S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 12, стр. 704–713 (2015) УДК 519.725
DOI 10.17377/semi.2015.12.056 MSC 11T71

ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ БИОРТОГОНАЛЬНЫХ НАБОРОВ ФИЛЬТРОВ

Д.В. ЧЕРНИКОВ

Abstract. The paper presents the error-correcting coding scheme using biorthogonal filter banks and the method of construction of such mappings using the Euclidean algorithm of calculating the GCD in the ring of polynomials over a finite field.

Keywords: error-correcting coding, biorthogonal transforms, biorthogonal filter banks, perfect reconstruction filter banks, wavelet transform over a finite field.

1. Введение

Непрерывные и дискретные вейвлет-преобразования над комплексным и вещественным полями в настоящее время хорошо изучены и широко применяются для анализа сигналов различной природы во многих областях науки, таких как теория цифровой обработки сигналов и изображений, распознавание речи, оптика, геофизика, исследования климата, медицина и других.

Изложение теории вейвлет-преобразований над конечными полями представлено в [1], однако случай, когда характеристика поля равна 2, в данной статье считается исключительным и не рассматривается. Дальнейшее развитие теория вейвлет-преобразований над конечными полями получила в статье [2], где рассмотрен случай характеристики поля равной 2. В отличии от [1] авторы не строят классическую цепочку вложенных подпространств и ограничиваются лишь одним уровнем разложения.

Первые прикладные результаты построенной теории представлены в статьях [3, 4], где предложен подход к реализации кодов, корректирующих ошибки, с

Chernikov, D.V., Error-correcting codes using biorthogonal filter banks.

Поступила 21 декабря 2014 г., опубликована 14 октября 2015 г.

использованием ортогональных вейвлет-преобразований над конечным полем. Практическое применение этого метода затруднено необходимостью построения вейвлет-функции с заданными свойствами. Задача была решена с использованием методов факторизации унитарных и параунитарных матриц над конечным полем в работах [7], [8], [9] и [10].

Современная теория цифровой обработки сигналов над комплексным и вещественным полями разработала большее число эффективных алгоритмов построения наборов фильтров, обладающих нужными свойствами. Примером может являться кратномасштабное разбиение пространства $L^2(\mathbb{R})$ с помощью биортогонального набора фильтров точного восстановления [5].

В данной работе представлена схема помехоустойчивого кодирования над конечным полем с использованием биортогональных наборов фильтров точного восстановления и предложен метод построения таких фильтров, на основе лифтинговой схемы [6].

Применение биортогональных наборов фильтров и построение фильтров над полями характеристики не равной 2 обсуждалось автором в [11]. Некоторые вопросы построения биортогональных наборов фильтров над полями характеристики равной 2 были представлены в [12].

2. Биортогональные преобразования над конечными полями и их связь с наборами фильтров точного восстановления

Пусть $n \in \mathbb{N}$ – четное, $GF(q)$, $q = p^r$, p – простое. Допустим, что найдется пара разбиений пространства векторов $V_0 = GF(q)^n$ в прямую сумму подпространств

$$\begin{gathered} V_0 = V_1 \oplus W_1 = \widetilde{V}_1 \oplus \widetilde{W}_1, \\ \dim V_1 = \dim W_1 = \dim \widetilde{V}_1 = \dim \widetilde{W}_1 = n/2. \end{gathered} \tag{1}$$

В подпространствах V_1 и $\widetilde{V}_1$ и их дополнениях W_1 и $\widetilde{W}_1$ выберем базисы и составим матрицы из компонент базисных векторов в качестве строк

$$H,\ G,\ \widetilde{H} \text{ и } \widetilde{G}\,.$$

Обозначим I - единичную и O - нулевую матрицы над полем $GF(q)$.

Будем говорить, что разбиения пространства V_0 удовлетворяет условиям биортогональности, если

$$\begin{gathered} \widetilde{H}H^T = I_{n/2\times n/2}\,,\ \widetilde{G}G^T = I_{n/2\times n/2}\,, \\ \widetilde{H}G^T = O_{n/2\times n/2}\,,\ \widetilde{G}H^T = O_{n/2\times n/2}\,, \end{gathered} \tag{2}$$

и удовлетворяют условиям точного восстановления, если

$$H^T\widetilde{H} + G^T\widetilde{G} = I_{n\times n}. \tag{3}$$

Теорема 1. *Для двух разбиений пространства V_0 вида* (1)*, заданных двумя парами матриц H, G, $\widetilde{H}$ и $\widetilde{G}$, условие биортогональности* (2) *выполняется тогда, и только тогда, когда выполняется условие точного восстановления* (3)*.*

Доказательство. Перепишем условие точного восстановления (3) в виде блочного произведения матриц

$$\begin{bmatrix} H^T & G^T \end{bmatrix} \begin{bmatrix} \widetilde{H} \\ \widetilde{G} \end{bmatrix} = I_{n\times n}. \tag{4}$$

Тогда матрица

$$\begin{bmatrix} H^T & G^T \end{bmatrix}_{n\times n}$$

является обратимой в кольце квадратных матриц и имеет полный ранг.

Домножим справа обе части равенства (4) на матрицу $\begin{bmatrix} H^T & G^T \end{bmatrix}$ и перенесем все по одну сторону от знака равенства, получим

$$\begin{bmatrix} H^T & G^T \end{bmatrix} \left(\begin{bmatrix} \widetilde{H}H^T & \widetilde{H}G^T \\ \widetilde{G}H^T & \widetilde{G}G^T \end{bmatrix} - I_{n\times n} \right) = O_{n\times n}.$$

Отсюда следуют соотношения (2).

Обратно, запишем (2) в виде

$$\begin{bmatrix} \widetilde{H}H^T & \widetilde{H}G^T \\ \widetilde{G}H^T & \widetilde{G}G^T \end{bmatrix} = I_{n\times n}.$$

и представим матрицу как произведение блочных матриц

$$\begin{bmatrix} \widetilde{H} \\ \widetilde{G} \end{bmatrix} \begin{bmatrix} H^T & G^T \end{bmatrix} = I_{n\times n}.$$

Первый множитель – матрица размеров $n \times n$, она обратима в кольце квадратных матриц. Домножим полученное выражение на эту матрицу справа и перенесем все по одну сторону от знака равенства. В результате, приходим к соотношению

$$\begin{bmatrix} \widetilde{H} \\ \widetilde{G} \end{bmatrix} \left(\begin{bmatrix} H^T & G^T \end{bmatrix} \begin{bmatrix} \widetilde{H} \\ \widetilde{G} \end{bmatrix} - I_{n\times n} \right) = O_{n\times n}.$$

Выполнив в скобках блочное умножение, получим условие точного восстановления (3). □

Далее ограничимся рассмотрением случая, когда матрицы H, G, $\widetilde{H}$, $\widetilde{G}$ размеров $n/2 \times n$ являются 2-циркулянтными. 2-циркулянтная матрица задается первой строкой и каждая последующая строка является сдвигом предыдущей на 2 позиции вправо. Для задания 2-циркулянтных матриц в дальнейшем будем использовать следующее обозначение

$$H = cir_2(h_0, h_1, \ldots, h_{n-1}) = \begin{bmatrix} h_0 & h_1 & \ldots & h_{n-1} \\ h_{n-2} & h_{n-1} & \ldots & h_{n-3} \\ \ldots & \ldots & \ldots & \ldots \\ h_2 & h_3 & \ldots & h_1 \end{bmatrix},$$

где cir - обозначает циркулянтность, то есть что строки матрицы получены циклическим сдвигом первой строки вправо, индекс 2 - обозначает количество позиций, на сколько производится сдвиг каждой строки относительно предыдущей, а последовательность $(h_0, h_1, \ldots, h_{n-1})$ представляет первую строку матрицы. Для обозначения 1-циркулянтных (циркулянтных) матриц индекс будем отбрасывать.

Аналогично, обозначим

$$G = cir_2(g_0, g_1, \ldots, g_{n-1}),$$
$$\widetilde{H} = cir_2(\widetilde{h}_0, \widetilde{h}_1, \ldots, \widetilde{h}_{n-1}),$$
$$\widetilde{G} = cir_2(\widetilde{g}_0, \widetilde{g}_1, \ldots, \widetilde{g}_{n-1}).$$

В случае 2-циркулянтных матриц биортогональное разбиение пространства V_0 строится с использованием набора фильтров точного восстановления: пары фильтров анализа $(\widetilde{h}, \widetilde{g})$ и пары фильтров синтеза (h, g).

3. Помехоустойчивое кодирование с использованием биортогональных наборов фильтров

Для помехоустойчивого кодирования с использованием наборов фильтров точного восстановления некоторые свойства вейвлет-преобразований в частотной области, такие как локализация по частоте (свойство нулевого среднего) и сохранение энергии сигнала при разложении, не являются необходимыми, в то же время накладывают существенные ограничения на используемые фильтры. Обязательным является лишь условие точного восстановления, поэтому далее, в отличии от [3, 4], будем вести речь о более широком классе преобразований – классе биортогональных преобразований, включающем в себя вейвлеты. В отличие от [1], в схеме помехоустойчивого кодирования используется только один уровень разложения пространства в прямую сумму подпространств, поэтому размерность векторов не обязательно должна быть степенью двойки, а может быть любым четным числом, тем самым не исключается случай, когда характеристика поля равна 2.

Схема помехоустойчивого кодирования с использованием биортогональных наборов фильтров описывается следующим образом (Рис. 1).

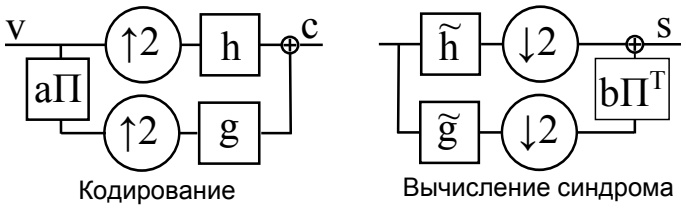

Рис. 1. Схема помехоустойчивого кодирования.

Информационное слово $\vec{v}$ представляет собой последовательность длины $n/2$ элементов поля $GF(q)$, $q = p^r$, p – простое, n – четно. Полученное кодовое слово $\vec{c}$ есть последовательность длины n над полем $GF(q)$. Множество всех таких кодовых слов является линейным кодом над полем $GF(q)$ с порождающей матрицей

$$H^T + aG^T\Pi \tag{5}$$

и проверочной матрицей

$$\widetilde{H} + b\Pi^T\widetilde{G}, \tag{6}$$

где $a, b \in GF(q), ab = (p-1) \bmod p$ и $\Pi = cir(0, 0, \ldots, 0, 1)$ – циркулянтная матрица размеров $n/2 \times n/2$, имеюшая вид

$$\Pi = \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix},$$

при этом $\Pi^{-1} = \Pi^T$.

Использование биортогональных фильтров обеспечивает необходимые свойства для синдромного декодирования. Действительно

$$\begin{aligned}\left(\widetilde{H}+b\Pi^T\widetilde{G}\right)\left(H^T+aG^T\Pi\right)&=\\&=\widetilde{H}H^T+ab\Pi^T\widetilde{G}G^T\Pi+a\widetilde{H}G^T\Pi+b\Pi^T\widetilde{G}H^T=\\&=I+(p-1)I=O.\end{aligned}$$

Кроме того, информационное слово легко восстанавливается из кодового слова с помощью одного из фильтров анализа $(\widetilde{h},\widetilde{g})$, например

$$\widetilde{H}\vec{c}=\widetilde{H}\left(H^T+aG^T\right)\vec{v}=\left(\widetilde{H}H^T+a\widetilde{H}G^T\right)\vec{v}=\vec{v}$$

Следует заметить, что полученный код является 2-циклическим, то есть каждая циклическая перестановка кодового слова на 2 позиции также является кодовым словом, что в случае синдромного декодирования позволяет значительно сократить требования к памяти для хранения таблицы лидеров смежных классов.

4. Построение биортогональных наборов фильтров

Для построения подходящих фильтров точного восстановления используем метод лифтинга, изложенный в [6].

В случае конечных полей нечетной характеристики все соотношения и выводы сохраняются с переносом арифметики из кольца многочленов Лорана в усеченное кольцо многочленов над конечным полем $GF(q)[x]/(x^n-1)$.

Условие точного восстановления для полиномиального представления фильтров записывается в виде

$$\begin{aligned}h(x)\widetilde{h}(x^{n-1})+g(x)\widetilde{g}(x^{n-1})&=2,\\h(x)\widetilde{h}(-x^{n-1})+g(x)\widetilde{g}(-x^{n-1})&=0.\end{aligned}\tag{7}$$

Это условие не определено в полях характеристики 2. Для снятия ограничений на характеристику поля обратимся к рассмотрению полифазных компонент $h_e(x)$ и $h_o(x)$, таких что

$$h(x)=h_e(x^2)+xh_o(x^2),\tag{8}$$

где h_e содержит только четные компоненты, h_o – только нечетные компоненты. С фильтрами g, $\tilde{h}$ и $\tilde{g}$ поступим подобным же образом.

Степени многочленов $h_e(x)$ и $h_o(x)$ не превосходят $n/2-1$. Далее все полифазные компоненты рассматриваются как элементы кольца $GF(q)[x]/(x^{n/2}-1)$.

Для полифазных матриц

$$P(x)=\begin{bmatrix}h_e(x) & g_e(x)\\ h_o(x) & g_o(x)\end{bmatrix},\ \widetilde{P}(x)=\begin{bmatrix}\widetilde{h}_e(x) & \widetilde{g}_e(x)\\ \widetilde{h}_o(x) & \widetilde{g}_o(x)\end{bmatrix}\tag{9}$$

условие (7) перепишется в виде

$$P(x)\widetilde{P}(x^{n/2-1})^T=I,\quad I\text{- единичная матрица.}\tag{10}$$

Следующее утверждение связывает условие точного восстановления для матричного и полифазного представлений биортогонального набора фильтров.

Теорема 2. *Для двухканальной схемы анализа-синтеза условие точного восстановления* (3) *выполняется тогда и только тогда, когда полифазные матрицы P и $\widetilde{P}$ пар фильтров (h, g) и $(\widetilde{h}, \widetilde{g})$ в кольце $GF(q)[x]/(x^{n/2}-1)$ связаны соотношением* (10).

Доказательство. Перепишем условие (10) в виде произведения полифазных компонент

$$h_e(x)\widetilde{h}_e(x^{n/2-1}) + g_e(x)\widetilde{g}_e(x^{n/2-1}) = 1, \tag{11a}$$

$$h_o(x)\widetilde{h}_e(x^{n/2-1}) + g_e(x)\widetilde{g}_e(x^{n/2-1}) = 0, \tag{11b}$$

$$h_e(x)\widetilde{h}_o(x^{n/2-1}) + g_e(x)\widetilde{g}_o(x^{n/2-1}) = 0, \tag{11c}$$

$$h_o(x)\widetilde{h}_o(x^{n/2-1}) + g_o(x)\widetilde{g}_o(x^{n/2-1}) = 1. \tag{11d}$$

Выполнив умножение в (11a), получим

$$\sum_{i=0,j=0}^{n/2-1} h_{2i}\widetilde{h}_{2j}x^{j-i} + \sum_{i=0,j=0}^{n/2-1} g_{2i}\widetilde{g}_{2j}x^{j-i} = 1.$$

Выделим свободный член в левой части

$$\sum_i (h_{2i}\widetilde{h}_{2i} + g_{2i}\widetilde{g}_{2i}) + \sum_{i\neq j}(h_{2i}\widetilde{h}_{2j} + g_{2i}\widetilde{g}_{2j})x^{j-i} = 1.$$

Отсюда следует, что

$$h_{2i}\widetilde{h}_{2j} + g_{2i}\widetilde{g}_{2j} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases} \quad i, j \in \overline{0, n/2-1}. \tag{12}$$

Обратимся к матричному представлению фильтров. Подействуем на равенство (3) справа матрицей $U = \begin{bmatrix} U_e \\ U_o \end{bmatrix}$ и слева матрицей $U^T = \begin{bmatrix} U_e^T & U_o^T \end{bmatrix}$, где $U_e = cir_2(1,0,0,\ldots,0)$, $U_o = cir_2(0,1,0,\ldots,0)$ – циркулянтные, размеров $n/2 \times n$. Домножение дает перестановку столбцов и строк в левой части равенства (3) таким образом, что это соотношение примет вид

$$\begin{bmatrix} H_e^T \\ H_o^T \end{bmatrix} \begin{bmatrix} \widetilde{H}_e & \widetilde{H}_o \end{bmatrix} + \begin{bmatrix} G_e^T \\ G_o^T \end{bmatrix} \begin{bmatrix} \widetilde{G}_e & \widetilde{G}_o \end{bmatrix} = I_{n\times n},$$

где $H_e, H_o, G_e, G_o, \widetilde{H}_e, \widetilde{H}_o, \widetilde{G}_e, \widetilde{G}_o$ – циркулянтные матрицы размеров $n/2 \times n/2$ с только четными, или только нечетными столбцами исходных матриц H, G, $\widetilde{H}$ и $\widetilde{G}$ соответственно.

Выполним блочное умножение матриц

$$\begin{bmatrix} H_e^T\widetilde{H}_e + G_e^T\widetilde{G}_e & H_e^T\widetilde{H}_o + G_e^T\widetilde{G}_o \\ H_o^T\widetilde{H}_e + G_o^T\widetilde{G}_e & H_o^T\widetilde{H}_o + G_o^T\widetilde{G}_o \end{bmatrix} = I_{n\times n}.$$

Иначе

$$H_e^T\widetilde{H}_e + G_e^T\widetilde{G}_e = I_{n/2\times n/2}, \tag{13a}$$

$$H_e^T\widetilde{H}_o + G_e^T\widetilde{G}_o = O_{n/2\times n/2}, \tag{13b}$$

$$H_o^T\widetilde{H}_e + G_o^T\widetilde{G}_e = O_{n/2\times n/2}, \tag{13c}$$

$$H_o^T\widetilde{H}_o + G_o^T\widetilde{G}_o = I_{n/2\times n/2}. \tag{13d}$$

Перемножив и сложив матрицы в (13а), получим соотношение

$$||h_{2i}\widetilde{h}_{2j} + g_{2i}\widetilde{g}_{2j}||_{n/2\times n/2} = I,$$

эквивалентное (12).

Аналогично проверяется эквивалентность оставшихся соответствующих выражений из (11) и (13). □

Таким образом, метод построения наборов фильтров точного восстановления с использованием алгоритма Евклида нахождения НОД из [6] применим и над конечными полями, не исключая поля характеристики 2.

Задача построения биортогональных наборов фильтров сводится к построению пары фильтров (h, g), определитель полифазной матрицы для которых равен 1. Такая пара фильтров в теории кратномасштабного анализа называется комплементарной.

Комплементарные фильтры можно получить с помощью разложения по алгоритму Евклида нахождения НОД [6]

$$\begin{bmatrix} h_e(x) \\ h_o(x) \end{bmatrix} = \prod_{i=1}^{m} \begin{bmatrix} q_i(x) & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} K \\ 0 \end{bmatrix}, \tag{14}$$

$$P(x) = \begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} = \prod_{i=1}^{m} \begin{bmatrix} q_i(x) & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} K & 0 \\ 0 & (-1)^m 1/K \end{bmatrix}. \tag{15}$$

Аналогично [6], в случае конечного поля можно утверждать, что если (h, g) - пара комплементарных фильтров и произведение $h_e(x)h_o(x) \neq 0 \left(mod(x^{n/2} - 1)\right)$, тогда для любого другого фильтра g_s, комплементарного h, существует $s(x) \in GF(q)[x]/(x^{n/2} - 1)$, такой что

$$g_s(x) = g(x) + h(x)s(x^2). \tag{16}$$

Соответствующая полифазная матрица $P_s(x)$ имеет вид

$$P_s(x) = P(x) \begin{bmatrix} 1 & s(x) \\ 0 & 1 \end{bmatrix}. \tag{17}$$

Двойственная пара фильтров $(\widetilde{h}, \widetilde{g})$, согласно (10), определяется соотношениями

$$\widetilde{h}(x) = -xg(-x^{n-1}), \quad \widetilde{g}(x) = xh(-x^{n-1}). \tag{18}$$

Для построения набора фильтров точного восстановления необходимо выполнить следующие действия:

(1) Выберем произвольный фильтр h.
(2) Выделим полифазные компоненты h_e и h_o.
(3) Выполним алгоритм Евклида нахождения НОД в усеченном кольце многочленов для $h_e(x)$ и $h_o(x)$, получим разложение (14).
(4) С помощью (15) найдем полифазные компоненты g_e и g_o комплементарного фильтра g.
(5) Восстановим комплементарный фильтр g с помощью (8).
(6) Двойственные фильтры $(\widetilde{h}, \widetilde{g})$ вычисляем по формулам (18).
(7) С использованием (16) можем получить любой другой фильтр g_s, комплементарный h.

Для задания помехоустоячивого кода с использованием построенного набора фильтров точного восстановления необходимо дополнительно выбрать константы $a, b \in GF(q), ab = (p-1) \bmod p$, тогда полученный код имеет порождающую матрицу вида (5) и проверочную матрицу вида (6).

Сложность построения кода длины n соответствует сложности алгоритма Евклида нахождения НОД многочленов степени не более n над конечным полем и составляет порядка $O(n^2)$ элементарных операций.

Примеры построения биортогональных кодов

Рассмотрим конечное поле $GF(7)$, в качестве примитивного элемента выберем $\alpha = 3$. Следуя описанному в предыдущей главе алгоритму, построим пример биортогонального кода с длиной фильтров равной $n = 6$:

1. Выберем фильтр $h(x) = 4x^4 + 5x^2 + 2x + 3$.
2. Его полифазные компоненты $h_e(x) = 4x^2 + 5x + 3$ и $h_o = 2$
3. Алгоритм Евклида нахождения НОД для полифазных компонент дает разложение

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

4. Получены полифазные компоненты $g_e(x) = 3$ и $g_o(x) = 0$.
5. Комплементарный фильтр записывается в виде $g(x) = 3$.
6. Двойственные фильтры $\widetilde{h}(x) = 4x$ и $\widetilde{g}(x) = 5x^5 + 4x^3 + 3x + 5$.

Если в схеме кодирования положить $a = 1$, то построенный набор фильтров точного восстановления задает биортогональный 2-циклический (6, 3)-код с порождающей матрицей

$$\begin{bmatrix} 3 & 2 & 1 & 0 & 4 & 0 \\ 4 & 0 & 3 & 2 & 1 & 0 \\ 1 & 0 & 4 & 0 & 3 & 2 \end{bmatrix}.$$

Такой код имеет кодовое расстояние $d = 3$.

Экспериментально установлено, что, применив лифтинг с помощью многочлена $s(x) = 1$, получим (6,3)-код с порождающей матрицей

$$\begin{bmatrix} 0 & 2 & 4 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 & 4 & 2 \\ 4 & 2 & 2 & 0 & 0 & 2 \end{bmatrix}$$

и с максимально возможным для заданной скорости и длины кода расстоянием $d = 4$.

В работе [3] рассмотрен пример самодвойственного (24, 12, 8)-кода над $GF(2)$, эквивалентного расширенному коду Голея и задаваемого парой фильтров

$$h(x) = x^{22} + x^{20} + x^5 + x + 1,$$
$$g(x) = x^{23} + x^{21} + x^{19} + x^{17} + x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x.$$

Для такого кода выполняется условие точного восстановления (3), но он не может быть построен с использованием алгоритма Евклида нахождения НОД, так как определитель соответствующей полифазной матрицы не равен 1. Построим аналогичный пример по описанному выше алгоритму.

1. Выберем фильтр h

$$h(x) = x^{22} + x^{20} + x^5 + x + 1.$$

2. Выделим полифазные компоненты

$$h_e(x) = x^{11} + x^{10} + 1, \;\; h_o(x) = x^2 + 1.$$

3. Осуществим разложение по алгоритму Евклида:

$$\begin{bmatrix} h_e(x) & g_e(x) \\ h_o(x) & g_o(x) \end{bmatrix} = \begin{bmatrix} x^9 + x^8 + x^7 + \ldots + x + 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} =$$
$$= \begin{bmatrix} x^{11} + x^{10} + 1 & x^{10} + x^9 + x^8 + \ldots + x + 1 \\ x^2 + 1 & x \end{bmatrix}.$$

4. Полифазные компоненты у комплементарного фильтра следующие:

$$g_e(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \;\; g_o(x) = x.$$

5. Комплементарный фильтр имеет вид:

$$g(x) = x^{20} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^4 + x^3 + x^2 + 1.$$

6. Двойственные фильтры

$$\widetilde{h}(x) = x^{23} + x^{22} + x^{21} + x^{19} + x^{17} + x^{15} + x^{13} + x^{11} + x^9 + x^7 + x^5 + x,$$
$$\widetilde{g}(x) = x^{20} + x^5 + x^3 + x + 1.$$

Приняв константу $a = 1$, получим биортогональный 2-циклический (24,12)-код с кодовым расстоянием $d_{max} = 4$. Применив лифтинг с помощью многочлена $s(x) = 1$, получим биортогональный код с фильтрами

$$h(x) = x^{22} + x^{20} + x^5 + x + 1,$$
$$g_s(x) = x^{22} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x.$$

Такой код имеет кодовое расстояние $d_{max} = 8$ и, аналогично расширенному коду Голея, исправляет 3 ошибки.

Реализация алгоритма построения помехоустойчивого кода с использованием алгоритма Евклида нахождения НОД для двухканального набора биортогональных фильтров, выполненная в среде SageMath, доступна для ознакомления по ссылке [13].

Заключение

Изложенный метод позволяет реализовать линейное 2-циркулярное помехоустойчивое кодирование со скоростью 1/2. На практике удалось достичь максимального возможного кодового расстояния для заданной скорости и длины кода. Применение биортогональных наборов фильтров дает возможность подбирать необходимые параметры фильтров, а также использовать лифтинг для получения биортогональных кодов с хорошими корректирующими свойствами.

В дальнейшем предполагается рассмотреть возможность построения биортогональных кодов с максимально возможным кодовым расстоянием.

References

[1] G. Caire, R. L. Grossman, H. V. Poor, *Wavelet Transforms Associated with Finite Cyclic Groups*, IEEE Trans. Inf. Theory, **39**:4 (1993), 1157–1166. MR1267152

[2] F. Fekri, R. M. Mersereau, R. W. Schafer, *Theory of wavelet transform over finite fields*, Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on, vol.3 (1999), pp. 1213–1216. MR1945586

[3] F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer, *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 Comput. Sci., **1719** (1999), 355–364. MR1846511

[4] F. Fekri, S. W. McLaughlin, R. M. Mersereau and R. W. Schafer, *Error Control Coding Using Finite-Field Wavelet Transforms*, Center for Signal Image Processing, Georgia Institute of Technology, Atlanta, GA, **30332** (1999), 1–13.

[5] S. Mallat, *A Wavelet Tour of Signal Processing, Second Edition*, Academic Press, 2 edition, 1999. Zbl 0998.94510

[6] I. Doubechies, W. Sweldens, *Factoring Wavelet Transforms into Lifting Steps*, The Journal of Fourier Analysis and Applications, **4**:3 (1998).

[7] P. P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice-Hall, NJ, 1993. Zbl 0784.93096

[8] A. K. Soman, P. P. Vaidyanathan and T. Q. Nquyen, *Linear-phase paraunitary filter banks: Theory, factorizations and designs*, IEEE Trans. Signal Processing, **41**:12 (1993), 3480–3496. Zbl 0873.93064

[9] S. M. Phoong, P. P. Vaidyanathan, *Paraunitary Filter Banks Over Finite Fields*, IEEE Trans. Signal Proc., **45**:6 (1997), 1443–1457. Zbl 1053.94524

[10] F. Fekri, R. M. Mersereau, R. W. Schafer, *Theory of paraunitary filter banks over fields of characteristic two*, IEEE Trans. Inform. Theory, **48**:11 (2002), pp. 2964—2979.

[11] D. Chernikov, *Error-correcting codes using biorthogonal transforms over finite field* , Contemporary Problems of Mathematics and Its Applications 2011 Conf. Proceedings., IMM Ural Branch of RAS, Yekaterinburg, (2011), 247–249.

[12] D. Chernikov. *Error-correcting codes using biorthogonal transforms over $GF(2^m)$.* // Scientific session TUSUR 2012 Conf. Proceedings., **1**, Tomsk State University of Control Systems and Radioelectronics, Tomsk, (2012), 17–20.

[13] D. Chernikov. *Biorthogonal coding algorithm implementations* [SageMath Cloud Services]. // `https://cloud.sagemath.com/projects/1ccf53b4-fab7-4a6d-9e8a-11495608d884/files/biorth-codes-construct.sagews`

Dmitry Vladimirovich Chernikov
Chelyabinsk State University,
129 Bratiev Kashirinykh st.,
454001, Chelyabinsk, Russia
E-mail address: `cherninkiy@gmail.com`