Математическая логика, алгебра и теория чисел

Mathematical logic, algebra and number theory

УДК 519.725

ОБОБЩЕННЫЕ БЧХ-КОДЫ. ПОЛИНОМИАЛЬНО-НОРМЕННОЕ ДЕКОДИРОВАНИЕ ОШИБОК

А. В. КУШНЕРОВ[1)]***, В. А. ЛИПНИЦКИЙ***[1), 2)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*
[2)]*Военная академия Республики Беларусь, пр. Независимости, 220, 220057, г. Минск, Беларусь*

Классические коды Боуза – Чоудхури – Хоквингема (БЧХ-коды) и их изучение составляют обширную область теории кодов, исправляющих ошибки. Обобщение БЧХ-кодов позволяет расширить спектр деятельности в практической коррекции ошибок. Среди обобщенных БЧХ-кодов были найдены коды, превосходящие по числу исправляемых ошибок классический БЧХ-код. Вопрос методики коррекции ошибок потребовал глубокой теоретической проработки и компьютерного эксперимента на ее основе. Итогом этого стал полиномиально-норменный метод декодирования, который показал себя значительно более эффективным, чем классический синдромный метод декодирования. В некоторых случаях полиномиально-норменный метод является единственным возможным. Результатом исследования выступает модель полиномиально-норменного декодера для обобщенного БЧХ-кода длиной 65.

Ключевые слова: помехоустойчивые коды; коды Боуза – Чоудхури – Хоквингема; автоморфизмы кодов; норменный метод декодирования; полиномиально-норменный метод декодирования.

Образец цитирования:
Кушнеров АВ, Липницкий ВА. Обобщенные БЧХ-коды. Полиномиально-норменное декодирование ошибок. *Журнал Белорусского государственного университета. Математика. Информатика.* 2020;2:36–48.
https://doi.org/10.33581/2520-6508-2020-2-36-48

For citation:
Kushnerov AV, Lipnitski VA. Generic BCH codes. Polynomial-norm error decoding. *Journal of the Belarusian State University. Mathematics and Informatics*. 2020;2:36–48. Russian.
https://doi.org/10.33581/2520-6508-2020-2-36-48

Авторы:
Александр Викторович Кушнеров – старший преподаватель кафедры дифференциальных уравнений и системного анализа механико-математического факультета.
Валерий Антонович Липницкий – доктор технических наук, профессор; заведующий кафедрой высшей математики[2)], профессор кафедры дифференциальных уравнений и системного анализа механико-математического факультета[1)].

Authors:
Alexander V. Kushnerov, senior lecturer at the department of differential equations and system analysis, faculty of mechanics and mathematics.
al.v.kushnerov@gmail.com
Valery A. Lipnitski, doctor of science (engineering), full professor; head of the department of higher mathematics[b] and professor at the department of differential equations and system analysis, faculty of mechanics and mathematics[a].
valipnitski@yandex.by

GENERIC BCH CODES. POLYNOMIAL-NORM ERROR DECODING

A. V. KUSHNEROV [a], ***V. A. LIPNITSKI*** [a, b]

[a] *Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
[b] *Military Academy of the Republic of Belarus, 220 Niezaliežnasci Avenue, Minsk 220057, Belarus*
Corresponding author: A. V. Kushnerov (al.v.kushnerov@gmail.com)

The classic Bose – Chaudhuri – Hocquenghem (BCH) codes is famous and well-studied part in the theory of error-correcting codes. Generalization of BCH codes allows us to expand the range of activities in the practical correction of errors. Some generic BCH codes are able to correct more errors than classic BCH code in one message block. So it is important to provide appropriate method of error correction. After our investigation it was found that polynomial-norm method is most convenient and effective for that task. The result of the study was a model of a polynomial-norm decoder for a generic BCH code at length 65.

Keywords: error correcting codes; Bose – Chaudhuri – Hocquenghem codes; automorphisms of codes; norm decoding method; polynomial-norm decoding method.

Введение

Конструирование и эксплуатация современных цифровых инфокоммуникационных систем (ИКС) отягощены проблемой быстрой передачи больших объемов информации. Это сопровождается необходимостью синхронной коррекции многократных ошибок, неизбежно возникающих в процессе передачи информации в каналах с шумами и помехами. Наиболее популярными в высокоскоростных ИКС оказались линейные циклические коды, особенно из семейства кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов) [1–4], для которых, помимо классических синдромных, разработаны эффективные норменные [5–7] и полиномиально-норменные методы коррекции ошибок [8–10]. Соответствующие алгоритмы базируются на многогранной связи БЧХ-кодов с полями Галуа [1; 11; 12], наличии группы автоморфизмов в этих кодах [6; 7; 13], а также на обнаруженных синдромных, норменных и полиномиально-норменных инвариантах автоморфизмов реверсивных кодов и БЧХ-кодов. На сегодняшний день эти алгоритмы являются единственными возможными для коррекции ошибок, кратность которых превышает конструктивные возможности БЧХ-кодов, что наиболее ярко видно на классе непримитивных БЧХ-кодов (см., например, [14; 15]).

В статьях [16; 17] расширяется класс БЧХ-кодов в целях применения к ним полиномиально-норменных методов и алгоритмов коррекции ошибок. Раскрытию предполагаемых возможностей обобщенных БЧХ-кодов (ОБЧХ-кодов) и посвящена данная работа.

ОБЧХ-коды. Основные определения и свойства

ОБЧХ-коды, как и классические БЧХ-коды, имеют нечетную длину $n > 7$ и поле определения $GF\left(2^m\right)$, которое характеризуется минимальным значением m с условием $2^m - 1$ делится на n. Для целочисленной функции Эйлера $\varphi(n)$ (согласно теореме Эйлера [18; 19]) величина $2^{\varphi(n)} - 1$ всегда делится на n. Поэтому иногда $\varphi(n)$ совпадает с m. Из теории конечных полей [12; 18] следует, что m должно быть делителем $\varphi(n)$. Пусть целое $t > 1$ таково, что $t \cdot m < n$, а β – примитивный элемент степени n в поле $GF\left(2^m\right)$. Например, если $2^m - 1 = \upsilon \cdot n$ и α – примитивный элемент поля $GF\left(2^m\right)$, то в качестве β можно взять элемент α^{υ}.

При введенных условиях над полем $GF\left(2^m\right)$ существует классический двоичный циклический код длиной n с проверочной матрицей

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \dots & \alpha^{(2t-1)(n-1)} \end{pmatrix}. \quad (1)$$

Пусть $k_1, k_2, \ldots, k_t$ – целые числа с условиями:

1) $1 \le k_1 < k_2 < \ldots < k_t \le 2^m - 2$;

2) они принадлежат попарно различным циклотомическим классам по модулю n или, что эквивалентно, среди элементов поля Галуа $\beta^{k_1}, \beta^{k_2}, \ldots, \beta^{k_t}$ не имеется ни одной пары сопряженных, т. е. принадлежащих множеству корней одного неприводимого над $GF(2) = Z/2Z$ полинома.

Второе условие без явных оговорок считается автоматически выполняющимся и для кодов с проверочной матрицей (1). В противном случае ранг матрицы (1) будет меньше $m \cdot t$ (см. теорему 6.3 [6]) и она теряет статус проверочной матрицы. В силу этой же причины и включено в определение 1 второе условие.

Определение 1. ОБЧХ-кодом длиной n над полем $GF\left(2^m\right)$ с конструктивным расстоянием $\delta = 2t + 1$ называется помехоустойчивый линейный код $C = C^{\delta, n}_{\text{ОБЧХ}} = C\left(k_1, k_2, \ldots, k_t\right)$ с проверочной матрицей

$$H^{\delta}_{\text{ОБЧХ}} = \left(\beta^{k_1 i}, \beta^{k_2 i}, \ldots, \beta^{k_t i}\right)^{\mathrm{T}}. \tag{2}$$

Очевидно, что такой код является циклическим. Определим на множестве двоичных векторов с n координатами циклическую подстановку σ по правилу: для некоторого вектора $\bar{e} = \left(e_1, e_2, \ldots, e_n\right) \in V_n$ $\sigma\left(\bar{e}\right) = \left(e_n, e_1, e_2, \ldots, e_{n-1}\right)$. Далее рассмотрим циклотомическую подстановку φ на координатах вектора $\bar{e}$. Для некоторого вектора $\bar{e} = \left(e_1, e_2, \ldots, e_n\right) \in V_n$ $\varphi\left(\bar{e}\right) = \left(e'_1, e'_2, \ldots, e'_n\right)$ согласно следующему правилу:

$$e'_i = \begin{cases} e_{2i-1}, & 2i - 1 \le n, \\ e_{2i-1-n}, & 2i - 1 > n. \end{cases}$$

Циклическая подстановка σ и циклотомическая подстановка φ являются автоморфизмами ОБЧХ-кода [6; 7]. Следовательно, в группе $\mathrm{Aut}\left(C^{\delta, n}_{\text{ОБЧХ}}\right)$ содержатся группы Γ и G, порожденные подстановкой σ и подстановками σ и φ соответственно [6; 7].

Исходя из условий определения 1, класс БЧХ-кодов с проверочной матрицей (1) является частным случаем ОБЧХ-кода. С другой стороны, для всех ОБЧХ-кодов, представляющих практический интерес, можно считать $k_1 = 1$. В самом деле, если $k_1 > 1$ и среди k_i, $1 \le i \le t$, имеется хотя бы одно значение k_j с условием $\text{НОД}\left(k_j, n\right) = 1$, то $\beta^{k_j} = \gamma$ останется элементом порядка n в поле $GF\left(2^m\right)$. Заменив в определении 1 элемент β на γ, мы получим ОБЧХ-код, у которого $k_1 = 1$.

Если же окажется, что $\text{НОД}\left(k_1, k_2, \ldots, k_t, n\right) = \mu > 1$, то минимальное расстояние кода $C^{2t+1, n}_{\text{ОБЧХ}}$ равно 2, поскольку матрица (2) при таких условиях содержит одинаковые столбцы. Как показывают многочисленные вычисления и примеры, ОБЧХ-коды с условиями $\text{НОД}\left(k_1, k_2, \ldots, k_t, n\right) = 1$, но $\text{НОД}\left(k_i, n\right) > 1$ для всех i, $1 \le i \le t$, имеют минимальное расстояние, не превосходящее величину $\delta = 2t + 1$.

Классическая теория и практика БЧХ-кодов имеет дело с примитивными кодами (когда $n = 2^m - 1$ и $\beta = \alpha$ – примитивный элемент поля $GF\left(2^m\right)$); тогда, как правило, $d = \delta$ и корректируются ошибки, кратность которых не выходит за рамки конструктивных возможностей.

Исследуя ОБЧХ-коды, мы получаем возможность отыскать коды, которые имеют корректирующие возможности, превосходящие конструктивные, а также декодирующие возможности стандартных БЧХ-кодов и реверсивных кодов той же длины.

Пример 1. Пусть $n = 65$, тогда $m = 12$. Множество $T = \{1, 2, \ldots, 64\}$ разбивается на шесть циклотомических классов по модулю 65:

$$C_1 = \{1, 2, 4, 8, 16, 32, 33, 49, 57, 61, 63, 64\},\ C_3 = \{3, 6, 12, 17, 24, 31, 34, 41, 48, 53, 59, 62\},$$

$$C_5 = \{5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60\},\ C_7 = \{7, 9, 14, 18, 28, 29, 36, 37, 47, 51, 56, 58\} = C_9,$$

$$C_{11} = \{11, 19, 21, 22, 23, 27, 38, 42, 43, 44, 46, 54\},\ C_{13} = \{13, 26, 39, 52\}.$$

Из определения 1 следует, что существует $C^2_6 = 15$ различных ОБЧХ-кодов $C\left(k_1, k_2\right)$ длиной 65 с $\delta = 5$: $C(1, 3)$, $C(1, 5)$, $C(1, 7)$, $C(1, 11)$, $C(1, 13)$, $C(3, 5)$, $C(3, 7)$, $C(3, 11)$, $C(3, 13)$, $C(5, 7)$, $C(5, 11)$, $C(5, 13)$, $C(7, 11)$, $C(7, 13)$, $C(11, 13)$.

Классический непримитивный БЧХ-код $C(1, 3)$ длиной 65 имеет минимальное расстояние 5, как показывают расчеты. Поскольку $64 \in C_1$, то β^{64} сопряжено с β, и реверсивный код данной длины не существует, точнее, совпадает с непримитивным кодом Хемминга. Последний также имеет минимальное расстояние 5 [15].

Код $C(1, 11)$ эквивалентен коду $C(1, 3)$. Действительно, у проверочной матрицы $H(1, 11)$ седьмой столбец есть $(\beta^6, \beta^{66}) = (\beta^6, \beta)^{\mathrm{T}}$. Циклический сдвиг столбцов данной матрицы с тем, чтобы седьмой столбец стал первым, а также перестановка подматриц (β^{6i}) и (β^i) приводят к коду $C(1, 6)$. Так как согласно разбиению на циклотомические классы элементы поля $GF(2^m)$ β^3 и β^6 являются сопряженными, коды $C(1, 3)$ и $C(1, 11)$ эквивалентны.

Аналогичным образом можем получить разбиение множества всех кодов $C(k_1, k_2)$ длиной 65 на классы эквивалентности. Результаты вычислений представлены в табл. 1.

Таблица 1

Распределение ОБЧХ-кодов длиной 65 с конструктивным расстоянием 5 по классам эквивалентности

Table 1

Distribution of generic BCH codes at length 65 with a constructive distance of 5 by equivalence classes

Классы эквивалентных кодов	Количество кодов в классе	Минимальное расстояние
$C(1, 3)$, $C(1, 11)$, $C(3, 7)$, $C(7, 11)$	4	5
$C(1, 5)$, $C(3, 5)$, $C(5, 7)$, $C(5, 11)$	4	8
$C(1, 7)$, $C(3, 11)$	2	5
$C(1, 13)$, $C(3, 13)$, $C(7, 13)$, $C(11, 13)$	4	5
$C(5, 13)$	1	4

Синдромы ошибок в ОБЧХ-кодах и их свойства

Благодаря структуре проверочной матрицы (2) ОБЧХ-кода $C = C^{\delta, n}_{\text{ОБЧХ}}$ синдром $S(\bar{e})$ любого вектора-ошибки $\bar{e}$ в нем имеет вид $S(\bar{e}) = H \cdot \bar{e}^{\mathrm{T}} = (s_1, s_2, \ldots, s_t)$, т. е. состоит из t компонент s_i, $1 \le i \le t$, принадлежащих полю Галуа $GF(2^m)$. В силу линейности кода C количество синдромов оценивается величиной 2^{tm}. Это существенно больше количества $K = C_n^1 + C_n^2 + \ldots + C_n^t$ конструктивно допустимых исправляемых ошибок весом от 1 до t. Благодаря этому обстоятельству возможно применение различных синдромных методов для коррекции ошибок ОБЧХ-кодами.

Так, исправление t-кратной ошибки кодом $C = C_n(k_1, k_2, \ldots, k_t)$ равносильно решению следующей системы алгебраических уравнений над полем Галуа $GF(2^m)$:

$$\begin{cases} x_1^{k_1} + x_2^{k_1} + \ldots + x_t^{k_1} = s_1, \\ x_1^{k_2} + x_2^{k_2} + \ldots + x_t^{k_2} = s_2, \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots \\ x_1^{k_t} + x_2^{k_t} + \ldots + x_t^{k_t} = s_t. \end{cases} \tag{3}$$

Для ОБЧХ-кода в узком смысле (когда $k_1 = 1$), заданного проверочной матрицей

$$H = (\beta^i, \beta^{k_2 i}, \ldots, \beta^{k_t i})^{\mathrm{T}}, \tag{2′}$$

первое уравнение становится линейным: $x_1 + x_2 + \ldots + x_t = s_1$. И в данном уравнении, и в системе (3) неизвестные $x_1, x_2, \ldots, x_t$ – элементы первой из t строк матрицы (2′), соответствующие неизвестным ненулевым координатам вектора $\bar{e}$. Решив систему (3), мы определим значения $x_1, x_2, \ldots, x_t$ и тем самым однозначно найдем вектор $\bar{e}$.

Решение системы (3) в общем виде возможно только методом перебора, что требует большого объема вычислений (на практике это практически не осуществимо). Возможно решение этой системы для малых значений t при конкретном задании параметров $k_1, k_2, \ldots, k_t$. Так, при $t = 2$ для кода $C_n(1, 5)$ система (3) имеет вид

$$\begin{cases} x + y = s_1, \\ x^5 + y^5 = s_2. \end{cases} \tag{4}$$

После замены $y = x + s_1$ второе уравнение системы (4) превращается в уравнение $x^5 + (x + s_1)^5 = s_2$ или, после возведения в степень и приведения подобных, в уравнение $x^4 + s_1^3 x + b = 0$ для $b = s_1^4 + \frac{s_2}{s_1}$. Полученное уравнение вполне можно решать методом Чэня, т. е. переборным методом.

Для кода $C_n(1, 7)$ аналогом системы (4) будет система

$$\begin{cases} x + y = s_1, \\ x^7 + y^7 = s_2. \end{cases} \tag{5}$$

Та же замена, что и в системе (4), приводит второе уравнение системы (5) к виду $s_1 x^6 + s_1^2 x^5 + s_1^3 x^4 + s_1^4 x^3 + s_1^5 x^2 + s_1^6 x + s_1^7 = s_2$. Разделим полученное уравнение на s_1^7 и выполним замену $z = \frac{x}{s_1}$. Имеем уравнение $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = \frac{s_2}{s_1^7}$. Умножив обе части последнего уравнения на $z + 1$, получим окончательно уравнение $z^7 + cz + d = 0$, где $c = \frac{s_2}{s_1^7}$, $d = c + 1$. Данное уравнение также можно решать методом Чэня, как это делается в декодерах для классического БЧХ-кода $C_n(1, 3)$.

Пример 2. В коде $C_{65}(1, 13)$ из примера 1, определенном над полем $GF(2^{12})$ с примитивным полиномом $p(x) = x^{12} + x^{10} + x^2 + x + 1$ и имеющем минимальное расстояние 5, согласно табл. 1 найдем ошибку $\bar{e}$ в принятом сообщении $\bar{z}$ с синдромом $S(\bar{z}) = S(\bar{e}) = (\alpha^{2469}, \alpha^{3822})$.

В данном случае аналог системы (4) имеет вид $x + y = s_1, x^{13} + y^{13} = s_2$. Выражение y из первого уравнения подставим во второе. После приведения подобных членов и деления на s_1 получим равенство $x^{12} + x^9 s_1^3 + x^8 s_1^4 + x^5 s_1^7 + x^4 s_1^8 + x s_1^{11} + c = 0$ для $c = s_1^{12} + \frac{s_2}{s_1}$.

Для заданного сообщения $\bar{z}$ полученное уравнение имеет вид $x^{12} + x^9\alpha^{3312} + x^8\alpha^{1686} + x^5\alpha^{903} + x^4\alpha^{3372} + x\alpha^{2589} + \alpha^{1028} = 0$. Как показывают вычисления, уравнение можно представить следующим образом: $(x + \alpha^{378})(x + \alpha^{3780})(x^{10} + x^9\alpha^{2469} + x^8\alpha^{193} + x^6\alpha^{3506} + x^5\alpha^{1880} + x^4\alpha^{3699} + x^3\alpha^{3568} + x^2\alpha^{2917} + x\alpha^{706} + \alpha^{965}) = 0$. Значит, оно имеет лишь два корня в поле $GF(2^{12})$: $x_1 = \alpha^{378} = \beta^6$ и $x_2 = \alpha^{3780} = \beta^{60}$. Следовательно, в сообщении $\bar{z}$ содержится вектор-ошибка весом 2 с единицами на позициях 7 и 61.

Таким образом, прямой синдромный метод в ОБЧХ-кодах вновь актуализирует проблематику решения алгебраических уравнений и систем над полями Галуа. Отметим, что уже для кода $C_n(3, 5)$ сложности решения аналога системы (4) удваиваются. Главные недостатки метода уравнений: 1) не ясно, что делать при наличии более двух корней в методе Чэня; 2) подобный подход не дает возможности находить координаты ошибок, кратность которых выходит за конструктивные рамки (наиболее интересный случай).

Для решения последней проблемы мы видим единственный путь – переходить к норменным методам.

Г-орбиты ошибок и их нормы в ОБЧХ-кодах

Для начала рассмотрим следующую теорему.

Теорема 1 (теорема 2.1 [6]). *Пусть* σ *– оператор циклического сдвига вправо на единицу координат векторов двоичного пространства* V_n. *Тогда для всякого вектора* $\bar{e} \in V_n$ Г*-орбита* $J = \langle \bar{e} \rangle = \langle \bar{e} \rangle_\Gamma$, *им порожденная, состоит из* ν *элементов, где* $\nu = n$ *или* ν *делит* n, *и имеет следующую структуру:*

$$\langle \bar{e} \rangle = \left\{ \bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\nu-1}(\bar{e}) \right\}, \tag{6}$$

при этом ν – наименьшее натуральное число с условием $\sigma^{\nu}(\bar{e}) = \bar{e}$.

Группы Г и G содержатся в группе автоморфизмов семейства всех двоичных циклических БЧХ-кодов нечетной длины, строение и количество Г-орбит и G-орбит ошибок зависят только от значений длины n. Выбор кода данной длины сказывается лишь на синдромах ошибок и, следовательно, на конкретных значениях синдромных инвариантов орбит этих ошибок.

Пусть φ – циклотомическая подстановка на пространстве двоичных векторов нечетной размерности V_n, $n = 2k + 1$, $k \in \mathbb{N}$ [1; 5; 6]. Действие σ и φ на векторы-ошибки отражается на синдромах векторов-ошибок следующим образом.

Теорема 2. *Пусть* $S = S(\bar{e}) = (s_1, s_2, \ldots, s_t)$ *– синдром вектора-ошибки* $\bar{e}$ *в ОБЧХ-коде* C *с проверочной матрицей (2). Тогда* $S(\sigma(\bar{e})) = (\beta^{k_1} s_1, \beta^{k_2} s_2, \ldots, \beta^{k_t} s_t)$, $S(\varphi(\bar{e})) = (s_1^2, s_2^2, \ldots, s_t^2)$.

Доказательство практически дословно повторяет обоснование предложений 3.9 и 3.17 [6].

В подавляющем большинстве случаев Г-орбиты векторов-ошибок являются полными, т. е. содержат максимально возможное количество векторов, по мощности совпадают с мощностью группы Г и длиной n кода C.

Определение 2. Спектром синдромов $S(J)$ Г-орбиты J называется множество синдромов всех векторов этой Г-орбиты. Спектр синдромов называется полным, если его мощность совпадает с мощностью самой Г-орбиты: $|S(J)| = |J|$.

Из теорем 1, 2 непосредственно вытекает следствие 1.

Следствие 1. *Пусть* Г*-орбита* $\langle \bar{e} \rangle$ *состоит из* ν *векторов. Тогда спектр синдромов этой* Г*-орбиты имеет следующую структуру:*

$$S(\langle \bar{e} \rangle) = \left\{ (\beta^{ik_1} s_1, \beta^{ik_2} s_2, \ldots, \beta^{ik_t} s_t),\ 0 \le i \le \nu - 1 \right\}. \tag{7}$$

Формулы (6) и (7) демонстрируют синхронную циклическую структуру Г-орбит и их синдромных спектров, причем значения спектра взаимно однозначно представляют всю Г-орбиту: i-кратное действие оператора σ на вектор $\bar{e}$ синхронно отражается в спектре $S(\langle \bar{e} \rangle)$ i-кратным умножением компонент s_j синдрома $S(\bar{e})$ на соответствующие коэффициенты β^{k_j}, $1 \le j \le t$.

Из формулы (7) непосредственно следует, что мощность $|S(J)| \le |J|$, и если окажется, что $|S(J)| = n$, то Г-орбита J обязательно должна быть полной. На этом наблюдении базируется следствие 2.

Следствие 2 (синдромные признаки полноты Г-орбиты ошибок). *Пусть в ОБЧХ-коде* C *у вектора-ошибки* $\bar{e}$ *для целого* i, $1 \le i \le t$, *компонента синдрома* $s_i \ne 0$ *и* НОД$(k_i, n) = 1$. *Тогда* Г*-орбита* $\langle \bar{e} \rangle$ *является полной. В частности, утверждение выполняется при* $i = 1$ *и* $k_1 = 1$.

Доказательство полностью повторяет доказательство предложения 3.10 [6].

Следствие 3. *Пусть в условиях следствия 2 ОБЧХ-код* C *является примитивным, т. е.* $n = 2^m - 1$. *Тогда в спектре синдромов* $S(\langle \bar{e} \rangle)$ *i-я компонента принимает ненулевые значения поля Галуа* $GF(2^m)$.

Определение 3. Нормой синдрома $S(\bar{e}) = H \cdot \bar{e}^{\mathrm{T}} = (s_1, s_2, \ldots, s_t)^{\mathrm{T}}$ вектора ошибок $\bar{e}$ в ОБЧХ-коде с проверочной матрицей (2) называется вектор $N(S(\bar{e})) = (N_{12}, N_{13}, \ldots, N_{1t}, N_{23}, \ldots, N_{(t-1)t})$ с C_t^2 координатами N_{ij}, $1 \le i < j \le t$, которые вычисляются по формулам

$$\begin{gathered} N_{ij} = \infty, \text{ если } s_j \ne 0,\ s_i = 0;\ N_{ij} \text{ не определена, если } s_i = s_j = 0; \\ N_{ij} = \frac{s_j^{k_i/d_{ij}}}{s_i^{k_j/d_{ij}}} \text{ для } d_{ij} = \text{НОД}(k_i, k_j), \text{ если } s_i \ne 0. \end{gathered} \tag{8}$$

Приведенное определение полностью согласовано с определением нормы синдрома БЧХ-кода в работах [5; 6] и построено таким образом, чтобы выполнялось следующее утверждение.

Теорема 3. *Пусть* $\bar{e}$ *– произвольный вектор-ошибка в ОБЧХ-коде* C *с проверочной матрицей (2),* $S = S(\bar{e}) = (s_1, s_2, \ldots, s_t)$ *– синдром данной ошибки,* σ *– оператор циклического сдвига координат векторов вправо на одну координату,* $N(S(\bar{e})) = (N_{12}, N_{13}, \ldots, N_{1t}, N_{23}, \ldots, N_{(t-1)t})$. *Тогда* $N(S(\sigma(\bar{e}))) = N(S(\bar{e}))$.

Доказательство вытекает из определения 3 и теоремы 2.

Из теоремы 3 получаем следствие 3.

Следствие 3. *В ОБЧХ-коде C нормы синдромов всех векторов-ошибок каждой отдельно взятой* Г-*орбиты* $J = \langle \bar{e} \rangle$ *совпадают друг с другом.*

Определение 4. Норма синдрома $N\left(S\left(\bar{e}\right)\right)$ любого вектора-ошибки $\bar{e}$ Г-орбиты J называется нормой этой Г-орбиты и обозначается одним из символов: $N\left(J\right)$, $N\left(\langle \bar{e} \rangle\right)$ или N_J.

Методом от противного доказывается следующая теорема.

Теорема 4. *Если нормы* Г-*орбит* J_1 *и* J_2 *различны, то и синдромы векторов-ошибок этих орбит попарно различны.*

Теорема 5. *Пусть в примитивном ОБЧХ-коде C векторы* $\bar{e}$ *и* $\bar{f}$ *имеют одинаковую компоненту i, удовлетворяющую условиям следствия 2, а* $N\left(S\left(\bar{e}\right)\right) = N\left(S\left(\bar{f}\right)\right)$. *Тогда спектры синдромов* $S\left(\langle \bar{e} \rangle\right)$ *и* $S\left(\langle \bar{f} \rangle\right)$ *совпадают.*

Доказательство вытекает из следствия 3.

Замечание. Пусть ОБЧХ-код C не является примитивным, его длина $n = \dfrac{2^m - 1}{\tau}$ для некоторого целого $\tau > 1$. Тогда в этом коде может найтись до τ полных Г-орбит с одинаковыми нормами, но с попарно различными спектрами синдромов. Действительно, если синдром $S = \left(s_1, s_2, \ldots, s_t\right)$ имеет норму N, то эту же норму имеют и синдромы $S_i = \left(\alpha^{ik_1} s_1, \alpha^{ik_2} s_2, \ldots, \alpha^{ik_t} s_t\right)$ для примитивного элемента $\alpha \in GF\left(2^m\right)$ и всех целых i, $0 \le i \le 2^m - 2$. Количество различных таких синдромов вполне может достигать величины $2^m - 1$. Тогда их полное количество может распределиться как минимум по $\dfrac{2^m - 1}{n} = \tau$ полным Г-спектрам синдромов полных Г-орбит.

Пример 3. Согласно данным табл. 1 ОБЧХ-код $C_{65}\left(1, 5\right)$ имеет минимальное расстояние 8 и, следовательно, способен корректировать все ошибки весом 1–3. Одиночные ошибки составляют одну Г-орбиту с нормой 1, двойные делятся на 32 полные Г-орбиты. Для двойных ошибок каждое значение нормы соответствует в точности двум Г-орбитам, что подтверждает табл. 2, содержащая образующие $\bar{e} = \left(i, j\right)$ с единичными координатами на позициях i и j (остальные 63 – нулевые), компоненты s_1 и s_2 синдромов образующих $S\left(\bar{e}\right) = \left(s_1, s_2\right)$, а также норм синдромов образующих $N = N\left(S\left(\bar{e}\right)\right)$.

Таблица 2

Г-орбиты двойных ошибок

Table 2

Г-orbits of double errors

Образующие Г-орбит $\bar{e} = \left(i, j\right)$	Синдромы образующих $S\left(\bar{e}\right)$	Норма синдрома $N\left(S\left(\bar{e}\right)\right)$
$\left(1, 14\right), \left(1, 27\right)$	$\left(\alpha^{3822}, 0\right), \left(\alpha^{3549}, 0\right)$	0
$\left(1, 17\right), \left(1, 26\right)$	$\left(\alpha^{764}, \alpha^{4015}\right), \left(\alpha^{1535}, \alpha^{3775}\right)$	α^{195}
$\left(1, 16\right), \left(1, 33\right)$	$\left(\alpha^{4015}, \alpha^{4085}\right), \left(\alpha^{1528}, \alpha^{3935}\right)$	α^{390}
$\left(1, 15\right), \left(1, 20\right)$	$\left(\alpha^{1546}, \alpha^{4090}\right), \left(\alpha^{696}, \alpha^{3935}\right)$	α^{455}
$\left(1, 2\right), \left(1, 31\right)$	$\left(\alpha^{3119}, \alpha^{4090}\right), \left(\alpha^{3935}, \alpha^{4075}\right)$	α^{780}
$\left(1, 28\right), \left(1, 29\right)$	$\left(\alpha^{3093}, \alpha^{4090}\right), \left(\alpha^{3092}, \alpha^{4085}\right)$	α^{910}
$\left(1, 3\right), \left(1, 6\right)$	$\left(\alpha^{2143}, \alpha^{4085}\right), \left(\alpha^{4090}, \alpha^{1535}\right)$	α^{1560}
$\left(1, 13\right), \left(1, 32\right)$	$\left(\alpha^{1223}, \alpha^{3775}\right), \left(\alpha^{1594}, \alpha^{1535}\right)$	α^{1755}

Окончание табл. 2
Ending table 2

Образующие Г-орбит $\bar{e} = (i, j)$	Синдромы образующих $S(\bar{e})$	Норма синдрома $N(S(\bar{e}))$
$(1, 10), (1, 12)$	$(\alpha^{2656}, \alpha^{2815}), (\alpha^{2784}, \alpha^{3455})$	α^{1820}
$(1, 9), (1, 21)$	$(\alpha^{382}, \alpha^{4055}), (\alpha^{4075}, \alpha^{2045})$	α^{2145}
$(1, 8), (1, 24)$	$(\alpha^{773}, \alpha^{2045}), (\alpha^{1797}, \alpha^{3070})$	α^{2275}
$(1, 7), (1, 18)$	$(\alpha^{2659}, \alpha^{3935}), (\alpha^{1868}, \alpha^{4075})$	α^{2925}
$(1, 5), (1, 11)$	$(\alpha^{191}, \alpha^{4075}), (\alpha^{4085}, \alpha^{3070})$	α^{3120}
$(1, 22), (1, 30)$	$(\alpha^{174}, \alpha^{4055}), (\alpha^{166}, \alpha^{4015})$	α^{3185}
$(1, 4), (1, 25)$	$(\alpha^{3377}, \alpha^{4015}), (\alpha^{2446}, \alpha^{3455})$	α^{3510}
$(1, 19), (1, 23)$	$(\alpha^{1217}, \alpha^{1535}), (\alpha^{1473}, \alpha^{2815})$	α^{3640}

Данные вычислены для кода $C_{65}(1, 5)$, определенного над полем $GF(2^{12})$ с примитивным полиномом $p(x) = x^{12} + x^{10} + x^2 + x + 1$. Значения табл. 2 полностью противоречат сложившейся уверенности, что в классических БЧХ-кодах (как в примитивных, так и в непримитивных) нормы Г-орбит одиночных и двойных ошибок в обязательном порядке попарно различны (см. теорему 4.2 [6]).

Тройные ошибки в ОБЧХ-коде $C_{65}(1, 5)$ делятся на $\frac{1}{65}C_{65}^3 = \frac{65 \cdot 64 \cdot 63}{65 \cdot 2 \cdot 3} = 32 \cdot 21 = 672$ полные Г-орбиты. Вычисления показывают, что 586 из них имеют уникальные нормы, 78 – по две одинаковые нормы, а 8 – по четыре одинаковые нормы. Последний случай детализирован в табл. 3.

Таблица 3

Некоторые Г-орбиты тройных ошибок

Table 3

Some Г-orbits of triple errors

Образующая Г-орбиты $\bar{e} = (i, j)$	Синдром образующей $S(\bar{e})$	Норма синдрома $N(S(\bar{e}))$
$(1, 2, 34)$	$(\alpha^{129}, \alpha^{2010})$	α^{1365}
$(1, 3, 5)$	$(\alpha^{516}, \alpha^{3945})$	α^{1365}
$(1, 9, 17)$	$(\alpha^{2064}, \alpha^{3495})$	α^{1365}
$(1, 14, 27)$	$(\alpha^{2184}, 1)$	α^{1365}
$(1, 2, 3)$	$(\alpha^{258}, \alpha^{4020})$	α^{2730}
$(1, 5, 9)$	$(\alpha^{1032}, \alpha^{3795})$	α^{2730}
$(1, 14, 40)$	$(\alpha^{1092}, 1)$	α^{2730}
$(1, 17, 33)$	$(\alpha^{33}, \alpha^{2895})$	α^{2730}

Норменный метод коррекции ошибок в ОБЧХ-кодах

Метод алгебраических уравнений коррекции ошибок линейными кодами сводит поиск координат ошибок до нахождения корней этих уравнений в полях Галуа – полях определения кода C. Норменный метод еще более сокращает поисковые процедуры. Он требует рассортировки векторов-ошибок декодируемой совокупности K по Г-орбитам. Чтобы зафиксировать это разбиение, следует составить список K_Γ образующих Г-орбит ошибок корректируемой совокупности K, список $S(K_\Gamma)$ синдромов образующих и список $N_K = N(S(K_\Gamma))$ норм синдромов образующих. Инфокоммуникационная система, функционирующая на основе ОБЧХ-кода C, приняв очередное сообщение $\bar{x}$, вычисляет синдром его ошибок $S(\bar{x}) = (s_1^*, s_2^*, \ldots, s_t^*)$, а затем и норму $N_{\text{выч}} = N(S(\bar{x}))$.

Вычисленную норму сравниваем с данными списка N_K. Если $N_{\text{выч}} = N_i \in N_K$, то в списке $S(K_\Gamma)$ находим все синдромы $S_{i1}, S_{i2}, \ldots, S_{ij}$ с нормой $N_i = N_{\text{выч}}$. Искомый вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$ принадлежит единственной Г-орбите из множества $\langle \bar{e}_{it} \rangle$, $1 \le t \le j$, с синдромами образующих $S(\bar{e}_{it}) = S_{it}$. Если $s_1^* \neq 0$, то вычисляем частные $\frac{s_1^*}{s_1^{ik}}$ для всех первых компонент s_1^{ik} синдромов S_{ik}, $1 \le k \le j$. Из структуры спектра синдромов Г-орбит ошибок (формула (6)) и из принадлежности $S(\bar{x}) = (s_1^*, s_2^*, \ldots, s_t^*)$ какому-то конкретному из спектров $S(\langle \bar{e}_{it} \rangle)$, $1 \le t \le j$, следует, что существует единственное значение $k = q$, для которого вычисленное частное $\frac{s_1^*}{s_1^{iq}} = k_1 l$ для некоторого целого l. Если и $s_2^* \neq 0$, то для убедительности можно проверить, что и $\frac{s_2^*}{s_2^{iq}} = k_2 l$. Следовательно, $S(\bar{x})$ принадлежит спектру синдромов $S(\langle \bar{e}_{iq} \rangle)$ и получается i-кратным умножением компонент $S(\bar{e}_{iq})$ на коэффициенты из формулы (7). В силу формул (6) и (7) можно с уверенностью утверждать, что искомая ошибка $\bar{e} \in \langle \bar{e}_{iq} \rangle$ и, более того, что $\bar{e} = \sigma^l(\bar{e}_{iq})$. На выход декодера подается истинное сообщение $\bar{c} = \bar{x} + \bar{e}$.

Конечно, с ростом длин ОБЧХ-кодов, а также кратности исправляемых ошибок соответственно растут и названные списки образующих Г-орбит. Этот фактор в конце концов скажется на скорости работы норменного декодера. Применение G-орбит и их инвариантов позволит существенно сократить поисковые процедуры норменного метода.

G-орбиты ошибок и их инварианты в ОБЧХ-кодах

Циклотомическая подстановка φ задана на двоичном пространстве возможных ошибок E_n, которое, в общем, совпадает с пространством V_n, таким образом, чтобы ее действие отражалось на синдромах векторов-ошибок как действие автоморфизма Фробениуса в поле Галуа $GF(2^m)$ (см. теорему 2). Более того, имеет место следующая теорема.

Теорема 6. *В ОБЧХ-коде C для всякой* Г*-орбиты векторов-ошибок* $J \subset \mathrm{E}_n$ $\varphi(J) = J'$ *– новая* Г*-орбита. Если норма* $N_J = (N_{12}, N_{13}, \ldots, N_{(t-1)t})$ *с компонентами* $N_{ij} \in GF(2^m)$, *то* $N_{\varphi(J)} = (N_{12}^2, N_{13}^2, \ldots, N_{(t-1)t}^2)$.

Из первой части теоремы 6 следует наглядное строение G-орбит.

Теорема 7. *Для всякого вектора-ошибки* $\bar{e}$ *в ОБЧХ-коде C G-орбита* $\langle \bar{e} \rangle_G$ *имеет следующую структуру:* $\langle \bar{e} \rangle_G = \left\{ \langle \bar{e} \rangle_\Gamma, \langle \varphi(\bar{e}) \rangle_\Gamma, \ldots, \langle \varphi^{\mu-1}(\bar{e}) \rangle_\Gamma \right\}$ *для наименьшего целого* $\mu \ge 1$ *такого, что* $\langle \varphi^{\mu}(\bar{e}) \rangle_\Gamma = \langle \bar{e} \rangle_G$. *При этом* $\mu = m$ *или же является делителем m.*

Определение 5. В условиях теоремы 7 совокупность $N_{J_G} = \left\{ N(J_\Gamma), N(\varphi(J_\Gamma)), \ldots, N(\varphi^{\mu-1}(J_\Gamma)) \right\}$ всех попарно различных норм Г-орбит, составляющих G-орбиту J_G, называется норменным спектром этой G-орбиты. G-орбита J_G называется полной, если $|J_G| = mn$. Норменный спектр G-орбиты J_G называется полным, если $|N_{J_G}| = m$.

Теорема 8 (о полноте норменного спектра G-орбиты). *Пусть в ОБЧХ-коде C с* $t = 2$ *(с конструктивным расстоянием* $\partial = 2t + 1 = 5$*) норма* $N(J)$ Г*-орбиты J принадлежит полю* $GF(2^m)$, *но не принад-*

лежит ни одному из собственных подполей этого поля. Тогда норменный спектр N_{J_G} является полным и сама G-орбита J_G также является полной.

Доказательство. Пусть в условиях теоремы норма некоторой Г-орбиты $N(J) = N_0 \in GF(2^m)$ и не принадлежит ни одному из подполей данного поля. Так как всякий элемент поля $GF(2^m)$ является алгебраическим над $Z/2Z$, N_0 – это корень единственного неприводимого над $Z/2Z$ полинома степени m. Следовательно, N_0 имеет $m-1$ сопряженных в поле $GF(2^m)$ элементов: $\left\{N_0, N_0^2, N_0^4, \ldots, N_0^{2^{m-1}}\right\}$. Очевидно, что они различны и, как следует из теоремы 6, составляют спектр норм G-орбиты J_G, состоящей из уникальных m элементов. Теорема доказана.

Пусть $\overline{e}$ – произвольный вектор-ошибка с синдромом $S(\overline{e})$ и нормой $N = N(S(\overline{e}))$ в ОБЧХ-коде C с $t = 2$, причем $N \in GF(2^m)$. Тогда в силу теорем 6 и 7 норменный спектр G-орбиты J_G есть множество $T = \left\{N, N^2, \ldots, N^{2^{\mu-1}}\right\}$ для целого $\mu = m$ или же делящего m. Как всякий элемент поля $GF(2^m)$, N является алгебраическим над $Z/2Z$, т. е. выступает корнем некоторого полинома с коэффициентами из $Z/2Z$. Следовательно, в кольце полиномов $Z/2Z[x]$ существует единственный неприводимый многочлен с корнем N, обозначаемый, как правило, через $\mathrm{Irr}(N, x)$. Согласно теории полей Галуа множество T представляет все множество корней полинома $\mathrm{Irr}(N, x)$. В силу теоремы Безу

$$\mathrm{Irr}(N, x) = x^{\mu} + p_{\mu-1}x^{\mu-1} + \ldots + p_0 = (x - N)\cdot\left(x - N^2\right)\cdot\ldots\cdot\left(x - N^{2^{\mu-1}}\right). \quad (9)$$

Теорема 9. *В ОБЧХ-коде C при $t = 2$ (с конструктивным расстоянием $\partial = 2t + 1 = 5$) для всякой G-орбиты J_G с нормой $N \in GF(2^m)$ множество T и полином (9) являются инвариантами этой G-орбиты, т. е. не зависят от выбора представителя $\overline{e} \in J_G$.*

Определение 6. В условиях теоремы 9 полином (9) называется полиномиальным инвариантом G-орбиты J_G.

Теорема 10. *Пусть $\langle\overline{e}_1\rangle_G$ и $\langle\overline{e}_2\rangle_G$ – две G-орбиты векторов-ошибок из декодируемой ОБЧХ-кодом C с $t = 2$ совокупности K, имеющие различные полиномиальные инварианты $p_1(x)$ и $p_2(x)$. Тогда множества T_1 и T_2 норменных спектров данных G-орбит не пересекаются.*

Доказательство следует из того факта, что различные неприводимые полиномы не могут иметь общих корней.

Пример 4. В продолжение примера 3 заметим, что в коде $C_{65}(1, 5)$ множество Г-орбит векторов-ошибок весом 1–3 разбивается на 67 G-орбит. Одна G-орбита совпадает с Г-орбитой одиночных ошибок, их синдромы имеют единичную норму. Двойные ошибки укладываются в шесть G-орбит, две из них имеют уникальные инварианты, что подробно показано в табл. 4.

Таблица 4

Полиномиальные инварианты *G*-орбит двойных ошибок для кода $C(1, 5)$ длиной 65

Table 4

Polynomial invariants of double error *G*-orbits for code $C(1, 5)$ at length 65

G-орбита	Количество Г-орбит	Полиномиальный инвариант
$(1, 2)$	6	$1 + x + x^2 + x^4 + x^6$
$(1, 4)$	6	$1 + x + x^3$
$(1, 6)$	6	$1 + x + x^2 + x^4 + x^6$
$(1, 8)$	6	$1 + x^3 + x^6$
$(1, 12)$	6	$1 + x^3 + x^6$
$(1, 14)$	2	x

Отметим интересную особенность структуры Г-орбит внутри некоторых *G*-орбит. Рассмотрим *G*-орбиту $\langle(1, 4)\rangle_G = \{\langle(1, 4)\rangle_\Gamma, \langle(1, 32)\rangle_\Gamma, \langle(1, 18)\rangle_\Gamma, \langle(1, 25)\rangle_\Gamma, \langle(1, 13)\rangle_\Gamma, \langle(1, 7)\rangle_\Gamma\}$. Запишем спектр норм Г-орбит внутри орбиты $\langle(1, 4)\rangle_G$: $N_{\langle(1, 4)\rangle_G} = \{\alpha^{3510}, \alpha^{1755}, \alpha^{2925}, \alpha^{3510}, \alpha^{1755}, \alpha^{2925}\} = \{\alpha^{3510}, \alpha^{1755}, \alpha^{2925}\}$. Заметим, что норменный спектр имеет мощность $\left|N_{\langle(1, 4)\rangle_G}\right| = 3$, в то время как *G*-орбита характеризуется мощностью $\left|\langle(1, 4)\rangle_G\right| = 6$, а значит, *G*-орбита мощностью 6 имеет полиномиальный инвариант степени 3. Также отметим, что *G*-орбита $\langle(1, 14)\rangle_G = \{\langle(1, 14)\rangle_\Gamma, \langle(1, 27)\rangle_\Gamma\}$ состоит из двух Г-орбит с одинаковыми нулевыми нормами.

Тройные ошибки разбиты на 60 *G*-орбит. Уникальные полиномы в качестве своей характеристики имеют 52 *G*-орбиты, остальные 8 орбит имеют повторяющиеся по 2 раза нормы. Опустим список всех *G*-орбит тройных ошибок ввиду их большого объема. Отметим только, что ситуация несовпадения мощности орбиты и спектра норм, описанная выше, также встречается в двух *G*-орбитах тройных ошибок.

Также следует упомянуть о том, что полиномиальные инварианты $1 + x + x^3$ и $1 + x^3 + x^6$ соответствуют некоторым *G*-орбитам и двойных, и тройных ошибок одновременно.

Полиномиально-норменный метод коррекции ошибок ОБЧХ-кодами

Множество Γ_K Г-орбит векторов-ошибок корректируемой ОБЧХ-кодом *C* совокупности *K* делим на более крупные блоки – *G*-орбиты – и получаем множество G_K. Далее группируем норменные спектры T_i этих *G*-орбит и сопоставляем их полиномиальные инварианты – список $K_{p_i(x)}$. Приняв очередное сообщение $\bar{x}$, вычислив его синдром $S(\bar{x})$ и норму $N^* = N(S(\bar{x}))$ согласно формуле (8), мы можем указать неприводимый над $Z/2Z$ полином $p^*(x)$ с корнем N^*. Этот полином ищем в списке $K_{p_i(x)}$. Пусть $p^*(x) = p_j(x)$. Полиномиальный инвариант $p_j(x)$ имеет небольшой список *G*-орбит: $\{\langle\bar{e}_{j1}\rangle_G, \langle\bar{e}_{j2}\rangle_G, \ldots, \langle\bar{e}_{js}\rangle_G\} \subset G_K$. В каждой из перечисленных *G*-орбит находим по единственной Г-орбите с нормой N^*. Дальше действуем в соответствии с приведенным выше норменным методом.

Пример 5. Продемонстрируем работу полиномиально-норменного метода на ОБЧХ-коде из примера 3.

Пусть декодер некоторой ИКС, использующий код $C_{65}(1, 5)$, принял следующее сообщение:

$$\bar{x} = \begin{pmatrix} 0, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, \mathbf{0}, 0, 0, 0, 0, \\ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, \mathbf{0}, 1, 0, 0, 0, 1, 1, 0 \end{pmatrix}.$$

Для заданного сообщения вычисляем синдром ошибки $S(\bar{x}) = (\alpha^{849}, \alpha^{2760})$ и норму синдрома $N^* = N(S(\bar{x})) = \frac{s_2}{s_1^5} = \frac{\alpha^{2760}}{\alpha^{849 \cdot 5}} = \alpha^{2610}$. Далее в списке полиномиальных инвариантов $K_{p_i(x)}$ отыщем полином $p^*(x) = 1 + x^2 + x^3 + x^{11} + x^{12}$ с корнем N^*. Данному полиномиальному инварианту соответствуют две *G*-орбиты: $N^*G = \{\langle(1, 4, 22)\rangle_G, \langle(1, 4, 30)\rangle_G\}$. Среди Г-орбит, входящих в *G*-орбиты из списка N^*G, находим две Г-орбиты с нормой N^*: $N^*\Gamma = \{\langle(1, 15, 42)\rangle_\Gamma, \langle(1, 14, 32)\rangle_\Gamma\}$. Далее действуем в соответствии с норменным методом. Для каждой Г-орбиты из списка $N^*\Gamma$ находим значение $l_i = \frac{\deg(s_1) - \deg(s_1^k)}{z}$, где $1 \le k \le 2$, $z = \frac{2^{12} - 1}{65} = 63$, а s_1^k – первая компонента синдрома образующих для орбит из списка $N^*\Gamma$. Имеем $l_1 = \frac{849 - 1920}{63} = -17$, $l_2 = \frac{849 - 2250}{63} = -\frac{467}{21}$. Фиксируем целое $l = l_1 = -17$ и вычисляем искомый вектор-ошибку $\bar{e} = \sigma^{-18(\mathrm{mod}\,65)}(1, 15, 42) = (25, 49, 63)$. Верное сообщение получим по формуле $\bar{c} = \bar{x} + \bar{e}$.

Пример 6. Отдельно проанализируем случай, описанный в примере 3. Рассмотрим некоторую ошибку из G-орбиты $\langle(1, 4)\rangle_G$. Напомним, что в данной G-орбите мощность норменного спектра не совпадает с мощностью самой орбиты.

Пусть декодер ИКС, использующий код $C_{65}(1, 5)$, принял следующее сообщение:

$$\overline{x} = \begin{pmatrix} 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, \mathbf{0}, 0, 0, 0, 0, \\ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 \end{pmatrix}.$$

Вычисляем синдром $S(\overline{x}) = \left(\alpha^{2785}, \alpha^{470}\right)$. Далее определяем норму синдрома $N^* = N\left(S(\overline{x})\right) = \alpha^{2925}$. В списке $K_{p_i(x)}$ полиномиальных инвариантов находим подходящий полином с корнем N^*: $p^*(x) = 1 + x + x^3$. Инварианту $p^*(x)$ соответствуют две G-орбиты: $N^*G = \left\{\langle(1, 4)\rangle_G, \langle(1, 6, 11)\rangle_G\right\}$. Среди Г-орбит, входящих в G-орбиты из списка N^*G, находим Г-орбиты с нормой N^*: $N^*\Gamma = \left\{\langle(1, 18)\rangle_\Gamma, \langle(1, 7)\rangle_\Gamma, \langle(1, 6, 11)\rangle_\Gamma, \langle(1, 16, 41)\rangle_\Gamma\right\}$. Далее действуем аналогично примеру 4. Для каждой Г-орбиты из списка $N^*\Gamma$ находим значение $l_i = \dfrac{\deg(s_1) - \deg\left(s_1^k\right)}{z}$, где $1 \le k \le 4$, $z = 63$. Несложными вычислениями получаем следующие значения: $l_1 = \dfrac{-131}{9}$, $l_2 = -2$, $l_3 = \dfrac{1235}{63}$, $l_4 = \dfrac{710}{63}$. Далее фиксируем целое $l = l_2 = -2$ и получаем искомый вектор-ошибку $\overline{e} = \sigma^{-2(\mathrm{mod}\,65)}(1, 7) = (3, 9)$. Приведенный пример показывает, что аномалии норменного спектра не влияют на корректность работы декодера.

Заключение

Класс ОБЧХ-кодов существенно шире класса классических БЧХ-кодов. Для исследования их свойств и корректирующих возможностей требуются трудоемкие математические и компьютерные вычисления. Они показывают наличие ОБЧХ-кодов, по корректирующим возможностям превосходящих все имеющиеся классические БЧХ-коды данной длины. Для декодирования ошибок, кратность которых совпадает с конструктивной, вполне годны синдромные методы, однако они требуют соответствующих модификаций и определенных усложнений. Для ОБЧХ-кодов с минимальным расстоянием, превосходящим конструктивное, подходят только норменные и полиномиально-норменные методы. При этом применима теория норм синдромов в упрощенном виде, что вовсе не является недостатком, так как облегчает вычисления и использование для них перестановочных методов.

Таким образом, в помехоустойчивом кодировании найдены новые линейные коды с эффективными декодирующими алгоритмами, перспективные для приложений.

Библиографические ссылки

1. Мак-Вильямс ФДж, Слоэн НДжА. *Теория кодов, исправляющих ошибки.* Грушко ИИ, Зиновьева ВА, переводчики; Бассалыго ЛА, редактор. Москва: Связь; 1979. 744 с.

2. Морелос-Сарагоса Р. *Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение.* Афанасьев ВБ, переводчик. Москва: Техносфера; 2005. 320 с.

3. Кудряшов БД. *Основы теории кодирования.* Санкт-Петербург: БХВ-Петербург; 2016. 400 с.

4. Конопелько ВК, Липницкий ВА, Дворников ВД, Бобов МН, Королев АИ, Борискевич АА и др. *Теория прикладного кодирования.* Конопелько ВК, редактор. Минск: БГУИР; 2004. 2 тома.

5. Конопелько ВК, Липницкий ВА. *Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов.* Минск: БГУИР; 2000. 241 с.

6. Липницкий ВА, Конопелько ВК. *Норменное декодирование помехоустойчивых кодов и алгебраические уравнения.* Минск: Издательский центр БГУ; 2007. 239 с.

7. Липницкий ВА. *Теория норм синдромов.* Минск: БГУИР; 2011. 96 с.

8. Липницкий ВА, Середа ЕВ. Полиномиальные инварианты G-орбит ошибок в непримитивных БЧХ-кодах с конструктивным расстоянием 5. *Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 2. Матэматыка. Фізіка. Інфарматыка, вылічальная тэхніка і кіраванне*. 2019;9(1):118–127.

9. Липницкий ВА, Середа ЕВ. Свойства G-орбит тройных ошибок и их инвариантов в кодах Боуза – Чоудхури – Хоквингема C_7. *Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-тэхнічных навук.* 2019;64(1):110–117. DOI: 10.29235/1561-8358-2019-64-1-110-117.

10. Кушнеров АВ, Липницкий ВА. Свойства и применение полиномиальных инвариантов G-орбит ошибок в реверсивных кодах. *Журнал Белорусского государственного университета. Математика. Информатика.* 2018;3:21–28.

11. Блейхут Р. *Теория и практика кодов, контролирующих ошибки.* Грушко ИИ, Блиновский ВМ, переводчики; Зигангиров КШ, редактор. Москва: Мир; 1986. 576 с.

12. Лидл Р, Нидеррайтер Г. *Конечные поля.* Жуков АЕ, Петров ВИ, переводчики; Нечаев ВИ, редактор. Москва: Мир; 1988. 2 тома.

13. Lu C-C, Welch LR. On automorphism groups of binary primitive BCH codes. In: *Proceedings of 1994 IEEE International symposium on information theory; 1994 June 27 – July 1; Trondheim, Norway*. [S. l.]: Institute of Electrical and Electronics Engineers; 1994. p. 51. DOI: 10.1109/ISIT.1994.394919.

14. Липницкий ВА, Олексюк АО. Теория норм синдромов и плюс-декодирование. *Доклады БГУИР.* 2014;8:72–78.

15. Липницкий ВА, Олексюк АО. Перестановочный декодер для коррекции многократных ошибок непримитивными БЧХ-кодами. *Доклады БГУИР.* 2015;3:117–123.

16. Кушнеров АВ, Липницкий ВА, Королёва МН. Обобщенные коды Боуза – Чоудхури – Хоквингема и их параметры. *Вестник Полоцкого государственного университета. Серия С: Фундаментальные науки.* 2018;4:28–33.

17. Кушнеров АВ, Липницкий ВА, Королева МН. Свойства и параметры обобщенных кодов Боуза – Чоудхури – Хоквингема. *Весці Нацыянальнай акадэміі навук Беларусі. Серыя фізіка-матэматычных навук.* 2020;56(2):157–165. DOI: 10.29235/1561-2430-2020-56-2-157-165.

18. Липницкий ВА. *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа.* Минск: БГУИР; 2005. 88 с.

19. Виноградов ИМ. *Основы теории чисел.* 8-е издание, исправленное. Москва: Наука; 1972. 167 с.

References

1. MacWilliams FJ, Sloane NJA. *The theory of error-correcting codes*. Amsterdam: North-Holland Publishing Company; 1977. XX, 762 p. (North-Holland mathematical library; volume 16).

Russian edition: MacWilliams FJ, Sloane NJA. *Teoriya kodov, ispravlyayushchikh oshibki*. Grushko II, Zinov'eva VA, translators; Bassalygo LA, editor. Moscow: Svyaz'; 1979. 744 p.

2. Morelos-Zaragoza RH. *The art of error correcting coding*. Chichester: Jon Wiley & Sons; 2002. 238 p.

Russian edition: Morelos-Zaragoza R. *Iskusstvo pomekhoustoichivogo kodirovaniya. Metody, algoritmy, primenenie*. Afanas'ev VB, translator. Moscow: Tekhnosfera; 2005. 320 p.

3. Kudryashov BD. *Osnovy teorii kodirovaniya* [Fundamentals of coding theory]. Saint Petersburg: BHV-Petersburg; 2016. 400 p. Russian.

4. Konopel'ko VK, Lipnitski VA, Dvornikov VD, Bobov MN, Korolev AI, Boriskevich AA, et al. *Teoriya prikladnogo kodirovaniya* [Theory of applied coding]. Konopel'ko VK, editor. Minsk: Belarusian State University of Informatics and Radioelectronics; 2004. 2 volumes. Russian.

5. Konopel'ko VK, Lipnitski VA. *Teoriya norm sindromov i perestanovochnoe dekodirovanie pomekhoustoichivykh kodov* [Syndrome norm theory and permutation decoding of error-correcting codes]. Minsk: Belarusian State University of Informatics and Radioelectronics; 2000. 241 p. Russian.

6. Lipnitski VA, Konopel'ko VK. *Normennoe dekodirovanie pomekhoustoichivykh kodov i algebraicheskie uravneniya* [Norm decoding of error-correcting codes and algebraic equations]. Minsk: Publishing Center of Belarusian State University; 2007. 239 p. Russian.

7. Lipnitski VA. *Teoriya norm sindromov* [Theory of syndrome norms]. Minsk: Belarusian State University of Informatics and Radioelectronics; 2011. 96 p. Russian.

8. Lipnitski VA, Sereda EV. Polynomial invariants of *G*-orbits of errors in non-primitive BCH codes with designed distance of 5. *Vesnik Grodzenskaga dzjarzhawnaga wniversitjeta imja Janki Kupaly. Seryja 2. Matjematyka. Fizika. Infarmatyka, vylichal'naja tjehnika i kiravanne.* 2019;9(1):118–127. Russian.

9. Lipnitski VA, Serada AU. Properties of triple error orbits *G* and their invariants in Bose – Chaudhuri – Hocquenghem codes C_7. *Proceedings of the National Academy of Sciences of Belarus. Physical-technical series.* 2019;64(1):110–117. Russian. DOI: 10.29235/1561-8358-2019-64-1-110-117.

10. Kushnerov AV, Lipnitski VA. Properties and applications of *G*-orbits polynomial invariants of errors in reverse codes. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;3:21–28. Russian.

11. Blahut RE. *Theory and practice of error control codes*. Reading: Addison-Wesley Publishing Company; 1984. 452 p.

Russian edition: Blahut R. *Teoriya i praktika kodov, kontroliruyushchikh oshibki*. Grushko II, Blinovskii VM, translators; Zigangirov KSh, editor. Moscow: Mir; 1986. 576 p.

12. Lidl R, Niederreiter H. *Introduction to finite fields and their applications.* Cambridge: Cambridge University Press; 1986. VIII, 407 p.

Russian edition: Lidl R, Niederreiter H. *Konechnye polya*. Zhukov AE, Petrov VI, translators; Nechaev VI, editor. Moscow: Mir; 1988. 2 volumes.

13. Lu C-C, Welch LR. On automorphism groups of binary primitive BCH codes. In: *Proceedings of 1994 IEEE International symposium on information theory; 1994 June 27 – July 1; Trondheim, Norway*. [S. l.]: Institute of Electrical and Electronics Engineers; 1994. p. 51. DOI: 10.1109/ISIT.1994.394919.

14. Lipnitski VA, Aliaksiuk AO. Theory of normal syndrome and plus-decoding. *Doklady BGUIR.* 2014;8:72–78. Russian.

15. Lipnitski VA, Aliaksiuk AO. Correction commute decoder for multiple errors with not primitive BCH-codes. *Doklady BGUIR.* 2015;3:117–123. Russian.

16. Kushnerov AV, Lipnitski VA, Koroliova MN. Properties and options of the generic BCH-codes. *Vestnik Polotskogo gosudarstvennogo universiteta. Seriya S: Fundamental'nye nauki.* 2018;4:28–33. Russian.

17. Kushnerov AV, Lipnitski VA, Koroliova MN. The properties and parameters of generic Bose – Chaudhuri – Hocquenghem codes. *Proceedings of the National Academy of Sciences of Belarus. Physics and mathematics series.* 2020;56(2):157–165. Russian. DOI: 10.29235/1561-2430-2020-56-2-157-165.

18. Lipnitski VA. *Sovremennaya prikladnaya algebra. Matematicheskie osnovy zashchity informatsii ot pomekh i nesanktsionirovannogo dostupa* [Modern applied algebra. The mathematical principles of protecting information from interference and unauthorized access]. Minsk: Belarusian State University of Informatics and Radioelectronics; 2005. 88 p. Russian.

19. Vinogradov IM. *Osnovy teorii chisel* [Fundamentals of number theory]. 8th edition, revised. Moscow: Nauka; 1972. 167 p. Russian.

Статья поступила в редколлегию 29.01.2020.
Received by editorial board 29.01.2020.