Челябинский физико-математический журнал. 2017. Т. 2, вып. 1. С. 66–79.

УДК 519.725

БИОРТОГОНАЛЬНЫЙ ВЕЙВЛЕТ-КОД В ПОЛЯХ ХАРАКТЕРИСТИКИ ДВА

А. А. Соловьёв[a], **Д. В. Черников**[b]

Челябинский государственный университет, Челябинск, Россия
[a] *alsol@csu.ru,* [b] *cherninkiy@gmail.com*

Предложена схема построения помехоустойчивых циклических вейвлет-кодов на основе биортогонального преобразования над конечными полями чётной характеристики. Представленный метод построения использует алгоритм Евклида нахождения НОД многочленов, что упрощает возможность построения вейвлет-кодов с заданными свойствами. Доказано, что среди вейвлет-кодов имеются коды с заданным кодовым расстоянием.

Ключевые слова: *полифазная схема, биортогональное преобразование, вейвлет-коды, конечные поля.*

Введение

Вейвлет-коды являются подклассом квазициклических кодов с циклическим сдвигом кодовых слов на две позиции [1]. Первоначально порождающие матрицы вейвлет-кодов строились с помощью ортогональных фильтров масштабирующей функции и вейвлет-функции [2; 3]. Практическое применение этого метода было затруднено необходимостью построения масштабирующих функций с заданными свойствами (см. [4; 5]) На основании результатов работы [6] о факторизации параунитарных матриц в работе [7] (см. также [8]) и работах других авторов трудность с построением требуемых порождающих многочленов вейвлет-кодов была преодолена.

В дальнейшем класс вейвлет-кодов был расширен путём использования биортогональных наборов фильтров [9; 10]. Это упростило построение порождающих многочленов и позволило находить вейвлет-коды с требуемыми свойствами.

В работе [11] была предложена улучшенная схема помехоустойчивого кодирования над конечным полем с использованием биортогональных наборов фильтров точного восстановления. Вместо алгоритма факторизации использовалась лифтинговая схема [12], основанная на алгоритме Евклида нахождения НОД многочленов. Подобный подход позволил упростить и расширить возможности построения вейвлет-кодов с заданными свойствами. Однако в поле чётной характеристики конструкция из [11] не позволила найти среди вейвлет-кодов коды с максимально возможным кодовым расстоянием.

В данной работе над полем характеристики 2 предложена другая схема кодирования, названная полифазной. Подробное её изложение и схема восстановления информационной последовательности приведены в первом разделе.

Возможности алгоритма демонстрируются в последующих разделах статьи. Так, во втором разделе с помощью этой схемы строятся вейвлет-коды с максимальным кодовым расстоянием. Доказывается, что найденные коды являются кодами Рида — Соломона, построенными во временной области. В третьем разделе

строятся вейвлет-коды с заданным кодовым расстоянием. Найденные коды являются подпространствами кодов Рида — Соломона во временной области. Поэтому к построенным кодам применим алгоритм помехоустойчивого декодирования Берлекампа — Велча [13], первоначально предложенный для декодирования кодов Рида — Соломона (см. также [14]).

В каждом из этих разделов приводятся примеры конкретных кодов с заданными свойствами и реализуется процедура декодирования зашумлённых сообщений.

При построении вейвлет-кодов удобно пользоваться терминологией теории цифровой обработки сигналов, принятой в теории вейвлетов.

1. Полиномиальная схема построения циклического биортогонального вейвлет-кода в поле характеристики два

Выберем в поле $GF(2^m)$ примитивный элемент α. Опишем биортогональные циклические вейвлет-коды длины $n = 2^m - 1$ с длиной информационных слов $\frac{n-1}{2}$, а также схему полифазного кодирования.

Фильтру h с импульсным откликом $\{h_k\}_{k=0}^{n-1}$ поставим в соответствие многочлен

$$h(x) = \sum_{i=0}^{n-1} h_i x^i = h_0 + h_1 x + \dots h_{n-1} x^{n-1}\,.$$

Представим $h(x)$ в виде суммы полифазных компонент $h(x) = h_e(x^2) + x h_o(x^2)$, где

$$h_e(x) = \sum_{k=0}^{(n-1)/2} h_{2k} x^k,\;\; h_o(x) = \sum_{k=0}^{(n-3)/2} h_{2k+1} x^k.$$

Наряду с фильтром h рассмотрим фильтр $g = \{g_k\}_{k=0}^{n-1}$. Введём в рассмотрение полифазную матрицу

$$P(x) = \begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix}.$$

Будем говорить, что фильтры h и g комплементарны, если $\det P(x) = 1$.

Пусть $\boldsymbol{v} = (v_0 \dots v_{n-1})$ — вектор с компонентами из $GF(2^m)$. Дискретное преобразование Фурье определяется как вектор $\boldsymbol{V} = \mathcal{F}(\boldsymbol{v}) = (V_0, \dots, V_{n-1})$ с компонентами

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} v_i,\;\; j = 0, \dots, n-1\,.$$

Обратное преобразование Фурье имеет вид

$$v_i = \sum_{i=0}^{n-1} \alpha^{-ij} V_j,\;\; i = 0, \dots, n-1\,.$$

Определение 1. *Полифазные компоненты кодового слова $c(x)$ в кольце $GF_{2^m}[x]/(x^n - 1)$ вводятся следующим образом*:

$$\begin{bmatrix} c_e(x^2) \\ c_o(x^2) \end{bmatrix} = \begin{bmatrix} h_e(x^2) & g_e(x^2) \\ h_o(x^2) & g_o(x^2) \end{bmatrix} \begin{bmatrix} 1 \\ x^2 \end{bmatrix} i(x^2),$$

где $i(x) = \sum_{j=0}^{(n-3)/2} i_j x^j$ — информационный многочлен степени не выше $\frac{n-3}{2}$ с длиной информационной последовательности, равной $\frac{n-1}{2}$.

В определении и в последующих рассуждениях умножение многочленов производится в кольце $GF_{2^m}[x]/(x^n-1)$. Кодовый многочлен $c(x)$, как и при биортогональном кодировании (см. [11]), запишется в виде

$$c(x) = c_e(x^2) + xc_o(x^2) = \big(h(x) + x^2 g(x)\big)\, i(x^2) \bmod (x^n - 1)\,.$$

Многочлен $F(x) = h(x) + x^2 g(x)$ будем называть порождающим.

Вместе с парой фильтров (h, g) рассмотрим пару комплементарных фильтров $(\tilde{h}, \tilde{g})$ с полифазной матрицей

$$\tilde{P} = \begin{bmatrix} \tilde{h}_e(x) & \tilde{g}_e(x) \\ \tilde{h}_o(x) & \tilde{g}_o(x) \end{bmatrix}.$$

Введём условие точного восстановления

$$P(x^2)\tilde{P}(x^{n-1}) = I_{2\times 2}, \quad I \text{ — единичная матрица},$$

отличное от условия точного восстановления в поле нечётной характеристики (см. [11]).

По правилу Крамера связь между полифазными компонентами (h, g) и $(\tilde{h}, \tilde{g})$ выражается соотношениями

$$\begin{aligned} g_o(x^2) &= \tilde{h}_e(x^{n-1}), \;\; g_e(x^2) = -\tilde{h}_o(x^{n-1}), \\ h_o(x^2) &= -\tilde{g}_e(x^{n-1}), \;\; h_e(x^2) = \tilde{g}_o(x^{n-1}). \end{aligned} \tag{1}$$

Информационное слово восстанавливается из кодового с помощью фильтров $\tilde{h}$ и $\tilde{g}$. В самом деле,

$$\begin{bmatrix} \tilde{h}_e(x^{n-1}) & \tilde{h}_o(x^{n-1}) \end{bmatrix} \begin{bmatrix} h_e(x^2) & g_e(x^2) \\ h_o(x^2) & g_o(x^2) \end{bmatrix} \begin{bmatrix} 1 \\ x^2 \end{bmatrix} =$$

$$= \begin{bmatrix} g_o(x^2) & -g_e(x^2) \end{bmatrix} \begin{bmatrix} h_e(x^2) + x^2 g_e(x^2) \\ h_o(x^2) + x^2 g_o(x^2) \end{bmatrix} =$$

$$= \big(h_e(x^2)g_o(x^2) - g_e(x^2)h_o(x^2)\big) + x^2\left(g_o(x^2)g_e(x^2) - g_e(x^2)g_o(x^2)\right) = 1\,.$$

Нам потребуется следующее утверждение.

Лемма 1. *Среди значений спектральной последовательности $\{F(\alpha^j)\}_{j=0}^{n-1}$ порождающего многочлена $F(x)$ найдутся $\frac{n-1}{2}$ ненулевых элементов.*

Доказательство. Так как отображение $i(x) = \sum_{j=0}^{\{(n-3)/2\}} i_j x^j \to c(x)$ инъективно, то в частотной области отображение

$$\{i(\alpha^j)\}_{j=0}^{n-1} \longrightarrow \{c(\alpha^j)\}_{j=0}^{n-1}$$

взаимно однозначно. Поэтому ранг отображения

$$\{i_0, \ldots, i_{\frac{n-3}{2}}\} \longrightarrow \{c(\alpha^j)\}_{j=0}^{n-1}$$

максимален и равен $\frac{n-1}{2}$. В частотной области имеем

$$c(\alpha^j) = F(\alpha^j) i(\alpha^{2j})\,, \;\; j = 0, \ldots, n-1. \tag{2}$$

Так как $\alpha^0, \alpha^2, \ldots, \alpha^{2(\frac{n-1}{2})}$ различны, то среди $F(\alpha^j)_{j=0}^{n-1}$ найдутся $\frac{n-1}{2}$ ненулевых элементов. □

2. Построение вейвлет-кода с максимальным кодовым расстоянием

В этом разделе будет доказано, что среди вейвлет-кодов имеются коды с максимальным кодовым расстоянием.

Как и выше, рассмотрим фильтр $h = \{h_k\}_{k=1}^{n-1}$ и комплементарный ему фильтр $g = \{g_k\}_{k=1}^{n-1}$. Введём полифазную матрицу

$$P(x^2) = \begin{bmatrix} h_e(x^2) & g_e(x^2) \\ h_o(x^2) & g_o(x^2) \end{bmatrix}, \quad \det P(x^2) = \det P(x) = 1.$$

С помощью лифтинга (см. [12]) по паре фильтров (h, g) строятся другие пары комплементарных фильтров (h, g_s) с полифазной матрицей

$$P_s(x^2) = P(x^2) \begin{bmatrix} 1 & s(x^2) \\ 0 & 1 \end{bmatrix},$$

где $s(x)$ — многочлен степени не больше $\frac{n-3}{2}$ с коэффициентами из поля $GF(2^m)$. Фильтр g_s, комплементарный h, имеет вид

$$g_s(x) = g(x) + h(x)s(x^2)\,.$$

Теорема 1. *Среди вейвлет-кодов над полем характеристики* 2 *имеются* $(n, \frac{n-1}{2})$*-коды с максимальным кодовым расстоянием.*

Доказательство. Пусть

$$F(x) = h(x) + x^2 g(x) \;\text{ и }\; F_s(x) = h(x) + x^2\left(g(x) + h(x)s(x^2)\right),$$

где $s(x) = s_0 + s_1 x + \cdots + s_{\frac{n-3}{2}} x^{\frac{n-3}{2}}$. Введём дополнительный параметр β и положим $h^*(x) = \beta h(x)$ и $g^*(x) = \beta^{-1} g(x)$. Через $F_s^*(x)$ будем обозначать функцию

$$h^*(x) + x^2(g^*(x) + h^*(x)s(x^2)) \bmod (x^n - 1).$$

Построим лифтинговый многочлен $s(x)$, такой, что

$$F_s^*(\alpha^{2^{m-1}}) = F_s^*(\alpha^{2^{m-1}+1}) = \cdots = F_s^*(\alpha^n) = 0\,.$$

Будем предполагать, что $h(\alpha^i) \neq 0$ при $i = 2^{m-1}, \ldots, 2^m - 1 = n$. Многочлен $s(x)$ определяется из системы уравнений

$$s(\alpha^{2i}) = -(\alpha^{-2i} + \beta^{-2} g(\alpha^i)/h(\alpha^i)), \;\; i = 2^{m-1}, \ldots, n\,.$$

Из первых $2^{m-1} - 1$ уравнений находятся $s_0, s_1, \ldots, s_{\frac{n-3}{2}}$ как линейные функции параметра β^{-2}. Подставив найденные переменные в последнее уравнение, найдём значение переменной β^{-2} и затем $s_0, s_1, \ldots, s_{\frac{n-3}{2}}$.

Положим, например, $g_o(1) = 0$ и зададим $g_o(\alpha^{2i})$, $i = 2^{m-1}, \ldots, n-1$ (всего $2^{m-1}-1$ значений). Дополнительно потребуем, чтобы $h_0(\alpha^{2i}) \neq 0$ при $i = 2^{m-1}, \ldots, n$. Тогда $h_e(\alpha^{2i})$ находятся из соотношений $h_e(\alpha^{2i}) = h(\alpha^i) - \alpha^i h_0(\alpha^{2i})$ при указанных значениях i.

Заметим, что многочлен $g(x)$ выражается через $g_o(x)$, если многочлен $h(x)$ известен. В самом деле,

$$g(x) = \frac{g_e(x^2)h_o(x^2) + xg_o(x^2)h_o(x^2)}{h_0(x^2)} = \\ = \frac{h_e(x^2)g_o(x^2) + xg_o(x^2)h_o(x^2) + 1}{h_0(x^2)} = \frac{g_o(x^2)h(x) + 1}{h_o(x^2)}.$$

Пусть $g(x) = g_o + g_1x + g_2x^2 + \cdots + g_{n-1}x^{n-1}$, тогда $g_o(x) = g_1 + g_3x + \cdots + g_{n-2}x^{\frac{n-3}{2}}$. Всего неизвестных коэффициентов $\frac{n-3}{2} + 1 = 2^{m-1} - 1$. Заданных значений $g_o(\alpha^{2i})$, $i = 2^{m-1}, \ldots, n-1$, достаточно, чтобы найти коэффициенты многочлена $g_o(x)$.

Группа $GF(2^m)^*$ ненулевых элементов поля $GF(2^m)$ является циклической. Поэтому для того, чтобы многочлены $h(x)$ и $g(x)$ были комплементарными, достаточно потребовать при всех $i = 0, \ldots, n-1$ выполнения соотношений

$$\det \begin{bmatrix} h_e(\alpha^i) & g_e(\alpha^i) \\ h_o(\alpha^i) & g_o(\alpha^i) \end{bmatrix} = 1.$$

Так как $g_o(\alpha^{2i})$ заданы при значениях $i = 2^{m-1}, \ldots, n$, то из условия комплементарности $h_e(\alpha^{2i})g_o(\alpha^{2i}) - h_o(\alpha^{2i})g_e(\alpha^{2i}) = 1$ находим

$$g_e(\alpha^{2i}) = \frac{h_e(\alpha^{2i})g_o(\alpha^{2i}) + 1}{h_0(\alpha^{2i})}.$$

Тем самым $g(\alpha^i) = g_e(\alpha^{2i}) + \alpha^i g_o(\alpha^{2i})$ определены при $i = 2^{m-1}, \ldots, n$.

При $i = 1, 2, \ldots, 2^{m-1} - 1$ значения $h(\alpha^i)$ и $g(\alpha^i)$ выберем так, чтобы удовлетворить условию комплементарности. Таким образом, последовательности $\{h(\alpha^i)\}_{i=0}^{n-1}$ и $\{g(\alpha^i)\}_{i=0}^{n-1}$ построены. Выполняя обратное преобразование Фурье, находим коэффициенты комплементарных многочленов $h(x)$ и $g(x)$.

Для кодового многочлена $c(x) = i(x^2)F_s^*(x)$ спектральный многочлен имеет вид

$$\sum_{j=1}^{\frac{n-1}{2}} i(\alpha^{2j})F_s^*(\alpha^j)y^j = y\left(\sum_{j=0}^{\frac{n-3}{2}} i(\alpha^{2j+2})F_s^*(\alpha^{j+1})y^j\right).$$

Число ненулевых корней этого многочлена не превышает $\frac{n-3}{2}$. Поэтому вес кодового вектора длиной n не более $n - \frac{n-3}{2} = \frac{n+3}{2}$.

Так как $n - k + 1 = n - \frac{n-1}{2} + 1 = \frac{n+3}{2}$, то по теореме Синглтона кодовое расстояние равно $\frac{n+3}{2}$. Тем самым построенный $\left(n, \frac{n-1}{2}\right)$-вейвлет-код имеет максимальное кодовое расстояние. □

Построенный код является линейным, так как группа $GF(2^m)^*$ является циклической.

Декодирование вейвлет-кода с максимальным кодовым расстоянием

В рассматриваемом случае длина информационного вектора равна $\frac{n-1}{2}$, кодовый многочлен имеет степень не более $n-1$, и в преобразовании Фурье $\{C_j = c(\alpha^j)\}$, $j = 0, \ldots, n-1$, кодовой последовательности $\{c_j\}_{j=0}^{n-1}$ компоненты $C_0, C_{\frac{n+1}{2}}, \ldots, C_{n-1}$ равны нулю.

Если α — примитивный элемент поля $GF(2^m)$, то α^{-1} также является примитивным элементом. Поэтому последовательность $\{\alpha^j c_j\}_{j=0}^{n-1}$ является кодовой последовательностью кода Рида — Соломона с параметрами $(n,\ (n-1)/2)$.

Согласно лемме (1) коэффициенты C_j, $j = 1, \ldots, \frac{n-1}{2}$, не равны нулю. Поэтому любой многочлен вида $\sum_{j=1}^{\frac{n-1}{2}} \beta_j y^j$ является спектральным многочленом, так как система уравнений

$$i(\alpha^{2k})F(\alpha^k) = \beta_k, \quad k = 1, \ldots, \frac{n-1}{2},$$

однозначно разрешима относительно коэффициентов $i_0, \ldots, i_{\frac{n-3}{2}}$ информационного многочлена. Таким образом, построенный код является $(n, \frac{n-1}{2})$-кодом Рида — Соломона во временной области.

К построенному коду применим алгоритм декодирования Берлекампа — Велча. Реализация алгоритма может быть найдена в [14]. Информационное слово восстанавливается по кодовому слову из системы (2) согласно лемме 1.

Пример кода с максимальным кодовым расстоянием

Рассмотрим конечное поле $GF(2^3)$, порождённое многочленом $x^3 + x + 1$. Следуя описанному выше методу, построим пример вейвлет-кода длины $n = 7$ с максимальным кодовым расстоянием. В качестве примитивного элемента выберем $\alpha = \alpha(x) = x$.

1. Выберем фильтр h с коэффициентами Фурье

$$\{h(\alpha^i)\}_{i=0}^{6} = \{\alpha^3, \alpha^3, \alpha^4, 0, \alpha^2, \alpha^2, \alpha^4\}.$$

Такой фильтр задаётся многочленом $h(x) = \alpha^5 x^6 + \alpha^4 x^5 + \alpha^6 x^4 + \alpha x^2 + \alpha^6 x$.

2. Его полифазные компоненты равны $h_e(x) = \alpha^5 x^3 + \alpha^6 x^2 + \alpha x$, $h_o(x) = \alpha^4 x^2 + \alpha^6$.

3. Алгоритм Евклида нахождения НОД для полифазных компонент даёт разложение

$$\begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} = \begin{bmatrix} \alpha x + \alpha^2 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha x + \alpha^6 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha x + \alpha^6 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha^5 & 0 \\ 0 & \alpha^2 \end{bmatrix} =$$
$$= \begin{bmatrix} \alpha^5 x^3 + \alpha^6 x^2 + \alpha x & x^2 + \alpha^6 x + \alpha \\ \alpha^4 x^2 + \alpha^6 & \alpha^6 x + \alpha^4 \end{bmatrix}.$$

4. Полифазные компоненты комплементарного фильтра представляются как $g_e(x) = x^2 + \alpha^6 x + \alpha$, $g_o(x) = \alpha^6 x + \alpha^4$.

5. Таким образом, комплементарный фильтр записывается в виде

$$g(x) = x^4 + \alpha^6 x^3 + \alpha^6 x^2 + \alpha^4 x + \alpha.$$

6. Система уравнений для коэффициентов лифтинг-многочлена $s(x)$ и коэффициента β имеет вид

$$\begin{cases} s_0 + \alpha s_1 + \alpha^2 s_2 + \alpha\beta^{-2} = \alpha^6, \\ s_0 + \alpha^3 s_1 + \alpha^6 s_2 + \alpha^2\beta^{-2} = \alpha^4, \\ s_0 + \alpha^5 s_1 + \alpha^3 s_2 + \alpha\beta^{-2} = \alpha^2. \\ s_0 + s_1 + s_2 + \alpha^3\beta^{-2} = 1. \end{cases}$$

Решая систему, находим $s(x) = \alpha^3 x^2 + \alpha^4 x + \alpha^5$ и $\beta = 1$.

7. Многочлен комплементарного фильтра с учётом лифтинга имеет представление $g(x) = \alpha^4 x^6 + \alpha^2 x^3 + x^2$.

8. Спектральная последовательность порождающего многочлена $F(x) = \alpha^5 x^6 + \alpha x^5 + \alpha^2 x^4 + \alpha x^2 + \alpha^3 x$ равна $\{0, \alpha^3, \alpha^4, \alpha^6, 0, 0, 0\}$ и определяет (7, 3)-код с максимальным кодовым расстоянием $d = 5$.

Порождающей матрицей кода является матрица

$$\begin{bmatrix} 0 & \alpha^3 & \alpha & 0 & \alpha^2 & \alpha & \alpha^5 \\ \alpha & \alpha^5 & 0 & \alpha^3 & \alpha & 0 & \alpha^2 \\ 0 & \alpha^2 & \alpha & \alpha^5 & 0 & \alpha^3 & \alpha \end{bmatrix}.$$

Зададим информационный многочлен $i(x) = \alpha x^2 + \alpha^2 x + 1$ и внесём ошибку $e(x) = x^4$ в кодовое слово. Тогда для кодового многочлена

$$c(x) = \alpha^6 x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha x^3 + \alpha^4 x^2 + x + \alpha^3$$

многочлен ошибочной последовательности имеет вид

$$r(x) = \alpha^6 x^6 + \alpha^2 x^5 + \alpha^4 x^4 + \alpha x^3 + \alpha^4 x^2 + x + \alpha^3 = \sum_{j=0}^{6} r_j x^j.$$

Процедура декодирования осуществляется согласно [14] за несколько шагов:

1. На первом шаге строится интерполяционный многочлен $T(x)$, такой, что $T(\alpha^i) = r_i \;\; i = 0, \ldots, 6$. Получим $T(x) = \alpha^3 x^6 + \alpha^6 x^5 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha x^2 + \alpha^4 x + 1$.

2. Расширенный алгоритм Евклида для многочленов $x^n - 1$ и $T(x)$ выполняем до тех пор, пока степень остатка не станет меньше $(n + \frac{n-1}{2})/2 = 5$:

$$(x^7 + 1) + (\alpha^4 x + 1)T(x) = x^4 + \alpha^3 x^3.$$

Введём обозначения $P(x) = x^4 + \alpha^3 x^3$, $W(x) = \alpha^4 x + 1$.

3. Преобразование Фурье исправленного кодового слова находится делением многочлена $P(x)$ на многочлен $W(x)$:

$$M(x) = \frac{P(x)}{W(x)} = \alpha^3 x^3.$$

4. Исправленное кодовое слово получаем с помощью обратного преобразования Фурье.

5. Восстанавливаем информационное слово с помощью системы (2) для $j = 1, 2, 3$:

$$\begin{cases} i_0 + \alpha^2 i_1 + \alpha^4 i_2 = 0, \\ i_0 + \alpha^4 i_1 + \alpha i_2 = 0, \\ i_0 + \alpha^6 i_1 + \alpha^5 i_2 = \alpha^4. \end{cases}$$

Решением системы является информационный вектор $(1, \alpha^2, \alpha)$.

3. Построение вейвлет-кода с заданным кодовым расстоянием

В этом разделе будет показано, что для любого d, $0 < d < (n-3)/2$, среди вейвлет-кодов найдутся коды с кодовым расстоянием $d + 2$.

Если порождающая матрица имеет вид

$$G = \begin{bmatrix} h_e(x^2) + x^2 g_e(x^2) \\ h_o(x^2) + x^2 g_o(x^2) \end{bmatrix},$$

то проверочная матрица запишется в виде

$$H = \begin{bmatrix} \tilde{h}_e(x^{n-1}) + x^{n-2}\tilde{g}_e(x^{n-1}) & \tilde{h}_o(x^{n-1}) + x^{n-2}\tilde{g}_o(x^{n-1}) \end{bmatrix}.$$

Учитывая (1), проверочное соотношение при вейвлет-кодировании перепишется следующим образом:

$$\begin{bmatrix} g_o(x^2) - x^{n-2}h_o(x^2) & g_e(x^2) - x^{n-2}h_e(x^2) \end{bmatrix} \begin{bmatrix} c_e(x^2) \\ c_o(x^2) \end{bmatrix} = 0.$$

Выполнив действия, представим проверочное соотношение в виде

$$-x^{n-2}c_e(x^2)h_o(x^2) + x^{n-2}c_o(x^2)h_e(x^2) = -c_e(x^2)g_o(x^2) + c_o(x^2)g_e(x^2)$$

или

$$c_o(x^2)h_e(x^2) - c_e(x^2)h_o(x^2) = x^2\big(c_o(x^2)g_e(x^2) - c_e(x^2)g_o(x^2)\big)\,. \tag{3}$$

Напомним, что полифазные компоненты фильтров h и g связаны условием комплементарности

$$g_o(x^2)h_e(x^2) - g_e(x^2)h_0(x^2) = 1\,.$$

Лемма 2. *Для любого d, $0 < d < (n-3)/2$, существуют многочлены $h(x)$ и $g(x)$ степени не больше $n-1$, для которых имеют место равенства*

$$h(\alpha^j) + \alpha^{2j}g(\alpha^j) = 0 \quad \textit{при} \quad j = 0, \ldots, d\,.$$

Доказательство. Построим $h(x)$ и $g(x)$ таким образом, чтобы порождающий многочлен удовлетворял соотношениям $F(\alpha^i) = 0$, $i = 0, \ldots, d$. Этого можно добиться, если воспользоваться теоремой о лифтинге [12]. В самом деле, пусть $s(x)$ — корректирующий лифтинг-многочлен степени $\frac{n-1}{2} - 1$. В частотной области кодовый вектор запишется в виде

$$i(\alpha^{2i})\big(h(\alpha^i) + \alpha^{2i}g(\alpha^i)\big) = C_i, \quad i = 0, \ldots, n-1\,.$$

С учётом лифтинга приходим к системе

$$h(\alpha^i) + \alpha^{2i}(g(\alpha^i) + h(\alpha^i)s(\alpha^{2i})) = F(\alpha^i), \quad i = 0, \ldots, \frac{n-3}{2}\,, \tag{4}$$

где $F(\alpha^i) = 0$, $i = 0, \ldots, d$. Выберем многочлен $h(x)$ так, чтобы

$$h(\alpha^i) \neq 0, \quad i = 0, \ldots, \frac{n-3}{2}.$$

Из соотношений (4) находим

$$s(\alpha^{2i}) = -\big(\alpha^{-2i}(h(\alpha^i)) - g(\alpha^i)\big)(h(\alpha^i))^{-1}, \quad i = 0, \ldots, \frac{n-3}{2}. \tag{5}$$

Относительно коэффициентов $s_0, s_1, \ldots, s_{\frac{n-3}{2}}$ система уравнений (5) разрешима, так как ранг системы максимален. □

Для построенных фильтров h и g_s для многочлена $h(x) + x^2 g_s(x)$ в частотной области получим

$$\big\{h(\alpha^i)) + \alpha^{2i}(g_s(\alpha^i)\big\}_{i=0}^{n-1} = \big(0, \ldots, 0, F(\alpha^{d+1}), \ldots, F(\alpha^{n-1})\big)\,.$$

Поэтому преобразование Фурье кодового многочлена $c(x)$, равное

$$c(\alpha^j) = i(\alpha^{2j})\big\{h(\alpha^i)) + \alpha^{2i}(g_s(\alpha^i))\big\}, \quad j = 0, \ldots, n-1,$$

запишется в виде $C = (0, \ldots, 0, C_{d+1}, \ldots, C_{n-1})$. Воспользуемся утверждением, что j-я временная компонента кодового вектора $\boldsymbol{c}$ равна нулю тогда и только тогда, когда α^{-j} является корнем многочлена

$$C(x) = C_{d+1}\, x^{d+1} + \cdots + C_{n-1}x^{n-1} = x^{d+1}\big(C_{d+1} + \cdots + C_{n-1}x^{n-d-2}\big)\,.$$

Так как число корней многочлена $C_{d+1} + \cdots + C_{n-1}x^{n-d-2}$ не превышает степени, то вес кодового слова $\boldsymbol{c}$ не может быть меньше числа $n - (n - d - 2)$. Поэтому минимальное кодовое расстояние построенного кода не меньше числа $d + 2$.

Теорема 2. *Для любого d, $0 < d < (n-3)/2$, среди построенных вейвлет-кодов над полем $GF(2^m)$ найдётся код с заданным кодовым расстоянием $d + 2$.*

Доказательство. В качестве спектрального многочлена выберем многочлен

$$C(x) = x^{d+1}(x - \alpha^{-d-2}) \ldots (x - \alpha^{-n+1}) = C_{d+1}x^{d+1} + C_{d+2}x^{d+2} + \cdots + C_{n-1}x^{n-1}$$

степени $n - 1$. Отметим, что первые $d + 1$ компонент последовательности $\{C_i\}_{i=0}^{n-1}$ равны нулю. Убедимся, что последовательность $c_i = C(\alpha^{-i})$ принадлежит одному из кодовых пространств и имеет вес равный $d + 2$.

В точках $x = \alpha^i$ условие комплементарности запишется в виде

$$h_e(\alpha^{2i})g_o(\alpha^{2i}) - h_o(\alpha^{2i})g_e(\alpha^{2i}) = 1, \quad i = 0, \ldots, n-1\,. \tag{6}$$

Принадлежность вектора $(c_0, c_1, \ldots, c_{n-1})$ кодовому пространству согласно (3) проверяется условиями

$$\begin{aligned} &g_e(\alpha^{2i})\alpha^i c_o(\alpha^{2i}) - g_o(\alpha^{2i})\alpha^i c_e(\alpha^{2i}) = \\ &= h_e(\alpha^{2i})\alpha^{-i} c_o(\alpha^{2i}) - h_o(\alpha^{2i})\alpha^{-i} c_e(\alpha^{2i})\,, \quad i = 0, \ldots, n-1\,. \end{aligned} \tag{7}$$

Кроме того, на многочлены $h(x)$ и $g(x)$ накладываются дополнительные условия:

$$h(\alpha^i) + \alpha^{2i} g(\alpha^i) = 0, \quad i = 0, \ldots, d\,.$$

Перепишем эти соотношения в виде

$$h_e(\alpha^{2i}) + \alpha^{2i} g_e(\alpha^{2i}) + \alpha^i (h_o(\alpha^{2i}) + \alpha^{2i} g_o(\alpha^{2i})) = 0\,. \tag{8}$$

Покажем, что системы уравнений (6), (7) и (8) совместно разрешимы.

Полагая $i = 0, \ldots, d$, умножим последнее соотношение на $g_o(\alpha^{2i})$ и вычтем из условия комплементарности. Получим

$$-h_o(\alpha^{2i})g_e(\alpha^{2i}) - \alpha^{2i} g_e(\alpha^{2i})g_o(\alpha^{2i}) - \alpha^i h_o(\alpha^{2i})g_o(\alpha^{2i}) - \alpha^{3i} g_o(\alpha^{2i})g_o(\alpha^{2i}) = 1\,.$$

Отсюда выразим $h_o(\alpha^{2i})$:

$$h_o(\alpha^{2i}) = -\frac{1}{g_e(\alpha^{2i}) + \alpha^i g_o(\alpha^{2i})} - \alpha^{2i} g_o(\alpha^{2i})\,. \tag{9}$$

Подставим $h_o(\alpha^{2i})$ в условие комплементарности, найдём $h_e(\alpha^{2i})$:

$$h_e(\alpha^{2i}) = -\alpha^{2i} g_e(\alpha^{2i}) + \frac{\alpha^i}{g_e(\alpha^{2i}) + \alpha^i g_o(\alpha^{2i})}\,. \tag{10}$$

Зная $h_e(\alpha^{2i})$ и $h_o(\alpha^{2i})$, из проверочного соотношения находим

$$\alpha^{-i}\frac{c_o(\alpha^{2i})\alpha^i + c_e(\alpha^{2i})}{g_e(\alpha^{2i}) + \alpha^i g_o(\alpha^{2i})} = 0\,.$$

Выберем $g(\alpha^i) \neq 0$, $i = 0, \ldots, d$. В этом случае приходим к равенству

$$c_o(\alpha^{2i})\alpha^i + c_e(\alpha^{2i}) = c(\alpha^i) = C_i = 0\,.$$

Таким образом, выбирая $g_e(\alpha^{2i})$ и $g_o(\alpha^{2i})$ так, чтобы знаменатель в (9) и (10) не обращался в нуль, находим $h_e(\alpha^{2i})$ и $h_o(\alpha^{2i})$. Из (9) и (10) следует, что $h(\alpha^i) = \alpha^{2i} g(\alpha^i)$, $i = 0, \ldots, d$. В частности, получаем, что $h(\alpha^i) \neq 0$.

При $i = d+1, \ldots, n-1$ из соотношений (6) и (7) составим системы уравнений

$$\begin{cases} h_e(\alpha^{2i})g_o(\alpha^{2i}) - h_o(\alpha^{2i})g_e(\alpha^{2i}) = 1, \\ g_o(\alpha^{2i})\alpha^{2i}c_e(\alpha^{2i}) - g_e(\alpha^{2i})\alpha^{2i}c_o(\alpha^{2i}) = h_o(\alpha^{2i})c_e(\alpha^{2i}) - h_e(\alpha^{2i})c_o(\alpha^{2i}). \end{cases} \tag{11}$$

Определитель Δ_i i-й системы (11) относительно $h_e(\alpha^{2i})$ и $h_o(\alpha^{2i})$ имеет вид

$$\Delta_i = \begin{vmatrix} -g_e(\alpha^{2i}) & g_o(\alpha^{2i}) \\ c_e(\alpha^{2i}) & -c_o(\alpha^{2i}) \end{vmatrix}, \quad i = d+1, \ldots, n-1.$$

В предположении, что вторая строка матрицы определителя ненулевая, систему уравнений перепишем следующим образом:

$$\begin{cases} h_e(\alpha^{2i})g_o(\alpha^{2i}) - h_o(\alpha^{2i})g_e(\alpha^{2i}) = 1, \\ h_e(\alpha^{2i})c_o(\alpha^{2i}) + h_o(\alpha^{2i})c_e(\alpha^{2i}) = \alpha^{2i}\Delta_i\,. \end{cases} \tag{12}$$

Выберем $g_e(\alpha^{2i})$ и $g_o(\alpha^{2i})$ так, чтобы $\Delta_i \neq 0$. Тогда $h_e(\alpha^{2i})$ и $h_o(\alpha^{2i})$ определятся из системы (12). Решением системы являются

$$h_o(\alpha^{2i}) = \Delta_i^{-1}c_o(\alpha^{2i}) + \alpha^{2i}g_o(\alpha^{2i}) \;\text{ и }\; h_e(\alpha^{2i}) = \Delta_i^{-1}c_e(\alpha^{2i}) + \alpha^{2i}g_e(\alpha^{2i})\,.$$

Отсюда находим $F(\alpha^i) = h(\alpha^i) + \alpha^{2i}g(\alpha^i) = \Delta_i^{-1}c(\alpha^i)$. В частности, имеем

$$F(\alpha^{d+1}) = \Delta_{d+1}^{-1}c(\alpha^{d+1}) = \Delta_{d+1}^{-1}C_{d+1} = \Delta_{d+1}^{-1}\prod_{j=d+2}^{n-1}\alpha^{-j} \neq 0.$$

Если же вторая строка нулевая, то второе уравнение тождественно выполняется. В этом случае выберем $g_e(\alpha^{2i})$, $g_o(\alpha^{2i})$, $h_e(\alpha^{2i})$ и $h_o(\alpha^{2i})$ так, чтобы выполнялось условие комплементарности.

По найденным $\{h_e(\alpha^{2i})\}_{i=0}^{n-1}$ и $\{h_o(\alpha^{2i})\}_{i=0}^{n-1}$ вычисляем $\{h(\alpha^i)\}_{i=0}^{n-1}$. Так как в поле характеристики 2 все α^{2i}, $i = 0, \ldots, n-1$, различны, из системы линейных уравнений относительно $h_0, h_1, \ldots, h_{n-1}$ находим многочлен $h(x)$. Аналогично строится многочлен $g(x)$.

Таким образом, фильтры $h(x)$ и $g(x)$ обладают необходимыми свойствами, так как удовлетворяют условию комплементарности и первые $d+1$ компонент последовательности $\{h(\alpha^i) + \alpha^{2i}g(\alpha^i)\}_{i=0}^{n-1}$ равны нулю. Кроме того, вектор $\boldsymbol{c}$ удовлетворяет проверочному соотношению, а значит, является кодовым вектором построенного вейвлет-кода и имеет заданное кодовое расстояние. В самом деле, согласно лемме 2, кодовое расстояние не меньше числа $d+2$. С другой стороны, вес кодового многочлена по построению не более $n - (n - d - 2) = d + 2$. Значит, вес кодовой последовательности $\boldsymbol{c}$ равен $d+2$. Это доказывает, что построенный вейвлет-код имеет заданное кодовое расстояние. □

Декодирование вейвлет-кода с заданным кодовым расстоянием

Пусть $i(x) = \sum_{k=0}^{(n-3)/2} i_k x^k$ — информационный многочлен с коэффициентами i_k, $k = 0, \ldots, (n-3)/2$, и $c(x) = i(x^2)(h(x) + ax^2 g(x))$ — кодовый многочлен. Через $C_j = c(\alpha^i)$, $j = 0, \ldots, n-1$, где $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, обозначим преобразование Фурье кодового многочлена. Будем считать, что фильтры $h(x)$ и $g(x)$ подобраны так, что спектральная последовательность имеет вид $\big(0, \ldots, 0, C_{d+1}, C_{d+2}, \ldots, C_{n-1},\big)$. Для $C(x) = C_{d+1}x^{d+1} + C_{d+2}x^{d+2} + \cdots + C^{n-1}x^{n-1}$ имеем $C(\alpha^{-j}) = c_j$, $j = 0, \ldots, n-1$.

Если α — примитивный элемент поля $GF(2^m)$, то α^{-1} также является примитивным элементом. Значит, обратное преобразование Фурье последовательности $\{C_i\}_{i=0}^{n-1}$ является кодовой последовательностью кода Рида — Соломона с параметрами $(n, n-d-1)$.

Поэтому к зашумлённым кодовым словам вейвлет-кода применим, например, алгоритм Берлекампа — Велча декодирования алгебраических кодов (см. [14]). Информационное слово восстанавливается по кодовому слову из системы (2) согласно лемме 1.

Пример кода с заданным кодовым расстоянием

Построим пример (7, 3)-кода над $GF(2^3)$ с кодовым расстоянием 3. Для этого зададим параметр $d = 1$ (так что $d + 2 = 3$). Как и в предыдущем примере, в качестве неприводимого многочлена выберем $x^3 + x + 1$ и в качестве примитивного элемента возьмём $\alpha = \alpha(x) = x$.

1. Спектральный многочлен кодового слова имеет вид

$$C(x) = x^2(x - \alpha^{-3})(x - \alpha^{-4})(x - \alpha^{-5})(x - \alpha^{-6}) = x^6 + \alpha^3 x^5 + x^4 + \alpha x^3 + \alpha^3 x^2.$$

2. Выполнив обратное преобразование Фурье, получим кодовый многочлен $c(x) = x^2 + \alpha^3 x + \alpha$.

3. Полифазные компоненты кодового многочлена равны соответственно $c_e(x) = x + \alpha$, $c_o(x) = \alpha^3$.

4. Выберем $g_e(x)$ и $g_o(x)$ так, чтобы знаменатель в (9) и (10) не обращался в нуль. Пусть $g_e(x) = x^2 + \alpha^4$ и $g_o(x) = x$. Тогда

$$\{g_e(\alpha^{2i}) + \alpha^i g_o(\alpha^{2i})\}_{i=0}^{n-1} = \{\alpha^4, \alpha^3, 1, \alpha^6, \alpha^6, 1, \alpha^3\}.$$

5. Находим $g(x)$ из полифазных компонент: $g(x) = x^4 + x^3 + \alpha^4$.

6. Определители системы (11) равны

$$\{\Delta_i\}_{i=0}^{n-1} = \{1, \alpha^6, \alpha, \alpha^6, \alpha^4, \alpha^4, \alpha\}.$$

7. Решением системы (11) являются

$$\{h_e(\alpha^{2i})\}_{i=0}^{n-1} = \{\alpha^2, \alpha^5, \alpha^5, 0, \alpha^2, \alpha^4, 1\}, \quad \{h_o(\alpha^{2i})\}_{i=0}^{n-1} = \{\alpha, 0, \alpha^4, 1, 1, 0, \alpha^5\}.$$

8. Находим коэффициенты Фурье для $h(x)$:

$$\{h(\alpha^i)\}_{i=0}^{n-1} = \{\alpha^4, \alpha^5, \alpha, \alpha^3, \alpha, \alpha^4, \alpha^5\}.$$

9. С помощью обратного преобразования Фурье вычисляем $h(x)$:

$$h(x) = \alpha x^5 + \alpha^2 x^4 + \alpha^4 x^3 + \alpha^5 x^2 + \alpha x + \alpha^3.$$

10. Спектральная последовательность порождающего многочлена $F(x) = x^6 + \alpha^3x^5+\alpha^2x^4+\alpha^4x^3+x^2+\alpha x+\alpha^3$ равна $\{0, 0, \alpha^2, \alpha^2, \alpha^3, \alpha^6, \alpha^6\}$ и определяет (7, 3)-код с кодовым расстоянием 3. Порождающая матрица кода имеет вид

$$\begin{bmatrix} \alpha^3 & \alpha & 1 & \alpha^4 & \alpha^2 & \alpha^3 & 1 \\ \alpha^3 & 1 & \alpha^3 & \alpha & 1 & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^2 & \alpha^3 & 1 & \alpha^3 & \alpha & 1 \end{bmatrix}.$$

Осуществим процедуру декодирования. В качестве информационного многочлена выберем $i(x) = \alpha x^2+\alpha x+1$ и введём ошибку $e(x) = x^4$. Информационный многочлен выбран так, чтобы спектральный многочлен кодового слова $c(x) = x^2+\alpha^3x+\alpha$ совпал с многочленом $C(x) = \alpha^3x^2+\alpha x^3+x^4+\alpha^3x^5+x^6$, рассмотренным в теореме 2.

В качестве спектрального примем многочлен

$$U(x) = x^{-2}C(x) = \alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4.$$

В качестве кодовой последовательности $\{u_j = U(\alpha^{-j}) = \alpha^{2j}c_j\}_{j=0}^6$ рассмотрим вектор $\{\alpha, \alpha^5, \alpha^4, 0, 0, 0, 0\}$. Тогда многочлен ошибочной последовательности примет вид $r(x) = \alpha + \alpha^5x + \alpha^4x^2 + \alpha x^4$. Далее следуем рекомендациям статьи [14]:

1. Построим интерполяционный многочлен, такой, что $T(\alpha^j) = r_j$. Выполняя прямое преобразование Фурье, находим $T(x) = 1+\alpha^6x+\alpha^6x^2+\alpha^4x^3+\alpha x^4+x^5+\alpha^4x^6$.

2. Расширенный алгоритм Евклида для многочленов $x^n - 1$ и $T(x)$ выполняем до тех пор, пока степень остатка не станет меньше $(n + \frac{n-1}{2})/2 = 5$:

$$(x^7 + 1) = (\alpha^3x + \alpha^6)T(x) + \alpha^3x^5 + \alpha^5x^3 + \alpha^3x^2 + \alpha^2x + \alpha^2.$$

Введём $P(x) = \alpha^3x^5 + \alpha^5x^3 + \alpha^3x^2 + \alpha^2x + \alpha^2$ и $W(x) = \alpha^3x + \alpha^6$.

3. Спектральный многочлен $U(x)$ преобразования Фурье кодового слова $\{u_j\}_{j=0}^6$ находится делением многочлена $P(x)$ на многочлен $W(x)$:

$$U(x) = \frac{P(x)}{W(x)} = \alpha^3 + \alpha x + x^2 + \alpha^3x^3 + x^4.$$

4. На заключительном шаге восстанавливаем спектральный многочлен: $C(x) = x^2U(x)$.

Заключение

В работе вводится полифазный метод помехоустойчивого кодирования над полем $GF(2^m)$. В качестве приложений полифазной схемы строятся коды с заданным кодовым расстоянием.

Результатом построения являются подпространства кодов Рида — Соломона во временной области.

Список литературы

1. **Мак-Вильямс, Ф. Дж.** Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М. : Связь, 1979. — 744 с.
2. Double circulant self-dual codes using finite-field wavelet transforms / F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer // Applied Algebra, Algebraic Algorithms and Error Correcting Codes Conf. (Honolulu, HI, 1999). Lecture Notes in Computer Sciences. — 1999. — Vol. 1719. — P. 355–364.
3. Error Control Coding Using Finite-Field Wavelet Transforms / F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer // Atlante : Center for Signal Image Processing, Georgia Inst. of Technology. — 1999. — No. 30332. — P. 1–13.

4. **Добеши, И.** Десять лекций по вейвлетам / И. Добеши. — Ижевск : РТЦ Регуляр. и хаотич. динамика, 2001. — 464 с.
5. **Mallat, S.** A Wavelet Tour of Signal Processing / S. Mallat. — 2nd ed. — Academic Press, 1999. — 637 p.
6. **Phoong, S. M.** Paraunitary filter banks over finite fields / S. M. Phoong, P. P. Vaidyanathan // IEEE Trans. Signal Processing. — 1997. — Vol. 45, no. 6. — P. 1443–1457.
7. **Fekri, F.** Theory of paraunitary filter banks over fields of characteristic two / F. Fekri, R. M. Mersereau, R. W. Schafer // IEEE Trans. on Inform. Theory. — 2002. — Vol. 48, no. 11. — P. 2964-–2979.
8. **Fekri, F.** Finite-Field Wavelet Transforms with Applications in Cryptography and Coding / F. Fekri, F. Delgosha. — Prentice Hall PTR, 2010.
9. **Caire, G.** Wavelet transforms associated with finite cyclic groups / G. Caire, R. L. Grossman, H. V. Poor // IEEE Trans. on Inform. Theory. — 1993. — Vol. 39, no. 4. — P. 1157–1166.
10. **Fekri, F.** Theory of wavelet transform over finite fields / F. Fekri, R. M. Mersereau, R. W. Schafer // Proc. of IEEE Intern. Conf. on Acoustics, Speech, and Signal Processing. — 1999. — Vol. 3. — P. 1213–1216.
11. **Chernikov, D. V.** Error-correcting codes using biorthogonal filter banks / D. V. Chernikov // Siberian Electronic Mathematical Rep. — 2015. — Vol. 12. — P. 704–713.
12. **Doubechies, I.** Factoring wavelet transforms into lifting steps / I. Doubechies, W. Sweldens // The J. of Fourier Analysis and Applications. — 1998. — Vol. 4, no. 3. — P. 247–269.
13. **Berlekamp, E.** Error Correction of Algebraic Block Codes / E. Berlekamp, L. Welch. — US Patent Number 4,633,470.
14. **Fedorenko, S. V.** A simple algorithm for decoding Reed — Solomon codes and its relation to the Welch — Berlekamp algorithm / S. V. Fedorenko // IEEE Trans. on Inform. Theory. — 2005. — Vol. 51, no. 3. — P. 1196–1198.

Поступила в редакцию 16.02.2017
После переработки 22.03.2017

Сведения об авторах

Соловьёв Александр Артёмович, доктор физико-математических наук, профессор, заведующий кафедрой компьютерной безопасности и прикладной алгебры, Челябинский государственный университет, Челябинск, Россия; e-mail: alsol@csu.ru.

Черников Дмитрий Владимирович, аспирант кафедры компьютерной безопасности и прикладной алгебры, Челябинский государственный университет, Челябинск, Россия; e-mail: cherninkiy@gmail.com.

Chelyabinsk Physical and Mathematical Journal. 2017. Vol. 2, iss. 1. P. 66–79.

BIORTHOGONAL WAVELET CODE IN FIELDS OF CHARACTERISTIC TWO

A.A. Soloviev[a], **D.V. Chernikov**[b]

Chelyabinsk State University, Chelyabinsk, Russia
[a] *alsol@csu.ru;* [b] *cherninkiy@gmail.com*

In this paper we propose a scheme for the constructing of error-correcting cyclic wavelet codes on the basis of the biorthogonal transformation over finite fields of the even characteristic. The method of such codes constructing uses the Euclidean algorithm of the polynomials greatest common divisor calculating. It simplifies the possibility of the constructing of wavelet codes with specified properties. It is proved that there are wavelet codes with a given code distance.

Keywords: *polyphasic scheme, biorthogonal transform, wavelet code, finite field.*

1. **MacWilliams F.J., Sloane N.J.A.** *The theory of error-correcting codes.* Moscow, Svyaz' Publ., 1979. 744 p. (In Russ.).
2. **Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W.** Double circulant self-dual codes using finite-field wavelet transforms. *Applied Algebra, Algebraic Algorithms and Error Correcting Codes Conference (Honolulu, HI, 1999), Lecture Notes in Computer Sciences*, 1999, vol. 1719, pp. 355–364.
3. **Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W.** Error Control Coding Using Finite-Field Wavelet Transforms. *Atlanta, Center for Signal Image Processing, Georgia Institute of Technology*, 1999, no. 30332, pp. 1–13.
4. **Daubechies I.** *Desyat' lektsiy po veyvletam* [Ten lectures on wavelets]. Izhevsk, RTTS Regulyarnaya i khaoticheskaya dinamika Publ., 2001. 464 p. (In Russ.).
5. **Mallat S.** *Wavelet Tour of Signal Processing.* 2nd ed. Academic Press, 1999.
6. **Phoong S.M., Vaidyanathan P.P.** Paraunitary filter banks over finite fields. *IEEE Transactions on Signal Processing*, 1997, vol. 45, no. 6, pp. 1443–1457.
7. **Fekri F., Mersereau R.M., Schafer R.W.** Theory of paraunitary filter banks over fields of characteristic two. *IEEE Transactions on Information Theory*, 2002, vol. 48, no. 11, pp. 2964–2979.
8. **Fekri F., Delgosha F.** *Finite-Field Wavelet Transforms with Applications in Cryptography and Coding.* Prentice Hall PTR, 2010.
9. **Caire G., Grossman R.L., Poor H.V.** Wavelet transforms associated with finite cyclic groups. *IEEE Transactions on Information Theory*, 1993, vol. 39, no. 4, pp. 1157–1166.
10. **Fekri F., Mersereau R.M., Schafer R.W.** Theory of wavelet transform over finite fields. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing*, 1999, vol. 3, pp. 1213–1216.
11. **Chernikov D.V.** Error-correcting codes using biorthogonal filter banks. *Siberian Electronic Mathematical Reports*, 2015, vol. 12, pp. 704–713.
12. **Doubechies I., Sweldens W.** Factoring Wavelet Transforms into Lifting Steps. *The Journal of Fourier Analysis and Applications*, 1998, vol. 4, no. 3, pp. 247–269.
13. **Berlekamp E., Welch L.** *Error Correction of Algebraic Block Codes.* US Patent Number 4,633,470.
14. **Fedorenko S.V.** A simple algorithm for decoding Reed — Solomon codes and its relation to the Welch — Berlekamp algorithm. *IEEE Transactions on Information Theory*, 2005, vol. 51, no. 3, pp. 1196–1198.

Accepted article received 16.02.2017
Corrections received 22.03.2017