УДК 519.725

О СПИСОЧНОМ ДЕКОДИРОВАНИИ ВЕЙВЛЕТ-КОДОВ НАД КОНЕЧНЫМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ ДВА

Д. В. Литичевский

Челябинский государственный университет, г. Челябинск, Россия

Доказывается, что вейвлет-код над полем $\mathrm{GF}(2^m)$ с длиной кодовых и информационных слов $n = 2^m - 1$ и $(n-1)/2$ соответственно, у которого среди коэффициентов спектрального представления порождающего многочлена имеется $d+1$ последовательных нулей, $0 < d < (n-3)/2$, допускает списочное декодирование за полиномиальное время. Шаги алгоритма, осуществляющего списочное декодирование с исправлением до $e < n - \sqrt{n(n-d-2)}$ ошибок, реализованы в виде программы. Приведены примеры её применения для списочного декодирования зашумленных кодовых слов. Отмечено, что неравенство Варшамова — Гилберта при достаточно больших n не позволяет судить о существовании вейвлет-кодов с максимальным кодовым расстоянием $(n-1)/2$.

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

DOI 10.17223/20710410/44/7

ON LIST DECODING OF WAVELET CODES OVER FINITE FIELDS OF CHARACTERISTIC TWO

D. V. Litichevskiy

Chelyabinsk State University, Chelyabinsk, Russia

E-mail: litichevskiydv@gmail.com

In this paper, we consider wavelet code defined over the field $\mathrm{GF}(2^m)$ with the code length $n = 2^m - 1$ and information words length $(n-1)/2$ and prove that a wavelet code allows list decoding in polynomial time if there are $d+1$ consecutive zeros among the coefficients of the spectral representation of its generating polynomial and $0 < d < (n-3)/2$. The steps of the algorithm that performs list decoding with correction up to $e < n - \sqrt{n(n-d-2)}$ errors are implemented as a program. Examples of its use for list decoding of noisy code words are given. It is also noted that the Varshamov — Hilbert inequality for sufficiently large n does not allow to judge about the existence of wavelet codes with a maximum code distance $(n-1)/2$.

Keywords: *wavelet codes, polyphase coding, list decoding.*

Введение

Вейвлет-коды, согласно [1], являются подклассом квазициклических кодов с циклическим сдвигом кодовых слов на две позиции. Первоначально их порождающие матрицы строились с помощью ортогональных фильтров масштабирующей функции и вейвлет-функции. Описание этих подходов доступно в [2, 3]. Однако практическое применение описанных методик было затруднено необходимостью построения масштабирующих функций с заданными свойствами [4, 5]. На основании результатов [6] о факторизации параунитарных матриц в работах [7, 8], а также в 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 [11] предложена схема помехоустойчивого кодирования, основанная на использовании биортогональных наборов фильтров точного восстановления. Использование лифтинговой схемы из [12] расширило возможности построения вейвлет-кодов с заданными характеристиками, в частности позволило построить биортогональные вейвлет-коды с максимально возможным и заданным кодовым расстоянием над конечными полями нечётной характеристики.

Однако предложенная в [11] схема кодирования не позволяет строить коды с максимально возможным кодовым расстоянием над полем характеристики два. Поэтому в работе [13] предложена иная схема помехоустойчивого кодирования, названная полифазной, и доказано, что с помощью этой схемы возможно построение над конечным полем $\mathrm{GF}(2^m)$ биортогональных вейвлет-кодов с длиной кодовых и информационных слов n и $(n-1)/2$ соответственно с максимально возможным и заданным кодовым расстоянием, где m — натуральное число, $n = 2^m - 1$.

В полифазной схеме кодирования для вычисления кодового многочлена $c(x)$ используется пара комплементарных фильтров (h, g), где $h(x) = \sum\limits_{j=0}^{n-1} h_j x^j$ и $g(x) = \sum\limits_{j=0}^{n-1} g_j x^j$. Пара фильтров (h, g) называется комплементарной, если определитель их полифазной матрицы $P(x)$

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

равен 1, где $h_e(x)$, $h_o(x)$ и $g_e(x)$, $g_o(x)$ — полифазные компоненты фильтров $h(x)$ и $g(x)$ соответственно.

Определение 1 [13]. Полифазные компоненты кодового многочлена $c(x)$ в кольце $\mathrm{GF}_{2^m}[x]/(x^n - 1)$ 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 $v(x) = \sum\limits_{j=0}^{(n-3)/2} v_j x^j$ — информационный многочлен.

Тогда кодовый многочлен $c(x)$ имеет вид

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

все операции умножения многочленов выполняются в кольце $\mathrm{GF}_{2^m}[x]/(x^n - 1)$.

Определение 2. Многочлен $f(x) = h(x) + x^2 g(x) \bmod (x^n - 1)$ называется порождающим многочленом вейвлет-кода.

Процедура построения порождающих многочленов $f(x)$ для вейвлет-кодов с максимально возможным и заданным кодовым расстоянием при помощи процедуры лифтинга (см. [12]) описана в работе [13].

Существование вейвлет-кодов с максимально возможным и заданным кодовым расстоянием над конечными полями характеристики два согласуется с результатом Э. Берлекэмпа [14], согласно которому над конечным полем $\mathrm{GF}(q)$ существуют линейные коды с произвольно большой длиной кодового слова n, скоростью R и кодовым расстоянием d, которые удовлетворяют соотношению

$$\frac{d}{n} \geqslant \delta(R),$$

где $\delta(R)$ — наименьшее решение уравнения

$$R = 1 - H_q(\delta(R));$$

$H_q(p) = p\log_q(q-1) - p\log_q p - (1-p)\log_q(1-p)$ — q-значная энтропия Шеннона. При этом неравенство Варшамова — Гильберта, которое, согласно [15], записывается в виде

$$V_q(2e, n) \leqslant q^{n(1-R)},$$

где $V_q(2e, n)$ — объём (число элементов) шара радиуса $2e$ в пространстве слов длины n, состоящих из символов алфавита мощности q, напротив, не позволяет судить о существовании найденных в [13] вейвлет-кодов, поскольку оно является только достаточным условием существования кода.

В [13] также доказано, что найденные вейвлет-коды с максимально возможным кодовым расстоянием являются кодами Рида — Соломона, построенными во временной области, а коды с заданным кодовым расстоянием являются подпространствами кодов Рида — Соломона во временной области, поэтому к ним применим алгоритм помехоустойчивого декодирования Берлекэмпа — Уэлча, описанный в [16].

Одним из важнейших свойств кода является существование для него алгоритма, осуществляющего декодирование списком за полиномиальное время от параметров кода. В классической задаче декодирования требуется, чтобы исправление ошибки в принятом кодовом слове осуществлялось однозначно. В задаче декодирования списком допускается на выходе декодера иметь до L вариантов декодирования при некотором фиксированном L. Код допускает декодирование списком длины L с исправлением e ошибок, если множество кодовых слов обладает следующим свойством: любой шар радиуса e в кодовом пространстве содержит не более L кодовых слов. Тогда утверждение о том, что алгоритм позволяет осуществлять списочное декодирование кода с исправлением e ошибок, означает, что любой шар радиуса e в кодовом пространстве содержит не больше некоторого заранее фиксированного для кода количества кодовых слов, формирующих возвращаемый алгоритмом список. В [17] показано существование кодов, допускающих декодирование списком длины $n+1$ с исправлением до $e < \sqrt{n(n-d)}$ ошибок, вблизи границы Хэмминга

$$q^k V_q(e, n) \leqslant q^n, \tag{2}$$

где q — мощность алфавита, над которым построен код; n и k — длины кодовых и информационных слов соответственно; $V_q(e, n)$ — объём шара радиуса e в пространстве слов длины n, состоящих из символов алфавита мощности q. К сожалению, сложность описания таких кодов, а также экспоненциальная зависимость процедур их кодирования и декодирования от длины кодового слова n значительно ограничивают область их применения.

Однако для кода Рида — Соломона $\mathrm{RS}[n, k, d = n - k + 1]$ разработаны алгоритмы списочного декодирования, сложность которых полиномиально зависит от длины кодового слова. В кодах Рида — Соломона $\mathrm{RS}[n, k]$ со спектральной схемой кодирования информационному слову $v_0, v_1, \ldots, v_{k-1}$ ставится в соответствие кодовое слово $y_0, y_1, \ldots, y_{n-1}$, где $y_i = v(x_i) = \sum\limits_{\ell=0}^{k-1} v_\ell x_i^\ell$. Здесь $x_0, x_1, \ldots, x_{n-1}$, $x_i \neq x_j$ при $i \neq j$, — произвольные зафиксированные для конкретного кода элементы поля $\mathrm{GF}(q)$, над которым определён код.

Первоначальная версия алгоритма списочного декодирования для кода Рида — Соломона, описанная в [18], позволяла исправлять до $e < n - \sqrt{2n(k-1)}$ ошибок. Это означает, что в любом шаре радиуса $\leqslant e$ содержится не более L кодовых слов, при этом L полиномиально зависит от параметров кода. На вход алгоритма подаётся принятое искажённое кодовое слово $\widetilde{y}_0, \widetilde{y}_1, \ldots, \widetilde{y}_{n-1}$, на выходе получается список кодовых слов, содержащихся в шаре радиуса e с центром в принятом искажённом кодовом слове. Построение списка кодовых слов состоит из двух этапов: интерполяционного и факторизационного. На интерполяционном этапе алгоритма выполняется поиск отличного от нуля многочлена от двух переменных $R(x, y) \in \mathrm{GF}(q)[x, y]$, такого, что $R(x, y)$ обращается в нуль во всех точках $(x_j, \widetilde{y}_j)$, $j = 0, \ldots, n-1$, и его $(1, k-1)$-взвешенная степень не превосходит фиксированного значения, являющегося функцией от параметров кода n и k. (w_x, w_y)-Взвешенная степень монома $r_{j_1 j_2} x^{j_1} y^{j_2}$ равна $j_1 w_x + j_2 w_y$; (w_x, w_y)-взвешенная степень многочлена $R(x, y) = \sum\limits_{j_1, j_2} r_{j_1 j_2} x^{j_1} y^{j_2}$ равна максимальной среди всех (w_x, w_y)-взвешенных степеней его мономов с ненулевыми коэффициентами $r_{j_1 j_2}$. На факторизационном шаге осуществляется поиск всех многочленов $v(x) \in \mathrm{GF}(q)[x]$ степени не выше $k - 1$, таких, что $y - v(x)$ делит $R(x, y)$ и $v(x_i) = \widetilde{y}_i$ не менее чем в $n - e$ точках. Найденные многочлены формируют искомый список кодовых слов.

Позднее в [19] представлена улучшенная версия алгоритма, позволяющая исправлять уже до $e < n - \sqrt{n(k-1)} = n - \sqrt{n(n-d)}$ ошибок, что является улучшением упомянутого результата из [17], поскольку при таком же радиусе шаров количество попадающих в них кодовых слов получается меньшим и их список восстанавливается за полиномиальное время. При этом общая структура алгоритма не претерпела изменений, он по-прежнему состоит из интерполяционного и факторизационного шагов. Однако на многочлен $R(x, y)$ при построении на интерполяционном шаге накладываются дополнительные требования, а именно: должны существовать натуральные r и l, связанные соотношениями

$$l > \sqrt{nr(k-1)(r+1)}, \quad l \leqslant r(n-e),$$

такие, что каждая из точек (x_i, y_i), $i = 0, \ldots, n-1$, должна быть нулём кратности r многочлена $R(x, y)$, а его $(1, k-1)$-взвешенная степень не должна превосходить l. Многочлен $R(x, y)$ имеет в точке (a, b) нуль кратности r, если многочлен $R(u+a, v+b)$ не имеет мономов, $(1, 1)$-взвешенная степень которых меньше r.

Возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием над полем нечётной характеристики, описанных в [11], была изучена в [20]. Данная работа является её продолжением, в ней рассматривается возможность списочного декодирования вейвлет-кодов с заданным кодовым расстоянием над полем характеристики два, описанных в [13].

В работе доказывается, что если для порождающего многочлена $f(x)$ некоторого вейвлет-кода, определённого над полем $\mathrm{GF}(2^m)$ ($m \in \mathbb{N}$) с примитивным элементом α, с длиной кодовых и информационных слов $n = 2^m - 1$ и $(n-1)/2$ соответственно имеют место равенства

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

где $0 \leqslant j^* \leqslant n - 1 - d$ и $0 < d < (n-3)/2$, то вейвлет-код с кодовым расстоянием $d + 2$ допускает списочное декодирование.

Помимо этого, в работе приводится одна из возможных реализаций алгоритма списочного декодирования для допускающих его вейвлет-кодов, определённых над полем характеристики два, работающая за полиномиальное время, а также даются примеры её использования.

Устанавливается факт, что неравенство Варшамова — Гильберта не позволяет судить о существовании вейвлет-кодов с заданным кодовым расстоянием над полем характеристики два.

1. Допустимость списочного декодирования вейвлет-кода

Выберем в поле $\mathrm{GF}(2^m)$ примитивный элемент α. Рассмотрим вейвлет-код с длиной кодовых слов $n = 2^m - 1$, длиной информационных слов $(n-1)/2$, порождающим многочленом $f(x)$ и процедурой кодирования (1). Символом $W[n, (n-1)/2, d]$ будем обозначать кодовое пространство $(n, (n-1)/2)$-вейвлет-кода с кодовым расстоянием d.

Лемма 1. Если для порождающего многочлена $f(x)$ вейвлет-кода с длиной кодовых и информационных слов n и $(n-1)/2$ соответственно выполняются соотношения

$$f(\alpha^j) = 0 \ \text{ при } \ j = j^*, \ldots, j^* + d, \quad 0 < d < (n-3)/2,$$

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

Доказательство. Выберем d так, чтобы выполнялось $0 < d < (n-3)/2$. Будем считать, что для многочлена $f(x)$ степени не больше $n - 1$ имеют место равенства

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

где $0 \leqslant j^* \leqslant n - 1 - d$. Согласно [21], многочлен $f(x)$ является порождающим многочленом вейвлет-кода, то есть найдётся комлементарная пара фильтров $h(x)$ и $g(x)$, такая, что $f(x) = h(x) + ax^2 g(x) \bmod (x^n - 1)$, где $a \in \mathrm{GF}(2^m)$, $a \neq 0$. Преобразование Фурье кодового многочлена $c(x)$, равное

$$c(\alpha^i) = v(\alpha^{2i}) f(\alpha^i),\ i = 0, \ldots, n-1,$$

запишется в виде

$$\bigl(C_0, \ldots, C_{j^*-1}, \underbrace{0, \ldots, 0}_{d+1}, C_{j^*+d+1}, \ldots, C_{n-1}\bigr).$$

Спектральный многочлен $C(y) = C_0 + C_1 y + \ldots + C_{n-1} y^{n-1}$, $y \in \mathrm{GF}(2^m)$, представим в виде

$$\begin{gathered} C(y) = C_0 + \cdots + C_{j^*-1} y^{j^*-1} + C_{j^*+d+1} y^{j^*+d+1} + \cdots + C_{n-1} y^{n-1} = \\ = C_{j^*+d+1} y^{j^*+d+1} + \cdots + C_{n-1} y^{n-1} + C_0 y^n + \cdots + C_{j^*-1} y^{n+j^*-1} = \\ = y^{j^*+d+1} (C_{j^*+d+1} + \cdots + C_{n-1} y^{n-j^*-d-2} + C_0 y^{n-j^*-d-1} + \cdots + C_{j^*-1} y^{n-d-2}). \end{gathered}$$

Так как коэффициент $c_i = C(\alpha^{-i})$ равен нулю тогда и только тогда, когда α^{-i} является корнем многочлена $C(y)$, а число его отличных от нуля корней не превосходит $n-d-2$, вес кодового слова построенного вейвлет-кода не может быть меньше $n-(n-d-2)$, следовательно, кодовое расстояние будет не меньше $d+2$. ■

Теорема 1 (о допустимости списочного декодирования вейвлет-кода).

Существует алгоритм, позволяющий осуществлять списочное декодирование вейвлет-кода $W[n,(n-1)/2,d+2]$, $0 < d < (n-3)/2$, со схемой кодирования (1), для порождающего многочлена которого выполняются соотношения

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

Доказательство. Опираясь на полученное в лемме 1 представление спектрального многочлена $C(y)$, c_i запишем в виде

$$c_i = \alpha^{-i(j^*+d+1)} \left(\sum_{j=0}^{n-j^*-d-2} C_{j+j^*+d+1}\alpha^{-ij} + \sum_{j=n-j^*-d-1}^{n-d-2} C_{j+j^*+d-n+1}\alpha^{-ij} \right),$$

где $i = 0, \ldots, n-1$, иначе

$$c_i\alpha^{i(j^*+d+1)} = \sum_{j=0}^{n-j^*-d-2} C_{j+j^*+d+1}\alpha^{-ij} + \sum_{j=n-j^*-d-1}^{n-d-2} C_{j+j^*+d-n+1}\alpha^{-ij}. \tag{3}$$

Полученное в (3) представление задаёт код Рида — Соломона $RS(n, n-d-1)$, в котором кодовое слово $s = \{s_i\}_{i=0}^{n-1}$ получается из некоторого информационного слова $\beta = \{\beta_j\}_{j=0}^{n-d-2}$ по формулам

$$s_i = \sum_{j=0}^{n-d-2} \beta_j\alpha^{-ij}, \quad i = 0, \ldots, n-1, \tag{4}$$

поскольку α^{-1} также является примитивным элементом поля $\mathrm{GF}(2^m)$.

Список возможных спектральных многочленов $C(y)$ может быть получен при помощи любого алгоритма списочного декодирования кода Рида — Соломона $RS(n, n-d-1)$ с процедурой кодирования (4). Однако в этот список могут попасть последовательности, не порождённые кодовыми словами вейвлет-кода.

Согласно процедуре кодирования (1) вейвлет-кода $W[n,(n-1)/2,d+2]$, значения C_j, $j = 0, \ldots, n-1$, могут быть найдены как

$$v(\alpha^{2j})f(\alpha^j) = C_j,\ j = 0, \ldots, n-1.$$

Данные равенства задают систему линейных уравнений относительно коэффициентов информационного многочлена $v(x)$, решая которую, можно либо найти коэффициенты $v(x)$, либо показать, что не существует кодового многочлена $c(x)$, соответствующего значениям C_j, $j = 0, \ldots, n-1$. По свойствам порождающего многочлена $f(x)$, $(d+1)$ уравнений системы являются вырожденными. С учётом результатов о декодировании кода Рида — Соломона полученную систему линейных уравнений можно записать в виде

$$\begin{cases} v(\alpha^{2j})f(\alpha^j) = \beta_{j+n-j^*-d-1},\ j = 0, \ldots, j^*-1, \\ v(\alpha^{2j})f(\alpha^j) = \beta_{j-j^*-d-1},\ j = j^*+d+1, \ldots, n-1. \end{cases} \tag{5}$$

Система уравнений, заданная (5), содержит $(n-1)/2$ неизвестных и $n-d-1 > (n-1)/2$ уравнений. Это означает, что рассматриваемый вейвлет-код $W[n,(n-1)/2, d+2]$ является подпространством кода Рида — Соломона $\mathrm{RS}[n, n-d-1]$. Поэтому для него длина списка и число исправляемых ошибок не превосходят таковых для кода $\mathrm{RS}[n, n-d-1]$. ■

Замечание 1. На основании теоремы 1 алгоритм списочного декодирования вейвлет-кода $W[n,(n-1)/2, d+2]$ с порождающим многочленом $f(x)$ состоит из следующих шагов:

1) вместо полученного зашумлённого кодового слова $\widetilde{c} = \{\widetilde{c}_i\}_{i=0}^{n-1}$ вейвлет-кода $W[n,(n-1)/2, d+2]$ рассматривается зашумлённое слово $\widetilde{s} = \{\widetilde{s}_i\}_{i=0}^{n-1}$, $s_i = \widetilde{c}_i\alpha^{i(j^*+d+1)}$, кода Рида — Соломона $\mathrm{RS}[n, n-d-1]$;
2) к зашумлённому слову $\widetilde{s}$ применяется алгоритм списочного декодирования кода Рида — Соломона $\mathrm{RS}[n, n-d-1]$ с процедурой кодирования (4), в результате получаем список информационных слов β;
3) для каждого найденного информационного слова β решаем систему уравнений (5). Из найденных векторов v формируем список информационных слов вейвлет-кода $W[n,(n-1)/2, d+2]$.

Замечание 2. Существует алгоритм, позволяющий осуществлять списочное декодирование вейвлет-кода $W[n,(n-1)/2, d+2]$, $0 < d < (n-3)/2$, для порождающего многочлена которого выполняются соотношения

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

Замечание 3. При использовании в качестве алгоритма списочного декодирования кода Рида — Соломона улучшенной версии алгоритма Гурусвами — Судана, описанной в [19], алгоритм списочного декодирования вейвлет-кода $W[n,(n-1)/2, d+2]$ будет исправлять до $n - \sqrt{n(n-d-2)}$ ошибок и работать за полиномиальное время от параметров кода.

Замечание 4. Предельный случай $d = (n-3)/2$ в теореме не рассматривается, так как, согласно результатам работы [13], он соответствует вейвлет-коду $W[n,(n-1)/2,(n+3)/2]$ с максимально возможным кодовым расстоянием, то есть является кодом Рида — Соломона, построенным во временной области. Поэтому списочное декодирование в этом случае может быть осуществлено при помощи алгоритмов списочного декодирования кодов Рида — Соломона $\mathrm{RS}[n,(n-1)/2]$.

Замечание 5. О применимости неравенства Варшамова — Гилберта в вопросе существования вейвлет-кода с максимальным кодовым расстоянием.

Рассмотрим вейвлет-код $W[n,(n-1)/2, d+2]$, $0 < d < (n-3)/2$, определённый над полем $\mathrm{GF}(2^m)$, $n = 2^m - 1$. При $n = 2^m - 1$ и $k = (n-1)/2$ неравенство Варшамова — Гилберта (см. [15]) имеет вид

$$\sum_{j=0}^{d} n^j C_{n-1}^j < (n+1)^{(n+1)/2}. \tag{6}$$

Учитывая поведение C_{n-1}^j при больших n и то, что $d < (n-3)/2$, получаем, что самым большим слагаемым в сумме является $n^d C_{n-1}^d$. Оценим снизу значение суммы

$\sum\limits_{j=0}^{d} n^j C_{n-1}^j$ при максимально допустимом $d = (n-5)/2$:

$$\sum_{j=0}^{d} n^j C_{n-1}^j > n^d C_{n-1}^d = n^{(n-5)/2} C_{n-1}^{(n-5)/2}.$$

Применив к полученному выражению формулу Стирлинга, находим

$$n^{(n-5)/2} C_{n-1}^{(n-5)/2} \sim n^{(n-5)/2} \frac{\sqrt{n-1}}{\sqrt{2\pi \left(\frac{n-5}{2}\right)\left(\frac{n+3}{2}\right)}} \frac{(n-1)^{n-1}}{\left(\frac{n-5}{2}\right)^{(n-5)/2}\left(\frac{n+3}{2}\right)^{(n+3)/2}} =$$

$$= \frac{n^{(n-5)/2}\sqrt{n-1}}{\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \frac{2^{n-1}(n-1)^{n-1}}{(n-5)^{(n-5)/2}(n+3)^{(n+3)/2}}.$$

Правую часть представим в виде

$$\frac{n^{(n-5)/2}\sqrt{n-1}}{\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \frac{2^{n-1}(n-1)^{n-1}}{(n-5)^{(n-5)/2}(n+3)^{(n+3)/2}} =$$

$$= \frac{2^{n-1} n^{(n-5)/2}\sqrt{n-1}}{\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \left(\frac{n-1}{n-5}\right)^{(n-5)/2} \left(\frac{n-1}{n+3}\right)^{(n+3)/2} =$$

$$= \frac{2^{n-1} n^{(n-5)/2}\sqrt{n-1}}{\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \left(1 + \frac{4}{n-5}\right)^{((n-5)/4)\cdot 2} \left(1 - \frac{4}{n+3}\right)^{(-(n+3)/4)(-2)}.$$

Поделив полученное выражение на правую часть неравенства (6), приходим к соотношению

$$\frac{2^{n-1}\sqrt{n-1}}{\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \frac{n^{(n-5)/2}}{(n+1)^{(n+1)/2}} \left(1 + \frac{4}{n-5}\right)^{((n-5)/4)\cdot 2} \left(1 - \frac{4}{n+3}\right)^{(-(n+3)/4)(-2)} =$$

$$= \frac{2^{n-1}\sqrt{n-1}}{n^3\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \left(\frac{n}{n+1}\right)^{(n+1)/2} \left(1 + \frac{4}{n-5}\right)^{((n-5)/4)\cdot 2} \left(1 - \frac{4}{n+3}\right)^{(-(n+3)/4)(-2)} =$$

$$= \frac{2^{n-1}\sqrt{n-1}}{n^3\sqrt{\frac{\pi}{2}(n-5)(n+3)}} \left(1 - \frac{1}{n+1}\right)^{-(n+1)(-1/2)} \times$$

$$\times \left(1 + \frac{4}{n-5}\right)^{((n-5)/4)\cdot 2} \left(1 - \frac{4}{n+3}\right)^{(-(n+3)/4)(-2)}.$$

Полученное выражение при достаточно больших n больше 1 и стремится к бесконечности при $n \to +\infty$. Поэтому, начиная с некоторого n, код $W[n, (n-1)/2, d+2 = (n-1)/2]$ не удовлетворяет неравенству Варшамова — Гилберта.

Таким образом, неравенство Варшамова — Гилберта не позволяет судить о существовании найденных в [13] вейвлет-кодов.

2. Примеры

Чтобы проиллюстрировать работу алгоритма, описанного в замечании 1, приведём примеры его использования для списочного декодирования зашумлённых кодовых слов нескольких вейвлет-кодов.

Пример 1. Рассмотрим некоторый вейвлет-код, определённый над полем GF(8) с неприводимым многочленом $1+x+x^3$ и порождающим элементом α, с длиной кодовых и информационных слов 7 и 3 соответственно, порождающим многочленом

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

и процедурой кодирования (1). При этом комплементарные фильтры h и g, использованные при построении вейвлет-кода, равны соответственно

$$h(x) = 3 + 2x + 7x^2 + 6x^3 + 4x^4 + 2x^5,$$
$$g(x) = 5 + 3x + 2x^2 + 2x^3 + x^4 + 3x^5 + 2x^6.$$

Для того чтобы при помощи леммы 1 получить кодовое расстояние построенного вейвлет-кода, вычислим значения кодового многочлена $f(x)$ в точках $1, \alpha, \ldots, \alpha^6$. 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 $W[7,3,4]$.

Для иллюстрации работы алгоритма рассмотрим кодовое слово

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

и соответствующее ему зашумлённое кодовое слово

$$\widetilde{c} = (1,7,0,0,0,0,0).$$

Описанный в п. 1 алгоритм позволяет найти все информационные слова вейвлет-кода $W[7,3,4]$, соответствующие кодовые слова которых попадают в шар радиуса 2 с центром в зашумлённом кодовом слове $\widetilde{c}$. На первом шаге алгоритм преобразует принятое зашумлённое кодовое слово $\widetilde{c}$ вейвлет-кода $W[7,3,4]$ в зашумлённое кодовое слово кода Рида — Соломона RS[7, 4]

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

На втором шаге алгоритм применяет к зашумлённому кодовому слову $\widetilde{s}$ процедуру списочного декодирования кодов Рида — Соломона и получает список информационных слов β кода Рида — Соломона RS[7, 4]

$$(0,0,0,0),\ (1,1,0,1),\ (5,7,0,3).$$

На третьем шаге алгоритм решает систему из трёх линейных уравнений с тремя неизвестными

$$\begin{cases} v_0 + 5v_1 + 7v_2 = \beta_0, \\ 4v_0 + 3v_1 + 6v_2 = \beta_1, \\ 5v_0 + 6v_1 + 4v_2 = \beta_3 \end{cases}$$

для каждого информационного слова β из списка, полученного на втором шаге, и получает список информационных слов v вейвлет кода $W[7,3,4]$

$$(0,0,0),\ (4,0,2),\ (0,0,2).$$

Полученным информационным словам соответствуют кодовые слова

$$(0,0,0,0,0,0,0),\ (1,7,3,0,5,0,0),\ (1,7,0,2,0,0,4)$$

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

Пример 2. Рассмотрим некоторый вейвлет-код, определённый над полем $\mathrm{GF}(32)$ с неприводимым многочленом $1+x^3+x^5$ и порождающим элементом α, с длиной кодовых и информационных слов 31 и 15 соответственно, порождающим многочленом

$$\begin{aligned} f(x) = 7 &+ 24x + 2x^2 + 5x^4 + 29x^5 + 2x^6 + 18x^7 + 3x^8 + x^9 + 15x^{10} + 22x^{11} + x^{12} + \\ &+ 16x^{13} + 29x^{14} + 17x^{15} + 6x^{16} + 16x^{17} + 17x^{18} + 25x^{19} + 21x^{20} + 26x^{21} + \\ &+ 10x^{22} + 30x^{23} + 18x^{24} + 6x^{25} + 24x^{26} + 4x^{27} + 31x^{28} + 14x^{29} + 15x^{30} \end{aligned}$$

и процедурой кодирования (1). При этом комплементарные фильтры h и g, использованные при построении вейвлет-кода, равны соответственно

$$\begin{aligned} h(x) &= 23 + 13x + 27x^2 + x^3 + 15x^4 + 13x^5 + x^6 + 16x^7 + x^8 + 21x^9 + 28x^{10} + 30x^{11} + \\ &\quad + 12x^{12} + 19x^{13} + 17x^{14} + 4x^{15} + x^{16} + 19x^{17} + 14x^{18} + 3x^{20} + 5x^{21} + 6x^{22}, \\ g(x) &= 25 + x + 10x^2 + 16x^3 + 3x^4 + 2x^5 + 2x^6 + 20x^7 + 19x^8 + 8x^9 + 13x^{10} + 3x^{11} + \\ &\quad + 12x^{12} + 21x^{13} + 7x^{14} + 3x^{15} + 31x^{16} + 25x^{17} + 22x^{18} + 31x^{19} + 12x^{20} + 30x^{21} + \\ &\quad + 18x^{22} + 6x^{23} + 24x^{24} + 4x^{25} + 31x^{26} + 14x^{27} + 15x^{28} + 16x^{29} + 21x^{30}. \end{aligned}$$

Для того чтобы при помощи леммы 1 получить кодовое расстояние построенного вейвлет-кода, вычислим значения кодового многочлена $f(x)$ в точках $1,\alpha,\ldots,\alpha^{30}$. Получаем, что $f(\alpha^j)=0$ при $j=0,\ldots,2$, следовательно, параметры j^* и d равны 0 и 13 соответственно, поэтому, согласно лемме 1, рассматриваемый вейвлет-код имеет кодовое расстояние 15 и может быть обозначен как $W[31,15,15]$.

Для иллюстрации работы алгоритма рассмотрим кодовое слово

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

и соответствующее ему зашумлённое кодовое слово

$$\widetilde{c} = (1,3,1,8,6,12,19,17,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0).$$

Описанный в п. 1 алгоритм позволяет найти все информационные слова вейвлет-кода $W[31,15,15]$, соответствующие кодовые слова которых попадают в шар радиуса 8 с центром в зашумлённом кодовом слове $\widetilde{c}$. На первом шаге алгоритм преобразует принятое зашумлённое кодовое слово $\widetilde{c}$ вейвлет-кода $W[31,15,15]$ в зашумлённое кодовое слово кода Рида — Соломона $\mathrm{RS}[31,17]$

$$\widetilde{s} = (1,5,5,3,29,28,2,20,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0).$$

На втором шаге алгоритм применяет к зашумлённому кодовому слову $\widetilde{s}$ процедуру списочного декодирования кодов Рида — Соломона и получает список информационных слов β кода Рида — Соломона $\mathrm{RS}[31,17]$

$$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0),$$
$$(28,22,21,17,8,15,26,0,8,6,4,12,20,5,26,7,21).$$

На третьем шаге алгоритм решает систему из семнадцати линейных уравнений с пятнадцатью неизвестными (в связи с большой размерностью она не приведена) для каждого информационного слова β из списка, полученного на втором шаге, и получает список информационных слов v вейвлет-кода $W[31, 15, 15]$

$$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(21, 31, 18, 19, 6, 12, 11, 8, 25, 9, 24, 8, 6, 5, 22).$$

Полученным информационным словам соответствуют кодовые слова

$$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(12, 3, 1, 8, 6, 12, 19, 17, 31, 0, 2, 0, 5, 0, 17, 0, 0, 27, 0, 23, 0, 0, 0, 0, 0, 0, 0, 11, 0, 0, 0)$$

вейвлет-кода $W[31, 15, 15]$ с процедурой кодирования (1) и порождающим многочленом $f(x)$, каждое из которых попадает в шар радиуса 8 с центром в зашумленном кодовом слове $\widetilde{c}$.

Заключение

В работе доказано, что вейвлет-код, определённый над полем $\mathrm{GF}(2^m)$, с длиной кодовых и информационных слов $n = 2^m - 1$ и $(n-1)/2$ соответственно и процедурой кодирования (1), с порождающим многочленом $f(x)$, для которого выполняются соотношения

$$f(\alpha^j) = 0 \text{ при } j = j^*, \ldots, j^* + d,\ 0 < d < \frac{n-3}{2},$$

имеет кодовое расстояние $\geqslant d + 2$ и допускает списочное декодирование. На основании приведённых доказательств описаны шаги алгоритма, позволяющего осуществлять списочное декодирование вейвлет-кодов.

Алгоритм реализован в виде программы, реализующей декодирование вейвлет-кода $W[n, (n-1)/2, d+2]$ 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 из [19]. Написанная программа была успешно применена для декодирования зашумлённых кодовых слов кодов $W[7, 3, 4]$ и $W[31, 15, 15]$.

Доказано, что неравенство Варшамова — Гилберта не позволяет судить о существовании вейвлет-кода $W[n, (n-1)/2, d+2]$, $0 < d < (n-3)/2$, над полем характеристики два с кодовым расстоянием $(n-1)/2$ при достаточно больших n.

ЛИТЕРАТУРА

1. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1974. 744 с.
2. *Fekri F., McLaughlin S. W., Mersereau R. M., and Schafer R. W.* Double circulant self-dual codes using finite-field wavelet transforms // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Berlin: Springer, 1999. P. 355–363.
3. *Fekri F., McLaughlin S. W., Mersereau R. M., and Schafer R. W.* Error Control Coding using Finite-Field Wavelet Transforms. Atlanta: Center for Signal Image Processing, 1999. 13 p.
4. *Daubechies I.* Десять лекций по вейвлетам. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
5. *Mallat S.* Wavelet Tour of Signal Processing. 2nd ed. Boston: Academic Press, 1999. 799 p.

6. *Phoong S. M. and Vaidyanathan P. P.* Paraunitary filter banks over finite fields // IEEE Trans. Signal Processing. 1997. V. 45. No. 6. P. 1443–1457.
7. *Fekri F., Mersereau R. M., and Schafer R. W.* Theory of paraunitary filter banks over fields of characteristic two // IEEE Trans. Inform. Theory. 2002. V. 48. No. 11. P. 2964–2979.
8. *Fekri F. and Delgosha F.* Finite-Field Wavelet Transforms with Applications in Cryptography and Coding. Upper Saddle River: Prentice Hall, 2010. 304 p.
9. *Caire G., Grossman R. L., and Poor H. V.* Wavelet transforms associated with finite cyclic groups // IEEE Trans. Inform. Theory. 1993. V. 39. No. 4. P. 1157–1166.
10. *Fekri F., Mersereau R. M., and Schafer R. W.* Theory of wavelet transform over finite fields // Proc. IEEE Intern. Conf. Acoustics, Speech, and Signal Processing. 1999. V. 3. P. 1213–1216.
11. *Черников Д. В.* Помехоустойчивое кодирование с использованием биортогональных наборов фильтров // Сибирские электрон. матем. известия. 2015. Т. 12. С. 704–713.
12. *Doubechies I. and Sweldens W.* Factoring wavelet transforms into lifting steps // J. Fourier Anal. Appl. 1998. V. 4. No. 3. P. 247–269.
13. *Соловьев А. А., Черников Д. В.* Биортогональные вейвлет-коды в полях характеристики два // Челяб. физ.-мат. журн. 2017. Т. 2. №1. С. 66–79.
14. *Берлекэмп Э.* Алгебраическая теория кодирования. М.: Мир, 1971. 479 с.
15. *Сидельников В. М.* Теория кодирования. М.: Физматлит, 2008. 324 с.
16. *Berlekamp E. R. and Welch L. R.* Error Correction of Algebraic Block Codes. US Patent 4633470A. 30.12.1986.
17. *Ромащенко А. Е., Румянцев А. Ю., Шень А.* Заметки по теории кодирования. М.: МЦНМО, 2011. 80 с.
18. *Sudan M.* Decoding of Reed Solomon codes beyond the error-correction bounds // J. Complexity. 1997. V. 13. No. 1. P. 180–193.
19. *Guruswami V. and Sudan M.* Improved decoding of Reed — Solomon and algebraic-geometric codes // IEEE Trans. Inform. Theory. 1999. V. 45. No. 6. P. 1757–1767.
20. *Литичевский Д. В.* Списочное декодирование биортогональных вейвлет-кодов с заданным кодовым расстоянием в поле нечётной характеристики // Прикладная дискретная математика. 2018. № 39. С. 72–77.
21. *Соловьев А А.* Комплементарное представление многочленов над конечными полями // Челяб. физ.-мат. журн. 2017. Т. 2. Вып. 2. С. 199–209.

REFERENCES

1. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Elsevier, 1977. 744 p.
2. *Fekri F., McLaughlin S. W., Mersereau R. M., and Schafer R. W.* Double circulant self-dual codes using finite-field wavelet transforms. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Berlin, Springer, 1999, pp. 355–363.
3. *Fekri F., McLaughlin S. W., Mersereau R. M., and Schafer R. W.* Error Control Coding using Finite-Field Wavelet Transforms. Atlanta, Center for Signal Image Processing, 1999, 13 pp.
4. *Daubechies I.* Desyat' lektsiy po veyvletam [Ten Lectures on Wavelets]. Izhevsk, SRC "Regular and Chaotic Dynamics", 2001. 464 p. (in Russian)
5. *Mallat S.* Wavelet Tour of Signal Processing, 2nd ed. Boston, Academic Press, 1999. 799 p.
6. *Phoong S. M. and Vaidyanathan P. P.* Paraunitary filter banks over finite fields. IEEE Trans. Signal Processing, 1997, vol. 45, no. 6, pp. 1443–1457.
7. *Fekri F., Mersereau R. M., and Schafer R. W.* Theory of paraunitary filter banks over fields of characteristic two. IEEE Trans. Inform. Theory, 2002, vol. 48, no. 11, pp. 2964–2979.

8. *Fekri F. and Delgosha F.* Finite-Field Wavelet Transforms with Applications in Cryptography and Coding. Upper Saddle River, Prentice Hall, 2010. 304 p.
9. *Caire G., Grossman R. L., and Poor H. V.* Wavelet transforms associated with finite cyclic groups. IEEE Trans. Inform. Theory, 1993. vol. 39, no. 4, pp. 1157–1166.
10. *Fekri F., Mersereau R. M., and Schafer R. W.* Theory of wavelet transform over finite fields // Proc. IEEE Intern. Conf. Acoustics, Speech, and Signal Processing, 1999, vol. 3, pp. 1213–1216.
11. *Chernikov D. V.* Pomekhoustoychivoye kodirovaniye s ispol'zovaniyem biortogonal'nykh naborov fil'trov [Error-correcting codes using biorthogonal filter banks]. Siberian Electronic Mathematical Rep., 2015, vol. 12, pp. 704–713. (in Russian)
12. *Doubechies I. and Sweldens W.* Factoring wavelet transforms into lifting steps. J. Fourier Anal. Appl., 1998, vol. 4, no. 3, pp. 247–269.
13. *Soloviev A. A. and Chernikov D. V.* Biortogonal'nyye veyvlet kody v polyakh kharakteristiki dva [Biorthogonal wavelet codes in the fields of characteristic two]. Chelyabinsk Physics and Mathematics J., 2017, vol. 2, no. 1, pp. 66–79. (in Russian)
14. *Berlekamp E. R.* Algebraic Coding Theory. N.Y., McGraw-Hill Book Company, 1968. 470 p.
15. *Sidelnikov V. M.* Teoriya kodirovaniya [Theory of Coding]. Moscow, Fizmatlit Publ., 2008. 324 p. (in Russian)
16. *Berlekamp E. R. and Welch L. R.* Error Correction of Algebraic Block Codes. US Patent 4633470A, 30.12.1986.
17. *Romashchenko A. E., Rumyantsev A. J., and Shen A.* Zametki po teorii kodirovaniya [Notes on the theory of coding]. Moscow, MCCME Publ., 2011. 80 p. (in Russian)
18. *Sudan M.* Decoding of Reed Solomon codes beyond the error-correction bounds. J. Complexity, 1997, vol. 13, no. 1, pp. 180–193.
19. *Guruswami V. and Sudan M.* Improved decoding of Reed — Solomon and algebraic-geometric codes. IEEE Trans. Inform. Theory, 1999, vol. 45, no. 6, pp. 1757–1767.
20. *Litichevskiy D. V.* Spisochnoye dekodirovaniye biortogonal'nykh veyvlet-kodov s zadannym kodovym rasstoyaniyem v pole nechetnoy kharakteristiki [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. (in Russian)
21. *Soloviev A. A.* Komplementarnoe predstavlenie polinomov nad konechnymi polyami [Complementary representation of polynomials over finite fields]. Chelyabinsk Physics and Mathematics J., 2017, iss. 2, pp. 199–209. (in Russian)