$$

The second bracket in (2) gives the total number of low-density periodic random error in a vector of length $n-b$. This is given by Theorem 3 as $1 + \sum\limits_{j=1}^{w_{\max}} R_{s,b|w}^{n-b}(j)$. Therefore, the total number of all the possible linear combinations of the right-hand side (2) is

$$\sum_{j=0}^{w-1} \binom{b-1}{j}(q-1)^j \left(\sum_{j=0}^{w} \binom{b-1}{j}(q-1)^j \right)^{\lambda-1} \sum_{j=0}^{\min\{w,g\}} \binom{g}{j}(q-1)^j \left(1 + \sum_{j=1}^{w_{\max}} R_{s,b|w}^{n-b}(j) \right). \tag{3}$$

Since we have at most q^{n-k} columns, so taking q^{n-k} greater than or equal to the term computed in (3) gives the sufficient condition for the existence of the required code. ■

In the following examples, λ', p'_i, and β'_j represent the values of λ, p_i, and β_j respectively, when n is replaced by $n-b$.

Example 4. Consider $n=11$, $s=3$, $b=2$, $w=1$, and $q=3$ in Theorem 4, then $\lambda=2$, $l=11 \bmod 5=1$, $\lambda'=1$, $p'_{s+1}=1$, $p'_{s+2}=1$, $\beta'_0=\beta'_1=\beta'_2=2$, $\beta'_3=\beta'_4=1$. Putting these values in the inequality (1), we get

$$3^{n-k} > \sum_{j=0}^{0}\binom{1}{j}(3-1)^j\left(\sum_{j=0}^{1}\binom{2-1}{j}(3-1)^j\right)^{1}\sum_{j=0}^{\min\{w=1,g=1\}}\binom{1}{j}(3-1)^j\left(1+\sum_{j=1}^{3}R_{3,2|1}^{11-2}(j)\right) =$$
$$= 1\cdot 3\cdot 3\,(1+66)\ \big[\text{Using Theorem 1 and Example 1}\big] = 603.$$

This implies $n-k \geqslant 6$. Thus, we can construct a parity check matrix H of order 6×11, which generates the $(11,5)$ ternary $\mathrm{LDP}_{(3,2|1),11,3}$RC-code:

$$H=\begin{bmatrix} 1 & 0 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\ 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 1 & 0 & 0\\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0\\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 \end{bmatrix}.$$

It can be verified from the Error Pattern-Syndromes Table 1 that the syndromes of all the errors are nonzero and distinct, showing that the code is a $(11,5)$ ternary $\mathrm{LDP}_{(3,2|1),11,3}$RC-code.

Table 1

Error Pattern-Syndrome

Error Patterns	Syndromes	Error Patterns	Syndromes
00 000 00 000 1	001002	20 000 02 000 2	210000
00 000 00 000 2	002001	10 000 10 000 1	221000
00 000 01 000 0	002000	10 000 10 000 2	222000
00 000 02 000 0	001000	10 000 20 000 1	021000
00 000 10 000 0	100000	10 000 20 000 2	022002
00 000 20 000 0	200000	20 000 10 000 1	011001
00 000 01 000 1	000002	20 000 10 000 2	012000
00 000 01 000 2	001001	20 000 20 000 1	111001
00 000 02 000 1	002002	20 000 20 000 2	112000
00 000 02 000 2	000001	0 00 000 01 000	000100
00 000 10 000 1	101002	0 00 000 02 000	000200
00 000 10 000 2	102001	0 01 000 00 000	200010
00 000 20 000 1	201002	0 02 000 00 000	100020
00 000 20 000 2	202001	0 01 000 01 000	200110
01 000 00 000 0	010100	0 01 000 02 000	200210
02 000 00 000 0	020200	0 02 000 10 000	100120
01 000 00 000 1	011102	0 02 000 20 000	100220
01 000 00 000 2	012101	0 01 000 10 000	202010
02 000 00 000 1	021202	0 01 000 20 000	201010
02 000 00 000 2	022201	0 02 000 10 000	102010
01 000 01 000 0	012100	0 02 000 20 000	101020
01 000 02 000 0	011100	0 10 000 01 000	010200
02 000 01 000 0	022200	0 10 000 02 000	010000

End of Table 1

Error Patterns	Syndroms	Error Patterns	Syndromes
02 000 02 000 0	021200	0 20 000 10 000	020000
01 000 10 000 0	110100	0 20 000 20 000	020100
01 000 20 000 0	210100	00 00 000 01 00	111111
02 000 10 000 0	120200	00 00 000 02 00	222222
02 000 20 000 0	220200	00 01 000 00 00	100111
01 000 01 000 1	010102	00 02 000 00 00	200222
01 000 01 000 2	011101	00 01 000 01 00	211222
01 000 02 000 1	012102	00 01 000 02 00	022000
01 000 02 000 2	010101	00 02 000 01 00	011000
02 000 01 000 1	020202	00 02 000 02 00	122111
02 000 01 000 2	021201	00 01 000 10 00	100211
02 000 02 000 1	022202	00 01 000 20 00	100011
02 000 02 000 2	020201	00 02 000 10 00	200022
01 000 10 000 1	111102	00 02 000 20 00	200122
01 000 10 000 2	112101	00 10 000 01 00	011121
01 000 20 000 1	211102	00 10 000 02 00	122202
01 000 20 000 2	212101	00 20 000 01 00	211101
02 000 10 000 1	121202	00 20 000 02 00	022212
02 000 10 000 2	122201	000 00 000 01 0	000010
02 000 20 000 1	221202	000 00 000 02 0	000020
02 000 20 000 2	222201	000 01 000 00 0	000200
10 000 00 000 0	120001	000 02 000 00 0	000100
20 000 00 000 0	210002	000 01 000 01 0	000210
10 000 00 000 1	121000	000 01 000 02 0	000220
10 000 00 000 2	122002	000 02 000 01 0	000110
20 000 00 000 1	211001	000 02 000 02 0	000120
20 000 00 000 2	212000	000 01 000 10 0	112011
10 000 01 000 0	122001	000 01 000 20 0	222122
10 000 02 000 0	121001	000 02 000 10 0	111211
20 000 01 000 0	212002	000 02 000 20 0	222022
20 000 02 000 0	211002	000 10 000 01 0	100121
10 000 10 000 0	220001	000 10 000 02 0	100101
10 000 20 000 0	020001	000 20 000 01 0	200202
20 000 10 000 0	010002	000 20 000 02 0	200212
20 000 20 000 0	110002	0000 01 000 10	100010
10 000 01 000 1	120000	0000 01 000 20	100020
10 000 01 000 2	121002	0000 02 000 10	200010
10 000 02 000 1	122000	0000 02 000 20	200020
10 000 02 000 2	120002	0000 10 000 01	001202
20 000 01 000 1	210001	0000 10 000 02	002201
20 000 01 000 2	211000	0000 20 000 01	001102
20 000 02 000 1	212001	0000 20 000 02	002101

Example 5. Consider $n = 12$, $s = 3$, $b = 2$, $w = 1$, and $q = 2$ in Theorem 4, then $\lambda = 2$, $l = 12 \bmod 5 = 2$, $\lambda' = 2$, $p'_{s+1} = 1$, $p'_{s+2} = 1$, $\beta'_0 = \beta'_1 = \cdots = \beta'_3 = 2$, $\beta'_4 = 1$. From inequality (1), we get

$$2^{n-k} > \sum_{j=0}^{0} \binom{2-1}{j} (2-1)^j \left(\sum_{j=0}^{1} \binom{2-1}{j} (2-1)^j \right)^{1 \min\{w=1,g=2\}} \sum_{j=0} \binom{2}{j} (2-1)^j \left(1 + \sum_{j=1}^{3} R_{3,2|1}^{12-2}(j) \right) =$$

$$= 1 \cdot 2^1 \cdot 3\,(1 + 24) = 150.$$

This implies $n-k \geqslant 8$, which gives rise to a $(12,4)$ binary $\mathrm{LDP}_{(3,2|1),12,2}$RC-code and its parity check matrix H is given by

$$H = \left[\begin{array}{cccccccccccc} 1&0&0&0&0&0&0&0&0&1&1&1\\ 0&1&0&0&0&0&0&0&0&1&0&1\\ 0&0&1&0&0&0&0&0&1&1&1&0\\ 0&0&0&1&0&0&0&0&1&1&0&1\\ 0&0&0&0&1&0&0&0&0&1&1&0\\ 0&0&0&0&0&1&0&0&1&1&0&0\\ 0&0&0&0&0&0&1&0&0&1&1&1\\ 0&0&0&0&0&0&0&1&0&1&0&1 \end{array}\right].$$

It can be verified like the previous one that the syndromes of all the errors are nonzero and distinct, so the code is a $(12,4)$ binary $\mathrm{LDP}_{(3,2|1),12,2}$RC-code.

Example 6. Consider $n=14$, $s=4$, $b=3$, $w=2$, and $q=2$ in Theorem 4, then $\lambda=2$, $l=14 \bmod 7=0$, $\lambda'=1$, $p'_{s+1}=1$, $p'_{s+2}=1$, $p'_{s+3}=2$, $\beta'_0=\beta'_1=\beta'_2=2$, $\beta'_3=\beta'_4=\beta'_5=\beta'_6=1$. Inequality (1) gives

$$2^{n-k} > \sum_{j=0}^{2-1}\binom{3-1}{j}(2-1)^j\left(\sum_{j=0}^{2}\binom{3-1}{j}(2-1)^j\right)^{1}\sum_{j=0}^{\min\{w=2,g=0\}}\binom{g}{j}(2-1)^j\left(1+\sum_{j=1}^{4}R_{4,3|2}^{14-3}(j)\right)=$$
$$= 3\cdot 4^1\cdot 1\,(1+135)=1632.$$

This implies $n-k \geqslant 11$ which leads to a $(14,3)$ binary $\mathrm{LDP}_{(3,2|2),14,2}$RC-code with parity check matrix

$$H = \left[\begin{array}{cccccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&1&1&1\\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1\\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1\\ 0&0&0&0&0&1&0&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&1&0&0&0&0&1&1&0\\ 0&0&0&0&0&0&0&1&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&1&0&0&1&1&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&0&1&1 \end{array}\right].$$

Here we can also verify that all error patterns give nonzero and distinct syndromes.

Finally, we give the probability of decoding error for a $\mathrm{LDP}_{(s,b|w),n,q}$RC-code over a binary symmetric channel.

Theorem 5. Let $\mathrm{PD}_R(E)$ be the probability of decoding error of an (n,k) binary $\mathrm{LDP}_{(s,b|w),n,2}$RC-code on a binary symmetric channel with transition probability ϵ, then

$$\mathrm{PD}_R(E) = 1-\sum_{j=1}^{w_{\max}} R_{s,b|w}^{n}(j)\,\epsilon^j(1-\epsilon)^{n-j}, \quad \text{where } R_{s,b|w}^{n}(j) \text{ is given by Theorem 1.}$$

Proof. Since the binary symmetric channel has the transition probability ϵ, the probability of occurring of any one of the error vector of weight j is $\epsilon^j(1-\epsilon)^{n-j}$. So the probability of occurring of any error vector from the set $\xi_{(s,b|w),n,q}$ is $\sum_{j=1}^{w_{\max}} R_{s,b|w}^{n}(j)\,\epsilon^j(1-\epsilon)^{n-j}$.

Since the code corrects all such error patterns, the probability of a decoding error of the code is $\mathrm{PD}_R(E) = 1 - \sum_{j=1}^{w_{\max}} R^n_{s,b|w}(j)\,\epsilon^j(1-\epsilon)^{n-j}$. ■

Remark 3. For $s = 3$, $b = 2$, and $\epsilon = 0.1$, we determine the probability of decoding error $\mathrm{PD}_R(E)$ of binary $\mathrm{LDP}_{(s,b|w),n,2}$RC-codes of different lengths as follows (Table 2).

Table 2
Values of $\mathbf{PD}_R(E)$

n	λ	l	$\mathrm{PD}_R(E)$
10	2	0	0.19
11	2	1	0.21
12	2	2	0.23
13	2	3	0.29
14	2	4	0.31
15	3	0	0.33

We find that the probability of decoding error of $\mathrm{LDP}_{(s,b|w),n,q}$RC-code increases as the length of the code increases. So a smaller length code is more efficient.

4. Conclusion

This paper derives the weight distribution of low-density periodic random errors. Then necessary and sufficient conditions for the existence of linear codes that correct such errors, along with the error decoding probability of the codes, are presented. It can be interesting to explore some more systematic methods by which we can construct such codes. We can also investigate array code or cyclic code instead of linear code that can deal with such errors.

5. Acknowledgement

The first author is supported by JRF fellowship from Council of Scientific and Industrial Research, India (File No. 09/796(0085)/2018-EMR-I).

REFERENCES

1. *Lange N.* Error correcting codes on periodically disturbed data channels. Proc. IEEE Intern. Symp. Inform. Theory, Trondheim, Norway, 1994, p. 33.
2. *Das P. K.* Codes on s-periodic random errors of length b. Palestine J. Math., 2014, vol. 3, no. 2, pp. 168–174.
3. *Das P. K. and Haokip L.* Correction and weight distribution of periodic random errors. Science & Technology Asia, 2021, vol. 26, no. 4, pp. 38–47.
4. *Wyner A. D.* Low-density-burst-correcting codes. IEEE Trans. Inform. Theory, 1963, vol. 9, no. 2, p. 124.
5. *Fire P.* A Class of Multiple-error-correcting Binary Codes for Non-independent Errors. Stanford University, 1959. 104 p.
6. *Das P. K. and Haokip L.* Periodical burst error correcting codes with decoding error probability. Discr. Math. Lett., 2022, vol. 8, pp. 49–56.
7. *Sack G. E.* Multiple burst error correction by means of parity-checks. IRE Trans. Inform. Theory, 1958, vol. 4, no. 4, pp. 145–147.
8. *Peterson W. W. and Weldon E. J.* Error Correcting Codes. 2nd ed. Cambridge, Massachusetts, MIT Press, 1972.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/62/9

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ ИЗВЛЕЧЕНИЯ КВАДРАТНОГО КОРНЯ ПО ПРОСТОМУ МОДУЛЮ[1]

А. Н. Рыбалов

Институт математики им. С. Л. Соболева СО РАН, г. Омск, Россия

E-mail: alexander.rybalov@gmail.com

Изучается генерическая сложность проблемы извлечения квадратного корня по простому модулю. Вопрос о вычислительной сложности этой проблемы до сих пор открыт. Однако известны алгоритмы (например, алгоритм Чиполлы), которые являются полиномиальными при условии истинности расширенной гипотезы Римана. Доказывается, что проблема является генерически разрешимой за полиномиальное время. Фактически это означает, что алгоритм Чиполлы работает за полиномиальное время для «почти всех» входов. Понятие «почти все» формализуется введением асимптотической плотности на множестве входных данных.

Ключевые слова: *генерическая сложность, квадратный корень по простому модулю.*

ON THE GENERIC COMPLEXITY OF THE SQUARE ROOT MODULO PRIME PROBLEM

A. N. Rybalov

Sobolev Institute of Mathematics, Omsk, Russia

We study the generic complexity of the problem of finding a square root modulo a prime number. The question about the computational complexity of this problem is still open. However, there are known algorithms (e.g. Cipolla's algorithm) which are polynomial if the extended Riemann hypothesis holds. We prove that this problem is generically decidable in polynomial time. In fact, this means that Cipolla's algorithm runs in polynomial time for "almost all" inputs. The notion "almost all" is formalized by introducing the asymptotic density on a set of input data.

Keywords: *generic complexity, square root modulo prime.*

Введение

Проблема нахождения квадратного корня по простому модулю является классической алгоритмической проблемой теории чисел, восходящей ещё к Эйлеру и Гауссу. В отличие от других классических проблем, таких, как проблема факторизации целых

[1]Работа поддержана грантом Российского научного фонда № 22-11-20019.

чисел или проблема дискретного логарифма, известны алгоритмы, которые решают её за полиномиальное время при условии истинности некоторых гипотез теории чисел. Например, алгоритм Чиполлы [1] является полиномиальным при условии истинности расширенной гипотезы Римана [2]. Проблема распознавания существования квадратного корня по простому модулю значительно проще — для неё известен эффективный критерий Эйлера.

Генерический подход [3] — это один из подходов к изучению алгоритмических проблем для «почти всех» входов. В рамках этого подхода алгоритмическая проблема рассматривается не на всём множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

В данной работе изучается генерическая сложность проблемы извлечения квадратного корня по простому модулю. Доказывается, что эта проблема генерически разрешима за полиномиальное время. Отметим, что для составного модуля неизвестно полиномиального алгоритма даже для распознавания существования квадратного корня [4]. Для данной проблемы получен результат об отсутствии полиномиальных генерических алгоритмов [5].

1. Предварительные сведения

Пусть p — простое число. Натуральное число $a < p$ называется *квадратичным вычетом*, если существует такое натуральное $x < p$, что $x^2 = a \pmod p$. В противном случае a называется *квадратичным невычетом*. Есть эффективный критерий проверки, является ли натуральное число квадратичным вычетом по простому модулю.

Теорема 1 (Эйлер). Пусть p — нечётное простое число. Натуральное число a является квадратичным вычетом по модулю p тогда и только тогда, когда

$$a^{(p-1)/2} = 1 \pmod p.$$

Из этой теоремы следует, что проблема распознавания квадратичных вычетов по простому модулю разрешима за полиномиальное время.

Проблема извлечения квадратного корня по простому модулю состоит в следующем. Даны простое число p и натуральное число $a < p$, записанные в двоичной системе. Необходимо найти натуральное число $x < p$, такое, что $x^2 = a \pmod p$, если это возможно, либо выдать ответ -1.

В отличие от проблемы распознавания квадратичных вычетов, для извлечения квадратного корня не доказана разрешимость за полиномиальное время [4]. Однако существует алгоритм Чиполлы [1], который решает эту задачу за полиномиальное время при условии знания какого-нибудь квадратичного невычета b по модулю p.

Алгоритм Чиполлы:

1) Вход: p, a и квадратичный невычет b.
2) Квадратный корень получается вычислением по формуле $x = \left(a + \sqrt{b}\right)^{(p+1)/2}$ в поле $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{b})$ — квадратичном расширении поля $\mathbf{F}_p$.

Обозначим через $\eta(p)$ наименьший квадратичный невычет по модулю p. Н. Анкени доказал [2], что в предположении истинности расширенной гипотезы Римана существует константа C, такая, что для любого простого p имеет место $\eta(p) < C(\log p)^2$. Здесь

и далее под $\log p$ понимается логарифм по основанию 2. Таким образом, в предположении истинности расширенной гипотезы Римана квадратичный невычет может быть найден за полиномиальное время и алгоритм Чиполлы становится полиномиальным.

2. Основной результат

Определение генерического полиномиального алгоритма можно найти в [3, 5].

Множество входов проблемы извлечения квадратного корня по простому модулю есть

$$I = \{(p, a) : p \text{ простое}, \ 0 < a < p\}.$$

Под размером входа (p, a) будем понимать длину двоичной записи числа p. Таким образом, множество входов размера n есть

$$I_n = \{(p, a) : (p, a) \in I, \ 2^n < p < 2^{n+1}\}.$$

Для конечного множества A через $|A|$ обозначается число его элементов; функция $\pi(x)$ задаёт количество простых чисел, не превосходящих x.

Лемма 1. Для достаточно больших n имеет место

$$\frac{2^{2n}}{n} < |I_n| < \frac{2^{2(n+1)}}{n}.$$

Доказательство. Заметим, что

$$|I_n| = \sum_{2^n < p < 2^{n+1}} p,$$

где суммирование идёт по простым числам. Отсюда

$$2^n(\pi(2^{n+1}) - \pi(2^n)) < |I_n| < 2^{n+1}(\pi(2^{n+1}) - \pi(2^n)). \tag{1}$$

Из асимптотического закона распределения простых чисел следует, что для достаточно больших n имеет место

$$\frac{0{,}9 \cdot 2^n}{n \ln 2} < \pi(2^n) < \frac{1{,}1 \cdot 2^n}{n \ln 2},$$

а также

$$\frac{0{,}9 \cdot 2^{n+1}}{(n+1) \ln 2} < \pi(2^{n+1}) < \frac{1{,}1 \cdot 2^{n+1}}{(n+1) \ln 2}.$$

Поэтому

$$\frac{0{,}9 \cdot 2^{n+1}}{(n+1) \ln 2} - \frac{1{,}1 \cdot 2^n}{n \ln 2} < \pi(2^{n+1}) - \pi(2^n) < \frac{1{,}1 \cdot 2^{n+1}}{(n+1) \ln 2} - \frac{0{,}9 \cdot 2^n}{n \ln 2}.$$

Отсюда получаем

$$\frac{2^n}{n} < \pi(2^{n+1}) - \pi(2^n) < \frac{2^{n+1}}{n},$$

что вместе с (1) даёт нужную оценку. ■

Рассмотрим следующее множество входов проблемы извлечения корня:

$$\mathcal{S} = \{(p, a) : (p, a) \in I, \ \eta(p) > 21 \log p\}.$$

Лемма 2. Для достаточно больших n имеет место

$$\frac{|\mathcal{S} \cap I_n|}{|I_n|} < \frac{1}{n}.$$

Доказательство. П. Эрдеш доказал [6], что существует константа C, $3 < C < 4$, такая, что

$$\lim_{k\to\infty} \frac{\sum\limits_{p\leqslant k} \eta(p)}{\pi(k)} = C.$$

Здесь суммирование берётся по простым p. Отсюда следует, что для достаточно больших k имеет место

$$3\pi(k) < \sum_{p\leqslant k} \eta(p) < 4\pi(k).$$

Используя это неравенство, оценим сумму

$$\sum_{2^n<p<2^{n+1}} \eta(p) = \sum_{p<2^{n+1}} \eta(p) - \sum_{p<2^n} \eta(p)$$

следующим образом:

$$3\pi(2^{n+1}) - 4\pi(2^n) < \sum_{2^n<p<2^{n+1}} \eta(p) < 4\pi(2^{n+1}) - 3\pi(2^n).$$

Используя асимптотический закон распределения простых чисел, для достаточно больших n получаем

$$\frac{2^{n+1}}{n} < \sum_{2^n<p<2^{n+1}} \eta(p) < \frac{10\cdot 2^n}{n}.$$

Из этих неравенств следует, что

$$\sum_{2^n<p<2^{n+1}} \eta(p)\, p < 2^{n+1} \sum_{2^n<p<2^{n+1}} \eta(p) < \frac{20\cdot 2^{2n}}{n}. \tag{2}$$

Допустим теперь, что лемма неверна, то есть существуют сколь угодно большие n, такие, что

$$\frac{|\mathcal{S} \cap I_n|}{|I_n|} > \frac{1}{n},$$

то есть

$$|\mathcal{S} \cap I_n| > \frac{|I_n|}{n}.$$

Заметим, что

$$|\mathcal{S} \cap I_n| = \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} p.$$

Тогда

$$\sum_{2^n<p<2^{n+1}} \eta(p)\, p = \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} \eta(p)\, p + \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)\leqslant 21n}} \eta(p)\, p \geqslant$$

$$\geqslant 21n \sum_{\substack{2^n<p<2^{n+1},\\ \eta(p)>21n}} p > 21n\, \frac{|I_n|}{n} = 21|I_n| > \frac{21\cdot 2^{2n}}{n}.$$

Последняя оценка следует из леммы 1. Но это противоречит оценке сверху (2). ■

Теорема 2. Проблема извлечения квадратного корня по простому модулю генерически разрешима за полиномиальное время.

Доказательство. Полиномиальный генерический алгоритм работает на входе (p, a) размера n следующим образом:

1) С помощью критерия Эйлера проверяет, является ли a квадратичным вычетом по модулю p. Если не является, выдаёт -1. Иначе переходит к следующему шагу.
2) Ищет среди чисел от 2 до $21n$ квадратичный невычет с помощью критерия Эйлера.
3) Если квадратичный невычет не найден, то выдаёт ответ «НЕ ЗНАЮ».
4) Если найден квадратичный невычет, то с его помощью по алгоритму Чиполлы находится квадратный корень из a по модулю p.

Генеричность этого алгоритма следует из того, что множество входов, на которых алгоритм выдаёт ответ «НЕ ЗНАЮ», является пренебрежимым, согласно лемме 2. ■

ЛИТЕРАТУРА

1. *Cipolla M.* Un metodo per la risoluzione della congruenza di secondo grado // Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche. Napoli, 1904. V. 10. No. 3. P. 144–150. (in Italian)
2. *Ankeny N. C.* The least quadratic non residue // Ann. Math. 1952. V. 55. P. 65–72.
3. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
4. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II // LNCS. 1994. V. 877. P. 291–322.
5. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2(28). С. 54–58.
6. *Erdos P.* Remarks on number theory I // Mat. Lapok. 1961. V. 12. P. 10–17.

REFERENCES

1. *Cipolla M.* Un metodo per la risoluzione della congruenza di secondo grado. Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche. Napoli, 1904, vol. 10, no. 3, pp. 144–150. (in Italian)
2. *Ankeny N. C.* The least quadratic non residue. Ann. Math., 1952, vol. 55, pp. 65–72.
3. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694.
4. *Adleman L. M. and McCurley K. S.* Open problems in number theoretic complexity, II. LNCS, 1994, vol. 877, pp. 291–322.
5. *Rybalov A. N.* O genericheskoy slozhnosti problemy raspoznavaniya kvadratichnykh vychetov [On generic complexity of the quadratic residuosity problem]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 54–58. (in Russian)
6. *Erdos P.* Remarks on number theory I. Mat. Lapok., 1961, vol. 12, pp. 10–17.

СВЕДЕНИЯ ОБ АВТОРАХ

АЛЕКСЕЕВ Евгений Константинович — кандидат физико-математических наук, начальник отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва. E-mail: **alekseev@cryptopro.ru**

АХМЕТЗЯНОВА Лилия Руслановна — кандидат физико-математических наук, заместитель начальника отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва. E-mail: **lah@cryptopro.ru**

БАБУЕВА Александра Алексеевна — ведущий инженер-аналитик отдела криптографических исследований ООО «КРИПТО-ПРО», г. Москва.
E-mail: **babueva@cryptopro.ru**

БЕТЕРОВ Илья Игоревич — кандидат физико-математических наук, научный сотрудник Института физики полупроводников им. А. В. Ржанова, г. Новосибирск.
E-mail: **beterov@isp.nsc.ru**

БОНИЧ Татьяна Андреевна — аспирантка Новосибирского государственного университета, г. Новосибирск. E-mail: **t.bonich@g.nsu.ru**

ГАЙДАМАКИН Николай Александрович — доктор технических наук, профессор, профессор кафедры алгебры и фундаментальной информатики Уральского федерального университета имени первого Президента России Б. Н. Ельцина, г. Екатеринбург. E-mail: **n.a.gaidamakin@urfu.ru**

ГОРОДИЛОВА Анастасия Александровна — кандидат физико-математических наук, старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **gorodilova@math.nsc.ru**

ДУПЛЕНКО Александр Геннадьевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград. E-mail: **dvplenko@mail.ru**

ИДРИСОВА Валерия Александровна — кандидат физико-математических наук, ассистент Новосибирского государственного университета, г. Новосибирск.
E-mail: **vvitkup@yandex.ru**

ИЩУКОВА Евгения Александровна — кандидат технических наук, доцент ИКТИБ ЮФУ, г. Таганрог. E-mail: **uaishukova@sfedu.ru**

КОЛОМЕЕЦ Николай Александрович — кандидат физико-математических наук, старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **kolomeec@math.nsc.ru**

КУНИНЕЦ Артем Андреевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград.
E-mail: **artkuninets@yandex.ru**

КУЦЕНКО Александр Владимирович — кандидат физико-математических наук, старший преподаватель Новосибирского государственного университета, г. Новосибирск. E-mail: **alexandrkutsenko@bk.ru**

МАЛЫГИНА Екатерина Сергеевна — кандидат физико-математических наук, доцент департамента прикладной математики МИЭМ НИУ ВШЭ, г. Москва.
E-mail: **emalygina@hse.ru**

МИРОНКИН Владимир Олегович — кандидат физико-математических наук, доцент базовой кафедры № 252 информационной безопасности МИРЭА — Российского технологического университета, г. Москва. E-mail: **mironkin.v@mail.ru**

НЕЙМАН Даниил Яковлевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград. E-mail: **reterior@yandex.ru**

ПАНКРАТОВА Ирина Анатольевна — кандидат физико-математических наук, доцент, заведующая лабораторией Томского государственного университета, г. Томск. E-mail: **pank@mail.tsu.ru**

ПАНФЕРОВ Матвей Андреевич — аспирант Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **m.panferov@g.nsu.ru**

ПОПКОВ Кирилл Андреевич — доктор физико-математических наук, старший научный сотрудник Института прикладной математики им. М. В. Келдыша РАН, г. Москва. E-mail: **kirill-formulist@mail.ru**

ПУДОВКИНА Марина Александровна — доктор физико-математических наук, профессор Национального исследовательского ядерного Университета «МИФИ», г. Москва. E-mail: **maricap@rambler.ru**

РАТОЧКА Вячеслав Леонидович — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград. E-mail: **willenst@gmail.com**

РЫБАЛОВ Александр Николаевич — кандидат физико-математических наук, старший научный сотрудник лаборатории комбинаторных и вычислительных методов алгебры и логики Института математики им. С. Л. Соболева СО РАН, г. Омск.
E-mail: **alexander.rybalov@gmail.com**

ТАРАСКИН Олег Геннадьевич — главный инженер-криптограф, Waves, г. Москва.
E-mail: **tog.postquant@gmail.com**

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, доцент Новосибирского государственного университета, г. Новосибирск.
E-mail: **crypto1127@mail.ru**

УДОВЕНКО Алексей Николаевич — кандидат физико-математических наук, CryptoExperts, г. Париж. E-mail: **aleksei.udovenko1@gmail.com**

DAS Pankaj Kumar — Department of Mathematical Sciences, Tezpur University, Napaam, Sonitpur, Assam-784028, India. E-mail: **pankaj4thapril@yahoo.co.in**

HAOKIP Letminthang — Department of Mathematical Sciences, Tezpur University, Napaam, Sonitpur, Assam-784028, India. E-mail: **h_letminthang@yahoo.com**

Журнал «Прикладная дискретная математика» входит в перечень ВАК рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание учёной степени кандидата и доктора наук по специальностям 2.3.5. «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» (технические науки), 2.3.6. «Методы и системы защиты информации, информационная безопасность» (физико-математические и технические науки), 1.1.5. «Математическая логика, алгебра, теория чисел и дискретная математика» (физико-математические науки), 1.2.3. «Теоретическая информатика, кибернетика» (физико-математические науки), а также в перечень журналов, рекомендованных ФУМО ВО ИБ в качестве учебной литературы по специальности «Компьютерная безопасность».

Журнал индексируется в базах данных Web of Science (Emerging Sources Citation Index (ESCI) и Russian Science Citation Index (RSCI)), Scopus, MathSciNet и Zentralblatt MATH. В сводном рейтинге журналов RSCI 2022 г. он отнесён к первому квартилю (Q1).

Журнал «Прикладная дискретная математика» распространяется по подписке; его подписной индекс 38696 в объединённом каталоге «Пресса России». Полнотекстовые электронные версии вышедших номеров журнала доступны на его сайте journals.tsu.ru/pdm и на Общероссийском математическом портале www.mathnet.ru. На сайте журнала можно найти также правила подготовки рукописей статей для публикации в журнале.

Тематика публикаций журнала:

- *Теоретические основы прикладной дискретной математики*
- *Математические методы криптографии*
- *Математические методы стеганографии*
- *Математические основы компьютерной безопасности*
- *Математические основы надёжности вычислительных и управляющих систем*
- *Прикладная теория кодирования*
- *Прикладная теория автоматов*
- *Прикладная теория графов*
- *Логическое проектирование дискретных автоматов*
- *Математические основы информатики и программирования*
- *Вычислительные методы в дискретной математике*
- *Математические основы интеллектуальных систем*
- *Исторические очерки по дискретной математике и её приложениям*