КОРРЕКТИРУЮЩАЯ СПОСОБНОСТЬ И ГРАНИЦЫ СУЩЕСТВОВАНИЯ МАТРОИДНЫХ КОДОВ

Бодян Г. К.
Технический университет Молдовы ТУМ
Шт. чел Маре, 168, Кишинев – MD2012, Р. Молдова
Тел.: +(37322) 237505; e-mail: gbodean@mail.md

Аннотация – Получены аналитические выражения для расчета характеристик матроидных кодов и определены границы их существования.

I. Введение

В работе [1] предложен подход к построению нового класса линейных кодов, названный матроидное кодирование. Матроидные коды позволили раздвинуть границы существования линейных кодов. Так, в [2] на стр.72 представлен список кодов Хэмминга с параметрами (n, k), а в комментарии к нему приводится сомнение по поводу существования линейных кодов заданной корректирующей способности t в расширенном поле Галуа $\mathbf{GF}^k(2^m)$, где k – размерность поля или число степеней свободы (фактически число оригинальных, исходных символов), 2^m – характеристика поля, m – разрядность символа.

Кодовые слова (вектора) линейного блокового кода имеют четко выделенную информационную и контрольную части. Отличительная особенность слов матроидного кода – отсутствие такого разделения. В этом случае, любое подмножество из k символов переданного слова длины n (n>k) может быть использовано декодером для восстановления исходной последовательности.

В данной работе представлены новые результаты по исследованию характеристик матроидных (М-)кодов, а именно, определена зависимость длины кода n от характеристик t и k, установлены (нижняя и верхняя) границы существования М-кодов над полем $\mathbf{GF}^k(2^m)$ для фиксированных значений t и k, приведены примеры матроидов для различных характеристик, в том числе, важного для практики случая, m=8.

II. Основная часть

Напомним, что для построения М-кодов используется однородный матроид, который представляет собой семейство линейно независимых подмножеств одинакового ранга k. Пример такого матроида, построенного над полем $\mathbf{GF}^2(2^2)$ с порождающим полиномом $p(x)=1+x+x^2$, является матрица вида $\mathbf{U}(k,n,m)$:

$$\mathbf{U}(2,4,2)=\begin{bmatrix}1 & 1 & 1 & 1\\ 0 & 3 & 1 & 2\end{bmatrix}. \qquad (1)$$

Кодовые слова $\mathbf{v}(x)$ формируются путем умножения исходного вектора $\mathbf{a}(x)$ на матрицу $\mathbf{U}(k,n,m)$, т.е. $\mathbf{v}=\mathbf{a}\cdot\mathbf{U}$. Учитывая, что операции умножения и сложения выполняются по модулю $p(x)$ – см. таблицу 1, получаем список векторов, представленный в таблице 2. Символы таблиц 1 и 2 имеют одну и ту же разрядность m, равную 2.

Интересно заметить, что число нулей и единиц в слове v(x), кроме первого и последнего (см. таблицу 2), находятся в равной пропорции – 4 и 4. С точки зрения разработчиков систем связи такой код приближается к идеальному, обеспечивая максимальную пропускную способность канала.

Таблица 1.
Table 1.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Таблица 2.
Table 2.

a(x)	v(x)
00	0000
01	0312
02	0123
03	0231
10	1111
11	1203
12	1032
13	1320
20	2222
21	3130
22	2301
23	2031
31	3021
32	3210
33	3102
30	3333

Матроидный код, заданный матрицей $\mathbf{U}(2,4,2)$, позволяет обнаружить и скорректировать одиночную ошибку, т.е. $t=1$. Под ошибкой подразумевается символ отличительный от переданного.

Обобщенный анализ корректирующей способности М-кода показал, что между характеристиками n, k и t существует следующая зависимость:

$$n=2t+k \text{ или } n=2t+k+1, \qquad (2)$$

причем t, для фиксированного k, есть функция от m.

Для поиска однородных матроидов в поле Галуа $\mathbf{GF}^k(2^m)$ была разработана специализированная программа, написанная на языке Delphi. На рисунке 1 представлен интерфейс этой программы. Результаты поиска однородных матроидов, при помощи разработанной программы, представлены в таблице 3. Символом √ отмечен факт наличия соответствующе-

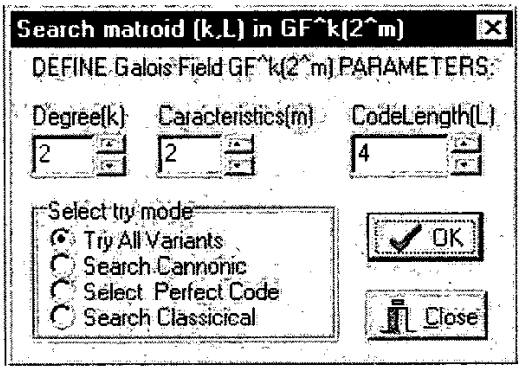

Рис. 1. Интерфейсная часть программы поиска однородных матроидов.

Fig. 1. Interface of the matroid searching software

2004 14th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2004). 13-17 September, Sevastopol, Crimea, Ukraine
 ISBN: 966-7968-69-3. IEEE Catalog Number: 04EX843

го однородного матроида, а символом ∅ – отсутствие такового.

Таблица 3.

Границы существования М-кодов над $GF^k(2^m)$
Bounds of matroid codes over $GF^k(2^m)$

k \ m	2	3	4	5	6	7	8
2	√	√	√	√	√	√	√
3	√	√	√	√	√	√	√
4	∅	√	√	√	√	√	√
5	∅	√	√	√	√	√	√
6	∅	√	√	√	√	√	√
7	∅	√	√	√	√	√	√
8	∅	∅	√	√	√	√	√

Зависимость t от m, например для k=2, представлена (частично) в таблице 4.

Таблица 4.

	2	3	3	4	4	4	4	5	...	5	6	...	6
t	1	2	3	4	5	6	7	8	...	15	16	...	31
n	4	6	8	10	12	14	16	18	...	32	34	...	64

Данные таблицы 4 необходимо интерпретировать следующим образом: для обеспечения большей корректирующей способности t необходимо переходить к полям более высокой степени m.

Верхний предел существования матроидов $U(k,m,n)$ для фиксированного k определяется периодом Эйлера над расширенным полем Галуа $GF^k(2^m)$:

$$\varphi(k,m) = \frac{2^{mk}-1}{2^m-1}. \qquad (3)$$

Например, $\varphi(k=2, m=4) = 17$.

Среди такого разнообразия матроидных кодов выбор остается за разработчиком. В качестве меры эффективности кода может быть использована величина $R=k/n$ – скорость кода [3]. При фиксированном t с ростом k увеличивается и значение скорости R. Очевидно, что при одинаковой скорости R следует отдавать предпочтение кодам с большей корректирующей способностью t. В таблице 5 приведены характеристики матроидных кодов с одинаковой скоростью R=1/3.

Таблица 5.

k, t	2	3	4	5	6	7	8
n	6	9	12	15	18	21	24

III. Заключение

Таким образом, получены характеристики матроидных кодов, исследованы границы их существования, разработано программное обеспечение для поиска М-кодов.

IV. Список литературы

[1] *Бодян Г. К.* Об одном методе помехозащищенного кодирования. Материалы Международной Крымской конференции «СВЧ-техника и телекоммуникационные технологии», Севастополь, сентябрь 8-12, 2003 г.

[2] *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986.

[3] *Кларк Дж., мл., Кейн Дж.* Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. – М.: Радио и связь, 1987.

CORRECTING ABILITY AND BOUNDS OF MATROID CODES

Bodyan Gh. C.
Technical University of Moldova
TUM, 168, St. cel Mare, Kishinau – MD2012, R. Moldova
phone: (37322) 237505
e-mail: gbodean@mail.md

Abstract –Analytical expressions to estimate the matroid codes parameters are obtained and bounds of matroid codes existence are found.

I. Introduction

Proposed in [1] was the technique to construct the new class of linear codes, named matroid coding. Matroid codes allow enlarging the bounds of linear codes. So, in [2] on page 72, the list of Hamming codes with parameters (n, k) are presented. Comments to this list doubts the existence of linear codes with the correcting capability (ability) over Galois field extension $GF^k(2^m)$, where k is degree of field, i.e. number of original symbols, 2^m – characteristics of field, m – bit codeword size.

Linear block codewords consist of information and control parts. Absences of such sharing (division) are distinctive particularities of matroid codes. In this case, any k symbols from n of the received codeword can be used to restore the original sequence.

New results about matroid (M-)codes parameters are presented in this work. Were established the dependences of the codeword length n from parameters t and k. Low and upper bounds of M-code existences over field $GF^k(2^m)$ for t and k fixed are found.

II. Main part

Uniform matroid $U(k,n)$ is used to generate M-codes. Example of such matroid over $GF^2(2^2)$ with $p(x)=1+x+x^2$ is given in (1). Codewords $\mathbf{v}(x)$ obtained by multiplication of the original vector $\mathbf{a}(x)$ on matrix $\mathbf{U}(k,n,m)$ are given in Table 2. The resulted codewords have correcting ability t=1. Error is a codeword symbol that differs from the transmitted one.

Dependences for M-code parameters n, k and t are given in (2), where $t=f(m)$ for k= fix. Software was elaborated for matroid codes searching. The interface of this software is presented in Figure 1. Results of matroid codes searching are given in Table 3, where symbol √ means the existence of uniform matroid, ∅ - absences of such matroid. The dependences t=f(m) for k=2 is given in Table 4. In this case the upper bound of matroids existences is given by Euler period (3).

The rate $R=k/n$ is other parameter of error controlling code. For R=1/3 the parameters of matroid code are given in Table 5. Selection of needed matroid code is up to the code designer.

III. Conclusion

In conclusion, parameters of matroid codes are found, bound of M-codes existences are analyzed, software to search the matroid codes was elaborated.

2004 14th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2004). 13-17 September, Sevastopol, Crimea, Ukraine

ISBN: 966-7968-69-3. IEEE Catalog Number: 04EX843