ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.725 DOI 10.17223/20710410/63/4

ВЫЧИСЛЕНИЕ ПАР, ИСПРАВЛЯЮЩИХ ОШИБКИ ДЛЯ АЛГЕБРОГЕОМЕТРИЧЕСКОГО КОДА[1]

А. А. Кунинец*, Е. С. Малыгина**

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

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

Для произвольного алгеброгеометрического кода и дуального к нему явно вычислены пары, исправляющие ошибки. Такая пара состоит из кодов, которые необходимы для эффективного алгоритма декодирования заданного кода. Вид пар зависит от степеней дивизоров, с помощью которых строится как исходный код, так и один из кодов, входящих в пару. Для алгеброгеометрического кода $\mathcal{C}_{\mathcal{L}}(D,G)$ длины n, ассоциированного с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g, парами, исправляющими $t=\lfloor(n-\deg(G)-g-1)/2\rfloor$ ошибок, при определённых ограничениях на степени дивизоров, участвующих в их построении, являются пары кодов $(\mathcal{C}_{\mathcal{L}}(D,F),\mathcal{C}_{\mathcal{L}}(D,G+F)^{\perp})$ или $(\mathcal{C}_{\mathcal{L}}(D,F)^{\perp},\mathcal{C}_{\mathcal{L}}(D,F-G))$. Выведены ограничения на степени дивизоров кодов $(\mathcal{C}_{\mathcal{L}}(D,F),\mathcal{C}_{\mathcal{L}}(D,G-F))$, составляющих пару, исправляющую $t=\lfloor(\deg(G)-3g+1)/2\rfloor$ ошибок для дуального кода $\mathcal{C}_{\mathcal{L}}(D,G)^{\perp}$. Рассмотрены случаи принадлежности одного из кодов, участвующих в построении пары, к классу MDS-кодов и выведены параметры, при которых данная ситуация возможна. Кроме того, вычислены возможные границы для дивизоров, участвующих в построении пар, исправляющих ошибки для подполевых подкодов $\mathcal{C}_{\mathcal{L}}(D,G)|_{\mathbb{F}_p}$ и $\mathcal{C}_{\mathcal{L}}(D,G)^{\perp}|_{\mathbb{F}_p}$ исходного алгеброгеометрического кода и дуального к нему, при степени расширения $m=2$ ($\mathbb{F}_q=\mathbb{F}_{p^2}$).

Ключевые слова: *функциональное поле, алгеброгеометрический код, исправляющая ошибки пара, подполевой подкод.*

CALCULATION OF ERROR-CORRECTING PAIRS FOR AN ALGEBRAIC-GEOMETRIC CODE

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

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

Error-correcting pairs are calculated explicitly for an arbitrary algebraic-geometric code and its dual code. Such a pair consists of codes that are necessary for an effective decoding algorithm for a given code. The type of pairs depends on the

[1]Работа первого автора поддержана грантом Российского научного фонда № 22-41-0441, работа второго автора выполнена в рамках Программы фундаментальных исследований НИУ ВШЭ.

degrees of divisors with which both the original code and one of the codes from error-correcting pair are constructed. So for the algebraic-geometric code $\mathcal{C}_{\mathcal{L}}(D,G)$ of the length n associated with a functional field $F/\mathbb{F}_q$ of genus g the error-correcting pair with number of errors $t=\lfloor(n-\deg(G)-g-1)/2\rfloor$ is $(\mathcal{C}_{\mathcal{L}}(D,F),\mathcal{C}_{\mathcal{L}}(D,G+F)^{\perp})$ or $(\mathcal{C}_{\mathcal{L}}(D,F)^{\perp},\mathcal{C}_{\mathcal{L}}(D,F-G))$. For the dual code $\mathcal{C}_{\mathcal{L}}(D,G)^{\perp}$ the error-correcting pair with number of errors $t=\lfloor(\deg(G)-3g+1)/2\rfloor$ is $(\mathcal{C}_{\mathcal{L}}(D,F),\mathcal{C}_{\mathcal{L}}(D,G-F))$. Considering each component of pair as MDS-code, we obtain additional conditions on the degrees of the divisors G and F. In addition, error-correcting pairs are calculated for subfield subcodes $\mathcal{C}_{\mathcal{L}}(D,G)|_{\mathbb{F}_p}$ and $\mathcal{C}_{\mathcal{L}}(D,G)^{\perp}|_{\mathbb{F}_p}$, where $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$. The form of a first component in the pair depends on the degrees of the divisors G and F and, in some cases, on the genus g.

Keywords: *functional field, algebraic-geometric code, error-correcting pair, subfield subcode.*

Введение

Исследование задачи декодирования кодов, построенных на алгебраических кривых, явилось очень востребованным за последние тридцать лет. Изначально Т. Хёхольдт и др. предложили синдромный алгоритм декодирования для кодов, ассоциированных с плоской кривой [1]. Затем А. Скоробогатов и С. Влэдуц обобщили этот алгоритм на произвольные кривые [2]. Далее Р. Пелликаан и Р. Кёттер независимо друг от друга предложили алгоритм декодирования, исключающий абстрактные понятия алгебраической геометрии и использующий пары, исправляющие ошибки [3, 4]. Парой, исправляющей ошибки для кода $\mathcal{C}$, является пара кодов $\mathcal{A}$ и $\mathcal{B}$, удовлетворяющая некоторым ограничениям на размерность и минимальное расстояние, а также условию, что покомпонентное произведение кодовых слов $\mathcal{A}$ и $\mathcal{B}$ содержится в дуальном коде $\mathcal{C}^{\perp}$. Существование такой пары обеспечивает эффективный алгоритм декодирования для алгеброгеометрических кодов (АГ-кодов), который использует лишь методы линейной алгебры. Особый интерес представляет построение таких пар, поскольку сама пара является входным параметром для алгоритма декодирования. Стоит также отметить, что пары, исправляющие ошибки, заслуживают внимания и с криптографической точки зрения, поскольку лежат в основе атаки на АГ-коды [5].

Структура работы следующая: в п. 1 мы даём предварительные сведения, касающиеся базовых объектов теории функциональных полей и алгебраических кривых, необходимых для задания АГ-кода с помощью пространства Римана — Роха, а также для задания дуального АГ-кода с помощью пространства дифференциалов. В п. 2 представлен основной результат работы, заключающийся в ряде теорем. Первоначально мы задаём пары, исправляющие ошибки для АГ-кода и дуального к нему, накладывая ограничения на степени их дивизоров. Затем мы исследуем, при каких значениях код из пары или исходный код, для которого находится пара, является MDS-кодом (т. е. минимальное расстояние кода достигает максимального значения границы Синглтона). Далее мы даём полную классификацию пар, исправляющих ошибки для подполевых подкодов исходного АГ-кода и дуального к исходному АГ-коду при условии, что эти коды определены над квадратичным расширением конечного поля. Классификация включает в себя явный вид кодов из пары, значение рода кривой, длину кода, а также условия, налагаемые на степени дивизоров, ассоциированных с исходным кодом и его подполевым подкодом.

Данная работа является продолжением работы, представленной на конференции SIBECRYPT'23 [6].

1. Предварительные сведения

1.1. Алгебраические кривые и функциональные поля

Будем обозначать через $\mathbb{F}_q$ конечное поле, состоящее из q элементов, где q — степень простого числа.

Под *проективной кривой* над конечным полем $\mathbb{F}_q$ понимается проективное многообразие над $\mathbb{F}_q$ размерности один, где проективное многообразие представляет собой неприводимое замкнутое подмножество в проективном пространстве $\mathbb{P}^n$ [7]. Далее будем обозначать проективную кривую через $\mathcal{X}$.

В большинстве случаев в теории кодирования используются кривые, определённые над конечным полем. Под *проективной кривой $\mathcal{X}$, определённой над* $\mathbb{F}_q$, будем понимать кривую $\mathcal{X} \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$, где $\overline{\mathbb{F}}_q$ — алгебраическое замыкание поля $\mathbb{F}_q$, причём однородный многочлен, определяющий кривую, имеет коэффициенты в $\mathbb{F}_q$.

Определим *поле функций кривой* $\mathcal{X}$:

$$\mathbb{F}_q(\mathcal{X}) = \left\{ \frac{g}{h} : g, h \in \mathbb{F}_q[x_1, \ldots, x_{n-1}],\ h \neq 0 \right\}.$$

Здесь сама кривая определена однородным многочленом из кольца $\mathbb{F}_q[X_1, \ldots, X_n]$ и $x_1 = \dfrac{X_1}{X_n}$, $\ldots$, $x_{n-1} = \dfrac{X_{n-1}}{X_n}$. Говорят, что $\mathbb{F}_q(\mathcal{X})$ является *функциональным полем кривой* $\mathcal{X}/\mathbb{F}_q$.

Пусть P — точка кривой $\mathcal{X}$. Функция $f \in \mathbb{F}_q(\mathcal{X})$ называется *регулярной в точке* P, если её можно записать в виде $f = \dfrac{g}{h}$ и $g(P) \neq 0$. Множество регулярных функций в точке P образует кольцо, называемое *локальным кольцом* $\mathcal{O}_P$. Отметим, что точка кривой может иметь степень. Точки кривой, имеющие координаты в $\mathbb{F}_q$, называются *рациональными точками* или *точками степени один*. Если координаты точки кривой лежат в расширении базового конечного поля, то точка имеет степень, равную степени этого расширения.

Приведём базовые определения и свойства функциональных полей, чтобы посмотреть, как они связаны с алгебраическими кривыми.

Алгебраическим функциональным полем $\mathcal{F}/\mathbb{F}_q$ от одной переменной называется расширение $\mathbb{F}_q(x)$ поля $\mathbb{F}_q$, являющееся конечным алгебраическим расширением для некоторого трансцендентного над $\mathbb{F}_q$ элемента $x \in \mathbb{F}_q(x)$. Соответственно функциональным полем от n переменных является конечное алгебраическое расширение $\mathbb{F}_q(x_1, \ldots, x_n)$, где $x_1, \ldots, x_n$ трансцендентны над $\mathbb{F}_q$.

Для функциональных полей аналогом локального кольца в случае алгебраических кривых является кольцо нормирования. *Кольцом нормирования* функционального поля $\mathcal{F}/\mathbb{F}_q$ называется кольцо $\mathcal{O}$, такое, что:

— $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$;
— для любого элемента $x \in \mathcal{F}$ выполняется: $x \in \mathcal{O}$ или $x^{-1} \in \mathcal{O}$.

Следует отметить, что если мы работаем над алгебраически замкнутым полем, то существует взаимно однозначное соответствие между точками кривой и точками её функционального поля, хотя точка функционального поля имеет совсем иную специфику. *Точкой* P функционального поля $\mathcal{F}/\mathbb{F}_q$ называется максимальный идеал некоторого кольца нормирования $\mathcal{O}$.

По свойствам кольца нормирования оно является локальным кольцом, а значит, $\mathcal{O}$ можно ассоциировать с его единственным максимальным идеалом P:

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

Кроме того, по свойствам кольца нормирования P является главным идеалом, следовательно, $P = t_P\mathcal{O}_P$, при этом элемент t_P называется *локальным параметром точки* P. Теперь определим *степень точки* P как степень расширения поля $\mathcal{O}_P/P$ над $\mathbb{F}_q$, а именно:

$$\deg(P) = [\mathcal{O}_P/P : \mathbb{F}_p].$$

Далее будем отождествлять кривую с её функциональным полем и перейдём к рассмотрению основополагающих объектов для определения АГ-кода — дивизорам кривой (или её функционального поля).

Группой дивизоров $\mathrm{Div}(\mathcal{X})$ проективной кривой $\mathcal{X}$ называется свободная абелева группа, порождённая точками $\mathcal{X}$. Элементы группы $D \in \mathrm{Div}(\mathcal{X})$ называются *дивизорами* и представляют собой формальную сумму точек:

$$D = \sum_{P\in\mathcal{X}} n_P P,$$

причём только конечное число $n_P \in \mathbb{Z}$ отлично от нуля.

Определим *степень дивизора* как

$$\deg(D) = \sum_{P\in\mathcal{X}} n_P \cdot \deg(P).$$

В группе $\mathrm{Div}(\mathcal{X})$ определено частичное упорядочивание:

$$\sum_{P\in\mathcal{X}} n_P P \geqslant \sum_{P\in\mathcal{X}} m_P P \;\Leftrightarrow\; n_P \geqslant m_P \text{ для любой точки } P \in \mathcal{X}.$$

Теперь определим *дивизор функции*. Пусть $f \in \mathbb{F}_q(\mathcal{X})^*$. Обозначим через Z (через N) множество нулей (полюсов) функции f, определяемых с помощью точек $P \in \mathcal{X}$. Тогда для функции f определим:

— её дивизор нулей:

$$(f)_0 = \sum_{P\in Z} n_P\, P, \text{ где } n_P \text{ — кратность, соответствующая точке } P;$$

— дивизор полюсов:

$$(f)_\infty = \sum_{P\in N} (-n_P)\, P, \text{ где } n_P \text{ — кратность, соответствующая точке } P;$$

— главный дивизор:

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

Чтобы определить дуальный код, потребуется ряд понятий, связанных с дифференцированием и дифференциалами.

Определим *дифференцирование* над $\mathbb{F}_q(\mathcal{X})$ как $\mathbb{F}_q$-линейное отображение

$$\triangle : \mathbb{F}_q(\mathcal{X}) \to \mathbb{F}_q(\mathcal{X}),$$

удовлетворяющее правилу Лейбница $\triangle(fg) = f\triangle(g) + g\triangle(f)$ для $f, g \in \mathbb{F}_q(\mathcal{X})$. Множество таких дифференцирований $\mathrm{Der}(\mathbb{F}_q(\mathcal{X}))$ образует векторное пространство над $\mathbb{F}_q(\mathcal{X})$.

Дифференциальной формой или *дифференциалом* на кривой $\mathcal{X}$ называется $\mathbb{F}_q(\mathcal{X})$-линейное отображение $\mathrm{Der}(\mathbb{F}_q(\mathcal{X})) \to \mathbb{F}_q(\mathcal{X})$. Множество всех дифференциалов кривой $\mathcal{X}$ будем обозначать $\Omega(\mathcal{X})$.

Рассмотрим отображение

$$\delta : \begin{cases} \mathbb{F}_q(\mathcal{X}) \to \Omega(\mathcal{X}), \\ f \mapsto \delta f, \end{cases}$$

сопоставляющее всякой функции f дифференциал $\delta f : \mathrm{Der}(\mathbb{F}_q(\mathcal{X})) \to \mathbb{F}_q(\mathcal{X})$ по правилу $\delta f(\triangle) = \triangle(f)$ для любого $\triangle \in \mathrm{Der}(\mathbb{F}_q(\mathcal{X}))$.

Отметим, что любой дифференциал $\omega \in \Omega(\mathcal{X})$ можно уникально представить как $\omega = f\delta t_P$ для точки $P \in \mathcal{X}$ и локального параметра t_P, где $f \in \mathbb{F}_q(\mathcal{X})$. Будем говорить, что P является нулём ω, если P — нуль функции f, аналогично P — полюс ω, если P является полюсом функции f. Тогда по аналогии с главным дивизором для функции $f \in \mathbb{F}_q(\mathcal{X})^*$ можно определить дивизор для дифференциала $\omega \in \Omega(\mathcal{X})^*$:

$$(\omega) = \sum_{P \in N} n_P P,$$

однако специфика вычисления значения n_P достаточно сложная, поэтому за деталями можно обратиться к [8]. При этом дивизор (ω) называется *каноническим*. Обозначим $W = (\omega)$, тогда, согласно [8], $\deg(W) = 2g - 2$.

Одним из важных понятий является понятие рода кривой (её функционального поля). Если $\mathcal{X}$ является гладкой проективной плоской кривой (как правило, именно такие кривые рассматриваются для приложений в теории кодирования) степени r, то $g(\mathcal{X}) = (r-1)(r-2)/2$.

1.2. Алгеброгеометрические коды и дуальные к ним

Рассмотрим две конструкции АГ-кодов, а именно: конструкцию АГ-кода с привлечением пространства Римана — Роха и конструкцию дуального к нему АГ-кода с привлечением пространства дифференциалов.

Построение $\mathcal{C}_{\mathcal{L}}(D, G)$

Пусть G — дивизор кривой $\mathcal{X}$. Определим множество

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : (f) \geqslant -G\}.$$

Оно является векторным пространством над $\mathbb{F}_q$ и называется *пространством Римана — Роха*. Обозначим $\dim_{\mathbb{F}_q}(\mathcal{L}(G)) = \ell(G)$. Благодаря теореме Римана — Роха, можно получить значение $\ell(G)$.

Теорема 1 [8, Theorem 1.5.15]. Пусть $\mathcal{X}$ — гладкая проективная кривая, W — её канонический дивизор. Тогда для любого дивизора $G \in \mathrm{Div}(\mathcal{X})$ справедливо равенство

$$\ell(G) = \deg(G) + 1 - g(\mathcal{X}) + \ell(W - G).$$

Кроме того, если $\deg(G) > 2g - 2$, то $\ell(G) = \deg(G) + 1 - g(\mathcal{X})$.

Пусть $P_1, P_2, \ldots, P_n$ — попарно различные рациональные точки кривой $\mathcal{X}$ или точки функционального поля $\mathbb{F}_q(\mathcal{X})$ степени один. Обозначим $D = P_1 + \ldots + P_n$ и G — дивизоры кривой $\mathcal{X}$, причём в записи дивизора G не участвуют точки дивизора D и $\deg(G) < n$. Рассмотрим отображение

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

Определение 1. АГ-кодом $\mathcal{C}_{\mathcal{L}}(D,G)$, ассоциированным с кривой $\mathcal{X}$ и дивизорами D и G, называется подпространство в $\mathbb{F}_q^n$ вида

$$\mathcal{C}_{\mathcal{L}}(D,G) = \{ev_D(f) : f \in \mathcal{L}(G)\}.$$

Отметим, что всякий код $\mathcal{C}_{\mathcal{L}}(D,G)$ можно задать параметрами $[n,k,d]$, где n — длина кода (число точек в записи дивизора D); $k = k(\mathcal{C})$ — размерность кода (размерность пространства Римана — Роха $\mathcal{L}(G)$); $d = d(\mathcal{C})$ — минимальное расстояние кода.

Согласно [8, Theorem 2.2.2], код $\mathcal{C}_{\mathcal{L}}(D,G)$ является $[n,k,d]$-кодом, причём

$$k \geqslant \deg(G) + 1 - g,\ d \geqslant n - \deg(G),$$

и если $2g - 2 < \deg(G) < n$, то $k = \deg(G) + 1 - g$.

Если $\{f_1, \ldots, f_k\}$ — базис $\mathcal{L}(G)$, то порождающая матрица кода $\mathcal{C}_{\mathcal{L}}(D,G)$ имеет следующий вид:

$$\begin{pmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ f_k(P_1) & f_k(P_2) & \ldots & f_k(P_n) \end{pmatrix}.$$

Построение $\mathcal{C}_{\Omega}(D,G)$

Для определения дуального кода к коду $\mathcal{C}_{\mathcal{L}}(D,G)$ определим множество

$$\Omega(G) = \{\omega \in \Omega(\mathcal{X}) : (\omega) \geqslant G\}.$$

Оно является векторным пространством над $\mathbb{F}_q$ и называется *пространством дифференциалов*. Размерность $\dim_{\mathbb{F}_q}(\Omega(G)) = i(G)$ называется *индексом специальности* дивизора G и равна

$$i(G) = \ell(G) - \deg(G) + g(\mathcal{X}) - 1.$$

Чтобы задать дуальный код непосредственно, нужно ввести понятия вычета дифференциала $\omega = f\delta t_P$ в точке P, где $f \in \mathbb{F}_q(\mathcal{X})$ и t_P — локальный параметр. Для этого разложим функцию f в ряд Лорана по степеням t_P:

$$f = \sum_{i=\alpha}^{\infty} \alpha_i t_P^i,$$

где $\alpha \in \mathbb{Z}$. *Вычетом дифференциала* ω *в точке* P называется коэффициент α_{-1} в представленном разложении, он обозначается $\mathrm{Res}_{\omega}(P)$.

Как и ранее, пусть $P_1, P_2, \ldots, P_n$ — попарно различные рациональные точки кривой $\mathcal{X}$, $D = P_1 + \ldots + P_n$ и G — дивизоры кривой $\mathcal{X}$, такие, что в записи дивизора G не участвуют точки дивизора D и $\deg(G) > 2g - 2$. Рассмотрим отображение

$$res_D : \begin{cases} \Omega(G) \to \mathbb{F}_q^n, \\ \omega \mapsto (\mathrm{Res}_{\omega}(P_1), \ldots, \mathrm{Res}_{\omega}(P_n)). \end{cases}$$

Определение 2. АГ-кодом $\mathcal{C}_{\Omega}(D,G)$, ассоциированным с кривой $\mathcal{X}$ и дивизорами D и G и являющимся дуальным к $\mathcal{C}_{\mathcal{L}}(D,G)$, называется

$$\mathcal{C}_{\Omega}(D,G) = \{res_D(\omega) : \omega \in \Omega(G - D)\}.$$

Если параметры кода $\mathcal{C}_\Omega(D,G)$ обозначить через $[n,k',d']$, то, согласно [8, Theorem 2.2.7],

$$k' = n + g - 1 - \deg G, \quad d' \geqslant \deg G - (2g-2),$$

если $2g-2 < \deg G < n$.

С учётом построения имеем

$$\mathcal{C}_\mathcal{L}(D,G)^\perp = \mathcal{C}_\Omega(D,G) \quad \text{и} \quad \mathcal{C}_\Omega(D,G) = \mathcal{C}_\mathcal{L}(D, D-G+W),$$

где $W = (\omega)$ — канонический дивизор кривой $\mathcal{X}$.

В общем случае рассматриваемые коды могут исправить до $\lfloor (d(d')-1)/2 \rfloor$ ошибок, где d и d' — минимальные расстояния кодов $\mathcal{C}_\mathcal{L}(D,G)$ и $\mathcal{C}_\Omega(D,G)$ соответственно. Будем называть код MDS-кодом, если его минимальное расстояние достигает границы Синглтона, т. е. $d(\mathcal{C}) = n + 1 - k(\mathcal{C})$.

1.3. Пары, исправляющие ошибки

Произведение Шура двух векторов $a, b \in \mathbb{F}_q^n$ определяется как произведение их соответствующих координат:

$$(a_1,\ldots,a_n) * (b_1,\ldots,b_n) = (a_1b_1,\ldots,a_nb_n),$$
$$(a_1,\ldots,a_n)^i = (a_1^i,\ldots,a_n^i).$$

Для кодов $\mathcal{A},\mathcal{B} \subset \mathbb{F}_q^n$ произведение Шура $\mathcal{A} * \mathcal{B}$ определяется следующим образом:

$$\mathcal{A} * \mathcal{B} = \mathrm{Span}_{\mathbb{F}_q}\{a * b \mid a \in \mathcal{A}, b \in \mathcal{B}\}.$$

Определение 3. 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) $\dim(\mathcal{A}) > t$;
3) $d(\mathcal{B}^\perp) > t$;
4) $d(\mathcal{A}) + d(\mathcal{C}) > n$.

В обозначениях определения считаем, что $d(\mathcal{C}) \geqslant 2t+1$.

В [9, 10] описаны условия существования пары $\mathcal{A}$ и $\mathcal{B}$, исправляющей t ошибок.

2. Основной результат

Несмотря на наличие ряда работ, посвящённых вопросу существования пар, исправляющих ошибки для линейных кодов, ни в одной из них не представлено нахождение такой пары для произвольного АГ-кода. Исключением является работа [5, Theorem 14], посвящённая криптоанализу криптосистемы Мак-Элиса, в которой рассмотрен общий вид пары, исправляющей ошибки для дуального кода. В следующих теоремах мы не только описываем вид кодов в паре, исправляющей ошибки для $\mathcal{C}_\mathcal{L}(D,G)$ и $\mathcal{C}_\mathcal{L}(D,G)^\perp$, но также задаём классификацию относительно рода функционального поля и степеней дивизоров, ассоциированных с кодами из пары. Отметим, что теорему 14 из [5] мы специализируем на случай принадлежности одного из кодов пары, исправляющей ошибки, к MDS-кодам.

Теорема 2 [11, Theorem 6]. Пусть $\mathcal{F}/\mathbb{F}_q$ — некоторое функциональное поле рода g; $D = P_1 + \ldots + P_n$ — дивизор, носитель которого состоит из точек степени один поля $\mathcal{F}$; G и H — дивизоры, такие, что $\mathrm{supp}(D) \cap (\mathrm{supp}(G) \cup \mathrm{supp}(H)) = \varnothing$. Тогда

$$\mathcal{C}_\mathcal{L}(D,G) * \mathcal{C}_\mathcal{L}(D,H) \subseteq \mathcal{C}_\mathcal{L}(D,G+H).$$

Если $\deg(G) \geqslant 2g$, $\deg(H) \geqslant 2g+1$, то выполняется равенство

$$\mathcal{C}_{\mathcal{L}}(D,G) * \mathcal{C}_{\mathcal{L}}(D,H) = \mathcal{C}_{\mathcal{L}}(D,G+H).$$

На основе теоремы 2 построим пару, исправляющую t ошибок для кода $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$.

Теорема 3. Пусть $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$ — АГ-код, ассоциированный с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g. Тогда если $\operatorname{supp}(G) \cap \operatorname{supp}(F) = \varnothing$, то парами, исправляющими $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$ ошибок для кода $\mathcal{C}$, являются следующие коды:

1) $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D,G+F)^{\perp}$, если $t+g \leqslant \deg(F) < n - \deg(G) - t$ и $2g-2 < \deg(G) < n-g-1$;
2) $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)^{\perp}$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D,F-G)$, если $\deg(G)+t+2g-2 < \deg(F) \leqslant n+g-t-2$ и $2g-2 < \deg(G) < n-g-1$.

Доказательство. Выведем вид пары $(\mathcal{A},\mathcal{B})$, исправляющей ошибки для кода $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$ и покажем, при каких параметрах и ограничениях на степени дивизоров будут выполняться все условия определения 3.

Обоснуем равносильность условий $\mathcal{A}*\mathcal{B} \subseteq \mathcal{C}^{\perp}$ и $\mathcal{B} \subseteq (\mathcal{A}*\mathcal{C})^{\perp}$. Действительно, пусть $a \in \mathcal{A}$, $b \in \mathcal{B}$ и $c \in \mathcal{C}$, тогда если имеет место включение $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^{\perp}$, то $\langle a*b, c\rangle = 0$, а по свойствам скалярного произведения $\langle a*b, c\rangle = \langle b, a*c\rangle$, откуда $\langle b, a*c\rangle = 0$, а значит, $\mathcal{B} \subseteq (\mathcal{A}*\mathcal{C})^{\perp}$. Обратное рассуждение, а именно: если выполняется условие $\mathcal{B} \subseteq (\mathcal{A}*\mathcal{C})^{\perp}$, то верно и $\mathcal{A}*\mathcal{B} \subseteq \mathcal{C}^{\perp}$, — аналогично.

1) Обозначим $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)$ для некоторого дивизора F. Далее оценим $\deg(F)$, но прежде построим код $\mathcal{B}$ так, чтобы выполнялось условие 1 определения 3.

Поскольку условие $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^{\perp}$ равносильно условию $\mathcal{B} \subseteq (\mathcal{A}*\mathcal{C})^{\perp}$, покажем, что код $\mathcal{B}$ имеет вид $\mathcal{C}_{\mathcal{L}}(D,G+F)^{\perp}$:

$$\mathcal{C}_{\mathcal{L}}(D,F) * \mathcal{C}_{\mathcal{L}}(D,G) \subseteq \mathcal{C}_{\mathcal{L}}(D,G+F) \;\Leftrightarrow\; \mathcal{B} = \mathcal{C}_{\mathcal{L}}(D,G+F)^{\perp} \subseteq (\mathcal{C}_{\mathcal{L}}(D,F) * \mathcal{C}_{\mathcal{L}}(D,G))^{\perp}.$$

Далее, исходя из трёх оставшихся условий определения 3, выведем границы для $\deg(F)$:

— Если степень дивизора F лежит в границах $t+g \leqslant \deg(F) < n$, то по теореме Римана — Роха

$$k(\mathcal{A}) \geqslant \deg(F) + 1 - g \geqslant t+g+1-g = t+1 > t.$$

Учитывая верхнюю границу $\deg(G+F) < n$ на степень дивизора $G+F$, получаем ограничение $\deg(G) < n-g-t$. Раскрывая t, получаем неравенство

$$\deg(G) < n - g - \lfloor (n - \deg(G) - g - 1)/2 \rfloor,$$

откуда, накладывая ограничение $t \geqslant 0$, получаем верхнюю границу

$$\deg(G) \leqslant n - g - 1$$

на степень дивизора G.

— Если $\deg(F) \leqslant n - \deg(G) - t - 1$, то

$$d(\mathcal{B}^{\perp}) \geqslant n - \deg(F+G) = n - \deg(G) - \deg(F) \geqslant n - \deg(G) - n + \deg(G) + t + 1 = t+1 > t.$$

— Если $\deg(F+G) < n$ (что справедливо, учитывая предыдущие ограничения), то выполняется условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant n - \deg(F) + n - \deg(G) = 2n - \deg(F+G) > n.$$

2. Обозначим $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)^{\perp}$ для некоторого дивизора F. Далее проверим выполнимость условия 1 определения 3.

По аналогии с предыдущим случаем покажем, что $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, F-G)$:

$$\mathcal{C}_{\mathcal{L}}(D,F)^{\perp} * \mathcal{C}_{\mathcal{L}}(D,G) = \mathcal{C}_{\mathcal{L}}(D, D-F+(\omega)) * \mathcal{C}_{\mathcal{L}}(D,G)) \subseteq \mathcal{C}_{\mathcal{L}}(D, D+G-F+(\omega)) =$$
$$= \mathcal{C}_{\mathcal{L}}(D, D-(D+G-F+(\omega))+(\omega))^{\perp} = \mathcal{C}_{\mathcal{L}}(D, F-G)^{\perp} \;\Rightarrow\; \mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, F-G) \subseteq (\mathcal{A} * \mathcal{C})^{\perp}.$$

Рассмотрим три оставшихся условия определения 3 с целью уточнения границ для степени дивизора F:

— Если $\deg(F) > 2g-2$, то по теореме Римана — Роха выполняется

$$k(\mathcal{A}) \geqslant n + g - 1 - \deg(F).$$

Следовательно, условие 2 выполняется при $\deg(F) \leqslant n+g-t-2$. Учитывая нижнюю границу $\deg(F-G) > 2g-2$ и то, что $t \geqslant 0$, как и в прошлом случае, получаем ограничение $\deg(G) \leqslant n-g-1$ на степень дивизора G.

— Если $\deg(F) \geqslant \deg(G) + t + 2g - 1$, то выполняется следующее:

$$d(\mathcal{B}^{\perp}) \geqslant \deg(F-G) - 2g + 2 \geqslant \deg(G) + t + 2g - 1 - \deg(G) - 2g + 2 = t + 1 > t.$$

— Если $\deg(F-G) > 2g-2$ (всегда верно, учитывая предыдущие ограничения), то выполняется условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant \deg(F) - 2g + 2 + n - \deg(G) = n + \deg(F-G) - 2g + 2 > n.$$

Теорема 3 доказана. ■

Следующая теорема даёт некоторую классификацию относительно параметров как кодов из пары, исправляющей ошибки, так и самого кода, для которого эта пара представлена.

Теорема 4. Пусть $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$ — АГ-код, ассоциированный с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g. Если пара кодов $(\mathcal{A},\mathcal{B})$ является парой, исправляющей

$$t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$$

ошибок для кода $\mathcal{C}$, то:

1. В случае $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, G+F)^{\perp}$:
   - 1.1) если $\mathcal{A} = [n, t+1, n-t]$, то g — произвольный, $2g-2 < \deg(G) < n-3g+3$ и $\deg(F) = t+g$;
   - 1.2) если $\mathcal{B} = [n, t, n-t+1]$, то $g=0$, $0 < \deg(G) < n$ и $\deg(F) = n - \deg(G) - t - 1$;
   - 1.3) если $\mathcal{C} = [n, n-2t, 2t+1]$, то $g=0$, $\deg(G) = n-2t-1$ и $\deg(F) = t$.
2. В случае $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)^{\perp}$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, F-G)$:
   - 2.1) если $\mathcal{A} = [n, t+1, n-t]$, то g — произвольный, $2g-2 < \deg(G) < n-3g+3$ и $\deg(F) = n+g-t-2$;

2.2) если $\mathcal{B} = [n, t, n-t+1]$, то $g = 0$, $0 < \deg(G) < n$ и $\deg(F) = \deg(G)+t-1$;
2.3) если $\mathcal{C} = [n, n-2t, 2t+1]$, то $g = 0$, $\deg(G) = n-2t-1$ и $\deg(F) = n-t-2$.

Доказательство.

1. Вид кодов $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, G+F)^{\perp}$ получен в теореме 3.

1.1. Очевидно, если код $\mathcal{A}$ имеет параметры $[n, t+1, n-t]$, то $\mathcal{A}$ является MDS-кодом. Таким образом, если $2g-2 < \deg(F) < n$, то

$$k(\mathcal{A}) = \deg(F) + 1 - g = t + 1,$$

откуда $\deg(F) = t+g$. Учитывая, что $\deg(F) > 2g-2$, получаем ограничение $\deg(G) < n - 3g + 3$ на степень дивизора G.

Теперь проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{A} = [n, t+1, n-t]$:

— Поскольку $\deg(F) = t + g$, имеем

$$k(\mathcal{A}) = \deg(F) + 1 - g = t + 1 > t.$$

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) = d(\mathcal{C}_{\mathcal{L}}(D, G+F)) \geqslant n - \deg(G+F) = n - \deg(G) - t - g.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant n - \deg(G) - t - g > t$. Данное неравенство имеет место при любых значениях $\deg(G)$, поскольку $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant n - \deg(F) + n - \deg(G) = 2n - t - g - \deg(G).$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}) > n$, если $t < n - g - \deg(G)$. Ввиду того, что $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$, неравенство $(n - \deg(G) - g - 1)/2 \leqslant n - g - \deg(G)$ выполняется всегда.

1.2. Если код $\mathcal{B}$ имеет параметры $[n, t, n-t+1]$, то он является MDS-кодом. Таким образом, если $2g-2 < \deg(G+F) < n$, то

$$k(\mathcal{B}) = n + g - 1 - \deg(G+F) = t,$$

откуда $\deg(F) = n + g - 1 - t - \deg(G)$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{B} = [n, t, n-t+1]$:

— Поскольку $\deg(F) = n + g - 1 - t - \deg(G)$, имеем

$$k(\mathcal{A}) = \deg(F) + 1 - g = n - t - \deg(G) > t,$$

следовательно, $t < (n - \deg(G))/2$, что выполняется при любых значениях $\deg(G)$ при $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) \geqslant n - \deg(G+F) = n - \deg(G) - \deg(F) = t + 1 - g.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant t + 1 - g > t$, что возможно лишь при $g = 0$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant n - \deg(F) + n - \deg(G) = n + t + 1.$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}) > n$, если $t > -1$. Поскольку $t = \lfloor (n - \deg(G) - 1)/2 \rfloor$, неравенство $(n - \deg(G) - 1)/2 > -1$ выполняется при $\deg(G) < n + 1$, что всегда верно в силу первоначального выбора дивизора G.

1.3. Если код $\mathcal{C}$ имеет параметры $[n, n-2t, 2t+1]$, то он является MDS-кодом. Тогда если $2g - 2 < \deg(G) < n$, то

$$k(\mathcal{C}) = \deg(G) + 1 - g = n - 2t,$$

откуда $\deg(G) = n + g - 2t - 1$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{C} = [n, n - 2t, 2t + 1]$:

— Условие $k(\mathcal{A}) = \deg(F) + 1 - g > t$ имеет место, если $\deg(F) > t + g - 1$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) \geqslant n - \deg(G + F) = -g + 2t + 1 - \deg(F).$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant -g + 2t + 1 - \deg(F) > t$, т. е. $\deg(F) < t + 1 - g$. Окончательно имеем

$$t + g - 1 < \deg(F) < t + 1 - g,$$

что возможно лишь при $g = 0$ и, как следствие, $\deg(F) = t$.

— Проверим условие 4 определения 3 при $g = 0$:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant n - \deg(F) + n - \deg(G) = n + t + 1.$$

Очевидно, $d(\mathcal{A}) + d(\mathcal{C}) > n$.

2. Вид кодов $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)^{\perp}$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, F - G)$ получен в теореме 3.

2.1. Если код $\mathcal{A}$ имеет параметры $[n, t+1, n-t]$, то он является MDS-кодом. Таким образом, если $2g - 2 < \deg(F) < n$, то

$$k(\mathcal{A}) = n + g - 1 - \deg(F) = t + 1,$$

откуда $\deg(F) = n + g - t - 2$. Учитывая, что $\deg(F) > 2g - 2$, получаем ограничение $\deg(G) < n - 3g + 3$ на степень дивизора G.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{A} = [n, t + 1, n - t]$:

— Поскольку $\deg(F) = n + g - t - 2$, имеем

$$k(\mathcal{A}) = n + g - 1 - \deg(F) = t + 1 > t.$$

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) = d(\mathcal{C}_{\mathcal{L}}(D, F - G)) \geqslant \deg(F - G) - 2g + 2 = n - g - t - \deg(G).$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant n - g - t - \deg(G) > t$. Данное неравенство имеет место при любых значениях $\deg(G)$ при условии, что $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant \deg(F) - 2g + 2 + n - \deg(G) = 2n - t - g - \deg(G).$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}) > n$, если $t < n - g - \deg(G)$. Ввиду того, что $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$, неравенство $(n - \deg(G) - g - 1)/2 \leqslant n - g - \deg(G)$ выполняется всегда.

2.2. Если код $\mathcal{B}$ имеет параметры $[n, t, n-t+1]$, то он является MDS-кодом. Таким образом, если $2g - 2 < \deg(F - G) < n$, то

$$k(\mathcal{B}) = \deg(F - G) + 1 - g = \deg(F) - \deg(G) + 1 - g = t,$$

откуда $\deg(F) = \deg(G) + t + g - 1$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{B} = [n, t, n - t + 1]$:

— Поскольку $\deg(F) = \deg(G) + t + g - 1$, имеем

$$k(\mathcal{A}) = n + g - 1 - \deg(F) = n - t - \deg(G) > t,$$

следовательно, $t < (n - \deg(G))/2$, что справедливо при любых значениях $\deg(G)$ с учётом того, что $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) \geqslant \deg(F - G) - 2g + 2 = \deg(F) - \deg(G) - 2g + 2 = t + 1 - g.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant t + 1 - g > t$, что возможно лишь при $g = 0$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant \deg(F) + 2 + n - \deg(G) = n + t + 1.$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}) > n$, если $t > -1$. Поскольку $t = \lfloor (n - \deg(G) - 1)/2 \rfloor$, неравенство $(n - \deg(G) - 1)/2 > -1$ выполняется при $\deg(G) < n + 1$, что всегда верно в силу первоначального выбора дивизора G.

2.3. Если код $\mathcal{C}$ имеет параметры $[n, n-2t, 2t+1]$, то он является MDS-кодом. Тогда, если $2g - 2 < \deg(G) < n$, то

$$k(\mathcal{C}) = \deg(G) + 1 - g = n - 2t,$$

откуда $\deg(G) = n + g - 2t - 1$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{C} = [n, n - 2t, 2t + 1]$:

— Условие $k(\mathcal{A}) = n + g - 1 - \deg(F) > t$ имеет место, если $\deg(F) < n + g - t - 1$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу и $\deg(G) = n + g - 2t - 1$:

$$d(\mathcal{B}^{\perp}) \geqslant \deg(F - G) - 2g + 2 = \deg(F) - \deg(G) - 2g + 2 = \deg(F) - n - 3g + 2t + 3.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant \deg(F) - n - 3g + 2t + 3 > t$, т. е. $\deg(F) > n + 3g - t - 3$. Окончательно имеем

$$n + 3g - t - 3 < \deg(F) < n + g - t - 1,$$

что возможно лишь при $g = 0$ и, как следствие, $\deg(F) = n - t - 2$.

— Проверим условие 4 определения 3 при $g = 0$:

$$d(\mathcal{A}) + d(\mathcal{C}) \geqslant \deg(F) + 2 + n - \deg(G) = \deg(F) + 2t + 3.$$

Соответственно $d(\mathcal{A})+d(\mathcal{C}) > n$, если $\deg(F) > n-2t-3$, что справедливо, поскольку $\deg(F) = n - t - 2$.

Теорема 4 доказана. ■

Построим пару, исправляющую t ошибок для кода $\mathcal{C}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, G)^{\perp}$.

Теорема 5. Пусть $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ — АГ-код, ассоциированный с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g, и $\mathcal{C}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, G)^{\perp}$ — код, дуальный к $\mathcal{C}$. Если пара кодов $(\mathcal{A}, \mathcal{B})$ является парой, исправляющей $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$ ошибок для кода $\mathcal{C}^{\perp}$, то в случае $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ и $\mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, G - F)$:

1) если $\mathcal{A} = [n, t+1, n-t]$, то g — произвольный, $5g-5 < \deg(G) < n$ и $\deg(F) = t+g$;
2) если $\mathcal{B} = [n, t, n - t + 1]$, то $g = 0$, $0 < \deg(G) < n$ и $\deg(F) = \deg(G) - t + 1$;
3) если $\mathcal{C} = [n, t - 2t, 2t + 1]$, то $g = 0$, $\deg(G) = 2t - 1$ и $\deg(F) = t$.

Доказательство. Обозначим $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ для некоторого дивизора F. Далее мы оценим $\deg(F)$, но прежде построим код $\mathcal{B}$ так, чтобы выполнялось условие 1 определения 3.

Поскольку $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}$, то $\mathcal{B} \subseteq (\mathcal{A} * \mathcal{C}^{\perp})^{\perp}$. Положим $\mathcal{B} = (\mathcal{A} * \mathcal{C}^{\perp})^{\perp}$. В обозначениях АГ-кодов получаем

$$\mathcal{C}_{\mathcal{L}}(D, F) * \mathcal{C}_{\mathcal{L}}(D, G^{\perp}) \subseteq \mathcal{C}_{\mathcal{L}}(D, D-G+F+(\omega)) = \mathcal{C}_{\mathcal{L}}(D, G-F)^{\perp} \Rightarrow \mathcal{B} = \mathcal{C}_{\mathcal{L}}(D, G-F) \subseteq (\mathcal{A} * \mathcal{C}^{\perp})^{\perp}.$$

1. Если код $\mathcal{A}$ имеет параметры $[n, t + 1, n - t]$, то он является MDS-кодом. Таким образом, если $2g - 2 < \deg(F) < n$, то

$$k(\mathcal{A}) = \deg(F) + 1 - g = t + 1,$$

откуда $\deg(F) = t+g$. Учитывая, что $\deg(F) > 2g-2$, получаем ограничение $\deg(G) > > 5g - 5$ на степень дивизора G.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{A} = [n, t + 1, n - t]$:

— Поскольку $\deg(F) = t + g$, имеем

$$k(\mathcal{A}) = \deg(F) + 1 - g = t + 1 > t.$$

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) = d(\mathcal{C}_{\mathcal{L}}(D, G - F)^{\perp}) \geqslant \deg(G - F) - 2g - 2 = \deg(G) - t - 3g + 2.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant \deg(G) - t - 3g + 2 > t$. Данное неравенство имеет место при любых значениях $\deg(G)$ с учётом того, что $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}^{\perp}) \geqslant n - \deg(F) + \deg(G) - 2g + 2 = n + \deg(G) + 2 - t - 3g.$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}^{\perp}) > n$, если $t < \deg(G) + 2 - 3g$. Ввиду того, что $t = = \lfloor(\deg(G)+1-3g)/2\rfloor$, неравенство $(\deg(G)+1-3g)/2 \leqslant \deg(G)+2-3g$ выполняется всегда.

2. Если код $\mathcal{B}$ имеет параметры $[n, t, n-t+1]$, то он является MDS-кодом. Таким образом, если $2g-2 < \deg(G-F) < n$, то

$$k(\mathcal{B}) = \deg(G-F) + 1 - g = \deg(G) - \deg(F) + 1 - g = t,$$

откуда $\deg(F) = \deg(G) + 1 - g - t$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{B} = [n, t, n-t+1]$:

— Поскольку $\deg(F) = \deg(G) + 1 - g - t$, имеем

$$k(\mathcal{A}) = \deg(F) + 1 - g = \deg(G) + 2 - t - 2g > t,$$

следовательно, $t < (\deg(G)+2-2g)/2$. Данное неравенство выполняется при любых значениях $\deg(G)$, поскольку $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу и $\deg(F) = \deg(G) + 1 - g - t$:

$$d(\mathcal{B}^{\perp}) \geqslant \deg(G-F) - 2g + 2 = \deg(G) - \deg(F) - 2g + 2 = t + 1 - g.$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant t + 1 - g > t$, что возможно лишь при $g = 0$.

— Применяя аналогичные рассуждения, проверяем условие 4 определения 3:

$$d(\mathcal{A}) + d(\mathcal{C}^{\perp}) \geqslant n - \deg(F) + \deg(G) - 2g + 2 = n + t + 1.$$

Очевидно, что $d(\mathcal{A}) + d(\mathcal{C}^{\perp}) > n$.

3. Если код $\mathcal{C}$ имеет параметры $[n, n-2t, 2t+1]$, то он является MDS-кодом. Тогда если $2g-2 < \deg(G) < n$, то $k(\mathcal{C}) = n+g-1-\deg(G) = n-2t$, откуда $\deg(G) = 2t+g-1$.

Проверим, при каких ограничениях выполняются три оставшихся условия определения 3, если $\mathcal{C} = [n, n-2t, 2t+1]$:

— Условие $k(\mathcal{A}) = \deg(F) + 1 - g > t$ имеет место, если $\deg(F) > t + g - 1$.

— Оценим минимальное расстояние кода $\mathcal{B}^{\perp}$, учитывая его нижнюю границу:

$$d(\mathcal{B}^{\perp}) \geqslant \deg(G-F) - 2g + 2 = \deg(G) - \deg(F) - 2g + 2 = 2t - g + 1 - \deg(F).$$

По условию определения необходимо, чтобы $d(\mathcal{B}^{\perp}) \geqslant 2t - g + 1 - \deg(F) > t$, т. е. $\deg(F) < t + 1 - g$. Окончательно имеем

$$t + g - 1 < \deg(F) < t - g + 1,$$

что возможно лишь при $g = 0$ и, как следствие, $\deg(F) = t$.

— Проверим условие 4 определения 3 при $g = 0$:

$$d(\mathcal{A}) + d(\mathcal{C}^{\perp}) \geqslant n - \deg(F) + \deg(G) - 2g + 2 = n - \deg(F) + 2t + 1.$$

Соответственно $d(\mathcal{A}) + d(\mathcal{C}^{\perp}) > n$, если $\deg(F) < 2t+1$, что справедливо, поскольку $\deg(F) = t$.

Теорема 5 доказана. ■

Интересным объектом исследования относительно кодовых криптосистем являются подполевые подкоды, поскольку существует гипотеза, что именно такие коды являются стойкими к атаке на основе пар, исправляющих ошибки (по аналогии с классическими кодами Гоппы, являющимися некоторой модификацией подполевых подкодов обобщённых кодов Рида— Соломона). Дадим определение подполевого подкода.

Определение 4. Пусть код $\mathcal{C}$ определён над полем $\mathbb{F}_q$ ($\mathcal{C} \subseteq \mathbb{F}_q^n$) и $\mathbb{F}_p \subseteq \mathbb{F}_q$. *Подполевым подкодом* линейного кода $\mathcal{C}$ называется код $\mathcal{C}|\mathbb{F}_p = \mathcal{C} \cap \mathbb{F}_p^n$.

В действительности если $\mathcal{C}|\mathbb{F}_p$ — подполевой подкод кода $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$, определённого над $\mathbb{F}_q$, и $\mathbb{F}_p \subseteq \mathbb{F}_q$, то, согласно [9], пара, исправляющая t ошибок для кода $\mathcal{C}$, является парой, исправляющей такое же количество ошибок и для подполевого подкода $\mathcal{C}|\mathbb{F}_p$. При этом алгоритм декодирования работает над расширением $\mathbb{F}_q$ конечного поля $\mathbb{F}_p$ за время $\mathcal{O}((mn)^3)$, где $q = p^m$. Соответственно вопрос редукции сложности задачи декодирования подполевых подкодов сводится к нахождению пары, исправляющей ошибки для подполевого подкода над $\mathbb{F}_p$.

Теорема 6. Пусть $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$ — АГ-код, ассоциированный с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g, где $q = p^2$. Тогда если $\operatorname{supp}(G) \cap \operatorname{supp}(F) = \varnothing$, то парой, исправляющей $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$ ошибок для кода $\mathcal{C}|\mathbb{F}_p$, является пара кодов $(\tilde{\mathcal{A}}, \tilde{\mathcal{B}})$ при условии их существования:

1) $\tilde{\mathcal{A}} = (\mathcal{C}_{\mathcal{L}}(D, F)^{\perp})|_{\mathbb{F}_p}$, если

$$g = 0 \quad \text{и} \quad \left[\begin{array}{l} n = 6,\ \deg(G) = 1,\ \deg(F) = 1 \\ \text{или} \\ n = 5,\ \deg(G) \leqslant 2,\ \deg(F) = 1 \end{array}\right.$$

или

$$g = 1,\ n = 5,\ \deg(G) = 1,\ \deg(F) = 2.$$

2) $\tilde{\mathcal{A}} = (\mathcal{C}_{\mathcal{L}}(D, F)|_{\mathbb{F}_p})^{\perp}$, если

$$g = 0, \quad n = 4, \quad \deg(G) = 1, \quad \deg(F) \leqslant 2;$$

или

$$\begin{array}{l} 0 \leqslant g \leqslant 1, \\ n \text{ — чётное} \end{array} \quad \text{и} \quad \left[\begin{array}{l} n \geqslant 6,\ 2g-2 < \deg(G) < n-g-3,\ \deg(F) \leqslant (n - \deg(G) + g + 1)/2 \\ \text{или} \\ n \geqslant 10, \quad \deg(G) = n - g - 3, \quad \deg(F) \leqslant n - \deg(G) - 1; \end{array}\right.$$

или

$g = 2$, $n \geqslant 10$, n — чётное и $2 < \deg(G) < n - 5$, $\deg(F) \leqslant (n - \deg(G) + 3)/2$;

или

$$g \geqslant 3, \quad n > 5g - 4, \quad n \text{ — чётное}, \quad 2g - 2 < \deg(G) < n - 3g + 3,$$
$$\deg(F) \leqslant (n - \deg(G) + g + 1)/2;$$

или

$$g \leqslant (n-1)/3, \quad n = 4, 6, 8, \quad \deg(G) = n - g - 3, \quad \deg(F) \leqslant n - \deg(G) - 1,$$

и в каждом случае $\deg(F) > 2g - 2$.

3) $\tilde{\mathcal{A}} = \mathcal{C}_{\mathcal{L}}(D, F)|_{\mathbb{F}_p}$, если

$$g = 0, \quad n = 3, \quad \deg(G) = 1, \quad \deg(F) = 1.$$

4) $\tilde{\mathcal{A}} = ((\mathcal{C}_{\mathcal{L}}(D, F)^{\perp})|_{\mathbb{F}_p})^{\perp}$, если

$$g = 0 \quad \text{и} \quad \left[\begin{array}{l} n = 4, \quad \deg(G) = 1, \quad \deg(F) \geqslant \deg(G) \\ \text{или} \\ n = 6, 8, 10, \quad \deg(G) \leqslant n - 5, \quad \deg(F) \geqslant (n + \deg(G) - 5)/2; \end{array}\right.$$

или

$$1 \leqslant g \leqslant 2 \quad \text{и} \quad \left[\begin{array}{l} n \geqslant 3g+1,\ \deg(G) = n-g-3,\ \deg(F) \geqslant \deg(G)+2g-1 \\ \text{или} \\ n \geqslant 4g+2,\ 2g-1 \leqslant \deg(G) \leqslant n-g-4 \quad \text{и} \\ \quad \deg(F) \geqslant (n+\deg(G)+3g-5)/2; \end{array}\right.$$
n — чётное

или

$$g=3, \quad n \geqslant 12 \text{ и } n \text{ — чётное}, \quad 4 < \deg(G) \leqslant n-6, \quad \deg(F) \geqslant (n+\deg(G)+4)/2;$$

или

$$g \geqslant 5,\ n \geqslant 5g-5 \text{ и } n \text{ — чётное},\ 2g-2 < \deg(G) \leqslant n-3g+3,$$
$$\deg(F) \geqslant (n+\deg(G)+3g-5)/2,$$

и в каждом случае $\deg(F) < n$.

Во всех четырёх случаях $\tilde{\mathcal{B}} = (\tilde{\mathcal{A}} * \mathcal{C}|_{\mathbb{F}_p})^{\perp}$.

Доказательство. Обозначим $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D,F)$ и отметим, что изначально код $\mathcal{C}$ определён над квадратичным расширением поля $\mathbb{F}_p$, т. е. $\mathbb{F}_q = \mathbb{F}_{p^2}$.

1. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = \mathcal{A}^{\perp}|_{\mathbb{F}_p}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = k(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) \geqslant 2k(\mathcal{A}^{\perp}) - n = n + 2g - 2 - 2\deg(F)$.
Так как $t = (n - \deg(G) - g - 1)/2$, условие $k(\tilde{\mathcal{A}}) > t$ имеет место, если $\deg(F) \leqslant$ $\leqslant (\deg(G) + n + 5g - 3)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d(\mathcal{A}^{\perp}|_{\mathbb{F}_p} * \mathcal{C}|_{\mathbb{F}_p}) \geqslant d((\mathcal{A}^{\perp} * \mathcal{C})|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp} * \mathcal{C})$.
Поскольку $\mathcal{A}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, D - F + (\omega))$ и $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D,G)$, то

$$\mathcal{A}^{\perp} * \mathcal{C} \subseteq \mathcal{C}_{\mathcal{L}}(D, D + G - F + (\omega)) = \mathcal{C}_{\mathcal{L}}(D, F-G)^{\perp},$$

тогда

$$d(\mathcal{A}^{\perp} * \mathcal{C}) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, F-G)^{\perp})) \geqslant \deg(F-G) - 2g + 2 = \deg(F) - \deg(G) - 2g + 2.$$

Так как $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \geqslant$ $\geqslant (\deg(G) + n + 3g - 5)/2$.

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) + d(\mathcal{C}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp}) + d(\mathcal{C}) \geqslant \deg(F) - 2g + 2 + n - \deg(G)$.
Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) > n$, если $\deg(F) \geqslant \deg(G) + 2g - 1$.

Таким образом, $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$ — пара, исправляющая ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$, если имеет место следующая система:

$$\begin{cases} \deg(F) \leqslant (\deg(G) + n + 5g - 3)/4, \\ \deg(F) \geqslant (\deg(G) + n + 3g - 5)/2, \\ \deg(F) \geqslant \deg(G) + 2g - 1. \end{cases}$$

Здесь следует рассмотреть два случая:

— Условие $(\deg(G)+n+3g-5)/2 \leqslant \deg(F) \leqslant (\deg(G)+n+5g-3)/4$ выполняется, если $\deg(G) \leqslant n-g-3$ и $\deg(G) \leqslant -n-g+7$. Соответственно получаем следующие значения для рода g, длины n и степени $\deg(G)$:

$$\begin{array}{lll} g=0 & \text{и} & \begin{array}{lll} n=6, & \deg(G)=1, & \text{откуда } \deg(F)=1, \\ n=5, & \deg(G)\leqslant 2, & \text{откуда } \deg(F)=1; \end{array} \\ g=1 & \text{и} & n=5, \quad \deg(G)=1, \quad \text{откуда } \deg(F)=2. \end{array}$$

— Условие $\deg(G)+2g-1 \leqslant \deg(F) \leqslant (\deg(G)+n+5g-3)/4$ выполняется, если $n-g-3 \leqslant deg(G) \leqslant (n-3g+1)/3$. Соответственно получаем следующие значения для рода g, длины n и степени $\deg(G)$:

$$\begin{array}{llllll} g=0 & \text{и} & n=5, & \deg(G)=2, & \text{откуда} & \deg(F)=1; \\ g=1 & \text{и} & n=5, & \deg(G)=1, & \text{откуда} & \deg(F)=2. \end{array}$$

2. Проверим, может ли пара кодов $\tilde{\mathcal{A}} = (\mathcal{A}|_{\mathbb{F}_p})^{\perp}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}|_{\mathbb{F}_p})^{\perp}$ являться парой, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = k((\mathcal{A}|_{\mathbb{F}_p})^{\perp}) = n - k(\mathcal{A}|_{\mathbb{F}_p})$.
Так как $t = \lfloor (n-\deg(G)-g-1)/2 \rfloor$, условие $k(\tilde{\mathcal{A}}) > t$ имеет место, если $\deg(F) \leqslant$ $\leqslant (\deg(G)+3n+5g-3)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d((\mathcal{A}|_{\mathbb{F}_p})^{\perp} * \mathcal{C}|_{\mathbb{F}_p})$.
Рассмотрим случай, когда код $\tilde{\mathcal{A}}$ является самодуальным, т. е. $(\mathcal{A}|_{\mathbb{F}_p})^{\perp} = \mathcal{A}|_{\mathbb{F}_p}$. Следовательно, $k(\mathcal{A}|_{\mathbb{F}_p}) = n/2$, что возможно при $\deg(F) \leqslant (3n+4g-4)/4$. Тогда получаем

$$d(\tilde{\mathcal{B}}^{\perp}) = d(\mathcal{A}|_{\mathbb{F}_p} * \mathcal{C}|_{\mathbb{F}_p}) \geqslant d((\mathcal{A}*\mathcal{C})|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}*\mathcal{C}) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, F+G)) \geqslant n-\deg(F)-\deg(G).$$

Поскольку $t = \lfloor (n-\deg(G)-g-1).2 \rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \leqslant$ $\leqslant (n+g+1-\deg(G)).2$.
Имеем два случая для определения $\deg(F)$:

— Случай $\deg(F) \leqslant (3n+4g-4)/4$ имеет место при $\deg(G) \leqslant (6-n-2g)/2$, что возможно, если

$$g=0, \quad n=2,4, \quad \deg(G) \leqslant 2$$

или

$$g=1, \quad n=2, \quad \deg(G)=1.$$

— Случай $\deg(F) \leqslant (n+g+1-\deg(G))/2$ имеет место при $\deg(G) > (6-n-2g)/2$.

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d((\mathcal{A}|_{\mathbb{F}_p})^{\perp}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d(\mathcal{A}|_{\mathbb{F}_p}) + d(\mathcal{C}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}) + d(\mathcal{C}) \geqslant 2n - \deg(F) -$ $- \deg(G)$. Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) > n$, если $\deg(F) < n - \deg(G)$.

Таким образом, построение пары $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$, возможно, если справедлива одна из систем:

$$\begin{cases} \deg(F) \leqslant (\deg(G)+3n+5g-3)/4, \\ \deg(F) \leqslant (3n+4g-4)/4, \\ \deg(G) \leqslant (6-n-2g)/2, \\ \deg(F) \leqslant n-\deg(G)-1 \end{cases} \quad \text{или} \quad \begin{cases} \deg(F) \leqslant (\deg(G)+3n+5g-3)/4, \\ \deg(F) \leqslant (n+g+1-\deg(G))/2, \\ \deg(G) > (6-n-2g)/2, \\ \deg(F) \leqslant n-\deg(G)-1. \end{cases}$$

Уточняя обе системы, окончательно получаем следующие результаты:

$$g=0,\quad n=4,\quad \deg(G)=1,\quad \deg(F)\leqslant 2,$$
$$0\leqslant g\leqslant 2,\ n\geqslant 9,\ 2g{-}2<\deg(G)<n{-}g{-}3,\ 2g{-}2<\deg(F)\leqslant (n{-}\deg(G){+}g{+}1)/2,$$
$$g\geqslant 3,\ n>5g{-}4,\ 2g{-}2<\deg(G)<n{-}3g{+}3,\ 2g{-}2<\deg(F)\leqslant (n{-}\deg(G){+}g{+}1)/2,$$
$$0\leqslant g\leqslant 1,\quad n\geqslant 9,\quad \deg(G)=n-g-3,\quad 2g-2<\deg(F)\leqslant n-\deg(G)-1,$$
$$g=0,1,\ n=6,8,\ 2g{-}2<\deg(G)<n{-}g{-}3,\ 2g{-}2<\deg(F)\leqslant (n{-}\deg(G){+}g{+}1)/2,$$
$$g\leqslant (n-1)/3,\quad n=4,6,8,\quad \deg(G)=n-g-3,\quad 2g-2<\deg(F)\leqslant n-\deg(G)-1.$$

Во всех случаях n — чётное.

3. Проверим, является ли пара кодов $\tilde{\mathcal{A}}=\mathcal{A}|_{\mathbb{F}_p}$ и $\tilde{\mathcal{B}}=(\tilde{A}*\mathcal{C}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}}*\tilde{\mathcal{B}}\subseteq(\mathcal{C}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}})=k(\mathcal{A}|_{\mathbb{F}_p})\geqslant 2k(\mathcal{A})-n=2\deg(F)+2-2g-n$.
Так как $t=\lfloor(n-\deg(G)-g-1)/2\rfloor$, условие $k(\tilde{\mathcal{A}})>t$ имеет место, если $\deg(F)\geqslant$ $\geqslant(3n+3g-\deg(G)-5)/4$.

— $d(\tilde{\mathcal{B}}^{\perp})=d(\mathcal{A}|_{\mathbb{F}_p}*\mathcal{C}|_{\mathbb{F}_p})\geqslant d((\mathcal{A}*\mathcal{C})|_{\mathbb{F}_p})\geqslant d(\mathcal{A}*\mathcal{C})$.
Поскольку $\mathcal{A}=\mathcal{C}_{\mathcal{L}}(D,F)$ и $\mathcal{C}=\mathcal{C}_{\mathcal{L}}(D,G)$, то $\mathcal{A}*\mathcal{C}\subseteq\mathcal{C}_{\mathcal{L}}(D,G+F)$ и

$$d(\tilde{\mathcal{B}}^{\perp})\geqslant d(\mathcal{C}_{\mathcal{L}}(D,F+G)))\geqslant n-\deg(F+G)=n-\deg(F)-\deg(G).$$

Так как $t=\lfloor(n-\deg(G)-g-1)/2\rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp})>t$ выполняется при $\deg(F)\leqslant$ $\leqslant(n+g+1-\deg(G))/2$.

— $d(\tilde{\mathcal{A}})+d(\mathcal{C}|_{\mathbb{F}_p})=d(\mathcal{A}|_{\mathbb{F}_p})+d(\mathcal{C}|_{\mathbb{F}_p})\geqslant d(\mathcal{A})+d(\mathcal{C})\geqslant 2n-\deg(F)-\deg(G)$.
Очевидно, что $d(\tilde{\mathcal{A}})+d(\mathcal{C}|_{\mathbb{F}_p})>n$, если $\deg(F)\leqslant n-\deg(G)-1$.

Таким образом, $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$ — пара, исправляющая ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$, если справедлива следующая система:

$$\begin{cases}\deg(F)\geqslant(3n+3g-\deg(G)-5)/4,\\ \deg(F)\leqslant(n+g+1-\deg(G))/2,\\ \deg(F)\leqslant n-\deg(G)-1.\end{cases}$$

Здесь следует рассмотреть два случая:

— Условие $(3n+3g-\deg(G)-5)/4\leqslant\deg(F)\leqslant n-\deg(G)-1$ выполняется, если $\deg(G)\geqslant n-g-2$ и $\deg(G)\leqslant(n+1-3g)/3$. Соответственно получаем следующие значения рода g, длины n, степени $\deg(G)$, а также степени $\deg(F)$:

$$g=0,\quad n=3,\quad \deg(G)=1,\quad \deg(F)=1.$$

— Условие $(3n+3g-\deg(G)-5)/4\leqslant\deg(F)\leqslant(n+g+1-\deg(G))/2$ не выполняется никогда, поскольку в результате накладывания ограничений на степени дивизоров получаем следующие несовместные системы:

$$\begin{cases}\deg(F)\geqslant(3n+3g-\deg(G)-5)/4,\\ \deg(F)\leqslant(n+g+1-\deg(G))/2,\\ n\leqslant 3;\quad 0<\deg(G)\leqslant n-g-3\end{cases}\qquad\text{или}\qquad\begin{cases}\deg(F)\geqslant(3n+3g-\deg(G)-5)/4,\\ \deg(F)\leqslant(n+g+1-\deg(G))/2,\\ n\geqslant 4;\quad 0<\deg(G)\leqslant 4-n-g.\end{cases}$$

4. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = (\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = k((\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp}) = n - k(\mathcal{A}^{\perp}|_{\mathbb{F}_p})$.
Для выполнения условия 2 определения 3 необходимо, чтобы $k(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) < n - t$. С другой стороны, $k(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) \geqslant 2k(\mathcal{A}^{\perp}) - n = n + 2g - 2\deg(F) - 2$. Принимая во внимание, что $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$, и уточняя, при каком ограничении на $\deg(F)$ выполняются неравенства

$$n + 2g - 2\deg(F) - 2 \leqslant k(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) < n - t,$$

получаем $\deg(F) \geqslant (n + 3g - \deg(G) - 5)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d((\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp} * \mathcal{C}|_{\mathbb{F}_p})$.
Здесь снова будем рассматривать случай, когда код $\tilde{\mathcal{A}}$ является самодуальным, т. е. $(\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp} = \mathcal{A}^{\perp}|_{\mathbb{F}_p}$. Следовательно, $k(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) = n/2$, что возможно при $\deg(F) \geqslant (n+4g-4)/4$. Тогда $d(\tilde{\mathcal{B}}^{\perp}) = d(\mathcal{A}^{\perp}|_{\mathbb{F}_p} * \mathcal{C}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp} * \mathcal{C})$. Поскольку $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ и $\mathcal{C} = \mathcal{C}_{\mathcal{L}}(D, G)$, то

$$d(\tilde{\mathcal{B}}^{\perp}) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, D-F+(\omega)) * \mathcal{C}_{\mathcal{L}}(D, G)) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, F-G)^{\perp}) \geqslant \deg(F) - \deg(G) - 2g + 2.$$

Так как $t = \lfloor (n - \deg(G) - g - 1)/2 \rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \geqslant (n + \deg(G) + 3g - 5)/2$.
Следует рассмотреть два случая, чтобы определить $\deg(F)$:
— Случай $\deg(F) \geqslant (n + \deg(G) + 3g - 5)/2$ имеет место при $\deg(G) > (6 - n - 2g)/2$.
— Случай $\deg(F) \geqslant (n + 4g - 4)/4$ имеет место при $\deg(G) \leqslant (6 - n - 2g)/2$, что возможно, если

$$g = 0, \quad n = 2, 4, \quad \deg(G) \leqslant 2$$

или

$$g = 1, \quad n = 2, \quad \deg(G) = 1.$$

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d((\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) + d(\mathcal{C}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp}) + d(\mathcal{C}) \geqslant \deg(F) - 2g + 2 + n - \deg(G)$. Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) > n$, если $\deg(F) > \deg(G) + 2g - 2$.

Таким образом, построение пары $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, исправляющей ошибки для кода $\mathcal{C}|_{\mathbb{F}_p}$, возможно, если справедлива одна из систем:

$$\begin{cases} \deg(F) \geqslant (n + 3g - \deg(G) - 5)/4, \\ \deg(F) \geqslant (n + \deg(G) + 3g - 5)/2, \\ \deg(G) > (6 - n - 2g)/2, \\ \deg(F) > \deg(G) + 2g - 2 \end{cases} \quad \text{или} \quad \begin{cases} \deg(F) \geqslant (n + 3g - \deg(G) - 5)/4, \\ \deg(F) \geqslant (n + 4g - 4)/2, \\ \deg(G) \leqslant (6 - n - 2g)/2, \\ \deg(F) > \deg(G) + 2g - 2. \end{cases}$$

Уточняя обе системы, окончательно получаем следующие результаты:

$$g = 0, \quad n = 4, \quad \deg(G) = 1, \quad \deg(G) \leqslant \deg(F) \leqslant n - 1,$$
$$g = 0,\ n = 6, 8, 10,\ (6 - n)/2 < \deg(G) \leqslant n - 5,\ (n + \deg(G) - 5)/2 \leqslant \deg(F) \leqslant n - 1,$$
$$g = 0,\ n \geqslant 5 \text{ и } n \text{ — чётное},\ n - 2 \leqslant \deg(G) \leqslant n - 1,\ \deg(G) - 1 \leqslant \deg(F) \leqslant n - 1,$$
$$g = 1,\ n \geqslant 4 \text{ и } n \text{ — чётное},\ n - 4 \leqslant \deg(G) \leqslant n - 2,\ \deg(G) + 1 \leqslant \deg(F) \leqslant n - 1,$$
$$g = 1,\ n \geqslant 6 \text{ и } n \text{ — чётное},\ 1 \leqslant \deg(G) \leqslant n - 5,\ (n + \deg(G) - 2)/2 \leqslant \deg(F) \leqslant n - 1,$$

$$g=2,\ n\geqslant 8 \text{ и } n \text{ — чётное},\ n-5\leqslant \deg(G)\leqslant n-4,\ \deg(G)+3\leqslant \deg(F)\leqslant n-1,$$
$$g=2,\ n\geqslant 9 \text{ и } n \text{ — чётное},\ 3\leqslant \deg(G)\leqslant n-6,\ (n+\deg(G)+1)/2\leqslant \deg(F)\leqslant n-1,$$
$$g=3,\ n\geqslant 12 \text{ и } n \text{ — чётное},\ 4<\deg(G)\leqslant n-6,\ \deg(F)\geqslant (n+\deg(G)+4)/2,$$
$$g\geqslant 5, n\geqslant 5g-5 \text{ и } n \text{ — чётное}, 2g-2<\deg(G)\leqslant n-3g+3, \deg(F)\geqslant (n+\deg(G)+3g-5)/2.$$

Теорема 6 доказана. ■

Теорема 7. Пусть $\mathcal{C}=\mathcal{C}_{\mathcal{L}}(D,G)$ — АГ-код, ассоциированный с функциональным полем $\mathcal{F}/\mathbb{F}_q$ рода g, где $q=p^2$, и $\mathcal{C}^{\perp}$ — дуальный к $\mathcal{C}$. Тогда если $\operatorname{supp}(G)\cap\operatorname{supp}(F)=\varnothing$, то парой, исправляющей $t=\lfloor(\deg(G)-3g+1)/2\rfloor$ ошибок для кода $(\mathcal{C}^{\perp})|_{\mathbb{F}_p}$, является пара кодов $(\tilde{\mathcal{A}},\tilde{\mathcal{B}})$ при условии их существования:

1) $\tilde{\mathcal{A}}=\mathcal{C}_{\mathcal{L}}(D,F)|_{\mathbb{F}_p}$, если

$$g=0 \quad \text{и} \quad \left[\begin{array}{llll} n=7, & \deg(G)=5, & \deg(F)=4,\\ \text{или} \quad n=6, & \deg(G)=3, & \deg(F)=3,\\ \text{или} \quad n=5, & \deg(G)=1, & \deg(F)=3,\\ \text{или} \quad n=3, & \deg(G)=1, & \deg(F)\leqslant 2. \end{array}\right.$$

2) $\tilde{\mathcal{A}}=(\mathcal{C}_{\mathcal{L}}(D,F)^{\perp})|_{\mathbb{F}_p}$, если

$$g=0 \quad \text{и} \quad n=5, \quad \deg(G)=1, \quad \deg(F)=1$$
$$\text{или} \quad g=1 \quad \text{и} \quad n=5, \quad \deg(G)=4, \quad \deg(F)=2.$$

3) $\tilde{\mathcal{A}}=(\mathcal{C}_{\mathcal{L}}(D,F)|_{\mathbb{F}_p})^{\perp}$, если

$$g=0 \text{ и } \left[\begin{array}{l} n=4,6,\ (3n-10)/2\leqslant \deg(G)\leqslant n,\ \deg(F)\leqslant (4n-\deg(G)-5)/4,\\ \text{или}\\ n=10,\ 1\leqslant \deg(G)\leqslant 8,\ \deg(F)\leqslant (35-\deg(G))/4,\\ \text{или}\\ n\geqslant 12 \text{ и } n \text{ — чётное},\ 1\leqslant \deg(G)\leqslant n-2,\ \deg(F)\leqslant (\deg(G)+3)/2, \end{array}\right.$$

или

$$g=1, \quad n\geqslant 4 \text{ и } n \text{ — чётное}, \quad 2\leqslant \deg(G)\leqslant n-1, \quad \deg(F)\leqslant (\deg(G)+2)/2,$$

или $\quad g\geqslant 2, \quad n\geqslant 6 \text{ и } n \text{ — чётное}, \quad \deg(G)=4, \quad \deg(F)=1,$

или

$$g\geqslant 2,\ n\geqslant 5g-5 \text{ и } n \text{ — чётное},\ 5g-6\leqslant \deg(G)\leqslant n-1,\ \deg(F)\leqslant (\deg(G)+3-g)/2.$$

4) $\tilde{\mathcal{A}}=((\mathcal{C}_{\mathcal{L}}(D,F)^{\perp})|_{\mathbb{F}_p})^{\perp}$, если

$$g=0 \quad \text{и} \quad \left[\begin{array}{l} n=4, \quad \deg(G)=2, \quad 1\leqslant \deg(F)\leqslant 3\\ \text{или}\\ n=6,8,\ 2\leqslant \deg(G)\leqslant (3n-11)/2,\ \deg(F)\geqslant (2n-\deg(G)-7)/2 \end{array}\right.$$

или $\quad 1\leqslant g\leqslant 3, \quad n\geqslant 3g+3 \text{ и } n \text{ — чётное}, \quad 3g+2<\deg(G)\leqslant n-1,$

$$\deg(F)\geqslant (2n-\deg(G)+5g-7)/2.$$

Во всех четырёх случаях $\mathcal{B}=(\mathcal{A}*(\mathcal{C}^{\perp})|_{\mathbb{F}_p})^{\perp}$.

Доказательство. Обозначим $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ и отметим, что изначально код $\mathcal{C}^{\perp}$ определён над квадратичным расширением поля $\mathbb{F}_p$, т. е. над $\mathbb{F}_q = \mathbb{F}_{p^2}$.

1. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = \mathcal{A}|_{\mathbb{F}_p}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = 2k(\mathcal{A}|_{\mathbb{F}_p}) \geqslant k(\mathcal{A}) - n = 2\deg(F) - 2g - n + 2$.
Так как $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, условие $k(\tilde{\mathcal{A}}) > t$ имеет место, если $\deg(F) \geqslant$ $\geqslant (2n + \deg(G) + g - 3)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d(\mathcal{A}|_{\mathbb{F}_p} * \mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A} * \mathcal{C}^{\perp})$.
Поскольку $\mathcal{A} = \mathcal{C}_{\mathcal{L}}(D, F)$ и $\mathcal{C}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, D - G + (\omega))$, то

$$\mathcal{A} * \mathcal{C}^{\perp} \subseteq \mathcal{C}_{\mathcal{L}}(D, D + F - G + (\omega)) = \mathcal{C}_{\mathcal{L}}(D, G - F)^{\perp},$$

тогда

$$d(\mathcal{A} * \mathcal{C}^{\perp}) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, G - F)^{\perp}) \geqslant \deg(G) + 2 - \deg(F) - 2g.$$

Так как $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \leqslant$ $\leqslant (\deg(G) + 3 - g)/2$.

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}) + d(\mathcal{C}^{\perp}) \geqslant n - \deg(F) + \deg(G) - 2g + 2$.
Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) > n$, если $\deg(F) < \deg(G) - 2g + 2$.

Таким образом, $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$ — пара, исправляющая ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$, если имеет место система

$$\begin{cases} \deg(F) \geqslant (2n + \deg(G) + g - 3)/4, \\ \deg(F) \leqslant (\deg(G) + 3 - g)/2, \\ \deg(F) < \deg(G) + 2 - 2g. \end{cases}$$

Здесь следует рассмотреть два случая:

— Условие $(\deg(G) + g + 2n - 3)/4 \leqslant \deg(F) \leqslant (\deg(G) + 3 - g)/2$ выполняется, если

$$g = 0 \quad \text{и} \quad \left[\begin{array}{llll} & n = 7, & \deg(G) = 5, & \deg(F) = 4, \\ \text{или} & n = 6, & \deg(G) = 3, & \deg(F) = 3, \\ \text{или} & n = 5, & \deg(G) = 1, & \deg(F) = 3, \\ \text{или} & n = 3, & \deg(G) = 1, & \deg(F) \leqslant 2. \end{array}\right.$$

— Условие $(\deg(G) + g + 2n - 3)/4 \leqslant \deg(F) < \deg(G) - 2g + 2$ не выполняется никогда.

2. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = (\mathcal{A}^{\perp})|_{\mathbb{F}_p}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = k((\mathcal{A}^{\perp})|_{\mathbb{F}_p}) \geqslant 2k(\mathcal{A}^{\perp}) - n = n + 2g - 2 - 2\deg(F)$.
Так как $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, условие $k(\tilde{\mathcal{A}}) > t$ имеет место, если $\deg(F) \leqslant$ $\leqslant (2n + 7g - \deg(G) - 5)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d((\mathcal{A}^{\perp})|_{\mathbb{F}_p} * \mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d((\mathcal{A}^{\perp} * \mathcal{C}^{\perp})|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp} * \mathcal{C}^{\perp})$.
Поскольку $\mathcal{A}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, D - F + (\omega))$ и $\mathcal{C}^{\perp} = \mathcal{C}_{\mathcal{L}}(D, D - G + (\omega))$, то $\mathcal{A}^{\perp} * \mathcal{C}^{\perp} \subseteq$ $\subseteq \mathcal{C}_{\mathcal{L}}(D, 2D - G - F + 2(\omega))$, тогда

$$d(\mathcal{A}^{\perp} * \mathcal{C}^{\perp}) \geqslant d(\mathcal{C}_{\mathcal{L}}(D, 2D - G - F + 2(\omega))) \geqslant \deg(G) + \deg(F) - n - 4g + 4.$$

Поскольку $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \geqslant$ $\geqslant (2n + 5g - \deg(G) - 7)/2$.

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp}) + d(\mathcal{C}^{\perp}) \geqslant \deg(F) + \deg(G) - 4g + 4$.
Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) > n$, если $\deg(F) > n + 4g - \deg(G) - 4$.

Таким образом, $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$ — пара, исправляющая ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$, если имеет место следующая система:

$$\begin{cases} \deg(F) \leqslant (2n + 7g - \deg(G) - 5)/4, \\ \deg(F) \geqslant (2n + 5g - \deg(G) - 7)/2, \\ \deg(F) > n + 4g - \deg(G) - 4. \end{cases}$$

Здесь следует рассмотреть два случая:

— Условие $(2n + 5g - \deg(G) - 7)/2 \leqslant \deg(F) \leqslant (2n + 7g - \deg(G) - 5)/4$ выполняется, если

$$g = 1 \quad \text{и} \quad n = 5, \quad \deg(G) = 4, \quad \deg(F) = 2$$

или

$$g = 0 \quad \text{и} \quad n = 5, \quad \deg(G) = 1, \quad \deg(F) = 1.$$

— Условие $n + 4g - \deg(G) - 4 \leqslant \deg(F) \leqslant (2n + 7g - \deg(G) - 5)/4$ выполняется, если

$$1 \leqslant n \leqslant 3 \quad \text{и} \quad (2n + 9g - 11)/3 < \deg(G) < 3g - 1.$$

3. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = (\mathcal{A}|_{\mathbb{F}_p})^{\perp}$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$ парой, исправляющей ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}^{\perp}|_{\mathbb{F}_p})^{\perp}$.

— $k(\tilde{\mathcal{A}}) = k((\mathcal{A}|_{\mathbb{F}_p})^{\perp}) = n - k(\mathcal{A}|_{\mathbb{F}_p})$.
Отметим, что $k(\mathcal{A}|_{\mathbb{F}_p}) \geqslant 2k(\mathcal{A}) - n = 2\deg(F) + 2 - 2g - n$. С другой стороны, необходимо, чтобы выполнялось $k(\tilde{\mathcal{A}}) > t$. Поскольку $t = \lfloor(\deg(G) - 3g + 1)/2\rfloor$, окончательно имеем $\deg(F) \leqslant (4n + 7g - \deg(G) - 5)/4$.

— $d(\tilde{\mathcal{B}}^{\perp}) = d((\mathcal{A}|_{\mathbb{F}_p})^{\perp} * \mathcal{C}|_{\mathbb{F}_p})$.
Рассмотрим случай, когда код $\tilde{\mathcal{A}}$ является самодуальным, т. е. $(\mathcal{A}|_{\mathbb{F}_p})^{\perp} = \mathcal{A}|_{\mathbb{F}_p}$. Следовательно, $k(\mathcal{A}|_{\mathbb{F}_p}) = n/2$, что возможно при $\deg(F) \leqslant (3n + 4g - 4)/4$. Тогда получаем

$$d(\tilde{\mathcal{B}}^{\perp}) = d(\mathcal{A}|_{\mathbb{F}_p} * \mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d((\mathcal{A} * \mathcal{C}^{\perp})|_{\mathbb{F}_p}) \geqslant d(\mathcal{A} * \mathcal{C}^{\perp}) \geqslant$$
$$\geqslant d(\mathcal{C}_{\mathcal{L}}(D, G - F)^{\perp}) \geqslant \deg(G) - \deg(F) - 2g + 2.$$

Так как $t = (\deg(G) + 1 - 3g)/2$, условие $d(\tilde{\mathcal{B}}^{\perp}) > t$ выполняется при $\deg(F) \leqslant$ $\leqslant (\deg(G) + 3 - g)/2$.
Следует рассмотреть два случая, чтобы определить $\deg(F)$:

— Случай $\deg(F) \leqslant (3n + 4g - 4)/4$ имеет место при $\deg(G) > (3n + 6g - 10)/2$, что возможно, если

$$g = 0, \quad n = 4, 6, 8, \quad \deg(G) \geqslant (3n - 10)/2, \quad \deg(F) \leqslant (3n - 4)/4$$

или

$$g = 1, \quad n = 2, \quad \deg(G) = 1, \quad \deg(F) = 1.$$

— Случай $\deg(F) \leqslant (\deg(G) + 3 - g)/2$ имеет место при $\deg(G) < (3n + 6g - 10)/2$.

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) = d((\mathcal{A}|_{\mathbb{F}_p})^\perp) + d(\mathcal{C}^\perp|_{\mathbb{F}_p}) = d(\mathcal{A}|_{\mathbb{F}_p}) + d(\mathcal{C}^\perp|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}) + d(\mathcal{C}) \geqslant n - \deg(F) + \deg(G) - 2g + 2$.
Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}|_{\mathbb{F}_p}) > n$, если $\deg(F) < \deg(G) + 2 - 2g$.

Таким образом, построение пары $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, исправляющей ошибки для кода $\mathcal{C}^\perp|_{\mathbb{F}_p}$, возможно, если справедлива одна из следующих систем:

$$\begin{cases} g = 0, n = 4, 6, 8, \\ \deg(G) > (3n - 10)/2, \\ \deg(F) \leqslant (3n - 4)/4, \\ \deg(F) \leqslant (4n - \deg(G) - 5)/4, \\ \deg(F) < \deg(G) + 2, \end{cases} \quad \text{или} \quad \begin{cases} g = 1, n = 2, \\ \deg(G) = 1, \\ \deg(F) = 1, \\ \deg(F) \leqslant (4n + 2 - \deg(G))/4, \\ \deg(F) < \deg(G), \end{cases}$$

$$\text{или} \quad \begin{cases} \deg(G) < (3n + 6g - 10)/2, \\ \deg(F) \leqslant (4n + 7g - \deg(G) - 5)/4, \\ \deg(F) \leqslant (\deg(G) + 3 - g)/2, \\ \deg(F) < \deg(G) + 2 - 2g. \end{cases}$$

Уточняя все три системы, окончательно получаем следующие результаты:

$$g = 0, \quad n = 4, 6, \quad (3n - 10)/2 \leqslant \deg(G) \leqslant n - 2, \quad \deg(F) \leqslant (4n - \deg(G) - 5)/4,$$
$$g = 0, \quad n = 10, \quad \deg(G) \leqslant 8, \quad \deg(F) \leqslant (35 - \deg(G))/4,$$
$$g = 0, \quad n > 10 \text{ и } n \text{ — чётное}, \quad 1 \leqslant \deg(G) \leqslant n - 2, \quad \deg(F) \leqslant (\deg(G) + 3)/2,$$
$$g = 1, \quad n \geqslant 4 \text{ и } n \text{ — чётное}, \quad 2 \leqslant \deg(G) \leqslant n - 1, \quad \deg(F) \leqslant (\deg(G) + 2)/2,$$
$$g \geqslant 2, \quad n \geqslant 6 \text{ и } n \text{ — чётное}, \quad \deg(G) = 4, \quad \deg(F) = 1,$$
$$g \geqslant 2, \ n \geqslant 5g - 5 \text{ и } n \text{ – чётное}, \ 5g - 6 \leqslant \deg(G) \leqslant n - 1, \ \deg(F) \leqslant (\deg(G) + 3 - g)/2.$$

4. Проверим, является ли пара кодов $\tilde{\mathcal{A}} = (\mathcal{A}^\perp|_{\mathbb{F}_p})^\perp$ и $\tilde{\mathcal{B}} = (\tilde{A} * \mathcal{C}^\perp|_{\mathbb{F}_p})^\perp$ парой, исправляющей ошибки для кода $\mathcal{C}^\perp|_{\mathbb{F}_p}$:

— Учитывая вид $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, получаем $\tilde{\mathcal{A}} * \tilde{\mathcal{B}} \subseteq (\mathcal{C}^\perp|_{\mathbb{F}_p})^\perp$.

— $k(\tilde{\mathcal{A}}) = k((\mathcal{A}^\perp|_{\mathbb{F}_p})^\perp) = n - k(\mathcal{A}^\perp|_{\mathbb{F}_p})$.
Для выполнения условия 2 определения 3 необходимо, чтобы $k(\mathcal{A}^\perp|_{\mathbb{F}_p}) < n - t$. С другой стороны, $k(\mathcal{A}^\perp|_{\mathbb{F}_p}) \geqslant 2k(\mathcal{A}^\perp) - n = n + 2g - 2\deg(F) - 2$. Принимая во внимание, что $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, и уточняя, при каком ограничении на $\deg(F)$ выполняются неравенства

$$n + 2g - 2\deg(F) - 2 \leqslant k(\mathcal{A}^\perp|_{\mathbb{F}_p}) < n - t,$$

получаем $\deg(F) \geqslant (\deg(G) + g - 3)/4$.

— $d(\tilde{\mathcal{B}}^\perp) = d((\mathcal{A}^\perp|_{\mathbb{F}_p})^\perp * \mathcal{C}^\perp|_{\mathbb{F}_p})$.
Рассмотрим случай, когда код $\tilde{\mathcal{A}}$ является самодуальным, т. е. $(\mathcal{A}|_{\mathbb{F}_p})^\perp = \mathcal{A}|_{\mathbb{F}_p}$. Следовательно, $k(\mathcal{A}|_{\mathbb{F}_p}) = n/2$, что возможно при $\deg(F) \geqslant (n + 4g - 4)/4$. Тогда $d(\tilde{\mathcal{B}}^\perp) = d(\mathcal{A}^\perp|_{\mathbb{F}_p} * \mathcal{C}^\perp|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^\perp * \mathcal{C}^\perp)$. Поскольку $\mathcal{A} = \mathcal{C}_\mathcal{L}(D, F)$ и $\mathcal{C} = \mathcal{C}_\mathcal{L}(D, G)$, то

$$d(\tilde{\mathcal{B}}^\perp) \geqslant d(\mathcal{C}_\mathcal{L}(D, D - F + (\omega)) * \mathcal{C}_\mathcal{L}(D, D - G + (\omega))) \geqslant$$
$$\geqslant d(\mathcal{C}_\mathcal{L}(D, 2D - G - F + 2(\omega))) \geqslant n + 2g - 2 - 2\deg(F).$$

Так как $t = \lfloor(\deg(G) + 1 - 3g)/2\rfloor$, условие $d(\tilde{\mathcal{B}}^\perp) > t$ выполняется при $\deg(F) \geqslant (2n + 5g - \deg(G) - 7)/2$.
Следует рассмотреть два случая, чтобы определить $\deg(F)$:

— Случай $\deg(F) \geqslant (2n+5g-\deg(G)-7)/2$ имеет место при $\deg(G) \leqslant (3n+6g-10)/2$.
— Случай $\deg(F) \geqslant (n+4g-4)/4$ имеет место при $\deg(G) > (3n+6g-10)/2$, что возможно, если

$$g=0, \quad n=4,6,8, \quad \deg(G) > (3n-10)/2, \quad \deg(F) \geqslant (n-4)/4.$$

— $d(\tilde{\mathcal{A}}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) = d((\mathcal{A}^{\perp}|_{\mathbb{F}_p})^{\perp}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) = d(\mathcal{A}^{\perp}|_{\mathbb{F}_p}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) \geqslant d(\mathcal{A}^{\perp}) + d(\mathcal{C}^{\perp}) \geqslant \deg(F) + \deg(G) - 4g + 4$.
Очевидно, что $d(\tilde{\mathcal{A}}) + d(\mathcal{C}^{\perp}|_{\mathbb{F}_p}) > n$, если $\deg(F) > n - \deg(G) + 4g - 4$.

Таким образом, построение пары $\tilde{\mathcal{A}}$ и $\tilde{\mathcal{B}}$, исправляющей ошибки для кода $\mathcal{C}^{\perp}|_{\mathbb{F}_p}$, возможно, если справедлива одна из систем:

$$\begin{cases} g=0, \\ n=4,6,8, \\ \deg(G) > (3n-10)/2, \\ \deg(F) \geqslant (n-4)/4, \\ \deg(F) \geqslant n - \deg(G) - 3, \end{cases} \quad \text{или} \quad \begin{cases} g=1, \\ n=2, \\ \deg(G)=1, \\ \deg(F)=1, \\ \deg(F) \geqslant n+1-\deg(G), \end{cases}$$

$$\text{или} \quad \begin{cases} \deg(G) \leqslant (3n+6g-10)/2, \\ \deg(F) \geqslant (2n+5g-\deg(G)-7)/2, \\ \deg(F) > n+4g-\deg(G)-3. \end{cases}$$

Уточняя системы, окончательно получаем следующие результаты:

$$g=0, \quad n=4, \quad \deg(G)=2, \quad 1 \leqslant \deg(F) \leqslant 3;$$

$g=0$, $6 \leqslant n \leqslant 8$ и n — чётное, $2 \leqslant \deg(G) \leqslant (3n-11)/2$, $\deg(F) \geqslant (2n-\deg(G)-7)/2$;

$1 \leqslant g \leqslant 3$, $n \geqslant 3g+3$ и n — чётное, $3g+2 < \deg(G) \leqslant n-1$, $\deg(F) \geqslant (2n-\deg(G)+5g-7)/2$.

Теорема 7 доказана. ■

Замечание 1. Стоит отметить, что в условиях теорем 6 и 7 вовсе не гарантируется, что пара, исправляющая ошибки, существует для любого кода C с заданными параметрами; получены границы, при которых существование пары в принципе возможно. В п. 2 и 4 теоремы 6 и в п. 3 и 4 теоремы 7 рассматривается случай самодуальности кода $\tilde{\mathcal{A}}$, что на практике труднодостижимо. В дополнение, ввиду грубости границы для оценки размерности подполевого подкода, в общем случае коды, составляющие пару, могут вырождаться. Необходимы дополнительные вычислительные эксперименты для уточнения полученных границ для параметров пар, исправляющих ошибки для подполевого подкода.

Заключение

Для обеспечения условия 2 в определении пары, исправляющей ошибки, в теоремах 4 и 5 мы ограничиваемся рассмотрением случаев, когда $\deg(F) = t+g$ и $\deg(F) = n+g-t-2$, хотя данные значения являются нижней и верхней границами соответственно для $\deg(F)$ в зависимости от вида кода $\mathcal{A}$.

Отметим, что теоремы 6 и 7 доказаны для случая, когда исходный АГ-код определён над квадратичным расширением $\mathbb{F}_{p^2}$, чтобы получить более компактные соотношения. Построение пар, исправляющих ошибки для произвольного АГ-кода, определённого над расширениями бóльших степеней, — всё ещё открытый вопрос. Кроме того,

следует отметить, что в подслучаях, где мы рассматриваем самодуальный код, наличие пары, исправляющей ошибки, возможно, но необязательно выполнимо. Для более сильного утверждения необходимо провести ряд вычислительных экспериментов.

Весьма интересным представляется также вычисление пар, исправляющих ошибки для трэйс-кодов (такие коды получены с помощью применения к кодовым словам кода $\mathcal{C}$, определённым над $\mathbb{F}_q$, функции следа $\mathrm{tr} : \mathbb{F}_{p^m} \to \mathbb{F}_p$), поскольку такие коды связаны с дуальными соотношением $(\mathcal{C}|_{\mathbb{F}_p})^\perp = \mathrm{tr}(\mathcal{C}^\perp)$.

ЛИТЕРАТУРА

1. *Justesen J., Larsen K., Jensen H., et al.* Construction and decoding of a class of algebraic geometry codes // IEEE Trans. Inform. Theory. 1989. No. 35(4). P. 811–821.
2. *Skorobogatov A. N. and Vlădut S. G.* On the decoding of algebraic-geometric codes // IEEE Trans. Inform. Theory. 1990. No. 36(5). P. 1051–1060.
3. *Pellikaan R.* On decoding by error location and dependent sets of error positions // Discrete Math. 1992. No. 106–107. P. 369–381.
4. *Kötter R.* A unified description of an error locating procedure for linear codes // Proc. Algebraic Combinatorial Coding Theory III. Hermes, 1992. P. 113–117.
5. *Couvreur A., Marquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes // IEEE Trans. Inform. Theory. 2017. No. 63. P. 5404–5418.
6. *Малыгина Е. С., Кунинец А. А.* Вычисление пар, исправляющих ошибки, для алгеброгеометрического кода // Прикладная дискретная математика. Приложение. 2023. № 16. С. 136–140.
7. *Milne J. S.* Algebraic Geometry. `https://www.jmilne.org/math/CourseNotes/AG510.pdf`.
8. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
9. *Pellikaan R.* On the existence of error-correcting pairs // Statistical Planning and Inference. 1996. No. 51. P. 229–242.
10. *Marquez-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`.
11. *Mumford D.* Varieties defined by quadratic equations // Questions on Algebraic Varieties. Berlin; Heidelberg: Springer, 2011. P. 29–100.

REFERENCES

1. *Justesen J., Larsen K., Jensen H., et al.* Construction and decoding of a class of algebraic geometry codes. IEEE Trans. Inform. Theory, 1989, no. 35(4), pp. 811–821.
2. *Skorobogatov A. N. and Vlădut S. G.* On the decoding of algebraic-geometric codes. IEEE Trans. Inform. Theory, 1990, no. 36(5), pp. 1051–1060.
3. *Pellikaan R.* On decoding by error location and dependent sets of error positions. // Discrete Math., 1992, no. 106–107, pp. 369–381.
4. *Kötter R.* A unified description of an error locating procedure for linear codes. Proc. Algebraic Combinatorial Coding Theory III, Hermes, 1992, pp. 113–117.
5. *Couvreur A., Marquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. IEEE Trans. Inform. Theory, 2017, no. 63, pp. 5404–5418.
6. *Malygina E. S. and Kuninets A. A.* Vychislenie par, ispravlyayushchikh oshibki, dlya algebro-geometricheskogo koda [Calculation of error-correcting pairs for an algebraic-geometric code]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2023, no. 16, pp. 136–140. (in Russian)

7. *Milne J. S.* Algebraic Geometry. https://www.jmilne.org/math/CourseNotes/AG510.pdf.
8. *Stichtenoth H.* Algebraic Function Fields and Codes. Springer Verlag, 1991.
9. *Pellikaan R.* On the existence of error-correcting pairs. Statistical Planning and Inference, 1996, no. 51, pp. 229–242.
10. *Marquez-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.
11. *Mumford D.* Varieties defined by quadratic equations. Questions on Algebraic Varieties. Berlin, Heidelberg, Springer, 2011, pp. 29–100.