ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 519.725

СПИСОЧНОЕ ДЕКОДИРОВАНИЕ БИОРТОГОНАЛЬНЫХ ВЕЙВЛЕТ-КОДОВ С ЗАДАННЫМ КОДОВЫМ РАССТОЯНИЕМ В ПОЛЕ НЕЧЁТНОЙ ХАРАКТЕРИСТИКИ

Д. В. Литичевский

Челябинский государственный университет, г. Челябинск, Россия

Представлено теоретическое обоснование возможности списочного декодирования для биортогональных вейвлет-кодов $W[n, n/2, d]$ с заданным кодовым расстоянием над полями нечётной характеристики. Для входного сообщения длины n задача списочного декодирования заключается в нахождении всех кодовых слов, расстояние Хэмминга до которых не превосходит заданного значения. Для кода $W[n, n/2, d]$ эта задача сводится к задаче списочного декодирования для кода Рида — Соломона $\mathrm{RS}[n, n-d+1]$ посредством преобразования входящего сообщения и последующего применения к его результатам улучшенной версии алгоритма Гурусвами — Судана. Результаты декодирования для кода $W[n, n/2, d]$ находятся путём решения системы линейных уравнений относительно коэффициентов информационного многочлена, полученной из преобразования Фурье кодового слова вейвлет-кода, для каждого найденного информационного слова кода $\mathrm{RS}[n, n-d+1]$, являющегося в решаемой системе столбцом свободных членов. Приведены примеры результатов списочного декодирования для кода $W[26, 13, 12]$, на которых длина результирующего списка равна 2.

Ключевые слова: *вейвлет-коды, коды с заданным кодовым расстоянием, декодирование списком.*

DOI 10.17223/20710410/39/6

LIST DECODING OF THE BIORTHOGONAL WAVELET CODE WITH PREDETERMINED CODE DISTANCE ON A FIELD OF ODD CHARACTERISTIC

D. V. Litichevskiy

Chelyabinsk State University, Chelyabinsk, Russia

E-mail: litichevskiydv@gmail.com

In the article, a list decoding algorithm for the biorthogonal wavelet codes $W[n, n/2, d]$ with a predetermined code distance on a field of odd characteristic is presented. The "list decoding" problem the algorithm solves is the following: given an input message of the length n, compute all the codewords the Hamming distance to which does not exceed the given value. The list decoding algorithm for the code $W[n, n/2, d]$ is based on the transformation of the list decoding problem for $W[n, n/2, d]$ to the list decoding problem for the Reed — Solomon code $\mathrm{RS}[n, n-d+1]$ by proper converting

the incoming messages and on the subsequent solution of the second problem by the improved Guruswami — Sudan algorithm. Decoding results for the code $W[n, n/2, d]$ are found by solving a system of linear equations with respect to the coefficients of the information polynomial. The system is obtained from the Fourier transform of the code word of the wavelet code for each found information word of the code $\mathrm{RS}[n, n-d+1]$. In the system, the symbols of this word are constant terms. Examples of the list decoding for the code $W[26, 13, 12]$ are given. The algorithm has been implemented in the form of a computer program for which an author's certificate has been received.

Keywords: *wavelet codes, code with predetermined code distance, list decoding.*

Введение

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.

Будем говорить, что код допускает декодирование списком длины L с исправлением e ошибок, если любой шар радиуса e содержит не более L кодовых слов. Для кодов Рида — Соломона задача полиномиального декодирования списком решена В. Гурусвами и М. Суданом и [1].

В настоящей работе рассматривается возможность использования алгоритма списочного декодирования Гурусвами — Судана для построенных ранее вейвлет-кодов с заданным кодовым расстоянием [2].

1. Алгоритм списочного декодирования

Введём следующие обозначения: $\mathrm{GF}(q)$ — конечное поле из q элементов; n — длина кодовых слов; k — длина информационных слов; e — число возможных ошибок; d $(d \leqslant n-k+1)$ — кодовое расстояние (равное $n-k+1$ для кодов Рида — Соломона).

Информационному слову $v_0, v_1, \ldots, v_{k-1}$ процедура кодирования кода Рида — Соломона ставит в соответствие набор значений многочлена $v(x) = \sum\limits_{j=0}^{k-1} v_j x^j$ в n точках поля. Пусть $x_1, x_2, \ldots, x_n$ ($x_i \neq x_j$ при $i \neq j$) и $y_1, y_2, \ldots, y_n$ — произвольные элементы поля $\mathrm{GF}(q)$. Построение списка кодовых слов алгоритм декодирования осуществляет в два этапа: интерполяционный и факторизационный.

На интерполяционном этапе выполняется поиск многочлена $Q(x, y) \in \mathrm{GF}(q)[x, y]$, такого, что $Q(x, y)$ обращается в нуль во всех точках (x_i, y_i), $i = 1, \ldots, n$.

Для натурального числа $a > \sqrt{2(k-1)n}$ доказано, что если многочлен $p(x)$ имеет степень меньше k и $p(x_i) = y_i$ в s точках (x_i, y_i), причём $s > a$, то $Q(x, p(x)) = 0$ и многочлен $Q(x, y)$ делится на $y - p(x)$. Число делителей вида $y - p(x)$ у многочлена $Q(x, y)$ меньше числа $a/(k-1)$. Неизвестными являются коэффициенты $a_{u\nu}$ многочлена

$$Q(x, y) = \sum_{u+(k-1)\nu<a} a_{u\nu} x^u y^\nu,$$

которые находятся из системы линейных уравнений

$$\sum_{u+(k-1)\nu<a} a_{u\nu} x_i^u y_i^\nu = 0, \ i = 1, \ldots, n,$$

при небольших значениях n, например методом Гаусса.

На факторизационном шаге выполняется поиск всех многочленов $p(x) \in \mathrm{GF}(q)[x]$, таких, что $y - p(x)$ делит $Q(x, y)$ и степень $p(x)$ меньше k. Найденные многочлены формируют искомый список кодовых слов. Эффективный алгоритм факторизации предложен в [3]. Подробное изложение алгоритма приводится в [4].

2. Схема полифазного кодирования

В поле $\mathrm{GF}(q)$, где $q = p^m$, m — натуральное и $p \neq 2$ — простое число, введём биортогональные вейвлет-коды длины n, $n = q - 1$, с информационными словами длины $n/2$.

Пусть

$$H = \mathrm{cir}_2(h_0, h_1, \ldots, h_{n-1}), \quad G = \mathrm{cir}_2(g_0, g_1, \ldots, g_{n-1}),$$
$$\widetilde{H} = \mathrm{cir}_2(\widetilde{h}_0, \widetilde{h}_1, \ldots, \widetilde{h}_{n-1}), \quad \widetilde{G} = \mathrm{cir}_2(\widetilde{g}_0, \widetilde{g}_1, \ldots, \widetilde{g}_{n-1})$$

— 2-циркулянтные матрицы, определяющие процедуры разложения и восстановления сигнала биортогонального кратномасштабного анализа и удовлетворяющие условию точного восстановления. 2-Циркулянтная матрица задаётся первой строкой, последующая строка получается из предыдущей циклическим сдвигом на две позиции вправо.

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

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

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

Введём полифазные матрицы для пар весовых функций $(h(x), g(x))$ и $(\widetilde{h}(x), \widetilde{g}(x))$:

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

Пара матриц $P(x)$ и $\widetilde{P}(x)$ удовлетворяет условию точного восстановления тогда и только тогда, когда

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

(см. [2, 5]). 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 наибольшего общего делителя и операции лифтинга. Для многочлена $s(x)$, $\deg s(x) < n/2$, 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 $P(x)^{-1} = \widetilde{P}(x^{n/2-1})$ и

$$g_o(x) = \widetilde{h}_e(x^{n/2-1}), \quad g_e(x) = -\widetilde{h}_o(x^{n/2-1}),$$
$$h_o(x) = -\widetilde{g}_e(x^{n/2-1}), \quad h_e(x) = -\widetilde{g}_o(x^{n/2-1}).$$

Процедура кодирования определяется с помощью полифазных составляющих

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

где $v(x) = \sum\limits_{j=0}^{n/2-1} v_j x^j$ — информационный многочлен, $a \in \mathrm{GF}(q)$. 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. Многочлен $F(x) = h(x) + x^2 g(x)$ будем называть *порождающим*.

Информационное слово восстанавливается по кодовому слову с помощью матрицы

$$\begin{bmatrix} \widetilde{h}_e(x^{n/2-1}) & \widetilde{g}_e(x^{n/2-1}) \end{bmatrix}.$$

Выберем d так, чтобы $0 < d < n/2$. Будем считать, что многочлены $h(x)$ и $g(x)$ степени $\leqslant n-1$ построены так (см. [2]), что имеют место равенства

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

Здесь α — примитивный элемент поля $\mathrm{GF}(q)$. Тогда преобразование Фурье кодового многочлена $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ запишется в виде

$$\big(\underbrace{0, \ldots, 0}_{d+1}, C_{d+1}, \ldots, C_{n-1}\big).$$

В [2] доказано, что для любого d, $0 < d < n/2$, среди построенных вейвлет-кодов над полем $\mathrm{GF}(q)$ найдётся код с заданным кодовым расстоянием $d+2$. Для $C(x) = C_{d+1}x^{d+1} + C_{d+2}x^{d+2} + \cdots + C_{n-1}x^{n-1}$ обратным преобразованием Фурье находятся коэффициенты кодового многочлена: $c_j = n^{-1}C(\alpha^{-j})$, $j = 0, \ldots, n-1$, где n^{-1} — элемент, обратный элементу $n \bmod p$ в поле $\mathrm{GF}(q)$.

Так как α^{-1}, как и α, — примитивный элемент поля $\mathrm{GF}(q)$, то обратное преобразование Фурье последовательности $\{C_i\}_{i=0}^{n-1}$ является кодовой последовательностью кода Рида — Соломона с параметрами $(n, n-d-1)$. Поэтому построенный 2-циркулярный вейвлет-код является подпространством кода Рида — Соломона.

Из результатов работы [1], в частности, следует, что длина списка вейвлет-кодов не превышает двух, чему соответствуют результаты проведённых численных экспериментов.

3. Декодирование списком вейвлет-кода

Пусть α — примитивный элемент поля $\mathrm{GF}(q)$. Обозначим через $W[n, n/2, d+2]$ вейвлет-код с заданным кодовым расстоянием $d+2$, $0 < d < n/2$. Обозначим через $v(x)$ информационный многочлен и $c(x)$ — кодовый многочлен вида

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

где $F(x)$ — порождающий многочлен кода. Согласно свойствам порождающего многочлена $F(x)$, последовательность

$$F(\alpha^0), F(\alpha^1), \ldots, F(\alpha^{n-1})$$

имеет непрерывный участок длины $d+1$, состоящий из нулевых элементов. Тогда спектральный многочлен

$$C(y) = \sum_{j=0}^{n-1} C_j y^j,$$

где $C_j = c(\alpha^j)$, $j = 0, \ldots, n-1$, — коэффициенты преобразования Фурье для кодового слова, имеет не более $n-d-1$ ненулевых коэффициентов и может быть представлен в виде

$$C(y) = y^{j^*} \sum_{j=0}^{n-d-2} C_{j+j^*} y^j,$$

где j^* — номер первого ненулевого C_j. Тогда представим $c_i = n^{-1}C(\alpha^{-i})$ в виде

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

или

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

Полученное в (2) преобразование соответствует коду Рида — Соломона $\mathrm{RS}(n, n-d-1)$, в котором кодовое слово s получается из информационного слова β по формулам

$$s_i = \sum_{j=0}^{n-d-2} \beta_j \alpha^{-ij},\ i = 0, \ldots, n-1, \tag{3}$$

что допустимо, поскольку α^{-1} является примитивным элементом поля $\mathrm{GF}(q)$. Таким образом, для получения списка возможных спектральных многочленов $C(y)$ можем воспользоваться декодером Гурусвами — Судана, применённым к коду $\mathrm{RS}(n, n-d-1)$ с процедурой кодирования (3), на вход которого подаётся кодовое слово $s_i = c_i n \alpha^{ij^*}$, $i = 0, \ldots, n-1$.

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

$$v(\alpha^{2j}) F(\alpha^j) = C_j.$$

Значит, должны выполняться соотношения

$$v(\alpha^{2(j+j^*)}) F(\alpha^{j+j^*}) = \beta_j,\ j = 0, \ldots, n-d-2. \tag{4}$$

Равенства (4) задают систему линейных уравнений относительно коэффициентов информационного многочлена вейвлет-кода, содержащую $n/2$ неизвестных и $n-d-1 > n/2$ уравнений. Поэтому рассматриваемый вейвлет-код $W[n, n/2, d+2]$ является подпространством кода $\mathrm{RS}[n, n-d-1]$ и не всякому информационному слову β из списка, возвращённого декодером Гурусвами — Судана, будет соответствовать информационное слово v вейвлет-кода, которое находится из системы (4).

4. Результаты численных экспериментов

Описанный подход проверялся в эксперименте с вейвлет-кодом $W[26, 13, 12]$ и соответствующим ему кодом $\mathrm{RS}[26, 15]$ над полем $\mathrm{GF}(27)$ с неприводимым многочленом $2 + 2x + x^3$ и порождающим элементом 2α, где α — корень выбранного неприводимого многочлена. В качестве фильтра $h(x)$ был произвольным образом выбран многочлен

$h(x) = 22 + x^3 + 2x^4 + 3x^5 + 4x^6 + x^7 + 6x^8 + 7x^9 + 8x^{10} + 9x^{11} + x^{12} + 10x^{13} + x^{14} + 12x^{15} + + x^{16} + 14x^{17} + x^{18} + 17x^{19} + x^{20} + 19x^{21} + 20x^{22} + x^{23} + x^{24} + x^{25}$, на основании которого был построен порождающий многочлен кода $W[26, 13, 12]$.

Для эксперимента рассматривалось нулевое информационное слово. В соответствующее ему нулевое кодовое слово вводились 6 случайных ошибок, правильными считались 20 принятых значений. В большинстве случаев список во временной области содержит единственное кодовое слово, например, для зашумленных слов

$$(1, 1, 8, 14, 15, 16, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$
$$(0, 0, 1, 0, 0, 0, 1, 0, 8, 0, 0, 0, 0, 0, 0, 14, 2, 0, 0, 0, 0, 0, 0, 4, 0, 0, 0)$$

список содержит только нулевое кодовое слово. Вместе с тем для зашумленного кодового слова $(0, 0, 1, 0, 0, 0, 1, 0, 12, 0, 0, 0, 0, 0, 0, 0, 12, 4, 0, 0, 0, 0, 0, 0, 3, 0, 0, 0)$ список во временной области содержит два информационных слова:

$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ и $(25, 22, 2, 6, 4, 11, 20, 25, 12, 8, 13, 22, 14)$.

Заключение

В работе описана процедура списочного декодирования биортогональных вейвлет-кодов с заданным кодовым расстоянием на примере вейвлет-кода $W[26, 13, 12]$. Предложенная процедура списочного декодирования может быть применена к любому коду, являющемуся подпространством кода Рида — Соломона. Алгоритм программно реализован (свидетельство № 2017619148).

Работа выполнена под руководством проф. А. А. Соловьева.

ЛИТЕРАТУРА

1. *Guruswami V. and Sudan M.* Improved Decoding of Reed — Solomon and Algebraic — Geometric Codes. Electronic Colloquium on Computational Complexity. 1998. Report No. 43.
2. *Соловьев А. А., Черников Д. В.* Биортогональные вейвлет-коды с заданным кодовым расстоянием // Дискретная математика. 2017. Т. 29. № 2. С. 96–108.
3. *Ruth R. and Ruckenstein G.* Efficient decoding of Reed — Solomon codes beyond half the minimum distance // IEEE Trans. Inform. Theory. 2000. V. 46. No. 1. P. 246–257.
4. *McEliece R. J.* The Guruswami — Sudan Decoding Algorithm for Reed — Solomon Codes. IPN Progress Report 42-153. May 15, 2003.
5. *Черников Д. В.* Полифазная схема помехоустойчивого кодирования над полями нечетной характеристики // Челябинский физико-математический журнал. 2016. Т. 1. № 3. С. 77–85.

REFERENCES

1. *Guruswami V. and Sudan M.* Improved Decoding of Reed — Solomon and Algebraic — Geometric Codes. Electronic Colloquium on Computational Complexity, 1998, Report no. 43.
2. *Soloviev A. A. and Chernikov D. V.* Biortogonal'nye veyvlet-kody s zadannym kodovym rasstoyaniem [Biorthogonal wavelet codes with predetermined code distance]. Diskr. Mat., 2017, vol. 29, no. 2, pp. 96–108. (in Russian)
3. *Ruth R. and Ruckenstein G.* Efficient decoding of Reed — Solomon codes beyond half the minimum distance. IEEE Trans. Inform. Theory, 2000, vol. 46, no. 1, pp. 246–257.
4. *McEliece R. J.* The Guruswami — Sudan Decoding Algorithm for Reed — Solomon Codes. IPN Progress Report 42-153. May 15, 2003.
5. *Chernikov D. V.* Polifaznaya skhema pomekhoustoychivogo kodirovaniya nad polyami nechetnoy kharakteristiki [Polyphase scheme of noise-immune encoding over fields of odd characteristic]. Chelyab. Fiz.-Mat. Zh., 2016, vol. 1, no. 3, pp. 77–85. (in Russian)