КОДИРОВАНИЕ И ДЕКОДИРОВАНИЕ МАТРОИДНОГО КОДА, ИСПРАВЛЯЮЩЕГО ПАКЕТЫ ОШИБОК

Бодян Г. К., Бодян Д. Г., Чернелев Д. П.
Технический Университет Молдовы, Шт. чел Маре, 168, Кишинев – MD2012, Р. Молдова
Тел.: (3732)237505; e-mail: gbodean@mail.md

Аннотация – Определены функции кодера и декодера матроидного кода. Разработана методика оптимизации вычислений и распознавания ошибки, рассмотрены особенности кодирования и декодирования матроидного кода.

I. Введение

Понятие *матроидный код* впервые было введено в работе [1]. В указанной работе предлагалось использовать матроиды для восстановления информации в случае возникновения потерь при передаче ее по сетям связи. Но, очертив проблему, авторы столкнулись с неразрешимостью (на тот момент) задачи построения однородных матроидов с заданной избыточностью и предложили "смягчить" требования к матроидному коду в ущерб надежности восстановления.

Данная работа посвящена задачам разработки кодера и декодера матроидного кода, представленного в его "жесткой" форме, т.е. однородным матроидом.

II. Основная часть

Функция кодера матроидного кода (или М-кода) определяется преобразованием **v= x • A:** на вход кодера (от источника) поступает информационное слово **x** длины k с m-разрядными символами; на выходе кодера формируется кодовое слово **v** удвоенной длины, т.е. равное $2\cdot k$, с m-разрядными символами; кодер выполняет матричное умножение **x** на **A** над полем $\mathbf{GF}^k(2^m)$, где матрица **A** представляет соответствующий однородный матроид.

Рассмотрим пример. Пусть k=3 и m=4. Для указанной характеристики m выберем в качестве порождающего (генератора поля) полином $p(x)=1+x+x^4$ с операциями над **GF**(2), а в качестве генератора кода – полином $g(x)=1+x+x^2+2x^3$ над $\mathbf{GF}^3(2^4)$. Составим таблицу умножения по модулю $p(x)$. Для этого представим элементы поля **GF**(p) в десятичном формате, т.е. 0 – это 0, 1 – это 1, 2 – это x, 3 – это $x+1$, 4 – это x^2, и т.д., 15 – это x^3+x^2+x+1. Результаты умножения mod $p(x)$ представлены в таблице 1.

Таблица 1

Умножение по модулю $p(x)=1+x+x^4$

Table 1

Multiplication mod $p(x)$, $p(x)=1+x+x^4$

•	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Аддитивные операции выполняются как поразрядное XOR над соответствующими двоичными представлениями указанных десятичных чисел.

В качестве однородного матроида выберем структуру, представленную матрицей:

$$\mathbf{A} = \begin{bmatrix} 13 & 10 & 8 & 2 & 1 & 1 \\ 6 & 13 & 6 & 5 & 3 & 4 \\ 4 & 9 & 15 & 9 & 12 & 2 \end{bmatrix}. \quad (1)$$

Матрица (1) является конструктивной основой для построения кодера М-кода над $\mathbf{GF}^3(2^4)$. Имеем:

$$\langle v_1 \; v_2 \; v_3 \; v_4 \; v_5 \; v_6 \rangle = \langle x_1 \; x_2 \; x_3 \rangle \begin{bmatrix} 13 & 10 & 8 & 2 & 1 & 1 \\ 6 & 13 & 6 & 5 & 3 & 4 \\ 4 & 9 & 15 & 9 & 12 & 2 \end{bmatrix}$$

или

$$\begin{cases} 13x_1 + 6x_2 + 4x_3 = v_1, \\ 10x_1 + 13x_2 + 9x_3 = v_2, \\ 8x_1 + 6x_2 + 15x_3 = v_3, \\ 2x_1 + 5x_2 + 9x_3 = v_4, \\ x_1 + 3x_2 + 12x_3 = v_5, \\ x_1 + 4x_2 + 2x_3 = v_6. \end{cases} \quad (2)$$

На рис.1 представлена блок-схема искомого М-кодера. Стрелки на схеме помечены мультипликативными коэффициентами, а ⊕ - это символ вышеупомянутой аддитивной операции. Таким образом, компо-

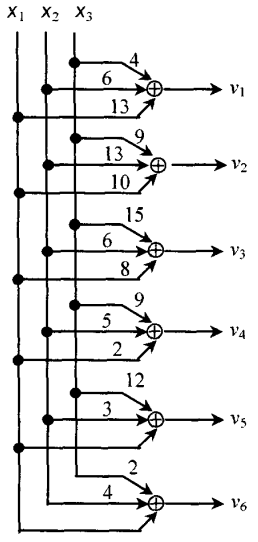

*Рис. 1. Блок-схема кодера М-кода с $g(x)=1+x+x^2+2x^3$ над $\mathbf{GF}^3(2^4)$ и $p(x)=1+x+x^4$ над **GF**(2)*

*Fig. 1. Block diagram of M-coder with $g(x)=1+x+x^2+2x^3$ over $\mathbf{GF}^3(2^4)$ and $p(x)=1+x+x^4$ over **GF**(2)*

2003 13th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2003). 8-12 September, Sevastopol, Crimea, Ukraine
 ISBN: 966-7968-26-X. IEEE Catalog Number: 03EX697

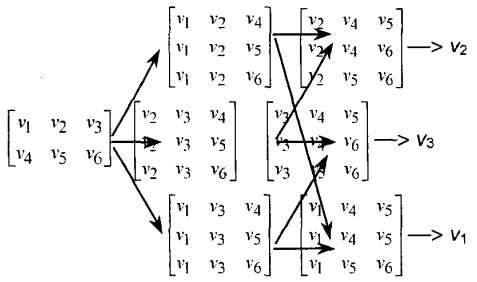

Рис. 2. Диаграмма последовательно-параллельного декодирования М-кода

Fig. 2. Diagram of sequential-concurrent M-code decoding

ненты x_1, x_2 и x_3 входного слова **x** умножаются на соответствующие мультипликативные коэффициенты, а потом суммируются по модулю $p(x)$; на выходе М-кодера имеем компоненты вектора **v**. Умножение выполняется асинхронно. Для этого разработана методика, позволяющая свести структуру комбинационной схемы умножителя, сложность которой порядка $O(m^4)$, к схеме с несколькими вентилями XOR. Например, умножение компоненты $x=(x_1, x_2, x_3, x_4)$ на 2 по модулю $p(x)$ будет выполняться по схеме: $x_1 \leftarrow x_4$, $x_2 \leftarrow x_1$ XOR x_4, $x_3 \leftarrow x_2$, $x_4 \leftarrow x_3$.

Декодер М-кода должен выполнять более сложную функцию, а именно, распознать ошибку в принятом векторе **v** и выбрать подсистему линейных уравнений, необходимых для восстановления исходных символов **x**. В общем случае, декодер должен распознать одну из $\sum_{i=1}^{k} C_{2k}^{i}$ ошибок вектора **v**. В приведенном примере допустима ошибка кратности 3; любая подсистема из 3-х уравнений системы (2) исправит ошибочную комбинацию. При поиске корректного решения можно перебрать (в наихудшем случае) C_{2k}^{k} подсистем линейных уравнений. Одним из способов оптимизации поисковой процедуры является представление иерархии решений в виде булевой решетки. Такое представление позволяет упорядочить процесс выбора подсистем уравнений и сократить (до минимума) число шагов распознавания ошибки. На рис.2 представлена диаграмма *последовательно-параллельного декодирования* для анализируемого примера; стрелка на диаграмме означает переход к следующей группе декодируемых (проверяемых на корректность) уравнений, если обнаружена ошибка; прерывистая стрелка указывает на ошибочную компоненту. Из диаграммы следует, что наиболее труднообнаружимая (и, соответственно, труднovосстанавливаемая) является одиночная ошибка.

III. Заключение

Предложены и исследованы эффективные схемы кодирования и декодирования матроидного кода. Кодирование и декодирование производятся асинхронно в режиме реального времени.

IV. Список литературы

[1] *Борщевич В. И., Олейник В. Л.* Матроидные коды – новый полход к защите информации в компьютерных системах. – Acta Academia, 1996-1997, pp. 40-49.

ENCODING AND DECODING OF THE MATROID BURST ERRORS CORRECTING CODE

Bodean Gh. C., Bodean D. Gh., Chernelev D. P.
Technical University of Moldova
St. cel Mare, 168, Kishinau – MD2012, R. Moldova
phone: (3732) 237505
e-mail: gbodean@mail.md

Abstract – Encoder and decoder algorithms of the matroid code are defined. The methods of calculus optimization and error recognition are elaborated. The features of the matroid code encoding/decoding are analyzed.

I. Introduction

Matroid codes were in [1], where a stochastic method of construction of the important variety of such codes - matrands, are considered. Also, it was shown that applications of matroid coding allows reaching the theoretical boundary of effective restoring of the lost data asymptotically. Present work deals with the tasks of encoder/decoder elaboration for the matroid (M-) code in its "pure" form.

II. Main part

The functioning of M-code encoder (or M-coder) is defined by **v= x • A:** the source codeword **x** of length k is applied to encoder; M-coder performs a matrix multiplication **x** by **A** over extended Galois field $\mathbf{GF}^k(2^m)$; the output is a vector **v** of length $n=2 \cdot k$. Vectors **x** and **v** consist of symbols that contain m bits and $k \times n$ matrix **A** represents a corresponding uniform matroid $\mathbf{U}_k$ of rank k.

For $k=3$ and $m=4$ a M-coding example is analyzed. Table 1 defines the multiplication modulo $p(x)$, where $p(x)$ is a field generator polynomial over **GF**(2) and the polynomials over $\mathbf{GF}(2^4)$ are shown in the decimal format. The sum mod $p(x)$ is performed as XOR bit-by-bit operation.

Matrix **A** given by (1) defines a uniform matroid generated by a polynomial $g(x)$ over $\mathbf{GF}^3(2^4)$. In this case the algorithm of functioning of M-coder will be defined by system (2). Fig. 1 shows the block diagram of such M-coder. The edges on Fig. 1 are marked by the multiplication coefficient, i.e. elements of the field $\mathbf{GF}(2^4)$. A method of optimal multiplication implementation was elaborated. As a result the multiplication scheme consists of some XOR gates. For the example above the multiplication of the vector's **x** component $x=(x_1, x_2, x_3, x_4)$ by 2 *mod* $p(x)$ will be performed as follows: $x_1 \leftarrow x_4$, $x_2 \leftarrow x_1$ XOR x_4, $x_3 \leftarrow x_2$, $x_4 \leftarrow x_3$.

The aim of M-code decoding is error recognition and original data restoration. A *sequential-concurrent decoding* algorithm is proposed (see Fig. 2). The basis of the scheme on Fig. 2 is the corresponding Boolean lattice. Such a way of error recognition scheme allows performing all operations in an asynchronous mode. Each edge in Fig. 2 means a transition if an error was found. From diagram in Fig. 2 results that single errors are most difficult to detect (see interrupted edges).

III. Conclusion

Efficient schemes of the matroid code encoding/decoding are proposed and analyzed in this paper. Encoding and decoding are asynchronously performed in real time.

2003 13th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2003). 8-12 September, Sevastopol, Crimea, Ukraine

ISBN: 966-7968-26-X. IEEE Catalog Number: 03EX697