УДК 621.394.147

А.А. КУЗНЕЦОВ, д-р техн. наук, Е.П. КОЛОВАНОВА, канд. техн. наук,
Д.И. ПРОКОПОВИЧ-ТКАЧЕНКО, канд. техн. наук, Т.Ю. КУЗНЕЦОВА

АНАЛИЗ И ИССЛЕДОВАНИЕ СВОЙСТВ АЛГЕБРОГЕОМЕТРИЧЕСКИХ КОДОВ

Введение

Алгеброгеометричекие коды как линейные системы на алгебраических кривых впервые были предложены В.Д. Гоппой [1, 2]. Асимптотические свойства таких кодов исследованы в [3]. Коды, построенные по кривым с большим числом точек по сравнению с родом, лежат выше границы Варшамова – Гилберта. Интерес представляют схемы практического применения этих кодов для помехоустойчивой передачи дискретных сообщений, алгоритмы их построения и декодирования, получаемый энергетический выигрыш от кодирования.

Цель данной работы – исследование алгоритмов построения и декодирования алгеброгеометрических кодов, оценка достигаемой энергетической эффективности.

1. Определение и конструктивные свойства алгеброгеометрических кодов

Зафиксируем конечное поле $GF(q)$. Пусть X – гладкая проективная алгебраическая кривая в проективном пространстве P^n, т.е. совокупность решений $p_1(x_0, x_1, ..., x_n)$, $p_2(x_0, x_1, ..., x_n)$, …, $p_N(x_0, x_1, ..., x_n)$, $\forall\ p \in P^n$ системы однородных неприводимых алгебраических уравнений степени d с коэффициентами из $GF(q)$.

Пусть $g = g(X)$ – род кривой, причем, согласно [4]:

– если $d < n$, то X – вырожденная кривая;
– если $d = n$, то X – рациональная нормальная кривая рода 0;
– если $n < d < 2n$, то $g \le d - n$;
– если $d = 2n$, то $g \le n + 1$;
– если $d \ge 2n$, то $g \le \frac{m(m-1)}{2}(n-1) + m\varepsilon$, где $m = \left[\frac{d-1}{n-1}\right]$, $\varepsilon = d - 1 - m(n-1)$.

В табл. 1 приведена верхняя оценки рода g кривой X.

Таблица 1

Верхняя оценка рода g кривой X в P^n

d	$g(P^2)$	$g(P^3)$	$g(P^4)$	$g(P^5)$	$g(P^6)$
2	0	-	-	-	-
3	1	0	-	-	-
4	3	1	0	-	-
5	6	2	1	0	-
6	10	4	2	1	0
7	15	6	3	2	1
8	21	9	5	3	2
9	28	12	7	4	3
10	36	16	9	6	4

Пусть $X(GF(q))$ – множество точек кривой X над конечным полем $GF(q)$, $N = \left|X(GF(q))\right|$ – их число. Число N точек кривой X над $GF(q)$ ограничено сверху выражением Хассе – Вейля [1 – 3]:

$$N \le 2\sqrt{q} \cdot g + q + 1.$$

В табл. 2 приведена верхняя оценка числа точек кривой над конечным полем.

Таблица 2

Оценка верхней границы числа точек гладкой проективной кривой

g	d	$N = \lvert X(GF(q)) \rvert$				
		$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
0	2	5	9	17	33	65
1	3	9	14	25	44	81
2	4	10	18	33	53	97
3	4	17	24	41	66	113
4	5	21	29	49	77	129
5	5		34	57	88	145
6	5		39	65	99	164
7	6		44	73	110	180
8	6		49	81	121	196
9	6		54	89	132	212
10	6		59	97	143	228
11	7		64	105	154	244
12	7		69	113	165	260
13	7			121	176	276
14	7			129	187	292
15	7			137	198	308

Предельные значения числа точек гладких кривых сведены в табл. 3.

Таблица 3

Максимальные значения точек X кривой в P^2 над $GF(q)$

d	$N = \lvert X(GF(q)) \rvert$				
	$GF(4)$	$GF(8)$	$GF(16)$	$GF(32)$	$GF(64)$
3	9	14	25	44	81
4	14	24	34	63	113
5	17	28	65	99	164

Пусть C – класс дивизоров на X степени α. Тогда C задает отображение $\phi: X \to P^m$, набор генераторных функций $y_i = \phi(x_i)$ задает алгеброгеометрический код длины $n \le N$. Кодовые характеристики (n, k, d) связаны соотношением $k + d \ge n - g + 1$ [1, 2]. 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 $(n, n - \alpha + g - 1, d_\perp), d_\perp \ge \alpha - 2g + 2$.

Для оценки потенциальных возможностей блоковых кодов проводят их сравнение с кодовыми границами. Кодовые границы указывают на наилучшие теоретически возможные линейные блоковые коды и подробно описаны в [5 – 8].

Граница Синлгтона указывает на максимально достижимое кодовое расстояние при заданных параметрах (n, k, d) кода и записывается в виде

$$d \le n - k + 1.$$

Коды, лежащие на границе Синлгтона, называют кодами с максимально достижимым кодовым расстоянием (МДР коды).

Граница Варшамова – Гилберта является нижней кодовой границей, т.е. она гарантирует существование кодов с параметрами (n, k, d), лежащими на этой границе. Обобщение границы Варшамова – Гилберта на недвоичные коды имеет вид

$$q^{n-k} \geq \sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i},$$

или

$$n - k \geq \log_q \left(\sum_{i=0}^{d-2} C_{n-1}^{i} (q-1)^{i} \right).$$

Для (n, k, d) кода рассмотрим параметры: $R = k/n$ – относительная скорость кода как доля информационных символов в передаваемых данных; $\delta = d/n$ – относительное минимальное расстояние кода как доля ошибок в принятом слове, которые может обнаружить код. Устремим $n \to \infty$.

Асимптотическая форма границы Синлгтона примет вид

$$R \leq 1 - \delta.$$

Асимптотическая граница Варшамова – Гилберта примет вид

$$R \leq 1 - H_q(\delta).$$

В [3] приведена асимптотическая граница алгеброгеометрических кодов

$$R \leq 1 - \delta - \left(\sqrt{q} - 1\right)^{-1}.$$

На рис. 1 представлены асимптотические границы: 1 – граница Синлгтона; 2 – граница Варшамова – Гилберта; 3 – граница алгеброгеометрических кодов.

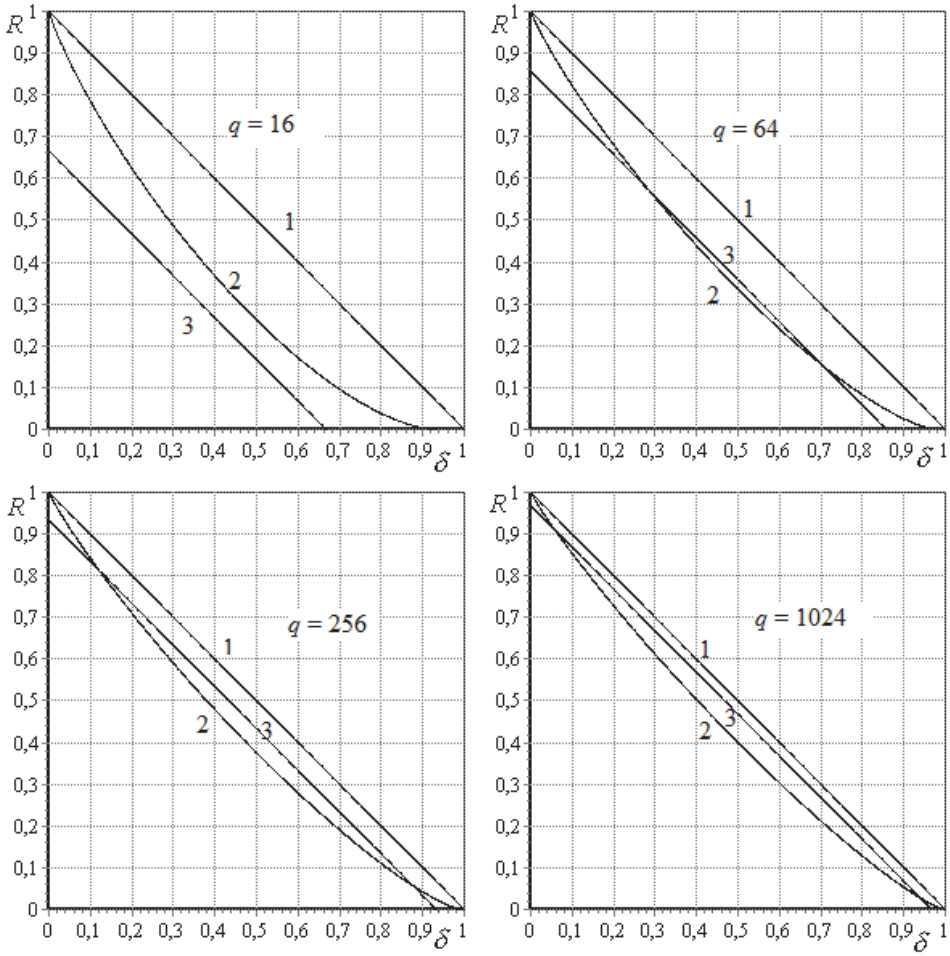

Рис. 1. Асимптотические свойства алгеброгеометрических кодов

Приведенные зависимости свидетельствуют о том, что при возрастании мощности q алфавита кодовых символов асимптотические свойства алгеброгеометрических кодов улучшаются. Очевидно, что при большом q эти коды лежат выше границы Варшамова – Гилберта, что свидетельствует о высоких потенциальных характеристиках.

Конструктивные кодовые характеристики алгеброгеометрических кодов по кривым рода $g=0$, $g=1$, $g=3$, $g=6$ над $GF(4)$ сведены в табл. 4. Соответствующие конструктивные оценки кодовых параметров по кривым различного рода $g=0$, $g=1$, $g=3$, $g=6$ над $GF(8)$, $GF(16)$, $GF(32)$, $GF(64)$ сведены в табл. 5 – 8.

2. Кодирование и декодирование алгеброгеометрическими кодами

Рассмотрим операции кодирования алгеброгеометрическими кодами для общего случая – для кривых, заданных в проективном пространстве P^u совокупностью решений *u – 1* однородных неприводимых алгебраических уравнений от *n* неизвестных, исследуем алгоритмы формирования кодовых слов в систематическом и несистематическом виде.

2.1. Кодирование в несистематическом виде через порождающую матрицу

Зафиксируем гладкую проективную алгебраическую кривую *X* в проективном пространстве P^u над полем $GF(q)$ как это совокупность решений *u – 1* однородных неприводимых алгебраических уравнений от n переменных с коэффициентами из $GF(q)$:

$$\begin{cases} f_1\left(x_0, x_1, ..., x_{u-1}\right) = 0 \\ f_2\left(x_0, x_1, ..., x_{u-1}\right) = 0 \\ ... \\ f_{u-1}\left(x_0, x_1, ..., x_{u-1}\right) = 0 \end{cases}. \tag{1}$$

Пусть $p_0\left(x_0, x_1, ..., x_{u-1}\right)$, $p_1\left(x_0, x_1, ..., x_{u-1}\right)$, …, $p_{N-1}\left(x_0, x_1, ..., x_{u-1}\right) - N$ совместных решений системы уравнений (1) – точек кривой *X*.

Зафиксируем дивизор D кривой X и множество рациональных функций, ассоциированных с дивизором D, т.е. множество, состоящее из нуля и функций $F \neq 0$, для которых $(F) + D \geq 0$. Это эквивалентно набору генераторных функций

$$F_0\left(x_0, x_1, ..., x_{u-1}\right),\ F_1\left(x_0, x_1, ..., x_{u-1}\right),\ F_2\left(x_0, x_1, ..., x_{u-1}\right),\ \ldots,\ F_{w-1}\left(x_0, x_1, ..., x_{u-1}\right),$$

где $F_0, F_1, ..., F_w$ – формы одинаковой степени и $F_0(x_0, x_1, ..., x_{u-1}) \neq 0$.

Иначе говоря,

$$\phi(x) = \left(F_0(x), F_1(x), ..., F_{w-1}(x)\right),$$

как точка в P^w.

Пусть α – степень класса дивизоров, $\alpha > g - 1$, тогда отображение $\phi: X \to P^w$ задает порождающую матрицу

$$G = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_0\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_0\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ F_1\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_1\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_1\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ ... & ... & ... & ... \\ F_{k-1}\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_{k-1}\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_{k-1}\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \end{pmatrix} \tag{2}$$

алгеброгеометрического кода, с конструктивными характеристиками $(n \leq N, k \geq \alpha - g + 1,\ d \geq n - \alpha)$.

Таблица 4

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(4)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	**5, 3, 3**	5, 2, 4	3	9, 3, 6	9, 6, 3	4	14, 2, 10	–	5	–	–
2	4			6	**9, 6, 3**	9, 3, 6	8	14, 6, 6	14, 8, 4	10	17, 5, 7	–
3	6			9			12	14, 10, 2	14, 4, 8	15	17, 10, 2	17, 7, 5

Таблица 5

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(8)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	9, 3, 7	9, 6, 4	3	14, 3, 11	14, 11, 3	4	24, 2, 20	–	5	–	–
2	4	9, 5, 5	9, 4, 6	6	14, 6, 8	14, 8, 6	8	24, 6, 16	24, 18, 4	10	28, 5, 18	–
3	6	**9, 7, 3**	9, 2, 8	9	**14, 9, 5**	14, 5, 9	12	24, 10, 12	**24, 14, 8**	15	28, 10, 13	28, 18, 5
4	8			12	14, 12, 2	14, 2, 12	16	24, 14, 8	24, 10, 12	20	28, 15, 8	28, 13, 10
5	10			15			20	24, 18, 4	24, 6, 16	25	28, 20, 3	28, 8, 15

Таблица 6

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(16)$

$\deg f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	17, 3, 15	17, 14, 4	3	25, 3, 22	25, 22, 3	4	34, 2, 30	–	5	–	–
2	4	17, 5, 13	17, 12, 6	6	25, 6, 19	25, 19, 6	8	34, 6, 26	34, 28, 4	10	65, 5, 55	–
3	6	17, 7, 11	17, 10, 8	9	25, 9, 16	**25, 16, 9**	12	34, 10, 22	34, 24, 8	15	65, 10, 50	65, 55, 5
4	8	17, 9, 9	17, 8, 10	12	25, 12, 13	25, 13, 12	16	34, 14, 18	**34, 20, 12**	20	65, 15, 45	65, 50, 10
5	10	**17, 11, 7**	17, 6, 12	15	25, 15, 10	25, 10, 15	20	34, 18, 14	34, 16, 16	25	65, 20, 40	**65, 45, 15**
6	12	17, 13, 5	17, 4, 14	18	25, 18, 7	25, 7, 18	24	34, 22, 10	34, 12, 20	30	65, 25, 35	65, 40, 20
7	14	17, 15, 3	17, 2, 16	21	25, 21, 4	25, 4, 21	28	34, 26, 6	34, 8, 24	35	65, 30, 30	65, 35, 25
8	16			24			32	34, 30, 2	34, 4, 28	40	65, 35, 25	65, 30, 30
9	18			27			36			45	65, 40, 20	65, 25, 35
10	20			30			40			50	65, 45, 15	65, 20, 40
11	22			33			44			55	65, 50, 10	65, 15, 45

Таблица 7

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(32)$

deg$f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	33, 3, 31	33, 30, 4	3	44, 3, 41	44, 41, 3	4	63, 2, 59	–	5	–	–
2	4	33, 5, 29	33, 28, 6	6	44, 6, 38	44, 38, 6	8	63, 6, 55	63, 57, 4	10	99, 5, 89	–
3	6	33, 7, 27	33, 26, 8	9	44, 9, 35	44, 35, 9	12	63, 10, 51	63, 53, 8	15	99, 10, 84	99, 89, 5
4	8	33, 9, 25	33, 24, 10	12	44, 12, 32	44, 32, 12	16	63, 14, 47	63, 49, 12	20	99, 15, 79	99, 84, 10
5	10	33, 11, 23	33, 22, 12	15	44, 15, 29	**44, 29, 15**	20	63, 18, 43	63, 45, 16	25	99, 20, 74	99, 79, 15
6	12	33, 13, 21	33, 20, 14	18	44, 18, 26	44, 26, 18	24	63, 22, 39	63, 41, 20	30	99, 25, 69	99, 74, 20
7	14	33, 15, 19	33, 18, 16	21	44, 21, 23	44, 23, 21	28	63, 26, 35	63, 37, 24	35	99, 30, 64	99, 69, 25
8	16	33, 17, 17	33, 16, 18	24	44, 24, 20	44, 20, 24	32	63, 30, 31	63, 33, 28	40	99, 35, 59	99, 64, 30
9	18	33, 19, 15	33, 14, 20	27	44, 27, 17	44, 17, 27	36	63, 34, 27	63, 29, 32	45	99, 40, 54	99, 59, 35
10	20	33, 21, 13	33, 12, 22	30	44, 30, 14	44, 14, 30	40	63, 38, 23	63, 25, 36	50	99, 45, 49	99, 54, 40
11	22	**33, 23, 11**	33, 10, 24	33	44, 33, 11	44, 11, 33	44	**63, 42, 19**	63, 21, 40	55	99, 50, 44	99, 49, 45
12	24	33, 25, 9	33, 8, 26	36	44, 36, 8	44, 8, 36	48	63, 46, 15	63, 17, 44	60	99, 55, 39	99, 44, 50
13	26	33, 27, 7	33, 6, 28	39	44, 39, 5	44, 5, 39	52	63, 50, 11	63, 13, 48	65	99, 60, 34	99, 39, 55
14	28	33, 29, 5	33, 4, 30	42	44, 42, 2	44, 2, 42	56	63, 54, 7	63, 9, 52	70	**99, 65, 29**	99, 34, 60
15	30	33, 31, 3	33, 2, 32	45			60	63, 58, 3	63, 5, 56	75	99, 70, 24	99, 29, 65
16	32			48			64		63, 1, 60	80	99, 75, 19	99, 24, 70
17	34			51			68			85	99, 80, 14	99, 19, 75
18	36			54			72			90	99, 85, 9	99, 14, 80
19	38			57			76			95	99, 90, 4	99, 9, 85
20	40			60			80			100		99, 4, 90

Таблица 8

Конструктивные кодовые характеристики алгеброгеометрических кодов над $GF(64)$

deg$f$	$\deg X = 2,\ g = 0$			$\deg X = 3,\ g = 1$			$\deg X = 4,\ g = 3$			$\deg X = 5,\ g = 6$		
	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d	a	n,k,d	n,k,d
1	2	65, 3, 63	65, 62, 4	3	81, 3, 78	81, 78, 3	4	113, 2, 109	–	5	–	–
2	4	65, 5, 61	65, 60, 6	6	81, 6, 75	81, 75, 6	8	113, 6, 105	113, 107, 4	10	164, 5, 154	–
3	6	65, 7, 59	65, 58, 8	9	81, 9, 72	81, 72, 9	12	113, 10, 101	113, 103, 8	15	164, 10, 149	164, 154, 5
4	8	65, 9, 57	65, 56, 10	12	81, 12, 69	81, 69, 12	16	113, 14, 97	113, 99, 12	20	164, 15, 144	164, 149, 10
5	10	65, 11, 55	65, 54, 12	15	81, 15, 66	81, 66, 15	20	113, 18, 93	113, 95, 16	25	164, 20, 139	164, 144, 15

6	12	65, 13, 53	65, 52, 14	18	81, 18, 63	81, 63, 18	24	113, 22, 89	113, 91, 20	30	164, 25, 134	164, 139, 20
7	14	65, 15, 51	65, 50, 16	21	81, 21, 60	81, 60, 21	28	113, 26, 85	113, 87, 24	35	164, 30, 129	164, 134, 25
8	16	65, 17, 49	65, 48, 18	24	81, 24, 57	81, 57, 24	32	113, 30, 81	113, 83, 28	40	164, 35, 124	164, 129, 30
9	18	65, 19, 47	65, 46, 20	27	81, 27, 54	**81, 54, 27**	36	113, 34, 77	113, 79, 32	45	164, 40, 119	164, 124, 35
10	20	65, 21, 45	65, 44, 22	30	81, 30, 51	81, 51, 30	40	113, 38, 73	113, 75, 36	50	164, 45, 114	164, 119, 40
11	22	65, 23, 43	65, 42, 24	33	81, 33, 48	81, 48, 33	44	113, 42, 69	113, 71, 40	55	164, 50, 109	164, 114, 45
12	24	65, 25, 41	65, 40, 26	36	81, 36, 45	81, 45, 36	48	113, 46, 65	113, 67, 44	60	164, 55, 104	164, 109, 50
13	26	65, 27, 39	65, 38, 28	39	81, 39, 42	81, 42, 39	52	113, 50, 61	113, 63, 48	65	164, 60, 99	164, 104, 55
14	28	65, 29, 37	65, 36, 30	42	81, 42, 39	81, 39, 42	56	113, 54, 57	113, 59, 52	70	164, 65, 94	164, 99, 60
15	30	65, 31, 35	65, 34, 32	45	81, 45, 36	81, 36, 45	60	113, 58, 53	113, 55, 56	75	164, 70, 89	164, 94, 65
16	32	65, 33, 33	65, 32, 34	48	81, 48, 33	81, 33, 48	64	113, 62, 49	113, 51, 60	80	164, 75, 84	164, 89, 70
17	34	65, 35, 31	65, 30, 36	51	81, 51, 30	81, 30, 51	68	113, 66, 45	113, 47, 64	85	164, 80, 79	164, 84, 75
18	36	65, 37, 29	65, 28, 38	54	81, 54, 27	81, 27, 54	72	113, 70, 41	113, 43, 68	90	164, 85, 74	164, 79, 80
19	38	65, 39, 27	65, 26, 40	57	81, 57, 24	81, 24, 57	76	**113, 74, 37**	113, 39, 72	95	164, 90, 69	164, 74, 85
20	40	65, 41, 25	65, 24, 42	60	81, 60, 21	81, 21, 60	80	113, 78, 33	113, 35, 76	100	164, 95, 64	164, 69, 90
21	42	**65, 43, 23**	65, 22, 44	63	81, 63, 18	81, 18, 63	84	113, 82, 29	113, 31, 80	105	164, 100, 59	164, 64, 95
22	44	65, 45, 21	65, 20, 46	66	81, 66, 15	81, 15, 66	88	113, 86, 25	113, 27, 84	110	164, 105, 54	164, 59, 100
23	46	65, 47, 19	65, 18, 48	69	81, 69, 12	81, 12, 69	92	113, 90, 21	113, 23, 88	115	**164, 110, 49**	164, 54, 105
24	48	65, 49, 17	65, 16, 50	72	81, 72, 9	81, 9, 72	96	113, 94, 17	113, 19, 92	120	164, 115, 44	164, 49, 110
25	50	65, 51, 15	65, 14, 52	75	81, 75, 6	81, 6, 75	100	113, 98, 13	113, 15, 96	125	164, 120, 39	164, 44, 115
26	52	65, 53, 13	65, 12, 54	78	81, 78, 3	81, 3, 78	104	113, 102, 9	113, 11, 100	130	164, 125, 34	164, 39, 120
27	54	65, 55, 11	65, 10, 56	81			108	113, 106, 5	113, 7, 104	135	164, 130, 29	164, 34, 125
28	56	65, 57, 9	65, 8, 58	84			112	113, 110, 1	113, 3, 108	140	164, 135, 24	164, 29, 130
29	58	65, 59, 7	65, 6, 60	87			116			145	164, 140, 19	164, 24, 135
30	60	65, 61, 5	65, 4, 62	90			120			150	164, 145, 14	164, 19, 140
31	62	65, 63, 3	65, 2, 64	93			123			155	164, 150, 9	164, 14, 145
32										160	164, 155, 4	164, 9, 150

Алгеброгеометрический код на кривой X над $GF(q)$, построенный через порождающую матрицу G, – это линейный код, все кодовые слова ($c_0, c_1, ..., c_{n-1}$) которого задаются равенством

$$\sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right) = c_j\ ,\ \ j = 0, ..., n-1\,.$$

Для формирования кодового слова $\left(c_0, c_1, ...c_{n-1}\right)$ алгеброгеометрического кода, заданного через порождающую матрицу, достаточно умножить информационный вектор $\left(I_0, I_1, ...I_{k-1}\right)$ на матрицу (2), т.е. для всех $j = 0, ..., n-1$ выполнить следующее преобразование:

$$c_j = \sum_{i=0}^{k-1} I_i F_i\left(p_j\left(x_0, x_1, ..., x_{u-1}\right)\right). \tag{3}$$

Очевидно, что формирование кодового слова осуществляется итеративной процедурой, позволяющей на каждом шаге работы алгоритма формировать соответствующий кодовый символ.

2.2. Кодирование в систематическом виде через проверочную матрицу

Пусть $\alpha > 2g - 2$, тогда отображение $\phi : X \to P^w$ задает проверочную матрицу

$$H = \begin{pmatrix} F_0\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_0\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_0\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ F_1\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_1\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_1\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \\ ... & ... & ... & ... \\ F_{n-k-1}\left(p_0\left(x_0, x_1, ..., x_{u-1}\right)\right) & F_{n-k-1}\left(p_1\left(x_0, x_1, ..., x_{u-1}\right)\right) & ... & F_{n-k-1}\left(p_{n-1}\left(x_0, x_1, ..., x_{u-1}\right)\right) \end{pmatrix} \tag{4}$$

алгеброгеометрического кода, с конструктивными характеристиками

$$\left(n \le N, k \ge n - \alpha + g - 1,\ d \ge \alpha - 2g + 2\right).$$

Алгеброгеометрический код по кривой X над $GF(q)$, построенный через проверочную матрицу H, – это линейный код, состоящий из всех слов $(c_0, c_1, ..., c_{n-1})$ длины $n \le N$, для которых выполняется равенство $d + g - 1$ уравнений

$$\sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = 0\ ,\ \ j = 0, ..., w\,. \tag{5}$$

Для формирования кодовых слов заданного таким образом алгеброгеометрического кода на пространственных кривых воспользуемся приемами обращения матриц.

Разобьем кодовое слово $\left(c_0, c_1, ...c_{n-1}\right)$ на множества информационных и проверочных позиций (см. рис. 2).

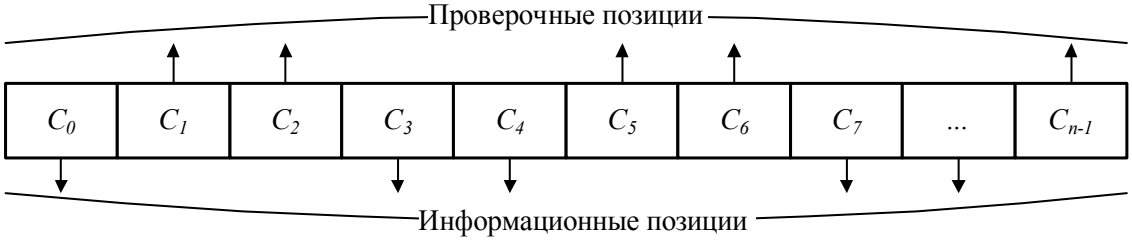

Рис. 2. Разбиение кодового слова на информационные и проверочные позиции

Пусть U – множество k информационных позиций кодового слова (т.е. множество номеров позиций, входящих в заданный информационный набор кода) и W – множество $r = n - k$ проверочных позиций. Объединение множеств $U \cup W$ содержит все целые числа (номера) от 0 до $n - 1$.

На k информационных позициях кодового слова, т.е. на позициях множества U, разместим k символов сообщения $\left(I_0, I_1, ...I_{k-1}\right)$, а на проверочных позициях множества W разместим r нулевых символов.

Вычислим суммы

$$S_j = \sum_{i=0}^{n-1} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right),\ j = \overline{0, r-1},$$

или в матричной форме

$$\left\|S_j\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r} \left\|c_i\right\|_k^T. \tag{6}$$

Задача формирования кодового слова состоит в том, чтобы вычислить и записать на r проверочных позициях такие символы c_i, $i \in W$, которые удовлетворяют уравнениям (5).

Из определения алгеброгеометрического кода следует, что значения $r=n-k$ проверочных символов могут быть найдены из системы линейных уравнений

$$\sum_{i \in W} c_i F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right) = -S_j,\ j = \overline{0, r-1}.$$

В матричном представлении последняя запись эквивалентна выражению

$$\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r} \left\|c_i\right\|_r^T = \left\|-S_j\right\|_r.$$

Для нахождения значений $r = n - k$ проверочных символов, используя методы обращения матриц, запишем

$$\left\|c_i\right\|_r = \left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1} \left\|-S_j\right\|_r^T, \tag{7}$$

где $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ – матрица, обратная матрице $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$, т.е.

$$\left\|\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right\|_{r,r}^{-1} = \left\|\frac{A\left[\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]}{\Delta_{\left\|F_j\right\|_{r,r}}}\right\|_{r,r},$$

где $A\left[\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}\right]$ – алгебраическое дополнение элемента $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$; $\Delta_{\left\|F_j\right\|_{r,r}}$ – определитель матрицы $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}$.

Поскольку размещение проверочных позиций обычно известно и фиксировано, то заранее можно найти обратную матрицу для системы уравнений (5) и получить все проверочные символы умножением вектора $\left(S_0, S_1, ...S_{r-1}\right)$ на матрицу $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$.

В качестве информационных могут быть выбраны любые k позиций кодового слова. Следовательно, всегда можно выбрать такое множество проверочных (и информационных) позиций, для которого матрица $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ наиболее удобна для вычислений.

Таким образом, для формирования кодового слова алгеброгеометрического кода, заданного через проверочную матрицу, достаточно хранить элементы матриц $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ и $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{r,r}^{-1}$ либо поочередно вычислять $\left\|F_j\left(p_i\left(x_0, x_1, ..., x_{u-1}\right)\right)\right\|_{k,r}$ как значения генераторных функций в точках пространственной кривой.

2.3. Декодирование алгеброгеометрических кодов

Рассмотрим кодовое слово алгеброгеометрического *(n, k, d)* кода над *GF(q)*, построенного по алгебраическим кривым в P^u. Предположим, что алгеброгеометрический код задан через проверочную матрицу:

$$H = \begin{pmatrix} F_{0,0,\ldots,0}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \\ F_{1,0,\ldots,0}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \\ \\ F_{0,0,\ldots,\deg F}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) \end{pmatrix},$$

где $F_{i_0,i_1,\ldots,i_{u-1}}$ – одночлен степени $i_0 + i_1 + \ldots + i_{u-1} \le \deg F$, т.е.

$$F_{i_0,i_1,\ldots,i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}},\ i = 0, \ldots, M-1; \quad M = C_{u+\deg F}^{u} - 1.$$

Справедливо равенство $C \cdot H^T = 0$, откуда следует

$$\sum_{j=0}^{n-1} C_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = 0,$$

для всех $i = 0, \ldots, M-1$.

Предположим, что при передаче по каналу с ошибками кодовое слово исказилось, вектор ошибок обозначим в виде

$$e = (e_0, e_1, \ldots, e_{n-1}),$$

а принятое с ошибками слово в виде

$$C^* = (C^*_0, C^*_1, \ldots, C^*_{n-1}) = C + e = (C_0 + e_0, C_1 + e_1, \ldots, C_{n-1} + e_{n-1}).$$

Определим синдромную последовательность как вектор

$$s = \left(s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F}\right),$$

вычисленный по правилу

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right),\ i = 0, \ldots, M-1.$$

По определению значение синдромной последовательности *s* зависит только от вектора ошибок *e* и не зависит от кодового слова *C*. Действительно, вычислим произведение

$$C^* \cdot H^T = 0,$$

получим

$$(C + e) \cdot H^T = C \cdot H^T + e \cdot H^T = e \cdot H^T,$$

откуда следует справедливость $i = 0, \ldots, M-1$ равенств:

$$\sum_{j=0}^{n-1} (c_j + e_j) \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}}\left(p_j\left(x_0, x_1, \ldots, x_{u-1}\right)\right) = s_{i_0,i_1,\ldots,i_{u-1}}. \quad (8)$$

Задача алгебраического декодирования состоит в нахождении вектора

$$e = (e_0, e_1, \ldots, e_{n-1})$$

по известной синдромной последовательности

$$s = \left(s_{0,0,\ldots,0}, s_{1,0,\ldots,0}, \ldots, s_{0,0,\ldots,\deg F}\right).$$

Нахождение вектора *e* позволяет, в свою очередь, восстановить кодовое слово *C* по известной последовательности C^*:

$$C = C^* - e = (C_0^* - e_0, C_1^* - e_1, ..., C_{n-1}^* - e_{n-1}).$$

Решение поставленной задачи сопряжено с нахождением *n* неизвестных в системе из M линейных уравнений, причем $M < n$. Строго говоря, при решении поставленной задачи методами линейной алгебры в общем случае существует множество решений обозначенной системы уравнений. В то же время следует отметить, что только

$$v \le t = \left\lfloor \frac{(d-1)}{2} \right\rfloor$$

значений последовательности

$$(e_0, e_1, \ldots, e_{n-1})$$

не равны нулю, т.е. почти все $e_j = 0$, за исключением некоторого (конечного) их числа (*v*). С учетом этого ограничения существует одно (единственное) решение совокупности уравнений (8).

Обозначим множество $e_j \neq 0$ символом *E*. Для однозначного нахождения вектора ошибок воспользуемся искусственным приемом, состоящем во введении многочлена локаторов ошибок:

$$\begin{aligned}\Lambda(x_0, x_1, ..., x_{u-1}) = x_0^{v-u+1} + a_{v-u,1,...,0} \cdot x_0^{v-u} \cdot x_1 + ... + \\ + a_{1,0,...,0} \cdot x_0 + a_{0,1,...,0} \cdot x_1 + ... + a_{0,0,...,1} \cdot x_{u-1} + a_{0,0,...,0},\end{aligned} \tag{9}$$

решениями которого являются локаторы – такие наборы $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, которые обращают в нуль многочлен (9), причем соответствующие элементы вектора ошибок $e_\xi \in E$.

Многочлен (9) однозначно задает расположение ошибок в векторе

$$e = (e_0, e_1, \ldots, e_{n-1}),$$

так как однозначно указывает на его ненулевые компоненты. Другими словами, нахождение коэффициентов $a_{i_0, i_1, ..., i_{u-1}}$ многочлена локаторов ошибок $\Lambda(x_0, x_1, ..., x_{u-1})$ позволяет однозначно указать расположение возникших при передаче кодового слова ошибок (но не их значения – истинные значения ненулевых величин e_j), например путем поочередной подстановки всех наборов $p_j(x_0, x_1, ..., x_{u-1}) = (X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ в многочлен $\Lambda(x_0, x_1, ..., x_{u-1})$ и проверке на его равенство нулю.

Умножим многочлен (9) на e_j и вычислим в точке $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, получим:

$$\begin{aligned}e_j \cdot X_{0_j}^{v-u+1} + a_{v-u,1,...,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + ... + \\ + a_{1,0,...,0} \cdot e_j \cdot X_{0_j} + a_{0,1,...,0} \cdot e_j \cdot X_{1_j} + ... + a_{0,0,...,1} \cdot e_j \cdot X_{u-1_j} + a_{0,0,...,0} \cdot e_j.\end{aligned} \tag{10}$$

Проанализируем полученное выражение.

Если $e_j \notin E$, т.е. $e_j = 0$, тогда все слагаемые полученного многочлена равны нулю, т.е. имеем равенство нулю всего выражения (10).

Если $e_j \in E$, т.е. $e_j \neq 0$, тогда соответствующие наборы $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ обращают в нуль многочлен (9) и, соответственно, многочлен (10).

Таким образом, при любом значении e_j имеем равенство нулю выражения (10).

Просуммируем по всем *j = 0,...,n-1*, получим:

$$\sum_{j=0}^{n-1} e_j \cdot X_{0_j}^{v-u+1} + \sum_{j=0}^{n-1} a_{v-u,1,\ldots,0} \cdot e_j \cdot X_{0_j}^{v-u} \cdot X_{1_j} + \ldots +$$
$$+ \sum_{j=0}^{n-1} a_{1,0,\ldots,0} \cdot e_j \cdot X_{0_j} + \sum_{j=0}^{n-1} a_{0,1,\ldots,0} \cdot e_j \cdot X_{1_j} + \ldots + \quad (11)$$
$$+ \sum_{j=0}^{n-1} a_{0,0,\ldots,1} \cdot e_j \cdot X_{u-1_j} + \sum_{j=0}^{n-1} a_{0,0,\ldots,0} \cdot e_j .$$

Проанализируем полученное выражение. Значения $a_{i_0,i_1,\ldots,i_{u-1}}$ не зависят от j, вынесем их за знак суммирования. С учетом введенных выше обозначений, значение одночлена

$$F_{i_0,i_1,\ldots,i_{u-1}} = x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$$

в точке $(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j})$ примет вид

$$F_{i_0,i_1,\ldots,i_{u-1}}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) = X_{0_j}^{i_0} \cdot X_{1_j}^{i_1} \cdot \ldots \cdot X_{u-1_j}^{i_{u-1}} .$$

С учетом последнего выражение (11) перепишется в виде:

$$\sum_{j=0}^{n-1} e_j \cdot F_{v-u+1,0,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{v-u,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{v-u,1,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + \ldots +$$
$$+ a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{1,0,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{0,1,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,1,\ldots,0}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + \ldots +$$
$$+ a_{0,0,\ldots,1} \sum_{j=0}^{n-1} \cdot e_j \cdot F_{0,0,\ldots,1}(X_{0_j}, X_{1_j}, \ldots, X_{u-1_j}) + a_{1,0,\ldots,0} \sum_{j=0}^{n-1} \cdot e_j = 0.$$

Но по введенному выше определению

$$s_{i_0,i_1,\ldots,i_{u-1}} = \sum_{j=0}^{n-1} e_j \cdot F_{i_0,i_1,\ldots,i_{u-1}} \left(p_j \left(x_0, x_1, \ldots, x_{u-1} \right) \right).$$

Следовательно, имеем:

$$s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots +$$
$$+ a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0.$$

Вернемся теперь к рассмотрению многочлена (9). Умножим его на произвольный одночлен $x_0^{i_0} \cdot x_1^{i_1} \cdot \ldots \cdot x_{u-1}^{i_{u-1}}$ и проведем аналогичные рассуждения. По аналогии с (10) сохранится равенство нулю при любом значении e_j. После суммирования по всем $j = 0,\ldots,n-1$ и выполнения очевидных подстановок получим рекуррентную формулу:

$$s_{i_0+v-u+1,i_1,\ldots,i_{u-1}} + a_{v-u,1,\ldots,0} \cdot s_{i_0+v-u,i_1+1,\ldots,i_{u-1}} + \ldots +$$
$$+ a_{1,0,\ldots,0} \cdot s_{i_0+1,i_1,\ldots,i_{u-1}} + a_{0,1,\ldots,0} \cdot s_{i_0,i_1+1,\ldots,i_{u-1}} + \ldots +$$
$$+ a_{0,0,\ldots,1} \cdot s_{i_0,i_1,\ldots,i_{u-1}+1} + a_{0,0,\ldots,0} \cdot s_{i_0,i_1,\ldots,i_{u-1}} = 0.$$

Выполнив соответствующие преобразования для всех $i = 0,\ldots,M-1$ получим систему линейных уравнений:

$$\begin{cases} s_{v-u+1,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{1,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{0,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{0,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{0,0,\ldots,0} = 0; \\ \\ s_{v-u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{1,0,\ldots,0} = 0; \\ \ldots \\ s_{2v-2u+2,0,\ldots,0} + a_{v-u,1,\ldots,0} \cdot s_{2v-2u+1,1,\ldots,0} + \ldots + \\ + a_{1,0,\ldots,0} \cdot s_{v-u+2,0,\ldots,0} + a_{0,1,\ldots,0} \cdot s_{v-u+1,1,\ldots,0} + \ldots + \\ + a_{0,0,\ldots,1} \cdot s_{v-u+1,0,\ldots,1} + a_{0,0,\ldots,0} \cdot s_{v-u+1,0,\ldots,0} = 0. \end{cases} \quad (12)$$

При числе неизвестных z в многочлене локаторов ошибок, меньшем числа элементов синдромной последовательности, система линейных уравнений (12) разрешима. Сложность ее решения, например методом Гаусса, составит z^2.

Решения системы (12) дают значения неизвестных коэффициентов многочлена локаторов ошибок $\Lambda(x_0, x_1, ..., x_{u-1})$ (9), который, в свою очередь, однозначно задает значения локаторов – таких наборов $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, которые обращают в нуль многочлен (9), причем соответствующие элементы $e_i \in E$.

Поиск искомых $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ может быть выполнен, например, поочередной подстановкой всех $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$, $j = 0,...,n-1$ в многочлен $\Lambda(x_0, x_1, ..., x_{u-1})$ и проверкой на равенство нулю.

Найденные $(X_{0_j}, X_{1_j}, ..., X_{u-1_j})$ локализуют ошибку в кодовом слове, т.е. приравняют нулю $n - v$ неизвестных в системе (8). Так как число оставшихся неизвестных $v < M$, система (8) разрешима. Сложность ее решения, например методом Гаусса, не превосходит v^2. Решение системы (8) дает искомые (ненулевые) значения вектора ошибок $e = (e_0, e_1, ..., e_{n-1})$, т.е. задача декодирования решена.

3. Энергетическая эффективность алгеброгеометрического кодирования

Для оценки энергетической эффективности алгеброгеометрического кодирования рассмотрим вариант передачи дискретных сообщений М-ми ортогональными сигналами.

При некодированной передаче сообщений вероятность ошибочного приема М-х символов при когерентном приеме ортогональных сигналов определяется выражением [5]:

$$P_c = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} \left[\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u+\sqrt{2\gamma}} e^{-\frac{z^2}{2}} dz \right]^{M-1} du, \quad (13)$$

где γ – отношение сигнал/шум для М-го символа, $M = 2^m$; γ_2 – нормированное отношение сигнал/шум на двоичную единицу, $\gamma_2 = \gamma / m$.

На рис. 3 представлены зависимости вероятности ошибочного приема М-го символа при когерентном приеме ортогональных сигналов.

Передача М-х 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.

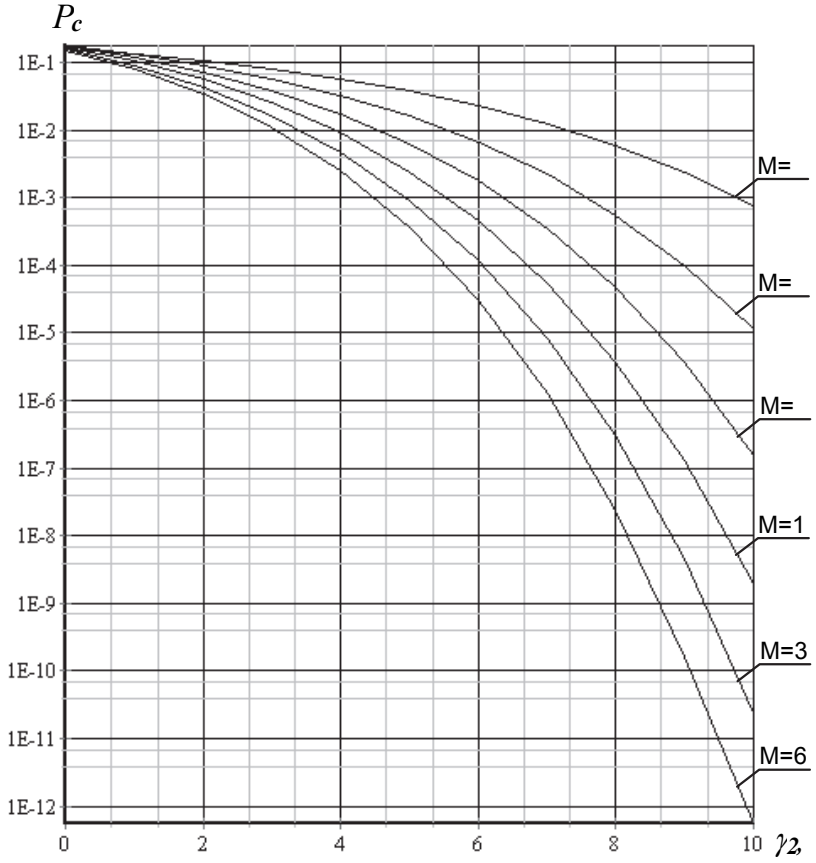

Рис. 3. Зависимости вероятности ошибочного приема М-х символов
от нормированного энергетического отношения сигнал/шум, приходящегося на один бит

Пусть задан 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

$$P_i = C_n^i P_o^i \left(1-P_o\right)^{n-i}. \tag{14}$$

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

$$P_{бл} = \sum_{i=t+1}^{n} P_i = \sum_{i=t+1}^{n} C_n^i P_o^i \left(1-P_o\right)^{n-i}. \tag{15}$$

Если принять предположение о случайном возникновении $2t+1$ и более ошибок в результате ошибочного декодирования кодового слова, то математическое ожидание ошибочных информационных символов на выходе декодера определяется выражением [6]

$$m_{ош} = \sum_{i=t+1}^{n-t} \frac{(i+t)k}{n} P_i + k \sum_{i=n-t+1}^{n} P_i, \tag{16}$$

а вероятность ошибочного декодирования информационного символа

$$P_{од} = m_{ош} P_{бл}. \tag{17}$$

Применение кодов, обнаруживающих и исправляющих ошибки, приводит к увеличению избыточности передаваемых данных. Если зафиксировать энергию сообщения, передаваемо-

го в канал, то энергия, приходящаяся на один символ, уменьшится пропорционально внесенной избыточности. Для расчета зависимостей вероятности ошибки на символ на выходе декодера (14) – (17) с учетом внесенной избыточности отношение сигнал/шум γ в выражении (13) уменьшим в $R = k/n$ раз.

Рассмотрим вариант передачи дискретных сообщений 4-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(4)$ (выбранные параметры кода выделены в табл. 4). На рис. 4 представлены зависимости вероятности ошибки 4-го символа от нормированного соотношения сигнал/шум при когерентном приеме 4-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=4», соответствует некодированной передачи. Зависимость, отмеченная как (5, 3, 3), соответствует алгеброгеометрическому коду по кривой рода $g = 0$, кодовые характеристики которого лежат на границе Синлгтона. Это код с максимально достижимым кодовым расстоянием (МДР код) – расширенный код Рида – Соломона. Наибольший энергетический выигрыш алгеброгеометрические коды (в том числе МДР коды) дают при скоростях $R \approx 2/3$.

Зависимости, представленные на рис. 4, свидетельствуют о преимуществах использования алгеброгеометрических кодов для помехоустойчивой передачи сообщений. Так, при значении вероятности ошибки на символ $P_c = 10^{-5}$ применение кода (9,6,3) дает энергетический выигрыш ≈0,6dB по сравнению с некодированной передачей сообщений и ≈0,2dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 8-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(8)$. Конструктивные кодовые характеристики выбранных кодов выделены в табл. 5. На рис. 5 представлены зависимости вероятности ошибки 8-го символа от нормированного соотношения сигнал/шум при когерентном приеме 8-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=8», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-6}$ применение кода (23,14,7) дает энергетический выигрыш ≈2dB по сравнению с некодированной передачей сообщений и ≈0,8dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 16-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(16)$. Конструктивные кодовые характеристики выбранных для оценки кодов выделены в табл. 6. На рис. 6 представлены зависимости вероятности ошибки 16-го символа от нормированного соотношения сигнал/шум при когерентном приеме 16-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=16», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-6}$ применение кода (65,45,15) дает энергетический выигрыш ≈3dB по сравнению с некодированной передачей сообщений и ≈1dB по сравнению с МДР кодом.

Рассмотрим вариант передачи дискретных сообщений 32-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(32)$. Выбранные кодовые характеристики выделены в табл. 7. На рис. 7 представлены зависимости вероятности ошибки 32-го символа от нормированного соотношения сигнал/шум при когерентном приеме 32-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=32», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-9}$ применение кода (99,65,29) дает энергетический выигрыш ≈4,5dB по сравнению с некодированной передачей сообщений и ≈1dB по сравнению с МДР кодом.

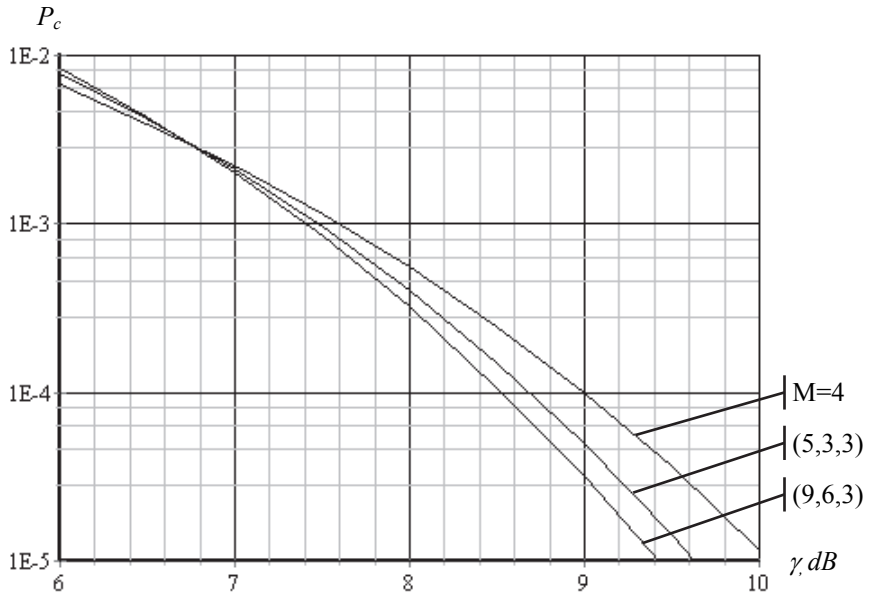

Рис. 4. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 4-х ортогональных сигналов

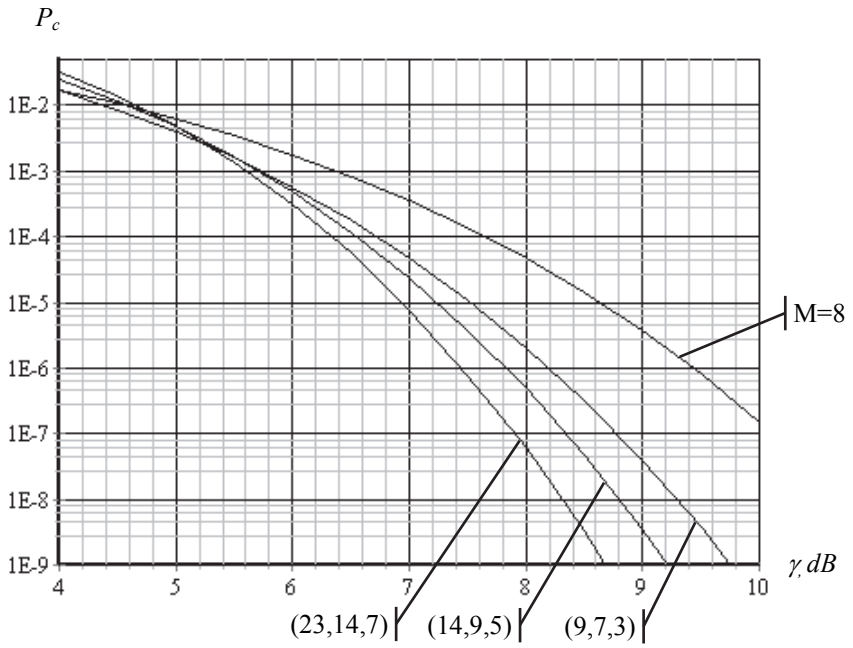

Рис. 5. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 8-х ортогональных сигналов

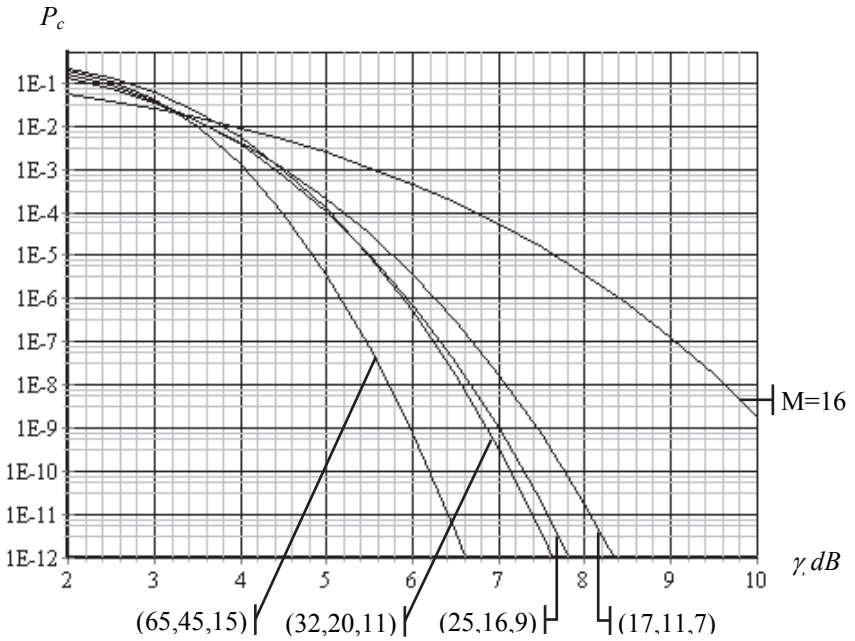

Рис. 6. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 16-х ортогональных сигналов

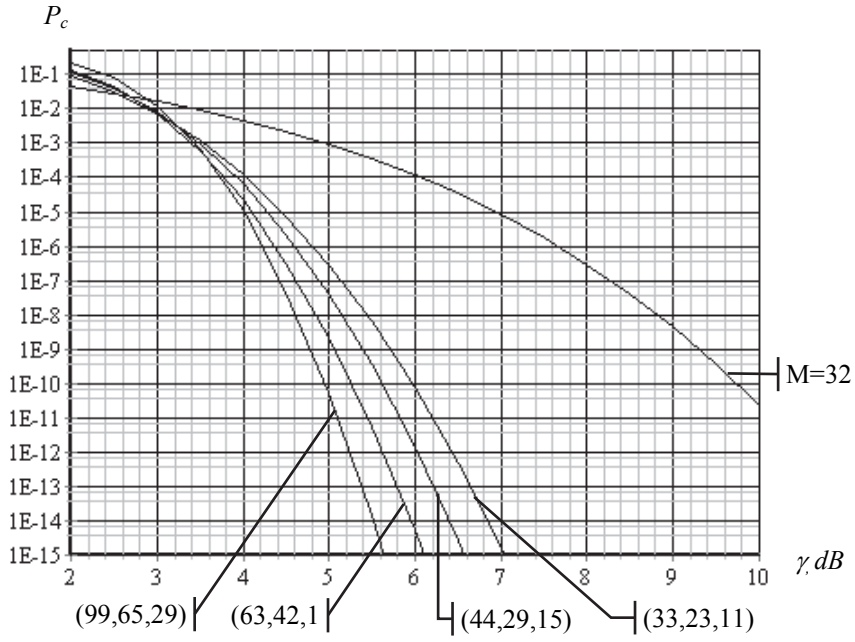

Рис. 7. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 32-х ортогональных сигналов

Рассмотрим вариант передачи дискретных сообщений 64-ми ортогональными сигналами. Передаваемые сообщения закодируем алгеброгеометрическим кодом, построенным над полем $GF(64)$ с параметрами, выделенными в табл. 8. На рис. 8 представлены зависимости вероятности ошибки 64-го символа от нормированного соотношения сигнал/шум при когерентном приеме 64-х ортогональных сигналов с использованием помехоустойчивых алгеброгеометрических кодов. Зависимость, отмеченная как «M=64», соответствует некодированной передаче. При значении вероятности ошибки на символ $P_c = 10^{-12}$ применение кода (164,110,49) дает энергетический выигрыш ≈6dB по сравнению с некодированной передачей сообщений и ≈0,8dB по сравнению с МДР кодом.

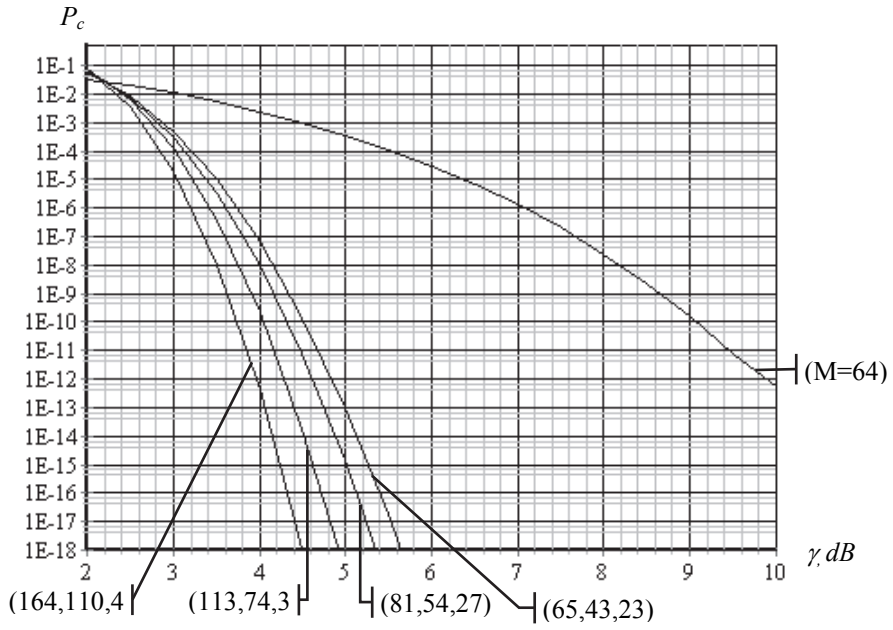

Рис. 8. Энергетическая эффективность алгеброгеометрических кодов при когерентном приеме 64-х ортогональных сигналов

Как следует из представленных на рис. 4 – 8 зависимостей, применение алгеброгеометрических кодов для повышения помехоустойчивости передачи сообщений в дискретных каналах без памяти приводит к значительному энергетическому выигрышу. Их использование позволяет существенно снизить вероятность ошибки на символ при фиксированном соотношении сигнал/шум, приходящемся на один передаваемый бит. Энергетический выигрыш возрастает при переходе к кодам, построенным по кривым с большим числом точек по отношению к роду кривой.

Сравним сложность реализации процедур кодирования-декодирования для рассмотренных кодов с известными схемами. Оценку сложности процедур кодирования-декодирования (так же, как и оценку энергетического выигрыша алгеброгеометрического кодирования) проведем в сравнении с кодами Рида – Соломона.

Если код задан порождающей матрицей G, то процедура систематического кодирования эквивалентна умножению информационного слова i на эту матрицу: $c = iG$, где c – кодовое слово. Сложность алгоритмов систематического кодирования алгеброгеометрических кодов и кодов Рида – Соломона в этом смысле практически равноценна.

Коды Рида – Соломона – подкласс кодов БЧХ, к их декодированию применимы те же методы, что и для кодов БЧХ. Одним из наиболее эффективных алгоритмов алгебраического декодирования кодов БЧХ является алгоритм Берлекэмпа – Месси и его модификации (улучшения). Известно [7], что алгоритм Берлекэмпа – Месси содержит число умножений, порядка t^2, или, формально, сложность алгоритма $O(t^2)$. Для большого t используют ускоренный алгоритм Берлекэмпа – Месси, позволяющий уменьшить вычислительную сложность алгоритма. Еще более эффективным, с точки зрения вычислительной сложности, является рекуррентный алгоритм Берлекэмпа – Месси. Асимптотическая сложность декодирования кодов Рида – Соломона в этом случае не превосходит величины $O(n\log^2 n)$, причем очень близка к величине $O(n\log n)$.

Алгоритмы декодирования алгеброгеометрических кодов получили развитие в работах [9 – 11]. Так, в работе [9] предложен алгоритм декодирования, сложность которого определяется величиной $O(n^3)$. Дальнейшее развитие процедуры декодирования в работе [10] позволило снизить сложность вычислений (показано на примере кодов по кривым Эрмита) до величины $O(n^{7/3})$. В работе [11] рассматривается алгоритм декодирования, сложности $O(n^2)$, допускающий распараллеливание вычислений (на n процессорах). Очевидно, существующие алгоритмы декодирования алгеброгеометрических кодов сопоставимы по вычислительной сложности с алгоритмами декодирования кодов БЧХ.

Выводы

Исследования показали, что алгеброгеметрические коды обладают высокими конструктивными характеристиками. В частности, приведенные на рис. 1 зависимости свидетельствуют о том, при возрастании мощности алфавита кодовые соотношения улучшаются. При большой длине алгеброгеметрические коды лежат выше границы Варшамова – Гилберта, что свидетельствует о высоких потенциальных характеристиках. Нами были получены кодовые характеристики для различных кривых над конечными полями $GF(2^m), m = 2,..,6$ (см. табл. 4 – 8).

Как показывают результаты исследований, практическая реализация алгоритмов кодирования и декодирования алгеброгеметрических кодов сводится к простым и вычислительно эффективным операциям над конечными полями. Нами были представлены несколько вариантов построения кодов (в систематическом и несистематическом виде), а также простой алгоритм декодирования. Реализация этих алгоритмов не требует существенных вычислительных затрат. Как показывает анализ, сложность кодирования и декодирования сопоставима с другими известными классами кодов.

Для оценки энергетической эффективности алгеброгеометрического кодирования мы рассмотрели вариант передачи дискретных сообщений М-ми ортогональными сигналами. Как следует из представленных на рис. 4 – 8 зависимостей, применение алгеброгеометрических кодов в дискретных каналах без памяти приводит к значительному энергетическому выигрышу. Энергетический выигрыш возрастает при переходе к длинным кодам, построенным по кривым с большим числом точек по отношению к роду кривой.

Высокая энергетическая эффективность алгеброгеометрического кодирования в сочетании с приемлемой сложностью практической реализации позволяют говорить о возможности построения эффективных помехоустойчивых систем, основанных на использовании таких кодов. Разработка и реализация практических рекомендаций по непосредственному использованию алгеброгеометрических кодов в современных телекоммуникационных системах и сетях является перспективным направлением дальнейшей работы.

Список литературы:

1. Гоппа В.Д. Коды на алгебраических кривых // Докл. АН СССР. – 1981. – Т.259. № 6. – С. 1289-1290.
2. Гоппа В.Д. Коды и информация // Успехи математических наук. – 1984. –Т.30, вып. 1(235). – С. 77-120.
3. Цфасман М.А. Коды Гоппы, лежащие выше границы Варшамова – Гилберта // Проблемы передачи информации. – 1982. – Т.18, №3. – С. 3-6.
4. Шафаревич И.Р. Основы алгебраической геометрии. – Москва : Наука, 1972. – 568с.
5. Стейн С., Джонс Дж. Принципы современной теории связи и их применение к передаче дискретных сообщений. – Москва : Связь, 1971. – 376с.
6. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. – Москва : Мир, 1978. – 576с.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки : пер. с англ. – Москва : Мир, 1986. – 576 с.
8. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – Москва : Связь, 1979. – 744 с.
9. Feng G.L., Rao T.R.N. Decoding algebraic geometric codes up to the designed minimum distance // IEEE Trans. Inform. Theory. – 1993. – Vol. 39, N 1 – P. 37-46.
10. Sakata S., Justesen J., Madelung Y., Jensen H.E., Hoholdt T. Fast Decoding of Algebraic-Geometric Codes up to the Designed Minimum Distance // IEEE Trans. Inform. Theory. – 1995. – Vol. 41, N 5 – P. 1672-1677.
11. Olshevksy V., Shokrollahi A. A displacement structure approach to decoding algebraic geometric codes // Proceedings of the 31st annual ACM Symposium on Theory of Computing (STOC). – 1999. – P. 235-244.

Харьковский национальный
университет имени В.Н.Каразина;
АО «Институт информационных технологий», Харьков;
Университет таможенного дела и финансов, Днепр

Поступила в редколлегию 05.11.2018