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.