УДК 681.3.06

А. А. КУЗНЕЦОВ, канд. техн. наук

ЭНЕРГЕТИЧЕСКИЙ ВЫИГРЫШ АЛГЕБРОГЕОМЕТРИЧЕСКОГО КОДИРОВАНИЯ

Одним из эффективных средств защиты информации от ошибок, возникающих при передаче по сетям связи, является помехоустойчивое кодирование. Основными требованиями к помехоустойчивому кодированию являются высокая обнаруживающая и исправляющая способность кода, низкая вносимая избыточность, высокое быстродействие и низкая сложность реализации процедур кодирования-декодирования. Недвоичные алгебраические блоковые коды, построенные по алгебраическим кривым (алгеброгеометрические коды), обладают высокой исправляющей способностью при небольшой доле вносимой избыточности [1].

Основная задача помехоустойчивого кодирования информации состоит в повышении энергетической эффективности телекоммуникационных систем. Под энергетической эффективностью систем связи понимают минимально необходимое соотношение сигнал/шум, которое требуется для обеспечения заданной достоверности приема цифровых сообщений. В качестве показателя достоверности используют вероятность ошибочного приема знаков (показатель потери достоверности), которая определяется отношением количества принятых знаков с ошибками к общему количеству переданных знаков за достаточно большой промежуток времени. Снижение минимально необходимого соотношения сигнал/шум при обеспечении заданной вероятности ошибочного приема знаков, которое позволяет получить применяемая система помехоустойчивого кодирования информации, называют энергетическим выигрышем от кодирования.

В статье проводится оценка энергетического выигрыша алгеброгеометрического кодирования информации, сравнение потенциальной помехоустойчивости М-ичных ортогональных сигналов и той помехоустойчивости, которая достигается при использовании алгеброгеометрических кодов.

1 Оценка потенциальной помехоустойчивости М-ичных ортогональных сигналов

Рассмотрим вариант некодированной передачи сообщений М-ичных символов и оценим помехоустойчивость когерентного приема ортогональных сигналов.

Вероятность ошибочного приема символа при когерентном приеме ортогональных сигналов определяется выражением [2-3]:

$$P_c = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} \left[\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u+\sqrt{2\gamma}} e^{-\frac{z^2}{2}} dz \right]^{M-1} du,$$

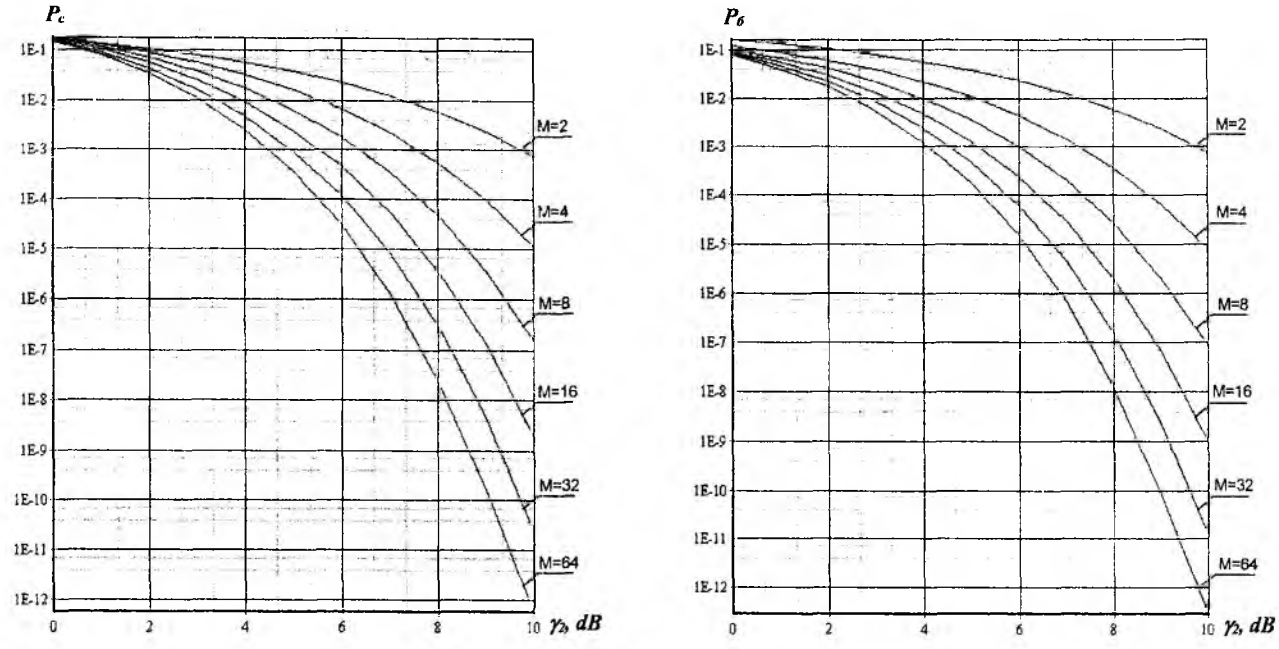
где γ – отношение сигнал/шум для М-ичного символа, $M = 2^m$.

Нормированное отношение сигал/шум на двоичную единицу запишется в виде $\gamma_2 = \gamma / m$.

На рис. 1а представлены зависимости вероятности ошибочного приема М-ичных символов для случаев М=2...64. Средняя вероятность ошибочного приема отдельного бита определяется выражением [3]:

$$P_б = \frac{2^{m-1}}{2^m - 1} P_c.$$

На рис. 1б представлены зависимости средней вероятности ошибочного приема отдельных бит М-ичного символа для случаев М=2...64.



а б

Рис. 1

Зависимости, представленные на рис. 1, свидетельствуют о том, что передача М-ичных ортогональных сигналов позволяет получить значительный выигрыш помехоустойчивости при фиксированном соотношении сигнал/шум или существенный энергетический выигрыш при фиксированной вероятности ошибки символа. При увеличении мощности ансамбля сигналов этот выигрыш возрастает. Целью данной работы является оценка энергетического выигрыша алгеброгеометрического кодирования информации при передаче М-ичных ортогональных сигналов.

2 Алгеброгеометрическое кодирование информации

Зафиксируем конечное поле $GF(q)$. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, $g = g(X)$ – род кривой, $X(GF(q))$ – множество ее точек над конечным полем, $N = |X(GF(q))|$ – их число. Пусть C – класс дивизоров на X степени α. Тогда C задает отображение $\varphi : X \to P^m$, набор генераторных функций $y_i = \varphi(x_i)$ задает алгеброгеометрический код длины $n \le N$. Кодовые характеристики (n, k, d) связаны соотношением $k + d \ge n - g + 1$.

Если $2g - 2 < \alpha \le n$, код связан характеристиками $(n, \alpha - g + 1, d), d \ge n - \alpha$. Дуальный к нему код также является алгеброгеометрическим с характеристиками $(n, n - \alpha + g - 1, d_\perp), d_\perp \ge \alpha - 2g + 2$ [4].

Рассмотрим многообразия, соответствующие проективным гиперповерхностям, заданным в P^n уравнениями $f = 0$, где f – однородные одночлены степени d в P^n. Тогда степень α класса дивизоров C на X определим как $\alpha = (X, f) = \deg X \cdot \deg f$.

Пример. Кривая X, заданная однородным многочленом $xz^2 + y^2 z + x^2 y + x^3 = 0$ над $GF(16)$ дает $N = |X(GF(16))| = 25$ точек, $\deg X = 3$, $g(X) = 1$. Точки кривой приведены в табл. 1.

Таблица 1

	1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***
x	0	1	0	1	1	13	10	2	9	13	4	2	3	10	11
y	1	1	0	0	1	2	3	4	4	4	5	7	7	7	8
z	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1

	16	***17***	***18***	***19***	***20***	***21***	***22***	***23***	***24***	***25***
x	7	5	7	9	6	3	4	5	11	6
y	9	10	10	10	12	13	13	13	14	15
z	1	1	1	1	1	1	1	1	1	1

Пусть $\alpha > g-1$, отображение $\varphi: X \to P^{k-1}$ задает порождающую матрицу G алгебро-геометрического кода с конструктивными характеристиками $(n \le N, k \ge \alpha - g + 1, d \ge n - \alpha)$, число генераторных функций $y_i = f_i(x, y, z)$ соответствует числу информационных кодовых символов k. Конструктивные характеристики кодов для случаев $\deg f = 1...7$ сведены в табл. 2.

Таблица 2

$\deg f$	α	Через G: $(n \le N, k \ge \alpha - g + 1, d \ge n - \alpha)$				
1	3	(25, 3, 22)	(24, 3, 21)	(22, 3, 19)	(20, 3, 17)	(18, 3, 15)
2	6	(25, 6, 19)	(24, 6, 18)	(22, 6, 16)	(20, 6, 14)	(18, 6, 12)
3	9	(25, 9, 16)	(24, 9, 15)	(22, 9, 13)	(20, 9, 11)	(18, 9, 9)
4	12	(25, 12, 13)	(24, 12, 14)	(22, 12, 10)	(20, 12, 8)	(18, 12, 6)
5	15	***(25, 15, 10)***	***(24, 15, 9)***	***(22, 15, 7)***	***(20, 15, 5)***	***(18, 15, 3)***
6	18	(25, 18, 7)	(24, 18, 6)	(22, 18, 4)	–	–
7	21	(25, 21, 4)	(24, 21, 3)	–	–	–

Пусть $\alpha > 2g - 2$, отображение $\varphi: X \to P^{r-1}$ задает проверочную матрицу H алгебро-геометрического кода с конструктивными характеристиками $(n \le N, k \ge n - \alpha + g - 1, d \ge \alpha - 2g + 2)$ число генераторных функций $y_i = f_i(x, y, z)$ соответствует числу проверочных символов кода $r = n - k$. Конструктивные характеристики кодов для случаев $\deg f = 1..7$ сведены в табл. 3.

Таблица 3

$\deg f$	α	Через H: $(n \le N, k \ge n - \alpha + g - 1, d \ge \alpha - 2g + 2)$			
1	3	(25, 22, 3)	(24, 21, 3)	(21, 18, 3)	***(18, 15, 3)***
2	6	(25, 19, 6)	(24, 18, 6)	***(21, 15, 6)***	(22, 12, 6)
3	9	(25, 16, 9)	***(24, 15, 9)***	(21, 12, 9)	(22, 9, 9)
4	12	(25, 13, 12)	(24, 12, 12)	(21, 9, 12)	(22, 6, 12)
5	15	(25, 10, 15)	(24, 9, 15)	(21, 6, 15)	(22, 3, 15)
6	18	(25, 7, 18)	(24, 6, 18)	(21, 3, 18)	–
7	21	(25, 4, 21)	(24, 3, 21)	–	–

В телекоммуникационных системах специального назначения циркулируют короткие формализованные кодограммы (10-15 четырехбитных символа). Для обеспечения высокой помехоустойчивости передаваемых сообщений предлагается применение помехоустойчивых кодов, выделенных в таблицах 2-3 курсивом.

Пример проверочной матрицы H в систематическом виде $H = [P\ I]$ кода (24, 15, 9) для случая $\deg F = 3$, $\alpha = \deg F \cdot \deg f = 9$ над полем $GF(16)$ приведен в табл. 4 (единичная матрица I опущена).

Таблица 4

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	5	6	13	6	13	8	6	10	5	12	1	10	1	7	12
2	5	10	0	12	9	11	3	2	6	13	3	10	10	13	15
3	6	14	1	0	11	8	5	6	14	7	10	3	13	8	1
4	10	5	14	13	6	12	5	15	8	7	0	10	14	5	4
5	1	13	7	4	15	7	8	2	6	3	13	11	0	2	8
6	6	3	15	11	7	4	8	4	15	15	8	13	1	2	9
7	15	10	9	6	14	1	6	6	0	11	7	1	13	6	13
8	11	10	1	5	3	0	2	5	8	2	5	10	7	4	5
9	9	15	5	7	6	14	11	15	6	4	9	7	10	3	14

Проведем оценку энергетического выигрыша предлагаемых кодовых конструкций.

3 Оценка энергетического выигрыша алгеброгеометрических кодов при когерентном приеме 16-х ортогональных сигналов

Рассмотрим код (n,k,d). Полагаем, что ошибки в последовательно передаваемых кодовых символах происходят независимо с вероятностью P_o. Тогда вероятность ошибки кратности i на длине блока n будет

$$P_i = C_n^i P_o^i (1-P_o)^{n-i}.$$

Если декодер исправляет $t=(d-1)/2$ ошибок, то вероятность ошибочного декодирования блока запишется в виде выражения

$$P_{бл} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i (1-P_o)^{n-i}.$$

Если принять предположение о случайном возникновения $2t+1$ и более ошибок в результате ошибочного декодирования кодового слова, то математическое ожидание ошибочных информационных символов на выходе декодера определяется выражением [5]

$$m_{ош} = \sum_{i=t+1}^{n-t} \frac{(i+t)k}{n} P_i + k \sum_{i=n-t+1}^{n} P_i,$$

а вероятность ошибочного декодирования информационного символа –

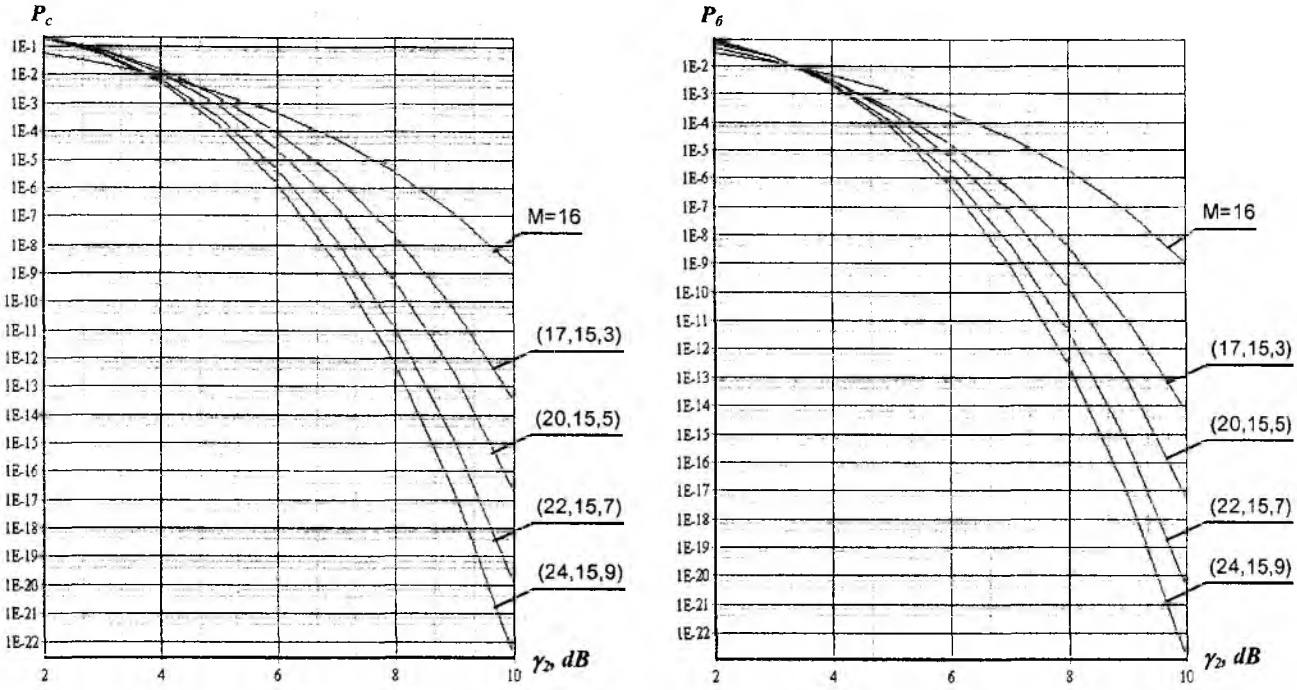
$$P_{оо} = m_{ош} P_{бл}.$$

Использование помехоустойчивого кодирования сопряжено с внесением избыточности в передаваемые данные. Если зафиксировать энергию сообщения, передаваемого в канал связи, то энергия, приходящаяся на один символ, уменьшится пропорционально внесенной избыточности. В выражении для расчета вероятности ошибки символа отношение сигнал/шум γ уменьшится в $R=k/n$ раз.

Зависимости вероятностей ошибок на выходе декодера приведены на рис. 2:

- на рис. 2а представлены зависимости вероятности ошибочного приема 16-ичных символов от нормированного энергетического отношения сигнал/шум, приходящегося на один бит;
- на рис. 2б представлены зависимости средней вероятности ошибочного приема отдельных бит 16-ичных символов от нормированного энергетического отношения сигнал/шум, приходящегося на один бит

Передача символов осуществляется 16-ичными ортогональными сигналами. Зависимость, отмеченная «M=16», соответствует некодированной передаче. На рис.2 приведена также зависимость вероятности ошибки символа при использовании кода Рида-Соломона.



а б

Рис. 2

Как следует из представленных на рис. 2 зависимостей, применение алгеброгеометрических кодов приводит к значительному энергетическому выигрышу. Так, для вероятности ошибочного приема символа 10^{-6} применение кода (24, 15, 9) позволяет получить энергетический выигрыш ≈2,5dB по сравнению с некодированной передачей и ≈0,8dB по сравнению с использованием расширенного кода Рида-Соломона (17, 15, 3). При значении нормированного энергетического отношения сигнал/шум 8dB удается понизить вероятность ошибки более чем на 6 порядков по сравнению с некодированной передачей и на 4 порядка по сравнению с использования кода Рида-Соломона.

Список литературы: 1. *Цфасман М.А.* Коды Гоппы, лежащие выше границы Варшамова – Гилберта. // Проблемы передачи информации. 1982. № 3. С. 3 – 6. 2. *С. Стейн, Дж. Джонс.* Принципы современной теории связи и их применение к передаче дискретных сообщений. М.: Связь, 1971. 376 с. 3. *В.И. Долгов.* Основы статистической теории приема дискретных сигналов. Харьков: ХВВКИУРВ, 1989. 448 с. 4. *Влэдуц С.Г., Манин Ю.И.* Линейные коды и модулярные кривые // Современные проблемы математики. М.: ВИНИТИ, 1984. Т. 25. С. 209 – 257. 5. *Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки.* Теория кодирования. М.: Мир, 1978. 576 с.

Харьковский военный университет

Харьковский национальный

университет радиоэлектроники

Поступила в редколлегию 20.11.2002