УДК 621.391.251

К ВОПРОСУ О ПОСТРОЕНИИ LDPC-КОДОВ НА ОСНОВЕ ЕВКЛИДОВЫХ ГЕОМЕТРИЙ

А. А. Овчинников,
канд. техн. наук, ассистент
Санкт-Петербургский государственный университет аэрокосмического приборостроения

В статье рассматриваются коды с малой плотностью проверок на четность, основанные на конечных Евклидовых геометриях. Для ряда таких кодов получены оценки их минимального расстояния и спектра, предложены процедуры укорочения Евклидово-геометрических конструкций и оценки расстояния полученных кодов. Приведены результаты моделирования рассматриваемых кодов в канале с аддитивным белым гауссовским шумом (АБГШ).

In this paper we consider the low-density parity-check codes based on finite Euclidean geometries. For the number of such codes the estimations of their minimal distance and spectrum are obtained, the shortening procedures and the estimations of distance for such codes are suggested. The simulation results in channel with AWGN are presented.

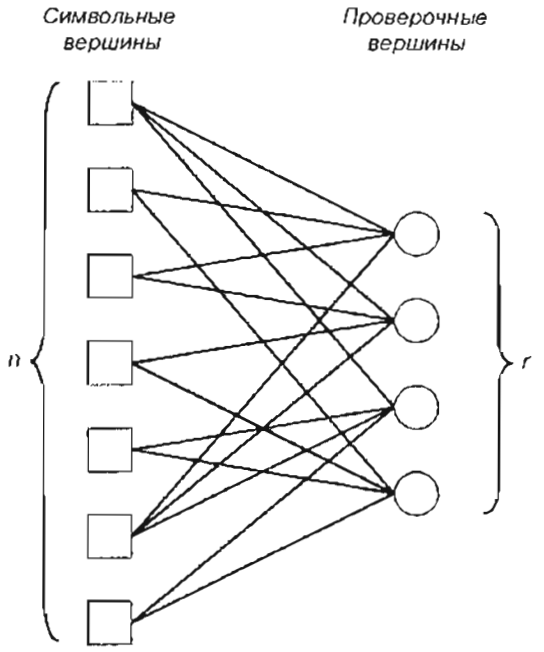
Введение

Коды с малой плотностью проверок на четность (LDPC-коды) были впервые предложены Р. Галлагером [1, 2] и позднее исследовались в работах [3–6]. Несмотря на то, что в течение долгого времени LDPC-коды были практически исключены из рассмотрения, в последние годы наблюдается увеличение количества исследований в этой области. Это связано с тем, что, обладая плохим минимальным расстоянием, коды с малой плотностью, тем не менее, обеспечивают высокую степень исправления ошибок при весьма малой сложности их декодирования. Было показано, что с ростом длины некоторые LDPC-коды могут превосходить турбо-коды и приближаться к пропускной способности канала с АБГШ [7]. Вместе с тем, многие предложенные конструкции LDPC-кодов являются циклическими или квазициклическими, что позволяет производить не только быстрое декодирование, но и эффективные процедуры кодирования. Кроме того, даже для LDPC-кодов, не обладающих свойством цикличности, были предложены эффективные процедуры кодирования [8].

Код с малой плотностью проверок на четность задается своей проверочной матрицей H, обладающей свойством разреженности, т. е. ее строки и столбцы содержат мало ненулевых позиций по сравнению с размерностью матрицы. Наравне с традиционным заданием кода как нулевого пространства проверочной матрицы, LDPC-коды часто задаются с помощью графа, для которого матрица H является матрицей смежности (так называемого графа Таннера). Это двудольный граф, вершины которого делятся на два множества: 1) n символьных вершин, соответствующих столбцам; 2) r проверочных вершин, соответствующих строкам проверочной матрицы. Ребра, соединяющие вершины графа, соответствуют ненулевым позициям в матрице H. Пример такого графа приведен на рис. 1.

LDPC-коды, у которых строки и столбцы содержат одинаковое число единиц, принято называть регулярными кодами, в то время как коды с неравным числом единиц называются нерегулярными. Как правило, построение хороших нерегулярных кодов использует вероятностные методы, анализ таких кодов производится в асимптотике, тогда как регулярные конструкции основаны на объектах (например, комбинаторных) с известными свойствами и могут анализироваться с учетом свойств этих объектов.

Настоящая статья рассматривает построение LDPC-кодов, основанных на Евклидовых геометриях. Евклидово-геометрические коды известны довольно давно [9–11], однако в качестве кодов с малой плотностью они стали рассматриваться только в последние годы [12]. Мы анализируем свойства LDPC-кодов, основанных на Евклидовой геометрии, и предлагаем методы построения новых кодов, используя свойства Евклидовых геометрий и проведенный анализ.



■ *Рис. 1. Граф Таннера LDPC-кода*

Конструкции и декодирование

Как и для всякого линейного (n, k)-кода, одной из оценок качества LDPC-кода является вероятность ошибочного декодирования, которая обычно характеризуется долей ошибочных бит в декодированном сообщении (BER), при заданных длине кода n и скорости $R = k / n$.

Одним из главных параметров, влияющих на вероятность ошибочного декодирования, является кодовое минимальное расстояние d_0. В случае LDPC-кодов, однако, часто минимальное расстояние кода мало, и низкая вероятность ошибки достигается за счет хороших спектральных свойств кода (небольшого количества слов малого веса).

Р. Галлагером были предложены алгоритмы декодирования LDPC-кодов как для дискретных (bit-flipping decoding), так и для полунепрерывных (belief propagation decoding) каналов. Общим свойством LDPC-декодеров является то, что они представляют собой итеративные процедуры, оперирующие не с блоками, а с отдельными символами принятого сообщения. Параметром декодера является максимальное число итераций, после которого декодер принимает решение о передававшемся слове. На практике часто бывает достаточно небольшого числа итераций, чтобы правильно продекодировать принятое слово. В работе М. С. Пинскера и В. В. Зяблова [3] показано, что сложность декодирования LDPC-кода составляет порядка $n\log n$. В работах [12, 13] рассмотрены ускоренные процедуры декодирования LDPC-кодов, дающие незначительное увеличение вероятности ошибки.

Работа декодера LDPC-кода ухудшается, если в графе Таннера соответствующего LDPC-кода присутствуют циклы небольшой длины. Как правило, циклы длины 6 не оказывают существенного влияния на качество декодирования, поэтому существующие на сегодня конструкции должны обеспечивать отсутствие циклов длины 4. Для этого достаточно, чтобы любые два столбца проверочной матрицы LDPC-кода не имели более одной общей ненулевой позиции.

В работах [6, 14] проведен асимптотический анализ декодера Галлагера «belief propagation» для некоторых каналов связи. Показано, что при использовании этого декодера существует некий порог, такой, что при определенном уровне помех в канале (превышающем этот порог) вероятность ошибки декодирования не стремится к нулю с ростом числа итераций. Величина этого порога зависит от распределения весов строк и столбцов проверочной матрицы LDPC-кода, и эти веса можно оптимизировать с помощью предлагаемой в работах [6, 14] процедуры «density evolution». Коды с распределениями, полученными с помощью этой процедуры, дают выигрыш на низких отношениях сигнал–шум (в канале с АБГШ), однако, как правило, обладают так называемым эффектом «error-floor», т. е. более медленным уменьшением вероятности ошибки при увеличении отношения сигнал–шум.

В последние годы было предложено много конструкций LDPC-кодов. Некоторые из них основывались на свойствах известных комбинаторных объектов – разностных множеств, блок-схем, геометрий [15, 16], другие – на различного рода вероятностных методах [7, 14]. В последнем параграфе данной работы приведены сравнительные результаты моделирования некоторых из них.

Конечные Евклидовы геометрии

Опишем вкратце Евклидовы геометрии [9, 10]. Приведенные здесь соотношения будут использоваться нами в дальнейшем для оценки параметров получаемых LDPC-кодов.

Евклидовой геометрией EG называется совокупность объектов – точек и прямых, удовлетворяющих следующим аксиомам:

1. Через любые две точки можно провести прямую, причем только одну;

2. Для любой прямой L и любой точки p, не лежащей на L, можно провести прямую, проходящую через p и не пересекающую L (т. е. прямую, параллельную прямой L).

3. Существуют три точки, не лежащие на одной прямой.

Следует отметить, что приведенный набор аксиом не является единственным, с помощью которого задается Евклидова геометрия, однако другие наборы аксиом могут быть сведены к этим трем, и наоборот.

Одной из наиболее часто используемых и практически важных форм задания Евклидовых геометрий является описание их с помощью конечных по-

лей. Евклидова геометрия $EG(m, q)$, где $q = p^s$, p – простое, задается с помощью конечного поля $GF(q^m)$ [расширения поля $GF(q)$] следующим образом: точками Евклидовой геометрии являются элементы поля $\alpha^j \in GF(q^m)$, $j = -\infty, 0, 1, \ldots, q^m - 2$, α – примитивный элемент поля $GF(q^m)$). Заметим, что в множество точек Евклидовой геометрии входит и нулевая точка — нулевой элемент $\alpha^{-\infty}$ поля $GF(q^m)$. Тогда линия, проходящая через нулевую точку и некоторую ненулевую точку α^j, задается уравнением

$$L(0,\alpha^j) = \{\beta\alpha^j\} = \{\beta\alpha^j : \beta \in GF(q), \alpha^j \in GF(q^m), \alpha^j \neq 0\}, \quad (1)$$

т. е. проходит через точки $\alpha^{-\infty} = 0$ и $\alpha^j \neq 0$, и содержит элементы поля, получаемые из α^j умножением на все элементы β (включая нулевой) подполя $GF(q)$. Если некоторые элементы α^i и α^j линейно независимы, то есть α^i не лежит на прямой $L(0,\alpha^j)$, то, в соответствии с аксиомой 2, можно провести линию, параллельную линии $L(0,\alpha^j)$ и проходящую через точку α^i:

$$L(\alpha^i,\alpha^j) = \{\alpha^i + \beta\alpha^j\} = \{\alpha^i + \beta\alpha^j : \beta \in GF(q)\}. \quad (2)$$

Так как элемент β в уравнениях (1), (2) принимает $q = p^s$ различных значений, каждая прямая в Евклидовой геометрии содержит

$$\rho = q = p^s \quad (3)$$

точек. Всего существует

$$|L| = q^{m-1}(q^m - 1)/(q - 1) \quad (4)$$

линий в $EG(m, q)$. Каждая линия имеет $q^{m-1} - 1$ параллельных, через каждую точку проходит

$$\gamma = (q^m - 1)/(q - 1) \quad (5)$$

прямых (или, другими словами, в каждой точке пересекается γ прямых).

Евклидова геометрия $EG(2, q)$ называется плоскостью. Точки плоскости могут быть получены как линейные комбинации трех точек α^i, α^j, α^k, не лежащих на одной прямой:

$$\{\alpha^i + \mu\alpha^j + \eta\alpha^k\}, \ \mu, \eta \in GF(q). \quad (6)$$

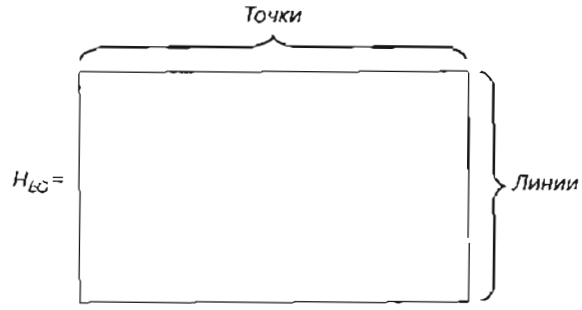
Из соотношений (4) и (6) следует, что плоскость содержит q^2 точек и $q(q + 1)$ прямых.

Теперь рассмотрим способы задания кодов, основанных на конечных Евклидовых геометриях.

Коды EG-LDPC

Евклидово-геометрические коды строятся как система инциденций геометрии $EG(m, q)$ [9, 11, 17]. Так как число единиц в проверочной матрице Евклидово-геометрического кода мало по сравнению с размерами матрицы, такой код можно рассматривать как LDPC-код.

LDPC-код, основанный на Евклидовой геометрии, с проверочной матрицей H_{EG}, строится следующим образом: строки проверочной матрицы



■ ***Рис. 2.*** *Проверочная матрица EG-кода*

соответствуют линиям Евклидовой геометрии, столбцы — ненулевым точкам в $EG(m, p^s)$. Элементы матрицы H_{EG} определяются из векторов инциденций линий Евклидовой геометрии (рис. 2):

$$H_{EG}(i,j) = \begin{cases} 1, & \text{если точка } j \text{ лежит на прямой } i \\ 0, & \text{в противном случае.} \end{cases} \quad (7)$$

Из уравнений (1)–(5) следует, что проверочная матрица H_{EG} имеет

$$n = q^m \quad (8)$$

столбцов и

$$r = q^{m-1}(q^m - 1)/(q - 1) \quad (9)$$

строк. Каждый столбец матрицы содержит

$$\gamma = (q^m - 1)/(q - 1) \quad (10)$$

единиц, каждая строка содержит

$$\rho = p^s \quad (11)$$

единиц.

Обычно рассматриваются Евклидово-геометрические коды при $p = 2$, не содержащие нулевой точки [12, 18]. Такие коды иногда называются EG-кодами типа 0, они являются циклическими [9, 11], их параметры

$$n = 2^{ms} - 1; \quad (12)$$

$$r = (2^{(m-1)s} - 1)(2^{ms} - 1)/(2^s - 1). \quad (13)$$

Число информационных символов таких кодов оценено в работе [19].

Наряду с заданием проверочной матрицы, как показано на рис. 2, можно рассматривать EG-LDPC код с матрицей, транспонированной к матрице (7). Тогда ее строки соответствуют точкам геометрии, а столбцы – линиям. В обоих случаях задания матрицы свойства геометрии и (8)–(11) обеспечивают выполнение следующих свойств проверочной матрицы.

1. Каждая строка содержит ρ единиц [следует из (11)].

2. Каждый столбец содержит γ единиц [следует из (10)].

3. Любые два столбца имеют не более чем одну общую ненулевую позицию (так как через две точки можно провести только одну прямую).

■ *Таблица 1. Параметры некоторых EG-LDPC кодов (параметр d_0 соответствует нижней оценке минимального расстояния)*

n	k	R	d_0	γ	ρ	$EG(m, q)$	Тип
16	7	0,4375	6	5	4	(2,4)	–
64	37	0,5781	10	9	8	(2,8)	
256	175	0,6836	18	17	16	(2,16)	
1024	781	0,7627	34	33	32	(2,32)	
64	13	0,2031	22	21	4	(3,4)	–
512	139	0,2715	74	73	8	(3,8)	
20	11	0,55	5	4	5	(2,4)	EG^T
72	45	0,625	9	8	9	(2,8)	EG^T
272	191	0,7022	17	16	17	(2,16)	EG^T
1056	813	0,7699	33	32	33	(2,32)	EG^T
336	285	0,8482	5	4	21	(3,4)	EG^T
4672	4299	0,9202	9	8	73	(3,8)	EG^T
90	9	0,1	9	8	73	(2,9)	EG^T
756	27	0,0357	9	8	73	(2,27)	EG^T
7371	6642	0,9011	10	9	91	(3,9)	EG^T

4. Любые две строки имеют не более одной общей ненулевой позиции (так как две прямые пересекаются не более чем в одной точке).

Свойства 3 и 4 означают, что граф Таннера как для кода с проверочной матрицей H_{EG}, так и для кода с проверочной матрицей H_{EG}^T не имеет циклов длины 4.

Параметры некоторых EG-LDPC кодов (включающих в себя точку 0) приведены в табл. 1. Параметры кодов с проверочной матрицей H_{EG}^T помечены как EG^T. Результаты моделирования EG-LDPC кодов в канале с АБГШ приведены в последнем параграфе.

Так как столбцы проверочной матрицы (7) имеют не более одной общей ненулевой позиции, любые γ столбцов матрицы линейно независимы и, значит, не могут образовать нулевой синдром. Тогда минимальное расстояние кода с проверочной матрицей (7) оценивается как

$$d_0 \geq \gamma + 1. \qquad (14)$$

Далее мы получим более точные оценки минимального расстояния EG-кодов.

Укорочение EG-LDPC кодов

В исследованиях [12, 20] приведены некоторые методы укорочения EG-LDPC кодов. С помощью моделирования показано, что вероятность ошибки при укорочении может уменьшаться, однако не приводится аналитических обоснований для выбора того или иного метода укорочения.

Рассмотрим методы укорочения LDPC-кодов и проведем анализ минимального расстояния некоторых Евклидово-геометрических кодов.

Рассмотрим Евклидово-геометрические коды, проверочная матрица которых является транспонированной к матрице (7):

$$H_{EG}(i, j) = \begin{cases} 1, & \text{если точка } i \text{ лежит на прямой } j \\ 0, & \text{в противном случае.} \end{cases} \qquad (15)$$

Рассмотрим Евклидово-геометрическое пространство, т. е. геометрии $EG(3, q)$, $q = p^s$. Такие коды имеют длину

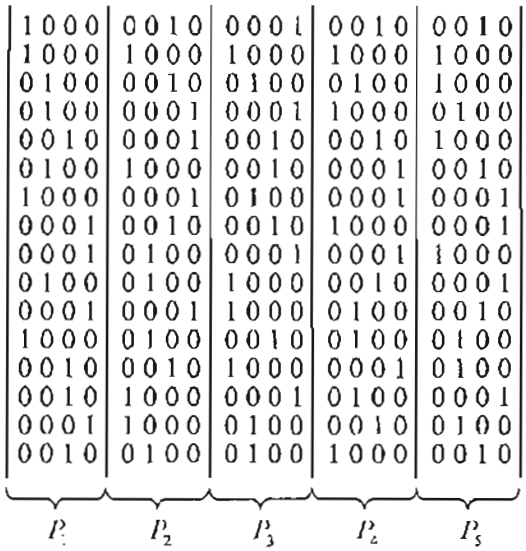
$$n = q^2(q^3 - 1)/(q - 1), \qquad (16)$$

их проверочная матрица H состоит из

$$r_H = q^3 \qquad (17)$$

строк. Заметим, что H не обязательно имеет полный ранг, поэтому r_H может использоваться только как верхняя оценка числа проверочных символов.

Рассмотрим прямую в такой Евклидовой геометрии. Прямая содержит q точек. Через каждую точку, не лежащую на прямой, можно провести единственную прямую, параллельную данной. Каждая такая прямая также содержит q точек. Так как всего в геометрии q^3 точек, всего существует q^2 прямых, параллельных друг другу. Назовем построенное таким образом множество прямых параллельным классом. Геометрия содержит $q^2(q^3 - 1)/(q - 1)$ прямых, которые могут быть разбиты на $(q^3 - 1)/(q - 1)$ параллельных классов по q^2 прямых в каждом. Укорачивая проверочную матрицу EG-кода на столбцы, соответствующие параллельным классам, мы будем получать код, в котором число единиц в строках и столбцах остается равным, так как каждая точка геометрии присутствует в параллельном классе ровно



■ ***Рис. 3.*** *Разбиение на параллельные классы для плоскости EG (2,4)*

один раз. При этом расстояние кода не ухудшилось, а число единиц в строке стало меньшим, что может улучшить работу итеративного декодера.

Описанный метод укорочения позволяет оптимизировать параметры кодов для требуемых длин, выбирая параметры геометрий и величину укорочения с учетом получающихся весов строк.

Попробуем оценить, как укорочение на параллельные классы влияет на дистанционные характеристики кода. Для этого рассмотрим Евклидову плоскость, т. е. геометрию $EG\ (2, q)$. Плоскость содержит $q(q+1)$ прямых, которые могут быть разбиты на $q+1$ параллельных классов по q прямых в каждом. Каждая точка плоскости присутствует в параллельном классе ровно один раз. Пример разбиения плоскости на параллельные классы $P_1, \ldots, P_5$ приведен на рис. 3 для плоскости $EG\ (2, 2^2)$.

Рассмотрим отдельно случаи $p = 2$ и $p \neq 2$. Пусть $p \neq 2$. Далее, пусть

$$W(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i \qquad (18)$$

– весовая функция кода [10], где A_i – число слов веса i в коде; x – число нулей; y – число единиц. Тогда справедлива следующая теорема.

Теорема 1. Если проверочная матрица (15) Евклидово-геометрического кода при $m=2$, $q=p^s$, $p \neq 2$ имеет полный ранг, тогда коэффициент A_i весовой функции (18) вычисляется как

$$A_i = \begin{cases} C_{q+1}^{i/q}, & i : 2q \\ 0, & \text{в противном случае.} \end{cases} \qquad (19)$$

Доказательство. Если ранг матрицы (15) является полным, т. е. равен q^2, то число информационных символов кода равно

$$k = n - r = q(q+1) - q^2 = q. \qquad (20)$$

Разобьем множество прямых плоскости на $q+1$ параллельных классов по q прямых в каждом. Заметим, что при $p \neq 2$ число q всегда нечетно, тогда как число $q+1$ всегда четно. Так как все точки присутствуют в параллельном классе ровно один раз, сумма всех столбцов проверочной матрицы, соответствующих параллельному классу, дает столбец из всех единиц. Тогда очевидно, что сумма всех столбцов четного числа параллельных классов даст нулевой столбец, т. е. задаст кодовое слово. Заметим, что, так как $q+1$ четно, максимальное четное число классов равно $q+1$, что соответствует кодовому слову из всех единиц. Четное число $2i$ параллельных классов можно выбрать из Евклидова пространства C_{q+1}^{2i} способами. Таким образом, общее количество кодовых слов, образованных параллельными классами, равно

$$C_{q+1}^0 + C_{q+1}^2 + C_{q+1}^4 + C_{q+1}^6 + \ldots + C_{q+1}^{q+1} = \sum_{i=0}^{(q+1)/2} C_{q+1}^{2i}. \qquad (21)$$

Как следствие биномиальной теоремы [21], имеем следующие тождества:

$$\sum_{i=0}^{n} C_n^i = 2^n; \qquad (22)$$

$$\sum_{i=0}^{n} (-1)^i C_n^i = 0. \qquad (23)$$

Пусть n четно. Тогда из тождества (23) имеем

$$\sum_{i=0}^{n/2} C_n^{2i} = \sum_{i=0}^{n/2-1} C_n^{2i+1},$$

т. е. суммы четных и нечетных членов ряда C_n^i равны. Тогда с учетом тождества (22)

$$\sum_{i=0}^{n/2} C_n^{2i} = 2^{n-1}. \qquad (24)$$

Из равенств (21) и (24) получаем

$$\sum_{i=0}^{(q+1)/2} C_{q+1}^{2i} = 2^q. \qquad (25)$$

Но из (20) следует, что в (25) учтены все кодовые слова. Отсюда следует утверждение теоремы.

Таким образом, пользуясь теоремой 1, можно указать минимальное расстояние для рассматриваемых кодов.

Следствие 1. Минимальное расстояние кода из теоремы 1 равно

$$d_0 = 2q. \qquad (26)$$

Для каждого конкретного кода ранг проверочной матрицы может быть вычислен экспериментально. Проведенные тесты показывают, что для рассматривавшихся параметров геометрий при $m = 2$, $p \neq 2$

■ ***Таблица 2.*** *Точное минимальное расстояние некоторых EG-LDPC кодов*

n	k	R	$\tilde{d}_0$	d_0	γ	ρ	$EG(m, \phi)$	Тип
20	11	0,55	5	5	4	5	(2,4)	*EG*
72	45	0,625	9	9	8	9	(2,8)	*EG*
272	191	0,7022	17	17	16	17	(2,16)	*EG*
1056	813	0,7699	33	33	32	33	(2,32)	*EG*
336	285	0,8482	5	5	4	21	(3,4)	*EG*
4672	4299	0,9202	9	9	8	73	(3,8)	
90	9	0,1	9	18	8	73	(2,9)	*EG*
756	27	0,0357	9	54	8	73	(2,27)	*EG*
7371	6642	0,9011	10	18	9	91	(3,9)	*EG*

ранг проверочной матрицы действительно является полным.

В табл. 2 приведены параметры некоторых LDPC-кодов, с их минимальными расстояниями, полученными на основе результатов теоремы 1. Здесь $\tilde{d}_0$ означает оценку минимального расстояния, d_0 – точное минимальное расстояние.

Теперь рассмотрим случай $p = 2$. Для поля характеристики 2 соотношение (20) не выполняется, т. е. проверочная матрица (15) содержит линейно зависимые строки. Таким образом, слова, образованные параллельными классами, не являются всеми кодовыми словами. В этом случае можно сформулировать следующие утверждения.

Теорема 2. Если код с проверочной матрицей (15) при $m = 2$, $p = 2$ имеет минимальное расстояние $q + 1$, тогда для слова веса $q + 1$ никакие две из линий, соответствующих ненулевым позициям этого слова, не лежат в одном параллельном классе.

Доказательство. Минимальное расстояние кода определяется минимальной линейной комбинацией столбцов проверочной матрицы, дающей в результате нулевой столбец-синдром. В случае рассматриваемых кодов столбец проверочной матрицы соответствует линии в Евклидовой геометрии. Каждая позиция синдрома соответствует точке Евклидовой плоскости и является суммой позиций столбцов, вошедших в линейную комбинацию. Таким образом, чтобы позиция синдрома равнялась нулю, необходимо, чтобы через соответствующую точку либо не проходили прямые из данной линейной комбинации, либо число прямых, проходящих через точку, было четным.

Следовательно, чтобы построить кодовое слово, нужно найти множество прямых L, такое, что через каждую точку геометрии либо не проходят прямые из L, либо в этой точке пересекается четное число прямых из L.

Тогда нахождению слова минимального веса соответствует нахождение множества L_0 минимальной мощности. Попробуем построить такое множество минимальной мощности.

Допустим, что на некотором шаге k уже сформировано множество прямых $L_0^{(k)}$. Обозначим $P^{'}$ те точки из $L_0^{(k)}$, через которые проходит нечетное число прямых, $P^{''}$ – те точки, через которые проходит четное число прямых. Чтобы число прямых в L_0 было минимальным, необходимо, чтобы каждая следующая добавляемая прямая проходила через как можно большее число точек $P^{'}$, не проходила через точки $P^{''}$ и добавляла как можно меньшее число новых точек, которые на следующем шаге увеличат множество $P^{'}$. Построение L_0 закончится тогда, когда множество точек $P^{'}$ станет пустым.

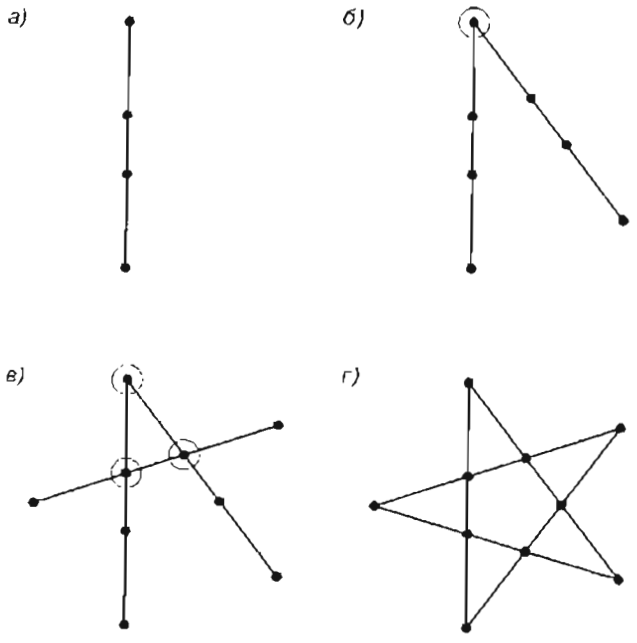
Это эквивалентно тому, что на шаге k новая прямая должна пересекать как можно большее число прямых, уже содержащихся в $L_0^{(k-1)}$, причем пересечение должно идти по точкам $P^{'}$.

Рассмотрим прямую $l^{(0)}$ Евклидовой плоскости Эта прямая содержит q точек и принадлежит какому-то классу параллельности. Следующая проведенная прямая $l^{(1)}$ может либо не пересечь данную, если она принадлежит тому же классу параллельности, что и $l^{(0)}$, либо пересечь в одной точке, если $l^{(1)}$ не параллельна $l^{(0)}$. Следующая проводимая прямая $l^{(2)}$ может пересечь либо одну прямую из уже выбранных, если она параллельна одной из них, либо пересечь обе, в противном случае.

Пример построения множества L_0 для случая $q = 4$ приведен на рис. 4. Точки множества $P^{''}$ обведены на этом рисунке кругами (кроме заключительный фигуры).

Таким образом, выбирая каждый раз прямую из еще не использовавшегося класса параллельности, мы будем пересекать все прямые, выбранные на предыдущих шагах. Добавление прямой к множеству $L_0^{(k-1)}$, в котором уже содержатся k прямых, добавляет $q - k$ новых точек. Всего в $L_0^{(k)}$ содержится

$$N_k = |L_0^{(k)}| = \sum_{i=0}^{k-1} (q - i), \; k \geq 0 \qquad (27)$$



■ ***Рис. 4.*** *Графическая интерпретация построения вектора минимального веса для EG(2,4): а – начальная линия; б – добавление второй линии; в – добавление третьей линии; г – замкнутая фигура*

точек. Оценим число $N_k^{\cdot}$ точек типа $P^{\cdot}$ на k-м шаге. На нулевом шаге $L_0^{(0)}$ содержит единственную прямую, и все $N_0 = q$ точек являются $P^{\cdot}$-точками. На первом шаге добавляемая прямая пересекает уже выбранную в одной точке, таким образом, в $L_0^{(1)}$ содержится одна точка типа $P^{\cdot\cdot}$ и $N_1 - 1$ точек типа $P^{\cdot}$. На втором шаге новая прямая пересекает две существующие еще в двух точках, и таким образом, в $L_0^{(2)}$ содержится уже три точки типа $P^{\cdot\cdot}$ и $N_2 - 3$ точек типа $P^{\cdot}$. В общем случае

$$N_k^{\cdot} = N_k - \sum_{i=0}^{k-1} i, \quad k \geq 0 \qquad (28)$$

или, с учетом (27),

$$N_k^{\cdot} = \sum_{i=0}^{k-1} (q-i) - \sum_{i=0}^{k-1} i = \sum_{i=0}^{k-1} (q-2i). \qquad (29)$$

Теперь найдем минимальное число линий, которые нужно провести, чтобы получить кодовое слово, т. е. найдем $|L_0|$. Для этого нужно просто определить номер шага k, при котором (29) обратится в ноль:

$$|L_0| = \{k : N_k^{\cdot} = 0\}, \; k \geq 0. \qquad (30)$$

Применив формулу суммы арифметической прогрессии, из соотношений (29) и (30) получим условие остановки построения L_0:

$$\sum_{i=0}^{k-1} (q-2i) = \frac{(q+q-2k+2))k}{2} = (q-k+1)k = 0. \qquad (31)$$

При условии $k > 0$ выполнение условия (31) возможно только при $k = q$. Таким образом, при указанном методе построения требуется $q+1$ прямых из разных классов параллельности, чтобы построить L_0, а в Евклидовой плоскости содержится как раз $q+1$ классов параллельности. Тогда из (30) и (31) имеем

$$|L_0| = q + 1,$$

что и завершает доказательство.

Однако в отношении теоремы 2 можно сформулировать следующее утверждение.

Замечание 1. Минимальное расстояние кода из теоремы 2 равно $q+1$ только в том случае, если можно провести прямые указанным способом, т. е. только через точки типа $P^{\cdot}$. Это утверждение не является доказанным, однако эксперименты показывают, что для полей характеристики 2 это действительно так. Таким образом, возможно, теорема 2 задает точное минимальное расстояние.

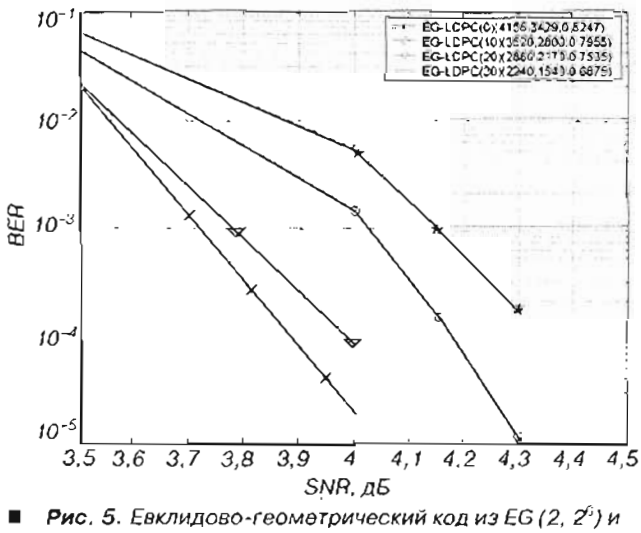
Следствие 2. Укорочение кода (15) при $m = 2$, $p = 2$ и с учетом замечания 1 на прямые, содержащие любой параллельный класс, приводит к коду с минимальным расстоянием

$$d_0 \geq q + 2. \qquad (32)$$

Доказательство. Как было показано в доказательстве теоремы 2, для построения L_0 требуется $q+1$ прямых из разных классов параллельности, которых в Евклидовой плоскости ровно $q+1$. Таким образом, любое ненулевое кодовое слово минимального веса имеет $q+1$ ненулевых позиций, по одной в каждом классе параллельности. Удаление любого класса параллельности приведет к тому, что в коде не останется слов веса $q+1$, отсюда следует утверждение следствия.

Сравнение конструкций в канале с АБГШ

Здесь мы приводим результаты моделирования для кодов, полученных с помощью укорочения на

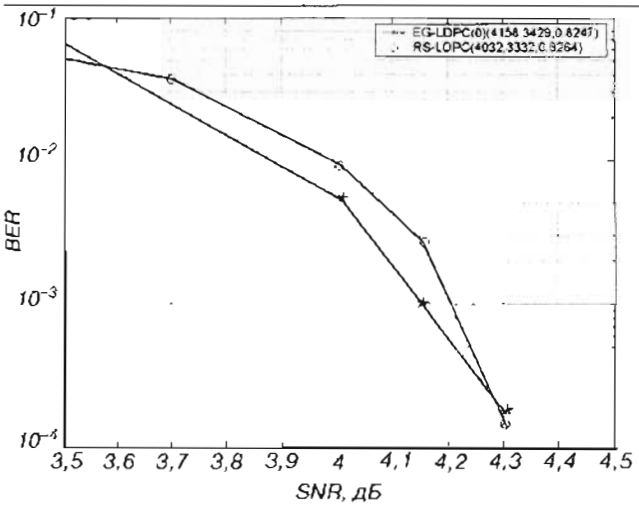


■ ***Рис. 5.*** *Евклидово-геометрический код из EG(2, 2^6) и его укорочения:*
EG-LDPC(0)(4158,3429,0.8247);
EG-LDPC(10)(3520,2800,0.7955);
EG-LDPC(20)(2880,2170,0.7535);
EG-LDPC(30)(2240,1540,0.6875)

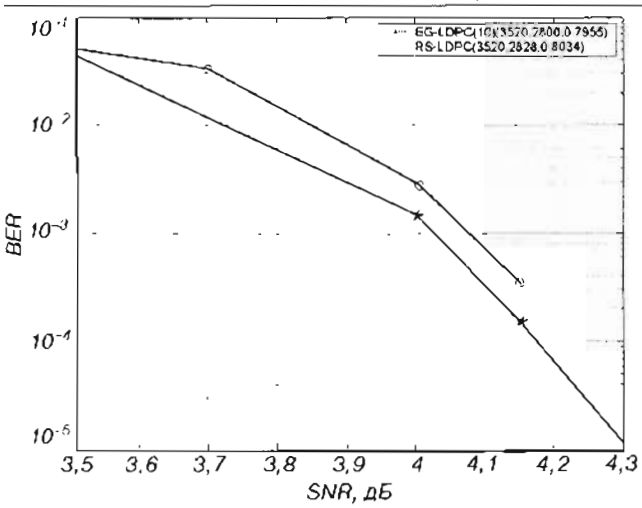
параллельные классы, описанного выше. Моделирование проводилось в канале с аддитивным белым гауссовским шумом (АБГШ), двоичной фазовой модуляцией, для декодирования использовался ускоренный декодер, описанный в работе [13], с ограничением максимального числа итераций 10.

В качестве исходного кода рассматривался Евклидово-геометрический код с проверочной матрицей (15), полученной с помощью конечной геометрии *EG* (2, 2^6). Укоротим этот код на 10, 20 и 30 параллельных классов, что приведет к кодам с разными длинами и скоростями. Результаты их моделирования в канале с АБГШ показаны на рис. 5.

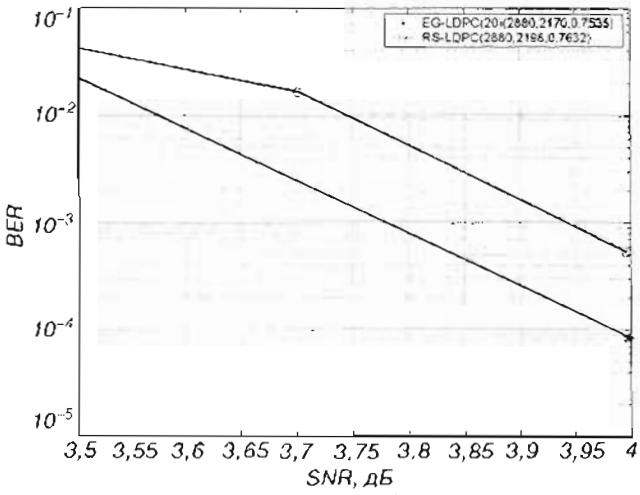
Для сравнения корректирующей способности полученных кодов с другими кодами рассмотрим конструкцию RS-LDPC, основанную на укороченных кодах Рида-Соломона [22]. На рис. 6–9 приведены результаты моделирования укороченных Евклидово-геометрических кодов и кодов RS-LDPC. Как видно из графиков, исходный Евклидово-геометрический код и его укорочения дают выигрыш по сравнению с кодом RS-LDPC при сравнимых длинах и кодовых скоростях. Таким образом, предложенный метод построения укороченных Евклидово-геометрических кодов дает способ получения новых эффективных кодов для различных скоростей и кодовых длин.



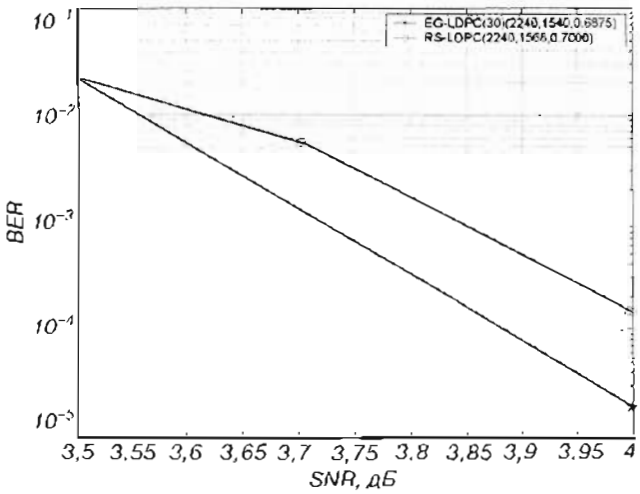
■ ***Рис. 6.*** *Евклидово-геометрический код из EG (2, 2^6) и код RS-LDPC (6, 63, 35):*
EG-LDPC(0)(4158, 3429, 0.8247);
RS-LDPC(4032, 3332, 0.8264)



■ ***Рис. 7.*** *Укорочение кода EG на 10 параллельных классов и код RS-LDPC (6, 55, 35):*
EG-LDPC(10)(3520, 2800, 0.7955);
RS-LDPC(3520, 2828, 0.8034)



■ ***Рис. 8.*** *Укорочение кода EG на 20 параллельных классов и код RS-LDPC (6, 45, 35):*
EG-LDPC(20)(2880, 2170, 0.7535);
RS-LDPC(2828, 2198, 0.7632)



■ ***Рис. 9.*** *Укорочение кода EG на 30 параллельных классов и код RS-LDPC (6, 35, 35):*
EG-LDPC(30)(2240, 1540, 0.6875);
RS-LDPC(2240, 1568, 0.7000)

Заключение

В данной статье рассмотрены свойства Евклидово-геометрических кодов. Для ряда EG-кодов получено описание их спектра, найдены более точные оценки минимального расстояния некоторых EG-кодов и их укорочений. Предложен метод построения LDPC-кодов, основанный на укорочении на параллельные классы. Данный метод позволяет более гибко задавать такие параметры кода, как длина и скорость. Проведенное моделирование в канале с АБГШ подтверждает эффективность кодов, полученных таким способом.

Литература

1. **Gallager R. G.** Low-density parity check codes // IRE Trans actions inform ation theory. – Jan. 1962.
2. **Gallager R. G.** Low density parity check codes. – Cambridge, MA: MIT Press, 1963.
3. **Зяблов В. В., Пинскер М. С.** Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Проблемы передачи информации. – Vol. XI. – N 1, 1975.
4. **MacKay D., Neal R. M.** Near shannon limit performance of low-density parity-check codes // IEEE Transactions on Information Theory. – Vol. 47. – Feb. 2001.
5. **MacKay D.** Good error correcting codes based on very sparse matrices // IEEE Transactions on information theory. – Vol. 45. – Mar. 1999.
6. **Richardson T. J., Urbanke R. L.** The capacity of low-density parity-check codes under message-passing decoding // IEEE transactions on information theory. – Vol. 47. – Feb. 2001.
7. **Forney G., Richardson T. J., Urbanke R. L., Chung S. Y.** On the design of low-density parity-check codes within 0.0045 db of the shannon limit // IEEE communications letters. – Vol. 5. – Feb. 2001.
8. **Richardson T. J., Urbanke R. L.** Efficient encoding of low-density parity-check codes // IEEE transactions on information theory. – Vol. 47. – Feb. 2001.
9. **Питерсон У., Уэлдон Э.** Коды, исправляющие ошибки. – М.: Мир, 1976.
10. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. –М.: Связь, 1979.
11. **Блейхут Р.** Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986.
12. **Kou Y., Lin S., Fossorier P. C.** Low-density parity-check codes based on finite geometries: A rediscovery and new results // IEEE transactions on information theory. – Vol. 47. – Nov. 2001.
13. **Fossorier M. P. C., Mihaljevic M., Imai H.** Reduced complexity iterative decoding of low-density parity-check codes based on belief propagation // IEEE transactions on communications. – Vol. 47. – May 1999.
14. **Richardson T. J., Urbanke R. L., Shokrollahi M.** Design of capacity-approaching irregular low-density parity-check codes // IEEE transactions on information theory. – Vol. 47. – Feb. 2001.
15. **Johnson S. J., Weller S. R.** Regular low-density parity-check codes from combinatorial designs // In Proc. IEEE Information Theory Workshop (Cairns, Australia). – Sept. 2001.
16. **Johnson S. J., Weller S. R.** Codes for iterative decoding from partial geometries // ISIT2002, submitted.
17. **Касами Т., Токура Н., Ивадари Е., Инагаки Я.** Теория кодирования. – М.: Мир, 1978.
18. **Lin S.** Shortened finite geometry codes // IEEE transactions on information theory. – Sept. 1972. – P. 692.
19. **Lin S.** On the number of information symbols in polynomial codes // IEEE transactions on information theory. – Vol. 18. – Nov. 1972. – P. 785–794.
20. **Lin S.** Shortened finite geometry codes // IEEE transactions on information theory. – Vol. 18. – Sept. 1972. – P. 692–696.
21. **Грэхем Р., Кнут Д., Паташник О.** Конкретная математика. Основание информатики. – М.: Мир, 1998.
22. **Djurdjevic I., Xu J., Abdel-Ghaffar K., Lin S.** A class of low-density parity-check codes constructed based on reed-solomon codes with two information symbols // IEEE communications letters. – Vol. 7. – July 2003.