УДК 004.6

ОБОБЩЕННЫЕ КОДЫ БОУЗА – ЧОУДХУРИ – ХОКВИНГЕМА И ИХ ПАРАМЕТРЫ

А.В. КУШНЕРОВ
(Белорусский государственный университет, Минск);
В.А. ЛИПНИЦКИЙ
(Военная академия Республики Беларусь, Минск);
М.Н. КОРОЛЁВА
(Белорусский национальный технический университет, Минск)

Проведено исследование помехоустойчивых обобщенных кодов Боуза – Чоудхури – Хоквингема. Как показало их изучение, представители данного семейства кодов имеют ряд замечательных свойств. Отдельное место отведено рассмотрению корректирующих возможностей кодов упомянутого класса и сравнению с таковыми у классических БЧХ-кодов. На представленных конкретных примерах рассмотрены некоторые параметры и особенности отдельных кодов.

Ключевые слова: *помехоустойчивые коды, минимальное расстояние кода, реверсивные коды, коды-БЧХ, норменный метод декодирования.*

Введение. Семейство кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) является классическим в теории помехоустойчивого кодирования и наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Цикличность кодов, их четкая конструктивность, возможность представления компонент синдромов ошибок элементами поля Галуа позволили развить алгебраические методы обработки этих кодов [1, 2]. Ярким образцом таких методов является коррекция ошибок БЧХ-кодами решением алгебраических уравнений в конечных полях. Теория норм синдромов (ТНС), последовательно применяя свойства автоморфизмов кодов, позволила предложить высокоскоростные перестановочные алгоритмы обработки БЧХ-кодов [3]. Эти алгоритмы оказались особенно эффективными для непримитивных кодов Хемминга и БЧХ – для коррекции ими многократных ошибок, кратность которых выходит далеко за конструктивные возможности самих кодов [4]. Логика исследования непримитивных БЧХ-кодов приводит к естественному расширению класса этих кодов с сохранением их базовых свойств. Об этом и пойдет в дальнейшем речь.

Основные определения и факты, связанные с БЧХ-кодами. В конечном поле $GF(q^m)$ из q^m элементов (расширении своего минимального подполя $GF(q)$ степени m, q – простое число) зафиксируем примитивный элемент α [1, 5]. Для всякого натурального n, делящего q^m-1, в поле Галуа $GF(q^m)$ найдется элемент β порядка n (например, $\beta=\alpha^c$ для натурального $c=(q^m-1)/n$). Зафиксируем целые числа $b\ge 0$, не делящееся на n, $\delta>1$, натуральное n, делящее или равное q^m-1, но не делящее q^s-1 для всех целых s, $0<s<m$. При этом значение δ должно быть таким, что выполняется неравенство: $m(\delta-1)<n$. В поле $GF(q^m)$ зафиксируем $\delta-1$ элементов $\beta^b, \beta^{b+1}, ..., \beta^{b+\delta-2}$. Для каждого из них в кольце полиномов $GF(\mathrm{p})[x]$ существует однозначно определенный неприводимый полином $g(\beta^i, x)$ с корнем β^i соответственно, $b\le i\le b+\delta-1$. Пусть $M(x)$ – наименьшее общее кратное полиномов $g(\beta^b, x), g(\beta^{b+1}, x), ..., g(\beta^{b+\delta-2}, x)$.

Определение 1. *Линейный циклический код* $C=J=<M(x)>$ *в кольце* $R_n=GF(\mathrm{p})[x]/<x^n-1>$ *называется кодом Боуза – Чоудхури – Хоквингема над полем* $GF(q^m)$ *длиной* n *и с конструктивным расстоянием* δ. *При* $n=q^m-1$ *элемент* $\beta=\alpha$ *и БЧХ-код* C *называют примитивным, если же* $n<q^m-1$, *код называют непримитивным.*

Согласно [1], таким образом заданный БЧХ-код C имеет в качестве одной из проверочных матриц матрицу

$$\mathrm{H}=\left[\begin{array}{cccc:c} 1 & \beta^b & \beta^{2b} & \beta^{3b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \beta^{3(b+1)} & \beta^{(n-1)(b+1)} \\ \hdashline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \beta^{3(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{array}\right]=[\beta^{bi},\beta^{(b+1)i},...,\beta^{(b+\delta-2)i}]^T, \qquad (1)$$

в которой каждый элемент β^i представляет собой столбец из m элементов поля $GF(q)$ – координат вектора β^i в базисе $\alpha^{m-1}, \alpha^{m-2}, ..., 1$.

Неравенство $m(\delta-1) < n$ гарантирует, что ядро матрицы (1) – код C – является линейным пространством над полем $GF(q)$ размерности, не меньшей, чем $n - m(\delta-1)$. Точное значение минимального расстояния БЧХ-кодов $d \le \delta$.

На практике наибольшее значение играют двоичные БЧХ-коды, то есть коды C над полем $GF(q) = GF(2)$. Здесь специализацией параметров можно существенно увеличить размерность и скорость кода. Так, при значении $b = 1$ элементы $\beta, \beta^2, \beta^4, ...$ являются сопряженными в поле $GF(2^m), m \ge 2,$ то есть являются корнями одного и того же неприводимого полинома над полем $GF(2) = Z / 2Z$ (детали см. в [1–3]). Тогда, с одной стороны, степень полинома $M(x)$ существенно уменьшится, а с другой – ранги следующих подматриц матрицы H окажутся равными: $\text{rang}[\beta, \beta^2, \beta^4, ...]^T = \text{rang}[\beta]$ [4]. Следовательно, в H подматрица $[\beta, \beta^2, \beta^4, ...]^T$ заменяется подматрицей $[\beta]$. Получаем каноническую проверочную матрицу двоичного БЧХ-кода C с конструктивным расстоянием $\delta = 2t + 1$:

$$H = [\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i}]^T. \qquad (2)$$

Размерность этого кода $k = n - mt$, а минимальное расстояние $d = 2t + 1$ в примитивном случае, как правило, а в не примитивном – велика доля кодов со значением $d > 2t + 1$ [5]. При $t = 1$ матрица (2) имеет вид $H = [\beta^i]$. Задаваемый ею код известен как код Хемминга, непримитивный при $\beta \ne \alpha$.

Цикличность означает, что код C вместе с каждым своим кодовым словом $\overline{c} = (c_1, c_2, ..., c_n)$ содержит и вектор $\sigma(\overline{c}) = (c_n, c_1, c_2, ..., c_{n-1})$ для оператора σ циклического сдвига координат векторов. Другими словами, оператор σ принадлежит группе $AutC$ автоморфизмов кода C вместе с порождаемой им циклической подгруппой Γ порядка n.

БЧХ-коды и их обобщение. Изучение циклотомических классов по различным модулям показывает, что существует бесчисленное море двоичных БЧХ-кодов с разнообразным и причудливым сочетанием сопряженных элементов в соответствующих полях Галуа и с весьма интересными упрощенными проверочными матрицами. Ряд подобных примеров дан в работах [4, 5]. Приведем еще несколько примеров.

Пример 1. Двоичные БЧХ-коды длиной 51 определены над полем Галуа $GF(2^8)$. Априори, их проверочная матрица (2) может иметь значения t в диапазоне от 1 до 6. Вычисления показывают, что по модулю 51 следующие циклотомические классы совпадают: $C_7 = C_5$; $C_{13} = C_1$; $C_{15} = C_9$. Это означает сопряженность элементов: β^{7i} и β^{5i}, β^i и β^{13i}, β^{15i} и β^{9i}. В силу сказанного выше, в БЧХ-коде с максимальным значением $t = 6$ и с проверочной матрицей $H = \left(\beta^i, \beta^{3i}, \beta^{5i}, \beta^{7i}, \beta^{9i}, \beta^{11i}\right)^T, 0 \le i \le 50,$ на самом деле подматрица $[\beta^{7i}]$ должна быть удалена. Таким образом, БЧХ-код длиной 51 с проверочной матрицей $H = \left(\beta^i, \beta^{3i}, \beta^{5i}, \beta^{9i}, \beta^{11i}\right)^T, 0 \le i \le 50,$ над полем $GF(2^8)$ имеет размерность $k = 51 - 8 \cdot 5 = 11$, его минимальное расстояние $d \ge 17$. Данный код способен исправлять все случайные ошибки весом от 1 до 8. Количество всех исправляемых ошибок равно $K = C_{51}^1 + C_{51}^2 + ... + C_{51}^8 = 773\,168\,721$.

Пример 2. Двоичные БЧХ-коды длиной 57 определены над полем $GF(2^{28})$. Здесь имеет место равенство следующих циклотомических классов: $C_7 = C_1$; $C_{13} = C_{17} = C_3$; $C_{15} = C_9 = C_3$. Следовательно, БЧХ-код длиной 57 с проверочной матрицей $H = \left(\beta^i, \beta^{3i}, \beta^{5i}\right)^T, 0 \le i \le 56,$ над полем $GF(2^{18})$ имеет размерность $k = 57 - 18 \cdot 3 = 3$, его минимальное расстояние $d \ge 19$. Данный код способен исправлять все

случайные ошибки весом от 1 до 9. Количество всех исправляемых ошибок равно $K = C_{57}^1 + C_{57}^2 + ... + C_{57}^9 = 10\,954\,161\,067$.

Пример 3. Двоичные БЧХ-коды длиной 119 определены над полем $GF(2^{24})$. Здесь имеет место равенство следующих циклотомических классов: $C_9 = C_1$; $C_5 = C_3$. Следовательно, БЧХ-код длиной 119 с проверочной матрицей $H = \left(\beta^i, \beta^{3i}, \beta^{7i}\right)^T$, $0 \le i \le 118$, имеет размерность $k = 119 - 24 \cdot 3 = 47$, его минимальное расстояние $d \ge 11$. Данный код способен исправлять все случайные ошибки весом от 1 до 5.

Пример 4. Двоичные БЧХ-коды длиной 143 определены над полем $GF(2^{60})$. Здесь имеет место равенство следующих циклотомических классов: $C_9 = C_7 = C_3 = C_1$. Следовательно, БЧХ-код длиной 143 с проверочной матрицей $H = \left(\beta^i, \beta^{5i}\right)^T$, $0 \le i \le 142$, имеет размерность $k = 23$, его минимальное расстояние $d \ge 11$. Данный код способен исправлять все случайные ошибки весом от 1 до 5.

Опираясь на изученные свойства двоичных БЧХ-кодов и приведенные примеры, возникает необходимость рассмотрения и исследования следующего класса линейных кодов.

Определение 2. Обобщенным двоичным БЧХ-кодом назовем двоичный линейный циклический код с проверочной матрицей

$$H = [\beta^{ki}, \beta^{li}, \beta^{si}, ...]^T, \tag{3}$$

где $1 \le k < l < s < ...$ и среди степеней $\beta^{ki}, \beta^{li}, \beta^{si}, ...$ не имеется ни одной пары сопряженных.

В этом случае данный код имеет конструктивное расстояние $\delta = 2t + 1$ для количества t последовательных двоичных подматриц по m строк в каждой в матрице (3), соответствующих элементам $\beta^{ki}, \beta^{li}, \beta^{si}, ...$.

По **определению 2**, к примитивным БЧХ-кодам длиной 31 и с конструктивным расстоянием 5 следует отнести не только уже ставший классическим БЧХ-код с проверочной матрицей $H = [\alpha^i, \alpha^{3i}]^T$, но и целый ряд других, к примеру, коды с проверочными матрицами $H = [\alpha^i, \alpha^{5i}]^T$, $H = [\alpha^i, \alpha^{7i}]^T$, $H = [\alpha^{3i}, \alpha^{5i}]^T$, $H = [\alpha^{3i}, \alpha^{7i}]^T$, $H = [\alpha^{5i}, \alpha^{7i}]^T$ и так далее, наконец, и реверсивный код с матрицей $H = [\alpha^i, \alpha^{30i}]^T$. Вычисления показывают, что минимальное расстояние каждого из названных кодов равно 5.

К обобщенным БЧХ-кодам применима теория норм синдромов, причем в упрощенном виде, что вовсе не является недостатком, так как облегчает вычисления и применение перестановочных методов к ним.

Обобщенные БЧХ-коды проявляют порой весьма интересные свойства.

Пример 5. Рассмотрим обобщенный БЧХ-код с конструктивным расстоянием 5 длиной 15, построенный над полем $GF\left(2^4\right)$ с примитивным полиномом $p(x) = 1 + x^3 + x^4$, проверочная матрица которого определяется формулой $H = \left(\alpha^i, \alpha^{5i}\right)^T$, $0 \le i \le 14$, где α – примитивный элемент названного поля. Согласно теории, размерность кодового пространства в данном случае равна $k = 15 - 2 \cdot 4 = 7$. Построим проверочную матрицу данного кода.

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Несложно заметить, что ранг данной матрицы равен 6, а не 8. А, следовательно, и размерность кодового пространства возрастает до 9. Дело в том, что элемент α^5 в мультипликативной группе поля $GF\left(2^4\right)$ имеет порядок 3, поэтому его степени в подматрице $\left(\alpha^{5i}\right)$ матрицы H имеют лишь три вариации, три различных столбца и, следовательно, ранг этой подматрицы $\text{rang}\left(\alpha^{5i}\right) \le 3$. Очевидно, этот ранг совпадает с рангом подматрицы из первых трех столбцов матрицы $\left(\alpha^{5i}\right)$, который, как легко видеть, равен 2. Ранг системы столбцов матрицы равен рангу системы ее строк. Все закономерно. Минимальное же расстояние этого кода равно 3, потому что сумма 5-го, 10-го и 15-го столбцов равна нулю. Это обстоятельство делает этот код не применимым на практике.

На длине 15 имеется четыре различных циклотомических класса: $C_1 = \{1, 2, 4, 8\}$; $C_3 = \{3, 6, 12, 9\}$; $C_5 = \{5, 10\}$; $C_7 = \{7, 11, 13, 14\}$ Исходя из этих свойств и **определения 2**, получим ряд БЧХ-кодов с конструктивным расстоянием 5, задаваемых проверочной матрицей вида $H = \left(\beta^{p_1 i}, \beta^{p_2 i}\right)^T$. Результаты вычислений минимального расстояния для различных комбинаций степеней p_1, p_2 представлены в таблице 1.

Таблица 1. – Параметры кодового расстояния для обобщенных БЧХ-кодов длины 15

Комбинация степеней p_1, p_2	Значение кодового расстояния
(1,3)	5
(1,5)	3
(1,7)	3
(3,5)	4
(3,7)	5
(5,7)	3

Подобные ситуации изменения параметра *k* обусловлены свойствами циклических подгрупп мультипликативной группы поля и могут проявлять себя на некоторых длинах и комбинациях степеней обобщенных БЧХ-кодов.

Конечно, реальный интерес представляют те обобщенные БЧХ-коды, чье минимальное расстояние больше конструктивного. Как и в случае непримитивных БЧХ-кодов, подобные обобщенные БЧХ-коды существуют и не являются чем-то исключительным.

Пример 6. Рассмотрим серию БЧХ-кодов с конструктивным расстоянием 5, длиной $n = 43$. Они определены над полем $GF\left(2^{14}\right)$. Сначала изучим корректирующие возможности кода с проверочной матрицей $H = \left(\beta^i, \beta^{3i}\right)^T$, $0 \le i \le 42$, где $\beta = \alpha^{\frac{2^{14}-1}{43}}$, α – примитивный элемент поля $GF\left(2^{14}\right)$, корень полинома $p(x) = 1 + x^3 + x^4 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{14}$, неприводимого над $Z/2Z$ и примитивного. Исходя из соотношения $HG^T = 0$, однозначно находим G – порождающую матрицу кода. В строках матрицы $G = \left[\overline{g}_1, \overline{g}_2, \ldots, \overline{g}_k\right]$ содержится $k = 43 - 2 \cdot 14 = 15$ базисных векторов кодового пространства. Тогда, по определению порождающей матрицы кода, любое кодовое слово $\overline{c}$ может быть получено как линейная комбинация строк матрицы G: $\overline{c} = \sum_{j=1}^{k} \overline{g}_j \cdot l_j$, где $l_j \in GF(2)$. Несложно вычислить, что все кодовое пространство данного БЧХ-кода содержит в точности $2^{15} = 32768$ векторов. Относительно небольшое количество кодовых слов открывает перспективы для подсчета минимального расстояния полным перебором кодового пространства. В ходе проведения необходимых вычислений устанавливаем, что минимальное расстояние данного кода равно 13. Найденное значение кодового расстояния подтверждает гистограмма весов кодовых слов.

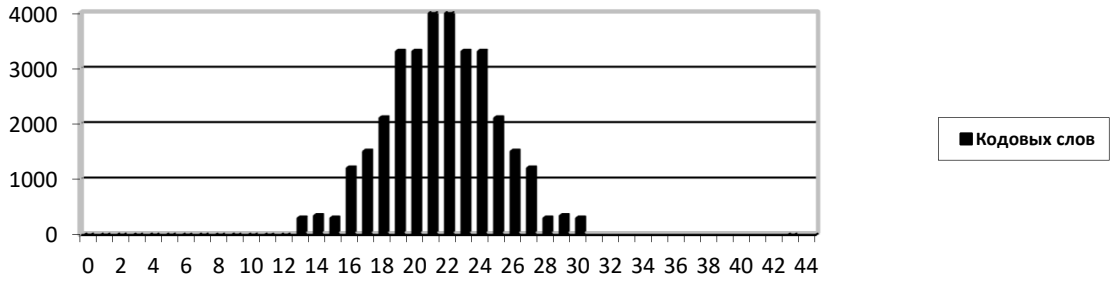

Рисунок 1. – Диаграмма весов кодовых слов классического БЧХ-кода длины 43

Попробуем вычислить аналогичным методом минимальное расстояние других БЧХ-кодов с конструктивным расстоянием 5 на длине 43. Общий вид проверочной матрицы для таких кодов $H = \left(\beta^{p_1 i}, \beta^{p_2 i}\right)^T$. На длине 43 имеются лишь три различных циклотомических класса:

$$C_1 = \{1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42\};$$
$$C_3 = \{3, 5, 6, 10, 12, 19, 20, 23, 24, 31, 33, 37, 38, 40\};$$
$$C_7 = \{7, 9, 13, 14, 15, 17, 18, 25, 26, 28, 29, 30, 34, 36\}.$$

Исходя из свойств циклотомических классов, определим комбинации степеней p_1, p_2 для изучения. В таблице 2 представлены найденные комбинации и значения минимального расстояния для обобщенных БЧХ-кодов длиной 43.

Таблица 2. – Параметры кодового расстояния для обобщенных БЧХ-кодов длины 43

Комбинация степеней p_1, p_2	Значение кодового расстояния
(1,3)	13
(1,7)	13
(3,7)	13

Видим, что корректирующие возможности различных БЧХ-кодов сходны с таковыми у классического кода с проверочной матрицей $H = \left(\beta^i, \beta^{3i}\right)$ и превосходят конструктивные.

Пример 7. Рассмотрим обобщенный БЧХ-код длиной $n = 69$, который определен над полем $GF\left(2^{22}\right)$ с примитивным полиномом $p(x) = 1 + x^{21} + x^{22}$. Здесь также имеются только три различных циклотомических класса и возможны лишь три различных БЧХ-кода. При подсчете минимального расстояния всех трех различных обобщенных БЧХ-кодов на данной длине можно обнаружить необычные свойства.

Таблица 3. – Параметры кодового расстояния для обобщенных БЧХ-кодов длины 69

Комбинация степеней p_1, p_2	Значение кодового расстояния
(1,3)	7
(1,15)	11

Как видим, в некоторых случаях минимальное расстояние обобщенного БЧХ-кода может и превышать минимальное расстояние классического БЧХ-кода на той же длине.

Заключение. Логика исследований семейства кодов Боуза – Чоудхури – Хоквингема приводит к необходимости рассмотрения обобщенных БЧХ-кодов. Как показывают первые исследования, обобщенные БЧХ-коды требуют более осторожного и тщательного подхода к ним.

Внешне стандартные задания этих кодов могут характеризоваться нетипичными особенностями: неожиданное увеличение размерности кода, всплески минимального расстояния как в сторону увеличе-

ния, так и в сторону уменьшения по сравнению с классическими БЧХ-кодами, тем не менее вводимый класс кодов обещает новые примеры, перспективные для приложений.

ЛИТЕРАТУРА

1. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки : пер. с англ. / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.
2. Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М. : Мир, 1986. – 576 с.
3. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В.А. Липницкий, В.К. Конопелько. – Минск : Издат. центр БГУ, 2007. – 216 с.
4. Липницкий, В.А. Теория норм синдромов и плюс-декодирование / В.А. Липницкий, А.О. Олексюк // Доклады БГУИР. – 2014. – № 8. – С. 71–78.
5. Лидл, Р. Конечные поля : в 2 т. : пер. с англ. / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988.
6. Липницкий, В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа / В.А. Липницкий. – 2-е изд. – Минск : БГУИР, 2006. – 88 с.
7. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М. : Наука, 1972. – 168 с.

Поступила 20.03.2018

PROPERTIES AND OPTIONS OF THE GENERIC BCH-CODES

A. KUSHNEROV, V. LIPINSKI, M. KOROLIOVA

This work is devoted to generic error-correcting BCH-codes investigation. During investigations we can make some interesting conclusions about its properties. Also we consider correcting possibilities of this codes in comparison with classic BCH-codes. There are some examples of codes in this work. Those examples show parameters and features of generic BCH-codes.

Keywords: *error correcting codes, code minimal distance, reverse codes, BCH-codes, norm method of error correction.*