ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 57 2021 Вып. 1

УДК 621.391 : 519.725 : 512.772.7

© 2021 г. **Н. Патанкер, С.К. Сингх**

АФФИННЫЕ ЭВАЛЮАЦИОННЫЕ КОДЫ ПО ГИПЕРЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Оценивается минимальное расстояние примарных мономиальных аффинных эвалюационных кодов, построенных по гиперэллиптической кривой $x^5 + x - y^2$ над $\mathbb{F}_7$. Для оценки минимального расстояния этих кодов применяются символьные вычисления на основе техники, предложенной Гейлом и Озбудаком. Для некоторых из этих кодов также вычислено расстояние по парам символов. Кроме того, получены нижние границы на обобщенные веса Хэмминга построенных кодов. Предложенный метод вычисления обобщенных весов Хэмминга можно применять к любым примарным мономиальным аффинным эвалюационным кодам.

Ключевые слова: аффинные эвалюационные коды, базис Грёбнера, гиперэллиптическая кривая, обобщенные веса Хэмминга, расстояние по парам символов.

DOI: 10.31857/S0555292321010058

§ 1. Введение

Аффинные эвалюационные коды (affine variety codes) являются специальным классом кодов, исправляющих ошибки. Они получаются с помощью вычисления значений (эвалюации) элементов координатного кольца аффинного многообразия в $\mathbb{F}_q$-рациональных точках этого многообразия. В [1] было показано, что любой линейный код над $\mathbb{F}_q$ можно представить как аффинный эвалюационный код. Таким образом, класс аффинных эвалюационных кодов содержит в себе весь класс линейных кодов.

Длина и размерность аффинного эвалюационного кода определяются очень легко, однако не существует общего простого метода, который позволил бы определить минимальное расстояние таких кодов. В работе [2] для оценки минимального расстояния аффинных эвалюационных кодов были переформулированы граница Фенга – Рао и граница из [3]. Там же с помощью техники базисов Грёбнера и понятия правильно устроенного (well-behaving) базиса и односторонне правильно устроенной (ОПУ) упорядоченной пары мономов была получена нижняя граница на минимальное расстояние аффинных эвалюационных кодов. В [4] Гейл и Озбудак рассматривали примарные мономиальные аффинные эвалюационные коды по кварткe Клейна с фиксированным взвешенным лексикографическим порядком. Для таких кодов с помощью некоторых компонентов алгоритма Бухбергера и полного перебора некоторых специальных случаев были получены более точные оценки минимального расстояния. Авторы предположили, что такой метод можно применять к любым примарным мономиальным аффинным эвалюационным кодам, причем основной упор был сделан на поиск новых семейств хороших аффинных эвалюационных кодов с хорошими параметрами. Также авторы предложили обобщить их

метод на вычисление высших весов. В настоящей статье мы применяем процедуру, предложенную в [4], для оценки минимального расстояния и обобщенных весов Хэмминга примарных кодов по гиперэллиптической кривой. Для заданной размерности k некоторые полученные таким образом коды являются наилучшими. В [5] с помощью подобной процедуры исследовались примарные коды по кривой типа Клейна $x^2y + y^2 + x$ над $\mathbb{F}_4$.

Важными параметрами кода являются его обобщенные веса Хэмминга [6]. Эти параметры полностью характеризуют поведение кода в канале с подслушиванием типа II. В настоящей статье техника Гейла и Озбудака из [4] распространяется на вычисление обобщенных весов Хэмминга построенных кодов. Еще одним параметром кода является его расстояние по парам символов (symbol-pair distance). Кодирование для пар символов было введено для работы с каналами, на выходе которых появляются перекрывающиеся пары символов. Для некоторых из построенных кодов мы вычисляем точное значение расстояния по парам символов.

Статья организована следующим образом. В § 2 напоминаются определения следа (footprint) идеала и примарных аффинных эвалюационных кодов, а также некоторые относящиеся к этому результаты. В § 3 процедура, предложенная в [4], применяется для вычисления веса Хэмминга различных возможных кодовых слов любого примарного мономиального аффинного эвалюационного кода, построенного по гиперэллиптической кривой $x^5 + x - y^2$ над полем $\mathbb{F}_7$. Получаемые таким образом границы лучше границ, получаемых методами работы [2]. В § 4 строятся примарные мономиальные аффинные эвалюационные коды над $\mathbb{F}_7$. Кроме того, для некоторых из этих кодов вычисляется расстояние по парам символов. В § 5 выводятся нижние границы на обобщенные веса Хэмминга построенных кодов. За исключением нескольких случаев получаемые таким образом границы нетривиальны.

§ 2. Предварительные сведения

Всюду далее через q будем обозначать степень простого числа p.

В этом параграфе дается определение примарных мономиальных аффинных эвалюационных кодов и напоминается известный результат о минимальном расстоянии аффинных эвалюационных кодов. Начнем с определения следа идеала кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

Пусть $\prec$ – фиксированный порядок на мономах из кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, и пусть $I \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ – идеал этого кольца. Через $\mathcal{M}(x_1, x_2, \ldots, x_m)$ обозначим множество всех мономов от $x_1, x_2, \ldots, x_m$ над полем $\mathbb{F}_q$.

О п р е д е л е н и е 1 [2, определение 4.2]. Следом идеала I относительно порядка $\prec$ называется множество

$$\Delta_\prec(I) := \{M \in \mathcal{M}(x_1, x_2, \ldots, x_m) \mid M \text{ не является старшим мономом никакого многочлена из } I\}.$$

Всюду далее будем обозначать через $\mathrm{LM}(P)$ старший моном многочлена P. Имеется следующий результат о следе идеала кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

П р е д л о ж е н и е 1 [2, предложение 4.4] или [4, теорема 1]. *Множество*

$$\{M + I \mid M \in \Delta_\prec(I)\}$$

образует базис кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ как векторного пространства над $\mathbb{F}_q$.

Д о к а з а т е л ь с т в о. Пусть $S := \{M + I \mid M \in \Delta_\prec(I)\}$. Рассмотрим произвольное конечное подмножество $B \subset S$, тогда

$$f := \sum_{M_\alpha + I \in B} a_\alpha (M_\alpha + I) = 0,$$

где $a_\alpha \in \mathbb{F}_q$. Тогда $\mathrm{LM}(f) \in \langle \mathrm{LM}(I)\rangle$, откуда следует, что $a_\alpha = 0$ для всех α. Таким образом, множество S линейно независимо над $\mathbb{F}_q$. Кроме того, пусть G – базис Грёбнера идеала I, а $g \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Тогда согласно алгоритму деления имеем $g = h + r$, где $h \in I$ и $r = 0$ или $r \in \Delta_\prec(I)$. Если $r = 0$, то $g + I = 0 + I \in \mathrm{Span}_{\mathbb{F}_q} S$. Если же $r \neq 0$, то $g - r = h \in I$. Таким образом, $g + I = r + I \in \mathrm{Span}_{\mathbb{F}_q} S$, что и доказывает предложение. ▲

Как следствие этого предложения, получаем следующий результат.

Следствие 1 [2, следствие 4.5]. *Пусть $f_1, f_2, \ldots, f_s \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Количество общих нулей многочленов $f_1, f_2, \ldots, f_s$ над $\mathbb{F}_q$ равно*

$$\#\Delta_\prec(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle).$$

Доказательство. Пусть $I_q := \langle f_1, \ldots, f_s, x_1^q - x_1, \ldots, x_m^q - x_m\rangle$. Положим $R := \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I_q$. Пусть $Q_1, Q_2, \ldots, Q_z$ – общие нули многочленов $f_1, f_2, \ldots, f_s$ в поле $\mathbb{F}_q$. Рассмотрим отображение

$$\varphi\colon R \to \mathbb{F}_q^z, \quad \varphi(g + I_q) = (g(Q_1), g(Q_2), \ldots, g(Q_z)).$$

Тогда φ является изоморфизмом векторных пространств над $\mathbb{F}_q$. Так как изоморфные векторные пространства имеют одинаковую размерность, то из предложения 1 вытекает, что $z = \#\Delta_\prec(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, \ldots, x_m^q - x_m\rangle)$. ▲

Предложение 2 [4, следствие 1]. *Пусть $I_q := I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$. Тогда размер (мощность) многообразия, соответствующего I_q, равен $\#\Delta_\prec(I_q)$.*

Пусть $\boldsymbol{V}_{\mathbb{F}_q}(I_q) := \{P_1, P_2, \ldots, P_n\}$, где $P_i \neq P_j$ при $i \neq j$.

Определение 2 [4, определение 2]. *В тех же обозначениях, что и выше, выберем $L \subseteq \Delta_\prec(I_q)$. Тогда*

$$C(I, L) := \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(M + I_q) := (M(P_1), M(P_2), \ldots, M(P_n)) \mid M \in L\}$$

называется примарным мономиальным аффинным эвалюационным кодом.

Из вышесказанного немедленно видно, что $C(I, L)$ является линейным кодом над полем $\mathbb{F}_q$ длины $n := \#\boldsymbol{V}_{\mathbb{F}_q}(I_q) = \#\Delta_\prec(I_q)$ и размерности $k = \#L$.

2.1. Граница на минимальное расстояние аффинных эвалюационных кодов. В работе [2] минимальное расстояние аффинных эвалюационных кодов оценивалось с помощью понятия односторонне правильно устроенной пары мономов, которое будет определено ниже. Вначале напомним определение аффинного эвалюационного кода.

Определение 3. Для тех же I_q и $P_1, P_2, \ldots, P_n$, что и в определении 2, и для подпространства $L' \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ аффинным эвалюационным кодом $C(I, L')$ назовем множество

$$C(I, L') := \{\mathrm{ev}(f + I_q) = (f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L'\}.$$

Всюду далее через $P \operatorname{rem} G$ будем обозначать остаток от деления многочлена P на G.

Определение 4 [2, определение 4.6]. Базис $\{b_1 + I_q, b_2 + I_q, \ldots, b_{\dim(L')} + I_q\}$ подпространства $L' \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, такой что $\mathrm{supp}(b_i) \subseteq \Delta_\prec(I_q)$ для $i = 1, 2, \ldots, \dim(L')$ и $\mathrm{LM}(b_1) \prec \mathrm{LM}(b_2) \prec \ldots \prec \mathrm{LM}(b_{\dim(L')})$, будем называть правильно устроенным относительно порядка $\prec$.

Определение 5 [2, определение 4.8]. Пусть G – базис Грёбнера для I_q относительно порядка $\prec$. Упорядоченная пара мономов (M_1, M_2), где $M_1, M_2 \in \Delta_\prec(I_q)$,

называется односторонне правильно устроенной (ОПУ), если $\forall\, h \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, такого что $\operatorname{supp}(h) \subseteq \Delta_\prec(I_q)$ и $\operatorname{LM}(h) = M_1$, выполняется

$$\operatorname{LM}(M_1 M_2 \operatorname{rem} G) = \operatorname{LM}(hM_2 \operatorname{rem} G).$$

Следующий результат задает границу на минимальное расстояние аффинного эвалюационного кода.

Т е о р е м а 1 [2, теорема 4.9]. *Пусть порядок $\prec$ фиксирован. Минимальное расстояние кода $C(I, L')$ не меньше, чем*

$$\min\bigl\{\#\{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q),\ \textit{такое что } (P, N) \textit{ – ОПУ пара}\\ \textit{и } \operatorname{LM}(PN \operatorname{rem} G) = K\} \mid P \in \{\operatorname{LM}(b_1), \operatorname{LM}(b_2), \ldots, \operatorname{LM}(b_{\dim(L')})\}\bigr\},$$

где $\{b_1 + I_q, \ldots, b_{\dim(L')} + I_q\}$ – любой правильно устроенный базис подпространства L'.

Д о к а з а т е л ь с т в о. Пусть $\boldsymbol{x} = \operatorname{ev}(f + I_q) \in C(I, L')$ для некоторого $f \in L'$. Положим $P := \operatorname{LM}(f) \in \{\operatorname{LM}(b_1), \operatorname{LM}(b_2), \ldots, \operatorname{LM}(b_{\dim(L')})\}$. Далее, если существует $N \in \Delta_\prec(I_q)$, такое что (P, N) – ОПУ пара и $\operatorname{LM}(PN \operatorname{rem} G) = K$, то

$$K \in \Delta_\prec(I_q) \setminus \Delta_\prec(\langle f\rangle + I_q).$$

Тогда согласно следствию 1

$$w_H(\boldsymbol{x}) = n - \#\Delta_\prec(\langle f\rangle + I_q) = \#\Delta_\prec(I_q) - \#\Delta_\prec(\langle f\rangle + I_q) \geqslant\\ \geqslant \{K \in \Delta_\prec(I_q) \mid \exists N \in \Delta_\prec(I_q),\ \text{такое что } (P, N) \text{ – ОПУ пара}\\ \text{и } \operatorname{LM}(PN \operatorname{rem} G) = K\},$$

откуда следует требуемый результат. ▲

§ 3. Веса кодовых слов примарных мономиальных аффинных эвалюационных кодов

В начале этого параграфа напомним технику, использовавшуюся в [4] для определения весов кодовых слов примарного мономиального аффинного эвалюационного кода, построенного по кривой Клейна над $\mathbb{F}_8$. Затем применим эту технику для нахождения весов кодовых слов примарных мономиальных аффинных эвалюационных кодов, построенных по конкретной гиперэллиптической кривой над $\mathbb{F}_7$.

Пусть $C(I, L)$ – примарный мономиальный аффинный эвалюационный код, определенный в § 2. Для кодового слова $\boldsymbol{c} := \operatorname{ev}(f + I_q) \in C(I, L)$, где $f \in \operatorname{Span}_{\mathbb{F}_q} L$, из следствия 1 известно, что вес Хэмминга слова $\boldsymbol{c}$ равен

$$w_H(\boldsymbol{c}) = n - \#\Delta_\prec(\langle f\rangle + I_q) = \#\Delta_\prec(I_q) \cap \operatorname{LM}(\langle f\rangle + I_q) =: \#\square_\prec(f),$$

где $\operatorname{LM}(g)$ – старший моном многочлена g относительно порядка $\prec$. Техника из [4] состоит в том, что нижнюю границу на $w_H(\boldsymbol{c})$ можно получить, добавляя мономы в множество $\square_\prec(f)$.

По теореме 1, если $P := \operatorname{LM}(f)$ и $N, K \in \Delta_\prec(I_q)$ удовлетворяют условию

$$(P, N) \text{ – ОПУ пара и } \operatorname{LM}(PN \operatorname{rem} G) = K,$$

то $K \in \square_\prec(f)$.

В настоящей статье мы сперва находим ОПУ пары и получаем элементы множества $\square_\prec(f)$ для различных выборов многочлена $f \in \operatorname{Span}_{\mathbb{F}_q} L$. Затем мы пытаемся добавить в $\square_\prec(f)$ больше мономов, используя технику из [4]. Получаемая таким

образом граница на минимальное расстояние кодовых слов кода $C(I, L)$ иногда оказывается строго лучше, чем граница из теоремы 1.

Прежде чем приступить к этому, введем понятие взвешенного лексикографического порядка на мономах из кольца $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$.

Определение 6 [2, определение 4.17]. Пусть $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}$ заданы. Определим вес монома $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}$ как

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) := i_1 w(x_1) + i_2 w(x_2) + \ldots + i_m w(x_m).$$

Взвешенный лексикографический порядок $\prec_w$ на мономах из $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ определяется следующим образом: $x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \prec_w x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}$, если либо

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) < w(x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}),$$

либо

$$w(x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m}) = w(x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m}), \quad \text{но} \quad x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \prec_{\text{lex}} x_1^{j_1} x_2^{j_2} \ldots x_m^{j_m},$$

где $\prec_{\text{lex}}$ – обычный лексикографический порядок, такой что $x_m \prec_{\text{lex}} \ldots \prec_{\text{lex}} x_1$.

3.1. Веса кодовых слов по гиперэллиптической кривой. Пусть $I = \langle x^5 + x - y^2 \rangle$ – идеал кольца $\mathbb{F}_7[x, y]$, и следовательно, $I_7 = \langle x^5 + x - y^2, x^7 - x, y^7 - y \rangle$. Соответствующее множество $\mathbb{F}_7$-рациональных точек этого многообразия имеет вид

$$\{(0,0), (1,3), (1,4), (3,1), (3,6), (5,1), (5,6)\}.$$

Зафиксируем порядок на мономах из кольца $\mathbb{F}_7[x, y]$ как взвешенный лексикографический порядок $\prec_w$, в котором $w(x) = 2$, $w(y) = 5$, причем $y \prec_{\text{lex}} x$ в обычном лексикографическом порядке. С помощью системы компьютерной алгебры SageMath находим базис Грёбнера идеала I_7 относительно порядка $\prec_w$:

$$\{x^3y - 2x^2y + 2xy - y, y^2 - 2x^3 + 3x^2 - 3x, x^4 - 2x^3 + 2x^2 - x\}.$$

Элементы следа $\Delta_{\prec_w}(I_7)$ и соответствующие им веса перечислены в следующей таблице:

1	y	x	xy	x^2	x^2y	x^3
0	5	2	7	4	9	6

.

В дальнейших пунктах мы будем оценивать мощность множества $\square_{\prec_w}(f)$, следуя технике из [4]. По очереди рассмотрим шесть различных возможных кодовых слов, получаемых из многочленов со старшими мономами из $\Delta_{\prec_w}(I_7)$.

Перед этим зафиксируем одно обозначение. Рассмотрим многочлены $a(x, y)$, $b(x, y)$ и $c(x, y)$. Запись

$$a(x, y) \xrightarrow{b(x,y)} c(x, y)$$

будет означать, что $c(x, y) = a(x, y) - s(x, y)b(x, y)$ для некоторого многочлена $s(x, y)$.

3.1.1. Старший моном, равный x: Рассмотрим слово $\boldsymbol{c} = \text{ev}(f + I_7)$, где $f = x + a_0$, $a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x, 1), (x, x), (x, x^2), (x, y), (x, xy)\}$ – ОПУ пары. Таким образом,

$$\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 5$. При этом слово $\text{ev}((x - 1) + I_7)$ имеет вес 5. Значит, в этом случае граница точна.

3.1.2. Старший моном, равный x^2: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^2 + a_1x + a_0$, $a_1, a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^2, 1), (x^2, x), (x^2, y)\}$ – ОПУ пары. Таким образом,

$$\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 3$. При этом слово $\mathrm{ev}((x-1)(x-3))$ имеет вес 3. Значит, в этом случае граница точна.

3.1.3. Старший моном, равный y: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = y + a_1x^2 + a_2x + a_3$, $a_1, a_2, a_3 \in \mathbb{F}_7$. Проверка показывает, что $\{(y, 1), (y, x), (y, x^2), (y, x^3)\}$ – ОПУ пары. Таким образом,

$$\{y, xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 3$. Теперь рассмотрим редукцию

$$yf \xrightarrow{y^2 - 2x^3 + 3x^2 - 3x} a_1x^2y + a_2xy + 2x^3 + a_3y - 3x^2 + 3x.$$

Если $a_1 \neq 0$, то

$$a_1x^2y + a_2xy + 2x^3 + a_3y - 3x^2 + 3x \xrightarrow{x^2 f}$$
$$\xrightarrow{x^2 f} -a_1^2x^4 + a_2xy + (2 - a_1a_2)x^3 + a_3y + (-3 - a_1a_3)x^2 + 3x \xrightarrow{x^4 - 2x^3 + 2x^2 - x}$$
$$\xrightarrow{x^4 - 2x^3 + 2x^2 - x} a_2xy + (2 - a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x.$$

Если $a_2 \neq 0$, то

$$a_2xy + (2 - a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x \xrightarrow{f}$$
$$\xrightarrow{f} (2 - 2a_1a_2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2 - a_2^2)x^2 + (3 - a_1^2 - a_2a_3)x.$$

Если $1 - a_1a_2 - a_1^2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $a_2 = a_1^{-1} - a_1$, и тогда остается

$$a_3y + (-1 - a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - a_1^{-1}a_3 + a_1a_3)x.$$

Теперь, если $a_3 \neq 0$, то

$$a_3y + (-1 - a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - a_1^{-1}a_3 + a_1a_3)x \xrightarrow{f}$$
$$\xrightarrow{f} (-1 - 2a_1a_3 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2 - 2a_1^{-1}a_3 + 2a_1a_3)x - a_3^2.$$

Если при этом $a_3 \neq 4a_1 - 4a_1^{-3} - 4a_1^{-1}$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $(1 + a_1^{-4})x - a_3^2$, тогда $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

А если $a_3 = 0$, то остается $(-1 + a_1^2 - a_1^{-2})x^2 + (3 - a_1^2)x$, и $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Если же $a_2 = 0$, то остается $(2 - 2a_1^2)x^3 + a_3y + (-3 - a_1a_3 + 2a_1^2)x^2 + (3 - a_1^2)x$. Если $a_1^2 \neq 1$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $a_1 \in \{1, 6\}$, и тогда имеется два случая:

Если $a_1 = 1$, то остается $a_3y + (-1 - a_3)x^2 + 2x$. Если $a_3 \neq 0$, то с помощью f получаем $(-1 - 2a_3)x^2 + 2x - a_3^2$. Теперь, если $a_3 \neq 3$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $2x - 2$, и таким образом, $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Но если $a_3 = 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Если же $a_1 = 6$, то остается $a_3y + (-1 - 6a_3)x^2 + 2x$. Если $a_3 \neq 0$, то с помощью f получаем $(-1 - 5a_3)x^2 + 2x - a_3^2$. Теперь, если $a_3 \neq 4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $2x - 2$, и таким образом, $\{x, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Но если $a_3 = 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$.

Далее, если $a_1 = 0$, то остается $a_2xy + 2x^3 + a_3y - 3x^2 + 3x$. Если $a_2 \neq 0$, то применяем редукцию

$$a_2xy + 2x^3 + a_3y - 3x^2 + 3x \xrightarrow{f} 2x^3 + a_3y + (-3 - a_2^2)x^2 + (3 - a_2a_3)x.$$

Таким образом, $x^3 \in \square_{\prec_w}(f)$. В противном случае, если $a_2 = 0$, то $x^3 \in \square_{\prec_w}(f)$.

Из всех этих вычислений следует, что в множестве $\square_{\prec_w}(f)$ содержится по крайней мере $3 + \min\{2, 3, 4, 2, 1, 2, 1, 1\} = 4$ элемента. Следовательно, $w_H(\boldsymbol{c}) \geqslant 4$.

3.1.4. Старший моном, равный $\boldsymbol{x^3}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_3, a_2, a_1, a_0 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^3, 1)\}$ – ОПУ пара. Таким образом,

$$\{x^3\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 1$. При этом слово $\mathrm{ev}((x-1)(x-3)(x-5) + I_7)$ имеет вес 1. Значит, в этом случае граница точна.

3.1.5. Старший моном, равный $\boldsymbol{xy}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = xy + a_4x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_7$. Проверка показывает, что $\{(xy, 1), (xy, x)\}$ – ОПУ пары. Таким образом,

$$\{xy, x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 2$. При этом слово $\mathrm{ev}((xy + 3x^3 + 2y + 6x^2 + I_7))$, как и некоторые другие кодовые слова, имеет вес 2. Значит, в этом случае граница точна.

3.1.6. Старший моном, равный $\boldsymbol{x^2y}$: Рассмотрим слово $\boldsymbol{c} = \mathrm{ev}(f + I_7)$, где $f = x^2y + a_5xy + a_4x^3 + a_3y + a_2x^2 + a_1x + a_0$, $a_0, a_1, a_2, a_3, a_4, a_5 \in \mathbb{F}_7$. Проверка показывает, что $\{(x^2y, 1)\}$ – ОПУ пара. Таким образом,

$$\{x^2y\} \subseteq \square_{\prec_w}(f).$$

Следовательно, $w_H(\boldsymbol{c}) \geqslant 1$. Теперь попробуем добавить в множество $\square_{\prec_w}(f)$ больше мономов при различных условиях на коэффициенты многочлена f.

Рассмотрим многочлен $xf = x^3y + a_5x^2y + a_4x^4 + a_3xy + a_2x^3 + a_1x^2 + a_0x$. Применим редукцию

$$xf \xrightarrow{x^3y - 2x^2y + 2xy - y} (a_5 + 2)x^2y + a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x.$$

Если $a_5 \neq 5$, то, продолжая редукцию, получаем

$$\begin{aligned}&(a_5 + 2)x^2y + a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x \xrightarrow{f}\\ &\xrightarrow{f} a_4x^4 + (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5 - 2a_4)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2)x^2 + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0.\end{aligned}$$

Если при этом $a_4 \neq 0$, то, продолжая редукцию, получаем

$$\begin{aligned}&a_4x^4 + (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5 - 2a_4)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2)x^2 + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0 \xrightarrow{x^4 - 2x^3 + 2x^2 - x}\\ &\xrightarrow{x^4 - 2x^3 + 2x^2 - x} (a_3 - 2 - a_5^2 - 2a_5)xy + (a_2 - a_4a_5)x^3 + (1 - a_3a_5 - 2a_3)y +\\ &+ (a_1 - a_2a_5 - 2a_2 - 2a_4)x^2 + (a_0 - a_1a_5 - 2a_1 + a_4)x - (a_5 + 2)a_0.\end{aligned}$$

Теперь рассмотрим различные случаи в зависимости от значения коэффициента a_5:

Если $a_5 = 0$, то остается

$$(a_3 - 2)xy + a_2x^3 + (1 - 2a_3)y + (a_1 - 2a_2 - 2a_4)x^2 + (a_0 - 2a_1 + a_4)x - 2a_0.$$

Если $a_3 \neq 2$, то $\{xy\} \subseteq \square_{\prec_w}(f)$. В противном случае остается

$$a_2x^3 + 4y + (a_1 - 2a_2 - 2a_4)x^2 + (a_0 - 2a_1 + a_4)x - 2a_0.$$

Если теперь $a_2 \neq 0$, то $\{x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае $\{y\} \subseteq \square_{\prec_w}(f)$.

Если $a_5 = 1$, то остается

$$(a_3 - 5)xy + (a_2 - a_4)x^3 + (1 - 3a_3)y + (a_1 - 3a_2 - 2a_4)x^2 + (a_0 - 3a_1 + a_4)x - 3a_0.$$

Если теперь $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - a_4)x^3 + (a_1 - 3a_2 - 2a_4)x^2 + (a_0 - 3a_1 + a_4)x - 3a_0.$$

Если при этом $a_2 \neq a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае остается $(a_1 - 5a_2)x^2 + + (a_0 - 3a_1 + a_2)x - 3a_0$. Тогда, если $a_1 \neq 5a_2$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$, а в противном случае остается $a_0x - 3a_0$. Если $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 1$.

Если $a_5 = 2$, то остается

$$(a_3 - 3)xy + (a_2 - 2a_4)x^3 + (1 - 4a_3)y + (a_1 - 4a_2 - 2a_4)x^2 + \\ + (a_0 - 4a_1 + a_4)x - 4a_0.$$

Если теперь $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - 2a_4)x^3 + 3y + (a_1 - 4a_2 - 2a_4)x^2 + (a_0 - 4a_1 + a_4)x - 3a_0.$$

Если при этом $a_2 \neq 2a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 3$, то остается

$$(a_3 - 3)xy + (a_2 - 3a_4)x^3 + (1 - 5a_3)y + (a_1 - 5a_2 - 2a_4)x^2 + \\ + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 - 3a_4)x^3 + (a_1 - 5a_2 - 2a_4)x^2 + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Тогда $x^3 \in \square_{\prec_w}(f)$, если $a_2 \neq 3a_4$. А если $a_2 = 3a_4$, то остается

$$(a_1 - 3a_4)x^2 + (a_0 - 5a_1 + a_4)x - 5a_0.$$

Если при этом $a_1 \neq 3a_4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае остается $a_0x - 5a_0$. Если $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 1$.

Если $a_5 = 4$, то

$$(a_3 - 5)xy + (a_2 - 4a_4)x^3 + (1 + a_3)y + (a_1 - 6a_2 - 2a_4)x^2 + (a_0 - 6a_1 + a_4)x + a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае, если к тому же $a_2 \neq 4a_4$, то $x^3 \in \square_{\prec_w}(f)$, а в противном случае $\{y, xy\} \subseteq \square_{\prec_w}(f)$.

Наконец, если $a_5 = 6$, то остается

$$(a_3 - 1)xy + (a_2 - 6a_4)x^3 + (1 - a_3)y + (a_1 - a_2 - 2a_4)x^2 + (a_0 - a_1 + a_4)x - a_0.$$

Если $a_3 \neq 1$, то $xy \in \square_{\prec_w}(f)$. В противном случае, если $a_2 \neq 6a_4$, то $x^3 \in \square_{\prec_w}(f)$. В случае $a_2 = 6a_4$, если $a_1 \neq a_4$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. А если $a_1 = a_4$ и $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае $w_H(c) \geqslant 1$.

Если же $a_4 = 0$, то остается

$$(a_3 - 2 - a_5^2 - 2a_5)xy + a_2x^3 + (1 - a_3a_5 - 2a_3)y + (a_1 - a_2a_5 - 2a_2)x^2 + \\ + (a_0 - a_1a_5 - 2a_1)x - (a_5 + 2)a_0.$$

Теперь рассмотрим различные случаи в зависимости от значения коэффициента a_5:

Если $a_5 = 0$, то остается

$$(a_3 - 2)xy + a_2x^3 + (1 - 2a_3)y + (a_1 - 2a_2)x^2 + (a_0 - 2a_1)x - 2a_0.$$

Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 2$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 1$, то остается

$$(a_3 - 5)xy + a_2x^3 + (1 - 3a_3)y + (a_1 - 3a_2)x^2 + (a_0 - 3a_1)x - 3a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. Если же $a_2 = 0$ и $a_1 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$, а в противном случае остается $a_0x - 3a_0$. Если теперь $a_0 \neq 0$, то $\{x, xy, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если $a_5 = 2$, то остается

$$(a_3 - 3)xy + a_2x^3 + (1 - 4a_3)y + (a_1 - 4a_2)x^2 + (a_0 - 4a_1)x - 4a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если $a_5 = 3$, то остается

$$(a_3 - 3)xy + a_2x^3 + (1 - 5a_3)y + (a_1 - 5a_2)x^2 + (a_0 - 5a_1)x - 5a_0.$$

Если $a_3 \neq 3$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 3$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $a_2 = 0$, и если при этом $a_1 \neq 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Если же $a_1 = 0$ и $a_0 \neq 0$, то $\{x, xy, x^2, x^3\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если $a_5 = 4$, то остается

$$(a_3 - 5)xy + a_2x^3 + (1 - 6a_3)y + (a_1 - 6a_2)x^2 + (a_0 - 6a_1)x + a_0.$$

Если $a_3 \neq 5$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 5$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $\{y, xy\} \subseteq \square_{\prec_w}(f)$.

Наконец, если $a_5 = 6$, остается

$$(a_3 - 1)xy + a_2x^3 + (1 - a_3)y + (a_1 - a_2)x^2 + (a_0 - a_1)x - a_0.$$

Если $a_3 \neq 1$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 1$, и если $a_2 \neq 0$, то $x^3 \in \in \square_{\prec_w}(f)$. В противном случае $a_2 = 0$, и если при этом $a_1 \neq 0$, то $\{x^2, x^3\} \subseteq \square_{\prec_w}(f)$. Если же $a_1 = 0$ и $a_0 \neq 0$, то $\{x, x^2, x^3, xy\} \subseteq \square_{\prec_w}(f)$. В противном случае непосредственными вычислениями убеждаемся, что $w_H(c) \geqslant 2$.

Если же в самом начале было $a_5 = 5$, то остается

$$a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x.$$

Если $a_4 \neq 0$, то продолжим редукцию:

$$a_4x^4 + (a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x \xrightarrow{x^4-2x^3+2x^2-x}$$
$$\xrightarrow{x^4-2x^3+2x^2-x} (a_3 - 2)xy + (a_2 + 2a_4)x^3 + y + (a_1 - 2a_4)x^2 + (a_0 + a_4)x.$$

Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае остается

$$(a_2 + 2a_4)x^3 + y + (a_1 - 2a_4)x^2 + (a_0 + a_4)x.$$

Если $a_2 \neq 5a_4$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Если же $a_4 = 0$, то остается $(a_3 - 2)xy + a_2x^3 + y + a_1x^2 + a_0x$. Если $a_3 \neq 2$, то $xy \in \square_{\prec_w}(f)$. В противном случае $a_3 = 2$, и остается $a_2x^3 + y + a_1x^2 + a_0x$. Если при этом $a_2 \neq 0$, то $x^3 \in \square_{\prec_w}(f)$. В противном случае $y \in \square_{\prec_w}(f)$.

Из сделанных вычислений мы заключаем, что если $a_5 \neq 5$ и $a_4 \neq 0$, то $w_H(c) \geqslant 1$, а в противном случае $w_H(c) \geqslant 2$.

В результате всех проделанных вычислений получаем следующую таблицу, в которой первая строка состоит из старших мономов различных кодовых слов $\mathrm{ev}(f)$, а во второй строке приведены границы на $\#\square_{\prec_w}(f)$:

1	x	x^2	y	x^3	xy	x^2y
7	5	3	4	1	2	1

.

§ 4. Построение кода

Для $1 \leqslant s \leqslant n$, следуя [4], определим код

$$C := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(M + I_7) \mid M \in \Delta_{\prec_w}(I_7),\ \delta(M) \geqslant s\},$$

где $\delta(M)$ – полученная выше оценка на $\#\square_{\prec_w}(M)$, приведенная в таблице. Параметры кодов с наилучшим возможным минимальным расстоянием таковы:

$$[7, 1, \geqslant 7], \qquad [7, 2, \geqslant 5], \qquad [7, 3, \geqslant 4], \qquad [7, 4, \geqslant 3], \qquad [7, 5, \geqslant 2], \qquad [7, 6, \geqslant 2].$$

Во всех этих случаях для заданного значения кодовой размерности оценка на минимальное расстояние получаемого таким образом кода либо равна наилучшему известному значению согласно таблице из [7], либо лишь на единицу меньше.

4.1. Расстояние по парам символов. Кодирование для пар символов было введено для работы с каналами, на выходе которых появляются перекрывающиеся пары символов. Тем самым, появился новый параметр кодов, называемый расстоянием по парам символов. Расстояние по парам символов для кода определяется следующим образом.

Пусть A – алфавит объема q. Для $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in A^n$ определим его вектор пар символов как

$$\pi_{\mathrm{sp}}(\boldsymbol{x}) := [(x_1, x_2), (x_2, x_3), \ldots, (x_{n-1}, x_n), (x_n, x_1)] \in (A^2)^n.$$

Тогда вес вектора $\boldsymbol{x}$ по парам символов определяется как

$$w_{\mathrm{sp}}(\boldsymbol{x}) := w_H(\pi_{\mathrm{sp}}(\boldsymbol{x})) = \#\{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (0, 0),\ x_{n+1} = x_1\}.$$

Для двух векторов $\boldsymbol{x}, \boldsymbol{y} \in A^n$ расстояние по парам символов между ними определяется как

$$d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) := d(\pi_{\mathrm{sp}}(\boldsymbol{x}), \pi_{\mathrm{sp}}(\boldsymbol{y})) =$$
$$= \#\{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (y_i, y_{i+1}),\ x_{n+1} = x_1,\ y_{n+1} = y_1\}.$$

Пусть C – линейный код над полем $\mathbb{F}_q$. Тогда расстояние по парам символов для кода C определяется как

$$d_{\mathrm{sp}}(C) := \min\{w_{\mathrm{sp}}(\boldsymbol{x}) \mid \boldsymbol{x} \in C,\ \boldsymbol{x} \neq 0\}.$$

Взаимосвязь между минимальным расстоянием Хэмминга кода C и его расстоянием по парам символов описывает следующее

Предложение 3 [8, предложение 1]. *Для $\boldsymbol{x}, \boldsymbol{y} \in A^n$ пусть $0 < d_H(\boldsymbol{x}, \boldsymbol{y}) < n$ – расстояние Хэмминга между $\boldsymbol{x}$ и $\boldsymbol{y}$. Тогда*

$$d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) \geqslant d(\boldsymbol{x}, \boldsymbol{y}) + 1.$$

Доказательство. Положим

$$\mathcal{A}_H := \{1 \leqslant i \leqslant n \mid x_i \neq y_i\}, \quad \mathcal{A}_{\mathrm{sp}} := \{1 \leqslant i \leqslant n \mid (x_i, x_{i+1}) \neq (y_i, y_{i+1})\}.$$

Каждый индекс $i \in \mathcal{A}_H$ принадлежит $\mathcal{A}_{\mathrm{sp}}$. Таким образом, $d_{\mathrm{sp}}(\boldsymbol{x}, \boldsymbol{y}) \geqslant d(\boldsymbol{x}, \boldsymbol{y})$. Поскольку $d(\boldsymbol{x}, \boldsymbol{y}) < n$, найдется по крайней мере одна пара индексов $(i, i+1)$, такая что ровно один из индексов i и $i+1$ принадлежит $\mathcal{A}_H$, пусть это будет, скажем, i. Тогда $(i-1, i)$ и $(i, i+1)$ принадлежат $\mathcal{A}_{\mathrm{sp}}$, откуда вытекает требуемый результат. ▲

Подробнее о расстоянии по парам символов для кодов см. в [8].

Используя предложение 3, получаем следующие результаты о кодах, построенных по гиперэллиптической кривой над полем $\mathbb{F}_7$.

Предложение 4. *Пусть $P_1 := (0, 0)$, $P_2 := (1, 3)$, $P_3 := (1, 4)$, $P_4 := (3, 1)$, $P_5 := (3, 6)$, $P_6 := (5, 1)$ и $P_7 := (5, 6)$ – порядок точек, в которых вычисляются значения для построения кодов. Тогда*

1. *Если*

$$C_1 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1 + I_7), \mathrm{ev}(x + I_7), \mathrm{ev}(x^2 + I_7), \mathrm{ev}(y + I_7)\},$$

то $d_{\mathrm{sp}}(C_1) = 4$;

2. *Если*

$$C_2 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1 + I_7), \mathrm{ev}(x + I_7), \mathrm{ev}(x^2 + I_7), \mathrm{ev}(y + I_7), \mathrm{ev}(xy + I_7), \mathrm{ev}(x^2 y + I_7)\},$$

то $d_{\mathrm{sp}}(C_2) = 3$.

Доказательство. Имеем $d_{\mathrm{sp}}(C_1) \geqslant d(C_1) + 1 = 4$. Для доказательства противоположного неравенства рассмотрим кодовое слово $\mathrm{ev}((x-1)(x-3) + I_7) \in C_1$. Его вес по парам символов равен 4. Таким образом, $d_{\mathrm{sp}}(C_1) \leqslant 4$, откуда следует утверждение 1.

Имеем $d_{\mathrm{sp}}(C_2) \geqslant d(C_2) + 1 = 3$. Далее, кодовое слово $\mathrm{ev}(y(x-1)(x-3) + I_7) \in C_2$ имеет вес по парам символов, равный 3. Таким образом, $d_{\mathrm{sp}}(C_2) \leqslant 3$, откуда следует утверждение 2. ▲

§ 5. Обобщенные веса Хэмминга кодов

Пусть C – $[n, k]$-код над полем $\mathbb{F}_q$. Обобщенные веса Хэмминга для линейных кодов были введены в [9, 10], а затем их независимо переоткрыл Вэй в [6]. Изучение этих параметров мотивировалось некоторыми приложениями в криптографии. Обобщенные веса Хэмминга линейных кодов определяются следующим образом.

Носителем линейного $[n, k]$-кода C над полем $\mathbb{F}_q$ называется множество

$$\mathrm{Supp}\, C := \{i \mid x_i \neq 0 \text{ для некоторого } \boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in C\}.$$

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

$$d_r(C) := \min\{\#\operatorname{Supp} D \mid D \text{ является линейным подкодом кода } C \text{ размерности } \dim_{\mathbb{F}_q}(D) = r\}.$$

Важное свойство обобщенных весов Хэмминга кода C описывает следующая

Теорема 2 [6, теорема 1]. *Для линейного $[n,k]$-кода C, такого что $k > 0$, справедливы неравенства*

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

Доказательство. Из определения следует, что $d_{r-1}(C) \leqslant d_r(C)$. Остается показать, что это неравенство строгое. Пусть D – линейный подкод кода C, имеющий размерность r, такой что $d_r(C) = \#\operatorname{Supp}(D)$. Пусть $i \in \operatorname{Supp}(D)$. Рассмотрим множество $D_i := \{(x_1, x_2, \ldots, x_n) \in D \mid x_i = 0\}$. Тогда $\dim_{\mathbb{F}_q}(D_i) = r-1$. Таким образом, $d_{r-1}(C) \leqslant \#\operatorname{Supp} D_i < \#\operatorname{Supp} D = d_r(C)$. ▲

В этом параграфе мы выведем нижние границы на обобщенные веса Хэмминга для кодов, построенных в § 4. Основная идея состоит в следующем.

Пусть C – $[n,k]$-код над полем $\mathbb{F}_q$. Для любого подкода D кода C, имеющего размерность r, $1 \leqslant r \leqslant k$, с базисом над $\mathbb{F}_q$ вида $\operatorname{ev}(g_1 + I_q), \operatorname{ev}(g_2 + I_q), \ldots, \operatorname{ev}(g_r + I_q)$, т.е. $D = \operatorname{Span}_{\mathbb{F}_q}\{\operatorname{ev}(g_1 + I_q), \operatorname{ev}(g_2 + I_q), \ldots, \operatorname{ev}(g_r + I_q)\}$, согласно следствию 1 имеем

$$\begin{aligned}&\#\operatorname{Supp} D = n - \#\Delta_{\prec_w}(\langle g_1, g_2, \ldots, g_r\rangle + I_q) = \\ &= \#\Delta_{\prec_w}(I_q) \cap \operatorname{LM}(\langle g_1, g_2, \ldots, g_r\rangle + I_q) =: \#\square_{\prec_w}(D).\end{aligned}$$

Поскольку $g_1, g_2, \ldots, g_r$ линейно независимы, всегда можно считать, что их старшие коэффициенты равны единице, а старшие мономы различны.

Предложение 5. *Пусть* $C_1 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1 + I_7), \operatorname{ev}(x + I_7), \operatorname{ev}(x^2 + I_7), \operatorname{ev}(y + I_7)\}$. *Тогда*

1. *C_1 является $[7, 4, \geqslant 3]$-кодом*;
2. $d_2(C_1) \geqslant 5$;
3. $d_3(C_1) \geqslant 6$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := y + a_1x^2 + a_2x + a_3, \quad f_2 := x^2 + b_1x + b_2, \quad f_3 := x + c_1, \quad f_4 := 1,$$

где $a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_1, тогда при различных выборах D получаем следующее:

- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7)\}$, то $\{x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 5$;
- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, y, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 6$;
- Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 5$.
- Во всех остальных случаях $\#\operatorname{Supp} D \geqslant 7$.

Следовательно, $d_2(C_1) \geqslant 5$. Это доказывает утверждение 2. Пусть D' – подкод размерности 3 кода C_1, тогда при различных выборах D' получаем следующее:

- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то $\{x, x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 6$;
- Во всех остальных случаях $\#\operatorname{Supp} D' \geqslant 7$.

Следовательно, $d_3(C_1) \geqslant 6$. Это доказывает утверждение 3. ▲

Аналогично, имеют место следующие результаты.

Предложение 6. *Пусть* $C_2 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1+I_7), \mathrm{ev}(x+I_7), \mathrm{ev}(y+I_7)\}$. *Тогда*
1. C_2 *является* $[7, 3, \geqslant 4]$-*кодом*;
2. $d_2(C_2) \geqslant 6$.

Предложение 7. *Пусть* $C_3 := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(1+I_7), \mathrm{ev}(x+I_7), \mathrm{ev}(x^2+I_7), \mathrm{ev}(y+I_7), \mathrm{ev}(xy+I_7), \mathrm{ev}(x^2y+I_7)\}$. *Тогда*
1. C_3 *является* $[7, 6, \geqslant 2]$-*кодом*;
2. $d_2(C_3) \geqslant 3$;
3. $d_3(C_3) \geqslant 4$;
4. $d_4(C_3) \geqslant 5$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := x^2y + a_1xy + a_2y + a_3x^2 + a_4x + a_5, \quad f_2 := xy + b_1y + b_2x^2 + b_3x + b_4,$$
$$f_3 := y + c_1x^2 + c_2x + c_3, \quad f_4 := x^2 + d_1x + d_2, \quad f_5 := x + e_1, \quad f_6 := 1,$$

где $a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, c_1, c_2, c_3, d_1, d_2, e_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_3, тогда при различных выборах D получаем следующее.

Если $D := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(f_1 + I_7), \mathrm{ev}(f_2 + I_7)\}$, то $\{xy, x^2y\} \subseteq \square_{\prec_w}(D)$. Применим редукцию

$$x^2 f_2 \xrightarrow{x^3y - 2x^2y + 2xy - y} (b_1 + 2)x^2y + b_2x^4 - 2xy + b_3x^3 + y + b_4x^2.$$

Если $b_1 \neq 5$, то продолжаем редукцию:

$$(b_1 + 2)x^2y + b_2x^4 - 2xy + b_3x^3 + y + b_4x^2 \xrightarrow{f_2}$$
$$\xrightarrow{f_2} b_2x^4 + (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1 - 2b_2)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3)x^2 - b_4(b_1 + 2)x.$$

Если $b_2 \neq 0$, то продолжаем редукцию:

$$b_2x^4 + (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1 - 2b_2)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3)x^2 - b_4(b_1 + 2)x \xrightarrow{x^4 - 2x^3 + 2x^2 - x}$$
$$\xrightarrow{x^4 - 2x^3 + 2x^2 - x} (-2 - b_1^2 - 2b_1)xy + (b_3 - b_2b_1)x^3 + y +$$
$$+ (b_4 - b_3b_1 - 2b_3 - 2b_2)x^2 + (-b_4b_1 - 2b_4 + b_2)x \xrightarrow{f_2}$$
$$\xrightarrow{f_2} (b_3 - b_1b_2)x^3 + (1 + 2b_1 + b_1^3 + 2b_1^2)y + (b_4 - b_1b_3 - 2b_3 + b_2b_1^2 + 2b_2b_1)x^2 +$$
$$+ (-b_4b_1 - 2b_4 + b_2 + 2b_3 + b_3b_1^2 + 2b_1b_3)x + b_4(2 + b_1^2 + 2b_1).$$

Если $b_3 \neq b_1b_2$, то $x^3 \in \square_{\prec_w}(D)$. В противном случае остается

$$(1 + 2b_1^2 + 2b_1 + b_1^3)y + b_4x^2 + (-b_1b_4 - 2b_4 + b_2 + 2b_1b_2 + b_2b_1^3 + 2b_2b_1^2)x +$$
$$+ b_4(2 + b_1^2 + 2b_1).$$

Если теперь $b_1 \notin \{2, 4, 6\}$, то $\{y\} \subseteq \square_{\prec_w}(D)$. В противном случае, продолжая редукцию с помощью f_1, получаем $\#\,\mathrm{Supp}\,D \geqslant 3$.

Если же $b_2 = 0$, то после редукции с помощью f_2 остается

$$b_3x^3 + (1 + 2b_1 + b_1^3 + 2b_1^2)y + (b_4 - b_1b_3 - 2b_3)x^2 +$$
$$+ (-b_1b_4 - 2b_4 + 2b_3 + b_3b_1^2 + 2b_1b_3)x + b_4(2 + b_1^2 + 2b_1).$$

Если $b_3 \neq 0$, то $x^3 \in \square_{\prec_w}(D)$. В противном случае, если $b_3 = 0$ и $b_1 \notin \{2, 4, 6\}$, то $y \in \square_{\prec_w}(D)$. В противном случае, продолжая редукцию, получаем $\#\operatorname{Supp} D \geqslant 3$.

Если же $b_1 = 5$, то остается $b_2x^4 - 2xy + b_3x^3 + y + b_4x^2$. Если $b_2 \neq 0$, то, продолжая редукцию, получаем, что если $b_3 \neq 5b_2$, то $x^3 \in \square_{\prec_w}(D)$, а в противном случае $y \in \square_{\prec_w}(D)$. А если $b_2 = 0$, то в случае $b_3 \neq 0$ имеем $x^3 \in \square_{\prec_w}(D)$, а в противном случае $y \in \square_{\prec_w}(D)$.

Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то $\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 3$.

Во всех остальных случаях $\#\operatorname{Supp} D \geqslant 4$.

Следовательно, $d_2(C_3) \geqslant 3$. Это доказывает утверждение 2. Аналогично, пусть D' – подкод размерности 3 кода C_3, тогда при различных выборах D' получаем следующее:

- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7)\}$, то получаем $\{y, xy, x^2y\} \subseteq \subseteq \square_{\prec_w}(D')$. При этом согласно п. 3.1.3 имеем $x^3 \in \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 4$.
- Если $D' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то $\{x^2, x^3, xy, x^2y\} \subseteq \subseteq \square_{\prec_w}(D')$. Таким образом, $\#\operatorname{Supp} D' \geqslant 4$.
- Во всех остальных случаях $\#\operatorname{Supp} D' \geqslant 5$.

Следовательно, $d_3(C_3) \geqslant 4$. Это доказывает утверждение 3. Аналогично, пусть D'' – подкод размерности 4 кода C_3, тогда при различных выборах D'' получаем следующее:

- Если $D'' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_3 + I_7), \operatorname{ev}(f_4 + I_7)\}$, то получаем $\{x^2, x^3, y, xy, x^2y\} \subseteq \square_{\prec_w}(D'')$. Таким образом, $\#\operatorname{Supp} D'' \geqslant 5$.
- Если $D'' := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7), \operatorname{ev}(f_4 + I_7), \operatorname{ev}(f_5 + I_7)\}$, то получаем $\{x, x^2, x^3, xy, x^2y\} \subseteq \square_{\prec_w}(D'')$. Таким образом, $\#\operatorname{Supp} D'' \geqslant 5$.
- Во всех остальных случаях $\#\operatorname{Supp} D'' \geqslant 6$.

Следовательно, $d_4(C_3) \geqslant 5$. Это доказывает утверждение 4. ▲

Предложение 8. *Пусть* $C_4 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1+I_7), \operatorname{ev}(x+I_7), \operatorname{ev}(x^2+I_7), \operatorname{ev}(y+I_7), \operatorname{ev}(xy + I_7)\}$. *Тогда*

1. C_4 *является* $[7, 5, \geqslant 2]$-*кодом*;
2. $d_2(C_4) \geqslant 4$;
3. $d_3(C_4) \geqslant 5$;
4. $d_4(C_4) \geqslant 6$.

Предложение 9. *Пусть* $C_5 := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(1+I_7), \operatorname{ev}(x+I_7), \operatorname{ev}(x^2+I_7), \operatorname{ev}(y+I_7), \operatorname{ev}(x^2y + I_7)\}$. *Тогда*

1. C_5 *является* $[7, 5, \geqslant 2]$-*кодом*;
2. $d_2(C_5) \geqslant 4$;
3. $d_3(C_5) \geqslant 5$;
4. $d_4(C_5) \geqslant 6$.

Доказательство. Утверждение 1 следует из результатов § 4. Далее, рассмотрим следующие многочлены:

$$f_1 := x^2y + a_1y + a_2x^2 + a_3x + a_4, \quad f_2 := y + b_1x^2 + b_2x + b_3,$$
$$f_3 := x^2 + c_1x + c_2, \quad f_4 := x + d_1 \quad f_5 := 1,$$

где $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2, d_1 \in \mathbb{F}_7$. Пусть D – подкод размерности 2 кода C_5, тогда при различных выборах D получаем следующее.

Если $D := \operatorname{Span}_{\mathbb{F}_7}\{\operatorname{ev}(f_1 + I_7), \operatorname{ev}(f_2 + I_7)\}$, то $\{y, xy, x^2y\} \subseteq \square_{\prec_w}(D)$. При этом согласно п. 3.1.3 имеем $x^3 \in \square_{\prec_w}(D)$. Таким образом, $\#\operatorname{Supp} D \geqslant 4$.

Если $D := \mathrm{Span}_{\mathbb{F}_7}\{\mathrm{ev}(f_1 + I_7), \mathrm{ev}(f_3 + I_7)\}$, то $\{x^2, x^3, x^2y\} \subseteq \square_{\prec_w}(D)$. Далее,

$$yf_3 \xrightarrow{f_1} c_1xy + (c_2 - a_1)y - a_2x^2 - a_3x - a_4.$$

Если $c_1 \neq 0$, то $xy \in \square_{\prec_w}(D)$. В противном случае остается $(c_2-a_1)y-a_2x^2-a_3x-a_4$. Если $c_2 \neq a_1$, то $\{y, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае остается $-a_2x^2 - a_3x - a_4$. Если $a_2 \neq 0$, то

$$-a_2x^2y - a_3xy - a_4y \xrightarrow{f_1} -a_3xy + (-a_4 + a_1a_2)y + a_2^2x^2 + a_2a_3x + a_2a_4.$$

Если $a_3 \neq 0$, то $xy \in \square_{\prec_w}(D)$. В противном случае остается $(-a_4+a_1a_2)y+a_2^2x^2+a_2a_4$. Если $a_4 \neq a_1a_2$, то $\{y, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае

$$a_2^2x^2 + a_2^2a_1 \to x^3y + a_1xy \xrightarrow{x^3y-2x^2y+2xy-y} 2x^2y + (a_1 - 2)xy + y \xrightarrow{f_1}$$
$$\xrightarrow{f_1} (a_1 - 2)xy + (1 - 2a_1)y - 2a_2x^2 - 2a_1a_2.$$

Если $a_1 \neq 2$, то $xy \in \square_{\prec_w}(D)$. В противном случае $y \in \square_{\prec_w}(D)$.

Если же $a_2 = 0$, то в случае $a_3 \neq 0$ имеем $\{x, xy\} \subseteq \square_{\prec_w}(D)$. В противном случае, если $a_3 = 0$, то $\{1, x, y, xy\} \subseteq \square_{\prec_w}(D)$. Если теперь $a_4 = 0$, то непосредственными вычислениями убеждаемся, что $\#\,\mathrm{Supp}\,D \geqslant 4$.

Таким образом, $\#\,\mathrm{Supp}\,D \geqslant 4$.

Во всех остальных случаях $\#\,\mathrm{Supp}\,D \geqslant 5$.

Следовательно, $d_2(C_5) \geqslant 4$. Это доказывает утверждение 2. Остальные утверждения доказываются аналогично. ▲

§ 6. Заключение

В статье получено несколько кодов с наилучшими возможными параметрами, построенных по гиперэллиптической кривой над полем $\mathbb{F}_7$ с помощью техники из работы [4]. Также вычислены обобщенные веса Хэмминга этих кодов. Кроме того, для некоторых кодов установлено расстояние по парам символов. За исключением нескольких обобщенных весов Хэмминга, которые можно получить с помощью теоремы 2, полученные нижние границы нетривиальны.

Для построения классов хороших кодов этот метод можно также применять к примарным мономиальным аффинным эвалюационным кодам, построенным по другим кривым.

Авторы выражают благодарность рецензенту за замечания и предложения, способствовавшие улучшению изложения.

СПИСОК ЛИТЕРАТУРЫ

1. *Fitzgerald J., Lax R.F.* Decoding Affine Variety Codes Using Gröbner Bases // Des. Codes Cryptogr. 1998. V. 13. № 2. P. 147–158. https://doi.org/10.1023/A:1008274212057
2. *Geil O.* Evaluation Codes from an Affine Variety Code Perspective // Advances in Algebraic Geometry Codes. Singapore: World Sci., 2008. P. 153–180. https://doi.org/10.1142/9789812794017_0004
3. *Andersen H.E., Geil O.* Evaluation Codes from Order Domain Theory // Finite Fields Appl. 2008. V. 4. № 1. P. 92–123. https://doi.org/10.1016/j.ffa.2006.12.004
4. *Geil O., Özbudak F.* On Affine Variety Codes from the Klein Quartic // Cryptogr. Commun. 2019. V. 11. № 2. P. 237–257. https://doi.org/10.1007/s12095-018-0285-6
5. *Patanker N., Singh S.K.* Quaternary Affine Variety Codes over a Klein-like Curve. Preprint, 2020.

6. *Wei V.K.* Generalized Hamming Weights for Linear Codes // IEEE Trans. Inform. Theory. 1991. V. 37. № 5. P. 1412–1418. https://doi.org/10.1109/18.133259
7. *Grassl M.* Bounds on the Minimum Distance of Linear Codes and Quantum Codes (electronic tables). Available online at http://www.codetables.de.
8. *Cassuto Y., Blaum M.* Codes for Symbol-Pair Read Channels // IEEE Trans. Inform. Theory. 2011. V. 57. № 12. P. 8011–8020. https://doi.org/10.1109/TIT.2011.2164891
9. *Helleseth T., Kløve T., Mykkelveit J.* The Weight Distribution of Irreducible Cyclic Codes with Block Lengths $n_1((q^l-1)/N)$ // Discrete Math. 1977. V. 18. № 2. P. 179–211. https://doi.org/10.1016/0012-365X(77)90078-4
10. *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. https://doi.org/10.1016/0012-365X(78)90114-0

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

Поступила в редакцию
11.09.2020
После доработки
14.01.2021
Принята к публикации
19.01.2021