КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ

УДК 621.391

А. В. Козлов, Е. А. Крук, А. А. Овчинников

ПОДХОД К ПОСТРОЕНИЮ БЛОЧНО-ПЕРЕСТАНОВОЧНЫХ КОДОВ С МАЛОЙ ПЛОТНОСТЬЮ ПРОВЕРОК НА ЧЕТНОСТЬ

Предложены некоторые способы построения кодов с малой плотностью проверок на четность, приводятся конструкции кодов и результаты их использования для передачи в канале с аддитивным белым гауссовым шумом.

Ключевые слова: *LDPC-коды, коды Гилберта, блочно-перестановочные конструкции.*

Введение и основные понятия. Коды с малой плотностью проверок на четность (LDPC-коды) были предложены Р. Галлагером в 1963 г. [1], авторы статьи [2] доказали, что они обладают уникальными свойствами. LDPC-коды обеспечивают экспоненциальное убывание вероятности ошибки с увеличением длины кода при логарифмическом росте числа операций, необходимых для декодирования одного символа кодового слова. Однако долгое время исследования в области LDPC-кодов носили в основном теоретический характер. Это было связано, прежде всего, с тем, что высокая корректирующая способность этих кодов достигается при большой длине кодовых слов (порядка нескольких тысяч символов). Реализация декодеров таких кодов представляла трудности. В последние годы развитие микроэлектронных технологий вернуло интерес к исследованиям практических аспектов применения LDPC-кодов. Развитие новых стандартов связи, таких как IEEE 802.3an (10G Ethernet), IEEE 802.15.3c (передача данных на частоте 60 ГГц), IEEE 802.11n (WiFi), IEEE 802.16e (WiMAX), а также систем хранения данных — многоуровневой флэш-памяти, магнитных носителей с высокой плотностью хранения информации, требующих обеспечения скоростей декодирования в несколько гигабит в секунду, — привело к необходимости поиска методов кодирования/декодирования, способных функционировать на таких скоростях при одновременном обеспечении требуемого уровня помехоустойчивости.

LDPC-код задается своей проверочной матрицей H, обладающей свойством разреженности, т.е. строки и столбцы матрицы содержат мало ненулевых позиций по сравнению с ее размерностью. Определим (n, γ, ρ)-код как линейный код длины n, каждый столбец и каждая строка проверочной матрицы которого содержит соответственно γ и ρ ненулевых позиций.

Минимальное расстояние Хэмминга рассматриваемых кодов, через которое определяется число исправляемых кодом ошибок, будем обозначать d_0. Расстояние LDPC-кодов, как правило, невелико, тем не менее эти коды показывают очень хорошие результаты. Связано это, с одной стороны, с хорошими спектральными свойствами кода, т.е. в коде присутствует лишь незначительное количество слов малого веса, а с другой — с особенностями работы декодера.

Итеративный алгоритм декодирования LDPC-кодов принимает решения по каждому символу в отдельности. Таким образом, даже при большом числе возникших в канале ошибок и принятии декодером неправильного решения о кодовом слове в целом вероятность ошибки на информационный бит для LDPC-кодов может оставаться достаточно низкой.

Несмотря на большое число публикаций [1—6] задача построения эффективных LDPC-кодов далека от своего решения. В настоящей статье предлагаются некоторые подходы к построению этих кодов.

Блочно-перестановочные конструкции. Наиболее общий подход к построению LDPC-кодов, предложенный еще в работе Р. Галлагера [1], — использование проверочной матрицы H, состоящей из блоков:

$$\mathrm{H}=\begin{bmatrix} \mathrm{H}_{1,1} & \mathrm{H}_{1,2} & \dots & \mathrm{H}_{1,\rho} \\ \mathrm{H}_{2,1} & \mathrm{H}_{2,2} & \dots & \mathrm{H}_{2,\rho} \\ \dots & \dots & \dots & \dots \\ \mathrm{H}_{\gamma,1} & \mathrm{H}_{\gamma,2} & \dots & \mathrm{H}_{\gamma,\rho} \end{bmatrix}. \qquad (1)$$

В качестве блоков $\mathrm{H}_{i,j}$ могут быть выбраны, например, матрицы перестановки, в каждой строке и столбце которых содержится ровно одна единица, и тогда такая конструкция задает регулярный LDPC-код. Наиболее часто в качестве блока рассматривается матрица циклической перестановки, степень которой задает параметр циклического сдвига. Например, коды такого семейства представлены в стандартах IEEE 802.16e и IEEE 802.11n.

В случае $\gamma=2$ такие коды становятся кодами Гилберта, исследованными в [6—8]:

$$\mathrm{H}_l=\begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{I}_m & \mathrm{C} & \mathrm{C}^2 & \dots & \mathrm{C}^{l-1} \end{bmatrix}, \qquad (2)$$

где I_m — единичная $(m\times m)$-матрица, а C — $(m\times m)$-матрица циклической перестановки. Такие коды имеют минимальное расстояние $d_0=4$, однако его можно повысить, выбрав другие степени C.

Теорема 1. Пусть H_l — матрица вида (2), $Z_l=\{0,1,\dots,l-1\}$ — множество вычетов по модулю $l-1$. Тогда в коде с проверочной матрицей H_l есть слово веса 2ω, если существуют наборы чисел $\{a_i\}$, $\{b_i\}$ такие, что выполняется равенство:

$$\sum_{i=0}^{\omega-1}(-1)^i\left(a_i-b_i\right)=0 \mod m,$$

где $a_i\in Z_l, b_i\in Z_l, a_0\neq b_0, a_{\omega-1}\neq b_{\omega-1}, a_i\neq a_{i-1}, b_i\neq b_{i-1}$.

Пользуясь этой теоремой, можно показать, что если $\{z_1,\dots,z_\rho\}$ — разностное (m, ρ, 1)-множество, тогда код с проверочной матрицей

$$\mathrm{H}=\begin{bmatrix} 0 & 0 & \dots & 0 \\ \mathrm{C}^{z_1} & \mathrm{C}^{z_2} & \dots & \mathrm{C}^{z_\rho} \end{bmatrix} \qquad (3)$$

имеет длину $n=m\rho$, скорость $R=\dfrac{m(\rho-2)+1}{m\rho}$ и минимальное расстояние $d_0=6$.

Обобщим конструкцию кодов Гилберта до случая $\gamma>2$:

$$\mathrm{H}_{s,l} = \begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{C}^0 & \mathrm{C}^1 & \mathrm{C}^2 & \dots & \mathrm{C}^{l-1} \\ \mathrm{C}^{i_0^{(3)}} & \mathrm{C}^{i_1^{(3)}} & \mathrm{C}^{i_1^{(3)}} & \dots & \mathrm{C}^{i_{l-1}^{(3)}} \\ \dots & \dots & \dots & \dots & \dots \\ \mathrm{C}^{i_0^{(s)}} & \mathrm{C}^{i_1^{(s)}} & \mathrm{C}^{i_2^{(s)}} & \dots & \mathrm{C}^{i_{l-1}^{(s)}} \end{bmatrix}, \quad (4)$$

где $\mathrm{H}_{s,l}$ — $(s \times l)$-матрица, $i_j^{(k)} \in \{0,\dots,m-1\}$. Так как одним из параметров LDPC-кода является длина минимального цикла в графе, соответствующем проверочной матрице, числа $i_j^{(k)}$ в любой полосе k не должны повторяться. Тогда множество $\left\{i_j^{(k)} : j = 0, ..., l-1\right\}$ задается перестановкой различных вычетов целых чисел по модулю m.

В этом случае кодовому слову соответствует набор связанных вложенных циклов (рис. 1, γ=3), поэтому добавление полос может обеспечить увеличение расстояния LDPC-кодов.

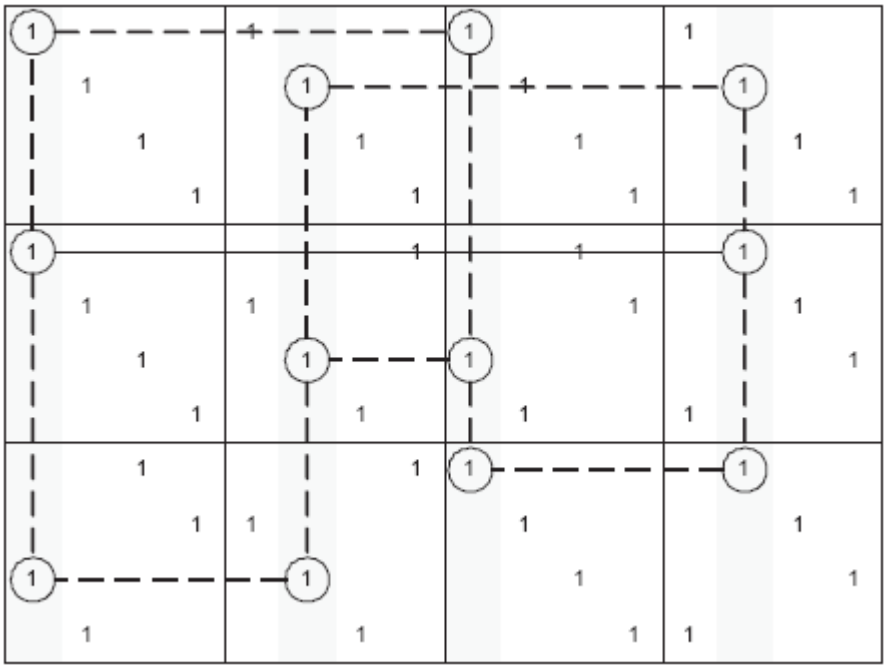

Рис. 1

В работе [9] предложено в качестве степеней матрицы циклической перестановки выбирать степени примитивного элемента матрицы Вандермонда:

$$\mathrm{H}_W = \begin{bmatrix} \mathrm{I}_m & \mathrm{I}_m & \dots & \mathrm{I}_m \\ \mathrm{I}_m & \mathrm{C} & \dots & \mathrm{C}^{\rho-1} \\ \dots & \dots & \dots & \dots \\ \mathrm{I}_m & \mathrm{C}^{\gamma-1} & \dots & \mathrm{C}^{(\gamma-1)(\rho-1)} \end{bmatrix}, \quad (5)$$

где $\rho \le m$. Такие коды имеют длину $n=m\rho$, и $\gamma + 1 \le d_0 \le 2m$.

Дальнейшую модификацию блочно-перестановочной конструкции (1) можно получить, если рассмотреть в качестве варианта заполнения блока $\mathrm{H}_{i,j}$ матрицей, состоящей из всех нулей. С одной стороны, это позволяет получать нерегулярные LDPC-коды и оптимизировать распределения весов строк и столбцов. С другой, как было показано на рис. 1, кодовым словам в блочно-перестановочной конструкции соответствуют множества вложенных циклов и

добавление нулевого блока может „разрывать“ эти циклы, уменьшая, таким образом, количество слов малого веса и улучшая спектр кода.

Выбор мест для расстановки нулевых блоков является отдельной задачей и зависит от конкретной проверочной матрицы. Несколько вариантов шаблонов, сохраняющих регулярную структуру матрицы, приведено на рис. 2.

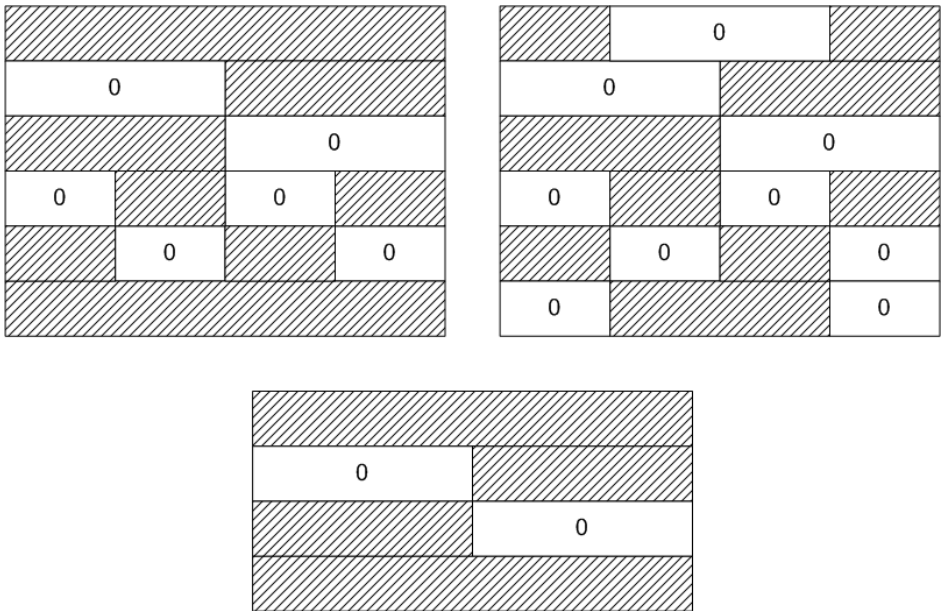

Рис. 2

На рис. 3, 4 приведены результаты моделирования описанных конструкций в канале с аддитивным белым гауссовым шумом (BER — вероятность ошибки на информационный бит; SNR — отношение сигнал/шум). На рис. 3 сравнивается классический код Гилберта (2) при $m = 29$ с кодом GGC (3), вторая полоса которого образована разностным множеством $\{0,5,7,18,19,28\}$. Код Гилберта имеет минимальное расстояние $d_0 = 4$, а у кода на основе (3) $d_0 = 6$.

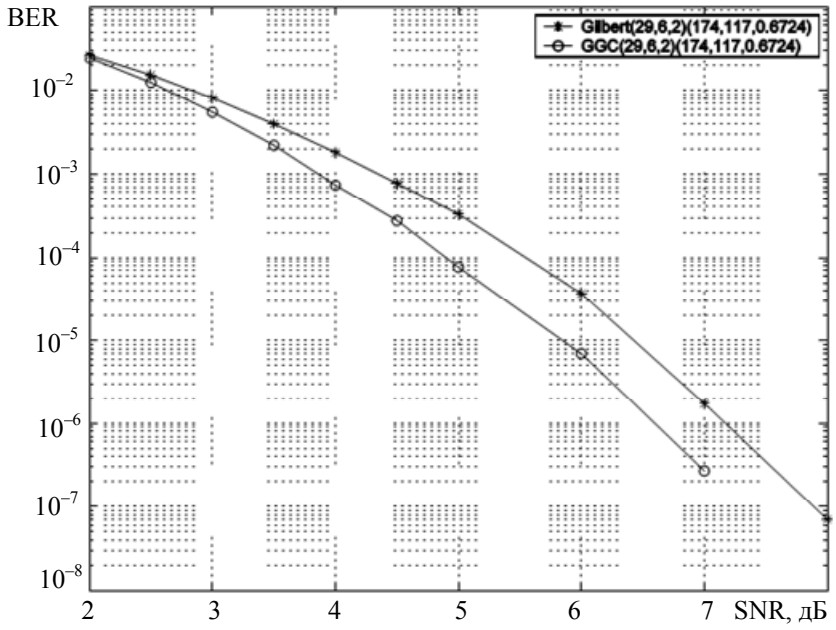

Рис. 3

На рис. 4 представлены кривые для кодов из четырех полос. Здесь W-LDPC обозначает выбор степеней в соответствии с матрицей Вандермонда (5) при $m = 79$, ρ=8, γ=4.

В качестве GGC использован код с проверочной матрицей

$$\mathrm{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 12 & 15 & 16 & 29 & 35 & 37 \\ 0 & 10 & 24 & 30 & 32 & 58 & 70 & 1 \\ 0 & 15 & 36 & 45 & 48 & 14 & 32 & 38 \end{bmatrix}, \qquad (6)$$

где $D = \{0,5,12,15,16,29,35,37\}$ — разностное множество, использованное для построения второй полосы проверочной матрицы. Третья и четвертая полосы получены как $2D \bmod 73$ и $3D \bmod 73$ соответственно. Выбранный таким образом код дает выигрыш над W-LDPC около 1 дБ при вероятности ошибки 10^{-6}.

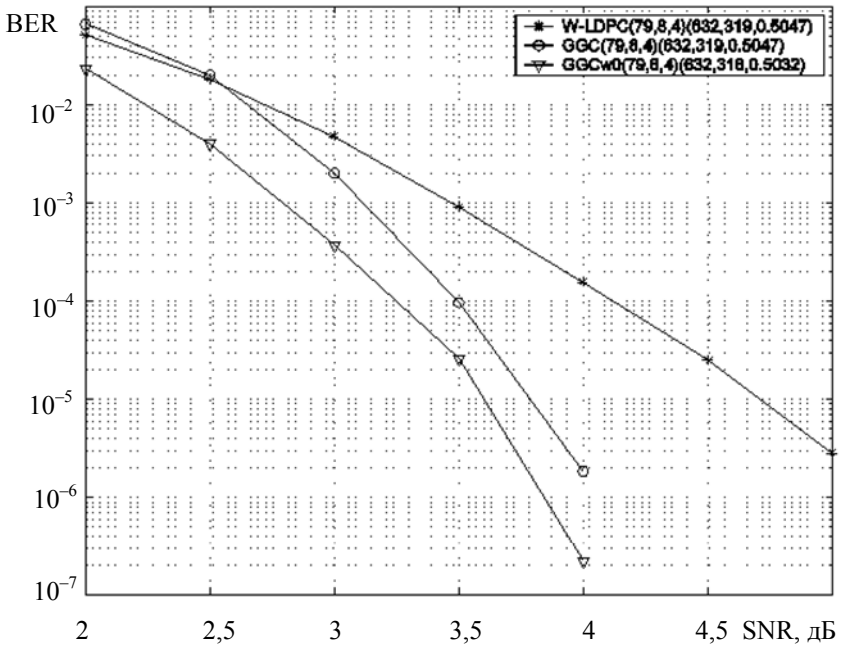

Рис. 4

Наконец, код GGCw0 соответствует проверочной матрице (6) с добавленными нулевыми блоками:

$$\mathrm{H} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 12 & -1 & 16 & -1 & 35 & -1 \\ -1 & 10 & -1 & 30 & -1 & 58 & -1 & 1 \\ 0 & 15 & 36 & 45 & 48 & 14 & 32 & 38 \end{bmatrix},$$

где -1 соответствует нулевому блоку. Полученный код является регулярным LDPC-кодом с γ=3, он дает 0,5—0,25 дБ преимущества по сравнению с первоначальным GGC кодом при одновременном снижении сложности декодирования, так как содержит меньше ненулевых позиций в проверочной матрице. Однако этот выигрыш снижается с ростом отношения сигнал/шум, так как выигрыш в спектре кода, полученный за счет нулевых блоков, дает преимущество при достаточно высоком уровне шума, однако с ростом отношения сигнал/шум, когда ошибки в канале сами по себе редки, вероятность ошибки определяется минимальным расстоянием кода.

Заключение. В настоящей статье рассмотрены подходы к построению кодов с малой плотностью проверок на четность с использованием блочно-перестановочных конструкций. Приведены методики выбора блоков на основе разностных множеств, а также подход к улучшению спектральных свойств кода на основе использования нулевых блоков.

СПИСОК ЛИТЕРАТУРЫ

1. *Gallager R. G*. Low Density Parity Check Codes. Cambridge, MA: MIT Press, 1963.

2. *Зяблов В. В., Пинскер М. С*. Оценка сложности исправления ошибок низкоплотностными кодами Галлагера // Проблемы передачи информации. 1975. Т. XI(1). С. 23—26.

3. *Белоголовый А. В., Крук Е. А*. Многопороговое декодирование кодов с низкой плотностью проверок на четность // ИУС. 2005. № 1(14). С. 25—31.

4. *Овчинников А. А*. К вопросу о построении LDPC-кодов на основе Евклидовых геометрий // ИУС. 2005. № 1(14). С. 32—40.

5. *Козлов А. В*. Декодирование LDPC-кодов в дискретном канале flash-памяти // ИУС. 2007. № 5(30). С. 31—35.

6. *Gilbert E*. A problem in binary encoding // Proc. of the Symp. in Applied Mathematics. 1960. Vol. 10. P. 291—297.

7. *Krouk E., Semenov S*. Low-density parity-check burst error-correcting codes // Proc. of 2nd Intern. Workshop on Algebraic and combinatorial coding theory. Leningrad, 1990. P. 121—124.

8. *Овчинников А. А*. Об одном классе кодов, исправляющих пакеты ошибок // Тез. докл. 2-й Междунар. школы-семинара БИКАМП'99. СПб, 1999. С. 34—35.

9. *Kabatiansky G., Krouk E., Semenov S.* Error correcting coding and security for data networks: Analysis of the superchannel concept. Wiley, 2005.

Сведения об авторах

Александр Владимирович Козлов — Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; ведущий программист; E-mail: akozlov@vu.spb.ru

Евгений Аврамович Крук — д-р техн. наук, профессор; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: ekrouk@vu.spb.ru

Андрей Анатольевич Овчинников — канд. техн. наук, доцент; Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра безопасности информационных систем; E-mail: mldoc@vu.spb.ru

Рекомендована кафедрой
№ 51 безопасности информационных систем

Поступила в редакцию
01.02.13 г.