УДК 519.17 DOI 10.17223/20710410/X/1

АНАЛИЗ МИНИМАЛЬНОГО РАССТОЯНИЯ АГ-КОДА, АССОЦИИРОВАННОГО С МАКСИМАЛЬНОЙ КРИВОЙ РОДА ТРИ[1]

Е. С. Малыгина, А. А. Кунинец

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

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

Рассматривается класс алгебро-геометрических кодов, ассоциированных с максимальной кривой рода три. С помощью аппарата функциональных полей устанавливается вид и степень дивизоров, участвующих в построении кода, при которых код является или не является MDS-кодом.

Ключевые слова: *алгебро-геометрический код, минимальное расстояние кода, mds-код, максимальная кривая, функциональное поле, дивизор.*

ANALYSIS OF MINIMAL DISTANCE OF AG-CODE ASSOCIATED WITH MAXIMAL CURVE OF GENUS THREE

E. S. Malygina, A. A. Kuninets

Immanuel Kant Baltic Federal University, Kaliningrad, Russia

We consider a class of algebraic geometry codes associated with a maximal curve of genus three whose number of rational points satisfies the upper Hasse-Weil-Serre bound. It is proved that the number of rational points of such curve is odd and has a classification: the first type includes 4-tuples of conjugate points of multiplicity 1, the second type – couples conjugate points of multiplicity 2, and the third type – a single point of multiplicity 4. It is found out for which types of points, the divisor of the functional field of the desired curve and consisting of these points, is the principle. We consider special cases when $\deg(G) = 2, 4$, and establish the form of a divisor D, when AG-code $\mathcal{C}_{\mathscr{L}}(D, G)$ associated with the divisors D and G is MDS-code. It is shown that the AG-code $\mathcal{C}_{\mathscr{L}}(D, G)$ is not an MDS-code if the divisor $D - G$ is principle and $\deg(G) \geqslant 5$. Also it is proved that $\mathcal{C}_{\mathscr{L}}(D, G)$ is an MDS code if the divisor D consists only of the first type points of curve conjugated to each other for $\deg(D) \geqslant 8$ and $G = \frac{\deg(D)+2}{2} P_\infty$. And finally it is shown that the dual equivalent code $\mathcal{C}_{\mathscr{L}}(D, H)^\perp$ to the code $\mathcal{C}_{\mathscr{L}}(D, G)$, which is not MDS, will also not be MDS with conditions $\deg(D) - \alpha < \deg(H) < \deg(D)$, $4 < \deg(G) < \alpha + 4$, $5 < \alpha < \deg(D) - 5$, and D consists only of conjugate points of the first type.

Keywords: *algebraic geometry code, minimal distance, mds-code, maximal curves, function field, divisor.*

[1]Работа выполнена за счет гранта Российского научного фонда № 22-41-0441 (https://rscf.ru/project/22-41-04411/).

Введение

Рассмотрим класс алгебро-геометрических кодов, ассоциированных с максимальной кривой рода три. Под линейным кодом $\mathcal{C}$ над простым конечным полем $\mathbb{F}_p$ характеристики p понимаем линейное подпространство векторного пространства $\mathbb{F}_p^n$. Обозначая за n длину кодового слова пространства $\mathcal{C}$, а за $k = [\mathcal{C} : \mathbb{F}_p]$— его размерность,считаем, что код $\mathcal{C}$ имеет параметры $[n, k]$. Кроме того, на векторном пространстве $\mathcal{C}$ задается в качестве метрики— вес Хэмминга— то есть число ненулевых координат кодового слова. Еще одним важным параметром кода является его минимальное расстояние $d(\mathcal{C})$ — минимальный вес Хэмминга среди всех весов Хэмминга кодовых слов кода $\mathcal{C}$. Оно позволяет определить число ошибок $t = \lfloor \frac{d-1}{2} \rfloor$, которое может быть исправлено кодом.

В 1981 г. В.Д. Гоппа в [1] представил класс кодов, ассоциированных с алгебраическими кривыми над конечными полями, которые получили название алгебро-геометрических кодов (АГ-коды). Для построения АГ-кода, описанного в статье, мы используем алгебраическую кривую, число точек которой достигает верхней границы Хассе— Вейля— Серра. Такие кривые называются максимальными и имеют большое число рациональных точек. Соответственно, чем выше отношение числа точек к роду кривой, тем лучшими характеристиками обладает построенный на кривой код.

Исследование АГ-кодов примечательно тем, что применяя аппарат теории функциональных полей, зачастую мы можем вычислить точные значения параметров кода, построенного на алгебраической кривой. Таким образом, анализ минимального расстояния рассматриваемого кода будет проведен с использованием дивизоров функционального поля, ассоциированного с максимальной кривой. Основное преимущество рассмотрения в качестве базовых инструментов исследования именно функциональных полей, а не геометрии алгебраических кривых, обусловлено тем, что функциональные поля кривых инвариантны относительно бирациональных изоморфизмов кривых.

Вычисление значения размерности k АГ-кода можно осуществить посредством вычисления размерности линейного пространства Римана— Роха, ассоциированного с некоторыми дивизорами кривой. Известная теорема Римана-Роха [2] во многих случаях позволяет сделать это точно. В общем случае минимальное расстояние кода удовлетворяет следующим неравенствам $n+1-g-k \leqslant d \leqslant n+1-k$. Задача вычисления точного значения минимального расстояния АГ-кодов затрагивает исследование, так называемых, MDS-кодов (maximum distance separable codes), минимальное расстояние которых достигает границы Синглтона, т.е. $d = n + 1 - k$. В работе представлен анализ некоторых случаев, когда АГ-коды являются/не являются MDS-кодами в зависимости от задания дивизоров функционального поля кривой, с которыми этот код ассоциирован.

Структура статьи следующая. В первом параграфе представлены предварительные сведения из теории функциональных полей, особое внимание уделено краткой теории дивизоров, поскольку именно они лежат в основе исследования. Второй параграф посвящен описанию максимальной кривой рода три, на базе которой строится АГ-код, и ее точек. В третьем параграфе отражен основной результат работы. Найдены ограничения на степени дивизоров D и G, ассоциированных с АГ-кодом $\mathcal{C}_{\mathscr{L}}(D, G)$, относительно которых показано, когда $\mathcal{C}_{\mathscr{L}}(D, G)$ является MDS-кодом, а когда нет.

1. Предварительные сведения из теории функциональных полей

На протяжении всех предварительных сведений под K будем понимать произвольное поле, при необходимости внося уточнения.

Определение 1. Алгебраическим функциональным полем F/K от одной переменной называется расширение F поля K, такое, что F является конечным алгебраическим расширением $K(x)$ для некоторого элемента $x \in F$, являющегося трансцендентным над K.

Для краткости будем называть F/K просто функциональным полем. Точками функционального поля являются максимальные идеалы, так называемого, кольца нормирования поля F, определение которого можно посмотреть в [2, Definition 1.1.4]. Под кольцом нормирования точки P будем понимать следующее множество:

$$\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}.$$

Множество всех точек функционального поля F/K будем обозначать $\mathbb{P}_F$. Степень точки P функционального поля F/K определим как степень расширения полей $\deg P = [\mathcal{O}_P/P : K]$.

Напомним, что, согласно [2], всякий элемент $0 \neq z \in F$ имеет единственное представление $z = t^n u$, если $P = t\mathcal{O}_P$, $u \in \mathcal{O}_P^*$ и $n \in \mathbb{Z}$.

Определение 2. С каждой точкой $P \in \mathbb{P}_F$ ассоциируем функцию

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

которая играет роль дискретного нормирования функционального поля F/K:

$$v_P(z) = n \quad \text{для} \quad z = t^n u, \quad v_P(0) = \infty.$$

Считаем, что точка P имеет нуль в z тогда и только тогда, когда $v_P(z) > 0$, и имеет полюс в z тогда и только тогда, когда $v_P(z) < 0$.

Определение 3. Абелева группа $\mathcal{D}_F$, порождённая точками функционального поля F/K, называется группой дивизоров поля F/K.

Элементы группы $\mathcal{D}_F$ называются дивизорами поля F/K. Дивизор представляет собой формальную сумму точек:

$$D = \sum_{P \in \mathbb{P}_F} n_P P, \quad \text{где} \quad n_P \in \mathbb{Z} \quad \text{и почти все} \quad n_P = 0.$$

Носителем дивизора D является множество

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

Для $P \in \mathbb{P}_F$ и дивизора D определим $v_P(D) = n_P$. Таким образом,

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

На $\mathcal{D}_F$ определено также частичное упорядочивание, а именно,

$$D_1 \leqslant D_2 \Leftrightarrow v_P(D_1) \leqslant v_P(D_2) \quad \text{для всех} \quad P \in \mathbb{P}_F.$$

Степень дивизора определяется следующим образом:

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

Определение 4. Пусть $f \in F \setminus \{0\}$. Обозначим через Z (через N) множество нулей (полюсов) функции f в $\mathbb{P}_F$. Тогда для 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:

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

Отметим также, что

$$\deg(f)_0 = \deg(f)_\infty = [F : K(f)].$$

Далее определим отношение эквивалентности в группе дивизоров $\mathcal{D}_F$.

Определение 5. Множество дивизоров вида

$$Princ_F = \{(x) : 0 \neq x \in F\}$$

называется группой главных дивизоров поля F/K.

Несложно проверить, что $Princ_F$ действительно является подгруппой группы $\mathcal{D}_F$ относительно операции сложения $(f) + (g) = (fg)$ для $f, g \in F \setminus \{0\}$.

Определение 6. Факторгруппа

$$Cl_F = \mathcal{D}_F / Princ_F$$

называется группой классов дивизоров поля F/K. Элементами Cl_F являются классы $[D]$, задаваемые представителями D. Будем говорить, что два дивизора D и D' из $\mathcal{D}_F$ эквивалентны $D \sim D'$, если имеет место равенство $D = D' + (f)$ для некоторой ненулевой функции $f \in F$.

Теперь дадим определение пространству Римана — Роха, одному из главных понятий в теории функциональных полей.

Определение 7. Для дивизора $D \in \mathcal{D}_F$ пространством Римана — Роха называется множество вида:

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

Отметим, что $\mathscr{L}(D)$ является конечномерным векторным пространством над полем K, при этом, целое $\dim D = \dim \mathscr{L}(D)$ называется размерностью дивизора D.

Определение 8. Род функционального поля F/K определён следующим образом

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

Отметим также, что благодаря некоторым ограничениям, накладываемым на степень дивизора, мы можем точно вычислить размерность пространства Римана — Роха, ассоциированного с этим дивизором, или для простоты размерность самого дивизора. Формула для подсчета размерности непосредственно следует из известной теоремы Римана-Роха [2, Theorem 1.5.15]:

Теорема 1. Если D — дивизор F/K и $\deg(D) \geqslant 2g - 1$, то

$$\dim(D) = \deg(D) + 1 - g.$$

2. Максимальная кривая рода три

Определение 9. Пусть C — гладкая неприводимая проективная кривая рода g, определённая над конечным полем $\mathbb{F}_p$. Назовем кривую C оптимальной, если число её рациональных точек удовлетворяет границе Хассе — Вейля — Серра

$$\#C(\mathbb{F}_p) = p + 1 \pm g(C)\lfloor 2\sqrt{p}\rfloor.$$

В случае «$-$» кривая называется минимальной, в случае «$+$» — максимальной.

В работе мы будем рассматривать максимальные кривые рода три. Максимальность обеспечит построение длинных кодов, а значение рода $g(C) = 3$ позволит задать кривую явно согласно [3, Предложение 3.2.1]:

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases} \tag{1}$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, a, b \in \mathbb{F}_p$.

Такие кривые существуют над определенными конечными полями, а именно, над полями с дискриминантами $\{-19, -43, -67, -163\}$ [3]. Под дискриминантом конечного поля $\mathbb{F}_p$ будем понимать число

$$d(\mathbb{F}_p) = \lfloor 2\sqrt{p}\rfloor^2 - 4p.$$

Мы можем упростить уравнение (1), сведя его к переменным x и z. Выражая из первого уравнения системы значение $y = \frac{z^2-\alpha_2 x^2-\alpha_1 x-\alpha_0}{\beta_0}$ и подставляя его во второе уравнение, получаем

$$z^4+(-2\alpha_2 x^2-2\alpha_1 x-2\alpha_0)z^2+(\alpha_2^2 x^4+(2\alpha_1\alpha_2-\beta_0^2)x^3+(2\alpha_0\alpha_2+\alpha_1^2)x^2+(2\alpha_0\alpha_1-\beta_0^2 a)x+(\alpha_0^2-\beta_0^2 b)) = 0.$$

Очевидно, что при заданном значении $x \in \mathbb{F}_p$ уравнение может иметь 4 различных простых корня, либо 2 различных корня кратности 2 каждый или один корень кратности 4. Сопоставим эти корни точкам кривой согласно трём типам:

— Если уравнение имеет 4 различных корня, соответствующих точкам P_1, P_2, P_3, P_4, то будем относить эти точки к типу I.
— Если уравнение имеет только 2 различных корня кратности 2 каждый, соответствующих точкам Q_1 и Q_2, то будем относить эти точки к типу II.
— Если уравнение имеет единственный корень кратности 4, соответствующий точке P, то будем относить эту точку к типу III.

Отметим, что число рациональных точек рассматриваемой кривой является нечетным.

Утверждение 1. Число рациональных точек кривой $C/\mathbb{F}_p$ всегда будет нечетным и иметь вид $4s_1 + 2s_2 + 1$.

Доказательство. Согласно границе Хассе— Вейля— Серра, число точек максимальной кривой удовлетворяет условию

$$|C(\mathbb{F}_p)| = p + 1 + 3\lfloor 2\sqrt{p}\rfloor.$$

Мы рассматриваем кривые над конечными полями с нечетными дискриминантами $d = (\lfloor 2\sqrt{p}\rfloor)^2 - 4p$. Учитывая, что характеристика поля p — нечетное число, имеем $\lfloor 2\sqrt{p}\rfloor$ — нечетно, откуда $|C(\mathbb{F}_p)|$ — нечетно.

Принимая во внимание типы точек, получаем

$$|C(\mathbb{F}_p)| = n = 4s_1 + 2s_2 + 1,$$

где s_1— число четверок типа I, s_2— число двоек типа II. Заметим, что точка с координатой $(x, 0)$ у рассматриваемого типа кривой будет, всегда одна. ■

Замечание 1. Отметим, что бесконечно удаленная точка кривой C, которую обозначим P_∞, не является $\mathbb{F}_p$-рациональной.

Согласно [3, Предложение 3.1.2] оптимальная кривая C рода 3 над $\mathbb{F}_p$ является двойным накрытием оптимальной эллиптической кривой. Обозначив это накрытие $f : C \to E$, получаем, что при отображении f бесконечно удаленная точка P_∞ кривой C лежит над бесконечно удаленной точкой ∞ эллиптической кривой E, которая, в свою очередь, лежит над бесконечной точкой проективной прямой $\mathbb{P}^1$. При этом $\deg P_\infty = 2$, что соответствует степени накрытия.

3. Основной результат

Пусть $F = \mathbb{F}_p(C)$ — функциональное поле кривой, заданной уравнением (1), $P_1, P_2, \ldots, P_n$ — попарно различные точки поля $F/\mathbb{F}_p$ степени один и $D = P_1 + \ldots + P_n$. Напомним, что P_∞ — бесконечно удаленная точка поля $F/\mathbb{F}_p$ степени два. Обозначим за G — дивизор поля $F/\mathbb{F}_p$, кратный P_∞, тогда $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \varnothing$.

Определение 10. АГ-кодом $\mathcal{C}_{\mathscr{L}}(D, G)$, ассоциированным с дивизорами D и G, является образ гомоморфизма:

$$ev : \begin{cases} \mathscr{L}(G) \to \mathbb{F}_p^n, \\ f \mapsto (f(P_1), \ldots, f(P_n)). \end{cases}$$

Очевидно, что ядро этого гомоморфизма $Ker(ev) = \mathscr{L}(G - D)$. Если $\deg G < n$, то $\mathscr{L}(G - D) = \{0\}$. Следовательно, ev — инъективно и

$$\dim \mathcal{C}_{\mathscr{L}}(D, G) = \dim(G) = \dim \mathscr{L}(G) = \deg(G) + 1 - g = \deg(G) - 2$$

при условии, что $\deg(G) \geqslant 2g - 1 = 5$. Здесь используем утверждение Теоремы 1.

Отметим, что, согласно [2, Theorem 2.2.2], $\mathcal{C}_{\mathscr{L}}(D, G)$ является $[n, k, d]$-кодом с параметрами

$$k = \dim(G) - \dim(G - D) \quad \text{и} \quad d \geqslant n - \deg(G).$$

Для вычисления минимального расстояния $d = d(\mathcal{C})$ проведем следующие рассуждения. Пусть $c \in \mathcal{C}_{\mathscr{L}}(D, G)$ — кодовое слово веса δ. Тогда существует функция $f \in \mathscr{L}(G)$, такая, что $ev(f) = c$ и f обнуляется в точках $\{P_i | i \in I\}$ для некоторого $I \subseteq \{1, \ldots, n\}$ и $|I| = n - \delta$.

Если изначально рассмотреть $f \in \mathscr{L}(G - \sum_I P_i) \subset \mathscr{L}(G)$, то по определению пространства Римана-Роха имеем соотношение $(f) \geqslant \sum_I P_i - G$. Кроме того, $\deg(\sum_I P_i - G) = n - \delta - \deg(G)$. Если $\deg(G) = n - \delta$, то $\deg(\sum_I P_i - G) = 0$ и $(f) = \sum_I P_i - G$. Соответственно, $\sum_I P_i - G$ — главный дивизор.

Поскольку $G - \sum_I P_i < G$, то $\dim(G - \sum_I P_i) < \dim(G)$. Тогда, очевидно,

$$\dim(G - \sum_I P_i) + d(\mathcal{C}) < \dim(G) + d(\mathcal{C}) \leqslant n + 1.$$

Согласно вышесказанному и принимая во внимание, что $\deg(G) \geqslant 5$ и $\deg(G) = |\{P_i\}|$, имеем следующее утверждение:

Утверждение 2. Обозначим $D = \sum_I P_i$, где $I \subseteq \{1, \ldots, n\}$. Если дивизор $D - G$ является главным при условии, что $\deg(G) \geqslant 5$, то код $\mathcal{C}_{\mathscr{L}}(D, G)$ не является MDS-кодом.

Выясним, какие дивизоры в функциональном поле кривой $F/\mathbb{F}_p$ являются главными.

Лемма 1. Пусть $F = \mathbb{F}_p(C)$ — функциональное поле оптимальной кривой C рода три.

1) Точка P является точкой типа III тогда и только тогда, когда дивизор $4P - 2P_\infty$ является главным.
2) Точки Q_1 и Q_2 являются точками типа II тогда и только тогда, когда дивизор $2(Q_1 + Q_2) - 2P_\infty$ является главным.
3) Точки P_1, P_2, P_3, P_4 являются точками типа I тогда и только тогда, когда дивизор $P_1 + P_2 + P_3 + P_4 - 2P_\infty$ является главным.

Доказательство. Отметим, что для $f \in F \setminus \{0\}$ выполняется

$$\deg(f)_0 = \deg(f)_\infty = [F : \mathbb{F}_p(x)] = 4.$$

Далее приведем доказательство лишь первого случая, поскольку для оставшихся случаев рассуждения будут аналогичны.

(Достаточность): По условию существует функция $f \in F$, такая, что ее главный дивизор имеет вид

$$(f) = 4P - 2P_\infty.$$

Вычислим $\dim(2P_\infty)$. Учитывая, что кривая C не является гиперэллиптической [3, Лемма 3.1.3], и тот факт, что в гиперэллиптическом случае, если $\deg(P_\infty) = 2$, то $\dim(P_\infty) \geqslant 2$ [2, Lemma 6.2.2], получаем $\dim(P_\infty) = 1$. Согласно теореме Клиффорда [2, Theorem 1.6.13] имеем

$$\dim(2P_\infty) \leqslant 1 + \frac{1}{2} \cdot \deg(2P_\infty) = 3.$$

Определение оптимальной кривой уравнением (1) соответствует рассмотрению случая $\dim(2P_\infty) = 3$ [3]. Тогда в качестве f можем рассмотреть функцию $f \in \mathscr{L}(2P_\infty) = \langle 1, x, z \rangle$. Следовательно, $f \in \mathbb{F}_p(x, z)$ и $4P$ является дивизором нулей функции f в $\mathbb{F}_p(x, z)$, а значит, P — нуль функции f с кратностью 4. Таким образом, точка P относится к типу III.

(Необходимость): Если точка P над $\mathbb{F}_p(x)$ относится к типу III, значит, P является нулем некоторой функции $f \in \mathbb{F}_p(x, z)$ кратности 4. Тогда дивизор $4P - 2P_\infty$ имеет нулевую степень и по построению является главным, т.е. $(f) = 4P - 2P_\infty$. ■

Замечание 2. Отметим, что различные линейные комбинации представленных выше главных дивизоров также дадут главный дивизор.

Замечание 3. Поскольку в Утверждении 2 в записи дивизора D фигурируют точки без учета их кратности, то D является главным, если P_i, $1 \leqslant i \leqslant 4$ относятся к типу I и образуют четверки сопряженных точек.

Следовательно, $\mathcal{C}_{\mathscr{L}}(D, G)$ является MDS-кодом, если дивизор $D - G$ не является главным, причем дивизор $D = \sum_I P_i$, $I \subseteq \{1, \ldots, n\}$ все также состоит из четверок сопряженных точек, относящихся к типу I, и $\deg G \geqslant 5$. Однако не ясно, чему в этом случае равна степень дивизора G.

Прежде чем определить вид дивизора G при $\deg(G) \geqslant 5$, чтобы код $\mathcal{C}_{\mathscr{L}}$ являлся MDS-кодом, рассмотрим случаи, когда $\deg(G) < 5$.

Теорема 2. $\mathcal{C}_{\mathscr{L}}(D, P_\infty)$ является MDS-кодом для некоторого дивизора D степени 2.

Доказательство.

Поскольку $G = P_\infty$, то $\deg(G) = 2$ и $\dim(G) = 1$. Следовательно, базис пространства Римана— Роха $\mathscr{L}(G)$ состоит из единственной функции $\{1\}$. В качестве дивизора D рассмотрим $D = P_1 + \ldots + P_n$, где P_i, $1 \leqslant i \leqslant n$, — точки степени один любого типа. Соответственно, порождающая матрица кода имеет вид

$$(\,1(P_1) \quad \ldots \quad 1(P_n)\,) = (\,1 \quad \ldots \quad 1\,).$$

Очевидно, $k = 1$ и вес единственной строки матрицы равен числу точек n дивизора D. Таким образом, минимальное расстояние кода $d(\mathcal{C}) = n$, что есть верхняя граница Синглтона. Следовательно, код $\mathcal{C}_{\mathscr{L}}(D, P_\infty)$ является MDS-кодом. ■

Теорема 3. $\mathcal{C}_{\mathscr{L}}(D, 2P_\infty)$ является MDS-кодом, если дивизор D имеет следующий вид:

1) $D = P_1 + P_2 + P_3 + P_4$, где P_i — четверка сопряженных точек.
2) $D = P_1 + P_2 + Q_1 + Q_2$, где P_i и Q_i — пары сопряженных точек типа I или II.
3) $D = P_1 + P_2 + Q + S$, где P_i — пара сопряженных точек типа I или II, $Q \neq S$ — точки любого типа.

Доказательство. По условию $G = 2P_\infty$ и $\dim(G) = 3$. Соответственно, базис пространства Римана— Роха $\mathscr{L}(G)$ равен $\{1, x, z\}$, тогда порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет вид

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x(P) & x(Q) & x(S) & x(T) \\ z(P) & z(Q) & z(S) & z(T) \end{pmatrix},$$

где $P, Q, S, T \in supp(D)$.

1) Пусть $D = P_1 + P_2 + P_3 + P_4$. Порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет вид

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x(P_1) & x(P_2) & x(P_4) & x(P_4) \\ z(P_1) & z(P_2) & z(P_4) & z(P_4) \end{pmatrix}.$$

Поскольку $\{P_i\}_{1 \leqslant i \leqslant 4}$ образуют четверку сопряженных точек, то $x(P_1) = x(P_2) = x(P_4) = x(P_4)$, и, следовательно, первая и вторая строки матрицы эквивалентны. Это значит, что размерность кода $k = 2$ и $rank(M) = 3 = d(\mathcal{C})$, и $\mathcal{C}_{\mathscr{L}}(D, G)$ — MDS-код, так как $d(\mathcal{C}) = n + 1 - k$.

2) Пусть $D = P_1 + P_2 + Q_1 + Q_2$, где P_i и Q_i — пары сопряженных точек типа I или II. Порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет вид

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x(P_1) & x(P_2) & x(Q_1) & x(Q_2) \\ z(P_1) & z(P_2) & z(Q_1) & z(Q_2) \end{pmatrix}.$$

Поскольку $\{P_i\}_{1 \leqslant i \leqslant 2}$ и $\{Q_i\}_{1 \leqslant i \leqslant 2}$ образуют двойки сопряженных точек, то $x(P_1) = x(P_2)$ и $x(Q_1) = x(Q_2)$. Следовательно, $k = 3$ и $rank(M) = 2 = d(\mathcal{C})$. Тогда $\mathcal{C}_{\mathscr{L}}(D, G)$ — MDS-код, так как $d(\mathcal{C}) = n + 1 - k$.

3) $D = P_1 + P_2 + Q + S$, где P_i — пара сопряженных точек типа I или II, $Q \neq S$ — точки любого типа. Порождающая матрица кода $\mathcal{C}_{\mathscr{L}}(D, G)$ имеет вид

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x(P_1) & x(P_2) & x(Q) & x(S) \\ z(P_1) & z(P_2) & z(Q) & z(S) \end{pmatrix}.$$

Поскольку $\{P_i\}_{1 \leqslant i \leqslant 2}$ образуют двойки сопряженных точек, то $x(P_1) = x(P_2)$. Следовательно, $k = 3$ и $rank(M) = 2 = d(\mathcal{C})$. Тогда $\mathcal{C}_{\mathscr{L}}(D, G)$ — MDS-код. ■

Замечание 4. Отметим, что Теорема 3 работает в том случае, когда третья строка матрицы M состоит из различных элементов.

Замечание 5. Если $D = P_1 + P_2 + P_3 + Q$, где $\{P_i\}_{1 \leqslant i \leqslant 3}$ — сопряженные точки типа I, Q — точка любого типа, то $k = 3$, $d(\mathcal{C}) = 1$ и $\mathcal{C}_{\mathscr{L}}(D, G)$ не является MDS-кодом.

Теперь сформулируем и докажем теорему, когда D состоит из четверок сопряженных точек типа I, а $\deg(G) \neq 2, 4, n$.

Теорема 4. $\mathcal{C}_{\mathscr{L}}(D, G)$ является MDS-кодом, если дивизор D состоит только из четверок сопряженных точек типа I, $\deg(D) = n$, $n \geqslant 8$ и $G = \frac{n+2}{2} P_\infty$.

Доказательство. Поскольку число точек в записи дивизора D равно $n \equiv 0 \mod 4$, то $n = 4k$ для $k \in \mathbb{N}$ и

$$D = P_1^{(1)} + P_2^{(1)} + P_3^{(1)} + P_4^{(1)} + \ldots + P_1^{(k)} + P_2^{(k)} + P_3^{(k)} + P_4^{(k)},$$

где все точки $P_i^{(j)}$, $1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant k$, являются точками типа I.

Согласно Утверждению 2, $\mathcal{C}_{\mathscr{L}}(D, G)$ не является MDS-кодом, если $\deg(G) = n$, поскольку в этом случае дивизор $D - G$ является главным.

Определим, при каком G код $\mathcal{C}_{\mathscr{L}}(D, G)$ будет являться MDS-кодом. Так как

$$\frac{n}{2} P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) \leqslant \left(\frac{n}{2} + 1\right) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}),$$

то

$$\mathscr{L}\left(\frac{n}{2} P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)})\right) \subseteq \mathscr{L}\left(\left(\frac{n}{2} + 1\right) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)})\right).$$

Здесь мы рассматриваем ближайшее по включению пространство, учитывая, что $\dim \mathscr{L}(P_\infty) = 1$. Соответственно,

$$\frac{n}{2} P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) = \left(\frac{n}{2} + 1\right) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) - P_\infty,$$

откуда имеем

$$(2k + 1) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) = 2k P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) + P_\infty.$$

Поскольку дивизор $2k P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)})$ — главный, получаем

$$(2k + 1) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)}) \sim P_\infty.$$

Так как P_∞ не является главным дивизором, то дивизор $(2k + 1) P_\infty - (P_1^{(1)} + \ldots + P_4^{(k)})$ также неглавный. Следовательно, код $\mathcal{C}_{\mathscr{L}}(D, G)$ является MDS-кодом при $D = P_1^{(1)} + \ldots + P_4^{(k)}$ и $G = \left(\frac{n+2}{2}\right) P_\infty$. ■

Рассмотрим более общий случай, когда степень дивизора, с помощью которого вычисляется размерность кода, меньше числа точек дивизора D.

Теорема 5. Пусть $n \geqslant 12$, $\alpha \in \mathbb{N}$, $5 < \alpha < n-5$ и пусть задан дивизор $D = P_1^{(1)} + \ldots + P_4^{(k)}$, где $P_i^{(j)}$ образуют четверки сопряженных точек типа I и $n = 4k$, а также задан дивизор G, где $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \varnothing$ и $4 < \deg(G) < \alpha + 4$. Будем считать, что $\mathcal{C}_{\mathscr{L}}(D, G)$ не является MDS-кодом. Тогда существует дивизор H функционального поля F, такой, что $\operatorname{supp}(H) \cap \operatorname{supp}(D) = \varnothing$ и $n - \alpha < \deg(H) < n$, и код $\mathcal{C}_{\mathscr{L}}(D, H)$ не является MDS-кодом.

Доказательство. Доказательство проведем от противного. Предположим, что существует дивизор H, удовлетворяющий условиям теоремы, но код $\mathcal{C}_{\mathscr{L}}(D, H)$ является MDS-кодом. Согласно [4, Theorem 2.5], существует дивизор G, $\operatorname{supp}(G) \cap \operatorname{supp}(D) = \varnothing$ и $0 \leqslant \deg G \leqslant n$, и вектор $a \in \mathbb{F}_p^n$ веса n, такие, что

$$a \cdot \mathcal{C}_{\mathscr{L}}(D, G) = \mathcal{C}_{\mathscr{L}}(D, H)^{\perp}.$$

Для более детального ознакомления со структурой дуального кода см. [2]. Здесь мы только отметим, если $\mathcal{C}_{\mathscr{L}}(D, H)$ — дуальный код к $\mathcal{C}_{\mathscr{L}}(D, G)$, то

$$\dim(G) + \dim(H) = k.$$

Если $\mathcal{C}_{\mathscr{L}}(D, H)$ — MDS-код, то $\mathcal{C}_{\mathscr{L}}(D, H)^{\perp}$ также является MDS-кодом тогда и только тогда, когда $a \cdot \mathcal{C}_{\mathscr{L}}(D, G)$ — MDS-код, а это выполняется тогда и только тогда, когда $\mathcal{C}_{\mathscr{L}}(D, G)$ — MDS-код.

При этом, если $\deg(G) \geqslant 5$ и $\deg(H) \geqslant 5$, что выполняется по условию, то

$$\deg(G) - 2 = \dim(G) = n - \dim(H) = n - (\deg(H) - 2) = n + 2 - \deg(H).$$

Следовательно, $\deg(H) = n + 4 - \deg(G)$. Поскольку $n - \alpha < \deg(H) < n$, то

$$n - \alpha < n + 4 - \deg(G) < n,$$

откуда

$$4 < \deg(G) < \alpha + 4,$$

что противоречит условию, что $\mathcal{C}_{\mathscr{L}}(D, G)$ не является MDS-кодом. ■

ЛИТЕРАТУРА

1. *Goppa V. D.* Geometry and Codes. Kluwer Academic Publishers, 1988.
2. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
3. *Алексеенко Е. С.* Явные конструкции оптимальных кривых рода три. Кандидатская диссертация. 2016. http://iitp.ru/upload/content/1203/AES_disser.pdf
4. *Stichtenoth H.* Self dual Goppa codes // J. Pure Appl. Algebra. 1988. V. 55. P. 199–211.

REFERENCES

1. *Goppa V. D.* Geometry and Codes. Kluwer Academic Publishers, 1988.
2. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
3. *Alekseenko E.* Explicit constructions of optimal curves of genus three. PHD-thesis. 2016. http://iitp.ru/upload/content/1203/AES_disser.pdf
4. *Stichtenoth H.* Self dual Goppa codes // J. Pure Appl. Algebra. 1988. V. 55. P. 199–211.

МАЛЫГИНА Екатерина Сергеевна — кандидат физико-математических наук, доцент ОНК «Институт высоких технологий», младший научный сотрудник

лаборатории «Математические методы защиты и обработки информации» научно-образовательного математического центра «Северо-Западный центр математических исследований имени Софьи Ковалевской» БФУ им. И. Канта, г. Калининград.
E-mail: **emalygina@kantiana.ru**

КУНИНЕЦ Артем Андреевич — студент специальности «Компьютерная безопасность» ОНК «Институт высоких технологий» БФУ им. И. Канта, г. Калининград.
E-mail: **artkuninets@yandex.ru**