ISSN 1561-2430 (Print)
ISSN 2524-2415 (Online)
УДК 004.6
https://doi.org/10.29235/1561-2430-2020-56-2-157-165

Поступила в редакцию 19.07.2019
Received 19.07.2019

А. В. Кушнеров[1], В. А. Липницкий[2], М. Н. Королева[3]

[1]Белорусский государственный университет, Минск, Беларусь
[2]Военная академия Республики Беларусь, Минск, Беларусь
[3]Белорусский национальный технический университет, Минск, Беларусь

СВОЙСТВА И ПАРАМЕТРЫ ОБОБЩЕННЫХ КОДОВ БОУЗА – ЧОУДХУРИ – ХОКВИНГЕМА

Аннотация. Семейство линейных циклических кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) относится к классу наиболее популярных в теории и наиболее массовых в практическом применении помехоустойчивых кодов. Их тесная связь с теорией полей Галуа позволила создать для БЧХ-кодов теорию норм синдромов – синдромных инвариантов Г-орбит ошибок, развить теорию полиномиальных инвариантов G-орбит ошибок. Данная теория в целом послужила основой разработки эффективных перестановочных полиномиально-норменных методов и алгоритмов коррекции ошибок, на порядок снижающих влияние проблемы селектора. На сегодняшний день эти методы представляют единственный подход к коррекции ошибок непримитивными БЧХ-кодами, кратность которых выходит за пределы конструктивных границ.

Настоящая работа посвящена определению и исследованию помехоустойчивых обобщенных двоичных кодов Боуза – Чоудхури – Хоквингема (ОБЧХ-кодов). Произведена достаточно точная оценка количества этих кодов каждой конкретной длины. Установлен ряд свойств и взаимосвязей ОБЧХ-кодов. Наиболее подробно рассмотрены ОБЧХ-коды с конструктивным расстоянием три и пять, так как подобные коды чаще всего и используются на практике. Дано их практически полное описание в диапазоне длин от 7 до 107. Работа содержит достаточно четкую теоретическую классификацию ОБЧХ-кодов. Особое внимание уделено корректирующим возможностям кодов данного класса – расчету минимальных расстояний этих кодов с различными параметрами. Найдены коды, корректирующие возможности которых существенно превосходят таковые у известных БЧХ-кодов с теми же конструктивными параметрами.

Ключевые слова: помехоустойчивые коды, минимальное расстояние кода, циклотомические классы, коды Хемминга, БЧХ-коды, обобщенные БЧХ-коды

Для цитирования. Кушнеров, А. В. Свойства и параметры обобщенных кодов Боуза – Чоудхури – Хоквингема / А. В. Кушнеров, В. А. Липницкий, М. Н. Королева // Вес. Нац. акад. навук Беларусі. Сер. фіз.-мат. навук. – 2020. – Т. 56, № 2. – С. 157–165. https://doi.org/10.29235/1561-2430-2020-56-2-157-165

Alexander V. Kushnerov[1], Valery A. Lipniski[2], Maria N. Koroliova[3]

[1]Belarusian State University, Minsk, Belarus
[2]Military Academy of the Republic of Belarus Minsk, Belarus
[3]Belarusian National Technical University, Minsk, Belarus

THE PROPERTIES AND PARAMETERS OF GENERIC BOSE – CHAUDHURI – HOCQUENGHEM CODES

Abstract. The Bose – Chaudhuri – Hocquenghem type of linear cyclic codes (BCH codes) is one of the most popular and widespread error-correcting codes. Their close connection with the theory of Galois fields gave an opportunity to create a theory of the norms of syndromes for BCH codes, namely, syndrome invariants of the G-orbits of errors, and to develop a theory of polynomial invariants of the G-orbits of errors. This theory as a whole served as the basis for the development of effective permutation polynomial-norm methods and error correction algorithms that significantly reduce the influence of the selector problem. To date, these methods represent the only approach to error correction with non-primitive BCH codes, the multiplicity of which goes beyond design boundaries.

This work is dedicated to a special error-correcting code class – generic Bose – Chaudhuri – Hocquenghem codes or simply GBCH-codes. Sufficiently accurate evaluation of the quantity of such codes in each length was produced during our work. We have investigated some properties and connections between different GBCH-codes. Special attention was devoted to codes with constructive distances of 3 and 5, as those codes are usual for practical use. Their almost complete description is given in the range of lengths from 7 to 107. The paper contains a fairly clear theoretical classification of GBCH-codes. Special attention is paid to the corrective capabilities of the codes of this class, namely, to the calculation of the minimal distances of these codes with various parameters. The codes are found whose corrective capabilities significantly exceed those of the well-known GBCH-codes with the same design parameters.

Keywords: error correcting codes, code minimal distance, reverse codes, bch codes, Hamming codes

For citation. Kushnerov A. V., Lipinski V. A., Koroliova M. N. The properties and parameters of generic Bose – Chaudhuri – Hocquenghem codes. *Vestsi Natsyianal'nai akademii navuk Belarusi. Seryia fizika-matematychnykh navuk = Proceedings of the National Academy of Sciences of Belarus. Physics and Mathematics series*, 2020, vol. 56, no. 2, pp. 157–165 (in Russian). https://doi.org/10.29235/1561-2430-2020-56-2-157-165

Введение. Семейство кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) – классическое в теории помехоустойчивого кодирования – является наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Свойства цикличности этих кодов и четкой конструктивности, возможность представления компонент синдромов ошибок как элементов поля Галуа – все это позволило развить и расширить алгебраические методы обработки названных кодов [1, 2]. Среди них – коррекция ошибок в БЧХ-кодах 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, единственно возможными для коррекции в них многократных ошибок, кратность которых выходит далеко за конструктивные возможности самих кодов [4]. Логика исследования непримитивных БЧХ-кодов привела к естественному расширению класса этих кодов с сохранением их базовых свойств – к рассмотрению обобщенных БЧХ-кодов [5]. Данная работа посвящена развитию теории предложенного расширенного класса БЧХ-кодов.

Обобщенные коды Хемминга и их основные свойства. Пусть n – фиксированное нечетное число, большее 1. Пусть m – наименьшее натуральное число с условием: $2^m - 1$ делится на n: $2^m - 1 = n \cdot \nu$ для некоторого натурального $\nu \geq 1$. Пусть $GF(2^m)$ – поле Галуа из 2^m элементов с примитивным элементом α. Тогда $\beta = \alpha^\nu$ – элемент поля $GF(2^m)$ порядка n. Более точно, по своему построению – это корень некоторого неприводимого и непримитивного полинома $f_\beta(x)$ m-й степени и показателя n. Как известно, остальные $m - 1$ корней полинома $f_\beta(x)$ принадлежат полю $GF(2^m)$, строятся с помощью степеней автоморфизма Фробениуса $f : x \to x^2$, следовательно, они имеют вид: $\beta^2, \beta^4, ..., \beta^{2^{m-1}}$ [6, 7]. Их принято называть сопряженными с элементом β. Зафиксируем натуральное k в диапазоне $1 \leq k \leq n-1$. Очевидно, $\gamma = \beta^k \neq 1$. Следовательно, γ не принадлежит минимальному подполю $GF(2)$ поля $GF(2^m)$, как и сопряженный с ним элемент $\gamma^2 \neq \gamma$.

Определение 1. Обобщенным двоичным кодом Хемминга $\tilde{N}^k_{\chi,n}$ длины n называется линейный код с проверочной матрицей

$$H^k_{\chi,n} = [\beta^{ki}] = \left(1, \beta^k, \beta^{2k}, \beta^{3k}, ..., \beta^{k(n-1)}\right). \quad (1)$$

Таким образом, формально, имеется $n - 1$ различных обобщенных кодов Хемминга длиной n. Покажем, что в реальности их имеется существенно меньше.

Предложение 1. *В принятых выше обозначениях для сопряженных элементов* γ *и* γ^2 *обобщенные коды Хемминга длины n с проверочными матрицами* $H_1 = [\gamma^i]$ *и* $H_2 = [\gamma^{2i}]$ *совпадают.*

Доказательство сводится к установлению того факта, что ядра матриц H_1 и H_2 совпадают. Введем следующее обозначение: пусть $(i_1, i_2, ..., i_l)$ – вектор с координатами 0 и 1, у которого координаты 1 стоят на местах с номерами $i_1, i_2, ..., i_l$. Пусть $\overline{c} = (i_1, i_2, ..., i_\varpi)$ – кодовое слово первого кода, т. е. вектор из ядра матрицы H_1. Это означает, что произведение

$$H_1 \cdot \overline{c}^T = \gamma^{i_1 - 1} + \gamma^{i_2 - 1} + ... + \gamma^{i_\varpi - 1} = 0.$$

Умножим матрицу H_2 на этот же вектор. Получим

$$H_2 \cdot \overline{c}^T = \gamma^{2(i_1 - 1)} + \gamma^{2(i_2 - 1)} + ... + \gamma^{2(i_\varpi - 1)} = (\gamma^{i_1 - 1} + \gamma^{i_2 - 1} + ... + \gamma^{i_\varpi - 1})^2 = 0^2 = 0,$$

что и требовалось доказать.

Следствие 1. *Проверочные матрицы* $H^k_{\chi,n} = [\beta^{ki}]$ *и* $H^l_{\chi,n} = [\beta^{li}]$ *с сопряженными в поле Галуа GF*(2^m) *элементами* β^k *и* β^l *задают один и тот же обобщенный код Хемминга.*

Множество $T_\beta = \{\beta, \beta^2, ..., \beta^{n-1}\}$ замкнуто относительно действия автоморфизма Фробениуса, а потому разбивается на непересекающиеся классы сопряженных друг с другом элементов, составляющих совокупность всех корней того или иного неприводимого над полем *GF*(2) полинома μ-й степени, где, как правило, μ = *n* или же является делителем *n*. Отсюда вытекает

Следствие 2. *Количество различных обобщенных кодов Хемминга длины n меньше, либо равно количеству* N_β *всех неприводимых над полем GF*(2) *полиномов с корнями* $\beta^k, 1 \le k \le (n-1)$.

Показатели степеней элементов из множества T_β образуют множество $T_n = \{1, 2, ..., n-1\}$. Разбиению T_β на подмножества корней неприводимых полиномов взаимно-однозначно соответствует разбиение множества *T* на непересекающиеся циклотомические классы по модулю *n* [1], обращение с которыми проще и удобнее, чем с полиномами. Следствие 2 можно переформулировать следующим образом.

Следствие 3. *Количество различных обобщенных кодов Хемминга длины n меньше, либо равно количеству* N_n *всех циклотомических классов по модулю n, на которые разбивается множество* T_n.

Пример 1. Исследуем все возможные коды Хемминга длины 15. Эти коды определены над полем *GF*(2^4). Зафиксируем примитивный элемент α как корень полинома $x^4 + x + 1$. Очевидно, остальными корнями этого полинома являются $\alpha^2, \alpha^4, \alpha^8$. Им соответствует циклотомический класс $C_1 = \{1, 2, 4, 8\}$. Рассмотрим обратные по умножению элементы к корням полинома $x^4 + x + 1$: $\alpha^{14}, \alpha^{13}, \alpha^{11}, \alpha^7$. Эти элементы будут корнями полинома $x^4 + x^3 + 1$. Показатели этих корней образуют циклотомический класс по модулю 15 $C_7 = \{7, 14, 13, 11\}$. Элементы α^5, α^{10} принадлежат полю *GF*(2^2), так как они являются корнями полинома $x^2 + x + 1$. Их показатели образуют отдельный циклотомический класс $C_5 = \{5, 10\}$. Оставшиеся, пока не рассмотренные элементы поля *GF*(2^4), – $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ являются корнями неприводимого и непримитивного полинома 4-й степени $x^4 + x^3 + x^2 + x + 1$. Их показатели образуют циклотомический класс $\tilde{N}_3 = \{3, 6, 12, 9\}$. Классический код Хемминга $\tilde{N}^1_{\chi,15}$ с проверочной матрицей $H^1_{\chi,15} = [\alpha^i] = (1, \alpha, \alpha^2, \ldots, \alpha^{14})$ имеет минимальное расстояние 3.

Матрица

$$H^7_{\chi,15} = [\alpha^{7i}] = (1, \alpha^7, \alpha^{14}, \alpha^6, \alpha^{13}, \alpha^5, \alpha^{12}, \alpha^4, \alpha^{11}, \alpha^3, \alpha^{10}, \alpha^2, \alpha^9, \alpha, \alpha^8)$$

получается перестановкой столбцов матрицы $H^1_{\chi,15}$, а потому задает код, эквивалентный коду $\tilde{N}^1_{\chi,15}$. Код $\tilde{N}^3_{\chi,15}$ имеет минимальное расстояние *d* = 2, так как задается проверочной матрицей

$$H^3_{\chi,15} = [\alpha^{3i}] = (1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}, 1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}, 1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12})$$

с одинаковыми столбцами. Наконец проверочная матрица кода $\tilde{N}^5_{\chi,15}$ состоит из 5 последовательных блоков по 3 столбца в каждом – $(1, \alpha^5, \alpha^{10})$, и также имеет *d* = 2. Итак, имеется 4 различных обобщенных кода Хемминга длины 15 в полном соответствии со следствиями из предложения 1.

Предложение 2. *Пусть для нечетного числа n* > 1 *и целого числа k* НОД$(k, n) = 1$, *а циклотомический класс* C_k *по модулю n не совпадает с классом* C_1, *но имеет ту же мощность m. Тогда обобщенный код Хемминга* $\tilde{N}^k_{\chi,n}$ *длины n эквивалентен коду* $\tilde{N}^1_{\chi,n}$.

Доказательство. Столбцы матрицы $H^1_{\chi,n} = [\beta^i] = (1, \beta, \beta^2, \beta^3, ..., \beta^{n-1})$ можно рассматривать как элементы поля Галуа *GF*(2^m). В этом качестве они образуют циклическую подгруппу <β> порядка *n* в мультипликативной группе *GF*(2^m)*, порожденную элементом β. В таком случае столбцы матрицы (1) для каждого целого *k* образуют подгруппу в группе <β>, совпадающую иногда с самой группой <β>. Последнее происходит в случае, когда НОД$(k, n) = 1$, поскольку

здесь β^k имеет порядок n в группе $<\beta>$. Действительно, пусть порядок β^k равен l. Согласно теореме Лагранжа о подгруппах конечных групп величина l должна быть делителем n. С другой стороны, поскольку $\beta^{kl} = 1$, то произведение kl должно делиться на n. Но, поскольку $\text{НОД}(k, n) = 1$, то l должно делиться на n (см. [7, лемма 1.4.1] или [8, гл. 1, п. 2]). Таким образом, $l = n$, что и требовалось доказать. Следовательно, матрица (1) получается перестановкой столбцов матрицы $H^1_{\chi,n} = (1, \beta, \beta^2, \beta^3, ..., \beta^{n-1})$, что подтверждает эквивалентность кодов $\tilde{N}^k_{\chi,n}$ и $\tilde{N}^1_{\chi,n}$.

Непримитивные коды Хемминга $\tilde{N}^1_{\chi,n}$ систематически исследованы в работе [9].

Обобщенные БЧХ-коды, основные определения и свойства. Пусть в принятых выше обозначениях целое t таково, что произведение $mt < n$. Пусть $k = n - mt$.

Определение 2. Обобщенным двоичным (n,k)-кодом БЧХ 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

$$H = H_n(k_1, k_2, ..., k_t) = \begin{pmatrix} 1 & \beta^{k_1} & \beta^{2k_1} & \cdots & \beta^{(n-1)k_1} \\ 1 & \beta^{k_2} & \beta^{2k_2} & \cdots & \beta^{(n-1)k_2} \\ 1 & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta^{k_t} & \beta^{2k_t} & \cdots & \beta^{(n-1)k_t} \end{pmatrix}, \qquad (2)$$

где $1 \le k_1 < k_2 < ... < k_t \le n-1$, $\beta = \alpha^b$ для $b = (2^m - 1)/n$, предполагается, что среди степеней $\beta^{k_1}, \beta^{k_2}, ..., \beta^{k_t}$ не имеется ни одной пары сопряженных в поле Галуа. Говорим, что данный код имеет конструктивное расстояние $\delta = 2t + 1$.

Требование отсутствия сопряженных элементов в матрице (1) связано с тем, что ранг этой матрицы должен быть максимальным – равным mt. А наличие хотя бы одной пары сопряженных в матрице (2) уменьшает этот ранг на m согласно следствию 1 из предложения 1.

Возрастающий порядок чисел $k_1, k_2, ..., k_t$ в матрице (2) объясняется лишь вкусами авторов, их тягой к некоторой систематичности. Любое иное расположение названных чисел в матрице (2), равно как и замена какого-нибудь из них иным из того же циклотомического класса, не изменяют кода как решения однородной системы линейных уравнений $H \cdot \overline{x}^T = \overline{0}^T$. Такой порядок иногда в дальнейшем будет нарушаться, например при составлении значений в табл. 1.

В классическом, наиболее общем определении БЧХ-кода (см. [1, гл. 7, п. 7.2]) проверочная матрица состоит из кортежа строк, которые начинаются элементами $\beta^b, \beta^{b+1}, \ldots$, где b – целое, $b \ge 1$. При этом говорится, что при $b = 1$ мы имеем БЧХ-код в узком смысле. Эту же терминологию сохраним и здесь: если в матрице (2) $k_1 = 1$, то говорим, что задан обобщенный БЧХ-код в узком смысле с проверочной матрицей

$$H = H_n(1, k_2, ..., k_t) = [\beta^i, \beta^{k_2 i}, ..., \beta^{k_t i}]^T. \qquad (2')$$

Длина кортежа в определении БЧХ-кода в [1] определяется другим параметром – конструктивным расстоянием кода δ. Реально же имеются скрытые ограничения на длину кортежа – это размерность кода, наличие сопряженных среди элементов $\beta^{b+i}, 1 \le i \le \delta - 2$. Наличие сопряженных элементов уменьшает конструктивные размеры матрицы и увеличивает минимальное расстояние. С возникновением ТНС появились реальные возможности декодирования возрастающего количества ошибок, выходящих за конструктивные рамки. Эти обстоятельства и способствовали введению и исследованию обобщенных БЧХ-кодов (ОБЧХ-кодов). Обобщенные БЧХ-коды в узком смысле (с $k_1 = 1$) более удобны для обработки. Ниже рассмотрим условия, позволяющие привести ОБЧХ-код к обобщенному БЧХ-коду в узком смысле.

Формально при выполнении условия $mt < n$ и при разложении множества $T_n = \{1, 2, ..., n-1\}$ в μ циклотомических классов существует C^t_μ различных обобщенных БЧХ-кодов длины n и с конструктивным расстоянием $\delta = 2t + 1$. О качестве и свойствах этих кодов мы можем судить из дальнейших, более детальных исследований.

Обобщением предложения 1 является

Предложение 3. *При условии* НОД$(k_1, k_2,..., k_t, n) > 1$ *обобщенные БЧХ-коды с проверочной матрицей* (2) *имеют минимальное расстояние* 2.

Доказательство. Пусть НОД$(k_1, k_2,..., k_t, n) = d > 1$ и $n = d \cdot \mu$ для некоторого целого $\mu, 1 < \mu < n$. Тогда в матрице (2) $(\mu + 1)$-й столбец состоит из компонент $\beta^{k_1\mu} = 1$, $\beta^{k_2\mu} = 1,..., \beta^{k_t\mu} = 1$, т. е. совпадает с первым столбцом этой же матрицы. Поскольку нулевых столбцов в матрице (2) не имеется, то отсюда следует, что минимальное расстояние рассматриваемого кода с проверочной матрицей (2) равно 2, что и требовалось доказать.

Пример 2. Обобщенные БЧХ-коды длины $n = 21$ определены, как легко видеть, над полем $GF(2^6)$. Здесь множество $T_{21} = \{1, 2,..., 20\}$ разбивается на 5 следующих циклотомических классов:

$$C_1 = \{1,2,4,8,16,11\},\ C_3 = \{3,6,12\},\ C_5 = \{5,10,20,19,17,13\},\ C_7 = \{7,14\},\ C_9 = \{9,18,15\}.$$

Следовательно, имеется $C_5^2 = 10$ различных обобщенных БЧХ-кодов длины 21 и с конструктивным расстоянием 5. Условиям предложения 3 удовлетворяет обобщенный БЧХ-код $C_{21}^{3,9}$. Его проверочная матрица $H_{21}(3, 9)$ состоит из трех последовательных одинаковых блоков длины 7 следующего вида:

$$\begin{pmatrix} 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} \\ 1 & \beta^9 & \beta^{18} & \beta^6 & \beta^{15} & \beta^3 & \beta^{12} \end{pmatrix}.$$

Здесь $\beta = \alpha^3$ для примитивного элемента α поля $GF(2^6)$. Следовательно, минимальное расстояние кода $C_{21}^{3,9}$ равно 2 в полном соответствии с предложением 3.

Следующее утверждение обеспечивает условия, при которых обобщенный БЧХ-код эквивалентен обобщенному БЧХ-коду в узком смысле.

Предложение 4. *Пусть в матрице* (2) *хотя бы для одного целого* $j, 1 \le j \le t,$ НОД$(k_j, n) = 1$. *Тогда обобщенный БЧХ-код с проверочной матрицей* (2) *эквивалентен обобщенному БЧХ-коду в узком смысле.*

Доказательство. Пусть для определенности НОД$(k_1, n) = 1$. Тогда для целых чисел k_1 и n выполняется соотношение Безу, т. е. существуют целые $\tilde{u}_1$ и v_1, удовлетворяющие равенству $k_1 \cdot \tilde{u}_1 + n \cdot v_1 = 1$. Пусть u_1 – остаток от деления $\tilde{u}_1$ на натуральное число n. Тогда в силу соотношения Безу $\beta^{k_1u_1} = \beta$. Пусть r_j – остаток от деления k_ju_1 на n для всех целых $j, 2 \le j \le t$. Тогда $(u_1 + 2)$-й столбец матрицы (2) имеет вид $(\beta, \beta^{r_2}, \beta^{r_3},..., \beta^{r_t})^T$, а $(2u_1 + 2)$-й ее столбец будет иметь вид $(\beta^2, \beta^{2r_2}, \beta^{2r_3},..., \beta^{2r_t})^T$ и т. д. Осуществим перестановку столбцов в матрице (2): $(u_1 + 2)$-й столбец поставим на второе место, $(2u_1 + 2)$-й ее столбец – на третье и т. д. Завершив перестановку столбцов, переставим 2-ю, 3-ю и т. д. t-ю строки полученной матрицы в порядке возрастания чисел $r_2, r_3,..., r_t$. В результате получим проверочную матрицу

$$H = H_n(1, r_2',..., r_t') = [\beta^i, \beta^{r_2 i},..., \beta^{r_t i}]^T$$

обобщенного БЧХ-кода в узком смысле. Предложение 4 полностью доказано.

Следствие 4. *Пусть* $C(1,k) = C_n(1, k)$ *– ОБЧХ-код в узком смысле длины n, с конструктивным расстоянием* 5 *и с условием:* НОД$(k, n) = 1$. *Пусть* $u = k^{-1}$ *в кольце Z/nZ. Тогда код* $C(1,k)$ *эквивалентен коду* $C_n(1,u) = C_n(1, s)$, *где s – наименьшее целое из циклотомического класса множества* T_n, *которому принадлежит u.*

Пример 3. Множество $T_{31} = \{1, 2,..., 30\}$ разбивается на 6 следующих циклотомических классов:

$$C_1 = \{1,2,4,8,16\},\quad C_3 = \{3,6,12,24,17\},\quad C_5 = \{5,10,20,9,18\},\quad C_7 = \{7,14,28,25,19\},$$
$$C_{11} = \{11,22,13,26,21\},\quad C_{15} = \{15,30,29,27,23\}.$$

Следовательно, существует $C_6^2 = 15$ различных обобщенных БЧХ-кодов длины 31 с конструктивным расстоянием 5. Из них 5 являются обобщенными БЧХ-кодами в узком смысле, 10 задаются

проверочными матрицами $H_{31}(k_1,k_2)$, где $1<k_1<k_2$. Согласно предложению 4 все эти 10 БЧХ-кодов должны быть эквивалентны БЧХ-кодам из первой пятерки, т. е. обобщенным БЧХ-кодам в узком смысле. Чтобы убедиться в этом, мы должны скрупулезно повторить вычисления из доказательства предложения 4. Результаты этих вычислений, а именно значения остатков r_{ij} от деления $k_2^j u_i$ для $u_i=(k_1^i)^{-1}$ в $Z/31Z$ для пар $\left(k_1^i,k_2^j\right)$ минимальных образующих циклотомических классов $C_3,C_5,C_7,C_{11},C_{15}$ множества $T_{31}=\{1,2,\ldots,30\}$, сведены в табл. 1.

Таблица 1

Table 1

k_1^i	k_2^j				
	$k_2^1=3$	$k_2^2=5$	$k_2^3=7$	$k_2^4=11$	$k_2^5=15$
$k_1^1=3$	$u_1=21$	12	23	14	5
$k_1^2=5$	13	$u_2=25$	20	27	12
$k_1^3=7$	27	14	$u_3=9$	6	11
$k_1^4=11$	20	23	26	$u_4=17$	7
$k_1^5=15$	25	21	17	9	$u_5=29$

Из первой строки табл. 1 следует, что обобщенный БЧХ-код $C_{31}^{3,5}=C(3,5)$ эквивалентен коду $C_{31}^{1,12}=C(1,12)$. Поскольку число 12 принадлежит циклотомическому классу C_3, то код $C(3,5)$ эквивалентен коду $C(1,3)$. Из второй строки табл. 1 следует, что код $C(3,5)$ эквивалентен коду $C(13,1)$. Из принадлежности числа 13 циклотомическому классу C_{11} следует эквивалентность $C(3,5)$ и $C(1,11)$. Из транзитивности отношения эквивалентности следует, что коды в узком смысле $C(1,11)$ и $C(1,3)$ также эквивалентны.

Внимательный анализ данных табл. 1 показывает, что коду $C(1,3)$ эквивалентны также коды $C(5,15)$, $C(7,15)$, $C(7,11)$, коду $C(1,5)$ – коды $C(1,7)$, $C(3,11)$, $C(5,7)$, $C(3,15)$, $C(11,15)$, а реверсивному коду $C(1,15)=C(1,30)$ эквивалентны коды $C(3,7)$, $C(5,11)$.

Для наглядности покажем, что коды $C(1,5)$ и $C(1,7)$ действительно эквивалентны. Рассмотрим проверочную матрицу кода $C(1,5)$:

$$H_{(1,5)}=\begin{pmatrix}1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \alpha^{15}\\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \alpha^{20} & \alpha^{25} & \alpha^{30} & \alpha^4 & \alpha^9 & \alpha^{14} & \alpha^{19} & \alpha^{24} & \alpha^{29} & \alpha^3 & \alpha^8 & \alpha^{13}\\ \alpha^{16} & \alpha^{17} & \alpha^{18} & \alpha^{19} & \alpha^{20} & \alpha^{21} & \alpha^{22} & \alpha^{23} & \alpha^{24} & \alpha^{25} & \alpha^{26} & \alpha^{27} & \alpha^{28} & \alpha^{29} & \alpha^{30} & \\ \alpha^{18} & \alpha^{23} & \alpha^{28} & \alpha^2 & \alpha^7 & \alpha^{12} & \alpha^{17} & \alpha^{22} & \alpha^{27} & \alpha & \alpha^6 & \alpha^{11} & \alpha^{16} & \alpha^{21} & \alpha^{26} & \end{pmatrix}.$$

Мы вполне можем выполнить перестановку столбцов полученной матрицы, упорядочив их в порядке следования степеней α во второй строке. Получим следующую матрицу:

$$H'_{(1,5)}=\begin{pmatrix}1 & \alpha^{25} & \alpha^{19} & \alpha^{13} & \alpha^7 & \alpha & \alpha^{26} & \alpha^{20} & \alpha^{14} & \alpha^8 & \alpha^2 & \alpha^{27} & \alpha^{21} & \alpha^{15} & \alpha^9 & \alpha^3\\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \alpha^{15}\\ \alpha^{28} & \alpha^{22} & \alpha^{16} & \alpha^{10} & \alpha^4 & \alpha^{29} & \alpha^{23} & \alpha^{17} & \alpha^{11} & \alpha^5 & \alpha^{30} & \alpha^{24} & \alpha^{18} & \alpha^{12} & \alpha^6 & \\ \alpha^{16} & \alpha^{17} & \alpha^{18} & \alpha^{19} & \alpha^{20} & \alpha^{21} & \alpha^{22} & \alpha^{23} & \alpha^{24} & \alpha^{25} & \alpha^{26} & \alpha^{27} & \alpha^{28} & \alpha^{29} & \alpha^{30} & \end{pmatrix}.$$

Очевидно, полученная матрица есть проверочная матрица кода $C(1,25)$, который в силу принадлежности числа 25 классу C_7 немедленно отсылает нас к коду $C(1,7)$, что и требовалось показать.

Таким образом, на длине 31 существуют лишь три различных, не эквивалентных друг другу кода с конструктивным расстоянием 5: классический БЧХ-код $C(1,3)$, классический реверсивный

код $C(1,30)$, а также код $C(1,5)$, который можно назвать кодом квадратично-вычетного типа, поскольку порождающие его циклотомические классы C_1, C_5, как легко видеть, состоят из квадратичных вычетов по модулю 31.

ОБЧХ-коды с конструктивным расстоянием 5 в диапазоне длин от 9 до 107. В силу проведенных выше исследований ОБЧХ-коды $C_n(k_1,k_2)$ длины n и с конструктивным расстоянием 5 либо относятся к кодам в узком смысле (коды первого типа), либо имеют общий вид, но при условии, что $\text{НОД}(k_1,n)=d_1>1$, $\text{НОД}(k_2,n)=d_2>1$, $НОД(d_1,d_2)=1$ (коды второго типа). Конечно, возможен случай $\text{НОД}(k_1,k_2,n)=d>1$ (коды третьего типа), но он абсолютно не интересен с практической точки зрения, так как соответствующий ОБЧХ-код $C_n(k_1,k_2)$ имеет минимальное расстояние, равное 2, согласно предложению 3.

Все рассматриваемые в данной статье коды имеют нечетные длины. В диапазоне от 9 до 107 имеется 51 нечетная длина. Для каждой из них имеется свое поле определения – поле Галуа $GF(2^m)$ с наименьшим m таким, что $2^m - 1$ делится на m. 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 $k = 1$ – самые не интересные коды. На еще четырех длинах также имеются только коды Хемминга, хотя и большей размерности. Это следующие длины: 9 ($m = 6$); 25 ($m = 20$); 27 ($m = 18$); 81 ($m = 54$). Еще для 8 длин рассматриваемого диапазона имеются БЧХ-коды с конструктивным расстоянием 5, но с размерностью $k = 1$ – также не представляющие практического интереса. Это длины 17, 23, 41, 47, 71, 79, 97, 103. Осталось 27 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, аналогично примеру 3, всех ОБЧХ-кодов $C_n(k_1,k_2)$ и их свойств. Проведено вычисление минимальных расстояний каждого из полученных кодов с помощью комбинаторной теоремы, связанной с рангами систем столбцов проверочной матрицы (см., напр., [10, теорема 1.8]). Основные результаты вычислений приведены в табл. 2.

Таблица 2

Table 2

#	n	m	Всего кодов	Классов	d $C(1,3)$	d min (среди остальных)	d max (среди остальных)
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

Окончание табл. 2

#	*n*	*m*	Всего кодов	Классов	*d C*(1,3)	*d* min (среди остальных)	*d* max (среди остальных)
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

Из табл. 2 следует, что на семи длинах имеются ОБЧХ-коды первого типа с наибольшим минимальным расстоянием, превосходящим минимальное расстояние классических реверсивных и БЧХ-кодов.

Заключение. Дано независимое определение двоичных обобщенных БЧХ-кодов. Изучены их свойства. Показано существование ОБЧХ-кодов практически на всех длинах, на которых существуют и классические БЧХ-коды. Найдены условия, при которых ОБЧХ-коды эквивалентны ОБЧХ-кодам в узком смысле. ОБЧХ-коды, имеющие конструктивное расстояние 5, разделены на три типа. Все они систематически исследованы в диапазоне длин от 9 до 107. Вычислены их минимальные расстояния. Показано, что примерно на трети длин существуют ОБЧХ-коды в узком смысле (первого типа), корректирующие возможности которых превосходят таковые у классических кодов. Таким образом, вводимый класс ОБЧХ-кодов предоставляет новые примеры кодов, перспективные для приложений.

Список использованных источников

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: Изд. центр БГУ, 2007. – 216 с.

4. Липницкий, В. А. Теория норм синдромов и плюс-декодирование / В. А. Липницкий, А. О. Олексюк // Докл. БГУИР. – 2014. – № 8. – С. 71–78.

5. Кушнеров, А. В. Обобщенные коды Боуза – Чоудхури – Хоквингема / А. В. Кушнеров, В. А. Липницкий, М. Н. Королева // Вестн. Полоцк. гос. ун-та. Сер. С, Фундамент. науки. – 2018. – № 4. – С. 28–33.

6. Лидл, Р. Конечные поля: в 2 т.: пер. с англ. / Р. Лидл, Г. Нидеррайтер. – М.: Мир, 1988. – 822 с.

7. 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.

8. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – М.: Наука, 1972. – 168 с.

9. Липницкий, В. А. Оценка минимальных расстояний непримитивных кодов Хемминга / В. А. Липницкий, А. О. Олексюк // Вес. Нац. акад. навук Беларусі. Сер. фіз.-тэхн. навук. – 2015. – № 2. – С. 103–110.

10. Липницкий, В. А. Теория норм синдромов / В. А. Липницкий. – Минск: БГУИР, 2011. – 96 с.

References

1. MacWilliams F. J., Sloane N. J. A. *The Theory of Error-Correcting Codes*. Elsevier Science, 1977. 744 p.

2. Blackhut R. *Theory and Practice of Error Control Codes*. Reading, MA, Addison-Wesley, 1983. 500 p.

3. Konopel'ko V. K., Lipnitskii V. A. *Norm Decoding of Error-correcting Codes and Algebraic Equations*. Minsk, BSU Publ., 2007. 216 p. (in Russian).

4. Lipnitskii V. A., Oleksiuk A. O. The theory of norms syndromes and plus-decoding. *Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki = Doklady BGUIR*, 2014, no. 8, pp 71–78 (in Russian).

5. Kushnerov A. V., Lipnitskii V. A., Koroliova M. N. Generic Bose – Chaudhuri – Hocquenghem codes. *Vestnik Polockogo gosudarstvennogo universiteta. Seriya C, Fundamental'nye nauki = Bulletin of Polotsk State University, part C, Fundamental science*, 2018, no 4, pp 28–33 (in Russian).

6. Liddle R., Niederraiter G. *Finite Fields.* Cambridge University Press, 1997. 755 p.

7. Lipnitskii V. A. *Modern Applied Algebra. Mathematical foundations of information protection from interference and unauthorized access*. Minsk, BSUIR Publ., 2005. 88 p. (in Russian).

8. Vinogradov I. M. *Fundamentals of Number Theory*. Moscow, Nauka Publ., 1972. 168 p. (in Russian).

9. Lipnitskii V. A., Oleksiuk A. O. Estimation of the minimum distances of non-primitive Hamming codes. *Vestsi Natsyyanal'nai akademii navuk Belarusi. Seryya fizika-technichnych navuk = Proceedings of the National Academy of Sciences of Belarus. Physical-technical series*, 2012, no. 2, pp 103–110 (in Russian).

10. Lipnitskii V. A. *Theory of Syndrome Norms*. Minsk, BSUIR Publ., 2011. 96 p. (in Russian).

Информация об авторах

Кушнеров Александр Викторович – старший преподаватель кафедры дифференциальных уравнений и системного анализа, механико-математический факультет, Белорусский государственный университет (пр. Независимости, 4, 220030, г. Минск, Республика Беларусь). E-mail: al.v.kushnerov@gmail.com

Липницкий Валерий Антонович – доктор технических наук, профессор, заведующий кафедрой высшей математики, Военная академия Республики Беларусь (пр. Независимости, 220, 220057, г. Минск, Республика Беларусь). E-mail: valipnitski@yandex.by

Королева Мария Николаевна – старший преподаватель кафедры высшей математики, Белорусский национальный технический университет (пр. Независимости, 65, 220013, г. Минск, Республика Беларусь).

Information about the authors

Alexander V. Kushnerov – Senior Lecturer of the Department of Differential Equations and System Analysis, Mechanic & Mathematics Faculty, Belarussian State University (4, Nezavisimosti Ave., 220030, Minsk, Republic of Belarus). E-mail: al.v.kushnerov@gmail.com

Valery A. Lipinski – Dr. Sc. (Engineering), Professor, Head of the Mathematics Department, Military Academy of the Republic of Belarus (220, Nezavisimosti Ave., 220057, Minsk, Republic of Belarus). E-mail: valipnitski@yandex.by

Maria N. Koroleva – Senior Lecturer of the Mathematics Department, Belarusian National Technical University (65, Nezavisimosti Ave., 220013, Minsk, Republic of Belarus).