ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.17 DOI 10.17223/20710410/65/5

ПОСТРОЕНИЕ КВАЗИЦИКЛИЧЕСКИХ АЛЬТЕРНАНТНЫХ КОДОВ И ИХ ПРИЛОЖЕНИЕ В КОДОВЫХ КРИПТОСИСТЕМАХ[1]

А. А. Кунинец*, Е. С. Малыгина**

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

E-mail: artkuninets@yandex.ru, emalygina@hse.ru

Представлен обзор квазициклических альтернантных кодов и их структурный анализ относительно классификации автоморфизмов. Детализированы методы восстановления структурной информации о коде, которые, в свою очередь, снабжены подробными примерами. Привлекательность рассматриваемого семейства кодов заключается в его возможном криптографическом приложении и, как следствие, в уменьшении длины ключа постквантовых схем на кодах, исправляющих ошибки. К тому же данный метод построения кодов является универсальным и может быть применён для получения подполевых подкодов квазициклических алгеброгеометрических кодов, ассоциированных с произвольной кривой с известной группой автоморфизмов. Однако ввиду особенностей построения квазициклических альтернантных кодов возникает возможность редукции ключевой безопасности оригинального кода к ключевой безопасности кода с меньшими параметрами, который может не являться стойким к структурной атаке.

Ключевые слова: *квазициклические коды, альтернантные коды, инвариантные коды, алгеброгеометрические коды, функциональные поля, группа автоморфизмов кода.*

CONSTRUCTION OF QUASI-CYCLIC ALTERNANT CODES AND THEIR APPLICATION IN CODE-BASED CRYPTOGRAPHY

A. A. Kuninets*, E. S. Malygina**

*Immanuel Kant Baltic Federal University, Kaliningrad, Russia
**HSE, Moscow, Russia

The paper presents an overview of quasi-cyclic alternant codes and their structural analysis regarding the classification of automorphisms. We also have detailed methods for recovering the structure of a given code. The attractiveness of the family of considered codes lies in their cryptographic applications and, as in theory, in reducing the key length of post-quantum code-based schemes. In addition, this method of constructing codes is universal and can be used to obtain subfield subcodes of quasi-cyclic algebraic-geometric codes associated with an arbitrary curve with a known

[1]Работа первого автора выполнена за счет гранта Российского научного фонда №22-41-0441 (https://rscf.ru/project/22-41-04411/); работа второго автора подготовлена в рамках Программы фундаментальных исследований НИУ ВШЭ.

group of automorphisms. However, as a result of constructing quasi-cyclic alternant codes, it becomes possible to reduce the key security of the source code to a code with smaller parameters, which may not be resistant to a structural attack.

Keywords: *quasi-cyclic codes, alternant codes, invariant codes, algebraic-geometric code, function fields, automorphism group of a code.*

Введение

Активное развитие квантовых технологий и стремительный рост вычислительной мощности квантового компьютера ставит под угрозу безопасность современных криптографических стандартов. Это связано с тем, что криптостойкость большинства асимметричных алгоритмов основывается на сложности задач факторизации целых чисел (например, криптосистема RSA) и дискретного логарифмирования (например, протокол Диффи — Хеллмана), что делает их неустойчивыми к атакам с использованием квантового компьютера. Однако в последние несколько лет успешно развивается направление постквантовой криптографии, к которому относятся алгоритмы, основывающиеся на сложности задач, для которых не существует полиномиального алгоритма решения, даже на квантовом компьютере.

В конце 2016 г. Национальный институт стандартов и технологий США (The National Institute of Standards and Technology — NIST) объявил о начале конкурса по стандартизации постквантовых алгоритмов. Одним из перспективных направлений в этой области стала криптография на кодах, исправляющих ошибки.

В данной работе рассмотрен принцип построения квазициклических кодов Гоппы. Далее описано редуцирование ключевой безопасности квазициклических кодов Гоппы к ключевой безопасности инвариантного кода с меньшими параметрами [1]; под термином «ключевая безопасность» понимается стойкость кода относительно атак, направленных на восстановление секретного ключа криптосистемы. Детализирована и снабжена примерами структурная атака на рассматриваемый квазициклический код.

1. Предварительные сведения

Мы опускаем базовые сведения из теории функциональных полей и алгебраической геометрии, предполагая, что читатель с ними ознакомлен. Для более подробного изучения можно обратиться к работам [2, 3].

1.1. АГ-коды, ассоциированные с проективной прямой

Введём понятия обобщённого кода Рида — Соломона (GRS-кода) и алгеброгеометрического кода (АГ-кода), ассоциированного с проективной прямой, а также его подполевого подкода, и покажем возможность построения кода Гоппы с помощью алгеброгеометрического подхода. В заключение рассмотрим связь между многочленом Гоппы и дивизорами, используемыми при построении кода в алгеброгеометрическом случае.

Определение 1. Зададим вектор $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$, состоящий из n различных элементов, и вектор $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in (\mathbb{F}_{q^m}^*)^n$, состоящий из n ненулевых элементов. Пусть $k \in \mathbb{Z}^+$. *Обобщённый код Рида — Соломона* (GRS-код) размерности k задаётся следующим образом:

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) = \{(y_1 f(x_1), \ldots, y_n f(x_n)) : f \in \mathbb{F}_{q^m}[z] \text{ и } \deg(f) < k\}.$$

Вектор $\mathbf{x}$ называется *носителем*, а вектор $\mathbf{y}$ — *множителем* кода $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

Отметим, что любой рациональный АГ-код является обобщённым кодом Рида — Соломона. Доказательство этого факта можно найти в [4]. Покажем, что аналогичную конструкцию кода можно получить, используя алгеброгеометрический подход.

Пусть $\mathbf{P}^1$ — это проективная прямая над полем $\mathbb{F}_{q^m}$, тогда $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(x)$ — функциональное поле проективной прямой $y = x$, где $\mathbb{F}_{q^m}(x)$ — *поле рациональных функций* над $\mathbb{F}_{q^m}$. Полюс функции x является бесконечно удалённой точкой прямой $\mathbf{P}^1$, которую будем обозначать P_∞. Рациональные точки, то есть точки степени один проективной прямой, имеют вид $P_i = (x_i : 1)$.

Обозначим $D = P_1 + \ldots + P_n$ — дивизор, являющийся формальной суммой попарно различных рациональных точек проективной прямой. Носителем дивизора называют множество точек, входящих в него: $\mathrm{supp}(D) = \{P_1, \ldots, P_n\}$. Через G обозначим дивизор, носитель которого не пересекается с носителем дивизора D. АГ-код $\mathcal{C}$, ассоциированный с проективной прямой $\mathbf{P}^1$, будем обозначать

$$\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G).$$

Чтобы провести аналогию с классическим определением GRS-кодов, построим порождающую матрицу кода $\mathcal{C}$. Будем считать, что $G \sim \deg(G)P_\infty$. Это означает, что $G + (h) = \deg(G)P_\infty$, где (h) — главный дивизор некоторой функции $h \in \mathbb{F}_{q^m}(x)$. Более того, для любого $s \in \mathbb{N}$ пространство Римана — Роха, ассоциированное с дивизором sP_∞, имеет вид

$$\mathscr{L}(sP_\infty) = \{x^i : i \in \{0, \ldots, s\}\}.$$

Теперь запишем пространство Римана — Роха, ассоциированное с дивизором G:

$$\mathscr{L}(G) = \{hx^i : i \in \{0, \ldots, s\}\}.$$

Согласно [4, следствие 2.2.3], размерность кода, ассоциированного с проективной прямой, равна $k = \deg(G) + 1$. Пусть $x = (x(P_1), \ldots, x(P_n)) = (x_1, \ldots, x_n)$ и $y = (h(P_1), \ldots, h(P_n))$, тогда матрица

$$\mathbf{V}(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} y_1 & \ldots & y_n \\ y_1x_1 & \ldots & y_nx_n \\ y_1x_1^2 & \ldots & y_nx_n^2 \\ \vdots & & \vdots \\ y_1x_1^{k-1} & \ldots & y_nx_n^{k-1} \end{pmatrix} \tag{1}$$

является порождающей матрицей кода $\mathcal{C}$.

Определение 2. Пусть $\mathbf{x} \in \mathbb{F}_{q^m}^n$ — это носитель, а $\mathbf{y} \in (\mathbb{F}_{q^m}^*)^n$ — множитель кода $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$, тогда *альтернантный код* над $\mathbb{F}_q$ задаётся следующим образом:

$$\mathcal{A}_{r,q}(\mathbf{x}, \mathbf{y}) = \mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp \cap \mathbb{F}_q^n,$$

где $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})^\perp$ — дуальный код к коду $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$ и r — размерность кода $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$.

Так как по построению альтернантные коды являются подполевыми подкодами GRS-кодов и соответственно являются подполевыми подкодами АГ-кодов, далее будем использовать алгеброгеометрическую нотацию:

$$\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^\perp \cap \mathbb{F}_q^n.$$

Определение 3. Пусть $\mathbf{x} \in \mathbb{F}_{q^m}^n$ — вектор с попарно различными координатами и $\Gamma \in \mathbb{F}_{q^m}[z]$ — многочлен, такой, что $\Gamma(x_i) \neq 0$ для любых $i \in \{0, \ldots, n-1\}$. *Классический код Гоппы* $\mathscr{G}_q(\mathrm{x}, \Gamma)$, ассоциированный с Γ и порождённый $\mathbf{x}$, определяется следующим образом:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{A}_{r,q}\left(\mathbf{x}, \Gamma(\mathbf{x})^{-1}\right).$$

Здесь $r = \deg \Gamma$. Многочлен Γ называют *многочленом Гоппы*, а m — *степенью расширения кода Гоппы.*

Покажем явный вид дивизоров и алгеброгеометрический способ построения классического кода Гоппы.

Теорема 1. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек проективной прямой $\mathbf{P}^1$ над $\mathbb{F}_{q^m}$; $G = G_0 - P_\infty$ — дивизор функционального поля $\mathbb{F}_{q^m}(\mathbf{P}^1)$, носитель которого не пересекается с носителем дивизора D, где $G_0 = (\Gamma)_0$ — дивизор нулей многочлена $\Gamma \in \mathbb{F}_q(\mathbf{P}^1)$; код $\mathcal{C}_{\mathscr{L}}(D, G)$ является АГ-кодом, определённым над $\mathbb{F}_{q^m}$. Тогда классический код Гоппы представим в следующей алгеброгеометрической форме:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp \cap \mathbb{F}_q^n = \mathcal{C}_{\mathscr{L}}(D, A - G_0) \cap \mathbb{F}_q^n,$$

где $\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp$ — дуальный к исходному коду; $A = (h'(z)) + (n-1)P_\infty$; $h(z) = \prod\limits_{x_i \in \mathbf{x}} (z - x_i)$.

Доказательство. Пусть $\mathbf{x} = \{x(P_1), \ldots, x(P_n)\} = \{x_1, \ldots, x_n\}$ и $\Gamma(z) \in \mathbb{F}_q(\mathbf{P}^1)$, где $P_i = (x_i : 1) \in \mathbf{P}^1$ — попарно различные точки; $\deg(\Gamma(z)) = r$, $1 \leqslant r \leqslant n-1$; $\Gamma(x_i) \neq 0$ для всех $x_i \in \mathbf{x}$. Рассмотрим код с порождающей матрицей

$$V = \begin{pmatrix} \Gamma(x_1)^{-1} & \Gamma(x_2)^{-1} & \ldots & \Gamma(x_n)^{-1} \\ x_1\Gamma(x_1)^{-1} & x_2\Gamma(x_2)^{-1} & \ldots & x_n\Gamma(x_n)^{-1} \\ \vdots & \vdots & & \vdots \\ x_1^{r-1}\Gamma(x_1)^{-1} & x_2^{r-1}\Gamma(x_2)^{-1} & \ldots & x_n^{r-1}\Gamma(x_n)^{-1} \end{pmatrix}.$$

Нетрудно заметить, что вид данной матрицы полностью совпадает с видом матрицы (1), являющейся порождающей для GRS-кода. Очевидно, что код с такой порождающей матрицей удовлетворяет определению 1, то есть является $\mathbf{GRS}_r(\mathbf{x}, \mathbf{y})$-кодом, где $\mathbf{y} = \left(\Gamma(x_i)^{-1} : x_i \in \mathbf{x}\right)$.

Докажем, что

$$\mathbf{GRS}_r(\mathbf{x}, \mathbf{y}) = \mathcal{C}_{\mathscr{L}}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty). \tag{2}$$

Для этого достаточно показать, что $z^j \cdot \Gamma(z)^{-1} \in \mathscr{L}(G_0 - P_\infty)$ для всех $j \in \{0, \ldots, r-1\}$. Рассмотрим дивизор нулей и дивизор полюсов функции $z^j \cdot \Gamma(z)^{-1}$, затем найдём её главный дивизор:

$$\begin{aligned} &(z^j \cdot \Gamma(z)^{-1})_0 = jP_0 + rP_\infty - jP_\infty, \text{ где } P_0 \text{ — нуль функции } z; \\ &(z^j \cdot \Gamma(z)^{-1})_\infty = G_0; \\ &(z^j \cdot \Gamma(z)^{-1}) = j(P_0 - P_\infty) - (G_0 - rP_\infty). \end{aligned}$$

Таким образом,

$$j(P_0 - P_\infty) - (G_0 - rP_\infty) = -G_0 + jP_0 + (r-j)P_\infty \geqslant -G_0 + P_\infty.$$

Так как $\dim(\mathscr{L}(G_0 - P_\infty)) = r$, то базис пространства Римана — Роха $\mathscr{L}(G_0 - P_\infty)$ имеет вид $\{z^j \cdot \Gamma(z)^{-1} : j = 0, \ldots, r-1\}$. Равенство (2) доказано.

Теперь докажем равенство кодов

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, A - G_0).$$

Для этого потребуется ввести понятие вычета дифференциала $\omega = f\delta t_P$ [4, 2] в точке P, где $f \in \mathbb{F}_q(\mathcal{X})$ и t_P — локальный параметр. Разложим функцию f в ряд Лорана по степеням t_P:

$$f = \sum_{i=s}^{\infty} a_i t_P^i.$$

Здесь $s \in \mathbb{Z}$. *Вычетом дифференциала ω в точке P* называется коэффициент a_{-1} в представленном разложении; обозначается $\mathrm{Res}_\omega(P)$.

Лемма 1 [4, Лемма 2.3.6]. Пусть $\mathbf{P}^1$ — проективная прямая над полем $\mathbb{F}_{q^m}$; $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(z)$ — рациональное функциональное поле; $\alpha = \{\alpha_1, \ldots, \alpha_n\}$ — различные элементы поля $\mathbb{F}_{q^m}$; $P_i \in \mathbf{P}^1$ — нули функций $z - \alpha_i$; $h(z) = \prod\limits_{\alpha_i \in \alpha} (z - \alpha_i)$. Пусть $\zeta \in \mathbb{F}_{q^m}(\mathbf{P}^1)$, такой, что $\zeta(P_i) = 1$ для любой P_i. Тогда существует дифференциал Вейля ω:

$$v_{P_i}(\omega) = -1,\ \mathrm{Res}_\omega(P_i) = 1,\ i = 1, \ldots, n,$$
$$(\omega) = (\zeta) + (h'(z)) - (h(z)) - 2P_\infty,$$

где $v_{P_i}(\omega)$ — нормирование ω в точке P_i [4, 2].

Предложение 1 [4, Предложение 2.2.10]. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек проективной прямой; G — дивизор функционального поля $\mathbb{F}_{q^m}(\mathbf{P}^1)$; η — дифференциал Вейля, такой, что $v_{P_i}(\eta) = -1$ и $\mathrm{Res}_\eta(P_i) = 1$ для всех $i = 1, \ldots, n$. Тогда

$$\mathcal{C}_{\mathscr{L}}(D, G)^\perp = \mathcal{C}_{\mathscr{L}}(D, D - G + (\eta)),\ \text{где } D = \sum_{i=1}^{n} P_i.$$

Теперь мы можем явно задать вид дивизоров дуального кода, используя предложение 1:

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, D - (G_0 - P_\infty) + (h'(z)) - (h(z)) - 2P_\infty). \tag{3}$$

Здесь $(h(z)) = (h(z))_0 - (h(z))_\infty = \sum\limits_{i=1}^{n} P_i - nP_\infty = D - nP_\infty$. Таким образом, равенство (3) принимает вид

$$\mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp = \mathcal{C}_{\mathscr{L}}(D, -G_0 + P_\infty + (h'(z)) + nP_\infty - 2P_\infty) = \mathcal{C}_{\mathscr{L}}(D, A - G_0),$$

следовательно, выполняется равенство и для исходного кода Гоппы:

$$\mathscr{G}_q(\mathbf{x}, \Gamma) = \mathcal{C}_{\mathscr{L}}(D, G_0 - P_\infty)^\perp \cap \mathbb{F}_q^n = \mathcal{C}_{\mathscr{L}}(D, A - G_0) \cap \mathbb{F}_q^n.$$

Теорема 1 доказана. ■

1.2. Группа автоморфизмов альтернантных кодов

Пусть $\mathfrak{S}_n$ — группа перестановок множества $\{1, \ldots, n\}$. Определим группу автоморфизмов кода.

Определение 4. Пусть $\mathcal{C}$ — линейный код длины n над полем $\mathbb{F}_q$; $\sigma \in \mathfrak{S}_n$ — перестановка, действующая на кодовое слово как $\sigma(\mathbf{c}) = \big(c_{\sigma(1)}, \ldots, c_{\sigma(n)}\big)$. *Группа автоморфизмов кода* $\mathcal{C}$ имеет вид

$$\mathrm{Aut}(\mathcal{C}) = \{\sigma \in \mathfrak{S}_n : \sigma(\mathcal{C}) = \mathcal{C}\}.$$

Так как альтернантные коды являются подполевыми подкодами GRS-кодов, сначала необходимо исследовать GRS-коды и их автоморфизмы.

Дадим определение *проективной линейной группы*:

$$\mathrm{PGL}_2(\mathbb{F}_{q^m}) = \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x : y) \mapsto (ax + by : cx + dy), \end{cases} \qquad a, b, c, d \in \mathbb{F}_{q^m},\ ad - bc \neq 0.$$

В [5] рассмотрено алгеброгеометрическое построение GRS-кодов, а также доказано, что вся группа автоморфизмов кода индуцирована действием проективной линейной группы $\mathrm{PGL}_2(\mathbb{F}_{q^m})$, являющейся группой автоморфизмов проективной прямой $\mathbf{P}^1$.

Элементы $\mathrm{PGL}_2(\mathbb{F}_{q^m})$ имеют также матричное представление, а именно: любой элемент $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ можно представить как

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},\ ad - bc \neq 0.$$

Определение 5. Пусть $D = P_1 + \ldots + P_n$ — дивизор, носителем которого являются n попарно различных рациональных точек; G, G' — дивизоры на $\mathbf{P}^1$, такие, что $(\mathrm{supp}(G) \cup \mathrm{supp}(G')) \cap \mathrm{supp}(D) = \varnothing$. Определим отношение эквивалентности дивизоров относительно дивизора D следующим образом:

$$G \sim_D G' \Leftrightarrow \exists f \in \mathbb{F}_{q^m}(\mathbf{P}^1)\big(f \neq 0 \ \ \& \ \ G - G' = (f) \ \ \& \ \ \forall P \in \mathrm{supp}(D)\, f(P) = 1\big).$$

Лемма 2 [5, Лемма 2.1]. Пусть $\mathrm{supp}(D) \subseteq \mathbf{P}^1$ и G, G' — два дивизора $\mathbf{P}^1$, такие, что $(\mathrm{supp}(G) \cup \mathrm{supp}(G')) \cap \mathrm{supp}(D) = \varnothing$. Если $G \sim_D G'$, то $\mathcal{C}_{\mathscr{L}}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G')$.

Следующая теорема определяет всевозможные автоморфизмы АГ-кода, ассоциированного с дивизором G.

Теорема 2 [5, Теорема 3.1]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G) \subseteq \mathbb{F}_{q^m}^n$ — АГ-код, $1 \leqslant \deg(G) \leqslant n - 3$. Тогда

$$\mathrm{Aut}(\mathcal{C}) = \left\{\sigma \in \mathrm{Aut}\left(\mathbf{P}^1\right) : \sigma(D) = D \ \ \& \ \ \sigma(G) \sim_D G\right\}.$$

Теперь перейдём непосредственно к построению GRS-кодов с помощью автоморфизма. Пусть $\sigma \in \mathrm{PGL}_2\left(\mathbb{F}_{q^m}\right)$ — автоморфизм, действующий на носитель дивизора D и дивизор $G \in \mathrm{Div}\left(\mathbf{P}^1\right)$. Тогда σ индуцирует автоморфизм кода $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$:

$$\tilde{\sigma} : \begin{cases} \mathcal{C} \longrightarrow \mathcal{C}, \\ \big(f(P_1), \ldots, f(P_n)\big) \longmapsto \big(f(\sigma(P_1)), \ldots, f(\sigma(P_n))\big). \end{cases}$$

Поскольку альтернантные коды являются подполевыми подкодами GRS-кодов, то их группа автоморфизмов включает в себя группу автоморфизмов исходного GRS-кода.

Замечание 1. Пусть $\mathcal{A}_{r,q}(D, G)$ — альтернантный код над $\mathbb{F}_q$ и $\sigma \in \mathrm{Aut}\left(C_{\mathscr{L}}(D, G)\right)$, тогда $\sigma \in \mathrm{Aut}(\mathcal{A}_{r,q}(D, G))$.

2. Квазициклические альтернантные коды

2.1. Квазициклические коды

Пусть $\mathbb{F}$ — конечное поле, ℓ — положительное целое.

Определение 6. Определим циклический и квазициклический сдвиги σ_ℓ и σ:

$$\sigma_\ell\colon \begin{cases} \mathbb{F}^\ell \to \mathbb{F}^\ell, \\ (x_0, x_1, \ldots, x_{\ell-1}) \mapsto (x_{\ell-1}, x_0, \ldots, x_{\ell-2}), \end{cases} \qquad \sigma\colon \begin{cases} \mathbb{F}^n \to \mathbb{F}^n, \\ (\mathbf{b}_1 \| \ldots \| \mathbf{b}_{n/\ell}) \mapsto (\sigma_\ell(\mathbf{b}_1) \| \ldots \| \sigma_\ell(\mathbf{b}_{n/\ell})). \end{cases}$$

Пусть n — целое и $\ell | n$. Тогда σ называется ℓ-квазициклическим сдвигом, полученным поблочным применением σ_ℓ, где $\mathbf{b}_i$ — блоки длины ℓ, $i = 1, \ldots, n/\ell$.

Определение 7. Код $\mathcal{C} \subseteq \mathbb{F}^n$ называется *ℓ-квазициклическим* (ℓ-QC), если для всех $c \in \mathcal{C}$ выполняется $\sigma(c) \in \mathcal{C}$, где σ — операция ℓ-квазициклического сдвига. При этом ℓ называется *порядком* квазицикличности кода.

Определение 8. Матрица $\mathbf{M}$ называется *ℓ-блочно-циркулянтной*, если она состоит из циркулянтных матриц $\mathbf{M}_i$ порядка ℓ:

$$\mathbf{M} = \left(\begin{array}{c|c|c} & & \\ \hline \ldots & \mathbf{M}_i & \ldots \\ \hline & & \end{array}\right), \quad \text{где} \quad \mathbf{M_i} = \begin{pmatrix} a_0 & a_1 & \ldots & a_{\ell-1} \\ a_{\ell-1} & a_0 & \ldots & a_{\ell-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & \ldots & a_{\ell-1} & a_0 \end{pmatrix}.$$

Матрица такого типа может быть представлена первыми строками каждого блока размера ℓ. Таким образом, можно восстановить ℓ-блочно-циркулянтную матрицу $\mathbf{M}$ из k строк, зная её строки с индексами $1, \ell+1, \ldots, k-\ell+1$.

Замечание 2. Код $\mathcal{C}$, имеющий ℓ-блочно-циркулянтную порождающую матрицу, является ℓ-QC-кодом. Отметим, что QC-код $\mathcal{C}$ размерности k не обязан иметь ℓ-блочно-циркулянтную порождающую матрицу, однако существует ℓ-блочно-циркулянтная матрица $\mathbf{G}$, состоящая из $k' \geqslant k$ строк, которая порождает данный код $\mathcal{C}$.

Для оптимального уменьшения размера открытого ключа криптосистемы Мак-Элиса можно рассматривать ℓ-QC-коды $\mathcal{C}$ с параметрами $[n, k]$, имеющие порождающую матрицу в систематическом виде

$$\mathbf{G} = \left(\mathbf{I}_k \,|\, \mathbf{M}\right),$$

где $\mathbf{I}_k$ — единичная матрица порядка k; $\mathbf{M}$ — ℓ-блочно-циркулянтная матрица. В этом случае будем называть код $\mathcal{C}$ *систематическим квазициклическим.*

Замечание 3. Для выполнения предыдущего условия размерность ℓ-QC-кода должна быть кратна ℓ.

Определение 9. Для матрицы $\mathbf{G}$ в систематической форме определим $\rho(\mathbf{G})$ как матрицу, полученную путём удаления всех строк каждого блока матрицы $\mathbf{M}$, кроме первой, т.е. $\rho(\mathbf{G})$ получается путём записывания строк из $\mathbf{M}$ с индексами 1, $\ell+1$, $2\ell+1$, …, $k-\ell+1$. Отсюда имеем следующее соотношение:

$$\text{Число строк матрицы } \mathbf{G} = \ell \cdot (\text{Число строк матрицы } \rho(\mathbf{G})).$$

Определение 10. Пусть $\mathcal{C} \subseteq \mathbb{F}^n$ — ℓ-QC-код. *Инвариантный код* определяется следующим образом:

$$\mathcal{C}^\sigma = \{c \in \mathcal{C} : \sigma(c) = c\}.$$

Так как инвариантный код имеет повторяющиеся элементы, далее будем использовать *проколотый инвариантный код*, который определяется следующим образом:

$$\overline{\mathcal{C}}^{\sigma} = \mathrm{Punct}_{\mathcal{I}_\ell}(\mathcal{C}^{\sigma}),$$

где $\mathcal{I}_\ell = \{1, \ldots, n\} \setminus \{1, \ell+1, \ldots, n-\ell+1\}$. Пусть $\sigma_{\mathcal{C}}$ — ℓ-QC-сдвиг σ, суженный на код $\mathcal{C}$, тогда можно записать $\overline{\mathcal{C}}^{\sigma} = \mathrm{Punct}_{\mathcal{I}_\ell}(\ker(\sigma_{\mathcal{C}} - \mathrm{id}))$.

Далее под инвариантным кодом будем иметь в виду и инвариантный, и проколотый инвариантный код, однако обозначения останутся разными.

Замечание 4. Инвариантность коммутирует с операцией вычисления подполевого подкода. Действительно, если $\mathcal{C}$ — ℓ-QC-код над $\mathbb{F}_{q^m}$, то

$$(\mathcal{C} \cap \mathbb{F}_q^n)^{\sigma} = \{c \in \mathcal{C} : c \in \mathbb{F}_q^n \ \ \& \ \ \sigma(c) = c\} = \mathcal{C}^{\sigma} \cap \mathbb{F}_q^n.$$

2.2. Построение квазициклических альтернантных кодов

Рассмотрим метод построения квазициклических альтернантных кодов, определённых над $\mathbb{F}_q$, с помощью заранее заданного автоморфизма.

Пусть $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и $\mathrm{ord}(\sigma) = \ell$. Для точки $P \in \mathbf{P}^1$ определим её орбиту:

$$\mathrm{Orb}_\sigma(P) = \left\{\sigma^i(P) : i \in \{0, \ldots, \ell-1\}\right\},$$

обозначим

$$D = \sum_{i=1}^{n/\ell} \sum_{P \in \mathrm{Orb}_\sigma(P_i)} P, \quad \mathrm{supp}(D) = \coprod_{i=1}^{n/\ell} \mathrm{Orb}_\sigma(P_i), \tag{4}$$

где $P_i \in \mathbf{P}^1(\mathbb{F}_{q^m})$ — попарно различные, не являющиеся инвариантными относительно заданного отображения σ точки с непересекающимися орбитами, не содержащими точку в бесконечности. Определим дивизор

$$G = \sum_{i=1}^{s} t_i \sum_{Q \in \mathrm{Orb}(Q_i)} Q, \tag{5}$$

где Q_i — точки $\mathbf{P}^1$, не содержащие в своих орбитах точку в бесконечности, такие, что $\mathrm{supp}(D) \cap Q_i = \varnothing$, $s \in \mathbb{N}$, $t_i \in \mathbb{Z}$ для $i \in \{1, \ldots, s\}$. При этом $\deg(G) = \sum\limits_{i=1}^{s} t_i \ell \deg(Q_i)$.

Как показано в п. 1.2, автоморфизм σ индуцирует автоморфизм кода $\mathcal{C}_{\mathscr{L}}(D, G)$. Для краткости и автоморфизм проективной прямой $\mathbf{P}^1$, и индуцированный автоморфизм будем обозначать через σ. Тогда, согласно лемме 1, σ также является автоморфизмом кода $\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n$. Таким образом, альтернантный код, полученный описанным способом, является квазициклическим при соответствующем упорядочивании точек.

3. Структурный анализ инвариантных кодов

Покажем, что инвариантный код для QC-альтернантного кода также является альтернантным кодом, но с меньшими параметрами. Так как инвариантность коммутирует с операцией взятия подполевого подкода, для анализа структуры инвариантных кодов Гоппы достаточно рассмотреть инвариантный код GRS-кода. Данные утверждения в дальнейшем позволят описать процесс восстановления параметров QC-альтернантного кода Гоппы, используя инвариантный проколотый код.

Для упрощения рассуждений будем предполагать, что G строится с использованием одной рациональной точки Q, т.е. $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$. В случае использования нескольких точек также возможно восстановить секретные параметры, однако алгоритмы восстановления принимают более громоздкий вид, поэтому в данной работе они опущены.

Зададим

$$\sigma^j(P_i) = (\alpha_{i\ell+j} : \beta_{i\ell+j}) \text{ для } i \in \{0, \ldots, n/\ell - 1\},\ j \in \{0, \ldots, \ell - 1\},$$
$$\sigma^j(Q) = (\gamma_j : \delta_j) \text{ для } j \in \{0, \ldots, \ell - 1\}.$$

Лемма 3. Пусть $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$, тогда пространство Римана — Роха, ассоциированное с дивизором G, имеет следующий вид:

$$\mathscr{L}(G) = \left\{ F(X,Y) \Big/ \prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t \colon F \in \mathbb{F}_{q^m}[X,Y] \text{ — однородный многочлен степени } t\ell \right\}.$$

Доказательство. Пусть $\mathbf{P}^1$ — проективная прямая над полем $\mathbb{F}_{q^m}$, тогда $\mathbb{F}_{q^m}(\mathbf{P}^1) = \mathbb{F}_{q^m}(x)$ — рациональное функциональное поле. Исходя из определения проективного многообразия, базис пространства Римана — Роха, в случае проективной прямой, имеет следующий вид:

$$\mathscr{L}(\mathbf{P}^1) = \left\{ \frac{f}{g} : f, g \in \mathbb{F}_{q^m}[X,Y] \text{ — однородные многочлены одинаковой степени}, g \neq 0 \right\}.$$

Рассмотрим дивизор $G = t \sum\limits_{R \in \mathrm{Orb}_\sigma(Q)} R$ и докажем, что

$$z = F(X,Y) \Big/ \prod_{j=0}^{\ell-1} (\delta_j X - \gamma_j Y)^t \in \mathscr{L}(G),$$

где $F \in \mathbb{F}_{q^m}[X,Y]$ — однородный многочлен степени $t\ell$. Пусть $\mathcal{Z}(f)$ — множество нулей функции f, тогда соответствующие дивизоры нулей и полюсов, а также главный дивизор функции z имеют следующий вид:

$$(z)_0 = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P + v_{P_\infty}(z) = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P,$$
$$(z)_\infty = \sum_{(\gamma_j : \delta_j) \in \mathrm{Orb}_\sigma(Q)} t(\gamma_j : \delta_j) = t \sum_{R \in \mathrm{Orb}_\sigma(Q)} R = G,$$
$$(z) = \sum_{P \in \mathcal{Z}(F(X,Y)) \setminus P_\infty} v_P(F(X,Y))P - G \geqslant -G.$$

Лемма 3 доказана. ■

Следующая лемма определяет понятие инвариантной функции. Так как мы рассматриваем QC-альтернантные коды с точки зрения АГ-кодов, необходимо понимать, какие функции из пространства Римана — Роха являются инвариантными относительно действия автоморфизма.

Лемма 4 [1, Лемма 3.3]. Пусть $\mathcal{C} = C_{\mathscr{L}}(D,G)$ и $\sigma \in \mathrm{Aut}(\mathcal{C})$. Если $c = (f(P_1), \ldots, f(P_n)) \in \mathcal{C}$ такое, что $\sigma(c) = c$, то f является σ-инвариантной функцией, т.е. $f \circ \sigma = f$.

Теорема 3 [1, Теорема 3.5]. Пусть $C_{\mathscr{L}}(D,G) \subseteq \mathbb{F}_{q^m}^n$ — АГ-код длины n, размерности k, с действующим на него автоморфизмом $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ порядка ℓ, где $\ell \mid n$. Пусть, как и ранее, определены D и G. Тогда инвариантный код $\overline{C_{\mathscr{L}}(D,G)}^{\sigma}$ является АГ-кодом длины n/ℓ и размерности $[k/\ell]$.

Следствие 1. Пусть $\mathcal{A}_{r,q}(D,G) = C_{\mathscr{L}}(D,G) \cap \mathbb{F}_q^n$ — альтернантный код длины n, порядка r, с действующим на него автоморфизмом $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ порядка ℓ, где $\ell \mid n$. Пусть D и G определены, как в (4) и (5). Тогда инвариантный код $\overline{\mathcal{A}_{\lfloor r/\ell \rfloor,q}(D,G)}^{\sigma}$ является альтернантным кодом длины n/l и порядка $[r/\ell]$.

Далее изучим действие автоморфизма $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ на пространство Римана — Роха $\mathscr{L}(G)$. Рассмотрим $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и $\mathrm{ord}(\sigma) = \ell$, а также дивизоры D и G, определённые ранее. Автоморфизм $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ можно представить в виде матрицы $M \in \mathrm{GL}_2(\mathbb{F}_{q^m})$. Нотация $M \sim N$, где $M, N \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, означает, что существует матрица $P \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$, такая, что $M = PNP^{-1}$. В зависимости от собственных векторов матрицы M можно выделить три случая:

1) $M \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, где $a \in \mathbb{F}_{q^m}$ (σ — диагонализируемый в $\mathbb{F}_{q^m}$);
2) $M \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, где $b \in \mathbb{F}_{q^m} \setminus \{0\}$ (σ — тригонализируемый в $\mathbb{F}_{q^m}$);
3) $M \sim \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix}$, где $\xi \in \mathbb{F}_{q^{2m}}$ (σ — диагонализируемый в $\mathbb{F}_{q^{2m}}$).

Возможность диагонализации или тригонализации зависит от собственных векторов матрицы. Поясним подробнее, когда можно привести матрицу M к одному из вышеописанных видов.

Теорема 4 [6, Теорема 2.2]. Пусть $M \in M_n(\mathbb{F})$, тогда матрица M диагонализируема в поле $\mathbb{F}$ тогда и только тогда, когда сумма размерностей собственных подпространств в точности равна n, что верно тогда и только тогда, когда существует базис в $\mathbb{F}^n$, состоящий из собственных векторов M.

Далее рассмотрим матрицы над конечным полем $\mathbb{F}_{q^m}$. Любое конечное поле является алгебраически незамкнутым, следовательно, минимальный многочлен $\pi_M(T)$ не обязательно раскладывается на линейные множители, как и характеристический многочлен. В таком случае количество собственных значений у матрицы $M \in M_n(\mathbb{F}_{q^m})$ меньше n, а условия теоремы 4 не выполняются.

Заметим, что если характеристический многочлен имеет кратный корень, то в общем случае при размерности больше 2 данный факт не говорит о том, что матрицу нельзя диагонализировать. Однако, рассматривая $M \in M_2(\mathbb{F}_{q^m})$, можно утверждать, что размерность собственных подпространств может быть равна $0, 1$ или 2. В первом случае условия теоремы 4 не выполняются, второй случай говорит о том, что матрица обязательно диагонализируема над $\mathbb{F}_{q^m}$, а в третьем случае условия выполнимы, только если матрица M уже является диагональной.

Теорема 5 [7]. Пусть $M \in M_2(\mathbb{F}_{q^m})$ не является диагональной. Матрица M диагонализируема в $\mathbb{F}_{q^m}$ тогда и только тогда, когда размерности всех собственных подпространств матрицы M равны 1, то есть характеристический многочлен имеет два различных корня кратности 1, что эквивалентно наличию двух различных собственных значений матрицы M.

Если характеристический многочлен разложим на множители, но имеет кратные корни, то можно тригонализировать матрицу M. В противном случае M всегда можно

диагонализировать в поле $\mathbb{F}_{q^{2m}}$, построенном при помощи добавления корня характеристического многочлена матрицы M.

При использовании минимального многочлена $\pi_M(T)$ матрицы M эти рассуждения можно представить в виде следующей теоремы:

Теорема 6 [7]. Пусть $M \in M_2(\mathbb{F}_{q^m})$, $\pi_M(T)$ — минимальный многочлен матрицы M. Тогда:

1) матрица M диагонализируема в $\mathbb{F}_{q^m} \iff \pi_M(T)$ раскладывается на различные линейные множители в $\mathbb{F}_{q^m}$;
2) матрица M тригонализируема в $\mathbb{F}_{q^m} \iff \pi_M(T)$ разложим в $\mathbb{F}_{q^m}$ на линейные множители, но имеет кратные корни;
3) матрица M диагонализируема в $\mathbb{F}_{q^{2m}} \iff \pi_M(T)$ сепарабельный.

Лемма 5 [1, Лемма 3.4]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код, такой, что $\sigma(\mathcal{C}) = \mathcal{C}$, и $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$. Тогда $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ индуцирует тот же автоморфизм кода $\mathcal{C}$, что и σ.

Лемма 5 показывает, что изучение GRS-кодов, инвариантных относительно индуцированного автоморфизма σ, сводится к одному из трёх случаев, описанных ранее. Далее рассмотрим инвариантные проколотые коды, для которых теорема 3 выполняется в каждом из этих случаев.

3.1. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Следующее предложение позволяет получить структуру однородных многочленов, инвариантных относительно диагонализируемого автоморфизма σ.

Предложение 2 [1, Предложение 3.8]. Пусть $F \in \mathbb{F}_{q^m}[X, Y]$ — однородный многочлен степени $t\ell$, элемент $a \in \mathbb{F}_{q^m}$ имеет порядок ℓ. Если $F(aX, Y) = F(X, Y)$, то $F(X, Y) = R\left(X^\ell, Y^\ell\right)$, где $R \in \mathbb{F}_{q^m}[X, Y]$ является однородным многочленом степени t.

Исходя из вида инвариантных относительно диагонализируемого автоморфизма многочленов, следующее предложение позволяет показать справедливость теоремы 3 в данном случае.

Предложение 3 [1, Предложение 3.9]. Пусть $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D, G)$ — АГ-код с параметрами $[n, k]$ и

$$\sigma : \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x : y) \mapsto (ax : y). \end{cases}$$

Определим $\tilde{D} = \sum \tilde{P}_i$, где $\tilde{P}_i \in \left\{\left(\alpha_i^\ell : \beta_i^\ell\right) : i \in \{1, \dots n\}\right\} = \mathrm{supp}(\tilde{D})$, и $\tilde{G} = t\left((-1)^{\ell-1} a^{\ell(\ell-1)/2} (\gamma_0/\delta_0)^\ell : 1\right)$ или $\tilde{G} = tP_\infty$. Тогда справедливо $\overline{\mathcal{C}}^\sigma = \mathcal{C}_{\mathscr{L}}(\tilde{D}, \tilde{G})$, а также $|\mathrm{supp}(\tilde{D})| = n/\ell$ и $\deg(\tilde{G}) = \deg(G)/\ell$.

Замечание 5. Инвариантный проколотый код $\overline{\mathcal{C}}^\sigma$ в предложении 3 имеет параметры $[n/\ell, \lceil k/\ell \rceil]$.

Стоит отметить, что элемент $a \in \mathbb{F}_{q^m}$ является корнем из единицы степени ℓ и не известен злоумышленнику. Исходя из того, что параметр ℓ относительно мал, даже не владея информацией об элементе a, возможно восстановить параметры D, G исходного кода, перебрав всех кандидатов для данного элемента.

3.2. Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Аналогично предыдущему случаю, рассмотрим структуру однородных многочленов, инвариантных относительно заданного тригонализируемого автоморфизма σ. Заметим, что данный случай возможен только тогда, когда $\mathrm{ord}(\sigma) = \mathrm{char}(\mathbb{F}_q) = p$.

Предложение 4 [8, Предложение 4]. Пусть $F \in \mathbb{F}_{q^m}[X,Y]$, $\deg(F) \leqslant tp$ и $b \in \mathbb{F}_q^*$. Если $F(X+bY,Y) = F(X,Y)$, то $F(X,Y) = R(X^p - b^{p-1}XY^{p-1}, Y^p)$, где p — характеристика поля $\mathbb{F}_{q^m}$ и $R \in \mathbb{F}_{q^m}[X,Y]$ — однородный многочлен степени $\deg(R) \leqslant t$.

Исходя из вида инвариантных многочленов, можно сделать вывод о структуре инвариантного проколотого кода в случае тригонализируемого автоморфизма.

Предложение 5 [1, Предложение 3.11]. Пусть $\mathcal{C} = C_{\mathscr{L}}(D,G)$ — АГ-код и

$$\sigma : \begin{cases} \mathbf{P}^1 \to \mathbf{P}^1, \\ (x:y) \mapsto (x+by:y). \end{cases}$$

Определим $\tilde{D} = \sum \tilde{P}_i$, где $\tilde{P}_i \in \{(\alpha_i^p - b^{p-1}\alpha_i\beta_i^{p-1} : \beta_i^p) : i \in \{1,\dots n\}\} = \operatorname{supp}(\tilde{D})$ и $\tilde{G} = t\left((\gamma_0/\delta_0)^p - b^{p-1}(\gamma_0/\delta_0) : 1\right)$ или $\tilde{G} = P_\infty$. Тогда справедливо $\overline{\mathcal{C}}^\sigma = C_{\mathscr{L}}(\tilde{D},\tilde{G})$, а также $|\operatorname{supp}(\tilde{D})| = n/\ell$ и $\deg(\tilde{G}) = \deg(G)/\ell$.

Замечание 6. Инвариантный проколотый код $\overline{\mathcal{C}}^\sigma$ в данном случае также имеет параметры $[n/\ell, \lceil k/\ell \rceil]$.

3.3. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$

Изучим GRS-код, определённый над $\mathbb{F}_{q^m}$, и построенный с его помощью проколотый инвариантный код относительно индуцированного автоморфизма $\sigma = \rho \circ \sigma_d \circ \rho^{-1}$, где автоморфизм σ_d — диагональный в $\mathrm{GL}_2(\mathbb{F}_{q^{2m}})$ и $\rho \in \mathrm{PGL}_2(\mathbb{F}_{q^{2m}})$.

Для кода $\mathcal{C} = \mathcal{C}_{\mathscr{L}}(D,G)$ над $\mathbb{F}_{q^m}$ рассмотрим расширенный код $\tilde{\mathcal{C}} = \mathcal{C}_{\mathscr{L}}(D^\otimes, G^\otimes)$ над $\mathbb{F}_{q^{2m}}$, такой, что $\mathcal{C}$ является его подполевым подкодом, т. е. $\mathcal{C} = \tilde{\mathcal{C}} \cap \mathbb{F}_{q^m} = \tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$. Тогда, во-первых, из леммы 5 следует, что $\overline{\tilde{\mathcal{C}}}^\sigma = \overline{\tilde{\mathcal{C}}}^{\sigma_d}$. Во-вторых, полагая, что $\mathrm{char}(\mathbb{F}_{q^{2m}}) \nmid \ell$, учтём следующие замечание и лемму:

Замечание 7. Характеристика p поля $\mathbb{F}_{q^m}$ не делит порядок ℓ автоморфизма σ.

Лемма 6 [1, Утверждение 3.1]. Пусть ℓ — положительное целое и $\mathcal{C}$ — ℓ-квазициклический код. Тогда

$$\phi_\ell(\mathcal{C}) \subseteq \overline{\mathcal{C}}^\sigma,$$

где ϕ_ℓ — функция свёртки, определённая следующим образом:

$$\phi_\ell : \begin{cases} \mathbb{F}^n \longrightarrow \mathbb{F}^{n/\ell}, \\ (x_1,\dots,x_n) \longmapsto \left(\sum\limits_{i=0}^{\ell-1} x_{\sigma^i(1)}, \sum\limits_{i=0}^{\ell-1} x_{\sigma^i(\ell+1)}, \dots, \sum\limits_{i=0}^{\ell-1} x_{\sigma^i(n-\ell+1)}\right). \end{cases}$$

Кроме того, если $\mathrm{char}(\mathbb{F}) \nmid \ell$, то $\phi_\ell(\mathcal{C}) = \overline{\mathcal{C}}^\sigma$.

Таким образом, имеем

$$\overline{\tilde{\mathcal{C}}}^\sigma = \phi_\ell(\{(f(P_1^\otimes),\dots,f(P_n^\otimes)) : f(P_i^\otimes) \in \mathbb{F}_{q^{2m}}\}) = \Big\{\Big(\sum_{i=0}^{\ell-1} f(P^\otimes_{\sigma^i(1)}), \dots, \sum_{i=0}^{\ell-1} f(P^\otimes_{\sigma^i(n-\ell+1)})\Big) :$$
$$f(P^\otimes_{\sigma^i(j)}) \in \mathbb{F}_{q^{2m}},\ i = 0,\dots,\ell-1,\ j = 1,\ell+1,\dots,n-\ell+1\Big\} = \phi_\ell(\tilde{\mathcal{C}}),$$

где $f \in \mathscr{L}(G^\otimes)$; $P_i^\otimes \in \operatorname{supp}(D^\otimes)$.

Если $\tilde{C}$ — GRS-код с параметрами $[n,k]$, то, согласно п. 3.1, $\overline{\tilde{\mathcal{C}}}^\sigma$ также является GRS-кодом с параметрами $\left[n/\ell, [k/\ell]\right]$.

Теперь изучим сужение автоморфизма σ на $\mathbb{F}_{q^m}$:

$$\sigma|_{\mathbb{F}_{q^m}} = (\rho \circ \sigma_d \circ \rho^{-1})|_{\mathbb{F}_{q^m}} = \rho|_{\mathbb{F}_{q^m}} \circ \sigma_d|_{\mathbb{F}_{q^m}} \circ \rho^{-1}|_{\mathbb{F}_{q^m}}.$$

Следовательно, $\sigma|_{\mathbb{F}_{q^m}} \in \mathrm{GL}_2(\mathbb{F}_{q^m}) \subset \mathrm{GL}_2(\mathbb{F}_{q^{2m}})$ и $\sigma_d|_{\mathbb{F}_{q^m}}$ — диагональный в $\mathrm{GL}_2(\mathbb{F}_{q^m})$. Рассмотрим диаграмму на рис. 1, где $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}}$ — подполевой подкод кода $\overline{\tilde{\mathcal{C}}^{\sigma}}$. Покажем, что $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}}$ является образом $\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$ при отображении $\phi_\ell|_{\mathbb{F}_{q^m}}$.

$$\begin{array}{ccc} \tilde{\mathcal{C}} & \xrightarrow{\phi_\ell} & \overline{\tilde{\mathcal{C}}^{\sigma}} \\ \downarrow & & \downarrow \\ \mathcal{C} = \tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}} & \xrightarrow{\phi_\ell|_{\mathbb{F}_{q^m}}} & \overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}} \end{array}$$

Рис. 1

Поскольку σ коммутирует с операцией построения подполевого подкода, учитывая замечание 4 и определение инвариантности, получаем $\overline{\tilde{\mathcal{C}}^{\sigma}}|_{\mathbb{F}_{q^m}} = \overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$. Кроме того, $\phi_\ell|_{\mathbb{F}_{q^m}}(\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}) = \overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$.

Окончательно заключаем, что $\overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$ является GRS-кодом, поскольку является подполевым подкодом GRS-кода. Если код $\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}$ имеет параметры $[n, k']$, то в силу отображения

$$\phi_\ell|_{\mathbb{F}_{q^m}}(\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}) = \phi_\ell(\{(f(\tilde{P}_1), \ldots, f(\tilde{P}_n)) : f(\tilde{P}_i) \in \mathbb{F}_{q^m}\}) =$$
$$= \left\{ \left(\sum_{i=0}^{\ell-1} f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(1)}), \ldots, \sum_{i=0}^{\ell-1} f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(n-\ell+1)}) \right) : f(\tilde{P}_{(\sigma|_{\mathbb{F}_{q^m}})^i(j)}) \in \mathbb{F}_{q^m} \right\},$$

где $i = 0, \ldots, \ell-1$, $j = 1, \ell+1, \ldots, n-\ell+1$, $f \in \mathscr{L}(\tilde{G})$, $\tilde{P}_i \in \tilde{D}$, согласно п. 3.1, код $\overline{\tilde{\mathcal{C}}|_{\mathbb{F}_{q^m}}}^{\sigma}$ имеет параметры $[n/\ell, k'/\ell]$.

4. Анализ безопасности квазициклических альтернантных кодов

Покажем, что ключевую безопасность QC-альтернантного кода можно редуцировать к ключевой безопасности его инвариантного кода. Рассмотрим автоморфизм $\sigma \in \mathrm{PGL}_2(\mathbb{F}_{q^m})$ и альтернантный код

$$\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n.$$

Дивизоры D и G определены в (4) и (5). Зная порождающую матрицу кода $\mathcal{A}_{r,q}(D, G)$ и индуцированный автоморфизм σ, можно вычислить инвариантный код $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$. Обозначим за инвариантный альтернантный код $\mathcal{A}_{r,q}(\tilde{D}, \tilde{G})$ для некоторых дивизоров $\tilde{D}$ и $\tilde{G}$ с малыми параметрами. Существует взаимосвязь между $\tilde{D}$ и $\tilde{G}$ инвариантного кода с дивизорами D и G исходного альтернантного кода, позволяющая восстановить исходные дивизоры при знании $\tilde{D}$ и $\tilde{G}$.

Будем предполагать, что $\tilde{D} = \sum_{i=1}^{n/\ell} \left(\tilde{\alpha}_i : \tilde{\beta}_i\right)$ и $\tilde{G} = t \cdot \tilde{Q}$ для инвариантного кода $\mathcal{A}_{r,q}(\tilde{D}, \tilde{G})$ известны и что G строится с помощью орбиты одной рациональной точки Q. Для исходного кода используем следующие обозначения:

$$\operatorname{supp}(D) = \{(\alpha_{i,j} : 1) : i \in \{1, \ldots, n/\ell\},\ j \in \{0, \ldots, \ell - 1\}\},$$
$$G = t \sum_{j=0}^{\ell-1} \sigma^j(Q),$$

где $\sigma^j(Q) = (\gamma_j : \delta_j) \neq P_\infty$ для всех $j \in \{0, \ldots, \ell - 1\}$.

4.1. Восстановление дивизора и носителя

Как показано в п.3, в зависимости от вида автоморфизма σ справедливы разные формульные соотношения, определяющие вид дивизоров, участвующих в построении инвариантного проколотого кода, следовательно, процесс восстановления дивизора и носителя исходного кода будет отличаться в зависимости от вида автоморфизма. Рассмотрим подробно данный процесс в каждом отдельном случае.

Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Замечание 8. Если $\tilde{Q} \neq P_\infty$, то для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$\tilde{Q} = \left((-1)^{\ell-1} \left(a^i\right)^{\ell(\ell-1)/2} (\gamma_i/\delta_i)^\ell : 1\right).$$

Далее будем предполагать, что точка $\tilde{Q}$ и дивизор $\tilde{G}$ известны. Покажем возможность восстановления исходного дивизора G.

Обозначим $\mu_\ell = \{\sigma^i(a) : i \in \{0, \ldots, \ell - 1\}\}$ и для каждого $a \in \mu_\ell$ восстановим соответствующую точку носителя дивизора G. Отметим, что множество μ_ℓ состоит из примитивных корней степени ℓ из единицы. Мощность множества равна количеству элементов порядка ℓ в поле $\mathbb{F}_{q^m}$, то есть $\varphi(\ell) < n$. Следовательно, существует всего $\varphi(\ell)$ вариантов выбора элемента a, что позволяет перебрать всевозможные варианты за приемлемое время.

Более детально вычисление дивизора G на основании знания $\tilde{G}$ описано в алгоритме 1. Основной и наиболее затратный шаг — вычисление корней многочлена $p(X) = a^{\ell(\ell-1)/2} X^\ell - \tilde{\gamma} \in \mathbb{F}_{q^m}[X]$, которые можно найти, используя, например, алгоритм Берлекэмпа.

Алгоритм 1. Восстановление дивизора G

Вход: $\tilde{G}$ — дивизор инвариантного кода $\overline{\mathcal{A}_{r,q}(D, G)}^\sigma$.
Выход: дивизор G.

1: $a := a^\ell \equiv 1 \pmod{q^m}$.
2: **Если** $\widetilde{Q} \neq P_\infty$, **то**
3: $\quad \Gamma :=$ корни $(a^{\ell(\ell-1)/2} X^\ell - \tilde{\gamma})$,
4: $\quad G := t \sum_{\gamma \in \Gamma} (\gamma : 1)$,
5: **иначе**
6: $\quad G := t \cdot \ell \cdot P_\infty$.
7: **Вернуть** G.

Далее восстановим носитель дивизора D' при условии, что коды $\mathcal{A}_{r,q}(D', G)$ и $\mathcal{A}_{r,q}(D, G)$ отличаются перестановкой координат. Координаты точки $P = (x : y) \in \in \operatorname{supp}(D)$ удовлетворяют системе

$$\begin{cases} x^\ell - \tilde{\alpha}_i = 0, \\ y^\ell - \tilde{\beta}_i = 0, \end{cases} \tag{6}$$

для $i \in \{1, \ldots, n/\ell\}$, где $(\tilde{\alpha}_i : \tilde{\beta}_i) = \tilde{P}_i$. Зная $\tilde{D}$, можно восстановить все элементы носителя D, однако они будут представлять собой неупорядоченное множество. Найдём решение (α'_i, β'_i) в (6) для каждого $i \in \{1, \ldots, n/\ell\}$ и выберем $a \in \mu_\ell$. Будем полагать, что множество

$$\operatorname{supp}(D') = \left\{ \left(a^j \frac{\alpha'_i}{\beta'_i} : 1 \right) : j \in \{0, \ldots, \ell - 1\},\ i \in \{1, \ldots, n/\ell\} \right\}$$

является носителем кода $\mathcal{A}_{r,q}(D', G)$, являющегося перестановочным относительно кода $\mathcal{A}_{r,q}(D, G)$. Для каждого множества решений $S = \{(\alpha'_i, \beta'_i) : i \in \{1, \ldots, n/\ell\}\}$ и всякого $a \in \mu_\ell$ имеем различные соответствующие им носители D'.

Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Замечание 9. Если $\tilde{Q} \neq P_\infty$, то для всех $i \in \{0, \ldots, \ell - 1\}$ имеем

$$\tilde{Q} = \left(\left(\frac{\gamma_i}{\delta_i} \right)^p - b^{p-1} \frac{\gamma_i}{\delta_i} : 1 \right).$$

В случае диагонализируемого автоморфизма σ поиск элемента a, такого, что $\operatorname{ord}(a) = \ell$, является тривиальным. Достаточно перебрать все корни степени ℓ из единицы. Существует следующий способ нахождения кандидатов для параметра b в случае тригонализируемого автоморфизма σ.

Лемма 7 [1, Лемма 4.1]. Число b — один из корней многочлена

$$P_b = \text{НОД}\left(\left\{ \operatorname{Res}_X \left(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X \right) : i \in \{1, \ldots, n/\ell\} \right\}, Y^{q^m} - Y \right),$$

где $\operatorname{Res}_X(F_1(X), F_2(X))$ — результант двух многочленов относительно переменной X.

Таким образом, $b \in \operatorname{roots}(P_b)$. Стоит отметить, что все элементы из орбиты b также являются корнями многочлена P_b, то есть $B = \{b, 2b, \ldots, (\ell-1)b\} \subseteq \operatorname{roots}(P_b)$. В общем случае $\deg(P_b) \geqslant |B|$. Для полей большого порядка ($\sim 2^m$, где $m \geqslant 10$) на практике всегда выполняется $B = \operatorname{roots}(P_b)$.

Далее будем предполагать, что точка $\tilde{Q}$ и дивизор $\tilde{G}$ известны. Алгоритм 2 восстанавливает исходный дивизор G, используя только параметры инвариантного проколотого кода $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$.

Алгоритм 2. Восстановление дивизора G

Вход: $\tilde{G}$, $\tilde{D}$ — дивизоры инвариантного кода $\overline{\mathcal{A}_{r,q}(D, G)}^{\sigma}$.
Выход: дивизор G и множество $B' \supseteq \{b, 2b, \ldots, (\ell - 1)b\}$.

$P_b := \text{НОД}\left(\left\{ \operatorname{Res}_X \left(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X \right) : i \in \{1, \ldots, n/\ell\} \right\}, Y^{q^m} - Y \right)$
$B' :=$ корни (P_b)
Если $\tilde{Q} \neq P_\infty$, **то**
    $\Gamma :=$ корни $(X^p - b^{p-1}X - \tilde{\gamma})$, $\quad$ // $b \in B'$
    $G := t \sum\limits_{\gamma \in \Gamma} (\gamma : 1)$,
иначе
    $G := t \cdot P_\infty$.
Вернуть G, B'.

Замечание 10. Самым сложным шагом алгоритма 2 является нахождение результантов, а также последующее нахождение наибольшего общего делителя двух

многочленов над полем $\mathbb{F}_{q^m}$. В свою очередь, самым трудозатратным шагом в вычислении результанта является нахождение определителя матрицы, которое выполняется за $\mathcal{O}((q^m+p)^\omega(q^m+p)(p-1))$ шагов в поле $\mathbb{F}_{q^m}$, где ω — экспонента в сложности умножения матриц. Сложность вычисления наибольшего общего делителя двух многочленов степени $q^m(p-1)$ в кольце $\mathbb{F}_{q^m}[Y]$ ограничена $\mathcal{O}(q^{2m}p^2)$, что меньше сложности вычисления определителей. Таким образом, учитывая, что данные алгоритмы срабатывают n/p раз, получаем итоговую сложность алгоритма $\mathcal{O}(n(q^m+p)^{\omega+1})$.

Далее восстановим носитель дивизора D' при условии, что $\mathcal{A}_{r,q}(D',G)=\mathcal{A}_{r,q}(D,G)$. Координаты точки $P=(x:y)\in\operatorname{supp}(D)$ удовлетворяют системе

$$\begin{cases} x^p - b^{p-1}x - \tilde{\alpha}_i = 0, \\ y^p - \tilde{\beta}_i = 0 \end{cases} \tag{7}$$

для $i\in\{1,\dots,n/\ell\}$, где $(\tilde{\alpha}_i:\tilde{\beta}_i)=\tilde{P}_i$. Зная $\tilde{D}$, мы можем восстановить все элементы носителя дивизора D, однако они будут представлять собой неупорядоченное множество. Найдём решение (α'_i,β'_i) в (7) для каждого $i\in\{1,\dots,n/\ell\}$ и выберем $b\in B'$. Множество

$$\operatorname{supp}(D')=\left\{\left(\frac{\alpha'_i}{\beta'_i}+b\cdot j:1\right):j\in\{0,\dots,\ell-1\},\ i\in\{1,\dots,n/\ell\}\right\}$$

составляет носитель кода $\mathcal{A}_{r,q}(D',G)$, являющегося перестановочным относительно кода $\mathcal{A}_{r,q}(D,G)$. Для каждого множества решений $S=\{(\alpha'_i,\beta'_i):i\in\{1,\dots,n/\ell\}\}$ и всякого $b\in B'$ имеем различные соответствующие им носители D'.

Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}}\backslash\mathbb{F}_{q^m}$

В этом случае $\sigma=\rho\circ\sigma_d\circ\rho^{-1}$, где $\rho\in\mathrm{PGL}_2(\mathbb{F}_{q^{2m}})$ и

$$\sigma_d:\begin{cases}\mathbf{P}^1\to\mathbf{P}^1,\\ (x:y)\mapsto(\xi x:\xi^{q^m}y),\end{cases}$$

где $\xi\in\mathbb{F}_{q^{2m}}$ — корень степени ℓ из единицы. Поскольку σ_d диагонален в $\mathbb{F}_{q^{2m}}$, мы можем восстановить носитель дивизора $D^\otimes$ и дивизор $G^\otimes$ в $\mathbb{F}_{q^{2m}}$, используя те же методы, что и в случае диагонализируемости и тригонализируемости в $\mathbb{F}_{q^m}$.

Для восстановления дивизоров D и G в $\mathbb{F}_{q^m}$ рассмотрим минимальный многочлен $\pi_\xi=X^2+aX+b\in\mathbb{F}_{q^m}[X]$ элемента ξ. Тогда

$$M_{\sigma_d}=\begin{pmatrix}\xi & 0\\ 0 & \xi^{q^m}\end{pmatrix}\sim\begin{pmatrix}0 & -b\\ 1 & -a\end{pmatrix}=M_{\sigma'}$$

и существует $\rho'\in\mathrm{GL}_2(\mathbb{F}_{q^{2m}})$, такой, что $\sigma_d=\rho'\circ\sigma'\circ\rho'^{-1}$, где $\sigma'\in\mathrm{PGL}_2(\mathbb{F}_{q^m})$ ассоциирован с $M_{\sigma'}$. Согласно лемме 5, можем предположить, что $\sigma=\sigma'$. Нахождение элемента ξ не составляет труда ввиду использования малого параметра ℓ, соответственно легко можем вычислить a и b. Чтобы восстановить ρ', достаточно диагонализировать матрицу $M_{\sigma'}$. Зная ρ', носитель дивизора $D^\otimes$ и дивизор $G^\otimes$ в $\mathbb{F}_{q^{2m}}$, можно восстановить оригинальный дивизор $D=\rho'^{-1}(D^\otimes)$ и дивизор $G=\rho'^{-1}(G^\otimes)$ в $\mathbb{F}_{q^m}$.

4.2. Восстановление перестановки

Восстановим перестановку между $\mathcal{A}_{r,q}(D', G)$ и $\mathcal{A}_{r,q}(D, G)$. Пусть $\mathbf{G}_{\text{pub}}$ — порождающая матрица кода $\mathcal{A}_{r,q}(D, G)$, $\mathbf{H}'$ — проверочная матрица кода $\mathcal{A}_{r,q}(D', G)$. Перестановку между $\mathcal{A}_{r,q}(D, G)$ и $\mathcal{A}_{r,q}(D', G)$ зададим с помощью матрицы $\mathbf{\Pi}$:

$$\mathbf{G}_{\text{pub}} \cdot \mathbf{\Pi} \cdot \mathbf{H}'^{\top} = 0. \tag{8}$$

Предположим, мы выбрали $a \in \mu_\ell$, тогда перестановочная матрица $\mathbf{\Pi}$ имеет следующий вид:

$$\begin{pmatrix} \sum\limits_{i=1}^{\ell} x_{1,i}\mathbf{J}^i & \dots & (0) \\ \vdots & \ddots & \vdots \\ (0) & \dots & \sum\limits_{i=1}^{\ell} x_{n/\ell,i}\mathbf{J}^i \end{pmatrix}, \text{ где } \mathbf{J} = \begin{pmatrix} 0 & \dots & \dots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Отметим, что $\mathbf{J}$ — матрица размера $\ell \times \ell$, $x_{j,i} \in \{0, 1\}$ — неизвестные для $j \in \{1, \dots, n/\ell\}$ и $i \in \{1, \dots, \ell\}$. В таком случае система (8) имеет n неизвестных. Если мы предположим, что $k \neq n$, то мы можем найти с большой вероятностью единственное решение для $\mathbf{\Pi}$ ввиду того, что в системе $(n-k)k$ уравнений и $n \leqslant (n-k)k$ неизвестных.

В алгоритме 3 представлено восстановление перестановочной матрицы $\mathbf{\Pi}$ при верном выборе элементов $a \in \mu_\ell$, $b \in \text{roots}(P_b)$.

Алгоритм 3. Восстановление $\text{supp}(D)$. Случай σ — диагонализируемый/тригонализируемый в $\mathbb{F}_{q^m}$

Вход: $\mathbf{G}_{\text{pub}}$ — порождающая матрица квазициклического альтернантного кода; дивизоры G, $\tilde{D}$.

Выход: $\varnothing$, если решение не найдено; в противном случае — D', такое, что $\mathcal{A}_{r,q}(D', G) = \mathcal{A}_{r,q}(D, G)$.

Для всех $i \in \{1, \dots, n\}$
  $\alpha'_i :=$ корни $(x^\ell - \tilde{\alpha}_i)$, // $\alpha'_i :=$ *корни* $(x^p - b^{p-1}x - \tilde{\alpha}_i)$
  $\beta'_i :=$ корни $(y^\ell - \tilde{\beta}_i)$. // $\beta'_i :=$ *корни* $(y^p - \tilde{\beta}_i)$
Для $a \in \mu_\ell$ // **для** $b \in B'$
  $\text{supp}(D') := \left\{ \left(a^j \dfrac{\alpha'_i}{\beta'_i} : 1 \right) : j \in \{0, \dots, \ell - 1\},\ i \in \{1, \dots, n/l\} \right\}$, // *supp*$(D') :=$
  $:= \left\{ \left(\dfrac{\alpha_i}{\beta_i} + b \cdot j : 1 \right) \right\}$
  $\mathcal{C} := \mathcal{A}_{r,q}(D', G)$.
  Если $\mathcal{C} = \mathcal{A}_{r,q}(D, G)$, **то**
    Вернуть D',
  иначе
    $\mathbf{H}' :=$ проверочная матрица $(\mathcal{C})$,
    $S :=$ решения $\mathbf{G}_{\text{pub}} \cdot \mathbf{\Pi} \cdot \mathbf{H}'^{\top} = 0$, где $\mathbf{\Pi}$ — перестановочная матрица.
    Если $\dim(S) = \ell$, **то**
      Вернуть $\pi(D')$. // $\pi \in \mathfrak{S}_n$ *ассоциирована с* $\mathbf{\Pi}$
Вернуть $\varnothing$.

Замечание 11. Размерность пространства решений в случае единственности решения равна ℓ, однако эти решения эквивалентны в контексте поиска перестановки для носителя квазициклического кода. Если представить решение системы в виде вектора, то, очевидно, по свойствам QC-кодов квазициклический сдвиг его блоков длины ℓ также является решением системы (8). Единственность решения нельзя гарантировать для произвольных параметров, так как возможно получение большого числа линейно зависимых уравнений в системе, однако для полей большого порядка ($\sim 2^m$, где $m \geqslant 10$) и параметров кода $[n \geqslant 2048, k \geqslant n/2]$, используемых на практике, данная проблема не возникает.

5. Примеры

Приведём примеры построения квазициклического альтернантного кода $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_q^n$ с помощью GRS-кода, а также рассмотрим примеры восстановления параметров оригинального кода через параметры кода $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma}$ для всех описанных случаев. Все вычисления выполнены в системах компьютерной алгебры Sage и Magma.

5.1. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^m}$

Построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D,G)$ над полем $\mathbb{F}_{2^6}$ с параметрами $[21,4]$ с помощью диагонализируемого автоморфизма

$$\sigma = \begin{pmatrix} \alpha^{21} & 0 \\ 0 & 1 \end{pmatrix},$$

где $\operatorname{ord}(\sigma) = \ell = 3$ и $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{64}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
\operatorname{Orb}_\sigma(P_1) &= \big\{(\alpha:1), (\alpha^4+\alpha^3+\alpha^2:1), (\alpha^4+\alpha^3+\alpha^2+\alpha:1)\big\},\\
\operatorname{Orb}_\sigma(P_2) &= \big\{(\alpha^2:1), (\alpha^5+\alpha^4+\alpha^3:1), (\alpha^5+\alpha^4+\alpha^3+\alpha^2:1)\big\},\\
\operatorname{Orb}_\sigma(P_3) &= \big\{(\alpha^3:1), (\alpha^5+\alpha^3+\alpha+1:1), (\alpha^5+\alpha+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_4) &= \big\{(\alpha^4:1), (\alpha^3+\alpha^2+1:1), (\alpha^4+\alpha^3+\alpha^2+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_5) &= \big\{(\alpha^5:1), (\alpha^4+\alpha^3+\alpha:1), (\alpha^5+\alpha^4+\alpha^3+\alpha:1)\big\},\\
\operatorname{Orb}_\sigma(P_6) &= \big\{(\alpha^4+\alpha^3+\alpha+1:1), (\alpha^5+\alpha^4+\alpha^2:1), (\alpha^5+\alpha^3+\alpha^2+\alpha+1:1)\big\},\\
\operatorname{Orb}_\sigma(P_7) &= \big\{(\alpha^5+\alpha^4+\alpha^2+\alpha:1), (\alpha^5+\alpha^4+\alpha+1:1), (\alpha^2+1:1)\big\},\\
\operatorname{supp}(D) &= \coprod_{i=1}^{n/\ell} \operatorname{Orb}_\sigma(P_i).
\end{aligned}$$

Замечание 12. Для наполнения носителя дивизора D необходимо выбирать точки с непересекающимися орбитами.

Для построения дивизора G используем единственную точку $Q = (\alpha^3+1:1)$ и параметр $t = 1$. В результате дивизор примет вид $G = \sum\limits_{R \in \operatorname{Orb}(Q)} R = (\alpha^3+1:1) + (\alpha^5 + \\ + \alpha^2+1:1) + (\alpha^5+\alpha^3+\alpha^2:1)$.

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, выглядит так:

$$\mathscr{L}(G) = \Big\{ \frac{X^3+Y^3}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\ \frac{X\cdot Y^2}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\\ \frac{X^2\cdot Y}{X^3+(\alpha^5+\alpha^2+\alpha+1)},\ \frac{X^3}{X^3+(\alpha^5+\alpha^2+\alpha+1)} \Big\}.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D,G)$ имеет следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix} 1&0&0&0&\alpha^{21}&\alpha^{9}&\alpha^{12}&\alpha^{40}&\alpha^{13}&\alpha^{35}&\alpha^{32}&\alpha^{55}&\alpha^{30}&\alpha^{35}&\alpha^{3}&\alpha^{35}&\alpha^{19}&\alpha^{54}&\alpha^{39}&\alpha^{32}&\alpha^{14}\\ 0&1&0&0&\alpha^{9}&\alpha^{61}&\alpha^{30}&1&\alpha^{29}&\alpha^{10}&\alpha^{58}&\alpha^{48}&\alpha^{41}&\alpha^{56}&\alpha^{28}&\alpha^{2}&\alpha^{56}&\alpha^{44}&\alpha^{44}&\alpha^{13}&\alpha^{22}\\ 0&0&1&0&\alpha^{61}&\alpha^{21}&\alpha^{18}&\alpha^{53}&\alpha^{24}&\alpha^{38}&\alpha^{5}&\alpha^{46}&\alpha^{38}&\alpha^{39}&\alpha^{21}&\alpha^{27}&\alpha^{58}&\alpha^{53}&\alpha^{24}&\alpha^{53}&\alpha^{38}\\ 0&0&0&1&1&1&\alpha^{43}&\alpha^{43}&\alpha^{43}&\alpha^{37}&\alpha^{37}&\alpha^{37}&\alpha^{27}&\alpha^{27}&\alpha^{27}&\alpha^{5}&\alpha^{5}&\alpha^{5}&\alpha^{10}&\alpha^{10}&\alpha^{10} \end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_q^n$. В результате получим квазициклический альтернантный код с параметрами $[21,3]$ и порождающей матрицей

$$\mathbf{G}_{\text{pub}} = \begin{pmatrix} 1&0&0&0&0&1&1&1&1&1&1&1&1&0&1&1&0&1&0&1&1\\ 0&1&0&1&0&0&1&1&1&1&1&1&1&1&0&1&1&0&1&0&1\\ 0&0&1&0&1&0&1&1&1&1&1&1&0&1&1&0&1&1&1&1&0 \end{pmatrix}.$$

Теперь покажем, что знание $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma} = \mathcal{A}_{r,q}(\tilde{D},\tilde{G})$, дивизоров $\tilde{D}$ и $\tilde{G}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала восстановим дивизор G. Как сказано ранее, если $\sigma \sim \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$, то дивизор G можно восстановить, применив алгоритм 1:

$$\tilde{G} = 1\cdot(\alpha^5+\alpha^2+\alpha+1:1),\\ a^{\ell(\ell-1)/2}X^{\ell} - \tilde{\gamma} = X^3 + (\alpha^5+\alpha^2+\alpha+1), \tag{9}$$

где $a = \alpha^{21}$ — корень из единицы степени ℓ.

Корням многочлена (9) соответствуют следующие точки проективной прямой:

$$(\alpha^3+1:1),\ (\alpha^5+\alpha^2+1:1),\ (\alpha^5+\alpha^3+\alpha^2:1).$$

Данные точки входят в носитель оригинального дивизора G. Таким образом, дивизор G полностью восстановлен.

Перейдём к восстановлению носителя дивизора D. В первую очередь необходимо найти одно решение системы (6) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \operatorname{supp}(\tilde{D})$, принимая во внимание, что

$$\operatorname{supp}(\tilde{D}) = \{(\alpha^3:1),\ (\alpha^4+\alpha^3+\alpha+1:1),\ (\alpha^5+\alpha^4+\alpha^2+1:1),\ (\alpha^5+\alpha^3+1:1),\\ (\alpha^5+\alpha^2,1),\ (\alpha^4+\alpha^2+\alpha+1:1),\ (\alpha^3+\alpha^2+\alpha:1)\}.$$

Корням системы соответствуют следующие точки проективной прямой:

$$(\alpha^4+\alpha^3+\alpha^2+\alpha:1),\ (\alpha^5+\alpha^4+\alpha^3+\alpha^2:1),\ (\alpha^5+\alpha^3+\alpha+1:1),\\ (\alpha^3+\alpha^2+1:1),\ (\alpha^4+\alpha^3+\alpha:1),\ (\alpha^4+\alpha^3+\alpha+1:1),\ (\alpha^5+\alpha^4+\alpha^2+\alpha:1).$$

При этом

$$\operatorname{supp}(D') = \left\{\left(a^j\frac{\alpha'_i}{\beta'_i} : 1\right) : j\in\{0,\dots,\ell{-}1\}, i\in\{1,\dots,n/l\}\right\} = \{(\alpha^4{+}\alpha^3{+}\alpha^2{+}\alpha : 1), (\alpha : 1),$$
$$(\alpha^4+\alpha^3+\alpha^2 : 1), (\alpha^5+\alpha^4+\alpha^3+\alpha^2 : 1), (\alpha^2 : 1), (\alpha^5+\alpha^4+\alpha^3 : 1), (\alpha^5+\alpha^3+\alpha+1 : 1),$$
$$(\alpha^5+\alpha+1 : 1), (\alpha^3 : 1), (\alpha^3+\alpha^2+1 : 1), (\alpha^4+\alpha^3+\alpha^2+1 : 1), (\alpha^4 : 1), (\alpha^4+\alpha^3+\alpha : 1),$$
$$(\alpha^5+\alpha^4+\alpha^3+\alpha : 1), (\alpha^5 : 1), (\alpha^4+\alpha^3+\alpha+1 : 1), (\alpha^5+\alpha^4+\alpha^2 : 1),$$
$$(\alpha^5+\alpha^3+\alpha^2+\alpha+1 : 1), (\alpha^5+\alpha^4+\alpha^2+\alpha : 1), (\alpha^5+\alpha^4+\alpha+1 : 1), (\alpha^2+1 : 1)\}.$$

Нетрудно заметить, что носители оригинального дивизора D и дивизора D' отличаются перестановкой. Последний шаг — восстановление перестановки между $\mathcal{A}_{r,q}(D',G)$ и $\mathcal{A}_{r,q}(D,G)$ путём решения матричного уравнения (8), где

$$\mathbf{H}'^{\top} = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&1&1&1&1&0&0&0&0&0&0&1&1&0&0&1&1&1\\
1&1&0&1&0&1&0&0&0&0&0&1&0&1&1&1&0&1
\end{pmatrix}.$$

В результате найденная перестановочная матрица имеет вид

$$\mathbf{\Pi} = \begin{pmatrix}
\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&\mathbf{1}
\end{pmatrix}.$$

Отметим, что в носителе $\mathrm{supp}(D')$ в блоках 1 и 2 на первом месте стоят третьи элементы из орбит соответствующих точек носителя оригинального дивизора, что соответствует единицам на главной диагонали матрицы $\mathbf{\Pi}$. В блоках 6 и 7 элементы не переставлены, а в блоках 3, 4 и 5 на первое место встали вторые элементы из орбит. Таким образом, найдя перестановку $\mathbf{\Pi}$, мы восстановили оригинальный носитель $\mathrm{supp}(D)$.

5.2. Случай, когда автоморфизм σ является тригонализируемым в $\mathbb{F}_{q^m}$

Сначала построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D, G)$ над $\mathbb{F}_{3^4}$ с параметрами $[15, 4]$ с помощью тригонализируемого автоморфизма

$$\sigma = \begin{pmatrix} 1 & 2\alpha^3 + \alpha^2 + \alpha + 1 \\ 0 & 1 \end{pmatrix},$$

где $\mathrm{ord}(\sigma) = \ell = \mathrm{Char}(\mathbb{F}_{q^m}) = 3$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{81}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
\mathrm{Orb}_\sigma(P_1) &= \big\{(1:1), (2\alpha^3 + \alpha^2 + \alpha + 2:1), (\alpha^3 + 2\alpha^2 + 2\alpha:1)\big\},\\
\mathrm{Orb}_\sigma(P_2) &= \big\{(2:1), (2\alpha^3 + \alpha^2 + \alpha:1), (\alpha^3 + 2\alpha^2 + 2\alpha + 1:1)\big\},\\
\mathrm{Orb}_\sigma(P_3) &= \big\{(2\alpha:1), (2\alpha^3 + \alpha^2 + 1:1), (\alpha^3 + 2\alpha^2 + \alpha + 2:1)\big\},\\
\mathrm{Orb}_\sigma(P_4) &= \big\{(2\alpha + 1:1), (2\alpha^3 + \alpha^2 + 2:1), (\alpha^3 + 2\alpha^2 + \alpha:1)\big\},\\
\mathrm{Orb}_\sigma(P_5) &= \big\{(2\alpha + 2:1), (2\alpha^3 + \alpha^2:1), (\alpha^3 + 2\alpha^2 + \alpha + 1:1)\big\}.
\end{aligned}$$

Для построения дивизора G используем единственную точку $Q = (\alpha^2 + \alpha + 2 : 1)$ и параметр $t = 1$. В результате дивизор примет вид

$$G = \sum_{R \in \mathrm{Orb}(Q)} R = (\alpha^2 + \alpha + 2:1) + (\alpha^3 + 1:1) + (2\alpha^3 + 2\alpha^2 + 2\alpha:1)\,.$$

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, можно записать так:

$$\mathscr{L}(G) = \Big\{\frac{X^3}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{Y^3}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{XY^2}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}, \ \frac{X^2Y}{X^3 + \alpha^{54}XY^2 + \alpha^7Y^3}\Big\}.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix}
\alpha^{77} & \alpha^{23} & \alpha^{29} & \alpha^{6} & \alpha^{38} & \alpha^{32} & \alpha^{25} & \alpha^{50} & \alpha^{67} & \alpha^{16} & \alpha^{26} & \alpha^{76} & \alpha^{65} & \alpha^{58} & 1 \\
\alpha^{77} & \alpha^{77} & \alpha^{77} & \alpha^{46} & \alpha^{46} & \alpha^{46} & \alpha^{62} & \alpha^{62} & \alpha^{62} & \alpha^{65} & \alpha^{65} & \alpha^{65} & \alpha^{21} & \alpha^{21} & \alpha^{21} \\
\alpha^{77} & \alpha^{59} & \alpha^{61} & \alpha^{6} & \alpha^{70} & \alpha^{68} & \alpha^{23} & \alpha^{58} & \alpha^{37} & \alpha^{22} & \alpha^{52} & \alpha^{42} & \alpha^{9} & \alpha^{60} & \alpha^{14} \\
\alpha^{77} & \alpha^{41} & \alpha^{45} & \alpha^{46} & \alpha^{14} & \alpha^{10} & \alpha^{64} & \alpha^{54} & \alpha^{12} & \alpha^{59} & \alpha^{39} & \alpha^{19} & \alpha^{77} & \alpha^{19} & \alpha^{7}
\end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D, G) = \mathcal{C}_{\mathscr{L}}(D, G)^{\perp} \cap \mathbb{F}_q^n$. В результате получим квазициклический альтернантный код с параметрами $[15, 3]$ и порождающей матрицей

$$\mathbf{G}_{\mathrm{pub}} = \begin{pmatrix}
1 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 2 \\
0 & 1 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 0 & 2 \\
0 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 0
\end{pmatrix}.$$

Покажем, что знание $\overline{\mathcal{A}_{r,q}(D,G)}^{\sigma} = \mathcal{A}_{r,q}(\tilde{D},\tilde{G})$, дивизоров $\tilde{D}$ и $\tilde{G}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала вычислим возможных кандидатов для элемента b, используя лемму 7:

$$P_b = \text{НОД}\left(\left\{\text{Res}_X(X^p - Y^{p-1}X - \tilde{\alpha}_i, X^{q^m} - X) : i \in \{1,\dots,n/\ell\}\right\}, Y^{q^m} - Y\right) = \\ = Y^9 + (\alpha^3 - \alpha^2 - \alpha)\,Y^7 + (-\alpha^3 - \alpha^2 - \alpha - 1)\,Y.$$

Таким образом, элемент b — один из корней многочлена P_b. Соответственно

$$B' = \text{roots}\,(P_b) = \{1,\ 2\alpha^3 + 2\alpha + 2,\ 2\alpha^2 + 2\alpha,\ \alpha^3 + \alpha + 1, \alpha^3 + 2\alpha^2 + 2\alpha + 1, \\ \alpha^3 + 2\alpha^2 + 2\alpha + 2,\ \alpha^2 + \alpha,\ 2\alpha^3 + \alpha^2 + \alpha + 1,\ 2\alpha^3 + \alpha^2 + \alpha + 2\}.$$

Далее покажем восстановление дивизора G при правильном выборе b. Если $\sigma \sim \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, то дивизор G можно восстановить, применив алгоритм 2:

$$\tilde{G} = 1 \cdot (\alpha^3 + 2\alpha^2 + 2\alpha + 2 : 1), \\ X^p - b^{p-1}X - \tilde{\gamma} = X^3 + (2\alpha^3 + 2\alpha^2 + 2\alpha + 1)X + 2\alpha^3 + \alpha^2 + \alpha + 1, \qquad (10)$$

где $b = 2\alpha^3 + \alpha^2 + \alpha + 1$.

Корням многочлена (10) соответствуют следующие точки проективной прямой:

$$(\alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 1 : 1),\ (2\alpha^3 + 2\alpha^2 + 2\alpha : 1).$$

Данные точки входят в носитель оригинального дивизора G. Таким образом, дивизор G полностью восстановлен.

Перейдём к восстановлению носителя дивизора D. В первую очередь необходимо найти одно решение системы (7) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \text{supp}(\tilde{D}) = \{(2\alpha^3 + 2\alpha^2 + \\ + 2\alpha + 2 : 1), (\alpha^3 + \alpha^2 + \alpha + 1 : 1), (\alpha^3 + \alpha^2 + 2\alpha + 1 : 1), (\alpha : 1), (2\alpha^3 + 2\alpha^2 + 2 : 1)\}$. Корням системы соответствуют следующие точки проективной прямой:

$$(1 : 1),\ (2\alpha^3 + \alpha^2 + \alpha : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha : 1),\ (2\alpha^3 + \alpha^2 : 1).$$

При этом

$$\text{supp}(D') = \left\{\left(\frac{\alpha'_i}{\beta'_i} + b \cdot j : 1\right) : j \in \{0,\dots,\ell-1\}, i \in \{1,\dots,n/\ell\}\right\} = \{(1 : 1), \\ (2\alpha^3 + \alpha^2 + \alpha + 2 : 1),\ (\alpha^3 + 2\alpha^2 + 2\alpha : 1),\ (2\alpha^3 + \alpha^2 + \alpha : 1),\ (\alpha^3 + 2\alpha^2 + 2\alpha + 1 : 1), \\ (2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 2 : 1),\ (2\alpha : 1),\ (2\alpha^3 + \alpha^2 + 1 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha : 1), \\ (2\alpha + 1 : 1),\ (2\alpha^3 + \alpha^2 + 2 : 1),\ (2\alpha^3 + \alpha^2 : 1),\ (\alpha^3 + 2\alpha^2 + \alpha + 1 : 1),\ (2\alpha + 2 : 1)\}.$$

Нетрудно заметить, что носители оригинального дивизора D и дивизора D' отличаются перестановкой. Последний шаг — восстановление перестановки между $\mathcal{A}_{r,q}(D',G)$ и $\mathcal{A}_{r,q}(D,G)$ путём решения матричного уравнения (8), где

$$\mathbf{H'}^{\top} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2 & 1 & 2 & 0 & 2 & 2 & 2 & 0 & 2 & 1 & 1 & 1 \\
2 & 2 & 1 & 2 & 0 & 2 & 2 & 2 & 0 & 1 & 1 & 1 \\
1 & 2 & 2 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 1
\end{pmatrix}.$$

В результате найденная перестановочная матрица имеет вид

$$\mathbf{\Pi} = \begin{pmatrix}
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1}
\end{pmatrix}$$

Отметим, что в носителе $\operatorname{supp}(D')$ в блоке 1 все элементы стоят на своих местах, в блоках 2 и 5 на первое место встали вторые элементы из орбит, а в блоках 3 и 4 на первом месте стоят третьи элементы из орбит соответствующих точек носителя оригинального дивизора, что соответствует единицам на главной диагонали матрицы $\mathbf{\Pi}$. Таким образом, найдя перестановку $\mathbf{\Pi}$, мы восстановили оригинальный носитель $\operatorname{supp}(D)$.

Замечание 13. В данном примере параметр b, а также перестановка, являющаяся решением системы (8), находятся неоднозначно, однако для полей большего порядка и параметров $[n \geqslant 2048, k \geqslant n/2]$, использующихся в криптографических схемах, экспериментально не удалось получить ни одного случая множественности решений. Ввиду этого выбор правильных параметров в примере был опущен.

5.3. Случай, когда автоморфизм σ является диагонализируемым в $\mathbb{F}_{q^{2m}} \backslash \mathbb{F}_{q^m}$

Будем полагать, что злоумышленнику известен оригинальный автоморфизм σ. В таком случае вычисление параметров исходного кода тривиально. В прошлых примерах поиск эквивалентного автоморфизма σ' был опущен, так как данная задача легко разрешима при использовании малого параметра ℓ. Здесь же рассмотрим, как осуществляется вычисление параметров кода $\overline{\tilde{\mathcal{C}}}^{\sigma}$, определённого над $\mathbb{F}_{q^{2m}}$, и покажем, что, зная автоморфизм, можно найти параметры оригинального кода, не используя алгоритмы, представленные в п. 4.

Сначала построим QC-GRS-код $\mathcal{C}_{\mathscr{L}}(D,G)$ над полем $\mathbb{F}_{125}$ с параметрами $[15,4]$ с помощью автоморфизма

$$\sigma = \begin{pmatrix} 3\alpha & 3\alpha^2+1 \\ 2\alpha^2+4 & 2\alpha+4 \end{pmatrix},$$

где $\operatorname{ord}(\sigma) = \ell = 3$.

Рассмотрим проективную прямую $\mathbf{P}^1$ над полем $\mathbb{F}_{125}$, а в качестве носителя дивизора D выберем следующие рациональные точки проективной прямой:

$$\begin{aligned}
&\operatorname{Orb}_\sigma(P_1) = \big\{(2:1),(2\alpha^2+2\alpha+1:1),(3\alpha^2+4\alpha+3:1)\big\},\\
&\operatorname{Orb}_\sigma(P_2) = \big\{(2\alpha:1),(3\alpha+3:1),(\alpha^2+2\alpha:1)\big\},\\
&\operatorname{Orb}_\sigma(P_3) = \big\{(2\alpha+1:1),(4\alpha^2+4\alpha+1:1),(2\alpha^2+3\alpha+4:1)\big\},\\
&\operatorname{Orb}_\sigma(P_4) = \big\{(2\alpha+2:1),(\alpha^2+4:1),(4\alpha^2+2\alpha+3:1)\big\},\\
&\operatorname{Orb}_\sigma(P_5) = \big\{(2\alpha+3:1),(\alpha+1:1),(\alpha^2+4\alpha:1)\big\}.
\end{aligned}$$

Для построения дивизора G используем единственную точку $Q = (\alpha^2+4\alpha+3:1)$ и параметр $t=1$. В результате дивизор примет вид

$$G = \sum_{R\in\operatorname{Orb}(Q)} R = (\alpha^2+4\alpha+3:1) + (\alpha^2+4\alpha+2:1) + (\alpha^2+2\alpha+1:1).$$

В соответствии с леммой 3 базис пространства Римана — Роха, ассоциированного с дивизором G, запишется так:

$$\mathscr{L}(G) = \Big\{\frac{X^3+Y^3}{T(X)}, \frac{XY^2}{T(X)}, \frac{X^2Y}{T(X)}, \frac{X^3}{T(X)}\Big\}, \text{ где } T(X) = X^3 + \alpha^{87}X^2Y + \alpha^{41}XY^2 + \alpha^{89}Y^3.$$

Таким образом, порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D,G)$ будет иметь следующий вид:

$$G_{\mathcal{C}_{\mathscr{L}}} = \begin{pmatrix}
\alpha^{118} & \alpha^{106} & \alpha^{6} & \alpha^{116} & \alpha^{64} & \alpha^{81} & \alpha^{39} & \alpha^{38} & \alpha^{98} & \alpha^{30} & \alpha^{123} & \alpha^{102} & \alpha^{42} & \alpha^{82} & \alpha^{30} \\
\alpha^{87} & \alpha^{85} & \alpha^{3} & \alpha^{72} & \alpha^{73} & \alpha^{2} & \alpha^{44} & \alpha^{64} & 4 & 3 & \alpha^{86} & \alpha^{40} & \alpha^{101} & \alpha^{55} & \alpha^{121} \\
\alpha^{118} & \alpha^{47} & \alpha^{54} & \alpha^{104} & \alpha^{14} & \alpha^{79} & \alpha^{70} & \alpha^{116} & \alpha^{85} & \alpha^{96} & \alpha^{37} & \alpha^{26} & \alpha^{111} & \alpha^{27} & \alpha^{101} \\
\alpha^{25} & \alpha^{9} & \alpha^{105} & \alpha^{12} & \alpha^{79} & \alpha^{32} & \alpha^{96} & \alpha^{44} & \alpha^{108} & \alpha^{99} & \alpha^{112} & \alpha^{12} & \alpha^{121} & \alpha^{123} & \alpha^{81}
\end{pmatrix}.$$

Далее вычислим код $\mathcal{A}_{r,q}(D,G) = \mathcal{C}_{\mathscr{L}}(D,G)^{\perp} \cap \mathbb{F}_5^n$. В результате получим квазициклический альтернантный код с параметрами $[15,5]$ и порождающей матрицей

$$\mathbf{G}_{\text{pub}} = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 3 & 4 & 4 & 1 & 0 & 4 & 4 & 4 & 1 & 4 \\
0 & 1 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 4 & 4 & 0 & 2 & 3 & 4 \\
0 & 0 & 1 & 0 & 0 & 3 & 3 & 4 & 2 & 0 & 3 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 4 & 1 & 3 & 1 & 0 & 2 & 3 & 4 & 2 & 4 \\
0 & 0 & 0 & 0 & 1 & 4 & 2 & 4 & 4 & 3 & 2 & 0 & 3 & 1 & 1
\end{pmatrix}.$$

Теперь покажем, что знание кода $\overline{\tilde{\mathcal{C}}}^{\sigma}$ и дивизоров $\tilde{D}^{\otimes}$ и $\tilde{G}^{\otimes}$ с малыми параметрами позволит восстановить оригинальные параметры кода $\mathcal{A}_{r,q}(D,G)$.

Сначала восстановим дивизор G. Если $\sigma = \rho\circ\sigma_d\circ\rho^{-1}$, где $\rho \in \mathrm{PGL}_2(\mathbb{F}_{5^6})$, то дивизор G можно восстановить, применив алгоритм 1 к коду, однако это полностью дублирует пример в п. 5.1, поэтому покажем нахождение дивизора при знании автоморфизма σ:

$$M_{\sigma_d} = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{q^m} \end{pmatrix}, \quad \tilde{G} = 1\cdot(3\alpha^2+1:1),$$
$$\xi^{\ell(\ell-1)/2}X^{\ell} - \tilde{\gamma} = X^3 + (2\alpha^2+4), \tag{11}$$

где $\xi = 4\beta + 3$ — корень из единицы степени ℓ поля $\mathbb{F}_{5^6} \cong \mathbb{F}_{5^3}[x]/(X^2 + 3X + 3)$; β — корень неприводимого над $\mathbb{F}_{5^3}$ многочлена $X^2 + 3X + 3$.

Замечание 14. В данном случае выполнение условия $\xi \in \mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$ должно быть обязательным, иначе автоморфизм σ можно диагонализировать над $\mathbb{F}_{q^m}$. Нахождение ξ не составляет труда, так как всего существует $\phi(\ell)$ элементов порядка ℓ в $\mathbb{F}_{q^{2m}}$.

Корнями многочлена (11) являются следующие элементы:

$$(\alpha^2 + 4\alpha + 3),\ ((4\alpha^2 + \alpha + 2)\beta + 3\alpha^2 + 2\alpha + 4),\ ((\alpha^2 + 4\alpha + 3)\beta + \alpha^2 + 4\alpha + 3),$$

причём один из корней всегда лежит в поле $\mathbb{F}_{q^m}$ и входит в орбиту оригинального дивизора G. Предыдущее утверждение легко проверить, рассмотрев вид точки $\tilde{Q}$:

$$\tilde{Q}^{\otimes} = \left((-1)^{\ell-1}\xi^{\ell(\ell-1)/2}\left(\frac{\gamma_0}{\delta_0 \cdot \xi^{q^m}}\right)^{\ell} : 1\right) \overset{\ell-\text{нечёт.}}{=} \left(\left(\frac{\gamma_0}{1}\right)^{\ell} : 1\right).$$

Таким образом, среди корней многочлена (11) всегда есть элемент γ_0, которому соответствует точка $(\gamma_0 : 1)$, входящая в оригинальный дивизор G. Поэтому при известном автоморфизме σ дальнейшее восстановление дивизора не требует рассмотрения оставшихся корней и соответствующих им точек из поля $\mathbb{F}_{5^6}$. Достаточно применить автоморфизм σ к найденной точке ℓ раз:

$$G = (\alpha^2 + 4\alpha + 3 : 1) + (\alpha^2 + 4\alpha + 2 : 1) + (\alpha^2 + 2\alpha + 1 : 1).$$

Перейдём к восстановлению носителя дивизора $D^{\otimes}$. В первую очередь необходимо найти одно решение системы (6) для каждой точки $(\tilde{\alpha}_i : \tilde{\beta}_i) \in \operatorname{supp}(\tilde{D}^{\otimes})$, принимая во внимание, что

$$\operatorname{supp}(\tilde{D}^{\otimes}) = \{(3 : 1),\ (\alpha + 1 : 1),\ (2\alpha^2 + 2\alpha + 2 : 1),\ (4\alpha^2 + 4 : 1),\ (\alpha^2 + 3 : 1)\}.$$

Как и в случае нахождения дивизора G, очевидно, среди корней системы будут те, что соответствуют точкам, входящим в носитель оригинального дивизора D, следовательно, применив автоморфизм σ к каждому решению ℓ раз, восстановим оригинальный носитель. Если решать систему над полем $\mathbb{F}_{5^6}$, то получаем

$$\operatorname{supp}(D'^{\otimes}) = \left\{\left(a^j \frac{\alpha_i'^{\otimes}}{\beta_i'^{\otimes}} : 1\right) : j \in \{0, \ldots, \ell - 1\}, i \in \{1, \ldots, n/l\}\right\} = \Big\{(2 : 1), (3\beta + 1 : 1),$$
$$(2\beta + 2 : 1), (2\alpha : 1), (3\alpha\beta + \alpha : 1), (2\alpha\beta + 2\alpha : 1), (2\alpha + 1 : 1), ((3\alpha + 4)\beta + \alpha + 3 : 1),$$
$$((2\alpha + 1)\beta + 2\alpha + 1 : 1), (2\alpha + 2 : 1), ((3\alpha + 3)\beta + \alpha + 1 : 1), ((2\alpha + 2)\beta + 2\alpha + 2 : 1),$$
$$(2\alpha + 3 : 1), ((3\alpha + 2)\beta + \alpha + 4 : 1), ((2\alpha + 3)\beta + 2\alpha + 3 : 1)\Big\},$$

что подтверждает предыдущее замечание.

При этом без знания автоморфизма σ необходимо восстанавливать перестановку, решая систему уравнений (8) над полем $\mathbb{F}_{5^6}$, чтобы получить исходный носитель. Затем, как показано в п. 4.1, необходимо найти отображение ρ', такое, что $\sigma_d = \rho' \circ \sigma' \circ \rho'^{-1}$, чтобы получить исходные дивизоры.

ЛИТЕРАТУРА

1. *Barelli E.* On the Security of Some Compact Keys for McEliece Scheme. `https://arxiv.org/abs/1803.05289`. 2018.
2. *Кунинец А. А., Малыгина Е. С.* Вычисление пар, исправляющих ошибки, для алгеброгеометрического кода // Прикладная дискретная математика. 2024. № 63. С. 65–90.
3. *Малыгина Е. С., Кунинец А. А., Раточка В. Л. и др.* Алгеброгеометрические коды и декодирование на основе пар, исправляющих ошибки // Прикладная дискретная математика. 2023. № 62. С. 83–105.
4. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
5. *Stichtenoth H.* On automorphisms of geometric Goppa codes // J. Algebra. 1990. No. 130(1). P. 113–121.
6. *Conrad K.* The Minimal Polynomial and some Applications. `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf`. 2008.
7. *Clark P. L.* Linear Algebra: Invariant Subspaces. `http://alpha.math.uga.edu/~pete/invariant_subspaces.pdf`. 2013.
8. *Faugére J.-C., Otmani A., Perret L., et al.* Folding alternant and Goppa codes with non-trivial automorphism groups // IEEE Trans. Inform. Theory. 2016. No. 62(1). P. 184–121.

REFERENCES

1. *Barelli E.* On the Security of Some Compact Keys for McEliece Scheme. `https://arxiv.org/abs/1803.05289`, 2018.
2. *Kuninets A. A. and Malygina E. S.* Vychislenie par, ispravlyayushchikh oshibki, dlya algebro-geometricheskogo koda [Calculation of error-correcting pairs for an algebraic-geometric code]. Prikladnaya Diskretnaya Matematika, 2024, no. 63, pp. 65–90. (in Russian)
3. *Malygina E. S., Kuninets A. A., Ratochka V. L., et al.* Algebrogeometricheskie kody i dekodirovanie na osnove par, ispravlyayushchikh oshibki [Algebraic-geometry codes and decoding by error-correcting pairs]. Prikladnaya Diskretnaya Matematika, 2023, no. 62, pp. 83–105. (in Russian)
4. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
5. *Stichtenoth H.* On automorphisms of geometric Goppa codes. J. Algebra, 1990, no. 130(1), pp. 113–121.
6. *Conrad K.* The Minimal Polynomial and some Applications. `https://kconrad.math.uconn.edu/blurbs/linmultialg/minpolyandappns.pdf`, 2008.
7. *Clark P. L.* Linear Algebra: Invariant Subspaces. `http://alpha.math.uga.edu/~pete/invariant_subspaces.pdf`, 2013.
8. *Faugére J.-C., Otmani A., Perret L., et al.* Folding alternant and Goppa codes with non-trivial automorphism groups. IEEE Trans. Inform. Theory, 2016, no. 62(1), pp. 184–121.