ХАРАКТЕРИСТИКИ СИСТЕМЫ СВЯЗИ С МАТРОИДНЫМ КОДИРОВАНИЕМ

Бодян Г. К., Дунай Л. Ф.
Технический университет Молдовы
ул. Шт. чел Маре 168, Кишинев - MD2012, Р. Молдова
тел.: +37322-237505, e-mail: gbodean@mail.md

Аннотация – Приведен анализ кодовых характеристик матроидных корректирующих кодов и энергетического выигрыша от применения этих кодов в системах связи. Также представлен алгоритм генерации оптимальной структуры умножителей над расширенным полем Галуа.

I. Введение

При оценке качества системы связи, содержащей устройства помехозащищенного кодирования и декодирования (*кодеки*), принято использовать отношение средней энергии на бит информации к спектральной мощности шума E_b/N_o. Среди известных *недвоичных* методов помехозащищенного кодирования самыми популярными и высокоэффективными являются коды Рида-Соломона (РС). Одним из "слабых мест" РС-кодов - это алгоритм декодирования и сложность его реализации. Известно, что сложность декодирования РС-кодов не превосходит величины $O(n \log^2 n)$ и зависит от сложности вычисления *свертки* в полях Галуа.

В работе [1] предложен и описан новый класс *линейных* кодов, названных *матроидными*. Матроидные (или М-) коды не уступают, по корректирующей способности, кодам РС. Для М-кодов разработаны алгоритмы кодирования и декодирования [2]. Благодаря своей линейности, аппаратная реализация кодека М-кода проще, чем для РС-кода. В докладе приводится расчет выигрыша от матроидного кодирования, а также представлен метод построения оптимальной структуры умножителей (мультипликаторов) на константу, используемых при вычислениях в *расширенных полях Галуа*.

II. Основная часть

Обычный метод определения энергетического выигрыша от кодирования (ЭВК) состоит в сравнении графиков, показывающих зависимость вероятности ошибки от E_b/N_o для систем без кодирования и с кодированием, с последующим определением разности значений E_b/N_o при данной вероятности ошибки. Матроидные коды – это *недвоичные линейные блоковые* (n, k) коды, построенные над расширенными полями Галуа **GF**(2^m), где n - число символов в кодовом слове, k - число исходных (информационных) символов на входе кодера, m - разрядность символов. М-коды с параметрами (n,k,t) существуют для всех n и k таких, что:

$$t = (n-k) \textbf{ div } 2 \text{ при } n \le 2^m+1, \quad (1)$$

где t – корректирующая способность кода, выраженная в символах. Между расстоянием Хэмминга d_{min} и параметром t соблюдается известное соотношение:

$$d_{min} = 2t+1 \text{ или } d_{min} = n-k+1. \quad (2)$$

Приведенные уравнения (1) и (2) устанавливают т.н. *границы для кодового расстояния* матроидных кодов с заданными параметрами (n, k, t) над полем **GF**(2^m). Легко видеть, что минимальное расстояние d_{min} прямо пропорционально (со знаком минус) скорости кода $R = k/n$.

Другой класс границ – это границы для *кодовых характеристик*. Алгоритм декодирования М-кодов является алгоритмом с *ограниченным расстоянием*, т.е. ни одна комбинация из более t ошибок не исправляется. Для таких алгоритмов вероятность отказа от декодирования, при появлении в кодовом слове более t ошибок, имеет бернуллевское распределение. С другой стороны, на вероятность ошибки на бит (BER) влияют отношения E_b/N_o. Лучшей считается та система, которая достигает желаемого значения BER при меньшей передаваемой мощности передатчика.

Для сравнения двух различных схем передачи сигналов исследуются графики зависимости BER от требуемых отношений E_b/N_o. Мощным средством исследования зависимостей BER от E_b/N_o является графическая среда **BERTool** системы **MATLAB**. На рис. 1 приведены характеристики матроидных кодов $(17, k, t)$ над **GF**(2^4) с различной скоростью R при использовании бинарной фазовой модуляции (когерентная система с жестким декодированием и аддитивным белым гауссовским шумом). Эти графики четко указывают, для каких скоростей R эффективно матроидное кодирование. Так, максимальный выигрыш от кодирования для BER=10^{-6}, характерной для коаксиального кабеля, достигается при t= 4 (соответственно R= 0,53) и составляет 4 дБ. (Известно, что каждый дополнительный децибел ЭВК дает в боль-

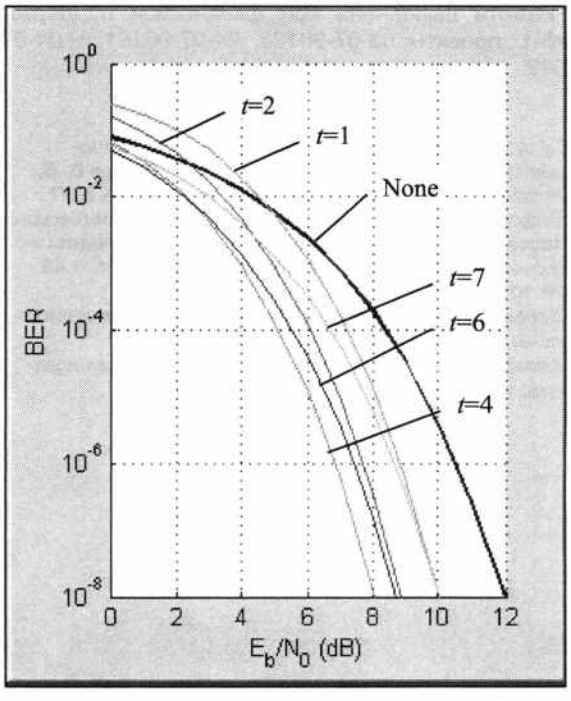

Рис. 1. Зависимость вероятности ошибки от отношения E_b/N_o для систем с М-кодированием.

Fig. 1. Bit-error probability versus E_b/N_o ratio for systems with M-coding

2005 15th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2005). 12-16 September, Sevastopol, Crimea, Ukraine

ших сетях экономический эффект в сотни миллионов долларов!) Дальнейшее увеличение значения t приводит к ухудшению эффективности М-кодирования.

Для снижения вычислительных затрат при реализации операции *свертки*, предложен и реализован алгоритм генерации структуры *мультипликатора на константу* :

Algorithm for calculating matrix $\mathbf{A}=[\mathbf{a}]_{m\times m}$
Enter: constant $\boldsymbol{C}$, field polynomial $p(x)$ of $\mathbf{GF}(2^m)$
Output: matrix **A**

```
for i,j=0 to m –1 do a_ij←0        // initialize A
for i= 0 to m-1 do                 // generate A
  a_i← C                           //copy C to row i
  ShiftLeft(C)
  if degree(C)= m then C← C⊕ p(x)  //bitwise XOR
end for
```

Матрица $\mathbf{A}=[\mathbf{a}_{ij}]$ отражает структуру умножителя на константу $\boldsymbol{C}$: $\mathbf{a}_{ij}$= 1, если существует связь $I \rightarrow j$; а противном случае $\mathbf{a}_{ij}$=0, где i есть индекс входного разряда, а j - выходного. При умножении на 1 матрица **A** - это единичная матрица, которой соответствует структура мультипликатора, представленная на рис.2, *a*). На рис.2, *b*) представлена матрица **A** и соответствующая схема умножителя на 9 над полем $\mathbf{GF}(2^4)$ с порождающим полиномом $p(x)=1+x+x^4$.

В нашем случае максимально сложная схема -

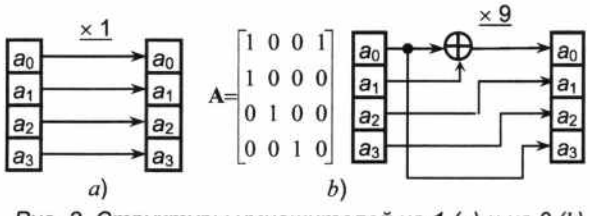

Рис. 2. Структуры умножителей на 1 (a) и на 9 (b).
Fig. 2. The structures of multipliers on 1 (a) and on 9 (b)

мультипликатор на 7, содержит 9 вентилей XOR, что в 4 раза проще, чем известная комбинационная схема, сложность которой составляет m^2 вентилей AND и $1{,}5(m^2-m)$ вентилей XOR. А в среднем, сложность мультипликаторов для приведенного примера составляет 4,25 (на порядок меньше!) вентилей XOR.

III. Заключение

Составлена *Simulink*-модель системы связи с матроидным кодированием. Моделирование позволило установить границы кодовых характеристик и оценить эффективность применения матроидных корректирующих кодов. Предложен алгоритм генерации оптимальной структуры мультипликаторов над полем Галуа.

IV. Список литературы

[1] *Бодян Г. К.* Об одном методе помехозащищенного кодирования. В кн.: 13-я Международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2003). Материалы конференции. — Севастополь: Вебер, 2003. - с. 357–358.

[2] *Бодян Г. К., Бодян Д. Г., Дунай Л. Ф.* Декодирование матроидных кодов. В кн.: 14-я Международная Крымская конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2004). Материалы конференции. — Севастополь: Вебер, 2004. - с.312–313.

PROPERTIES OF COMMUNICATION SYSTEM WITH MATROID CODING

Bodyan G. C., Dunai L. T.
Technical University of Moldova
St. cel Mare str., 168, Kishinau – MD2012, R. Moldova
Ph.: +37322-237505, e-mail: gbodean@mail.md

Abstract – Presented in this paper is the analysis of code characteristics for matroid codes and code gain at their use in communication systems. Also, the algorithm for generation of the optimal multiplier scheme over extended Galois field is presented.

I. Introduction

A new class of *nonbinary linear codes*, called *matroid* (or M-) *codes*, was proposed in [1]. Matroid codes have the same error-correcting performances as *Reed-Solomon* (R-S) *cyclic codes*, but the *matroid-decoding complexity* is less then for R-S codes. In this paper matroid-coding gain is calculated. Also, the method of generation the optimal structure of multiplier over extended Galois field is presented.

II. Main Part

Matroid (n, k, t) code on m-bit symbols exists for all n and k in relation (1), where t is the symbol-error correcting capability of the code, k is the number of data symbols being encoded, and n is the total number of code symbols in the encoded block. For matroid codes, the code minimum distance is given by (2).

Obviously, the coding gain of real-time communication system is estimated by the ratio of bit energy to noise-power spectral density, E_b/N_o, in decibels. Figure 1 shows a **MATLAB BERTool** plot of bit-error probability (BER) as a function of E_b/N_o for M-codes (17, k, t). The error performance over AWGN channel with PSK modulation improves when symbol error-correcting capability t, increase from t=1 to t=4. Further, as values t increases the error performance decreases. Thus, we can conclude that the optimum code rate is about 0.5 for Gaussian channel.

A procedure (see **Algorithm**) of reducing the multipliers hardware complexity is proposed. The multiplication operation is frequently used in the convolution operation over extended Galois field $\mathbf{GF}(2^m)$. The proposed **Algorithm** generates the optimal scheme of multiplier that contains only XOR gates. Thus, complexity of the multiplier is reduced about 10 times. In figure 2 the schemes of two multipliers over $\mathbf{GF}(2^4)$ with $p(x)=1+x+x^4$, generated by proposed **Algorithm** are shown.

In figure 3 presented is the interface of software that generates the matrix **A**. Having matrix **A**, it is always possible to restore the structure of constant multiplier.

III. Conclusion

A **Simulink**-model of communication system with matroid coding was implemented. An algorithm that generates the optimal scheme for constant multiplier over extended Galois field was analyzed.

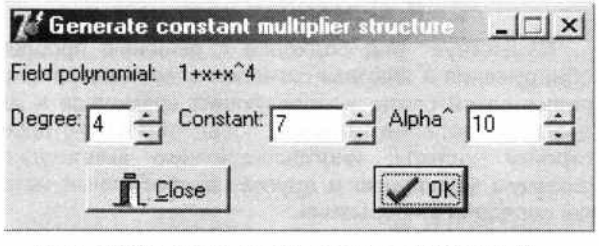

Рис. 3. Интерфейс генератора матрицы **A**.
Fig. 3. Software interface for **A** *matrix generator*