ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 3**

УДК 621.391.1 : 519.725 : 512.772.7

© 2020 г. **Н. Патанкер, С.К. Сингх**[1]

О ГЕОМЕТРИЧЕСКИХ КОДАХ ГОППЫ ПО ЭЛЕМЕНТАРНЫМ АБЕЛЕВЫМ p-РАСШИРЕНИЯМ ПОЛЯ $\mathbb{F}_{p^s}(x)$

Пусть p – простое число, а $s > 0$ – натуральное. Рассматриваются одноточечные геометрические коды Гоппы, ассоциированные с элементарными абелевыми p-расширениями поля $\mathbb{F}_{p^s}(x)$. Вычисляется их размерность и точное значение минимального расстояния в нескольких случаях. Эти коды являются частным случаем слабых за́мковых кодов. Также приводится список точных значений второго обобщенного веса Хэмминга этих кодов в нескольких случаях. Получены простые критерии самодвойственности и квазисамодвойственности этих кодов. Кроме того, построены примеры квантовых, сверточных и локально восстанавливаемых кодов по этим функциональным полям.

Ключевые слова: элементарное абелево p-расширение поля $\mathbb{F}_{p^s}(x)$, геометрические коды Гоппы, обобщенный вес Хэмминга.

DOI: 10.31857/S0555292320030031

§ 1. Введение

Пусть $\mathbb{F}_{p^s}$ – конечное поле из p^s элементов характеристики p (где s – натуральное число). Линейным кодом называется $\mathbb{F}_{p^s}$-подпространство пространства $\mathbb{F}_{p^s}^n$ – стандартного n-мерного векторного пространства над $\mathbb{F}_{p^s}$. Такие коды используются для передачи информации.

В [1] Гоппа заметил, что можно использовать дивизоры в поле алгебраических функций для построения класса линейных кодов. В конструкции Гоппы выбирается дивизор G и n рациональных точек (т.е. точек степени 1) алгебраического функционального поля, чтобы получить линейный код длины n. Такие коды называются геометрическими кодами Гоппы. Если G имеет вид rQ для точки Q функционального поля и некоторого целого r, то такие коды называются одноточечными. Одноточечные геометрические коды Гоппы на функциональном поле эрмитовой кривой изучались, например, в [2–5].

Элементарное абелево p-расширение поля рациональных функций $\mathbb{F}_{p^s}(x)$ – это расширение Галуа F поля $\mathbb{F}_{p^s}(x)$, такое что $\mathrm{Gal}(F/\mathbb{F}_{p^s}(x))$ является элементарной абелевой группой порядка p. Примером такого расширения является функциональное поле, ассоциированное с эрмитовой кривой. Свойства элементарных абелевых p-расширений поля $\mathbb{F}_{p^s}(x)$ изучались, в частности, в [2, 6–8]. Другим примером элементарного абелева p-расширения поля $\mathbb{F}_{p^s}(x)$ является функциональное поле $\mathbb{F}_{p^s}(x, y)/\mathbb{F}_{p^s}$, заданное уравнением $A(y) = B(x)$, где $A(T) \in \mathbb{F}_{p^s}[T]$ – сепарабельный аддитивный многочлен степени $q = p^t$ для некоторого t, все корни которого лежат в $\mathbb{F}_{p^s}$, а степень многочлена $B(T) \in \mathbb{F}_{p^s}[T]$ не кратна p. Неособая проективная

[1] Работа выполнена при финансовой поддержке премии ECR/2016/000649 Департамента науки и технологии (DST) правительства Индии.

кривая $\mathcal{X}$, ассоциированная с таким функциональным полем, изучалась в [8], где были получены параметры геометрических кодов Гоппы $C_{\mathcal{L}}(D,G)$ на этом функциональном поле в предположении, что $\deg D \geqslant 4g-2$. В настоящей статье мы изучаем одноточечные геометрические коды Гоппы на элементарном абелевом p-расширении поля $\mathbb{F}_{p^s}(x)$ без этого предположения.

Специальным типом элементарных абелевых p-расширений поля $\mathbb{F}_{p^s}(x)$, рассматриваемых в настоящей статье, являются примеры функциональных полей, ассоциированных со слабыми за́мковыми кривыми[2]. Замковые и слабые замковые кривые представляют интерес для целей теории кодирования. Многие известные коды принадлежат классу замковых и слабых замковых кодов. Замковые и слабые замковые кривые и коды на них изучались, в частности, в [9–12]. В [9] рассматривались одноточечные геометрические коды Гоппы, возникающие из замковых и слабых замковых кривых. Были получены границы на минимальное расстояние и обобщенные веса Хэмминга таких кодов. В [10] была выведена граница d^* типа порядковой границы на минимальное расстояние некоторых замковых кодов (т.е. одноточечных геометрических кодов Гоппы по замковым кривым), в частности, связанных с полугруппами, порожденными двумя элементами, и телескопическими полугруппами. В [11] была вычислена граница d_2^* на второй обобщенный вес Хэмминга для некоторых замковых кодов. В [12] изучались геометрические коды Гоппы, по которым можно построить квантовые коды. Особое внимание было уделено семейству замковых и слабых замковых кодов. В [13] были получены новые квантовые коды с хорошими параметрами, построенные по самоортогональным геометрическим кодам Гоппы на функциональных полях, ассоциированных с широким классом кривых. Наша цель в настоящей статье – определить точное значение второго обобщенного веса Хэмминга одноточечных геометрических кодов Гоппы, построенных по элементарным абелевым расширениям поля $\mathbb{F}_{p^s}(x)$.

Статья имеет следующую структуру. В § 2 напоминаются некоторые результаты о конструкции Гоппы линейных кодов и об обобщенных весах Хэмминга линейных кодов. В § 3 изучаются свойства элементарного абелева p-расширения $F/\mathbb{F}_{p^s}$. В § 4 определяются одноточечные геометрические коды Гоппы на этом функциональном поле и изучаются их параметры. В § 5 приведен список значений второго обобщенного веса Хэмминга этих кодов. В § 6 описываются простые условия самодвойственности и квазисамодвойственности таких кодов. В §§ 7, 8 получены примеры квантовых и сверточных кодов по одноточечным геометрическим кодам Гоппы, построенным в § 4. В § 9 получены локально восстанавливаемые коды по функциональным полям $F/\mathbb{F}_{p^s}$.

§ 2. Предварительные сведения

2.1. Геометрические коды Гоппы. Конструкция Гоппы линейных кодов над $\mathbb{F}_{p^s}$ (см. [2, гл. 2]) состоит в следующем.

Пусть $F'/\mathbb{F}_{p^s}$ – алгебраическое функциональное поле рода g'. Пусть $P_1,\dots,P_n$ – попарно различные точки степени 1 поля $F'/\mathbb{F}_{p^s}$. Положим $D' := P_1+\ldots+P_n$, и пусть G – дивизор поля $F'/\mathbb{F}_{p^s}$, такой что $\operatorname{supp}(G)\cap\operatorname{supp}(D')=\varnothing$. Геометрический код Гоппы $C_{\mathcal{L}}(D',G)$, ассоциированный с D' и G, определяется как

$$C_{\mathcal{L}}(D',G) := \{(x(P_1),\dots,x(P_n)) :\ x\in\mathcal{L}(G)\} \subseteq \mathbb{F}_{p^s}^n.$$

Таким образом, $C_{\mathcal{L}}(D',G)$ является $[n,k,d]$-кодом с параметрами $k=\dim(\mathcal{L}(G))-$ $-\dim(\mathcal{L}(G-D'))$ и $d\geqslant n-\deg(G)$.

[2] Замковые кривые (Castle curves) названы в честь замка (крепости) Ла Мота в Медина-дель-Кампо, Испания, на конференции в которой был впервые представлен доклад, посвященный таким кривым – *прим. ред.*

Еще один код, ассоциированный с дивизорами G и D', определяется с помощью локальных компонент дифференциалов Вейля. Код $C_\Omega(D', G) \subseteq \mathbb{F}_{p^s}^n$ определяется как

$$C_\Omega(D', G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) : \omega \in \Omega_{F'}(G - D')\}.$$

Таким образом, $C_\Omega(D', G)$ является $[n, k, d]$-кодом с параметрами $k = i(G-D')-i(G)$ и $d \geqslant \deg(G) - (2g' - 2)$.

Код $C_\Omega(D', G)$ является двойственным к $C_\mathcal{L}(D', G)$ относительно евклидова скалярного произведения на $\mathbb{F}_{p^s}^n$ т.е. $C_\Omega(D', G) = C_\mathcal{L}(D', G)^\perp$. Пусть η – дифференциал Вейля поля F', такой что $\nu_{P_i}(\eta) = -1$ и $\eta_{P_i}(1) = 1$ для $i = 1, \ldots, n$. Тогда $C_\mathcal{L}(D', G)^\perp = C_\Omega(D', G) = C_\mathcal{L}(D', D' - G + (\eta))$.

2.2. Обобщенные веса Хэмминга линейных кодов. Носителем линейного $[n, k]$-кода C над $\mathbb{F}_{p^s}$ называется множество

$$\operatorname{supp}(C) := \{i : x_i \neq 0 \text{ для некоторого } \boldsymbol{x} = (x_1, \ldots, x_n) \in C\}.$$

Для $1 \leqslant \ell \leqslant k$ назовем *ℓ-м обобщенным весом Хэмминга* кода C величину

$$d_\ell(C) := \min\{|\operatorname{supp}(D)| : D \text{ – линейный подкод } C, \text{ такой что } \dim(D) = \ell\}.$$

В частности, первый обобщенный вес Хэмминга кода C – это обычное минимальное расстояние. *Иерархией весов* кода C называется множество $\{d_1(C), \ldots, d_k(C)\}$ обобщенных весов Хэмминга. Обобщенные веса Хэмминга для линейных кодов были введены в [14, 15] и затем независимо в [16]. Мотивацией к изучению этих весов были некоторые приложения в криптографии.

Некоторые свойства обобщенных весов Хэмминга кода C перечислены в следующих теоремах.

Теорема 1 [16, теорема 1]. *Для линейного $[n, k]$-кода C, где $k > 0$, справедливы неравенства*

$$1 \leqslant d_1(C) < d_2(C) < \ldots < d_k(C) \leqslant n.$$

Пусть $\boldsymbol{H}$ – проверочная матрица кода C, и пусть $\boldsymbol{h}_i$, $1 \leqslant i \leqslant n$, – ее векторы-столбцы. Для $I \subseteq \{1, \ldots, n\}$ обозначим через $\langle \boldsymbol{h}_i : i \in I\rangle$ пространство, порожденное этими векторами. Тогда имеет место следующая

Теорема 2 [16, теорема 2]. *Справедливо равенство*

$$d_\ell(C) = \min\{|I| : |I| - \operatorname{rank}(\langle \boldsymbol{h}_i : i \in I\rangle) \geqslant \ell\}.$$

Для геометрического кода Гоппы $C_\mathcal{L}(D', G)$ его ℓ-й обобщенный вес Хэмминга описывает следующая

Теорема 3 [17, следствие 1]. *Пусть $C = C_\mathcal{L}(D', G)$ – код размерности k, и пусть $a := \dim(\mathcal{L}(G - D')) \geqslant 0$. Тогда для любого ℓ, $1 \leqslant \ell \leqslant k$, справедливы равенства*

$$d_\ell(C) = \min\{\deg(D'') : 0 \leqslant D'' \leqslant D', \dim(\mathcal{L}(G - D' + D'')) \geqslant \ell + a\} =$$
$$= \min\{n - \deg(D'') : 0 \leqslant D'' \leqslant D', \dim(\mathcal{L}(G - D'')) \geqslant \ell + a\}.$$

2.3. Расстояния Фенга – Рао числовых полугрупп. Расстояния Фенга – Рао числовых полугрупп были введены в [18]. Вкратце поясним их в этом пункте.

Пусть A – числовая полугруппа. Если для некоторого множества $G \subseteq A$ любой элемент $x \in A$ можно представить в виде линейной комбинации

$$x = \sum_{y \in G} \lambda_y y,$$

где лишь конечное число коэффициентов $\lambda_y \in \mathbb{N} \cup \{0\}$ отличны от нуля, то говорят, что A порождается множеством G. Хорошо известно, что любая числовая полугруппа конечно порождена. Элемент $x \in A$ называется неприводимым, если из равенства $x = a + b$ для $a, b \in A$ следует, что $ab = 0$. Любое порождающее множество содержит множество всех неприводимых элементов, и это множество неприводимых элементов порождает A. Число неприводимых элементов называется *размерностью вложения* полугруппы A. Пронумеруем элементы полугруппы A в порядке возрастания:

$$A = \{\rho_1 = 0 < \rho_2 < \ldots\}.$$

Для заданных $a, b \in \mathbb{Z}$ будем говорить, что a *делит* b, и записывать это в виде

$$a \leqslant_A b, \quad \text{если} \quad b - a \in A.$$

Это бинарное отношение является отношением порядка.

Через $D(y)$ обозначается множество *делителей* элемента y в A, и для заданного множества $M = \{m_1, \ldots, m_t\} \subseteq A$ положим $D(M) = D(m_1, \ldots, m_t) = \bigcup\limits_{i=1}^{t} D(m_i)$.

Определение 1. Пусть A – числовая полугруппа, т.е. подмоноид в $\mathbb{N}$, такой что $|\mathbb{N} \backslash A| < \infty$ и $0 \in A$. Величина $g := |\mathbb{N} \backslash A|$ называется *родом* полугруппы A. Единственный элемент $c \in A$, такой что $c - 1 \notin A$ и $c + u \in A$ для всех $u \in \mathbb{N}$, называется *кондуктором* полугруппы A. (Классическое) расстояние Фенга – Рао полугруппы A задается функцией

$$\delta_{\mathrm{FR}} \colon A \to \mathbb{N}, \quad x \mapsto \delta_{\mathrm{FR}}(x) := \min\{|D(m_1)| : \ m_1 \geqslant x, \ m_1 \in A\}.$$

Имеется несколько хорошо известных результатов о функции δ_{FR} для произвольной числовой полугруппы A. Одним из важных результатов является такой:

$$\delta_{\mathrm{FR}}(x) \geqslant x + 1 - 2g \quad \text{для всех } x \in A, \text{ таких что } x \geqslant c.$$

Следующий результат дает границу на обобщенные веса Хэмминга некоторых кодов через функцию δ_{FR}.

Теорема 4 [18, теорема 46]. *Пусть* $A = \{0 = \rho_1 < \rho_2 < \ldots < \rho_n < \ldots\}$ – *числовая полугруппа с размерностью вложения* 2. *Тогда*

$$d_\ell(C_t) \geqslant \delta_{\mathrm{FR}}(t+1) + \rho_\ell$$

для $\ell = 1, \ldots, k_t$, *где* C_t – *код из массива кодов, определенного в* [19], *а* k_t – *размерность кода* C_t.

§ 3. Элементарные абелевы p-расширения $F/\mathbb{F}_{p^s}$

Пусть $K := \mathbb{F}_{p^s}$, и пусть q – степень числа p. Предположим, что все корни уравнения $T^q + \mu T = 0$ лежат в поле K (выберем s достаточно большим, так чтобы все корни принадлежали K). Обозначим через $\beta_1, \ldots, \beta_q$ корни многочлена $T^q + \mu T$ в K. Пусть m – натуральное число, взаимно простое с p, такое что $m < p^s$. Выберем m различных элементов $\alpha_1, \ldots, \alpha_m \in K$. Положим $f(x) := \prod\limits_{i=1}^{m} (x - \alpha_i)$.

Рассмотрим функциональное поле F/K, заданное уравнением

$$y^q + \mu y = f(x) \in K[x], \tag{1}$$

где $0 \neq \mu \in K$.

Замечание 1. Имеет место неравенство $\min\{q, m\} \geqslant 2$ за исключением случая, когда $m = 1$ и поэтому F/K – поле рациональных функций.

Функциональное поле, заданное уравнением (1), является элементарным абелевым p-расширением поля $K(x)$, как указано в [2]. Некоторые свойства расширения F/K описывает следующая

Лемма 1 [2, с. 232]. *Справедливы следующие утверждения*:

1. *Расширение F/K имеет род $g = (q-1)(m-1)/2$;*
2. *Полюс $P_\infty \in \mathbb{P}_{K(x)}$ функции x в $K(x)$ имеет единственный прообраз $Q_\infty \in \mathbb{P}_F$ степени 1, причем $e(Q_\infty|P_\infty) = q$;*
3. *Дифференциал dx имеет дивизор*

$$(dx) = (2g-2)Q_\infty = ((q-1)(m-1)-2)Q_\infty;$$

4. *Функция x имеет дивизор полюсов $(x)_\infty = qQ_\infty$, а функция y – дивизор полюсов $(y)_\infty = mQ_\infty$;*
5. *Пусть $r \geqslant 0$. Тогда элементы $x^i y^j$, где*

$$0 \leqslant i, \quad 0 \leqslant j \leqslant q-1, \quad qi + mj \leqslant r,$$

образуют базис пространства $\mathcal{L}(rQ_\infty)$ над K;

6. *Точками F/K степени 1 являются точки P_{α_i,β_j}, где $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant q$.*

Пусть Q – точка степени 1 функционального поля F'/K'. Целое число $\ell \geqslant 0$ называется порядком полюса в точке Q, если существует элемент $z \in F'$, такой что $(z)_\infty = \ell Q$. Пусть $p_1 < p_2 < \ldots$ – последовательность порядков полюсов в точке Q (т.е. p_a – a-й порядок полюса в Q); таким образом, $\dim(\mathcal{L}(p_a Q)) = a$, так что $p_1 = 0$. Полугруппа Вейерштрасса H точки Q – это множество порядков полюсов в Q.

Имеется следующий результат о полугруппе Вейерштрасса H точки Q_∞.

Лемма 2 [2,20]. *Полугруппа Вейерштрасса H точки Q_∞ порождена числами m и q, т.е. $H = \langle q, m\rangle$. Наибольший пробел в точке Q_∞ равен $2g-1$, и H является симметрической числовой полугруппой.*

Пусть $\mathcal{X}'$ – неособая проективная кривая, ассоциированная с полем F/K. Тогда $K(\mathcal{X}') \cong F$. Далее мы покажем, что $\mathcal{X}'$ – слабая замковая кривая.

Кривой с отмеченной точкой над полем $\mathbb{F}_{p^s}$ называется пара $(\mathcal{X}, Q)$, где $\mathcal{X}$ – кривая, определенная над $\mathbb{F}_{p^s}$, а $Q \in \mathcal{X}(\mathbb{F}_{p^s})$ – рациональная точка.

Определение 2 [9, определение 2.1]. Кривая с отмеченной точкой $(\mathcal{X}, Q)$ над $\mathbb{F}_{p^s}$ называется слабой замковой кривой, если

- Полугруппа Вейерштрасса H точки Q симметрическая;
- Существуют морфизм $\varphi\colon \mathcal{X} \to \mathbb{P}^1$, такой что $\mathrm{div}_\infty(\varphi) = hQ$, а также элементы $\gamma_1, \ldots, \gamma_b \in \mathbb{F}_{p^s}$, такие что для всех $i = 1, \ldots, b$ выполнено $\varphi^{-1}(\gamma_i) \subseteq \mathcal{X}(\mathbb{F}_{p^s})$, причем $\#\varphi^{-1}(\gamma_i) = h$.

Лемма 3. $(\mathcal{X}', Q_\infty)$ – *слабая замковая кривая.*

Доказательство. По лемме 2 полугруппа H точки Q_∞ симметрическая. Положим $\varphi := x$, т.е.

$$\varphi\colon \mathcal{X}' \to \mathbb{P}^1, \quad P \mapsto [x(P) : 1].$$

Тогда $(x)_\infty = qQ_\infty$. Для $1 \leqslant i \leqslant m$ имеем

$$\varphi^{-1}(\alpha_i) = \{(\alpha_i, \beta_1), \ldots, (\alpha_i, \beta_q)\} \subseteq \mathcal{X}'(K).$$

(Из [21, теорема 3.1.15] следует, что K-рациональные точки кривой $\mathcal{X}'$ соответствуют точкам степени 1 поля F. Обозначим через P_{α_i} нуль функции $(x-\alpha_i)$ в $K(x)$, т.е. точку степени 1, соответствующую K-рациональной точке α_i на $\mathbb{P}^1$. Тогда согласно [2, с. 232] имеется ровно q точек P_{α_i,β_j}, $1 \leqslant j \leqslant q$, степени 1, лежащих над P_{α_i}, для каждого i, $1 \leqslant i \leqslant m$. Таким образом, P_{α_i,β_j} соответствует (α_i, β_j).) ▲

§ 4. Геометрические коды Гоппы на F/K

В [2] исследовались одноточечные геометрические коды Гоппы на эрмитовом функциональном поле. В [9] были определены одноточечные геометрические коды Гоппы на слабых замковых кривых (т.е. слабые замковые коды) и изучены их параметры. В этом параграфе мы определяем одноточечные геометрические коды Гоппы на F/K, следуя [9], и находим их параметры, используя идеи из [2, 5, 9].

Определение 3. Для $r \in \mathbb{Z}$ положим

$$C_r := C_{\mathcal{L}}(D, rQ_\infty),$$

где

$$D := \sum_{i=1}^{m} \sum_{j=1}^{q} P_{\alpha_i,\beta_j}.$$

Тогда C_r – код длины $N := qm$ над полем K. Для $r < 0$ имеем $\mathcal{L}(rQ_\infty) = \{0\}$, и поэтому $C_r = \{(0, \ldots, 0)\}$. Для $r > N + (2g-2) = 2qm - q - m - 1$ имеем $\dim(C_r) = N$, и поэтому $C_r = K^N$. Таким образом, остается изучить коды C_r для $0 \leqslant r \leqslant 2qm - q - m - 1$.

4.1. Код, двойственный к C_r. В [9, предложение 3.1] были описаны коды, двойственные к слабым замковым кодам. В этом пункте представлено подробное доказательство двойственности для C_r.

Пусть $f(x)$ и D те же, что и в §§ 3, 4. Рассмотрим дифференциал $\eta := \dfrac{f'(x)}{f(x)}\,dx$, тогда $\nu_P(\eta) = -1$ и $\operatorname{res}_P(\eta) = 1$ для всех точек $P \in \operatorname{supp}(D)$. Таким образом, получаем

$$C_{\mathcal{L}}(D, rQ_\infty)^\perp = C_{\mathcal{L}}(D, D + (\eta) - rQ_\infty).$$

Предложение 1. *Код, двойственный к C_r, имеет вид*

$$C_r^\perp = \bar{a} \star C_{2qm-q-m-1-r},$$

где $(\bar{a})^{-1} = \big((f'(x))(P_{\alpha_1,\beta_1}), \ldots, (f'(x))(P_{\alpha_m,\beta_q})\big) \in (K^*)^N$, *а через* $\star$ *обозначено покоординатное произведение в* K^N.

Доказательство. Имеем

$$\begin{aligned}
&C_r^\perp = C_{\mathcal{L}}(D, D + (\eta) - rQ_\infty) = \\
&= C_{\mathcal{L}}(D, D + (f'(x)) - (f(x)) + (dx) - rQ_\infty) = \\
&= C_{\mathcal{L}}(D, D + (f'(x)) - D + qmQ_\infty + (2g-2)Q_\infty - rQ_\infty) = \\
&= C_{\mathcal{L}}(D, (f'(x)) + (qm + 2g - 2 - r)Q_\infty) = \\
&= \bar{a} \star C_{\mathcal{L}}(D, (2qm - q - m - 1 - r)Q_\infty) = \\
&= \bar{a} \star C_{2qm-q-m-1-r}. \quad ▲
\end{aligned}$$

4.2. Параметры кода C_r. В [9, предложения 3.4, 3.6 и 3.8] были найдены размерность и минимальное расстояние кодов C_r для некоторых определенных значений r. В этом пункте мы повторим эти известные результаты и определим параметры кодов C_r для остальных значений r.

Для параметров геометрических кодов Гоппы $C_{\mathcal{L}}(D', G)$ имеется следующий результат.

Теорема 5 [2, теорема 2.2.2 и следствие 2.2.3]. *Код $C_{\mathcal{L}}(D', G)$ является $[n, k, d]$-кодом с параметрами*

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

Если $\deg(G) < n$, *то* $k = \dim(\mathcal{L}(G))$.

Перейдем к определению параметров кодов C_r.

Рассмотрим множество H порядков полюсов в точке Q_∞ (т.е. полугруппу Вейерштрасса точки Q_∞). Для $b \geqslant 0$ положим

$$H(b) := \{u \in H : \ u \leqslant b\}.$$

Тогда $|H(b)| = \dim(\mathcal{L}(bQ_\infty))$. По лемме 1 имеем

$$H(b) = \{u \leqslant b : \ u = iq + jm, \text{ где } i \geqslant 0 \text{ и } 0 \leqslant j \leqslant q - 1\}.$$

Отсюда

$$|H(b)| = |\{(i, j) \in \mathbb{N}_0 \times \mathbb{N}_0 : \ j \leqslant q - 1 \text{ и } iq + jm \leqslant b\}|.$$

Теорема 6. *Пусть* $0 \leqslant r \leqslant 2qm - q - m - 1$. *Тогда справедливы следующие утверждения*:

1. *Имеет место равенство* $\dim(C_r) = \dim(\mathcal{L}(rQ_\infty)) - \dim(\mathcal{L}((r - qm)Q_\infty))$. *Кроме того*,
   (a) *Для* $0 \leqslant r < qm$ *имеем* $\dim(C_r) = |H(r)|$;
   (b) *Положим* $s := 2qm - q - m - 1 - r$. *Для* $qm \leqslant r \leqslant 2qm - q - m - 1$ *имеем*
   $$\dim(C_r) = qm - |H(s)|;$$
   (c) *Для* $qm - q - m - 1 < r < qm$ *имеем* $\dim(C_r) = r + 1 - \dfrac{(q-1)(m-1)}{2}$.
2. *Минимальное расстояние* $d(C_r)$ *кода* C_r *удовлетворяет неравенству*
   $$d(C_r) \geqslant qm - r.$$
   Если $r = qb$, *где* $0 \leqslant b < m$, *а также если* $r = cm$, *где* $0 \leqslant c < q$, *то* $d(C_r) = qm - r$. *Кроме того, если* $r \geqslant qm - q - m$, *то* C_r *не является МДР-кодом.*

Доказательство. 1. Так как $D \sim qmQ_\infty$, то по теореме 5 имеем

$$\dim(C_r) = \dim(\mathcal{L}(rQ_\infty)) - \dim(\mathcal{L}((r - qm)Q_\infty)),$$

и если $0 \leqslant r < qm$, то $\dim(C_r) = \dim(\mathcal{L}(rQ_\infty)) = |H(r)|$.

Для $qm \leqslant r \leqslant 2qm - q - m - 1$ имеем $0 \leqslant s < qm$. Таким образом, из предложения 1 следует, что

$$\dim C_r = qm - \dim C_r^\perp = qm - \dim C_s = qm - |H(s)|.$$

Если $qm - q - m - 1 < r < qm$ (т.е. $2g - 2 < \deg(rQ_\infty) < N$), то по теореме Римана – Роха имеем

$$\dim(C_r) = \dim(\mathcal{L}(rQ_\infty)) = \deg(rQ_\infty) + 1 - g = r + 1 - \frac{(q-1)(m-1)}{2}.$$

2. Неравенство $d(C_r) \geqslant qm - r$ непосредственно вытекает из теоремы 5. Если $r = qb$, где $0 \leqslant b < m$, выберем b различных элементов из множества $\{\alpha_1, \ldots, \alpha_m\}$. Назовем эти элементы $\gamma_1, \ldots, \gamma_b$. Тогда элемент

$$z_1 := \prod_{j=1}^{b} (x - \gamma_j) \in \mathcal{L}(rQ_\infty)$$

имеет ровно $qb = r$ различных нулей в D. Вес соответствующего слова кода C_r равен $qm - r$. Следовательно, $d(C_r) = qm - r$.

Аналогично, если $r = cm$, где $0 \leqslant c < q$, то выберем c различных элементов из множества $\{\beta_1, \ldots, \beta_q\}$. Назовем их $\tau_1, \ldots, \tau_c$. Тогда элемент

$$z_2 := \prod_{j=1}^{c} (y - \tau_j) \in \mathcal{L}(rQ_\infty)$$

имеет в точности $cm = r$ различных нулей в D. Вес соответствующего слова кода C_r равен $qm - r$. Следовательно, $d(C_r) = qm - r$.

Если $r = qb$ и C_r является МДР-кодом, то из равенства $d(C_r) = qm - \dim(C_r) + 1$ следует $g = 0$, что невозможно. Аналогично для $r = cm$. ▲

В следующей теореме мы определим минимальное расстояние кода C_r для значений $qm \leqslant r \leqslant 2qm - q - m - 1$. Используя идеи из [5] и теорему 2, приходим к следующему результату.

Теорема 7. *Пусть $m > q$. Для $qm \leqslant r \leqslant 2qm - q - m - 1$ имеем $0 \leqslant r^\perp := 2qm - q - m - 1 - r \leqslant qm - q - m - 1$. Пусть $t^\perp \leqslant r^\perp$ – наибольшее целое число, такое что $t^\perp$ является порядком полюса в точке Q_∞, т.е. $t^\perp = aq + bm$, где $0 \leqslant a \leqslant m - 2$ и $0 \leqslant b \leqslant q - 1$. Тогда минимальное расстояние кода C_r имеет вид*

$$d(C_r) = a + 2.$$

Доказательство. Пусть $\boldsymbol{H}$ – проверочная матрица кода C_r. По лемме 1 множество $\{1, x, y, \ldots, x^a, x^{a-1}y, \ldots, y^b\}$ является базисом пространства $\mathcal{L}(t^\perp Q_\infty)$. Выберем элемент $\beta \in K$, такой что $\beta^q + \mu\beta = 0$. Пусть $\boldsymbol{H}_1$ – подматрица матрицы $\boldsymbol{H}$ со столбцами, соответствующими точкам $P_{\alpha_1,\beta}, \ldots, P_{\alpha_{a+2},\beta}$. Используя преобразования строк, представим $\boldsymbol{H}_1$ в следующем виде:

$$\boldsymbol{H}_1 = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_{a+2} \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \ldots & \alpha_{a+2}^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_1^a & \alpha_2^a & \alpha_3^a & \ldots & \alpha_{a+2}^a \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Здесь $\operatorname{rank}(\boldsymbol{H}_1) = a + 1$, и $\boldsymbol{H}_1$ имеет $a + 2$ столбцов, так что столбцы матрицы $\boldsymbol{H}_1$ линейно зависимы. Поэтому $d(C_r) \leqslant a + 2$.

С другой стороны, выберем любые $a + 1$ различных столбцов из $\boldsymbol{H}$. Назовем эту матрицу $\boldsymbol{H}_2$. Поскольку каждый столбец матрицы $\boldsymbol{H}$ соответствует точке $P_{\alpha,\beta}$ степени 1, переупорядочим столбцы матрицы $\boldsymbol{H}_2$ в соответствии со значениями α

следующим образом:

$$\begin{array}{llll} P_{\alpha_1,\beta_{1,1}}, & P_{\alpha_1,\beta_{1,2}}, & \ldots, & P_{\alpha_1,\beta_{1,w_1}} \\ P_{\alpha_2,\beta_{2,1}}, & P_{\alpha_2,\beta_{2,2}}, & \ldots, & P_{\alpha_1,\beta_{2,w_2}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\ P_{\alpha_\gamma,\beta_{\gamma,1}} & P_{\alpha_\gamma,\beta_{\gamma,2}} & \ldots, & P_{\alpha_\gamma,\beta_{\gamma,w_\gamma}}, \end{array}$$

где α_i попарно различны, $w_1+w_2+\ldots+w_\gamma = a+1$, причем $w_1 \geqslant w_2 \geqslant \ldots \geqslant w_\gamma \geqslant 1$. Для $0 \leqslant j_i \leqslant w_i - 1$, $1 \leqslant i \leqslant \gamma$, элемент $x^{i-1}y^{j_i}$ принадлежит базису $\mathcal{L}(t^\perp Q_\infty)$. Перепишем эти базисные элементы в виде

$$\begin{array}{lllll} 1, & y, & y^2, & \ldots, & y^{w_1-1} \\ x, & xy, & xy^2, & \ldots, & xy^{w_2-1} \\ x^2, & x^2y, & x^2y^2, & \ldots, & x^2y^{w_3-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ x^{\gamma-1}, & x^{\gamma-1}y, & x^{\gamma-1}y^2, & \ldots, & x^{\gamma-1}y^{w_\gamma-1}. \end{array}$$

Теперь выделим из $\boldsymbol{H}_2$ подматрицу $\boldsymbol{H'}$ размера $(a+1)\times(a+1)$ таким образом, чтобы каждая строка соответствовала вышеуказанным функциям в заданном порядке. Иначе говоря, $\boldsymbol{H'} = [\boldsymbol{H'}_{i,j}]$, $i,j = 1,2,\ldots,\gamma$, где матрица $\boldsymbol{H'}_{i,j}$ размера $w_i \times w_j$ имеет вид $\boldsymbol{H'}_{i,j} = \alpha_j^{i-1}\boldsymbol{B}_{i,j}$, где

$$\boldsymbol{B}_{i,j} = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \beta_{j,1} & \beta_{j,2} & \beta_{j,3} & \ldots & \beta_{j,w_j} \\ \beta_{j,1}^2 & \beta_{j,2}^2 & \beta_{j,3}^2 & \ldots & \beta_{j,w_j}^2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ \beta_{j,1}^{w_i-1} & \beta_{j,2}^{w_i-1} & \beta_{j,3}^{w_i-1} & \ldots & \beta_{j,w_j}^{w_i-1} \end{bmatrix}.$$

Тогда согласно [5, леммы 2 и 3] имеем

$$\det(\boldsymbol{H'}) = \left(\prod_{i=1}^{\gamma}\det(\boldsymbol{B}_{i,i})\right)\left(\prod_{j=2}^{\gamma}\rho_j^{w_j}\right),$$

где

$$\rho_j = \prod_{i=1}^{j-1}(\alpha_j - \alpha_i), \quad j = 2,3,\ldots,\gamma,$$

и любые $a+1$ столбцов матрицы $\boldsymbol{H}$ линейно независимы над K. Следовательно, $d(C_r) \geqslant a+2$. ▲

§ 5. Обобщенные веса Хэмминга кода C_r

В [9, предложения 3.7, 3.8] были получены границы на обобщенные веса Хэмминга кодов C_r с помощью понятий гональности и порядковых границ. Но в общем случае вычисление гональности является трудной задачей. В этом параграфе мы установим точные значения обобщенных весов Хэмминга, в частности, второго обобщенного веса Хэмминга кода C_r в нескольких случаях.

Следуя идеям из [17], получаем следующее утверждение.

Лемма 4. *Пусть $r \leqslant qm$ – порядок полюса в точке Q_∞. Тогда $r = iq + jm$, где $i \geqslant 0$ и $0 \leqslant j \leqslant q-1$. Если либо $i = 0$, либо $j = 0$, то существует дивизор $0 \leqslant D' \leqslant D$, такой что $rQ_\infty \sim D'$.*

Доказательство. Для $i = 0$ и $j = 0$ подходит дивизор $D' = 0$. Далее, если $i = 0$ и $j \neq 0$, то $r = jm$. Выберем j элементов из $\beta_1, \ldots, \beta_q$ и обозначим их через $\tau_1, \ldots, \tau_j$. Положим

$$z := \prod_{t=1}^{j} (y - \tau_t).$$

Тогда $(z) = D' - rQ_\infty$, откуда $D' \sim rQ_\infty$. Для случая $j = 0$ и $i \neq 0$ доказательство аналогично. ▲

Определение 4. Будем говорить, что натуральное число $r \leqslant qm$ обладает свойством $(*)$, если r является порядком полюса в точке Q_∞, $r = iq + jm$ для $i \geqslant 0$, $0 \leqslant j \leqslant q - 1$ и либо $i = 0$, либо $j = 0$.

Теорема 8. *Если для* $1 \leqslant \ell \leqslant \dim(C_r)$ *хотя бы одно из чисел* $r - p_\ell$ *и* $qm - r + p_\ell$ *обладает свойством* $(*)$, *то*

$$d_\ell(C_r) \leqslant qm - r + p_\ell.$$

Доказательство. Если $r - p_\ell$ обладает свойством $(*)$, то по лемме 4 существует дивизор D', такой что $0 \leqslant D' \leqslant D$ и $(r - p_\ell)Q_\infty \sim D'$. Таким образом,

$$\dim(\mathcal{L}(rQ_\infty - D')) = \dim(\mathcal{L}(p_\ell Q_\infty)) = \ell.$$

Тогда из теоремы 3 следует, что

$$d_\ell(C_r) \leqslant qm - r + p_\ell.$$

Если же $qm - r + p_\ell$ обладает свойством $(*)$, то снова найдется дивизор D'', такой что $0 \leqslant D'' \leqslant D$ и $(qm - r + p_\ell)Q_\infty \sim D''$. При этом $qmQ_\infty \sim D$, откуда $D - rQ_\infty + p_\ell Q_\infty \sim D''$. Поэтому $D' := D - D'' \sim (r - p_\ell)Q_\infty$. Следовательно,

$$d_\ell(C_r) \leqslant qm - r + p_\ell. \quad ▲$$

Из теоремы 8 немедленно вытекает

Следствие 1. *Если для* $1 \leqslant r < qm$ *хотя бы одно из чисел* r *и* $qm - r$ *обладает свойством* $(*)$, *то код* C_r *имеет минимальное расстояние* $d(C_r) = qm - r$.

Замечание 2. Для $k = \dim(C_r)$ справедливо $d_k(C_r) = qm$.

По лемме 2 полугруппа Вейерштрасса $H = \langle q, m \rangle$ точки Q_∞ является числовой полугруппой с размерностью вложения 2. Таким образом, из теоремы 4 получаем следующие результаты о втором обобщенном весе Хэмминга кода C_r.

Теорема 9. *Пусть* $m > q$. *Для* $r < qm$ *справедливо неравенство*

$$d_2(C_r) \geqslant qm - r + q.$$

Теорема 10. *Пусть* $m > q$. *Если для* $r < qm - 1$ *хотя бы одно из чисел* $r - q$ *и* $qm - r + q$ *обладает свойством* $(*)$, *то*

$$d_2(C_r) = qm - r + q.$$

Доказательство. Применяя теорему 8, получаем $d_2(C_r) \leqslant qm - r + q$.

С другой стороны, так как $\rho_2 = q$ и код, двойственный к C_r, образует кодовый массив (подробнее см. в [19]), то из теоремы 4 и предложения 1 получаем

$$d_2(C_r) = d_2(C^\perp_{2qm-q-m-1-r}) \geqslant \delta_{\mathrm{FR}}(2qm - q - m - r) + q.$$

Так как $r < qm$, то $2qm - q - m - r \geqslant 2g = qm - q - m + 1$, и поэтому

$$d_2(C_r) \geqslant \delta_{\mathrm{FR}}(2qm - q - m - r) + q \geqslant$$
$$\geqslant 2qm - q - m - r + 1 - (qm - q - m + 1) + q = qm - r + q,$$

что и требовалось. ▲

Теорему 10 можно обобщить на все значения ℓ, $1 \leqslant \ell \leqslant \dim(C_r)$.

Теорема 11. *Для $r < qm - 1$ и $1 \leqslant \ell \leqslant \dim(C_r)$, если хотя бы одно из чисел $r - p_\ell$ и $qm - r + p_\ell$ обладает свойством $(*)$, то*

$$d_\ell(C_r) = qm - r + p_\ell.$$

Доказательство. По теореме 8 имеем

$$d_\ell(C_r) \leqslant qm - r + p_\ell.$$

Обратное неравенство следует из доказательства теоремы 10. ▲

Следующий результат был доказан в [17].

Теорема 12 [17, предложение 4]. *Пусть $C_{\mathcal{L}}(D', G)$ – код размерности k с обильностью $\dim(\mathcal{L}(G - D')) =: a \geqslant 0$. Если существует точка Q степени 1, не входящая в D', и $C_{\mathcal{L}}(D', G - p_{\ell+a}Q) \neq \{0\}$, где p_ℓ – ℓ-й порядок полюса в точке Q, то для любого ℓ, $1 \leqslant \ell \leqslant k$,*

$$d_\ell(C_{\mathcal{L}}(D', G)) \leqslant d_1(C_{\mathcal{L}}(D', G - p_{\ell+a}Q)).$$

Применяя теоремы 9 и 12, получаем следующий результат.

Теорема 13. *Пусть $m > q$. Для $r < qm$, если числа $r - q$ и $qm - r + q$ не обладают свойством $(*)$, то*

$$qm - r + q \leqslant d_2(C_r) \leqslant qm - \overline{(r - q)},$$

где $\overline{(r-q)}$ – наибольший порядок полюса, меньший или равный $(r-q)$ и обладающий свойством $(*)$.

Теорема 14. *Для $1 \leqslant \ell \leqslant \dim C_r$ и $r < qm$, если числа $r - p_\ell$ и $qm - r + p_\ell$ не обладают свойством $(*)$, то*

$$d_\ell(C_r) \leqslant qm - \overline{(r - p_\ell)},$$

где $\overline{(r-p_\ell)}$ – наибольший порядок полюса, меньший или равный $(r - p_\ell)$ и обладающий свойством $(*)$.

Теперь перейдем к вычислению второго обобщенного веса Хэмминга кода C_r в случае $qm \leqslant r$. В доказательствах будем использовать следующий результат из [17].

Теорема 15 [17, предложение 6]. *Пусть $C = C_{\mathcal{L}}(D', G)$ – код размерности k, и пусть $\dim(\mathcal{L}(G - D')) =: a > 0$. Тогда для $1 \leqslant \ell \leqslant k$ справедливо неравенство $d_\ell(C) \leqslant \deg(D'')$ для любого эффективного дивизора $D'' \leqslant D$, такого что $\dim(\mathcal{L}(D'')) > \ell$.*

Теорема 16. *Пусть $m > q$. Если $qm \leqslant r \leqslant 2qm - q - m - 1$, то*

$$d_2(C_r) \leqslant \min\{2q, m\}.$$

Доказательство. Так как $p_3 = \min\{2q, m\}$, то по лемме 4 существует дивизор D', такой что $0 \leqslant D' \leqslant D$ и $p_3 Q_\infty \sim D'$. Тогда $\dim(\mathcal{L}(D')) = \dim(\mathcal{L}(p_3 Q_\infty)) = 3$. Отсюда $d_2(C_r) \leqslant \deg D' = p_3 = \min\{2q, m\}$. ▲

Теорема 17. *Пусть* $m > 2q$, *и пусть* $qm \leqslant r \leqslant 2qm - q - m - 1$. *Тогда* $0 \leqslant r^{\perp} := 2qm - q - m - 1 - r \leqslant qm - q - m - 1$. *Пусть* $t^{\perp} \leqslant r^{\perp}$ – *наибольшее целое число, такое что* $t^{\perp}$ *является порядком полюса в точке* Q_{∞}, *т.е.* $t^{\perp} = aq + bm$, *где* $0 \leqslant a \leqslant m - 3$ *и* $0 \leqslant b \leqslant q - 1$. *Тогда*

$$d_2(C_r) = a + 3.$$

Доказательство. Пусть $\boldsymbol{H}$ – проверочная матрица кода C_r над полем K. Выберем элемент $\beta \in K$, такой что $\beta^q + \mu\beta = 0$. Множество $\{1, x, y, \ldots, x^a, x^{a-1}y, \ldots, y^b\}$ является базисом пространства $\mathcal{L}(t^{\perp}Q_{\infty})$. Пусть $\boldsymbol{H}_1$ – подматрица матрицы $\boldsymbol{H}$ со столбцами, соответствующими точкам $P_{\alpha_1,\beta}, \ldots, P_{\alpha_{a+3},\beta}$ (это возможно, так как $a + 3 \leqslant m$). Применяя преобразования строк, приведем $\boldsymbol{H}_1$ к следующему виду:

$$\boldsymbol{H}_1 = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_{a+3} \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \ldots & \alpha_{a+3}^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_1^a & \alpha_2^a & \alpha_3^a & \ldots & \alpha_{a+3}^a \\ 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Здесь $\operatorname{rank}(\boldsymbol{H}_1) = a + 1$, и $\boldsymbol{H}_1$ имеет $a + 3$ столбцов. Поэтому по теореме 2 имеем $d_2(C_r) \leqslant a + 3$.

С другой стороны, из теоремы 1 имеем $d_2(C_r) \geqslant d_1(C_r) + 1 = (a + 2) + 1 = a + 3$, что завершает доказательство. ▲

Пример 1. Для $p = 2$ и $K = \mathbb{F}_4$ рассмотрим функциональное поле $F = K(x, y)$, заданное уравнением

$$y^2 + \omega y = x(x - 1)(x - \omega),$$

где ω – примитивный элемент поля K. Здесь $q = 2$, $m = 3$ и род $g = 1$. Список значений длины, размерности, минимального расстояния и второго обобщенного веса Хэмминга кода C_r приведен в следующей таблице:

r	N	$\dim(C_r)$	$d(C_r)$	$d_2(C_r)$
1	6	1	6	–
2	6	2	4	6
3	6	3	3	$\geqslant 5$ и $\leqslant 6$
4	6	4	2	4
5	6	5	$\geqslant 1$	3
6	6	5	2	$\leqslant 4$

§ 6. Условия квазисамодвойственности и самодвойственности кодов

Линейный код C называется самодвойственным, если $C = C^{\perp}$, где $C^{\perp}$ – код, двойственный к C относительно евклидова скалярного произведения на $\mathbb{F}_{p^s}^n$. Самодвойственные коды образуют важный класс линейных кодов. В этом параграфе приводится простой критерий самодвойственности геометрических кодов Гоппы на F/K.

Имеется следующий результат, доказанный в [22]. Но прежде чем сформулировать его, введем следующее определение для произвольного алгебраического функционального поля F'/K' рода g'.

Определение 5 [22, определение 2.15]. Выберем n точек $P_1, \ldots, P_n$ степени 1 поля F' и положим $D' := P_1 + \ldots + P_n$. Два дивизора G и H называются эквивалентными относительно D', если существует элемент $u \in F'$, такой что $H = G + (u)$ и $u(P_i) = 1$ для всех $i = 1, \ldots, n$.

Предложение 2 [22, следствие 4.15]. *Пусть $n > 2g' + 2$. Пусть G и H – два дивизора одинаковой степени m' в F'. Если $C_{\mathcal{L}}(D', G)$ не равно ни 0, ни $(K')^n$ и при этом $2g' - 1 < m' < n - 1$, то $C_{\mathcal{L}}(D', G) = C_{\mathcal{L}}(D', H)$ тогда и только тогда, когда G и H эквивалентны относительно D'.*

Теорема 18. *Если $qm - q - m + 1 \leqslant r \leqslant qm - 2$, то код C_r квазисамодвойствен тогда и только тогда, когда $r = (2qm - q - m - 1)/2$.*

Доказательство. Если $qm - q - m + 1 \leqslant r \leqslant qm - 2$, то по предложению 2 код C_r квазисамодвойствен тогда и только тогда, когда $r = (2qm - q - m - 1)/2$. ▲

Пусть G – дивизор поля F, такой что $\deg(G) = \dfrac{2qm - q - m - 1}{2}$. Очевидно, что $qm > qm - q - m + 3$ и $qm - q - m < \deg(G) < qm - 1$. Положим $H := D + (\eta) - G$, где D – такой дивизор, как в § 4. Тогда $\deg(G) = \deg(H)$. Условие самодвойственности кода $C_{\mathcal{L}}(D, G)$ дает следующая

Теорема 19. *Код $C_{\mathcal{L}}(D, G)$ самодвойствен тогда и только тогда, когда дивизор $2G$ эквивалентен $(f'(x)) + (2qm - q - m - 1)Q_\infty$ относительно D.*

Доказательство. По предложению 2

$$
\begin{aligned}
&C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D, D + (\eta) - G) \Leftrightarrow \\
&\Leftrightarrow G = D + (\eta) - G + (u) \text{ для некоторого } u \in F, \text{ такого что } u(P) = 1 \\
&\quad \text{для каждой точки } P \in \operatorname{supp}(D) \Leftrightarrow \\
&\Leftrightarrow (u) + (\eta) = 2G - D \Leftrightarrow \\
&\Leftrightarrow (u) + (f'(x)) + (dx) - (f(x)) = 2G - D \Leftrightarrow \\
&\Leftrightarrow (u) + (f'(x)) + [(q-1)(m-1) - 2]Q_\infty - D + qmQ_\infty = 2G - D \Leftrightarrow \\
&\Leftrightarrow (f'(x)) = 2G - (2qm - q - m - 1)Q_\infty - (u). \quad ▲
\end{aligned}
$$

Пример 2. Пусть $p = 2$ и $K = \mathbb{F}_4$. Пусть ω – примитивный элемент поля $\mathbb{F}_4$. Рассмотрим поле $F = K(x, y)$, где

$$y^2 + y = x(x - 1)(x - \omega).$$

Тогда все корни многочлена $T^2 + T$ лежат в K. Расширение F/K имеет род $g = 1$. Положим

$$f(x) := x(x - 1)(x - \omega).$$

Пусть P_0, P_1 и P_ω – нули элементов x, $(x - 1)$ и $(x - \omega)$ в $K(x)$ соответственно. Тогда каждая из точек P_0, P_1 и P_ω имеет ровно два прообраза в F. Аналогично, нуль функции $(x - \omega^2)$, который мы обозначим через P_{ω^2}, имеет два прообраза в F, скажем, Q_1 и Q_2. Положим $D := (f(x))_0$, и пусть G – дивизор поля F, эквивалентный $Q_1 + Q_2 + Q_\infty$ относительно D. Тогда код $C_{\mathcal{L}}(D, G)$ самодвойствен. И наоборот, если $C_{\mathcal{L}}(D, G)$ – самодвойственный код, то дивизор $2G$ эквивалентен $2(Q_1 + Q_2 + Q_\infty)$ относительно D.

§ 7. Квантовые коды по одноточечным геометрическим кодам Гоппы на $F/\mathbb{F}_{p^s}$

В этом параграфе строятся квантовые коды на основе одноточечных геометрических кодов Гоппы на $F/\mathbb{F}_{p^s}$. Вначале дадим краткое введение в квантовые коды.

Пусть q_0 – степень простого числа. Через $V_n := (\mathbb{C}^{q_0})^{\otimes n}$ обозначим n-ю тензорную степень q_0-мерного гильбертова пространства $\mathbb{C}^{q_0}$. Квантовым $[[n,k,d]]_{q_0}$-кодом называется q_0^k-мерное векторное подпространство пространства V_n с минимальным расстоянием d. Связь между квантовыми кодами и классическими линейными кодами была установлена в работе [23], после которой было построено много классов квантовых кодов на основе классических кодов, исправляющих ошибки.

Граница Синглтона для квантовых кодов утверждает, что для всякого квантового $[[n,k,d]]_{q_0}$-кода справедливо неравенство $2d \leqslant n-k+2$. Квантовый дефект Синглтона определяется как $\delta^Q := n-k-2d+2 \geqslant 0$, а относительным квантовым дефектом Синглтона называется $\Delta^Q := \delta^Q/n$. Если $\delta^Q = 0$, то код называется квантовым МДС-кодом.

Следующая лемма описывает конструкцию квантовых кодов по классическим линейным кодам.

Лемма 5 [24, лемма 17(a)]. *Пусть C_1 и C_2 – два линейных кода с параметрами $[n,k_i,d_i]_{q_0}$, $i=1,2$, и пусть $C_1 \subset C_2$. Тогда существует $[[n,k_2-k_1,d]]_{q_0}$-код с расстоянием $d = \min\{\mathrm{wt}(c) :\ c \in (C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}$, где $\mathrm{wt}(c)$ – вес слова c.*

Применим лемму 5 для получения квантовых кодов по одноточечным геометрическим кодам Гоппы, построенным в § 4.

Предложение 3. *Пусть m и q $(= p^{k'})$ такие, как в § 3. Пусть a,b – натуральные числа, такие что $qm-q-m-1 < a < b < qm$. Тогда существует $[[qm, b-a, d]]_{p^s}$-код с расстоянием $d \geqslant \min\{qm-b, a-qm+q+m+1\}$.*

Кроме того, если $m = q+x$ для некоторого $x \in \mathbb{N}$ и при этом $a = cq$ для некоторого натурального c, так что $qm-b \leqslant a-qm+q+m+1$, то относительный квантовый дефект Синглтона $\Delta^Q_{k'}$ получаемых квантовых кодов удовлетворяет условию

$$\lim_{k'\to\infty} \Delta^Q_{k'} = 0.$$

Доказательство. Пусть $C_1 := C_a$ и $C_2 := C_b$ такие, как в § 4. Тогда код C_1 имеет параметры $[qm,\ a+1-\dfrac{(q-1)(m-1)}{2},\ d_1 \geqslant qm-a]_{p^s}$, а C_2 – параметры $[qm,\ b+1-\dfrac{(q-1)(m-1)}{2},\ d_2 \geqslant qm-b]_{p^s}$. При этом $C_1 \subset C_2$. Тогда из леммы 5 следует, что существует $[[qm, b-a, d]]_{p^s}$-код с расстоянием $d \geqslant \min\{qm-b, a-qm+q+m+1\}$.

Далее, если $m = q+x$ и $a = cq$ таковы, что $qm-b \leqslant a-qm+q+m+1$, то

$$\Delta^Q_{k'} = \frac{qm-b+a-2d+2}{qm} \leqslant \frac{qm-b+a-2qm+2b+2}{qm} \leqslant$$

$$\leqslant \frac{a+1}{qm} = \frac{cq+1}{q(q+x)} = \frac{cp^{k'}+1}{p^{k'}(p^{k'}+x)} \to 0 \quad \text{при } k' \to \infty. \quad \blacktriangle$$

Пример 3. Пусть $K = \mathbb{F}_4$, $q=2$, $m=3$, $a=2$ и $b=4$. Тогда a и b удовлетворяют условиям предложения 3, и получаем $[[6,2,\geqslant 2]]_4$-код с наилучшими параметрами согласно таблице в [25]. Аналогично получаются квантовые коды с параметрами $[[6,4,\geqslant 1]]_4$, $[[10,4,\geqslant 2]]_8$, $[[12,4,\geqslant 2]]_9$, $[[14,6,\geqslant 2]]_{16}$ и т.д.

§ 8. Сверточные коды по одноточечным геометрическим кодам Гоппы на $F/\mathbb{F}_{p^s}$

Рассмотрим кольцо многочленов $R = \mathbb{F}_{q_0}[X]$. Сверточным кодом C называется R-подмодуль ранга k модуля R^n. Пусть $G(X) = (g_{ij}(X)) \in (\mathbb{F}_{q_0}[X])^{k\times n}$ – порождающая матрица кода C над $\mathbb{F}_{q_0}[X]$, $\gamma_i = \max\{\deg g_{ij}(X) :\ 1 \leqslant j \leqslant n\}$, $\gamma = \sum\limits_{i=1}^{k} \gamma_i$,

$m' = \max\{\gamma_i : 1 \leqslant i \leqslant k\}$, и пусть d_f – минимальный вес элемента $c \in C$. Тогда говорят, что C имеет длину n, размерность k, степень γ, память m' и свободное расстояние d_f. Если $m' = 1$, то C называется сверточным кодом с единичной памятью и обозначается через $(n, k, \gamma; 1, d_f)_{q_0}$.

Следующая теорема описывает метод построения сверточных кодов по геометрическим кодам Гоппы.

Лемма 6 [26, теорема 3]. *Пусть $F'/\mathbb{F}_{q_0}$ – функциональное поле рода g'. Рассмотрим код $C_\Omega(D', G)$, такой что $2g' - 2 < \deg(G) < n$, где $\deg(G)$ – степень дивизора G. Тогда существует сверточный код с единичной памятью с параметрами $(n, k - \ell, \ell; 1, d_f \geqslant d)_{q_0}$, где $\ell \leqslant k/2$, $k = \deg(G) + 1 - g'$ и $d \geqslant n - \deg(G)$.*

В следующем предложении с помощью леммы 6 строятся сверточные коды с единичной памятью по одноточечным геометрическим кодам Гоппы на $F/\mathbb{F}_{p^s}$. Длина получаемых таким образом сверточных кодов равна qm, где $q = p^{k'}$ и $\text{НОД}(m, q) = 1$ (так что $\max\{q, m\} < p^s$), отличаясь тем самым от кодов из [27].

Предложение 4. *Пусть $qm - q - m - 1 < r < qm$, где r обладает свойством $(*)$ (определение 4). Тогда существует сверточный код с единичной памятью с параметрами $(qm, r + 1 - g - a, a; 1, d_f \geqslant d)_{p^s}$, где $g = (q-1)(m-1)/2$, $a \leqslant (r+1-g)/2$ и $d = qm - r$.*

Доказательство. Рассмотрим код $C_\Omega(D, rQ_\infty)$ на $F/\mathbb{F}_{p^s}$ с дивизором D таким, как в § 4. Поскольку $qm - q - m - 1 < r < qm$, по лемме 6 получаем сверточный код с единичной памятью с параметрами $(qm, r + 1 - g - a, a; 1, d_f \geqslant d)_{p^s}$, где $g = (q-1)(m-1)/2$, $a \leqslant (r+1-g)/2$. Так как r обладает свойством $(*)$, то $d = qm - r$ согласно следствию 1. ▲

Пример 4. Пусть $K = \mathbb{F}_4$, $q = 2$, $m = 3$ и $r = 4$. Тогда получаем сверточный код с единичной памятью с параметрами $(6, 3, 1; 1, \geqslant 2)_4$. Аналогично получаются сверточные коды с единичной памятью с параметрами $(10, 3, 2; 1, \geqslant 4)_8$, $(14, 6, 2; 1, \geqslant 4)_{16}$ и т.д.

§ 9. Локально восстанавливаемые коды на $F/\mathbb{F}_{p^s}$

Код $C \subset \mathbb{F}_{q_0}^n$ называется локально восстанавливаемым (LRC-кодом) с локальностью r_0, если для любого $i \in [n] := \{1, 2, \ldots, n\}$ существует подмножество $A_i \subset [n] \setminus \{i\}$, $|A_i| \leqslant r_0$, и функция φ_i, такие что для любого кодового слова $x \in C$ выполнено $x_i = \varphi_i(\{x_j,\ j \in A_i\})$. LRC-код C длины n, мощности q_0^k и локальности r_0 обозначается через (n, k, r_0). Минимальное расстояние (n, k, r_0)-LRC-кода удовлетворяет неравенству

$$d \leqslant n - k - \left\lceil \frac{k}{r_0} \right\rceil + 2. \tag{2}$$

Коды, лежащие на границе (2), называются оптимальными LRC-кодами. Скорость (n, k, r_0)-LRC-кода удовлетворяет неравенству

$$\frac{k}{n} \leqslant \frac{r_0}{r_0 + 1}. \tag{3}$$

В [28] были построены LRC-коды на алгебраических кривых. Опишем вкратце эту конструкцию; подробнее см. в [28]. Пусть $F_X/\mathbb{F}_{q_0}$ и $F_Y/\mathbb{F}_{q_0}$ – функциональные поля. Пусть $\psi\colon X \to Y$ – рациональное сепарабельное отображение степени $r_0 + 1$ гладких проективных абсолютно неприводимых кривых X и Y, соответствующих полям F_X и F_Y соответственно. Пусть $\psi^*\colon F_Y \to F_X$ – соответствующее отображение функциональных полей. Поскольку ψ сепарабельно, по теореме о примитивном

элементе существует функция $y \in F_X$, такая что $F_X = F_Y(y)$. Эту функцию y можно рассматривать как отображение $y\colon X \to \mathbb{P}^1$, и его степень $\deg(y)$ обозначим через h. Пусть $S = \{P_1, \dots, P_{s_0}\}$ – множество точек степени 1 поля F_Y, а A – положительный дивизор степени $\ell \geqslant 1$, носитель которого не пересекается с S. Для каждого j пусть $\{P_{ij}\}$ – множество точек поля F_X, лежащих над P_j. Будем предполагать, что каждая P_j полностью распадается в F_X. Пусть $\{f_1, \dots, f_{m_0}\}$ – базис линейного пространства $\mathcal{L}(A)$. Пусть V – подпространство F_X размерности $r_0 m_0$, порожденное функциями $\{f_j y^i,\ i = 0, \dots, r_0 - 1,\ j = 1, \dots, m_0\}$. Тогда код $C(A, \psi)$ определяется как образ отображения

$$e\colon V \to \mathbb{F}_{q_0}^{(r_0+1)s_0}, \quad F \mapsto (F(P_{ij}),\ i = 0, \dots, r_0,\ j = 1, \dots, s_0).$$

Теорема 20 [28, теорема 3.1]. *Подпространство $C(A, \psi) \subseteq \mathbb{F}_{q_0}^{(r_0+1)s_0}$ образует линейный (n, k, r_0)-LRC-код с параметрами*

$$n = (r_0 + 1)s_0,$$
$$k = r_0 m_0 \geqslant r_0(\ell - g_Y + 1),$$
$$d \geqslant n - (r_0 + 1)\ell - (r_0 - 1)h$$

при условии, что правая часть неравенства для d является натуральным числом.

В следующем предложении с помощью теоремы 20 строятся локально восстанавливаемые коды.

Предложение 5. *Пусть q, m, $F_X := F$, $F_Y := \mathbb{F}_{p^s}(x)$ и $\psi := \varphi$ такие, как в §3. Положим $S := \{P_{\alpha_1}, \dots, P_{\alpha_m}\}$ и $A := \ell P_\infty$, $\ell \in \mathbb{N}$, и пусть P_∞ – бесконечная точка поля F_Y. Если $2m - \ell q$ – натуральное число, то существует линейный (n, k, r_0)-LRC-код $C(A, \psi)$ с параметрами*

$$n = qm, \quad k \geqslant (q-1)(\ell+1) \quad \text{и} \quad d \geqslant 2m - \ell q.$$

Если $q = 2$, то этот код оптимален с локальностью $r_0 = 1$.

Доказательство. В предыдущих обозначениях имеем $h := m$, $s_0 := m$, $r_0 := q - 1$, $n := qm$ и $g_Y = 0$. Таким образом, по теореме 20 получаем линейный (n, k, r_0)-LRC-код $C(A, \psi)$ с параметрами $n = qm$, $k \geqslant (q-1)(\ell+1)$ и $d \geqslant 2m - \ell q$. При этом

$$d + k + \frac{k}{r_0} \geqslant 2m - \ell q + q(\ell + 1) = n + 2 - (m-1)(q-2).$$

Поэтому при $q = 2$ получаем оптимальный локально восстанавливаемый код с локальностью $r_0 = 1$. ▲

Пример 5. Пусть $K = \mathbb{F}_9$, $q = 3$, $m = 4$ и $\ell = 2$. Тогда получаем локально восстанавливаемый $(12, \geqslant 6, 2)$-код с минимальным расстоянием $d \geqslant 2$. Тогда $d + k + \left\lceil \dfrac{k}{r_0} \right\rceil \geqslant 11$, в то время как для кода, лежащего на границе (2), должно быть $d + k + \left\lceil \dfrac{k}{r_0} \right\rceil = 13$. Поэтому этот локально восстанавливаемый код не оптимален, но разница невелика.

Аналогично получается LRC-код с параметрами $(15, \geqslant 6, 2)$ и минимальным расстоянием $d \geqslant 4$. В этом случае разница с (2) также невелика.

Следствие 2. *Пусть выполнены все условия предложения 5. Если $\ell \geqslant m - 1$, то существует линейный (n, k, r_0)-LRC-код $C(A, \psi)$ с параметрами*

$$n = qm, \quad k \geqslant (q-1)(\ell+1) \quad \text{и} \quad d \geqslant 2m - \ell q.$$

Параметры этого кода лежат на границе (3).

Доказательство. Первое утверждение вытекает из предложения 5. Далее, из (3) получаем

$$\frac{(q-1)}{q} \geqslant \frac{k}{n} \geqslant \frac{(q-1)(\ell+1)}{qm} \geqslant \frac{(q-1)}{q}.$$

Таким образом, полученные коды имеют наибольшую возможную скорость. ▲

§ 10. Заключение

В статье определены одноточечные геометрические коды Гоппы по элементарным абелевым p-расширениям поля $\mathbb{F}_{p^s}(x)$ и вычислены их размерность и точное минимальное расстояние в нескольких случаях. Приведен список точных значений второго обобщенного веса Хэмминга этих кодов в нескольких случаях. Также приведены простые критерии квазисамодвойственности одноточечных геометрических кодов Гоппы и самодвойственности геометрических кодов Гоппы с дивизором G (не обязательно одноточечных). Получены семейства квантовых и сверточных кодов по построенным одноточечным геометрическим кодам Гоппы. Получены также локально восстанавливаемые коды на $F/\mathbb{F}_{p^s}$. Было бы интересно вычислить высшие обобщенные веса Хэмминга этих кодов и других классов слабых замковых кодов.

Авторы выражают глубокую благодарность рецензенту за замечания и предложения, позволившие значительно улучшить качество изложения.

СПИСОК ЛИТЕРАТУРЫ

1. *Гоппа В.Д.* Коды, ассоциированные с дивизорами // Пробл. передачи информ. 1977. Т. 13. № 1. С. 33–39.
2. *Stichtenoth H.* Algebraic Function Fields and Codes. Berlin: Springer-Verlag, 2009.
3. *Stichtenoth H.* A Note on Hermitian Codes over GF(q^2) // IEEE Trans. Inform. Theory. 1988. V. 34. № 5. Part 2. P. 1345–1348.
4. *Tiersma H.J.* Remarks on Codes from Hermitian Curves // IEEE Trans. Inform. Theory. 1987. V. 33. № 4. P. 605–609.
5. *Yang K., Kumar P.V.* On the True Minimum Distance of Hermitian Codes // Coding Theory and Algebraic Geometry (Proc. Int. Workshop held in Luminy, France, June 17–21, 1991). Lect. Notes Math. V. 1518. Berlin: Springer, 1992. P. 99–107.
6. *Garzón Rojas Á., Teherán Herrera A.* Elementary Abelian p-Extensions and Curves with Many Points // Rev. Acad. Colombiana Cienc. Exact. Fís. Natur. 2012. V. 36. № 139. P. 243–252.
7. *García A., Stichtenoth H.* Elementary Abelian p-Extensions of Algebraic Function Fields // Manuscripta Math. 1991. V. 72. № 1. P. 67–79.
8. *Johnsen T., Manshadi S., Monzavi N.* A Determination of the Parameters of a Large Class of Goppa Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 5. P. 1678–1681.
9. *Munuera C., Sepúlveda A., Torres F.* Castle Curves and Codes // Adv. Math. Commun. 2009. V. 3. № 4. P. 399–408.
10. *Olaya-León W., Munuera C.* On the Minimum Distance of Castle Codes // Finite Fields Appl. 2013. V. 20. P. 55–63.
11. *Olaya-León W., Granados-Pinzón C.* The Second Generalized Hamming Weight of Certain Castle Codes // Des. Codes Cryptogr. 2015. V. 76. № 1. P. 81–87.
12. *Munuera C., Tenório W., Torres F.* Quantum Error-Correcting Codes from Algebraic Geometry Codes of Castle Type // Quantum Inf. Process. 2016. V. 15. № 10. P. 4071–4088.
13. *Hernando F., McGuire G., Monserrat F., Moyano-Fernández J.J.* Quantum Codes from a New Construction of Self-orthogonal Algebraic Geometry Codes // Quantum Inf. Process. 2020. V. 19. № 4. Paper No. 117 (25 pp.).

14. *Helleseth T., Kløve T., Mykkeltveit J.* The Weight Distribution of Irreducible Cyclic Codes with Block Length $n_1((q^l-1)/N)$ // Discrete Math. 1977. V. 18. № 2. P. 179–211.
15. *Kløve T.* The Weight Distribution of Linear Codes over $GF(q^l)$ Having Generator Matrix over $GF(q)$ // Discrete Math. 1978. V. 23. № 2. P. 159–168.
16. *Wei V.K.* Generalized Hamming Weights for Linear Codes // IEEE Trans. Inform. Theory. 1991. V. 37. № 5. P. 1412–1418.
17. *Munuera C.* On the Generalized Hamming Weights of Geometric Goppa Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 6. P. 2092–2099.
18. *Delgado M., Farrán J.I., García-Sánchez P.A., Llena D.* On the Weight Hierarchy of Codes Coming from Semigroups with Two Generators // IEEE Trans. Inform. Theory. 2014. V. 60. № 1. P. 282–295.
19. *Kirfel C., Pellikaan R.* The Minimum Distance of Codes in an Array Coming from Telescopic Semigroups // IEEE Trans. Inform. Theory. 1995. V. 41. № 6. Part 1. P. 1720–1732.
20. *Geil O., Munuera C., Ruano D., Torres F.* On the Order Bounds for One-Point AG Codes // Adv. Math. Commun. 2011. V. 5. № 3. P. 489–504.
21. *Niederreiter H., Xing C.* Algebraic Geometry in Coding Theory and Cryptography. Princeton, NJ: Princeton Univ. Press, 2009.
22. *Munuera C., Pellikaan R.* Equality of Geometric Goppa Codes and Equivalence of Divisors // J. Pure Appl. Algebra. 1993. V. 90. № 3. P. 229–252.
23. *Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A.* Quantum Error Correction via Codes over GF(4) // *IEEE Trans. Inform. Theory.* 1998. V. 44. № 4. P. 1369–1387.
24. *Aly S.A., Klappenecker A., Sarvepalli P.K.* On Quantum and Classical BCH Codes // IEEE Trans. Inform. Theory. 2007. V. 53. № 3. P. 1183–1188.
25. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available online at `http://www.codetables.de` (accessed on June 6, 2020).
26. *Pereira F.R.F., La Guardia G.G., de Assis F.M.* Classical and Quantum Convolutional Codes Derived from Algebraic Geometry Codes // IEEE Trans. Commun. 2019. V. 67. № 1. P. 73–82.
27. *La Guardia G.G.* On Optimal Constacyclic Codes // Linear Algebra Appl. 2016. V. 496. P. 594–610.
28. *Barg A., Tamo I., Vlăduţ S.* Locally Recoverable Codes on Algebraic Curves // IEEE Trans. Inform. Theory. 2017. V. 63. № 8. P. 4928–4939.

Патанкер Нупур
Сингх Санджай Кумар
Индийский институт науки, образования
и исследований, Бхопал, Индия
`nupurp@iiserb.ac.in`
`sanjayks@iiserb.ac.in`

Поступила в редакцию
12.02.2020
После доработки
15.06.2020
Принята к публикации
30.06.2020