УДК 621.391

НЕКТОРЫЕ СВОЙСТВА ОБОБЩЁННЫХ БЧХ-КОДОВ

В.А. ЛИПНИЦКИЙ[1], А.В. КУШНЕРОВ[2]

[1]Военная академия Республики Беларусь,[2]Белорусский государственный университет, Республика Беларусь

Поступила в редакцию 30 марта 2020

Аннотация. Произведена достаточно точная оценка количества различных обобщенных БЧХ-кодов (ОБЧХ-кодов) на каждой конкретной длине. Установлен ряд свойств и взаимосвязей этих кодов. Наиболее подробно рассмотрены ОБЧХ-коды с конструктивным расстоянием три и пять, поскольку подобные БЧХ-коды чаще всего и используются в реальных инфокоммуникационных системах. Дано практически полное описание названных кодов в диапазоне длин от 7 до 107.

Ключевые слова: линейные циклические коды, минимальное расстояние кода, проверочная матрица кода, БЧХ-коды, ОБЧХ-коды.

Введение

Коды Боуза-Чоудхури-Хоквингема – один из самых изученных и применяемых классов линейных помехоустойчивых кодов. Эти коды успешно зарекомендовали себя на практике. Свойства БЧХ-кодов располагают к успешному применению алгебраических методов для обнаружения и исправления ошибок [1]. В частности, единственным методом для исправления ошибок большой кратности в БЧХ-кодах являются методы теории норм синдромов (ТНС). В ходе исследования данного класса кодов и разработки методов декодирования возникла необходимость расширения класса БЧХ-кодов, что привело к рассмотрению обобщённых БЧХ-кодов. Такие коды сохраняют свойства семейства БЧХ, однако всё же требуют более детального исследования [5]. На определённых длинах ОБЧХ-коды демонстрируют корректирующие возможности, превосходящие таковые у классических кодов данного семейства [3,4].

Обобщённые БЧХ-коды

Пусть n – фиксированное число, превосходящее 1 и не кратное 2. В силу малой теоремы Ферма существует наименьшее натуральное число m, такое, что: $2^m - 1$ делится на n, тогда $2^m - 1 = n \cdot \nu$ для некоторого натурального $\nu \geq 1$. Пусть $GF(2^m)$ – конечное поле из 2^m элементов с примитивным элементом α. Тогда $\beta = \alpha^\nu$ – элемент поля $GF(2^m)$ порядка n. Далее, пусть t – натуральное число, такое что $mt < n$.

Обобщённым двоичным (n, k) – кодом БЧХ размерности $k = n - mt$ над полем Галуа $GF(2^m)$ называется линейный циклический код $C = C_n = C_n^{k_1, k_2, ..., k_e} = C_n(k_1, k_2, ..., k_t)$ с проверочной матрицей

$$H = H_n(k_1, k_2, ..., k_t) = [\beta^{k_1 i}, \beta^{k_2 i}, ..., \beta^{k_t i}]^T, \quad (1)$$

где $1 \leq k_1 < k_2 < ... < k_t \leq n-1$, $\beta = \alpha^b$ для $b = (2^m - 1)/n$, i последовательно принимает все целые значения в диапазоне $0 \leq i \leq n-1$, предполагается, что среди степеней $\beta^{k_1}, \beta^{k_2}, ..., \beta^{k_t}$ не имеется ни одной пары сопряженных в поле Галуа [6]. Говорим, что данный код имеет конструктивное расстояние $\delta = 2t + 1$.

Как и в классических БЧХ-кодах, в матрице (1) каждый элемент $\beta^{k_j i}$ заменен столбцом из координат этого элемента как $m-$мерного вектора линейного пространства $GF(2^m)$ над полем $GF(2)$ с базисом $\alpha^{m-1}, \alpha^{m-2}, ..., \alpha, 1.$

Стоит отметить, что порядок следования подматриц степеней элементов $\beta^{k_1}, \beta^{k_2}, ..., \beta^{k_t}$ не имеет значения, также любой из этих элементов может быть заменён на сопряжённый в поле Галуа. Из определения видно, что при условии $mt < n$ существует C_μ^t различных ОБЧХ-кодов длины n, где $\mu-$ количество циклотомических классов множества $T_n = \{1, 2, \ldots n-1\}$. Особняком в этом множестве кодов стоят ОБЧХ-коды с проверочной матрицей $H_n(1, k_2, ..., k_t)$, в которой одна из степеней равна 1: такой код называют ОБЧХ-кодом в узком смысле.

Внешнее отличие определения ОБЧХ-кода от определения классического БЧХ-кода (см. [1, 2]) устанавливается видом матрицы (1): у БЧХ-кода $k_{j+1} = k_j + 1$ для каждого $j, 2 \le j \le t.$ У нас такие ограничения отсутсвуют. Потребности практики рассчитывают на возможно большое значение размерности k кода. Этому требованию удовлетворяют БЧХ-коды в узком смысле – когда $k_1 = 1.$ В этом случае все четные степени β являюся сопряженными с теми или иными предыдущими степенями этого элемента. Но тогда соответствующие подматрицы проверочной матрицыв БЧХ-кода эквивалентны друг другу (теорема 6.3 [3]). Поэтому у проверочной матрицы двоичного БЧХ-кода остаются только нечетные степени. Этим же фактом объясняется наше требование об отсутствии сопряженных элементов в матрице (1).

Задание кодов матрицей (1) почти автоматически означает, что все ОБЧХ-коды являются помехоустойчивыми линейными циклическими кодами.

К примеру, для числа $n = 15$ разбиение на циклотомические классы выглядит следующим образом: $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 9, 12\}$, $C_5 = \{5, 10\}$, $C_7 = \{7, 11, 13, 14\}$, что гарантирует существование $C_4^2 = 6$ ОБЧХ-кодов длины 15 с конструктивным расстоянием 5: $C_{15}^{1,3}, C_{15}^{1,5}, C_{15}^{1,7}, C_{15}^{3,7}, C_{15}^{3,5}, C_{15}^{5,7}$. Коды $C_{15}^{1,3}, C_{15}^{1,5}, C_{15}^{1,7}$ будут обобщёнными БЧХ-кодами в узком смысле.

Классификация ОБЧХ-кодов

Множество ОБЧХ-кодов на конктретной длине требуется нужным образом классифицировать согласно их корректирующим возможностям. Это позволяет без лишних вычислительных экпериментов выделить перспективыные коды, только исходя из вида проверочной матрицы.

Как известно из классической теории кодирования, эквивалетные коды – это коды, которые отличаются только перестановкой отсчётов. Исходя из этого, множество из C_μ^t обощённых БЧХ-кодов заданной длины n может быть разбито на классы эквивалетности. В этом случае, для рассмотрения достаточно сосредоточиться на одном коде из класса, так как все остальные будут иметь в точности аналогичные свойства. Количество таких классов сложно спрогнозировать – требуется проведение отдельных вычислений для каждой длины и конструктивного расстояния.

Рассмотрим такое разбиение на примере обобщённого БЧХ-кода длины 15 с конструктивным расстоянием 5. Согласно определению, проверочная матрица кода $C_{15}^{1,3}$ имеет вид:

$$H_{15}(1,3) = \begin{pmatrix} 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ \alpha^8\ \alpha^9\ \alpha^{10}\ \alpha^{11}\ \alpha^{12}\ \alpha^{13}\ \alpha^{14} \\ 1\ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12}\ 1\ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12}\ 1\ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12} \end{pmatrix}.$$

Далее выпишем проверочную матрицу кода $C_{15}^{3,11}$:

$$H_{15}(3,11)=\begin{pmatrix}1\,\alpha^3\,\alpha^6\,\alpha^9\,\alpha^{12} & 1 & \alpha^3\,\alpha^6\,\alpha^9\,\alpha^{12} & 1\,\alpha^3\,\alpha^6\,\alpha^9\,\alpha^{12}\\ 1\,\alpha^{11}\,\alpha^7\,\alpha^3\,\alpha^{14}\,\alpha^{10}\,\alpha^6\,\alpha^2\,\alpha^{13}\,\alpha^9\,\alpha^5\,\alpha\,\alpha^{12}\,\alpha^8\,\alpha^4\end{pmatrix}.$$

Нетрудно заметить, что данные матрицы отличаются лишь перестановкой столбцов, что означает их эквивалентность. Рассуждая далее, согласно разбиению на циклотомические классы множества T_{15}, $C_7=\{7,11,13,14\}$, что влечёт за собой полное совпадение кодов $C_{15}^{3,11}$ и $C_{15}^{3,7}$, а значит можно сделать вывод об эквивалентности кодов $C_{15}^{1,3}$ □ $C_{15}^{3,7}$. Продолжая подобные рассуждения, получим полное разбиение ОБЧХ-кодов длины 15 с конструктивным расстоянием 5 на 4 класса эквивалентности: $\left(\{C_{15}^{1,3},C_{15}^{3,7}\},\{C_{15}^{1,5},C_{15}^{5,7}\},\{C_{15}^{1,7}\},\{C_{15}^{3,5}\}\right)$.

Обобщённые БЧХ-коды в узком смысле более удобны для обработки и декодирования, поэтому необходимо чёткое условие, при котором ОБЧХ-код может быть приведён к ОБЧХ-коду в узком смысле. В ходе исследования было установлено, что для ОБЧХ-кода длины n с проверочной матрицей $H_n(k_1,k_2,\dots k_t)$ достаточно выполнение условия $\text{НОД}(k_j,n)=1,\quad 1\le j\le t$, хотя бы для одного значения k_j, чтобы его можно было привести к ОБЧХ-коду в узком смысле. Иными словами, код, для которого будет выполнено указанное условие, эквивалентен ОБЧХ-коду в узком смысле.

Очевидно, что любой код представляет интерес в практическом плане только при приемлемых корректирующих возможностях. Число ошибок, которое способен обнаружить и исправить код линейно зависит от минимального расстояния кода. Вычисление этого параметра – трудоёмкая алгоритмическая задача, не всегда имеющая решение. К основным методикам нахождения минимального расстояния относят: метод рангов систем столбцов проверочной матрицы, полный перебор кодового пространства, метод синдромов и метод норм, базирующийся на теории норм синдромов.

Однако, прежде чем приступать к компьютерным вычислениям следует провести теоретическую оценку минимального расстояния там, где это возможно. По внешнему виду проверочной матрицы ОБЧХ-кода можно в определённых случаях однозначно установить минимальное расстояние кода. В частности, в случае если для проверочной матрицы ОБЧХ-кода длины n, имеющей вид $H_n(k_1,k_2,\dots k_t)$, выполнено условие $\text{НОД}(k_1,k_2,\dots k_t,n)>1$, то такой код имеет минимальное расстояние два. В такой ситуации помехоустойчивый код не представляет практического интереса. Классический БЧХ-код длины n с конструктивным расстоянием δ, с проверочной матрицей $H_n(1,3,5,\dots\delta-2)$ всегда имеет минимальное расстояние $d\ge\delta$. Такой код является лишь частным случаем ОБЧХ-кода и его свойства не всегда можно экстраполировать на все обобщённые коды данной длины. Нахождение полного спектра минимальных расстояний для ОБЧХ-кодов требует детального компьютерного эксперимента.

ОБЧХ-коды с конструктивным расстоянием 5 в диапазоне длин от 7 до 107

Все рассматриваемые в данной работе коды имеют нечетные длины. В диапазоне от 7 до 107 имеется 51 нечетных длин. Для каждой из них имеется своё поле определения – поле Галуа $GF(2^m)$ с наименьшим m, таким, что 2^m-1 делится на n. Для 12 простых длин рассматриваемого диапазона $m=n-1$. Это длины: 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107. На этих длинах имеются только коды Хемминга размерностью $k=1-$ не представляющие практического интереса. На ещё четырех длинах также имеются только коды Хемминга, хотя и большей размерности. Это длины: 9 ($m=6$): 25 ($m=20$); 27 ($m=18$); 81 ($m=54$). Ещё для 8 длин рассматриваемого диапазона имеются БЧХ-коды с конструктивным расстоянием 5, но с размерностью $k=1-$ также не представляющие практического интереса. Это длины: 7, 17, 23, 41, 47, 71, 79, 97, 103.

В указанном диапазоне осталось 26 длин (более половины длин) с приемлемым значением m, допускающим БЧХ-коды с конструктивным расстоянием 5 и с размерностью

$k > 1$. Это длины: 15, 21, 31, 33, 35, 39, 43, 45, 49, 51, 55, 57, 63, 65, 69, 73, 75, 77, 85, 87, 89, 91, 93, 95, 99, 105. Для каждой из перечисленных 26 длин проведено исследование всех ОБЧХ-кодов $C_n(k_1, k_2)$ и их свойств: установлены их вид и общее количество, проведено разбиение найденных кодов на классы эквивалентности; проведено вычисление минимальных расстояний каждого из кодов – представителей классов эквивалентности – с помощью комбинаторной теоремы, связанной с рангами систем столбцов проверочной матрицы. Основные результаты вычислений приведены в табл. 1. В предпоследнем столбце таблицы представлено наименьшее из минимальных расстояний рассматриваемых кодов данной длины – *mindmin*, а в последнем столбце – наибольшее из этих минимальных расстояний – *maxdmin*.

Таблица 1. **Параметры ОБЧХ-кодов $(\delta = 5)$ в диапазоне длин от 9 до 105**

№	n	m	Количество кодов	Количество экв. классов	$d_{C_n^{1,3}}$	*mindmin*	*maxdmin*
1	15	4	6	4	5	3	4
2	21	6	10	6	5	2	3
3	31	5	15	3	5	5	5
4	33	10	6	4	10	3	4
5	35	12	10	6	5	2	6
6	39	12	6	4	10	3	4
7	43	14	3	1	13	13	13
8	45	12	21	15	5	2	5
9	49	21	6	4	7	2	4
10	51	8	21	7	5	2	5
11	55	20	6	4	5	4	11
12	57	18	6	4	14	3	4
13	63	6	66	22	5	2	4
14	65	12	15	5	5	4	8
15	69	22	10	6	7	2	11
16	73	9	28	4	6	6	6
17	75	20	21	15	5	2	4
18	77	30	10	6	7	2	6
19	85	8	55	9	5	2	5
20	87	28	6	4	22	3	4
21	89	11	28	4	7	7	7
22	91	12	36	8	7	2	6
23	93	10	78	26	5	2	5
24	95	36	6	4	–	4	14
25	99	30	21	15	9	2	6
26	105	12	91	45	5	2	4

В табл. 1 представлены, как минимум, 4 новых ОБЧХ-кода, существенно превосходящие по своим корректирующим возможностям классические БЧХ-коды на тех же длинах, перспективные для дальнейших исследований и применений. К ним относятся коды на длинах: 55, 65, 69, 95 с минимальными расстояниями соответственно: 11, 8, 11, 14.

Заключение

В теорию и практику помехоустойчивого кодирования введено понятие обобщённого кода Боуза-Чоудхури-Хоквингема. Проведенная классификация таких кодов, а именно, разбиение их на классы эквивалентности, позволяет систематизировать знания по данному семейству кодов и чётко выделить перспективные коды с точки зрения их практического применения. Сформулированы условия приведения ОБЧХ-кода к более удобному виду – ОБЧХ-коду в узком смысле. При детальном изучении свойств ОБЧХ-кодов в выборке длин от 7 до 107 было установлено, что на определенных длинах корректирующие возможности ОБЧХ-кодов превосходят таковые у классических БЧХ-кодов.

Таким образом, найдены новые линейные циклические коды, близкие по построению и свойствам к классическим БЧХ-кодам. В ближайшей перспективе – доказательство того факта, что к ОБЧХ-кодам относится семейство квадратично-вычетных кодов. К обработке данного

класса кодов применимы методы теории полей Галуа, возможен перенос теории норм синдромов на новый класс кодов.

SOME PROPERTIES OF GENERIC BCH CODES

V.A. LIPNITSKI, A.V. KUSHNEROV

Abstract. This work is dedicated to generic BCH codes. Accurate estimation of quantity for that types of codes was carried out. Properties and correction possibilities of generic BCH codes were also considered. The main attention was paid to codes with constructive distance 5 and 3, because these codes are most applicable in practice. For the research, a range of lengths from 7 to 107 was chosen.

*Keywords:*linear cyclic codes, minimum code distance, code verification matrix, BCH codes, generic BCH codes.

Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. Перевод с англ. – М.: Связь, 1979.
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.
3. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн.: Издательский центр БГУ, 2007.
4. Липницкий В.А., Олексюк А.О. //Доклады БГУИР, 2014, №8. С. 71 – 78.
5. Кушнеров А.В., Липницкий В.А., Королёва М.Н. // Вестник Полоцкого государственного университета. Серия С. «Фундаментальные науки», 2018, №4. С. 28 – 33.
6. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. Пер. с англ. М.: Мир, 1988.