ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 56 **2020** **Вып. 4**

УДК 621.391 : 519.725

© 2020 г. **И.Ю. Могильных, Ф.И. Соловьева**

О БАЗИСАХ КОДОВ БЧХ С КОНСТРУКТИВНЫМ РАССТОЯНИЕМ 3 И ИХ РАСШИРЕНИЙ[1]

Рассматриваются коды БЧХ в узком смысле длины $p^m - 1$ над $\mathbb{F}_p$, $m \geqslant 3$. Доказано, что такой код с конструктивным расстоянием $\delta = 3$ и его расширение при $p \geqslant 5$ не порождаются множеством своих кодовых слов минимального ненулевого веса. Установлено, что расширенные коды БЧХ с конструктивным расстоянием $\delta = 3$ при $p \geqslant 3$ порождаются множеством слов веса 5, причем базисные векторы могут быть выбраны среди аффинных орбит некоторых кодовых слов.

Ключевые слова: код БЧХ, циклический код, аффинно-инвариантный код, базис минимального веса, аффинный порождающий элемент.

DOI: 10.31857/S0555292320040026

§ 1. Введение

Вопрос существования базиса, состоящего из векторов минимального или небольшого веса линейного кода, как компактного способа хранения информации, задающего код большой мощности, представляет интерес с точки зрения теории кодирования [1, § 3.2], а также теории тестов [2–4].

Так как циклический МДР-код достигает границы Синглтона, его порождающий многочлен имеет минимальный вес. Следовательно, существует базис из кодовых слов минимального веса для такого кода. К этим кодам относятся коды Рида–Соломона, а также некоторые другие связанные с ними коды [5, гл. 11, теоремы 9, 10].

Известно [5, теорема 10, гл. 13], что всякий код Рида–Маллера порождается словами минимального веса. Также базис, состоящий из векторов минимального веса, существует для q-ичных кодов Хэмминга вследствие их единственности для заданных параметров и леммы Глаголева (см. данный результат в работе [6] и аналогичный результат для q-ичного случая в [7]). Итеративная конструкция базисов из кодовых слов минимального веса для двоичного кода Хэмминга была получена в работе [8]. Отметим, что этот результат может быть обобщен на случай расширенных двоичных кодов Хэмминга и q-ичных кодов Хэмминга (со сходной схемой доказательства на основе конструкции Шонхайма). В [2] было доказано, что расширенные двоичные коды БЧХ в узком смысле достаточно большой длины порождаются множеством слов минимального веса.

С другой стороны, в работе [9] установлено, что совокупность слов минимального веса двоичного примитивного кода БЧХ с конструктивным расстоянием $2^{m-2} - 1$ совпадает с множеством слов минимального веса выколотого кода Рида–Маллера $RM(2, m)$.

[1] Работа выполнена при поддержке Министерства науки и высшего образования РФ (соглашение № 075-02-2020-1479/1).

В силу большей симметрии проблему существования базиса из кодовых слов минимального веса естественно рассматривать для расширенных кодов, к примеру, выдерживающих аффинные преобразования поля. Кодовое слово c аффинно-инвариантного кода называется *аффинным порождающим элементом* (single orbit affine generator, см. [4]), если орбита вектора c действия аффинной группы поля $\mathbb{F}_{p^m}$ содержит базис кода. Очевидно, аффинным порождающим элементом аффинно-инвариантного кода будет вектор, полученный расширением вектора, отвечающего порождающему многочлену выколотого циклического кода. Естественной представляется задача поиска аффинного порождающего элемента минимально возможного веса.

В [3] приводятся результаты, мотивирующие поиск аффинных порождающих элементов небольшого веса с позиций локальных тестирований. В работе [4] доказано, что двоичный расширенный код БЧХ в узком смысле с конструктивным расстоянием 5 имеет аффинный порождающий элемент минимального веса. В работе [10] авторами настоящей статьи были получены аффинные порождающие элементы минимального веса аффинно-инвариантных кодов, отвечающих функции Голда.

В данной статье исследуется вопрос существования аффинного порождающего элемента минимально возможного веса расширенного кода БЧХ над $\mathbb{F}_p$, $p \neq 2$. Отметим, что его структура для недвоичных кодов БЧХ с конструктивным расстоянием 3 существенно отличается от такового в двоичном случае (для двоичных расширенных кодов Хэмминга результат был получен в [4, следствие 8]).

В § 2 приводятся основные понятия и утверждения. В § 3 доказывается несуществование базисов, состоящих из векторов минимального веса для расширенных кодов БЧХ с конструктивным расстоянием 3 над $\mathbb{F}_p$ для любого простого p, $p \neq 2, 3$. В § 4 вводится понятие ранга кодового слова аффинно-инвариантного кода. Доказано, что ранг аффинного порождающего элемента веса 5 расширенного кода БЧХ с конструктивным расстоянием 3 равен 3. Ранг введен по аналогии с рангом кодового слова циклического кода [5, гл. 9, § 11], предложенным для определения минимального расстояния некоторых циклических кодов. Полученное ограничение на ранг неявно использовано при нахождении подходящего аффинного порождающего элемента в теореме 4. Отметим, что при $p = 3$ аффинный порождающий элемент имеет минимальный вес, поскольку кодовое расстояние кода равно 5, а при $p > 3$ имеет предминимальный вес, равный 5.

§ 2. Циклические и аффинно-инвариантные коды

Основные определения и обозначения см. в [5]. Линейный код называется *циклическим*, если циклический сдвиг любого его кодового слова является кодовым словом. В дальнейшем будем рассматривать лишь циклические коды длины $p^m - 1$ над простым полем $\mathbb{F}_p$. Для всякого ненулевого элемента β поля Галуа $\mathbb{F}_{p^m}$ справедливо $\beta^{p^m-1} = 1$. Элемент поля $\mathbb{F}_{p^m}$ называется *примитивным*, если его порядок равен $p^m - 1$. Координаты векторного пространства $\mathbb{F}_p^{p^m-1}$ перенумеруем числами $0, \ldots, p^m - 2$ и отождествим координату с номером i с элементом α^i, где $i \in \{0, \ldots, p^m - 2\}$ и α – примитивный элемент поля $\mathbb{F}_{p^m}$. *Циклотомическим классом элемента* $i \in \{0, \ldots, p^m - 2\}$ *по модулю* $p^m - 1$ называется множество

$$\mathrm{cl}(i) = \bigl\{ip^j \pmod{p^m - 1} : j \in \{0, \ldots, m-1\}\bigr\}.$$

Со всяким вектором $c = (c_0, \ldots, c_{p^m-2})$ в пространстве $\mathbb{F}_p^{p^m-1}$ отождествим многочлен $c(x) = \sum\limits_{i=0}^{p^m-2} c_i x^i$. Элемент поля $\mathbb{F}_{p^m}$ называется *нулем* p-ичного циклического кода длины $p^m - 1$, если он является корнем каждого его кодового многочлена. Известно, что множество нулей всякого циклического кода состоит из степеней примитивного элемента, пробегающих объединение некоторых циклотомических клас-

сов. Если $i_1, \ldots, i_\ell$ – представители некоторых циклотомических классов, то через $C_{i_1,\ldots,i_\ell}$ обозначим соответствующий циклический код

$$\{c(x):\ c(\alpha^j) = 0,\ j \in \mathrm{cl}(i_1) \cup \ldots \cup \mathrm{cl}(i_\ell)\}.$$

Согласно теореме о границе БЧХ, если найдется $\delta - 1$ подряд идущих степеней примитивного элемента α, являющихся нулями циклического кода, то кодовое расстояние в коде не меньше δ. Кодом с таким свойством является $C_{1,\ldots,\delta-1}$, именуемый *кодом БЧХ в узком смысле с конструктивным расстоянием* δ.

Для вектора $c = (c_0, \ldots, c_{p^m-2})$ длины $p^m - 1$ обозначим его расширение через $\bar{c}$, т.е.

$$\bar{c} = \left(c_0, \ldots, c_{p^m-2}, -\sum_{i=0}^{p^m-2} c_i\right).$$

Расширенный код $\{\bar{c}:\ c \in C\}$ обозначим через $\overline{C}$. В дальнейшем считаем, что добавляемая при расширении координата занумерована нулем поля Галуа $\mathbb{F}_{p^m}$. Таким образом, на координатных позициях векторного пространства $\mathbb{F}_p^{p^m}$ действует *аффинная группа поля* $\mathbb{F}_{p^m}$, состоящая из перестановок, которые могут быть описаны парами (γ, σ), а именно: $(\gamma, \sigma)(\beta) = \gamma\beta + \sigma$, где $\gamma, \sigma \in \mathbb{F}_{p^m}$, $\gamma \neq 0$, относительно операции композиции. Код длины p^m над $\mathbb{F}_p$ называется *аффинно-инвариантным*, если аффинная группа поля $\mathbb{F}_{p^m}$ оставляет на месте множество кодовых слов этого кода.

Пусть $i \in \{0, \ldots, p^m - 1\}$. Через I обозначим вектор, представляющий число i в p-ичной системе счисления, т.е. $i = \sum_{s=0}^{m-1} I_s p^s$. Пусть J и I – записи чисел j и i, соответственно, в p-ичной системе счисления. Обозначим $j \prec i$, если $J_s \leqslant I_s$ для всех $s \in \{0, \ldots, m-1\}$. Следующая теорема характеризует аффинно-инвариантные коды.

Теорема 1 [11]. *Пусть C – циклический код длины $p^m - 1$. Если α^i – нуль кода C и для всякого ненулевого j, $j \prec i$, элемент α^j является нулем кода C, тогда код $\overline{C}$ является аффинно-инвариантным. Верно и обратное.*

Следствие 1. *Расширенный код БЧХ $\overline{C_{1,2,\ldots,\delta-1}}$ для всякого $\delta \geqslant 2$, а также код $\overline{C_{1,2,p^2+1}}$ являются аффинно-инвариантными.*

В дальнейшем нам понадобится следующий факт.

Предложение. *Пусть конструктивное расстояние кода БЧХ в узком смысле совпадает с кодовым расстоянием d. Тогда расширение этого кода имеет кодовое расстояние $d + 1$.*

Доказательство. Предположим, что $\bar{c}$ – кодовое слово веса d расширенного кода БЧХ $\overline{C_{1,\ldots,d-1}}$. Тогда $c = (c_0, \ldots, c_{p^m-2})$ – кодовое слово веса d кода $C_{1,\ldots,d-1}$, а $\{i_1, \ldots, i_d\}$ – множество позиций ненулевых символов слова c, такое что

$$\sum_{j=1}^{d} c_{i_j} = 0.$$

Так как $c \in C_{1,\ldots,d-1}$, то

$$\sum_{j=1}^{d} c_{i_j} \alpha^{\ell i_j} = 0$$

для всех $\ell \in \{1, \ldots, d-1\}$. Учитывая, что матрица системы относительно неизвестных $c_{i_1}, \ldots, c_{i_d}$ является матрицей Вандермонда, и следовательно, невырождена, имеем $c_{i_1} = c_{i_2} = \ldots = c_{i_d} = 0$, противоречие. ▲

Кодовое расстояние кодов БЧХ и других кодов с двумя нулями было получено в работе [12]. При $p = 3$ имеем $C_{1,2} = C_{1,2,3}$, откуда в силу границы БЧХ кодовое расстояние $C_{1,2}$ равно 4. Отсюда получаем

Следствие 2. *Кодовое расстояние кода БЧХ $C_{1,2}$ равно 3 при всех простых p, $p \neq 3$, и равно 4 при $p = 3$. Расширения этих кодов имеют кодовые расстояния 4 и 5 соответственно.*

§ 3. Несуществование базисов кодов $C_{1,2}$ и $\overline{C_{1,2}}$ из слов минимального веса

Лемма 1. *Пусть $c \in C_2$ – такое кодовое слово, что для всякого i, для которого $c_i \neq 0$, имеет место $\alpha^i \in \mathbb{F}_p$. Тогда $c \in C_{2,p^2+1}$.*

Доказательство. Так как $c \in C_2$, то

$$\sum_{i \in \{0,\ldots,p^m-2\}:\, c_i \neq 0} c_i \alpha^{2i} = 0.$$

По условию леммы для всякого i, для которого $c_i \neq 0$, имеет место $\alpha^i \in \mathbb{F}_p$, откуда $\alpha^{ip^2} = \alpha^i$. Следовательно,

$$\sum_{i \in \{0,\ldots,p^m-2\}:\, c_i \neq 0} c_i \alpha^{(p^2+1)i} = \sum_{i \in \{0,\ldots,p^m-2\}:\, c_i \neq 0} c_i \alpha^{2i} = 0,$$

другими словами, α^{p^2+1} является корнем $c(x)$, который, в свою очередь, принадлежит C_{2,p^2+1}. ▲

Теорема 2. *Множество кодовых слов кода $C_{1,2}$ веса 3 содержится в $C_{1,2,p^2+1}$.*

Доказательство. Без ограничения общности имеем $c(x) = 1 + ax^i + bx^j$, $c(x) \in C_{1,2}$, где a, b – ненулевые элементы поля Галуа $\mathbb{F}_p$. По определению кода БЧХ выполнены проверочные соотношения

$$1 + a\alpha^i + b\alpha^j = 0, \tag{1}$$

$$1 + a\alpha^{2i} + b\alpha^{2j} = 0. \tag{2}$$

Покажем, что α^{p^2+1} является корнем многочлена $c(x)$, т.е.

$$1 + a\alpha^{(p^2+1)i} + b\alpha^{(p^2+1)j} \tag{3}$$

равно нулю. Возможны следующие случаи.

Случай 1. Пусть $b = -a$. Используя это равенство и подставляя выражение для α^j из (1) в (2), получаем $a - 1 - 2a\alpha^i = 0$. Таким образом, α^i и, следовательно, α^j принадлежат $\mathbb{F}_p$. Отсюда и из леммы 1 получаем требуемое.

Случай 2. Пусть $a + b \neq 0$. Обозначим $a + b$ через $-f^{-1}$. Преобразуем (1) и (2), используя замену

$$\alpha^i = by_i + f, \quad \alpha^j = ay_j + f. \tag{4}$$

Из (1) после преобразований имеем $y_i = -y_j$. Отсюда с учетом (2) и $a + b = -f^{-1}$ получаем

$$y_i^2 ab(a + b) = f - 1. \tag{5}$$

Преобразуем выражение (3), произведя замену (4) и принимая во внимание равенства $y_i = -y_j$, $a^{p^2} = a$ и $b^{p^2} = b$:

$$
\begin{aligned}
&1 + a\alpha^{(p^2+1)i} + b\alpha^{(p^2+1)j} = \\
&= 1 + a(by_i + f)^{p^2}(by_i + f) + b(-ay_i + f)^{p^2}(-ay_i + f) = \\
&= 1 + a(by_i^{p^2} + f)(by_i + f) + b(-ay_i^{p^2} + f)(-ay_i + f) = \\
&= 1 + ab(a + b)y_i^{p^2+1} + f^2(a + b).
\end{aligned}
$$

Из полученного выражения согласно обозначению $a + b = -f^{-1}$ получаем

$$y_i^{p^2+1}ab(a + b) + 1 - f.$$

Однако $(p^2 + 1)/2 = (p - 1)(p + 1)/2 + 1$, и так как из (5) следует, что $y_i^2 \in \mathbb{F}_p$, то

$$(y_i^2)^{(p^2+1)/2} = y_i^2.$$

Таким образом, приходим к выводу, что выражение (3) преобразуется в $y_i^2 ab(a+b)+$ $+1 - f$. Из (5) следует, что α^{p^2+1} является корнем $c(x)$. ▲

Следствие 3. *Для любого простого p, не равного 2 или 3, код $C_{1,2}$ и расширенный код $\overline{C_{1,2}}$ не порождаются множествами кодовых слов минимального ненулевого веса.*

Доказательство. В силу следствия 2 минимальные расстояния кодов $C_{1,2}$ и $\overline{C_{1,2}}$ равны 3 и 4 соответственно. Число $p^2 + 1$ не принадлежит циклотомическим классам $\mathrm{cl}(1) = \{p^i : i \in \{0, \ldots, m - 1\}\}$ и $\mathrm{cl}(2) = \{2p^i : i \in \{0, \ldots, m - 1\}\}$, следовательно, $C_{1,2,p^2+1}$ является собственным подкодом кода $C_{1,2}$. Из теоремы 2 заключаем, что все слова веса 3 кода $C_{1,2}$ содержатся в $C_{1,2,p^2+1}$.

Рассмотрим расширенные коды. Пусть $\bar{c}$ – кодовое слово веса 4 кода $\overline{C_{1,2}}$, полученное добавлением общей проверки на четность к кодовому слову c кода $C_{1,2}$. Покажем, что вектор $\bar{c}$ принадлежит коду $\overline{C_{1,2,p^2+1}}$. Пусть c имеет вес 4, т.е. в позиции вектора $\bar{c}$, занумерованной нулем поля $\mathbb{F}_{p^m}$, стоит символ 0. Пусть для некоторого i в позиции вектора $\bar{c}$, занумерованной элементом α^i, стоит ненулевой символ. В силу того, что аффинная группа поля действует 2-транзитивно на координатных позициях $\bar{c}$, найдется аффинное преобразование, меняющее местами позиции, занумерованные элементами 0 и α^i. Другими словами, представитель $\overline{c'}$ аффинной орбиты кодового слова $\bar{c}$ может быть выбран таким, что c' имеет вес 3 и $\sum\limits_{i=0}^{p^m-2} c'_i \neq 0$. В силу следствия 1 коды $\overline{C_{1,2}}$ и $\overline{C_{1,2,p^2+1}}$ аффинно-инвариантны, поэтому c и c' или содержатся в этих кодах одновременно, или одновременно не содержатся. Из теоремы 2 заключаем, что векторы $\overline{c'}$ и, следовательно, $\bar{c}$ принадлежат $\overline{C_{1,2,p^2+1}}$. ▲

§ 4. Базис кода $\overline{C_{1,2}}$ веса 5

4.1. Ранг аффинного порождающего элемента. *Рангом* вектора $\bar{c} \in \mathbb{F}_p^{p^m}$ назовем размерность векторного пространства над $\mathbb{F}_p$, натянутого на носитель вектора c, т.е. $\{\alpha^i : i \in \{0, \ldots, p^m - 2\},\ c_i \neq 0\}$.

Теорема 3. *Пусть c – кодовое слово кода $C_{1,2}$ веса 4 и $\bar{c}$ – аффинный порождающий элемент кода $\overline{C_{1,2}}$. Тогда $\bar{c}$ имеет вес 5 и ранг 3.*

Доказательство. По следствию 3 аффинный порождающий элемент кода $\overline{C_{1,2}}$ имеет вес не меньше 5. Пусть слово $\bar{c}$ веса 5 является аффинным порождающим

элементом кода $\overline{C_{1,2}}$. Так как вес c равен 4 и $c \in C_1$, то ранг $\bar{c}$ не превосходит 3. Если ранг $\bar{c}$ равен 1, то по лемме 1 вектор $\bar{c}$ принадлежит аффинно-инвариантному коду $\overline{C_{1,2,p^2+1}}$, являющемуся собственным подкодом кода $\overline{C_{1,2}}$. Следовательно, кодовое слово $\bar{c}$ не является аффинным порождающим элементом кода $\overline{C_{1,2}}$.

Пусть $c(x) = h + ax^i + bx^j + fx^k$ и кодовое слово $\bar{c}$ имеет ранг 2. Так как ранг $\bar{c}$ равен 2, то

$$\alpha^j = s + t\alpha^i, \quad \alpha^k = u + v\alpha^i$$

для некоторых элементов s, t, u, v поля Галуа $\mathbb{F}_p$.

Так как $c \in C_2$, то

$$\begin{aligned} &c(\alpha^2) = h + a\alpha^{2i} + b(s + t\alpha^i)^2 + f(u + v\alpha^i)^2 = \\ &= h + a\alpha^{2i} + bs^2 + 2bst\alpha^i + bt^2\alpha^{2i} + fu^2 + 2fuv\alpha^i + fv^2\alpha^{2i} = \\ &= a\alpha^{2i}(a + t^2b + v^2f) + 2\alpha^i(stb + uvf) + h + bs^2 + fu^2 = 0. \end{aligned} \tag{6}$$

Последнее равенство имеет место в случае тождества, т.е.

$$a + t^2b + v^2f = stb + uvf = h + bs^2 + fu^2 = 0, \tag{7}$$

или если $\alpha^i \in \mathbb{F}_{p^2}$.

Покажем, что $c(x) \in C_{1,2,p^2+1}$. Учитывая, что элементы s, t, u, v принадлежат простому полю $\mathbb{F}_p$, имеем

$$\begin{aligned} &c(\alpha^{p^2+1}) = h + a\alpha^{i(p^2+1)} + b(s + t\alpha^i)^{p^2+1} + f(u + v\alpha^i)^{p^2+1} = \\ &= a\alpha^{(p^2+1)i}(a + t^2b + v^2f) + (\alpha^{ip^2} + \alpha^i)(stb + uvf) + h + bs^2 + fu^2. \end{aligned}$$

Из этого выражения для $c(\alpha^{p^2+1})$ заключаем, что если выполнено условие (7), то $c(\alpha^{p^2+1}) = 0$. Если $\alpha^i \in \mathbb{F}_{p^2}$, то $\alpha^{ip^2} = \alpha^i$, и выражение для $c(\alpha^{p^2+1})$ совпадает с выражением для $c(\alpha^2)$ из (6), а следовательно, кодовое слово $\bar{c}$ из $\overline{C_{1,2,p^2+1}}$ не является аффинным порождающим элементом кода $\overline{C_{1,2}}$. ▲

4.2. Явный вид аффинного порождающего элемента. В следующей лемме найдем подходящий для дальнейших рассмотрений кодовый многочлен кода $C_{1,2}$.

Лемма 2. *Пусть α – примитивный элемент поля Галуа $\mathbb{F}_{p^m}$, $p, m \geqslant 3$. Тогда циклический код $C_{1,2}$ длины $p^m - 1$ содержит многочлен*

$$c(x) = 2 + x^i + x^j - 2x^k,$$

где i, j, k удовлетворяют условиям

$$\alpha^i = \alpha + 2^{-1}\alpha^2, \quad \alpha^j = -\alpha + 2^{-1}\alpha^2, \quad \alpha^k = 1 + 2^{-1}\alpha^2. \tag{8}$$

Доказательство. Справедливы следующие равенства:

$$\begin{aligned} &c(\alpha) = 2 + \alpha^i + \alpha^j - 2\alpha^k = 2 + \alpha + 2^{-1}\alpha^2 - \alpha + 2^{-1}\alpha^2 - 2 - \alpha^2 = 0, \\ &c(\alpha^2) = 2 + \alpha^{2i} + \alpha^{2j} - 2\alpha^{2k} = \\ &= 2 + \alpha^2 + 2^{-2}\alpha^4 + \alpha^3 + \alpha^2 + 2^{-2}\alpha^4 - \alpha^3 - 2 - 2^{-1}\alpha^4 - 2\alpha^2 = 0. \end{aligned}$$

Так как $c(\alpha) = c(\alpha^2) = 0$, то $c(x) \in C_{1,2}$. ▲

Обозначим многочлен

$$2 + (x + 2^{-1}x^2)^{sp^\ell + t} + (-x + 2^{-1}x^2)^{sp^\ell + t} - 2(1 + 2^{-1}x^2)^{sp^\ell + t}$$

через $P_{\ell,s,t}(x)$. Если i,j,k удовлетворяют (8) для $\alpha \in \mathbb{F}_{p^m}$ и $c(x)$ – многочлен, указанный в лемме 2, то $c(\alpha^{sp^\ell+t}) = P_{\ell,s,t}(\alpha)$.

Лемма 3. *Многочлен $P_{\ell,s,t}(x)$ не является тождественно нулевым при любых $s,t \in \{1,2\}$ и любых $\ell \in \{1,2,\ldots,m-1\}$, а также при $\ell = s = 0$, $t \in \{3,\ldots,p-1\}$.*

Доказательство. Коэффициент при x^2 произвольного многочлена $P_{\ell,s,t}(x)$ при указанных в формулировке ограничениях на ℓ,s,t является ненулевым. Действительно, при раскрытии скобок в слагаемых многочлена $P_{\ell,s,t}(x)$ только в последнем слагаемом имеем коэффициент при x^2, равный $-(sp^\ell+t)$. ▲

Теорема 4. *Для любого простого $p \geqslant 3$ и любого $m \geqslant 3$ существует примитивный элемент α поля Галуа $\mathbb{F}_{p^m}$, такой что слово $\bar{c}$, где*

$$c(x) = 2 + x^i + x^j - 2x^k$$

и i,j,k удовлетворяют условиям (8), *является аффинным порождающим элементом кода $\overline{C_{1,2}}$ длины $n = p^m$.*

Доказательство. Согласно лемме 2 вектор $\bar{c}$ принадлежит коду $\overline{C_{1,2}}$. Докажем, что существует примитивный элемент α поля $\mathbb{F}_{p^m}$, такой что аффинная орбита слова $\bar{c}$ порождает код $\overline{C_{1,2}}$, а координатные позиции кода $C_{1,2}$ перенумерованы степенями элемента α.

Пусть $\bar{D}$ – расширенный циклический код, являющийся линейной оболочкой аффинной орбиты вектора $\bar{c}$, и $\bar{D} \subsetneq \overline{C_{1,2}}$. Докажем, что множества нулей кодов $C_{1,2}$ и D совпадают.

Пусть α^r – нуль многочлена $c(x)$, где r – минимальное число относительно порядка $\prec$, такое что $r \notin \mathrm{cl}(1) \cup \mathrm{cl}(2)$. По определению циклотомического класса без ограничения общности r можно полагать не делящимся на p. Рассмотрим вектор R, являющийся p-ичным представлением числа r. Согласно теореме 1 возможны два случая: либо вектор $R = (t,0,\ldots,0)$ имеет вес 1, где $t \in \{3,\ldots,p-1\}$, либо $R = (t,0,\ldots,0,s,0,\ldots,0)$ имеет вес 2, т.е. $r = sp^\ell + t$, где $s,t \in \{1,2\}$, $\ell \in \{1,\ldots,m-1\}$. Предположим, что во втором случае ℓ больше, чем $\lfloor m/2 \rfloor$, где $\alpha^{sp^\ell+t}$ – корень многочлена $c(x)$. Тогда

$$\alpha^{(sp^\ell+t)p^{m-\ell}} = \alpha^{tp^{m-\ell}+s}$$

является корнем $c(x)$, поскольку $sp^\ell + t$ и $tp^{m-\ell} + s$ принадлежат одному и тому же циклотомическому классу. Следовательно, во втором случае достаточно рассмотреть $\ell \in \{1,\ldots,\lfloor m/2 \rfloor\}$.

Покажем, что найдется примитивный элемент α, не являющийся корнем многочлена

$$P_{\ell,s,t}(x) = c(x^{sp^\ell+t})$$

для любых s,t,ℓ, таких что $s = \ell = 0$, $t \in \{3,\ldots,p-1\}$ или $t,s \in \{1,2\}$, $\ell \in \{1,\ldots,\lfloor m/2 \rfloor\}$.

Для этого рассмотрим многочлен

$$Q(x) = \left(\prod_{t=3}^{p-1} P_{0,0,t}(x)\right)\left(\prod_{\ell=1}^{\lfloor m/2 \rfloor} \prod_{1 \leqslant s,t \leqslant 2} P_{\ell,s,t}(x)\right). \tag{9}$$

Так как по лемме 3 многочлены $P_{\ell,s,t}$ не являются тождественно нулевыми, то и многочлен Q не тождественно нулевой. Убедимся, что степень $\deg(Q)$ многочлена Q меньше числа всех примитивных элементов поля $\mathbb{F}_{p^m}$.

Из определения многочлена $P_{\ell,s,t}$ имеем

$$\deg(P_{\ell,s,t}) \leqslant 2sp^{\ell} + 2t.$$

Отсюда и из (9) получаем

$$\deg(Q) \leqslant (p+2)(p-3) + 12\frac{p^{\lfloor m/2 \rfloor + 1} - p}{p-1} + 6m. \tag{10}$$

Покажем, что $\deg(Q) < \varphi(p^m - 1)$ начиная с некоторого достаточно большого m, где $\varphi(p^m - 1)$ – число всех примитивных элементов поля Галуа $\mathbb{F}_{p^m}$. Учитывая хорошо известное неравенство для функции Эйлера φ

$$\varphi(n) > \frac{n}{\ln n} \cdot \frac{\ln 2}{2},$$

при $n = p^m - 1$ получаем

$$\varphi(p^m - 1) > \frac{p^m - 1}{\ln(p^m - 1)} \cdot \frac{\ln 2}{2}. \tag{11}$$

Сравнивая нижнюю оценку (11) для $\varphi(p^m - 1)$ с верхней оценкой (10) степени $\deg(Q)$ многочлена $Q(x)$, нетрудно видеть, что

$$\varphi(p^m - 1) > \deg(Q) \tag{12}$$

начиная с некоторого достаточно большого m. Следовательно, найдется примитивный элемент α в $\mathbb{F}_{p^m}$, такой что $Q(\alpha) \neq 0$, и значит, $D = C_{1,2}$.

В частности, (12) выполняется для всех простых $p \geqslant 101$ и любого $m \geqslant 3$. Для каждого простого $p < 101$ и $m \geqslant 3$, для которых (12) не выполняется, с помощью компьютера был найден примитивный элемент α, такой что $Q(\alpha) \neq 0$.

Следовательно, $D = C_{1,2}$, и кодовое слово $\bar{c}$ является аффинным порождающим элементом кода $\overline{C_{1,2}}$ длины $n = p^m$ для любого $m \geqslant 3$. ▲

Задача нахождения аффинного порождающего элемента наименьшего возможного веса оказалась достаточно трудной для расширенных кодов БЧХ и далека от своего полного решения для всех значений конструктивного расстояния. Открытой и сложной проблемой представляется поиск аффинного порождающего элемента для двоичных расширенных циклических кодов из различных APN-мономов [13] (напомним что в [10] получено решение этой задачи для функции Голда), а также расширенного двоичного кода БЧХ $\overline{C_{1,3,5}}$. В работе [14] установлено, что класс циклических кодов, получаемых из APN-мономов над троичными полями, имеет максимальное кодовое расстояние 4. В этой связи задача существования базиса из кодовых слов минимального веса может быть естественным образом сформулирована, например, для троичных аффинно-инвариантных кодов $\overline{C_{1,4}}$ длины 3^m при нечетных m.

Авторы выражают свою благодарность рецензенту за ряд замечаний и предложений, позволивших улучшить изложение статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Charpin P.* Open Problems on Cyclic Codes // Handbook of Coding Theory. Amsterdam: Elsevier, 1998. V. 1. Ch. 11. P. 965–1063.
2. *Kaufman T., Litsyn S.* Almost Orthogonal Linear Codes Are Locally Testable // Proc. 2005 46th Annu. IEEE Symp. on Foundations of Computer Science (FOCS'05). Pittsburgh, PA, USA. October 23–25, 2005. P. 317–326.

3. *Kaufman T., Sudan M.* Algebraic Property Testing: The Role of Invariance // Proc. 40th Annu. ACM Symp. on Theory of Computing (STOC'08). Victoria, BC, Canada. May 17–20, 2008. New York: ACM, 2008. P. 403–412.
4. *Grigorescu E., Kaufman T.* Explicit Low-Weight Bases for BCH Codes // IEEE Trans. Inform. Theory. 2011. V. 58. № 2. P. 78–81.
5. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
6. *Курляндчик Я.М.* О логарифмической асимптотике длины максимального цикла разброса $r > 2$ // Дискретный анализ. Новосибирск: Инст. матем. СО АН СССР, 1971. Вып. 19. С. 48–55.
7. *Simonis J.* On Generator Matrices of Codes // IEEE Trans. Inform. Theory. 1992. V. 38. № 2. P. 516–516.
8. *Соловьева Ф.И.* О факторизации кодообразующих д.н.ф. // Методы дискретного анализа в исследовании функциональных схем. Новосибирск: Инст. матем. СО АН СССР, 1988. Вып. 47. С. 66–88.
9. *Augot D., Charpin P., Sendrier N.* Studying the Locator Polynomials of Minimum Weight Codewords of BCH Codes // IEEE Trans. Inform. Theory. 1992. V. 38. № 3. P. 960–973.
10. *Mogilnykh I.Yu., Solov'eva F.I.* On Explicit Minimum Weight Bases for Extended Cyclic Codes Related to Gold Functions // Des. Codes Cryptogr. 2018. V. 86. № 11. P. 2619–2627.
11. *Kasami T., Lin S., Peterson W.W.* Some Results on Cyclic Codes Which Are Invariant under the Affine Group and Their Applications // Inform. Control. 1967. V. 11. № 5–6. P. 475–496.
12. *Charpin P., Tietäväinen A., Zinoviev V.* On the Minimum Distances of Non-binary Cyclic Codes // Des. Codes Cryptogr. 1999. V. 17. № 1–3. P. 81–85.
13. *Carlet C., Charpin P., Zinoviev V.* Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems // Des. Codes Cryptogr. 1998. V. 15. № 2. P. 125–156.
14. *Ding C., Helleseth T.* Optimal Ternary Cyclic Codes from Monomials // IEEE Trans. Inform. Theory. 2013. V. 59. № 9. P. 5898–5904.

Могильных Иван Юрьевич
Региональный научно-образовательный математический центр,
Томский государственный университет
Институт математики им. С.Л. Соболева СО РАН
Новосибирский Государственный университет
ivmog@math.nsc.ru
Соловьева Фаина Ивановна
Институт математики им. С.Л. Соболева СО РАН
Новосибирский государственный университет
sol@math.nsc.ru

Поступила в редакцию
10.07.2020
После доработки
26.10.2020
Принята к публикации
27.10.2020