Д. В. Зиновьев, П. Соле, Четверичные коды и двухфазные последовательности, полученные из кодов над $\mathbb{Z}_8$, *Пробл. передачи информ.*, 2004, том 40, выпуск 2, 50–62

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 40 2004 Вып. 2

УДК 621.391.15

© 2004 г. Д.В. Зиновьев[1], П. Соле

ЧЕТВЕРИЧНЫЕ КОДЫ И ДВУХФАЗНЫЕ ПОСЛЕДОВАТЕЛЬНОСТИ, ПОЛУЧЕННЫЕ ИЗ КОДОВ НАД $\mathbb{Z}_8$

Построено новое семейство четверичных циклических кодов, полученных из констациклических кодов над $\mathbb{Z}_8$ с константой 5 с помощью композиции отображения Карле с отображением, обратным к отображению Грея. Мотивацией к написанию статьи послужило семейство четверичных кодов, построенное Шанбагом, Кумаром и Хеллесетом, улучшающее характеристики кодов Дельсарта – Геталса. Мы полагаем, что эти коды над $\mathbb{Z}_4$ являются нелинейными. В качестве приложения построены новые семейства четырех- и двухфазных последовательностей.

§ 1. Введение

Пионерские работы [1, 2] и работа [3], получившая широкую известность, вызвали интерес к четверичным кодам, т.е. к кодам над алфавитом из четырех элементов. Соответствующий интерес вызвало построение семейства четверичных последовательностей большой мощности, основанное на кодах Дельсарта – Геталса [4]. Соответствующее семейство кодов было улучшено в [5] с помощью локальных оценок Вейля [6].

Целью настоящей статьи является построение кодов над кольцом $\mathbb{Z}_4$ с аналогичными характеристиками, но с меньшей линейностью. Мы рассматриваем аналог конструкции [5] над кольцом $\mathbb{Z}_8$. В частности, мы определяем отображение Z кольца $\mathbb{Z}_8$ в кольцо $\mathbb{Z}_4 \times \mathbb{Z}_4$. Это отображение является композицией отображения Карле [7] с отображением, обратным к отображению Грэя. Оно является масштабной изометрией (см. [8]) однородного веса с весом Ли. Оно отображает констациклические коды с константой 5 в циклические коды и совпадает с отображением ϕ^2 из [9]. Комбинируя оценку Вейля со свойствами нашего отображения Z, можно получить оценку снизу минимального расстояния Ли четверичных кодов, являющихся образами $\mathbb{Z}_8$-кодов при отображении Z. Так как эти четверичные коды могут быть в принципе нелинейными, необходимо провести спектральный анализ отображения Z, аналогичный анализу отображения MSB (в наиболее значимый бит) в [10]. Из этого мы получаем оценки для корреляции соответствующей четверичной последовательности.

Статья организована следующим образом. В § 2 изложен необходимый материал из теории колец Галуа. В § 3 изучаются свойства отображения Грея. В § 4 вводятся канонические многочлены над кольцами Галуа, которые затем используются в § 5 при построении кодов над $\mathbb{Z}_8$. В §§ 6 и 7 оцениваются корреляции четверичной и двоичной последовательностей. И наконец, в § 8 мы рассматриваем последовательности с удвоенным периодом в случае четного расширения $\mathbb{Z}_8$.

[1] Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (номер проекта 03-01-00098).

§ 2. Предварительные результаты

2.1. Кольцо Галуа характеристики 8. На протяжении всей статьи $n = 2^m$. Пусть $R = GR(8, m)$ – кольцо Галуа характеристики 8, содержащее 8^m элементов, ξ – порождающий элемент кольца R, т.е. $\mathrm{ord}(\xi) = n - 1$. Имеет место $\xi^{n-1} = 1$ и $\xi^{n'} \neq 1$ при $0 < n' < n - 1$. Тогда множество Тейхмюллера для кольца R определяется следующим образом:

$$\mathcal{T} = \{0\} \cup \{\xi^j,\ j = 0, 1, \ldots, n-2\}.$$

Для любого элемента $x \in R$ справедливо 2-адическое разложение

$$x = u + 2v + 4w,$$

где $u, v, w \in \mathcal{T}$. Для такого x определим оператор Фробениуса

$$F(u + 2v + 4w) = u^2 + 2v^2 + 4w^2$$

и след из кольца $GR(8, m)$ в кольцо $\mathbb{Z}_8$

$$\mathrm{Tr}(x) := \sum_{j=0}^{m-1} F^j(x).$$

Аналогично, пусть tr – след относительно расширения полей $\mathbb{F}_{2^m}/\mathbb{F}_2$, и пусть $y \in \in \mathbb{F}_{2^m}$. Тогда

$$\mathrm{tr}(y) := \sum_{j=0}^{m-1} y^{2^j}.$$

Положим $\beta = 5\xi$. Поскольку в кольце $\mathbb{Z}_8$ выполняется равенство $5^2 = 1$, получаем

$$\beta^{n-1} = (5\xi)^{n-1} = 5,$$

и следовательно, $\beta^{2(n-1)} = 1$.

Заметим, что элемент β играет центральную роль в построении констациклических кодов длины $n - 1$ с константой 5.

2.2. Локальная граница Вейля. Напомним теорему 1 из [6]. Пусть $f(x) \in R[x]$, т.е. $f(x)$ – многочлен с коэффициентами из кольца $GR(8, m)$. Тогда, применяя 2-адическое разложение для коэффициентов, имеем

$$f(x) = F_0(x) + 2F_1(x) + 4F_2(x).$$

Обозначим через n_i степень многочлена $F_i(x)$ относительно x. Для произвольного многочлена $f(x)$ его *взвешенную степень* обозначим

$$D_f = \max\{4n_0, 2n_1, n_2\}.$$

Пусть ψ – произвольный аддитивный характер кольца $GR(8, m)$. В обозначениях, введенных выше, при несущественных дополнительных условиях (см. [6]) имеет место следующая оценка:

$$\left| \sum_{x \in \mathcal{T}} \psi(f(x)) \right| \leq (D_f - 1)\sqrt{2^m}.$$

§ 3. Определение отображения Z

Пусть $\omega = e^{2\pi i/8} = (1 + i)/\sqrt{2}$, $i = \sqrt{-1}$, – примитивный корень восьмой степени из единицы, принадлежащий полю комплексных чисел. Пусть ψ_l – аддитивный характер кольца $\mathbb{Z}_8$ такой, что $\psi_l(x) = \omega^{lx}$.

Для любого $\boldsymbol{x} = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}_8^k$, где $k \geq 1$ – целое число, положим

$$\theta_8(\boldsymbol{x}) = \sum_{j=1}^{k} \omega^{x_j} \in L = \mathbb{Q}(i, \omega).$$

Поскольку поле $\mathbb{Q}(i, \omega)$ является алгебраическим расширением поля рациональных чисел $\mathbb{Q}$, порожденным элементами i и ω, где $i = \omega^4$, имеем $L = \mathbb{Q}(i, \omega) = \mathbb{Q}(\omega)$. Для любого вектора $\boldsymbol{y} = (y_1, y_2, \ldots, y_r) \in \mathbb{Z}_4^r$, где $r \geq 1$ – целое число, положим

$$\theta_4(\boldsymbol{y}) = \sum_{j=1}^{r} i^{y_j} \in K = \mathbb{Q}(i).$$

Заметим, что $[L : K] = 2$ и нетривиальный элемент группы Галуа $\mathrm{Gal}(L/K)$ отображает ω в $\omega^5 = -\omega$. Таким образом, для любого $a + \omega b \in L$ имеем

$$\mathrm{Tr}_{L/K}(a + \omega b) = (a + \omega b) + (a - \omega b) = 2a \in K.$$

Определение 1. *Зададим отображение Z из кольца $\mathbb{Z}_8$ в кольцо $\mathbb{Z}_4 \times \mathbb{Z}_4$ следующим образом. Для произвольного элемента $a_0 + 2a_1 + 4a_2 \in \mathbb{Z}_8$, где $a_0, a_1, a_2 \in \in \mathbb{Z}_2$, положим*

$$Z(a_0 + 2a_1 + 4a_2) = (a_1 + 2(a_0 + a_2), a_1 + 2a_2) \in \mathbb{Z}_4 \times \mathbb{Z}_4. \tag{1}$$

Кроме того, в кольце $\mathbb{Z}_8$ справедливо равенство

$$5(a_0 + 2a_1 + 4a_2) = a_0 + 2a_1 + 4(a_0 + a_2),$$

а по определению отображения Z имеем

$$Z(5(a_0 + 2a_1 + 4a_2)) = (a_1 + 2a_2, a_1 + 2(a_0 + a_2)). \tag{2}$$

Обозначим через T оператор сдвига для $\mathbb{Z}_4 \times \mathbb{Z}_4$. Тогда для любого $a \in \mathbb{Z}_8$ справедливо

$$Z(5a) = T \circ Z(a).$$

Напомним, что впервые понятие *однородного веса* было введено в [11] как отображение w: $\mathbb{Z}_m \to \mathbb{R}$, удовлетворяющее следующим свойствам:
$(W1)$ для любого $x \in \mathbb{Z}_m$: $w(x) = 0 \iff x = 0$,
$(W2)$ для любого $x \in \mathbb{Z}_m \backslash \{0\}$: $w(x) = w(d_x)$,
$(W3)$ для любого $x, y \in \mathbb{Z}_m$: $w(x + y) \leq w(x) + w(y)$,
$(W4)$ для любого $x \in \mathbb{Z}_m \backslash \{0\}$: $d_x w(x) = m\phi(m')$,
где d_x – наименьшее общее кратное чисел x и m, ϕ – функция Эйлера, а m' – произведение простых делителей числа m.

Заметим, что так как отображение Грея является взаимно однозначным, оно обратимо. Таким образом, наше отображение Z является композицией $\psi \circ \phi^{-1}$, где ψ – обобщенное отображение Грея из кольца $\mathbb{Z}_8$ в $\mathbb{F}_2^4$ (см. [7]), которое для любых $a, b, c \in \mathbb{Z}_2$ определяется как

$$\psi(a + 2b + 4c) = (c, c + a, c + b, c + a + b),$$

а ϕ^{-1} – обратное к отображению Грея ϕ (см. [3]) из $\mathbb{Z}_4$ в $\mathbb{F}_2^2$, которое для любых $a, b \in \mathbb{Z}_2$ определяется как

$$\phi(a + 2b) = (b, b + a).$$

Частным случаем [9, утверждение 2] при $k = 2$ является

Лемма 1. *Отображение Z является изометрией кольца $\mathbb{Z}_8$ с однородным весом и кольцом $\mathbb{Z}_4 \times \mathbb{Z}_4$ с весом Ли, являющимся также однородным.*

Доказательство непосредственно следует из соответствующих изометрических свойств отображений Карле и Грея и того факта, что однородный вес на $\mathbb{Z}_8$ определен как вес Хэмминга образа при отображении Карле. ▲

Для любого целого $k \geq 1$ продолжим наше отображение до отображения (обозначим его также через Z) $\mathbb{Z}_8^k$ в $\mathbb{Z}_4^k \times \mathbb{Z}_4^k$.

Определение 2. *Пусть $\boldsymbol{c} = (c_1, c_2, \ldots, c_k) \in \mathbb{Z}_8^k$ и $Z(c_j) = (a_j, b_j) \in \mathbb{Z}_4 \times \mathbb{Z}_4$, $j = 1, 2, \ldots, k$. Определим Z следующим образом:*

$$Z(\boldsymbol{c}) = (\boldsymbol{a}, \boldsymbol{b}), \tag{3}$$

где $\boldsymbol{a} = (a_1, a_2, \ldots, a_k) \in \mathbb{Z}_4^k$ и $\boldsymbol{b} = (b_1, b_2, \ldots, b_k) \in \mathbb{Z}_4^k$.

Определенное нами отображение имеет следующее корреляционное свойство.

Лемма 2. *Для любого целого числа $k \geq 1$ и $\boldsymbol{x} \in \mathbb{Z}_8^k$ имеем*

$$\theta_4(Z(\boldsymbol{x})) = \mathrm{Tr}_{L/K}(\theta_8(\boldsymbol{x})) = \theta_8(\boldsymbol{x}) + \theta_8(5\boldsymbol{x}).$$

Доказательство. Поскольку отображение $\mathrm{Tr}_{L/K}$ является линейной функцией, то достаточно проверить утверждение для $k = 1$. Пусть $x = a_0 + 2a_1 + 4a_2 \in \mathbb{Z}_8$, где $a_0, a_1, a_2 \in \mathbb{Z}_2$, тогда

$$\mathrm{Tr}_{L/K}(\theta_8(x)) = \omega^{a_0+2(a_1+2a_2)} + \omega^{5(a_0+2(a_1+2a_2))} =$$
$$= i^{a_1+2a_2}(\omega^{a_0} + \omega^{5a_0}) = i^{a_1+2a_2}\omega^{a_0}(1 + (-1)^{a_0}),$$

так как $\omega^2 = i$ и $\omega^4 = -1$. По определению $Z(x) = Z(a_0 + 2a_1 + 4a_2) = (a_1 + 2(a_0 + a_2), a_1 + 2a_2)$. Таким образом,

$$\theta_4(Z(x)) = i^{a_1+2(a_0+a_2)} + i^{a_1+2a_2} = i^{a_1+2a_2}(1 + (-1)^{a_0}).$$

Заметим, что в случае, когда $x \in \mathbb{Z}_8$ является четным (соответственно, $\omega^0 = 1$),

$$\mathrm{Tr}_{L/K}(\theta_8(x)) = \theta_4(Z(x)),$$

а в случае, когда x является нечетным (соответственно, $1 + (-1) = 0$),

$$\mathrm{Tr}_{L/K}(\theta_8(x)) = \theta_4(Z(x)) = 0. \quad ▲$$

§ 4. Многочлены над кольцом Галуа $GR(8, m)$

Многочлен

$$f(x) = \sum_{j=0}^{d} c_j x^j \in R[x]$$

назовем *каноническим*, если все коэффициенты при четных степенях x нулевые, т.е. $c_j = 0$ для всех четных j.

Пользуясь 2-адическим разложением коэффициентов, получаем

$$f(x) = f_0(x) + 2f_1(x) + 4f_2(x), \quad \text{где} \quad f_j(x) \in \mathcal{T}[x]. \tag{4}$$

Заметим, что многочлены $f_0(x)$, $f_1(x)$, $f_2(x)$ являются каноническими многочленами нечетных степеней, которые мы обозначим, соответственно, d_0, d_1, d_2. Напомним,

что взвешенная степень многочлена $f(x)$ равна

$$D_f = \max\{4d_0, 2d_1, d_2\}. \tag{5}$$

Для произвольного положительного целого числа $D \geq 4$ положим

$$S_D = \{f(x) \in R[x] : D_f \leq D, f \text{ – канонический}\}.$$

Заметим, что множество S_D является $GR(8, m)$-модулем. Основным результатом § 4 является оценка мощности этого множества.

Лемма 3. *Для любого целого $D \geq 4$ справедливо*

$$|S_D| = 2^{(D-\lfloor \frac{D}{8} \rfloor)m},$$

где $\lfloor x \rfloor$ – наибольшее целое число $\leq x$.

Доказательство. По определению взвешенной степени имеет место неравенство

$$\max\{4d_0, 2d_1, d_2\} \leq D,$$

и в частности,

$$4d_0 \leq D, \quad 2d_1 \leq D, \quad d_2 \leq D.$$

Поскольку d_2 нечетное, получаем

$$d_2 \leq D_2 = 2\left\lfloor \frac{D-1}{2} \right\rfloor + 1.$$

Аналогичным образом, для числа d_1 имеем

$$d_1 \leq D_1 = 2\left\lfloor \frac{D-2}{4} \right\rfloor + 1,$$

для числа d_0 имеем

$$d_0 \leq D_0 = 2\left\lfloor \frac{D-4}{8} \right\rfloor + 1.$$

Таким образом, для тройки нечетных чисел D_0, D_1, D_2 получаем

$$|\{f(x) \in R[x] : f \text{ – канонический; } d_0 \leq D_0, d_1 \leq D_1, d_2 \leq D_2\}| =$$
$$= 2^{m\left(\frac{D_0+1}{2} + \frac{D_1+1}{2} + \frac{D_2+1}{2}\right)}.$$

В результате

$$\frac{D_0+1}{2} + \frac{D_1+1}{2} + \frac{D_2+1}{2} = \left\lfloor \frac{D-4}{8} \right\rfloor + \left\lfloor \frac{D-2}{4} \right\rfloor + \left\lfloor \frac{D-1}{2} \right\rfloor + 3. \tag{6}$$

Поскольку для произвольного вещественного числа x и целого j имеет место равенство

$$\lfloor x + j \rfloor = \lfloor x \rfloor + j,$$

то правая часть в (6) равна

$$\left\lfloor \frac{D+4}{8} \right\rfloor + \left\lfloor \frac{D+2}{4} \right\rfloor + \left\lfloor \frac{D+1}{2} \right\rfloor.$$

Ясно, что существуют целые числа r и k такие, что $D = 8k + r$, где $0 \le r \le 7$, и данное выражение становится равным

$$7k + \left\lfloor \frac{r+1}{2} \right\rfloor + \left\lfloor \frac{r+2}{4} \right\rfloor + \left\lfloor \frac{r+4}{8} \right\rfloor. \tag{7}$$

Прямая проверка для случаев $r = 0, 1, \ldots, 7$ показывает, что

$$\left\lfloor \frac{r+1}{2} \right\rfloor + \left\lfloor \frac{r+2}{4} \right\rfloor + \left\lfloor \frac{r+4}{8} \right\rfloor = r.$$

Поскольку $k = \lfloor D/8 \rfloor$, то выражение (7) становится равным

$7k + r = D - \lfloor D/8 \rfloor$. ▲

§ 5. Коды над кольцом Галуа $GR(8, m)$

Напомним, что $n = 2^m$.

Лемма 4. *Пусть $f(x) \in R[x]$ – канонический многочлен взвешенной степени D_f. Положим $\boldsymbol{y} = Z(\boldsymbol{x}) \in \mathbb{Z}_4^{n-1} \times \mathbb{Z}_4^{n-1}$, где $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-2})$ и $x_j = \mathrm{Tr}\,(f(\beta^j)) \in \mathbb{Z}_8$, $j = 0, 1, \ldots, n-2$. Тогда*

$$|\theta_4(\boldsymbol{y})| \le 2(D_f - 1)\sqrt{2^m}. \tag{8}$$

Доказательство. Применяя лемму 2, получаем

$$\theta_4(\boldsymbol{y}) = \mathrm{Tr}_{L/K}(\theta_8(\boldsymbol{x})) = \sum_{j=0}^{n-2} \omega^{\mathrm{Tr}(f(\beta^j))} + \sum_{j=0}^{n-2} \omega^{5\mathrm{Tr}(f(\beta^j))}. \tag{9}$$

Заметим, что $\beta = 5\xi \in R$, где ξ – порождающий элемент множества Тейхмюллера ($\mathrm{ord}(\xi) = n - 1$). Поскольку в кольце R выполняется $5^2 = 1$ и f – канонический многочлен, то

$$f(\beta^j) = \begin{cases} f(\xi^j) & \text{для четных } j, \\ 5f(\xi^j) & \text{для нечетных } j. \end{cases}$$

В (9) переставим местами слагаемые, соответствующие четным значениям j. Поскольку Tr – линейная функция над $\mathbb{Z}_8$, то правая часть переписывается как

$$\sum_{j=0}^{n-2} \omega^{\mathrm{Tr}(f(\xi^j))} + \sum_{j=0}^{n-2} \omega^{\mathrm{Tr}(5f(\xi^j))}.$$

Заметим, что $5f$ – канонический многочлен взвешенной степени $\le D_f$. Для произвольного такого многочлена хорошо известна [6] оценка

$$\left| \sum_{x \in \mathcal{T}} \omega^{\mathrm{Tr}(f(x))} \right| \le (D_f - 1)\sqrt{2^m}. \quad ▲$$

Определение 3. *Для произвольного целого $D \ge 4$ обозначим через $C_8(m, D)$ множество, являющееся $\mathbb{Z}_8$-линейным кодом длины $n - 1$:*

$$C_8(m, D) = \left\{ \boldsymbol{x} = (x_0, x_1, \ldots, x_{n-2}) \in \mathbb{Z}_8^{n-1} : x_j = \mathrm{Tr}\,(f(\beta^j)),\ f \in S_D \right\}. \tag{10}$$

Лемма 5. *Определим множество* $ZC_4(m,D) = Z(C_8(m,D))$ *как образ множества* $C_8(m,D)$ (*см.* (10)) *при отображении* Z (*см.* (3)). *Тогда множество* $ZC_4(m,D)$ – *циклический код над* $\mathbb{Z}_4$ *длины* $2(n-1)$.

Доказательство. Очевидно, что множество $ZC_4(m,D)$ состоит из слов длины $2(n-1)$. Пусть $\boldsymbol{c}=(c_0,c_1,\ldots,c_{n-2})\in C_8(m,D)$ и $Z(\boldsymbol{c})=(\boldsymbol{a},\boldsymbol{b})$, где $\boldsymbol{a}=(a_0,a_1,\ldots,a_{n-2})$, $\boldsymbol{b}=(b_0,b_1,\ldots,b_{n-2})$ и $Z(c_j)=(a_j,b_j)\in\mathbb{Z}_4\times\mathbb{Z}_4$.

Поскольку код $C_8(m,D)$ – констациклический с константой 5, то $(5c_{n-2},c_0,\ldots,c_{n-3})\in C_8(m,D)$. По определению (2) имеем $Z(5c_{n-2})=(b_{n-2},a_{n-2})$ и, таким образом, кодовое слово

$$Z((5c_{n-2},c_0,\ldots,c_{n-3})) = (b_{n-2},a_0,a_1,\ldots,a_{n-3}|a_{n-2},b_0,b_1,\ldots,b_{n-3})$$

является циклическим сдвигом слова $(a_0,a_1,\ldots,a_{n-2}|b_0,b_1,\ldots,b_{n-2})$. ▲

В итоге мы имеем следующее утверждение.

Теорема 1. *Множество* $ZC_4(m,D)$ *является дистанционно-инвариантным циклическим* $\mathbb{Z}_4$*-кодом длины* $2(n-1)$ *мощности* $n^{D-\lfloor\frac{D}{8}\rfloor}$ *с минимальным расстоянием Ли* $\geq 2(n-1)-2(D-1)\sqrt{n}$.

Доказательство. Дистанционная инвариантность следует из свойств изометрии (см. лемму 1) для отображения Z. Мощность кода следует из леммы 3, а нижняя граница расстояния Ли вытекает из леммы 4 и связи между расстоянием Ли и комплексной корреляцией (см. [3, §2.3]):

$$d_L(\boldsymbol{x},\boldsymbol{y}) \geq n - \mathrm{Re}\,(\theta_4(\boldsymbol{x}-\boldsymbol{y})).$$ ▲

Рассмотрим код $C_4(m+1,D)'$, который получается из кода $C_4(m+1,D)$ вычеркиванием двух позиций. Тогда этот код имеет такую же длину $2(n-1)$, что и наш код $ZC_4(m,D)$, расстояние $2(n-1)-\sqrt{2}(D-1)\sqrt{n}$ и мощность $4(2n)^{3D/4}$, в то время как наш код содержит $n^{7D/8}$ слов. Таким образом, код $ZC_4(m,D)$ имеет меньшее расстояние, но большую мощность при $m>6+16/D$.

§ 6. Семейство четверичных последовательностей

Поскольку код ZC_4 может быть не $\mathbb{Z}_4$-линейным, то знание границы для $\theta_4(\boldsymbol{x})$ при каждом $\boldsymbol{x}\in ZC_4$ не является достаточным для оценки взаимной корреляции, соответствующей четверичной последовательности. Запишем отображение Z в виде двух компонент:

$$Z(\boldsymbol{u}) = (Z_1(\boldsymbol{u}),Z_2(\boldsymbol{u})).$$

Для любых двух слов $\boldsymbol{u},\boldsymbol{v}\in C_8(m,D)$ определим значение взаимной корреляции их образов при отображении Z для временного сдвига τ как

$$\Theta(Z)_{\boldsymbol{u},\boldsymbol{v}}(\tau) = \sum_{j=1}^{n-1}\left(i^{Z_1(u_j)-Z_1(v_{j+\tau})}+i^{Z_2(u_j)-Z_2(v_{j+\tau})}\right).$$

Следуя идеям работы [10], применим спектральный анализ к отображению Z. Для любого целого числа k пусть $\omega=e^{2\pi i/8}$ и ψ_k – аддитивный характер кольца $\mathbb{Z}_8$ такой, что

$$\psi_k(x) = \omega^{kx}$$

для всех $x\in\mathbb{Z}_8$.

Наша задача представить i^{Z_1} и i^{Z_2} как линейную комбинацию этих характеров.

Лемма 6. *Пусть* $\omega = e^{2\pi i/8}$ *– примитивный корень восьмой степени из единицы и положим* $\psi_k(u) = \omega^{ku}$, *где* k *– целое. Тогда для произвольного* $u \in \mathbb{Z}_8$ *имеют место следующие равенства:*

$$i^{Z_1(u)} = \mu_5\psi_1(u) + \mu_1\psi_5(u),$$
$$i^{Z_2(u)} = \mu_1\psi_1(u) + \mu_5\psi_5(u),$$

где $\mu_1 = (1-\omega^3)/2$, $\mu_5 = (1+\omega^3)/2$.

Доказательство. Напомним понятие преобразования Фурье на аддитивной группе $\mathbb{Z}_8$. Пусть μ – произвольная функция из $\mathbb{Z}_8$ в поле комплексных чисел. Тогда при любом $u \in \mathbb{Z}_8$ имеет место разложение

$$\mu(u) = \sum_{j=0}^{7} \mu_j\psi_j(u), \quad \text{где} \quad \mu_j = \frac{1}{8}\sum_{x=0}^{7} \mu(x)\psi_j(-x). \tag{11}$$

В частности, при $\mu(u) = i^{Z_2(u)}$ и $x = a_0 + 2a_1 + 4a_2$ получаем

$$\mu_j = \frac{1}{8}\sum_{a_0,a_1,a_2} i^{a_1+2a_2}\omega^{-j(a_0+2a_1+4a_2)}.$$

Упростив это выражение, получим

$$\mu_j = \frac{1}{8}(1+\omega^{-j})(1+i^{-j+1})(1+(-1)^{-j+1}).$$

Прямая подстановка $j = 0, 1, \ldots, 7$ и соответствующие упрощения дают окончательный результат (в частности, $\mu_j = 0$, $j \neq 1; 5$). Оценка для Z_1 получается аналогичным образом. ▲

Непосредственной проверкой получена

Лемма 7. *В обозначениях леммы* 6 *имеет место равенство*

$$(|\mu_1| + |\mu_5|)^2 = 1 + \frac{\sqrt{2}}{2},$$

где $\mu_1 = (1+\omega^7)/2$, $\mu_5 = (1+\omega^3)/2$.

Два кодовых слова $\boldsymbol{u}$ и $\boldsymbol{v}$ кода $C_8(m, D)$ назовем τ-*эквивалентными*, если $\boldsymbol{u}$ получается из $\lambda\boldsymbol{v}$ (где $\lambda \in \mathbb{Z}_8^* = \{1, 3, 5, 7\}$) сдвигом на τ позиций.

Теорема 2. *Для произвольных кодовых слов* $\boldsymbol{u}, \boldsymbol{v} \in C_8(m, D)$, *не являющихся* τ*-эквивалентными, имеет место следующая оценка:*

$$|\Theta(Z)_{\boldsymbol{u},\boldsymbol{v}}(\tau)| \leq (2+\sqrt{2})(D-1)\sqrt{2^m}.$$

Доказательство. Имеем

$$\Theta(Z)_{\boldsymbol{u},\boldsymbol{v}}(\tau) = \sum_{j=1}^{n-1}\left(i^{Z_1(u_j)-Z_1(v_{j+\tau})} + i^{Z_2(u_j)-Z_2(v_{j+\tau})}\right). \tag{12}$$

Рассмотрим сначала вклад от Z_1. Применяя лемму 6, имеем

$$i^{Z_1(u)} = \mu_5\psi_1(u) + \mu_1\psi_5(u).$$

Далее получаем

$$i^{Z_1(u_j)-Z_1(u_{j+\tau})} = (\mu_5\psi_1(u_j) + \mu_1\psi_5(u_j))(\overline{\mu}_5\psi_1(-v_{j+\tau}) + \overline{\mu}_1\psi_5(-v_{j+\tau})),$$

что можно записать в виде

$$\mu_5\overline{\mu}_5\psi_1(u_j - v_{j+\tau}) + \mu_1\overline{\mu}_1\psi_5(u_j - v_{j+\tau}) + \mu_5\overline{\mu}_1\psi_1(u_j - 5v_{j+\tau}) + \mu_1\overline{\mu}_5\psi_1(5u_j - v_{j+\tau}).$$

Затем мы воспользуемся оценкой сумм характеров, которая в данном случае применима, так как слова u, v не являются τ-эквивалентными, и заметим, что

$$|\mu_1|^2 + |\mu_5|^2 + |\mu_1\overline{\mu}_5| + |\mu_5\overline{\mu}_1| \;\le\; (|\mu_1| + |\mu_5|)^2.$$

Пользуясь этим неравенством, оценкой для сумм характеров и леммой 7, получаем

$$\left|\sum_{j=1}^{n-1} i^{Z_1(u_j) - Z_1(v_{j+\tau})}\right| \;\le\; (|\mu_1| + |\mu_5|)^2(D-1)\sqrt{2^m} \;=\; (1 + 1/\sqrt{2})(D-1)\sqrt{2^m}.$$

Вклад от Z_2 оценивается так же. ▲

Как и в [10], мы избавляемся от зависимости аргументов от τ путем разбиения многочленов, определяющих кодовые слова $C_8(m, D)$, на классы эквивалентности по модулю действия мультипликативной группы $\mathbb{Z}_8^* \times T^*$ на аргумент многочлена. А именно два многочлена $f(x), g(x) \in R[x]$ будем считать эквивалентными, если $g(x) = f(ax\alpha)$ для некоторых $a \in \mathbb{Z}_8^*$ и $\alpha \in T^*$. Легко видеть, что введенное таким образом отношение эквивалентности разбивает множество S_D на классы эквивалентности. Обозначим через $S_8(m, D)$ множество представителей (из S_D) этих классов. Заметим, что в каждом классе эквивалентности содержится не более $|\mathbb{Z}_8^*| \times |T^*|$ многочленов.

Если вещественная функция $f(n)$ от целого аргумента n ограничена сверху величиной $\kappa g(n)$, где n стремится к бесконечности и κ – некоторая константа, то

$$g(n) = \mathrm{O}\,(f(n)).$$

Теорема 3. *Множество $i^{Z(S_8(m,D))}$ содержит $O(T^{(7D/8)-1})$ последовательностей длины $T = 2(2^m - 1)$ с автокорреляцией и взаимной корреляцией, не превосходящей $(1 + \sqrt{2})(D-1)\sqrt{2^m}$.*

Доказательство. Мощность множества следует напрямую из определения $S_8(m, D)$. Длина последовательности вытекает из уравнения (2) и свойства цикличности кода $C_8(m, D)$. Оценка для корреляции вытекает из теоремы 2. ▲

Для сравнения семейство четверичных последовательностей, получающихся из кода $C_4(m, D)$ работы [5], содержит порядка $T^{3D/4}$ элементов длины $T = 2^m - 1$ с автокорреляцией и взаимной корреляцией, не превосходящей $(D-1)\sqrt{T}$.

§ 7. Двухфазные последовательности

Напомним, что отображение Z (из кольца $\mathbb{Z}_8$ в кольцо $\mathbb{Z}_4 \times \mathbb{Z}_4$) было введено следующим образом: пусть $u = a_0 + 2a_1 + 4a_2 \in \mathbb{Z}_8$, где $a_0, a_1, a_2 \in \mathbb{Z}_2$, тогда

$$Z(u) = (Z_1(u), Z_2(u)) = (a_1 + 2(a_0 + a_2), a_1 + 2a_2).$$

Определим отображение MSBZ: $\mathbb{Z}_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ следующим образом:

$$MSBZ(u) = (MSB(Z_1(u)), MSB(Z_2(u))),$$

а именно

$$MSBZ(a_0 + 2a_1 + 4a_2) = (a_0 + a_2, a_2),$$

т.е. рассматривая старшие биты каждой из компонент отображения Z (элементов кольца $\mathbb{Z}_4$).

Для любых двух слов $\boldsymbol{u}, \boldsymbol{v} \in C_8(m, D)$ определим значение взаимной корреляции их образов при отображении Z для временного сдвига τ как

$$\Theta(MSBZ)_{\boldsymbol{u},\boldsymbol{v}}(\tau) =$$
$$= \sum_{j=1}^{n-1} \left((-1)^{MSB(Z_1(u_j)) - MSB(Z_1(v_{j+\tau}))} + (-1)^{MSB(Z_2(u_j)) - MSB(Z_2(v_{j+\tau}))} \right).$$

Применим технику дискретного преобразования Фурье к функциям $(-1)^{MSB(Z_1(u))}$, $(-1)^{MSB(Z_2(u))}$, отображающим элемент $a_0 + 2a_1 + 4a_2$ кольца $\mathbb{Z}_8$, соответственно, в $(-1)^{a_0+a_2}$ и $(-1)^{a_2}$. Тогда имеет место

Лемма 8. *Пусть $\omega = e^{2\pi i/8}$ – примитивный корень восьмой степени из единицы, положим $\psi_k(u) = \omega^{ku}$, где k – целое. Тогда имеют место следующие равенства:*

$$(-1)^{MSB(Z_1(u))} = \mu_1\psi_1(u) + \mu_3\psi_3(u) + \mu_5\psi_5(u) + \mu_7\psi_7(u),$$
$$(-1)^{MSB(Z_2(u))} = \mu_5\psi_1(u) + \mu_7\psi_3(u) + \mu_1\psi_5(u) + \mu_3\psi_7(u),$$

где

$$\mu_1 = \frac{1}{4}(1 + \omega - \omega^2 + \omega^3), \qquad \mu_3 = \frac{1}{4}(1 + \omega + \omega^2 + \omega^3),$$
$$\mu_5 = \frac{1}{4}(1 - \omega - \omega^2 - \omega^3), \qquad \mu_7 = \frac{1}{4}(1 - \omega + \omega^2 - \omega^3);$$

кроме этого

$$(|\mu_1| + |\mu_3| + |\mu_5| + |\mu_7|)^2 = 2 + \sqrt{2}.$$

Доказательство. Применим преобразование Фурье на аддитивной группе $\mathbb{Z}_8$. Пусть μ – произвольная функция из $\mathbb{Z}_8$ в поле комплексных чисел. Тогда при любом $u \in \mathbb{Z}_8$ имеет место следующее разложение:

$$\mu(u) = \sum_{j=0}^{7} \mu_j\psi_j(u), \quad \text{где} \quad \mu_j = \frac{1}{8}\sum_{x=0}^{7} \mu(x)\psi_j(-x).$$

В частности, при $\mu(u) = (-1)^{MSB(Z_1(u))}$ и $x = a_0 + 2a_1 + 4a_2$ получаем

$$\mu_j = \frac{1}{8}\sum_{a_0,a_1,a_2} (-1)^{a_0+a_2}\omega^{-j(a_0+2a_1+4a_2)}.$$

После упрощения получим

$$\mu_j = \frac{1}{8}(1 - \omega^{-j})(1 + i^{-j})(1 + (-1)^{1-j}).$$

Прямая подстановка $j = 0, 1, \ldots, 7$ и соответствующие упрощения дают окончательный результат (в частности, $\mu_j = 0$, $j = 0, 2, 4, 6$). Для функции $(-1)^{MSB(Z_2(u))}$ результат получается аналогичным образом. ▲

Теорема 4. *Множество $(-1)^{MSBZ(S_8(m,D))}$ содержит $O(T^{(7D/8)-1})$ последовательностей длины $T = 2(2^m - 1)$ с автокорреляцией и взаимной корреляцией, не превосходящей $2(2 + \sqrt{2})(D - 1)\sqrt{2^m}$.*

Доказательство. Мощность множества следует из определения $S_8(m, D)$. Длина последовательностей вытекает из уравнения (2) и свойства цикличности кода

$C_8(m, D)$. Оценки корреляции получаются методом, аналогочным теореме 2, с использованием леммы 8. В частности, для взаимной корреляции получаем

$$|\Theta(MSBZ)_{\boldsymbol{u},\boldsymbol{v}}(\tau)| \le 2(2+\sqrt{2})(D-1)\sqrt{2^m}. \quad \blacktriangle$$

Для сравнения, семейство двухфазных последовательностей $S(m, D)$, получающихся из кода $C_4(m, D)$ работы [5], содержит порядка $T^{(3D/4)-1}$ элементов длины $T = 2(2^m - 1)$ с автокорреляцией и взаимной корреляцией, не превосходящей $2(D-1)\sqrt{2T}$.

§ 8. Коды над кольцом Галуа $GR(8, m)$ в случае четного m

Положим $n = 2^m$, где m – четное целое число. Пусть $\beta = \sqrt{5}\xi$, где $\sqrt{5}$ – решение уравнения $x^2 - 5 = 0$ (например, $\sqrt{5} = 1 + 2\alpha \in R$, где $\alpha \in \mathcal{T}$ такое, что $\alpha^2 + \alpha \equiv 1 \pmod 2$). Поскольку в кольце $\mathbb{Z}_8$ имеет место равенство $(\sqrt{5})^4 = 1$, то

$$\beta^{2(n-1)} = (\sqrt{5}\xi)^{2(n-1)} = 5,$$

и следовательно, $\beta^{4(n-1)} = 1$.

Лемма 9. *Пусть $f(x) \in R[x]$ – канонический многочлен взвешенной степени D_f. Возьмем $\boldsymbol{y} = Z(\boldsymbol{x}) \in \mathbb{Z}_4^{2(n-1)} \times \mathbb{Z}_4^{2(n-1)}$, где $\boldsymbol{x} = (x_0, x_1, \ldots, x_{2n-3})$ и $x_j = \mathrm{Tr}\,(f(\beta^j)) \in \mathbb{Z}_8$, $j = 0, 1, \ldots, 2n-3$. Тогда*

$$|\theta_4(\boldsymbol{y})| \le 4(D_f - 1)\sqrt{2^m}. \tag{13}$$

Доказательство. Применяя лемму 2, имеем

$$\theta_4(\boldsymbol{y}) = \mathrm{Tr}\,(\theta(\boldsymbol{x})) = \sum_{j=0}^{2n-3} \omega^{\mathrm{Tr}(f(\beta^j))} + \sum_{j=0}^{2n-3} \omega^{5\mathrm{Tr}(f(\beta^j))}. \tag{14}$$

Напомним, что $\beta = \sqrt{5}\xi \in R$, где ξ – порождающий элемент множества Тейхмюллера (соответственно, $\xi^{n-1} = 1$). Пусть

$$g(x) = f(\sqrt{5}x)/\sqrt{5}.$$

Заметим, что если многочлен f – канонический, то многочлен g – также канонический. Поскольку в кольце R имеем $(\sqrt{5})^4 = 1$, то

$$f(\beta^j) = \begin{cases} f(\xi^j), & \text{если } j \equiv 0 \pmod 4, \\ f(\sqrt{5}\xi^j), & \text{если } j \equiv 1 \pmod 4, \\ f(5\xi^j), & \text{если } j \equiv 2 \pmod 4, \\ f(5\sqrt{5}\xi^j), & \text{если } j \equiv 3 \pmod 4. \end{cases}$$

Разобьем первую сумму в (14) на четыре подсуммы, объединив в одну подсумму слагаемые, соответствующие одному значению j по модулю 4. Таким образом, данная сумма принимает вид

$$\sum_{j\equiv 0} \omega^{\mathrm{Tr}(f(\xi^j))} + \sum_{j\equiv 1} \omega^{\mathrm{Tr}(f(\sqrt{5}\xi^j))} + \sum_{j\equiv 2} \omega^{\mathrm{Tr}(f(5\xi^j))} + \sum_{j\equiv 3} \omega^{\mathrm{Tr}(f(5\sqrt{5}\xi^j))}. \tag{15}$$

Аналогичным образом вторая сумма в (14) принимает вид

$$\sum_{j\equiv 0} \omega^{5\mathrm{Tr}(f(\xi^j))} + \sum_{j\equiv 1} \omega^{5\mathrm{Tr}(f(\sqrt{5}\xi^j))} + \sum_{j\equiv 2} \omega^{5\mathrm{Tr}(f(5\xi^j))} + \sum_{j\equiv 3} \omega^{5\mathrm{Tr}(f(5\sqrt{5}\xi^j))}. \tag{16}$$

По определению многочлена g, поскольку функция Tr является $\mathbb{Z}_8$-линейной, выражение (15) принимает вид

$$\sum_{j\equiv 0}\omega^{\mathrm{Tr}(f(\xi^j))}+\sum_{j\equiv 1}\omega^{\mathrm{Tr}(\sqrt{5}g(\xi^j))}+\sum_{j\equiv 2}\omega^{\mathrm{Tr}(5f(\xi^j))}+\sum_{j\equiv 3}\omega^{\mathrm{Tr}(5\sqrt{5}g(\xi^j))}. \tag{17}$$

Аналогичным образом выражение (16) принимает вид

$$\sum_{j\equiv 0}\omega^{\mathrm{Tr}(5f(\xi^j))}+\sum_{j\equiv 1}\omega^{\mathrm{Tr}(5\sqrt{5}g(\xi^j))}+\sum_{j\equiv 2}\omega^{\mathrm{Tr}(f(\xi^j))}+\sum_{j\equiv 3}\omega^{\mathrm{Tr}(\sqrt{5}g(\xi^j))}. \tag{18}$$

Поскольку $n-1$ является нечетным и j пробегает все множество значений $0,1,\ldots$ $\ldots,n-2$, то $2j$ и $2j+1$ пробегают все множество значений $0,1,\ldots,n-2$ по модулю $n-1$. Таким образом, поскольку ξ – элемент порядка $n-1$, то, объединяя первую сумму в (17) с третьей суммой в (18), получаем

$$\sum_{j\equiv 0}\omega^{\mathrm{Tr}(f(\xi^j))}+\sum_{j\equiv 2}\omega^{\mathrm{Tr}(f(\xi^j))}=\sum_{j=0}^{n-2}\omega^{\mathrm{Tr}(f(\xi^j))}. \tag{19}$$

Аналогично, объединяя вторую сумму в (17) с четвертой суммой в (18), третью с первой, а четвертую со второй, получаем, что выражение (14) принимает вид

$$\sum_{j=0}^{n-2}\omega^{\mathrm{Tr}(f(\xi^j))}+\sum_{j=0}^{n-2}\omega^{\mathrm{Tr}(5f(\xi^j))}\sum_{j=0}^{n-2}\omega^{\mathrm{Tr}(\sqrt{5}g(\xi^j))}+\sum_{j=0}^{n-2}\omega^{\mathrm{Tr}(5\sqrt{5}g(\xi^j))}.$$

Заметим, что наряду с f многочлены $5f$, g и $5\sqrt{5}g$ – также канонические многочлены взвешенной степени $\le D_f$. Для таких многочленов справедлива следующая оценка (см. [6]):

$$\left|\sum_{x\in\mathcal{T}}\omega^{\mathrm{Tr}(f(x))}\right|\le (D_f-1)\sqrt{2^m}. \quad \blacktriangle$$

Определение 4. *Для произвольного целого $D\ge 4$ и многочлена $f(x)\in S_D$ обозначим через $C_8^{\mathrm{ev}}(m,D)$ следующий Z_8-линейный код длины $2(n-1)$:*

$$C_8^{\mathrm{ev}}(m,D)=\left\{\boldsymbol{x}=(x_0,x_1,\ldots,x_{2n-3})\in\mathbb{Z}_8^{2(n-1)}:x_j=\mathrm{Tr}\left(f(\beta^j)\right),\ f\in S_D\right\}. \tag{20}$$

Лемма 10. *Обозначим через $ZC_4^{\mathrm{ev}}(m,D)=Z(C_8^{\mathrm{ev}}(m,D))$ образ кода $C_8^{\mathrm{ev}}(m,D)$, определенного в* (20), *при отображении Z* (см. (3)). *Тогда множество $ZC_4^{\mathrm{ev}}(m,D)$ является циклическим кодом над $\mathbb{Z}_4$ длины $4(n-1)$.*

Доказательство идентично доказательству леммы 5.

Аналогом теоремы 1 является

Теорема 5. *Код $ZC_4^{\mathrm{ev}}(m,D)$ является циклическим $\mathbb{Z}_4$-кодом, возможно, нелинейным, дистанционно-инвариантным, длины $4(n-1)$, мощности $n^{D-\lfloor\frac{D}{8}\rfloor}$, с минимальным расстоянием Ли $\ge 4(n-1)-4(D-1)\sqrt{n}$.*

Для сравнения рассмотрим код $C_4(m+2,D)'$, который получается из кода $C_4(m+$ $+2,D)$ вычеркиванием четырех позиций. Тогда этот код имеет такую же длину $4(n-1)$, минимальное расстояние Ли $\ge 4(n-1)-2(D-1)\sqrt{n}$ и мощность порядка $4(4n)^{3D/4}$. Таким образом, код $ZC_4^{\mathrm{ev}}(m,D)$ имеет меньшее расстояние, но большую мощность (порядка $n^{7D/8}$) при больших n.

§ 9. Замечания и нерешенные задачи

В данной статье мы построили аналог четверичной (над кольцом $\mathbb{Z}_4$) конструкции, предложенной Шанбагом, Кумаром и Хеллесетом над кольцом $\mathbb{Z}_8$. Результирующие четверичные коды и двухфазные последовательности имеют сравнимые характеристики для минимального расстояния Ли и комплексной корреляции, как в [5].

Основным открытым вопросом остается вопрос линейности над $\mathbb{Z}_4$ наших четверичных кодов и $\mathbb{F}_2$-линейности для последовательностей. Из [9, теорема 5] следует, что эти две задачи являются эквивалентными.

Авторы выражают благодарность рецензенту, замечания которого способствовали улучшению статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Нечаев А.А.* Функция след на кольце Галуа и помехоустойчивые коды // Тр. V Всесоюз. симпоз. по теории колец, алгебр и модулей. Новосибирск, 1982. С. 97.
2. *Нечаев А.А.* Код Кердока в циклической форме // Дискр. мат. 1989. Т. 1. № 4. С. 123–139.
3. *Hammons A.R.,Jr., Kumar P.V., Calderbank A.R., Sloane N.J.A., Solé P.* The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes // IEEE Trans. Inform. Theory. 1994. V. 40. № 2. P. 301–319.
4. *Kumar P.V., Helleseth T., Calderbank A.R., Hammons A.R., Jr.* Large Families of Quaternary Sequences with Low Correlation // IEEE Trans. Inform. Theory. 1996. V. 42. № 2. P. 579–592.
5. *Shanbhag A., Kumar P.V., Helleseth T.* Improved Binary Codes and Sequence Families from $\mathbb{Z}_4$-Linear Codes // IEEE Trans. Inform. Theory. 1996. V. 42. № 5. P. 1582–1586.
6. *Kumar P.V., Helleseth T., Calderbank A.R.* An Upper Bound for Weil Exponential Sums over Galois Rings and Applications // IEEE Trans. Inform. Theory. 1995. V. 41. № 2. P. 456–468.
7. *Carlet C.* $\mathbb{Z}_{2^k}$-Linear Codes // IEEE Trans. Inform. Theory. 1998. V. 44. № 4. P. 1543–1547.
8. *Нечаев А.А., Хонольд Т.* Полновесные модули и представления кодов // Пробл. передачи информ. 1999. Т. 35. № 3. С. 18–39.
9. *Tapia-Recillas H., Vega G.* Some Constacyclic Codes over $\mathbb{Z}_{2^k}$ and Binary Quasi-Cyclic Codes // Discr. Appl. Math. 2003. V. 128. P. 305–316.
10. *Lahtonen J., Ling S., Solé P., Zinoviev D.* $\mathbb{Z}_8$-Kerdock Codes and Pseudo-Random Binary Sequences // J. Complexity. 2004. V. 20. P. 318–330.
11. *Константинеску И., Хайзе В.* Метрика для кодов над кольцами вычетов // Пробл. передачи информ. 1997. Т. 33. № 3. С. 22–28.

Зиновьев Дмитрий Викторович
Институт проблем передачи информации РАН
dzinov@iitp.ru
Соле Патрик
Национальный центр научных исследований, Франция
ps@essi.fr

Поступила в редакцию
15.07.2003

После переработки
08.01.2004