УДК 519.725

© *Д. В. Литичевский*

СПИСОЧНОЕ ДЕКОДИРОВАНИЕ ВЕЙВЛЕТ-КОДОВ

В работе обсуждается возможность списочного декодирования вейвлет-кодов и приводится утверждение, согласно которому вейвлет-коды над полем $GF(q)$ нечетной характеристики с длиной кодовых и информационных слов $n = q - 1$ и $n/2$ соответственно, а также над полем четной характеристики с длиной кодовых и информационных слов $n = q-1$ и $(n-1)/2$ соответственно допускают списочное декодирование, если среди коэффициентов спектрального представления их порождающих многочленов имеется $d+1$ последовательных нулей, $0 < d < n/2$ для полей нечетной характеристики и $0 < d < (n-3)/2$ для полей четной характеристики. Также описывается алгоритм, позволяющий выполнять списочное декодирование вейвлет-кодов при соблюдении перечисленных условий. В качестве демонстрации его работы приводятся пошаговые решения модельных задач списочного декодирования зашумленных кодовых слов вейвлет-кодов над полями четной и нечетной характеристики. Помимо этого, в работе построена вейвлет-версия квазисовершенного троичного кода Голея, длины его кодовых и информационных слов равны 8 и 4 соответственно, кодовое расстояние равно 4, минимальный радиус шаров с центрами в кодовых словах, покрывающих пространство слов длины 8, равен 3.

Ключевые слова: вейвлет-коды, полифазное кодирование, декодирование списком.

DOI: 10.20537/2226-3594-2019-53-10

Введение

Вейвлет-коды, согласно классификации, введенной Мак-Вильямсом и Слоэном в [1], являются подклассом квазициклических кодов с циклическим сдвигом кодовых слов на две позиции. Такие коды мы будем называть 2-циркулянтными.

Первоначальная методика построения вейвлет-кодов четной длины над конечными полями нечетной характеристики, основанная на использовании ортогональных вейвлет-преобразований, была описана в работах [2, 3], однако ее практическое применение было затруднено из-за необходимости построения масштабирующей функции с заданными свойствами (см. [4, 5]). В вышедших следом статьях [6, 7] по факторизации двухканального банка фильтров, основанных на схеме факторизации параунитарных матриц из [8], эта трудность была преодолена.

Результаты, изложенные в последующих трудах (см. [9,10]), позволили расширить класс вейвлет-кодов посредством использования биортогональных наборов фильтров, что упростило построение порождающих многочленов кодов и позволило находить вейвлет-коды с требуемыми свойствами.

В дальнейшем в статье [11] была предложена схема помехоустойчивого кодирования, основанная на использовании биортогональных наборов фильтров точного восстановления, и позволявшая при помощи лифтинговой схемы из работы Добеши и Свелденса [12] строить вейвлет-коды с длиной кодовых и информационных слов n и $\frac{n}{2}$ соответственно с максимально возможным и заданным кодовым расстоянием над полем $GF(q)$, где $q = p^m$, m – натуральное, $p \neq 2$ – простое число, $n = q - 1$.

Пусть

$$H = cir_2(h_0, h_1, \ldots, h_{n-1}), \quad G = cir_2(g_0, g_1, \ldots, g_{n-1})$$
$$\widetilde{H} = cir_2(\widetilde{h}_0, \widetilde{h}_1, \ldots, \widetilde{h}_{n-1}), \quad \widetilde{G} = cir_2(\widetilde{g}_0, \widetilde{g}_1, \ldots, \widetilde{g}_{n-1})$$

— 2-циркулянтные матрицы, определяющие процедуры разложения и восстановления сигнала биортогонального кратномасштабного анализа и выполняющие точное восстановление. 2-циркулянтная матрица задается первой строкой, последующая строка получается из предыдущей циклическим сдвигом на две позиции вправо. Способность выполнять точное восстановление означает, что при

любом входном сигнале последовательное применение процедур разложения и восстановления не искажает его. Элементы матриц H, G, $\widetilde{H}$, $\widetilde{G}$ являются элементами поля $GF(p^m)$.

Последовательность $\{h_k\}_{k=0}^{n-1}$ будем называть фильтром, многочлен $h(x) = \sum\limits_{k=0}^{n-1} x^k$ — весовым многочленом. Представим $h(x)$ в виде суммы полифазных компонент

$$h(x) = h_e(x^2) + xh_o(x^2),$$

где $h_e(x) = \sum\limits_{k=0}^{\frac{n}{2}-1} h_{2k}x^k$ и $h_o(x) = \sum\limits_{k=0}^{\frac{n}{2}-1} h_{2k+1}x^k$.

Аналогично поступим с весовыми многочленами $g(x)$, $\widetilde{h}(x)$, $\widetilde{g}(x)$, которые соответствуют фильтрам $\{g_k\}_{k=0}^{n-1}$, $\{\widetilde{h}_k\}_{k=0}^{n-1}$ и $\{\widetilde{g}_k\}_{k=0}^{n-1}$. Все операции умножения многочленов будут выполняться в кольце $GF_{p^m}[x]/(x^{n/2}-1)$.

Введем полифазные матрицы для пар фильтров (h, g) и $(\widetilde{h}, \widetilde{g})$

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

Пары фильтров (h, g) и $(\widetilde{h}, \widetilde{g})$ выполняют точное восстановление тогда и только тогда, когда их полифазные матрицы $P(x)$ и $\widetilde{P}(x)$ связаны соотношением

$$P(x)\,\widetilde{P}^{\intercal}(x^{\frac{n}{2}-1}) = I_{2\times 2}.$$

Многочлены $h(x)$ и $g(x)$ называются комплементарными, если полифазная матрица имеет единичный определитель. Для многочлена $h(x)$, $\deg h(x) \leqslant n-1$, комплементарный многочлен можно построить с помощью алгоритма Евклида нахождения НОД и операции лифтинга. Для многочлена $s(x) \in GF_{p^m}[x]/(x^{n/2}-1)$ определим операцию лифтинга как умножение полифазной матрицы $P(x)$ на треугольную матрицу вида

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

Из условия точного восстановления следует, что

$$P(x)^{-1} = \widetilde{P}^{\intercal}(x^{\frac{n}{2}-1})$$

и

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

Процедура кодирования, названная полифазной, определяется с помощью полифазных компонент

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

где $v(x) = \sum\limits_{j=0}^{\frac{n}{2}-1} v_j x^j$ – информационный многочлен над полем $GF(p^m)$, $a \in GF(p^m)$. Кодовый многочлен $c(x)$ имеет вид

$$c(x) = c_e(x^2) + xc_o(x^2) = (h(x) + ax^2 g(x))v(x^2) \bmod (x^n - 1).$$

Построенный вейвлет-код является 2-циркулянтным кодом. Многочлен $f(x) = h(x) + ax^2 g(x)$ будем называть порождающим многочленом вейвлет-кода, определенного над полем нечетной характеристики.

Процедура восстановления информационного слова по кодовому определяется с помощью полифазных компонент фильтра $\widetilde{h}$

$$v(x) = \begin{bmatrix} \widetilde{h}_e(x^{\frac{n}{2}-1}) & \widetilde{h}_o(x^{\frac{n}{2}-1}) \end{bmatrix} \begin{bmatrix} c_e(x) \\ c_o(x) \end{bmatrix}.$$

Предложенная схема кодирования, как было сказано выше, позволила строить при помощи процедуры лифтинга вейвлет-коды с максимально возможным и заданным кодовым расстоянием, однако она не позволяла строить коды с максимально возможным кодовым расстоянием над полем характеристики два. Поэтому в работе [13] была предложена иная схема помехоустойчивого кодирования и было доказано, что с ее помощью возможно построение над конечным полем $GF(q = 2^m)$ биортогональных вейвлет-кодов с длиной кодовых и информационных слов n и $(n-1)/2$ соответственно с максимально возможным и заданным кодовым расстоянием.

В новой схеме кодирования также используются две пары комплементарных фильтров (h, g) и $(\widetilde{h}, \widetilde{g})$, определенных над полем $GF(2^m)$, которые выполняют точное восстановление тогда и только тогда, когда их полифазные матрицы $P(x)$ и $\widetilde{P}(x)$ связаны соотношением

$$P(x^2)\,\widetilde{P}(x^{n-1}) = I_{2\times 2}.$$

Кодовый многочлен $c(x)$ вычисляется с использованием пары фильтров (h, g), его полифазные компоненты в кольце $GF_{2^m}[x]/(x^n - 1)$ определяются как

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

где $v(x) = \sum\limits_{j=0}^{\frac{n-3}{2}} v_j x^j$ — информационный многочлен над полем $GF(2^m)$. Кодовый многочлен $c(x)$ имеет вид

$$c(x) = c_e(x^2) + x c_o(x^2) = (h(x) + x^2 g(x)) v(x^2) \bmod (x^n - 1).$$

Многочлен $f(x) = h(x) + x^2 g(x) \bmod (x^n - 1)$ называется порождающим многочленом вейвлет-кода, определенного над полем характеристики два.

Процедура восстановления информационного слова по кодовому определяется с помощью полифазных компонент фильтра $\widetilde{h}$

$$v(x^2) = \begin{bmatrix} \widetilde{h}_e(x^{n-1}) & \widetilde{h}_o(x^{n-1}) \end{bmatrix} \begin{bmatrix} c_e(x^2) \\ c_o(x^2) \end{bmatrix}.$$

Найденные вейвлет-коды с максимально возможным кодовым расстоянием являются кодами Рида–Соломона, построенными во временно́й области, а коды с заданным кодовым расстоянием являются подпространствами кодов Рида–Соломона во временно́й области, поэтому к ним применим алгоритм помехоустойчивого декодирования Берлекэмпа–Уэлча, описанный в [14].

Одним из важнейших свойств кода является существование для него алгоритма, осуществляющего декодирование списком за полиномиальное время от параметров кода. Ключевое отличие списочного декодирования от классического заключается в том, что на выходе из декодера допускается получать не более некоторого заранее фиксированного числа кодовых слов. Или, более формально, код допускает декодирование списком длины L с исправлением e ошибок, если множество кодовых слов обладает свойством, что любой шар радиуса e должен содержать не более L кодовых слов (см. [15]). Тогда утверждение, что алгоритм позволяет осуществлять списочное декодирование кода с исправлением e ошибок, будет означать, что любой шар радиуса e содержит не более некоторого заранее фиксированного для кода количества кодовых слов, формирующих возвращаемый алгоритмом список.

Рассмотрим произвольный код $C[n, k, d]$, определенный над полем $GF(q)$, допускающий декодирование списком длины L с исправлением e ошибок. Через $V_n = GF(q)^n$ обозначим пространство слов длины n над полем $GF(q)$. Для кода $C[n, k, d]$ справедлив аналог неравенства Хэмминга:

$$q^k V_q(e, n) \leqslant L q^n,$$

которое означает, что шары радиуса e в количестве q^k штук покрывают q^n слов из V_n не более чем L раз. Выполнение записанного выше неравенства является необходимым условием существования кодов, допускающих декодирование списком длины L с исправлением e ошибок.

Так как вейвлет-коды с максимально возможным кодовым расстоянием являются кодами Рида–Соломона, построенными во временно́й области, а коды с заданным кодовым расстоянием являются подпространствами кодов Рида–Соломона во временно́й области, то они должны допускать декодирование списком.

Работы по изучению списочного декодирования в настоящий момент ведутся в двух направлениях: расширение класса кодов, допускающих декодирование списком (в частности, в [16] показана возможность списочного декодирования полярных кодов), и создание и оптимизация алгоритмов, позволяющих осуществлять списочное декодирование (так, в [17] представлен новый алгоритм списочного декодирования для кодов Рида–Соломона и кодов БЧХ). Возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием над полем нечетной характеристики, описанных в [11], была доказана в [18]. Возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием над полем четной характеристики, описанных в [13], была доказана в еще не опубликованной работе [L][1]. Эти результаты были представлены на конференции СоПроМат-2019 (см. [19]), в ходе которой возникло понимание необходимости представления модельных задач, демонстрирующих работу алгоритма списочного декодирования, а также поступило предложение рассмотреть троичный квазисовершенный код Голея как вейвлет-код и проверить возможность его списочного декодирования. В связи с этим в § 1 обсуждается возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием, в §§ 2 и 3 приводятся пошаговые решения модельных задач списочного декодирования зашумленных кодовых слов вейвлет-кодов над полями нечетной характеристики и характеристики два соответственно, в § 4 рассматривается возможность списочного декодирования вейвлет-версии кода Голея.

§ 1. Алгоритм списочного декодирования вейвлет-кода

Здесь обсуждается возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием, а также приводится алгоритм списочного декодирования. Символом $W[n,k,d]$ в дальнейшем будет обозначаться кодовое пространство (n,k) вейвлет-кода, определенного над полем $GF(q)$, где $q=p^m$, p — простое, m — натуральное, с примитивным элементом α, $n=q-1$,

$$k=\frac{n-1}{2} \quad \text{при} \quad p=2 \quad \text{и} \quad k=\frac{n}{2} \quad \text{при} \quad p\neq 2,$$

с кодовым расстоянием равным d.

Л е м м а 1. *Если для порождающего многочлена $f(x)$ вейвлет-кода с длиной кодовых и информационных слов n и k соответственно выполняются соотношения*

$$f(\alpha^j)=0 \quad \textit{при} \quad j=j^*,\dots,j^*+d, \quad 0<d<d^*,$$
$$d^*=\frac{n-3}{2} \quad \textit{при} \quad p=2 \quad \textit{и} \quad d^*=\frac{n}{2} \quad \textit{при} \quad p\neq 2,$$

то кодовое расстояние вейвлет-кода не меньше $d+2$.

Т е о р е м а 1 (О допустимости списочного декодирования вейвлет-кода). *Существует алгоритм, позволяющий осуществлять списочное декодирование вейвлет-кода $W[n,k,d+2]$, $0<d<d^*$, со схемой кодирования*

$$c(x)=f(x)v(x^2) \bmod (x^n-1), \tag{1}$$

для порождающего многочлена которого выполняются соотношения

$$f(\alpha^j)=0 \quad \textit{при} \quad j=j^*,\dots,j^*+d.$$

[1][L] Литичевский Д.В. О списочном декодировании вейвлет-кодов над конечными полями характеристики два // Прикладная дискретная математика (В печати).

Доказательство приведенных утверждений основывается на применении преобразования Фурье к кодовому многочлену $c(x)$ и анализе свойств спектрального многочлена $C(y) = C_0 + C_1 y + \ldots + C_{n-1} y^{n-1}$, $y \in GF(q)$, коэффициенты которого $C_j = v(\alpha^{2j}) f(\alpha^j)$, $j = 0, \ldots, n-1$, равны нулю при $j = j^*, \ldots, j^* + d$ согласно формулировкам леммы 1 и теоремы 1. Так как $c_i = n^{-1} C(\alpha^{-i})$, $i = 0, \ldots, n-1$, то описанное свойство коэффициентов спектрального многочлена позволяет показать, что рассматриваемый вейвлет-код является подпространством кода Рида–Соломона с параметрами $RS[n, n-d-1]$ с процедурой кодирования $s_i = \sum\limits_{j=0}^{n-d-2} \beta_j \alpha^{-ij}$, $i = 0, \ldots, n-1$, во временно́й области, из чего следуют оба сформулированных утверждения, полное доказательство которых приводится в [L] (с. 118)

З а м е ч а н и е 1. Основываясь на утверждении теоремы 1, алгоритм списочного декодирования вейвлет-кода $W[n, k, d+2]$ с порождающим многочленом $f(x)$ состоит из следующих шагов:

- вместо полученного зашумленного кодового слова $\widetilde{c} = \{\widetilde{c}_i\}_{i=0}^{n-1}$ вейвлет-кода $W[n, k, d+2]$ рассматривается зашумленное слово $\widetilde{s} = \{\widetilde{s}_i\}_{i=0}^{n-1}$, $s_i = \widetilde{c}_i n^* \alpha^{i(j^*+d+1)}$, где $n^* = n \bmod p$, кода Рида–Соломона $RS[n, n-d-1]$;
- к зашумленному слову $\widetilde{s}$ применяется алгоритм списочного декодирования кода Рида–Соломона $RS[n, n-d-1]$ с процедурой кодирования $s_i = \sum\limits_{j=0}^{n-d-2} \beta_j \alpha^{-ij}$, $i = 0, \ldots, n-1$; в результате, получаем список информационных слов β;
- для каждого найденного информационного слова β решаем систему уравнений

$$\begin{cases} v(\alpha^{2j}) \cdot f(\alpha^j) = \beta_{j+n-j^*-d-1}, & j = 0, \ldots, j^* - 1, \\ v(\alpha^{2j}) \cdot f(\alpha^j) = \beta_{j-j^*-d-1}, & j = j^* + d + 1, \ldots, n-1; \end{cases}$$

  из найденных векторов v формируем список информационных слов вейвлет-кода $W[n, k, d+2]$.

З а м е ч а н и е 2. Существует алгоритм, позволяющий осуществлять списочное декодирование вейвлет-кода $W[n, k, d+2]$, $0 < d < d^*$, для порождающего многочлена которого выполняются соотношения

$$f(\alpha^j) = 0 \text{ при } j = j^*, \ldots, j^* + d.$$

З а м е ч а н и е 3. При использовании в качестве алгоритма списочного декодирования кода Рида–Соломона улучшенной версии алгоритма Гурусвами–Судана, описанной в [20], алгоритм списочного декодирования вейвлет-кода $W[n, k, d+2]$ будет исправлять до $n - \sqrt{n(n-d-2)}$ ошибок и работать за полиномиальное время от параметров кода.

Алгоритм был реализован в виде программы, осуществляющей декодирование вейвлет-кода $W[n, k, d+2]$ с исправлением до $e < n - \sqrt{n(n-d-2)}$ ошибок за полиномиальное время от параметров n и d (получено авторское свидетельство № 2017619148). Для осуществления списочного декодирования кода Рида–Соломона используется улучшенная версия алгоритма Гурусвами–Судана.

§ 2. Модельная задача списочного декодирования вейвлет-кода над полем нечетной характеристики

Возьмем конечное поле $GF(9)$ с неприводимым многочленом $1 + x^2$ и порождающим элементом α. Все элементы $GF(9)$ могут быть представлены многочленами вида $a + bx$, где a и b — элементы поля $GF(3)$. Поэтому, для удобства обозначений, каждому элементу поля поставим в соответствие вещественное число, являющееся значением соответствующего ему многочлена при $x = 3$, и будем использовать полученные числа в качестве обозначений элементов.

Рассмотрим некоторый вейвлет-код, определенный над выбранным полем, с длиной кодовых и информационных слов 8 и 4 соответственно, порождающим многочленом

$$f(x) = 2 + 8x + 3x^2 + 8x^3 + 6x^5 + 2x^6 + 7x^7$$

и процедурой кодирования (1). При этом комплементарные фильтры h и g, определенные над полем $GF(9)$ и использованные при построении вейвлет-кода, равны соответственно

$$h(x) = 2 + x^2 + 7x^3 + 2x^4 + x^5,$$
$$g(x) = 5 + x + x^2 + 8x^3 + 2x^4 + 7x^5 + 8x^7.$$

Теперь, для того чтобы при помощи леммы 1 получить кодовое расстояние построенного вейвлет-кода, вычислим значения кодового многочлена $f(x)$ в точках $1, \alpha, \ldots, \alpha^7$. Получаем, что $f(\alpha^j) = 0$ при $j = 0, \ldots, 2$, следовательно, параметры j^* и d равны 0 и 2 соответственно, поэтому, согласно лемме 1, рассматриваемый вейвлет-код имеет кодовое расстояние 4 и может быть обозначен как $W[8, 4, 4]$.

Для иллюстрации работы алгоритма рассмотрим кодовое слово

$$c = (0, 0, 0, 0, 0, 0, 0, 0)$$

и соответствующее ему зашумленное кодовое слово

$$\widetilde{c} = (1, 6, 0, 0, 0, 0, 0, 0).$$

Описанный в предыдущем разделе алгоритм позволяет найти все информационные слова вейвлет-кода $W[8, 4, 4]$, соответствующие кодовые слова которых попадают в шар радиуса 2 с центром в зашумленном кодовом слове $\widetilde{c}$. На первом шаге алгоритм преобразует принятое зашумленное кодовое слово $\widetilde{c}$ вейвлет-кода $W[8, 4, 4]$ в зашумленное кодовое слово кода Рида–Соломона $RS[8, 5]$

$$\widetilde{s} = (2, 4, 0, 0, 0, 0, 0).$$

На втором шаге алгоритм применяет к зашумленному кодовому слову $\widetilde{s}$ процедуру списочного декодирования кодов Рида–Соломона и получает список информационных слов β кода Рида–Соломона $RS[8, 5]$

$$(0, 0, 0, 0, 0),$$
$$(5, 2, 2, 2, 6),$$
$$(7, 8, 5, 8, 7).$$

На третьем шаге алгоритм решает систему из пяти линейных уравнений с четырьмя неизвестными

$$\begin{aligned} v_0 + 3v_1 + 2v_2 + 6v_3 &= \beta_0, \\ 8v_0 + 8v_1 + 8v_2 + 8v_3 &= \beta_1, \\ 3v_0 + v_1 + 6v_2 + 2v_3 &= \beta_2, \\ 3v_0 + 6v_1 + 3v_2 + 6v_3 &= \beta_3, \\ 7v_0 + 4v_1 + 5v_2 + 8v_3 &= \beta_4 \end{aligned}$$

для каждого информационного слова β из списка, полученного на втором шаге, и получает список информационных слов v вейвлет кода $W[8, 4, 4]$

$$(0, 0, 0, 0),$$
$$(4, 5, 0, 8).$$

Полученным информационным словам соответствуют кодовые слова

$$(0, 0, 0, 0, 0, 0, 0, 0),$$
$$(1, 6, 0, 7, 0, 7, 0, 0)$$

вейвлет-кода $W[8, 4, 4]$ с процедурой кодирования (1) и порождающим многочленом $f(x) = 2 + 8x + {} + 3x^2 + 8x^3 + 6x^5 + 2x^6 + 7x^7$, каждое из которых попадает в шар радиуса 2 с центром в зашумленном кодовом слове $\widetilde{c} = (1, 6, 0, 0, 0, 0, 0, 0)$.

§ 3. Модельная задача списочного декодирования вейвлет-кода над полем четной характеристики

Возьмем конечное поле $GF(16)$ с неприводимым многочленом $1 + x^3 + x^4$ и порождающим элементом α. Все элементы $GF(16)$ могут быть представлены многочленами вида $a+bx+cx^2+dx^3$, где a, b, c и d — элементы поля $GF(2)$. Поэтому, для удобства обозначений, каждому элементу поля поставим в соответствие вещественное число, являющееся значением соответствующего ему многочлена при $x = 2$, и будем использовать полученные числа в качестве обозначений элементов.

Рассмотрим некоторый вейвлет-код, определенный над выбранным полем, с длиной кодовых и информационных слов 15 и 7 соответственно, порождающим многочленом

$$f(x) = 3+3x+13x^2+2x^3+4x^4+5x^5+2x^6+9x^7+11x^8+11x^9+14x^{10}+3x^{11}+9x^{12}+11x^{13}+10x^{14}$$

и процедурой кодирования (1). При этом комплементарные фильтры h и g, определенные над полем $GF(16)$ и использованные при построении вейвлет-кода, равны соответственно

$$h(x) = 3 + 2x + 7x^2 + 6x^3 + 4x^4 + 2x^5 + 11x^6 + 7x^7 + 5x^8,$$
$$g(x) = 10 + 4x + 7x^3 + 9x^4 + 14x^5 + 14x^6 + 11x^7 + 14x^8 + 3x^9 + 9x^{10} + 11x^{11} + 10x^{12} + x^{14}.$$

Теперь, для того чтобы при помощи леммы 1 получить кодовое расстояние построенного вейвлет-кода, вычислим значения кодового многочлена $f(x)$ в точках $1, \alpha, \ldots, \alpha^{14}$. Получаем, что $f(\alpha^j) = 0$ при $j = 0, \ldots, 6$, следовательно, параметры j^* и d равны 0 и 6 соответственно, поэтому, согласно лемме 1, рассматриваемый вейвлет-код имеет кодовое расстояние 4 и может быть обозначен как $W[15, 7, 8]$.

Для иллюстрации работы алгоритма рассмотрим кодовое слово

$$c = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

и соответствующее ему зашумленное кодовое слово

$$\widetilde{c} = (1, 8, 11, 10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

Описанный в предыдущем параграфе алгоритм позволяет найти все информационные слова вейвлет-кода $W[15, 7, 8]$, соответствующие кодовые слова которых попадают в шар радиуса 4 с центром в зашумленном кодовом слове $\widetilde{c}$. На первом шаге алгоритм преобразует принятое зашумленное кодовое слово $\widetilde{c}$ вейвлет-кода $W[15, 7, 8]$ в зашумленное кодовое слово кода Рида–Соломона $RS[15, 8]$

$$\widetilde{s} = (1, 10, 9, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

На втором шаге алгоритм применяет к зашумленному кодовому слову $\widetilde{s}$ процедуру списочного декодирования кодов Рида–Соломона и получает список информационных слов β кода Рида–Соломона $RS[15, 8]$

$$(0, 0, 0, 0, 0, 0, 0, 0),$$
$$(6, 7, 8, 6, 12, 9, 1, 10).$$

На третьем шаге алгоритм решает систему из восьми линейных уравнений с семью неизвестными (в связи с большой размерностью она не будет приведена в работе) для каждого информационного слова β из списка, полученного на втором шаге, и получает список информационных слов v вейвлет-кода $W[15, 7, 8]$

$$(0, 0, 0, 0, 0, 0, 0),$$
$$(13, 0, 10, 15, 10, 13, 1).$$

Полученным информационным словам соответствуют кодовые слова

$$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(1, 8, 11, 10, 0, 0, 0, 0, 3, 13, 0, 10, 0, 0, 12)$$

вейвлет-кода $W[15, 7, 8]$ с процедурой кодирования (1) и порождающим многочленом

$$f(x) = 3+3x+13x^2+2x^3+4x^4+5x^5+2x^6+9x^7+11x^8+11x^9+14x^{10}+3x^{11}+9x^{12}+11x^{13}+10x^{14},$$

каждое из которых попадает в шар радиуса 4 с центром в зашумленном кодовом слове

$$\widetilde{c} = (1, 8, 11, 10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

§ 4. Анализ списочного декодирования вейвлет-версии кода Голея

Согласно описанию, представленному в [1], код Голея G_{12} является квазисовершенным кодом, определенным над полем $GF(3)$, с длиной кодовых и информационных слов 12 и 6 соответственно и кодовым расстоянем 6. Кодовые слова G_{12} могут быть получены путем добавления общей проверки на четность к коду Голея G_{11}.

Код Голея G_{11} является совершенным кодом, также определенным над полем $GF(3)$ с длиной кодовых и информационных слов 11 и 6 соответственно и кодовым расстоянем 5. Согласно классификации, введенной Мак-Вильямсом и Слоэном в [1], G_{11} является квадратично-вычетным кодом, в качестве порождающего многочлена которого можно выбрать один из многочленов

$$\begin{aligned} &2 + x^2 + 2x^3 + x^4 + x^5, \\ &2 + 2x + x^2 + 2x^3 + x^5. \end{aligned} \tag{2}$$

Квадратично-вычетными кодами называются циклические коды кольца $GF(l)[x]/(x^p - 1)$ (идеалы), порождаемые многочленами $q(x)$, $(x-1)q(x)$, $n(x)$, $(x-1)n(x)$, где p — простое число, l — простое число, являющееся квадратичным вычетом по модулю p, α — примитивный корень степени p из единицы в некотором поле, содержащем поле $GF(l)$,

$$q(x) = \prod_{r \in Q} (x - \alpha^r),$$
$$n(x) = \prod_{n \in N} (x - \alpha^n),$$

Q — множество квадратичных вычетов по модулю p, N — множество квадратичных невычетов. Квадратичными вычетами по модулю p называются ненулевые квадраты чисел, приведенные по модулю p. Существует $(p-1)/2$ квадратичных вычетов по модулю p, оставшиеся $(p-1)/2$ чисел от 1 до $p-1$ называются квадратичными невычетами по модулю p. Нуль не является ни вычетом, ни невычетом.

Согласно результатам работы [21], любой многочлен $f(x)$ степени не выше $n-1$ над полем $GF(p^m)$, p — простое и $p \neq 2$, m — натуральное, $n = p^m - 1$, может быть представлен в виде

$$f(x) = h(x) + ax^2 g(x) \bmod (x^n - 1),$$

где $(h(x), g(x))$ — пара комплементарных многочленов над полем $GF(p^m)$, степени которых не превосходят $n-1$, $a \in GF(p^m)$, $a \neq 0$. Данное представление многочлена $f(x)$ называется комплементарным, оно не является единственным. Это означает, что многочлен $f(x)$ является порождающим многочленом вейвлет-кода с длиной кодовых и информационных слов n и $n/2$ соответственно и процедурой кодирования (1). Таким образом, для построения вейвлет-версии кода G_{12} необходимо рассмотреть порождающий многочлен $f(x)$ кода G_{11} как многочлен, определенный над полем $GF(3^m)$, где m — минимальное натуральное число, такое что степень $f(x)$ не превосходит $3^m - 2$, и получить одно из его возможных комплементарных представлений над этим полем. В качестве m возьмем значение 2 и при помощи алгоритма из [21] для каждого из возможных порождающих многочленов (2) кода Голея G_{11}, найдем комплементарное представление над полем $GF(9)$ с неприводимым многочленом $1 + x^2$ и порождающим элементом α.

Алгоритм поиска комплементарного представления, описанный в [21], сводится к решению нескольких систем линейных уравнений, которые, в силу большой размерности, не будут приведены в работе. Для порождающего многочлена

$$f(x) = 2 + x^2 + 2x^3 + x^4 + x^5$$

было найдено следующее комплементарное представление:

$$a = 1,$$
$$h(x) = 2 + x^2 + 2x^4 + 2x^5,$$
$$g(x) = 2x + 2x^2 + 2x^3.$$

Для порождающего многочлена

$$f(x) = 2 + 2x + x^2 + 2x^3 + x^5$$

было найдено следующее комплементарное представление

$$a = 1,$$
$$h(x) = 2 + 2x + 2x^3,$$
$$g(x) = 1 + x^3.$$

Таким образом, все шаги, необходимые для построения вейвлет-версии кода Голея G_{12}, были выполнены и ему будут соответствовать вейвлет-коды с длиной кодовых и информационных слов 8 и 4 соответственно.

Теперь для каждого из порождающих многочленов (2) вычислим значения в точках $1, \alpha, \ldots, \alpha^7$ для проверки условий допустимости списочного декодирования, зафиксированных в теореме 1. Однако, все вычисленные значения для каждого из порождающих многочленов отличны от нуля, поэтому описанный в замечании 1 алгоритм списочного декодирования к построенным вейвлет-кодам не применим и вычислить их кодовое расстояние при помощи леммы 1 также не представляется возможным. Чтобы все же получить некоторое представление о свойствах построенных кодов, вычислим для них кодовое расстояние, а также минимальный радиус шаров с центрами в кодовых словах, покрывающих пространство слов V_8, определенное над полем $GF(9)$.

В силу того, что построенные вейвлет-коды являются линейными кодами, их кодовое расстояние будет равно минимальному весу их кодовых слов. Перебрав все кодовые слова, получаем, что для каждого из возможных порождающих многочленов (2) минимальный вес кодового слова равен 4, поэтому кодовое пространство построенных вейвлет-кодов может быть обозначено как $W[8, 4, 4]$. Минимальный радиус шаров с центрами в кодовых словах, покрывающих пространство слов V_8, равен максимуму среди расстояний Хэмминга от каждого слова $x \in V_8$ до ближайшего кодового слова. Перебрав все слова $x \in V_8$, получаем, что минимальный радиус покрывающих шаров для построенных кодов равен 3. Для сравнения, у кодов Голея G_{11} и G_{12} минимальный радиус покрывающих шаров равен 2 и 3 соответственно, а у кода $W[8, 4, 4]$, приведенного в § 2, минимальный радиус покрывающих шаров равен 4. Таким образом, вейвлет-версии кода Голея G_{12} ближе к совершенным кодам, чем рассмотренный в § 2 вейвлет-код с такими же параметрами.

Заключение

В работе обсуждалась возможность декодирования списком вейвлет-кодов и было приведено утверждение, согласно которому вейвлет-код $W[n, k, d + 2]$ над полем $GF(q)$ с порождающим элементом α, $n = q - 1$, допускает списочное декодирование, если для его порождающего многочлена $f(x)$ выполняются соотношения

$$f(\alpha^j) = 0 \quad \text{при} \quad j = j^*, \ldots, j^* + d,\ 0 < d < d^*,$$

где $k = (n - 1)/2$, $d^* = (n - 3)/2$ при $n \bmod 2 \neq 0$ и $k = n/2$, $d^* = n/2$ при $n \bmod 2 = 0$. Был рассмотрен и описан алгоритм, позволяющий осуществлять списочное декодирование вейвлет-кодов.

В качестве демонстрации возможностей алгоритма, реализованного в виде программы, использующей улучшенную версию алгоритма Гурусвами–Судана из [20] (получено авторское свидетельство № 2017619148), приведено пошаговое решение модельных задач списочного декодирования зашумленных кодовых слов кодов $W[8, 4, 4]$ и $W[15, 7, 8]$.

Помимо этого, для вейвлет-версии кода Голея G_{12} было вычислено кодовое расстояние и минимальный радиус шаров с центрами в кодовых словах, покрывающих пространство слов V_8, определенное над полем $GF(9)$, они равны 4 и 3 соответственно.

Список литературы

1. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
2. Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Double circulant self-dual codes using finite-field wavelet transforms // Proceedings of 13th International Symposium «Applied Algebra, Algebraic Algorithms and Error-Correcting Codes» (AAECC-13). Honolulu, Hawaii, USA, 1999. P. 355–363. https://doi.org/10.1007/3-540-46796-3_35
3. Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Decoding of half-rate wavelet codes; Golay code and more // Proceedings of 2001 IEEE International Conference on Acoustics, Speech and Signal Processing. Salt Lake City, UT, USA, 2001. Vol. 4. P. 2609–2612. https://doi.org/10.1109/ICASSP.2001.940536
4. Добеши И. Десять лекций по вейвлетам. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
5. Mallat S. A wavelet tour of signal processing. 2nd edition. Academic Press, 1999.
6. 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. P. 2964–2979. https://doi.org/10.1109/TIT.2002.804049
7. Fekri F., Delgosha F. Finite-field wavelet transforms with applications in cryptography and coding. Upper Saddle River: Prentice Hall, 2012.
8. Phoong S.M., Vaidyanathan P.P. Paraunitary filter banks over finite fields // IEEE Transactions on Signal Processing. 1997. Vol. 45. No. 6. P. 1443–1457. https://doi.org/10.1109/78.599956
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. P. 1157–1166. https://doi.org/10.1109/18.243435
10. Fekri F., Mersereau R.M., Schafer R.W. Theory of wavelet transform over finite fields // Proceedings of 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. ICASSP99 (Cat. No.99CH36258). Phoenix, AZ, USA, 1999. Vol. 3. P. 1213–1216. https://doi.org/10.1109/ICASSP.1999.756196
11. Соловьев А.А., Черников Д.В. Биортогональные вейвлет-коды с заданным кодовым расстоянием // Дискретная математика. 2017. Т. 29. № 2. С. 96–108. https://doi.org/10.4213/dm1432
12. Doubechies I., Sweldens W. Factoring wavelet transforms into lifting steps // Journal of Fourier Analysis and Applications. 1998. Vol. 4. No. 3. P. 247–269. https://doi.org/10.1007/BF02476026
13. Соловьев А.А., Черников Д.В. Биортогональный вейвлет-код в полях характеристики два // Челябинский физико-математический журнал. 2017. Т. 2. № 1. С. 66–79. http://mi.mathnet.ru/chfmj46
14. Berlekamp E.R., Welch L.R. Error correction of algebraic block codes. US Patent Number US4633470A, 30.12.1986. https://patentview.ip-tools.io/api/pdf/US4633470A
15. Ромащенко А.Е., Румянцев А.Ю., Шень А. Заметки по теории кодирования. М.: МЦНМО, 2011.
16. Tal I., Vardy A. List decoding of polar codes // IEEE Transactions on Information Theory. 2015. Vol. 61. No. 5. P. 2213–2226. https://doi.org/10.1109/TIT.2015.2410251
17. Wu Y. New list decoding algorithms for Reed–Solomon and BCH codes // Proceedings of 2007 IEEE International Symposium on Information Theory. Nice, France, 2007. P. 2806–2810. https://doi.org/10.1109/ISIT.2007.4557643
18. Литичевский Д.В. Списочное декодирование биортогональных вейвлет-кодов с заданным кодовым расстоянием в поле нечетной характеристики // Прикладная дискретная математика. 2018. № 39. С. 72–77. https://doi.org/10.17223/20710410/39/6
19. Литичевский Д.В. Списочное декодирование вейвлет-кодов // Современные проблемы математики и её приложений: тез. докл. Междунар. (50-й Всероссийской) молодёжной школы-конференции. Институт математики и механики им. Н. Н. Красовского УрО РАН, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. Екатеринбург, 2019. С. 18–19. http://sopromat.imm.uran.ru/kungurka/proceedings-1103.pdf

20. Guruswami V., Sudan M. Improved decoding of Reed–Solomon and algebraic-geometric codes // IEEE Transactions on Information Theory. 1999. Vol. 45. No. 6. P. 1757–1767. https://doi.org/10.1109/18.782097
21. Соловьев А.А. Комплементарное представление многочленов над конечными полями // Челябинский физико-математический журнал. 2017. Т. 2. № 2. С. 199–209. http://mi.mathnet.ru/chfmj56

Поступила в редакцию 07.04.2019

Литичевский Дмитрий Владимирович, аспирант, кафедра компьютерной безопасности и прикладной алгебры, Челябинский государственный университет, 454001, Россия, г. Челябинск, ул. Братьев Кашириных, 129.
E-mail: litichevskiydv@gmail.com

D. V. Litichevskii
List decoding of wavelet codes

Citation: *Izvestiya Instituta Matematiki i Informatiki Udmurtskogo Gosudarstvennogo Univiversiteta*, 2019, vol. 53, pp. 115–126 (in Russian).

Keywords: wavelet codes, polyphase coding, list decoding.

MSC2010: 12Y05, 94B05, 94B60, 94B35

DOI: 10.20537/2226-3594-2019-53-10

This paper discusses the possibility of list decoding of wavelet codes and states that wavelet codes over the field $GF(q)$ of an odd characteristic with the length of the code and information words $n = q - 1$ and $\frac{n}{2}$, respectively, as well as over the field of an even characteristic with the length of the code and information words $n = q - 1$ and $\frac{n-1}{2}$, respectively, allow list decoding if among the coefficients of the spectral representation of the polynomials generating them there are $d + 1$ consecutive zeros, $0 < d < \frac{n}{2}$ for fields of the odd characteristic and $0 < d < \frac{n-3}{2}$ for fields of the even characteristic. Also, a description is given of an algorithm that allows one to perform list decoding of wavelet codes subject to the listed conditions. As a demonstration of the operation of this algorithm, step-by-step solutions for model problems of list decoding of noisy wavelet code words over fields of even and odd characteristics are given. In addition, a wavelet version of Golay's quasi-perfect ternary code is constructed. The lengths of its code and information words are 8 and 4, respectively, the code distance is 4, the minimum radius of balls with centers in code words covering the space of words of length 8 is 3.

REFERENCES

1. MacWilliams F.J., Sloane N.J.A. *The theory of error-correcting codes*, North Holland, 1977.
2. Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Double circulant self-dual codes using finite-field wavelet transforms, *Proceedings of 13th International Symposium "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes" (AAECC-13)*, Honolulu, Hawaii, USA, 1999, pp. 355–363. https://doi.org/10.1007/3-540-46796-3_35
3. Fekri F., McLaughlin S.W., Mersereau R.M., Schafer R.W. Decoding of half-rate wavelet codes; Golay code and more, *Proceedings of 2001 IEEE International Conference on Acoustics, Speech and Signal Processing*, Salt Lake City, UT, USA, 2001, vol. 4, pp. 2609–2612. https://doi.org/10.1109/ICASSP.2001.940536
4. Daubechies I. *Ten lectures on wavelets*, Philadelphia: Society for Industrial and Applied Mathematics, 1992. https://doi.org/10.1137/1.9781611970104
5. Mallat S. *A wavelet tour of signal processing*, 2nd edition, Academic Press, 1999.
6. 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. https://doi.org/10.1109/TIT.2002.804049
7. Fekri F., Delgosha F. *Finite-field wavelet transforms with applications in cryptography and coding*, Upper Saddle River: Prentice Hall, 2012.

8. 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. https://doi.org/10.1109/78.599956
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. https://doi.org/10.1109/18.243435
10. Fekri F., Mersereau R.M., Schafer R.W. Theory of wavelet transform over finite fields, *Proceedings of 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing. ICASSP99 (Cat. No.99CH36258)*, Phoenix, AZ, USA, 1999, vol. 3, pp. 1213–1216. https://doi.org/10.1109/ICASSP.1999.756196
11. Soloviev A.A., Chernikov D.V. Biorthogonal wavelet codes with prescribed code distance, *Discrete Mathematics and Applications*, 2018, vol. 28, issue 3, pp. 179–188. https://doi.org/10.1515/dma-2018-0017
12. Doubechies I., Sweldens W. Factoring wavelet transforms into lifting steps, *Journal of Fourier Analysis and Applications*, 1998, vol. 4, no. 3, pp. 247–269. https://doi.org/10.1007/BF02476026
13. Soloviev A.A., Chernikov D.V. Biorthogonal wavelet code in fields of characteristic two, *Chelyab. Fiz.-Mat. Zh.*, 2017, vol. 2, issue 1, pp. 66–79 (in Russian). http://mi.mathnet.ru/eng/chfmj46
14. Berlekamp E.R., Welch L.R. Error correction of algebraic block codes, *US Patent Number US4633470A*, 30.12.1986. https://patentview.ip-tools.io/api/pdf/US4633470A
15. Romashchenko A.E., Rumyantsev A.Yu., Shen' A. *Zametki po teorii kodirovaniya* (Notes on the theory of coding), Moscow: Moscow Center for Continuous Mathematical Education, 2011.
16. Tal I., Vardy A. List decoding of polar codes, *IEEE Transactions on Information Theory*, 2015, vol. 61, no. 5, pp. 2213–2226. https://doi.org/10.1109/TIT.2015.2410251
17. Wu Y. New list decoding algorithms for Reed–Solomon and BCH codes, *Proceedings of 2007 IEEE International Symposium on Information Theory*, Nice, France, 2007, pp. 2806–2810. https://doi.org/10.1109/ISIT.2007.4557643
18. Litichevskiy D.V. List decoding of the biorthogonal wavelet code with predetermined code distance on a field with odd characteristic, *Prikladnaya Diskretnaya Matematika*, 2018, no. 39, pp. 72–77. https://doi.org/10.17223/20710410/39/6
19. Litichevskiy D.V., List decoding of wavelet codes, *Modern problems in mathematics and its applications: Abstracts of International (50-th National) Youth School-Conference*, Institute of Mathematics and Mechanics, Ural Branch of the Russian Academy of Sciences, Ural Federal University named after the First President of Russia B. N. Yeltsin, Yekaterinburg, 2019, pp. 18–19 (in Russian). http://sopromat.imm.uran.ru/kungurka/proceedings-1103.pdf
20. Guruswami V., Sudan M. Improved decoding of Reed–Solomon and algebraic-geometric codes, *IEEE Transactions on Information Theory*, 1999, vol. 45, no. 6, pp. 1757–1767. https://doi.org/10.1109/18.782097
21. Soloviev A.A. Complementary representation of polynomials over finite fields, *Chelyab. Fiz.-Mat. Zh.*, 2017, vol. 2, issue 2, pp. 199–209 (in Russian). http://mi.mathnet.ru/eng/chfmj56

Received 07.04.2019

Litichevskii Dmitrii Vladimirovich, Postgraduate Student, Department of Computer Security and Applied Algebra, Chelyabinsk State University, ul. Brat'ev Kashirinykh, 129, Chelyabinsk, 454001, Russia.
E-mail: litichevskiydv@gmail.com