

УДК 519.856

## ПОЛИФАЗНАЯ СХЕМА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ НАД ПОЛЯМИ НЕЧЁТНОЙ ХАРАКТЕРИСТИКИ

Д. В. Черников

Челябинский государственный университет, Челябинск, Россия  
cherninkiy@gmail.com

В работе представлена полифазная схема помехоустойчивого кодирования на основе двухканального набора фильтров точного восстановления и предложен метод построения кодов с максимальным кодовым расстоянием над полями нечётной характеристики.

**Ключевые слова:** помехоустойчивое кодирование, биортогональные преобразования, биортогональный набор фильтров, набор фильтров точного восстановления, вейвлет-преобразование над конечным полем.

### Введение

Современная теория помехоустойчивого кодирования создала большое число кодов с разнообразными свойствами, эффективно решающих задачи обнаружения и исправления ошибок при передаче информации. Помехоустойчивые коды являются обязательной составляющей систем связи, а также широко используются в электронных средствах хранения и обработки данных. Наиболее распространённые коды имеют более чем полувековую историю, хорошо изучены, алгоритмы их декодирования продолжают совершенствоваться. Дальнейшее развитие теории в части проектирования кодов происходит преимущественно за счёт композиции известных методов. Зачастую трудно ожидать, что новые кодовые конструкции, как простые, так и с комплексной структурой, превзойдут по вычислительной сложности известные способы построения кодов и исправления ошибок.

В то же время развитие получают методы построения помехоустойчивых кодов, опирающиеся на теорию из смежных математических дисциплин. Так, в [1] представлен подход к построению помехоустойчивых 2-циклических вейвлет-кодов с использованием ортогональных наборов фильтров точного восстановления, известных из цифровой обработки сигналов. При описании таких кодов применяется теория вейвлет-преобразований над конечным полем [2; 3]. Задача построения вейвлет-фильтров решена с помощью методов факторизации унитарных и параунитарных матриц над конечным полем в [3; 4]. В последующих работах был предложен ряд помехоустойчивых кодов [5] и [6], обладающих хорошими корректирующими свойствами.

Вейвлет-преобразование над конечным полем реализует разбиение пространства векторов с использованием ортогональных наборов фильтров точного восстановления. В то же время существует более гибкая конструкция, где класс допустимых фильтров шире. Это наборы фильтров, реализующие биортогональные разбиения.

Основные положения, касающиеся кодирования с использованием биортогональных преобразований над конечными полями, раскрыты в [7]. Терминология биортогональных преобразований над конечными полями заимствована из теории цифровой обработки сигналов [8].

В данной работе представлена полифазная схема помехоустойчивого кодирования и в качестве иллюстрации предложен метод построения биортогональных вейвлет-кодов с максимально возможным кодовым расстоянием.

Биортогональные коды определяются заданием двух пар фильтров. Используя лифтинг [9], можно подобрать фильтры таким образом, чтобы часть компонент преобразования Фурье порождающего многочлена обращалась в нуль, и код, генерируемый таким кодовым многочленом, как и в теории кодов Рида — Соломона, имеет заданное, в том числе максимальное возможное кодовое расстояние. Для исправления ошибок предлагается метод декодирования полиномиальных кодов на основе алгоритма Берлекемпа — Велча; см., например, простой алгоритм декодирования алгебраических кодов, изложенный в [12].

Выражаю благодарность своему научному руководителю А. А. Соловьеву за помощь в работе.

## 1. Полифазная схема биортогонального вейвлет-кода

Опишем основные положения, касающиеся биортогональных вейвлет-кодов (см. [7]) в полифазном представлении.

Рассмотрим поле  $GF(q)$ ,  $q = p^m$ . Пусть  $n \in \mathbb{N}$  чётно, фильтру  $h = \{h_k\}_{k=0}^{n-1}$  поставим в соответствие многочлен

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

Под полифазным представлением многочлена  $h(x)$  будем понимать запись его в виде суммы  $h(x) = h_e(x^2) + x h_o(x^2)$ , где

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

полифазные компоненты, содержащие только чётные и только нечётные коэффициенты фильтра  $h$  соответственно. Наряду с фильтром  $h$  будем рассматривать фильтры  $g$ ,  $\tilde{h}$ ,  $\tilde{g}$  и их полифазные представления.

Определим полифазные матрицы

$$P(x) = \begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} \quad \text{и} \quad \tilde{P}(x) = \begin{bmatrix} \tilde{h}_e(x) & \tilde{g}_e(x) \\ \tilde{h}_o(x) & \tilde{g}_o(x) \end{bmatrix}.$$

Фильтры  $h$  и  $g$  будем называть комплементарными, если определитель соответствующей полифазной матрицы  $\det P(x)$  равен единице.

Введём в рассмотрение операцию лифтинга (см. [9]), задаваемую некоторым многочленом  $s(x) \in GF(q)[x]/(x^{n/2} - 1)$  как домножение полифазной матрицы на треугольную матрицу специального вида

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

Иначе

$$\begin{bmatrix} h_e(x) & g_{se}(x) \\ h_o(x) & g_{so}(x) \end{bmatrix} = \begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} \begin{bmatrix} 1 & s(x) \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} h_e(x) & h_e(x)s(x) + g_e(x) \\ h_o(x) & h_o(x)s(x) + g_o(x) \end{bmatrix}.$$

Отметим, что операция лифтинга не меняет определитель полифазной матрицы, поэтому если  $h$  и  $g$  — пара комплементарных фильтров, то пара фильтров  $h$  и  $g_s$  также будет комплементарной, при этом многочлены  $h(x)$ ,  $g(x)$  и  $g_s(x)$  связаны соотношением

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

Далее рассмотрим две пары комплементарных фильтров  $(h, g)$  и  $(\tilde{h}, \tilde{g})$ . Будем говорить, что для заданных пар фильтров выполнено условие точного восстановления, если их полифазные матрицы  $P$  и  $\tilde{P}$  в кольце  $GF(q)[x]/(x^{n/2}-1)$  удовлетворяют соотношению

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

Пары фильтров  $(h, g)$  и  $(\tilde{h}, \tilde{g})$ , для которых выполняется условие точного восстановления, будем называть двойственными.

Из условия точного восстановления следует, что

$$P(x)^{-1} = \tilde{P}(x^{n/2-1})^t.$$

Для комплементарных пар фильтров методом Крамера получаем соотношения между полифазными компонентами двойственных фильтров

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

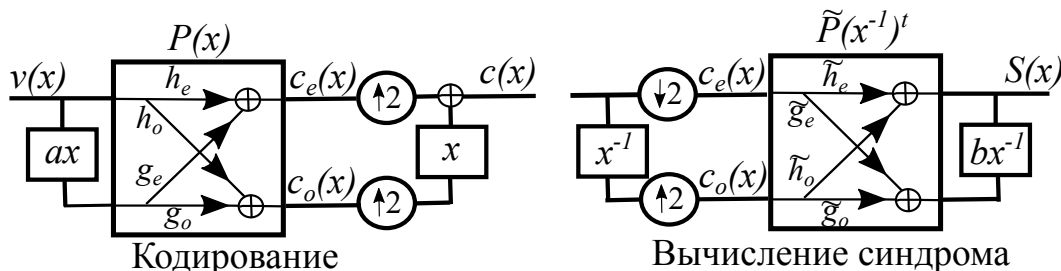
Из этих соотношений следует, что

$$\tilde{h}(x) = -xg(-x^{n/2-1}) \quad \text{и} \quad \tilde{g}(x) = xh(-x^{n/2-1}).$$

Определим процедуру полифазного кодирования

$$\begin{bmatrix} c_e(x) \\ c_o(x) \end{bmatrix} = \begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} \begin{bmatrix} 1 \\ ax \end{bmatrix} v(x) = \begin{bmatrix} h_e(x) + axg_e(x) \\ h_o(x) + axg_o(x) \end{bmatrix} v(x),$$

где  $v(x)$  — информационный многочлен степени не выше  $n/2 - 1$  и  $a \in GF(q)$  — константа,  $c(x)$  — многочлен кодового слова.



Полифазная схема биортогонального вейвлет-кода

Предложенная схема полифазного кодирования совпадает со схемой биортогонального вейвлет-кода (см. [7]), так как

$$h_e(x^2) + ax^2g_e(x^2) + x(h_o(x^2) + ax^2g_o(x^2)) = h(x) + ax^2g(x).$$

Пары фильтров  $(h, g)$  и  $(\tilde{h}, \tilde{g})$  со свойством точного восстановления обеспечивают возможность синдромного декодирования кодового многочлена  $c(x)$ :

$$S(x) = \begin{bmatrix} 1 & bx^{n/2-1} \end{bmatrix} \begin{bmatrix} \tilde{h}_e(x^{n/2-1}) & \tilde{h}_o(x^{n/2-1}) \\ \tilde{g}_e(x^{n/2-1}) & \tilde{g}_o(x^{n/2-1}) \end{bmatrix} \begin{bmatrix} c_e(x) \\ c_o(x) \end{bmatrix} = 0,$$

где  $b \in GF(q)$  — константа, такая, что  $ab = (p-1) \pmod p$ . В самом деле

$$\begin{aligned} & \begin{bmatrix} \tilde{h}_e(x^{n/2-1}) + bx^{n/2-1}\tilde{g}_e(x^{n/2-1}) & \tilde{h}_o(x^{n/2-1}) + bx^{n/2-1}\tilde{g}_o(x^{n/2-1}) \end{bmatrix} \begin{bmatrix} h_e(x) + axg_e(x) \\ h_o(x) + axg_o(x) \end{bmatrix} = \\ & = (g_o(x) - bx^{n/2-1}h_o(x))(h_e(x) + axg_e(x)) + (-g_e(x) + bx^{n/2-1}h_e(x))(h_o(x) + axg_o(x)) = \\ & = (g_o(x)h_e(x) - g_e(x)h_o(x)) + abx^{n/2}(-h_o(x)g_e(x) + h_e(x)g_o(x)) = \\ & = 1 + ab \cdot 1 = [1 + (p-1)] \pmod p = 0. \end{aligned}$$

Отметим, что преобразование кодирования инъективно. Поэтому по кодовому многочлену восстанавливается информационный многочлен:

$$\begin{aligned} & \begin{bmatrix} \tilde{h}_e(x^{n/2-1}) & \tilde{h}_o(x^{n/2-1}) \end{bmatrix} \begin{bmatrix} h_e(x) + axg_e(x) \\ h_o(x) + axg_o(x) \end{bmatrix} = g_o(x)(h_e(x) + axg_e(x)) - \\ & - g_e(x)(h_o(x) + axg_o(x)) = (g_o(x)h_e(x) - g_e(x)h_o(x)) = 1. \end{aligned} \quad (1)$$

## 2. Построение кода с максимальным расстоянием

Интерес представляют коды с большим кодовым расстоянием. Покажем, как над полями нечётной характеристики строятся вейвлет-коды с максимально возможным кодовым расстоянием.

Пусть во введённых ранее обозначениях  $p \neq 2$ ,  $n$  — чётно,  $\mathbf{v} = (v_0 \dots v_{n-1})$  — вектор над  $GF(q)$ ,  $\alpha$  — примитивный элемент поля. Дискретное преобразование Фурье определяется как вектор  $\mathbf{V} = \mathcal{F}(\mathbf{v}) = (V_0, \dots, V_{n-1})$  с компонентами

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

Обратное преобразование Фурье  $\mathbf{v} = \mathcal{F}^{-1}(\mathbf{V})$  имеет вид

$$v_i = (n)^{-1} \sum_{j=0}^{n-1} \alpha^{-ij} V_j,$$

здесь  $(n)$  интерпретируется как элемент поля, т. е. приводится по модулю  $p$ .

**Предложение 1.** Среди биортогональных вейвлет-кодов имеются коды с максимально возможным кодовым расстоянием.

*Доказательство.* Пусть  $\mathcal{F}(\mathbf{h}) = (h(\alpha^0), h(\alpha^1), \dots, h(\alpha^{n-1}))$  — преобразование Фурье вектора  $\mathbf{h} = (h_0, h_1, \dots, h_{n-1})$ . Докажем, что существуют многочлены  $h(x)$  и  $g(x)$ , для которых имеют место равенства

$$h(\alpha^j) + a\alpha^{2j}g(\alpha^j) = 0 \quad \text{при } j = \frac{n}{2}, \dots, n-1.$$

Если многочлен  $h(x)$  задан, то согласно теореме о лифтинге многочлен  $g(x)$  определяется с точностью до многочлена  $s(x)$  степени  $\leq \frac{n}{2} - 1$  (см. [9]):

$$\begin{pmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{pmatrix} \begin{pmatrix} 1 & s(x) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} h_e(x) & g_e(x) + h_e(x) \cdot s(x) \\ h_o(x) & g_o(x) + h_o(x) \cdot s(x) \end{pmatrix} = \begin{pmatrix} h_e(x) & g_{se}(x) \\ h_o(x) & g_{so}(x) \end{pmatrix},$$

где умножение реализуется в кольце полиномов  $GF(q)[x]/(x^{n/2} - 1)$ . Тогда

$$\begin{aligned} g_s(x) &= g_{se}(x^2) + xg_{so}(x^2) = g_e(x^2) + h_e(x^2)s(x^2) + x[g_o(x^2) + h_o(x^2)s(x^2)] = \\ &= g(x) + h(x)s(x^2). \end{aligned}$$

Добьёмся того, чтобы при  $i = \frac{n}{2}, \dots, n-1$  выполнялись соотношения

$$h(\alpha^i) + a\alpha^{2i}(g(\alpha^i) + h(\alpha^i)s(\alpha^{2i})) = 0. \quad (2)$$

Выберем многочлен  $h(x)$  так, чтобы

$$h(\alpha^i) \neq 0, \quad \text{при } i = \frac{n}{2}, \dots, n-1.$$

Оставшиеся частотные компоненты многочлена  $h(x)$  зададим произвольным образом.

Из (2) находим, что

$$s(\alpha^{2i}) = -g(\alpha^i)(h(\alpha^i))^{-1} - a^{-1}\alpha^{-2i}, \quad i = \frac{n}{2}, \dots, n-1.$$

Система линейных уравнений относительно коэффициентов многочлена  $s(x)$  степени  $\frac{n}{2} - 1$  имеет единственное решение, так как определителем системы является ненулевой определитель Вандермонда. В результате для многочленов  $h(x)$  и  $g_s(x)$  имеет место представление

$$\{h(\alpha^i) + a\alpha^{2i}g_s(\alpha^i)\}_{j=0}^{j=n-1} = (F(\alpha^0), \dots, F(\alpha^{\frac{n}{2}-1}), 0, \dots, 0),$$

где  $F(x) = h(x) + ax^2g(x)$ .

Таким образом, преобразование Фурье  $(C_0, \dots, C_{n-1})$  кодовой последовательности  $(c_0, \dots, c_{n-1})$  с компонентами

$$C_i = c(\alpha^i) = i(\alpha^{2i})(h(\alpha^i) + a\alpha^{2i}g_s(\alpha^i)), \quad i = 0, \dots, n-1,$$

имеет вид

$$\mathbf{C} = (C_0, \dots, C_{\frac{n}{2}-1}, 0, \dots, 0). \quad (3)$$

Далее рассуждаем, как в теории кодов Рида — Соломона:  $j$ -я временная компонента кодового вектора  $\mathbf{c}$  равна нулю тогда и только тогда, когда  $\alpha^{-j}$  является корнем многочлена  $C(x) = C_0 + C_1x + \dots + C_{n-1}x^{n-1}$ . В рассматриваемом случае степень многочлена  $C(x)$  не превышает  $\frac{n}{2} - 1$ . Поэтому многочлен  $C(x)$  может иметь в поле  $GF(p^m)$  не более  $\frac{n}{2} - 1$  корней. Следовательно, вес кодового вектора  $\mathbf{c}$  не может быть меньше числа  $n - (\frac{n}{2} - 1) = \frac{n}{2} + 1$ . Согласно же теореме Синглтона для кодового расстояния  $d_{\min}$  выполняется неравенство  $d_{\min} \leq n - \frac{n}{2} + 1 = \frac{n}{2} + 1$ . Поэтому вес кодового слова не больше  $\frac{n}{2} + 1$ , а значит,  $d_{\min} = \frac{n}{2} + 1$ .

По паре комплементарных фильтров  $(h, g)$  строим дополнительную пару фильтров  $(\tilde{h}, \tilde{g})$ . Тем самым построен 2-циклический  $(n, n/2)$  вейвлет-код с максимальным кодовым расстоянием.  $\square$

### 3. Помехоустойчивое декодирование

Пусть  $i(x) = i_0 + i_1x + \dots + i_{n/2-1}x^{n/2-1}$  — информационный многочлен,

$$c(x) = i(x^2)(h(x) + ax^2g(x)) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

соответствующий кодовый многочлен. Через  $C_j = c(\alpha^j)$ ,  $j = 0, \dots, n-1$ , обозначим преобразование Фурье кодового многочлена. Будем считать, что фильтры  $h(x)$  и  $g(x)$  подобраны так, что  $(C_0, C_1, \dots, C_{n/2-1}, 0, \dots, 0)$ . Для коэффициентов многочлена  $C(x) = C_0 + C_1x + \dots + C_{n/2-1}x^{n/2-1}$  имеют место соотношения  $c_j = (n)^{-1} C(\alpha^{-j})$ ,  $j = 0, \dots, n-1$ .

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

Поэтому построенный вейвлет-код является 2-циркулянтным подпространством кода Рида — Соломона и к зашумлённым кодовым словам применим алгоритм Берлекэмп — Велча декодирования алгебраических кодов [10]. Простая реализация алгоритма Берлекэмп — Велча предложена в [12].

Информационная последовательность восстанавливается из кодовой при помощи соотношения (1).

### 4. Примеры биортогональных вейвлет-кодов

Рассмотрим конечное поле  $GF(7)$ , в качестве примитивного элемента выберем  $\alpha = 3$ , положим  $a = 1$ . Следуя описанному выше методу, построим пример вейвлет-кода длины  $n = 6$  с максимальным кодовым расстоянием.

1. Выберем фильтр  $h$  с коэффициентами Фурье  $\{0, 0, 0, 1, 6, 1\}$ , такой фильтр задаётся многочленом  $h(x) = 4x^4 + 3x^3 + x^2 + 6$ .

2. Его полифазные компоненты имеют вид:  $h_e(x) = 4x^2 + x + 6$  и  $h_o(x) = 3x$ .

3. Алгоритм Евклида нахождения НОД для полифазных компонент даёт разложение

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

Тем самым получены полифазные компоненты фильтра  $g$ :  $g_e(x) = x + 2$  и  $g_o(x) = 6$ .

4. Комплементарный фильтр записывается в виде  $g(x) = x^2 + 6x + 2$ .

5. Система уравнений для коэффициентов лифтинг-многочлена  $s(x)$  имеет вид

$$\begin{cases} s_0 + s_1 + s_2 & = 2, \\ s_0 + 2s_1 + 4s_2 & = 3, \\ s_0 + 4s_1 + 2s_2 & = 4. \end{cases}$$

Решение системы:  $s(x) = x^2 + 5x + 3$ .

6. Многочлен комплементарного фильтра с учётом лифтинга имеет вид

$$g(x) = x^5 + 2x^4 + 2x^3 + 3x^2 + 2x + 6.$$

7. Многочлен  $F(x) = 2x^5 + 5x^3 + x + 1$  имеет спектр Фурье  $\{2, 2, 2, 0, 0, 0\}$  и задаёт (6, 3)-код с максимальным кодовым расстоянием  $d = 4$ .

Порождающая и проверочная матрицы равны соответственно

$$\begin{bmatrix} 1 & 1 & 0 & 5 & 0 & 2 \\ 0 & 2 & 1 & 1 & 0 & 5 \\ 0 & 5 & 0 & 2 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 5 & 0 & 1 & 6 & 2 & 0 \\ 2 & 0 & 5 & 0 & 1 & 6 \\ 1 & 6 & 2 & 0 & 5 & 0 \end{bmatrix}.$$

Осуществим процедуру декодирования. Зададим информационный многочлен  $i(x) = x^2 + 2x + 5$  и многочлен ошибки  $e(x) = x^4$ .

Многочлен соответствующего кодового слова и многочлен слова с ошибкой имеют вид

$$c(x) = x^4 + x^3 + 2x^2 + 5, \quad r(x) = 2x^4 + x^3 + 2x^2 + 5.$$

1. С помощью преобразования Фурье находим интерполяционный многочлен многочлена  $r(x)$

$$T(x) = 2x^5 + 4x^4 + x^3 + 4x^2 + 2x + 3.$$

2. Выполняем расширенный алгоритм Евклида для многочленов  $x^n - 1$  и  $T(x)$ , пока степень остатка не станет меньше числа  $(n + n/2)/2 = 3n/4$ :

$$(x^6 + 6) + (3x + 1)T(x) = 6x^3 + 3x^2 + 4x + 2.$$

Введём многочлены  $P(x)$  и  $W(x)$ , полагая

$$P(x) = 6x^3 + 3x^2 + 4x + 2, \quad W(x) = 3x + 1.$$

3. Преобразование Фурье исправленного кодового слова находится делением

$$M(x) = \frac{P(x)}{W(x)} = 2x^2 + 5x + 2.$$

4. Восстановленное кодовое слово получаем с помощью обратного преобразования Фурье и далее находим информационное слово.

Рассмотренные примеры реализованы в среде SageMath и доступны для ознакомления по ссылке [13].

## Заключение

Биортогональные вейвлет-коды с максимальным кодовым расстоянием подобны кодам Рида — Соломона, но являются 2-циклическими и в отличие от кодов Рида — Соломона строятся во временной области.

Другой отличительной особенностью построенных кодов является возможность восстановления информационного слова по кодовому с помощью пары двойственных фильтров (1), что даёт возможность декодирования во временной области по алгоритму Берлекэмпа — Велча.

## Список литературы

1. Error control coding using finite-field wavelet transforms / F. Fekri, S. W. McLaughlin, R. M. Mersereau, R. W. Schafer // Center for Signal Image Processing. — Georgia Institute of Technology, Atlanta, GA, 30332. — 1999. — P. 1–13.
2. Caire, G. Wavelet transforms associated with finite cyclic groups / G. Caire, R. L. Grossman, H. V. Poor // IEEE Transactions on Information Theory. 1993. — Vol. 39. — P. 1157–1166.

3. **Fekri, F.** Theory of paraunitary filter banks over fields of characteristic two / F. Fekri, R. M. Mersereau, R. W. Schafer // IEEE Transactions on Information Theory. — 2002. — Vol. 48. — P. 2964–2979.
4. **Phoong, S.M.** Paraunitary filter banks over finite fields / S.M. Phoong, P.P. Vaidyanathan // IEEE Transactions on Signal Processing. — 1997. — Vol. 45. — P. 1443–1457.
5. Decoding of half-rate wavelet codes, Golay code and more / F. Fekri, S. W. McLaughlin, R. M. Mersereau, R. W. Schafer // IEEE Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP). — 2001. — Vol. IV. — P. 2609–2612.
6. **Fekri, F.** Arbitrary rate maximum-distance separable wavelet codes / F. Fekri // IEEE Intern. Conf. on Acoustics, Speech and Signal Processing. — 2002. — Vol. 3. — P. 2253–6.
7. **Черников, Д. В.** Помехоустойчивое кодирование с использованием биортогональных наборов фильтров / Д. В. Черников // Сиб. электрон. мат. изв. — 2015. — Т. 12. — С. 704–713.
8. **Малла, С.** Вэйвлеты в обработке сигналов : пер. с англ. / С. Малла. — М. : Мир, 2005.
9. **Doubechies, I.** Factoring wavelet transforms into lifting steps. / I. Doubechies, W. Sweldens // The J. of Fourier Analysis and Applications. — 1998. — Vol. 4, iss. 3. — P. 247–269.
10. **Welch, L.** Error correction for algebraic block codes / L. Welch, E. R. Berlekamp. — U.S. Patent 4,633.470. Sept. 27, 1983.
11. **Blahut, R. E.** Algebraic methods for signal processing and communications coding / R. E. Blahut. — New York : Springer-Verlag, 1992.
12. **Федоренко, С. В.** Простой алгоритм декодирования алгебраических кодов / С. В. Федоренко // Информационно-управляющие системы. — 2008. — № 3. — С. 23–27.
13. **Chernikov, D.** Biorthogonal coding algorithm implementations. SageMath Cloud Services [Электронный ресурс]. — URL: [https:// cloud.sagemath.com/projects/1ccf53b4-fab7-4a6d-9e8a-11495608d884/files/biorth-codes-construct.sageaws](https://cloud.sagemath.com/projects/1ccf53b4-fab7-4a6d-9e8a-11495608d884/files/biorth-codes-construct.sageaws) (дата обращения: 01.09.2016).

*Поступила в редакцию 16.09.2016*

*После переработки 01.10.2016*

#### Сведения об авторе

**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. 2016. Vol. 1, iss. 3. P. 77–85.*

## THE POLYPHASIC SCHEME OF CODING THEORY OVER FIELDS OF ODD CHARACTERISTIC

**D.V. Chernikov**

*Chelyabinsk State University, Chelyabinsk, Russia*  
*cherninkiy@gmail.com*

The paper presents the polyphasic scheme of the error-correcting coding based on two-channel filter set the exact recovery and the method of construction of codes with maximum code distance over fields of odd characteristic.

**Keywords:** *error-correction coding, biorthogonal transform, biorthogonal set of filters, set of filters accurate recovery, wavelet-transform over a finite field.*

### References

1. **Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W.** Error Control Coding Using Finite-Field Wavelet Transforms. *Center for Signal Image Processing. Georgia Institute of Technology, Atlanta, GA, 30332*, 1999, Feb., pp. 1–13.
2. **Caire G., Grossman R.L., Poor H.V.** Wavelet transforms associated with finite cyclic groups. *IEEE Transactions on Information Theory*, 1993, vol. 39, pp. 1157–1166.
3. **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. 49, pp. 2964–2979.
4. **Phong S.M., Vaidyanathan P.P.** Paraunitary filter banks over finite fields. *IEEE Transactions on Signal Processing*, 1997, vol. 45, pp. 1443–1457.
5. **Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W.** Decoding of half-rate wavelet codes, Golay code and more. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2001, vol. IV, pp. 2609–2612.
6. **Fekri F.** Arbitrary rate maximum-distance separable wavelet codes. *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2002, vol. III, p. 2253–2256.
7. **Chernikov D.V.** Помехоустойчивое кодирование с использованием биортогональных наборов фильтров [Error-correcting codes using biorthogonal filter banks]. *Siberian Electronic Mathematical Reviews*, 2015, vol. 12, pp. 704–713. (In Russ.).
8. **Mallat S.** *A wavelet tour of signal processing*. 2nd edition. London, Academic Press, 1999. 637 p.
9. **Doubechies I., Sweldens W.** Factoring wavelet transforms into lifting steps. *The Journal of Fourier Analysis and Applications*, 1996, vol. 4, iss. 3.
10. **Welch L., Berlekamp E.R.** *Error correction for algebraic block codes*. U.S. Patent 4,633,470. September 27, 1983.
11. **Blahut R.E.** *Algebraic methods for signal processing and communications coding*. New York, Springer-Verlag, 1992.
12. **Fedorenko S.V.** A simple algorithm for decoding algebraic codes. *Information and control systems*, 2008, no. 3, pp. 23–27.
13. **Chernikov D.** *Biorthogonal coding algorithm implementations*. Available at: SageMath Cloud Services, <https://cloud.sagemath.com/projects/1ccf53b4-fab7-4a6d-9e8a-11495608d884/files/biorth-codes-construct.sagews>, accessed 01.09.2016.

*Accepted article received 16.09.2016*

*Corrections received 01.10.2016*