

**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ****INFORMATION TECHNOLOGIES AND SYSTEMS**

УДК 512 (075.8)

<https://doi.org/10.29235/1561-8358-2019-64-1-110-117>

Поступила в редакцию 25.01.2018

Received 25.01.2018

**В. А. Липницкий<sup>1</sup>, Е. В. Серeda<sup>2</sup>**<sup>1</sup>*Военная академия Республики Беларусь, Минск, Беларусь*<sup>2</sup>*Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь***СВОЙСТВА  $G$ -ОРБИТ ТРОЙНЫХ ОШИБОК И ИХ ИНВАРИАНТОВ В КОДАХ БОУЗА – ЧОУДХУРИ – ХОКВИНГЕМА  $C_7$** 

**Аннотация.** Данная работа является дальнейшим развитием теории норм синдромов (ТНС): расширяется теория полиномиальных инвариантов  $G$ -орбит ошибок относительно группы  $G$  автоморфизмов двоичных циклических кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов), получаемой присоединением к группе  $\Gamma$  степеней циклотомической подстановки и практически исчерпывающей группу автоморфизмов БЧХ-кодов. Определено, что для БЧХ-кодов с конструктивным расстоянием пять полиномиальные инварианты, как и нормы синдромов, имеют скалярный характер и являются взаимно-однозначными характеристиками своих орбит. Для примитивных циклических БЧХ-кодов с конструктивным расстоянием семь вслед за нормами синдромов, становящимися уже векторными величинами, вводятся соответствующие векторные полиномиальные инварианты, исследуются их основные свойства. Установлено, что нарушается свойство взаимной однозначности: существуют  $G$ -орбиты-изомеры, различные, но имеющие одинаковые векторные полиномиальные инварианты. Обосновано и на примерах демонстрируется, что это обстоятельство незначительно осложняет алгоритмы декодирования ошибок на основе полиномиальных инвариантов.

**Ключевые слова:** помехоустойчивое кодирование, циклические линейные коды, примитивные БЧХ-коды, автоморфизмы кодов, орбиты ошибок, синдромы ошибок, нормы синдромов, полиномиальные инварианты орбит ошибок

**Для цитирования:** Липницкий, В. А. Свойства  $G$ -орбит тройных ошибок и их инвариантов в кодах Боуза – Чоудхури – Хоквингема  $C_7$  / В. А. Липницкий, Е. В. Серeda // Вест. Нац. акад. наук Беларуси. Сер. физ.-техн. наук. – 2019. – Т. 64, № 1. – С. 110–117. <https://doi.org/10.29235/1561-8358-2019-64-1-110-117>

**V. A. Lipnitski<sup>1</sup>, A. U. Serada<sup>2</sup>**<sup>1</sup>*Military Academy of the Republic of Belarus, Minsk, Belarus*<sup>2</sup>*Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus***PROPERTIES OF TRIPLE ERROR ORBITS  $G$  AND THEIR INVARIANTS IN BOSE – CHAUDHURI – HOCQUENGHEM CODES  $C_7$** 

**Abstract.** This work is the further development of the theory of norms of syndromes: the theory of polynomial invariants of  $G$ -orbits of errors expands with the group  $G$  of automorphisms of binary cyclic BCH codes obtained by joining the degrees of cyclotomic permutation to the group  $\Gamma$  and practically exhausting the group of automorphisms of BCH codes. It is determined that polynomial invariants, like the norms of syndromes, have a scalar character and are one-to-one characteristics of their orbits for BCH codes with a constructive distance of five. The paper introduces the corresponding vector polynomial invariants for primitive cyclic BCH codes with a constructive distance of seven, next to the norms of the syndromes that are already vector quantities; the basic properties of the vector polynomial invariants are investigated. It is established that the property of mutual unambiguity is violated: there are  $G$ -orbit-isomers, which are different, but have the same vector polynomial invariants. It is substantiated and demonstrated by examples that this circumstance greatly complicates error decoding algorithms based on polynomial invariants.

**Keywords:** noise-immune encoding, cyclic linear codes, primitive BCH codes, code automorphism, orbit of errors, syndrome of errors, norm of syndrome, polynomial invariant of orbit of errors

**For citation:** Lipnitski V. A., Serada A. U. Properties of triple error orbits  $G$  and their invariants in Bose – Chaudhuri – Hocquenghem codes  $C_7$ . *Vesti Natsyunal'noi akademii nauk Belarusi. Seriya fizika-technichnykh nauk = Proceedings of the National Academy of Sciences of Belarus. Physical-technical series*, 2019, vol. 64, no. 1, pp. 110–117 (in Russian). <https://doi.org/10.29235/1561-8358-2019-64-1-110-117>

**Введение.** Созданная на рубеже XX–XXI вв. теория норм синдромов [1–3] дала норменный метод декодирования ошибок. Этот метод в реверсивных кодах и в кодах Боуза – Чоудхури – Хоквингема (БЧХ-кодах) действует на порядок быстрее иных синдромных методов, легко реализуется на ПЛИС, отличается усеченной процедурой поиска корректируемой ошибки, конструктивными возможностями расширения спектра исправляемых ошибок [2].

В семействе циклических БЧХ-кодов нечетной длины автоморфизм Фробениуса поля определения кода порождает автоморфизмы – циклотомические подстановки, которые вместе с группой  $\Gamma$  циклических сдвигов координат векторов образуют некоммутативную группу  $G$  автоморфизмов БЧХ-кодов [2–4].  $G$ -орбиты ошибок состоят из специальным образом взаимосвязанных  $\Gamma$ -орбит векторов-ошибок [2, 3]. Открытие полиномиальных инвариантов  $G$ -орбит ошибок [5, 6] создает хорошие перспективы к декодированию больших спектров ошибок. В данной работе расширяется понятие полиномиальных инвариантов, исследуются дальнейшие свойства  $G$ -орбит ошибок и свойства новых полиномиальных инвариантов

**БЧХ-коды.** Рассмотрим циклические примитивные двоичные БЧХ-коды  $C$  длиной  $n = 2^m - 1$ , задаваемые проверочными матрицами вида

$$H = [\alpha^i, \alpha^{3i}, \alpha^{5i}]^T, \quad 0 \leq i \leq n-1, \quad (1)$$

где  $\alpha$  – корень примитивного неприводимого над  $Z/2Z$  полинома степени  $m$ ,  $m \geq 3$  [2–4]. Минимальное расстояние данных кодов  $d$  равно 7 [4], что позволяет им корректировать одиночные, двойные и тройные ошибки, дать рассматриваемым БЧХ-кодам более точное обозначение  $C_7$ .

Пусть инфокоммуникационная система (ИКС), основанная на БЧХ-коде  $C_7$ , приняла сообщение  $\bar{x}$ . Приемное устройство ИКС в обязательном порядке вычисляет синдром ошибок  $S(\bar{x}) = H \cdot \bar{x}^T = (s_1, s_2, s_3)^T$ . Здесь  $s_1, s_2, s_3$  – элементы поля Галуа  $GF(2^m)$  из  $2^m$  элементов. Условие  $d = 7$  влечет попарное различие синдромов векторов-ошибок весом 1–3. Неравенство  $S(\bar{x}) \neq \bar{0}$  свидетельствует о наличии ошибок в принятом сообщении:  $\bar{x} = \bar{c} + \bar{e}$ , где  $\bar{c}$  – истинное передаваемое сообщение;  $\bar{e}$  – вектор ошибок, который наложился на сообщение в процессе передачи  $\bar{c}$  в канале с шумами. Поскольку  $H \cdot \bar{c}^T = \bar{0}$ , то  $S(\bar{x}) = S(\bar{e})$  зависит только от вектора-ошибки  $\bar{e}$ . Координаты вектора-ошибки  $\bar{e}$  весом 3 находятся, как правило, решением следующей системы

$$\text{алгебраических уравнений: } \begin{cases} x + y + z = s_1, \\ x^3 + y^3 + z^3 = s_2, \\ x^5 + y^5 + z^5 = s_3, \end{cases} \text{ которая преобразуется к кубическому уравнению}$$

(см. [2, 3]). Над полями Галуа характеристики 2 не существует достаточно эффективных алгоритмов решения алгебраических уравнений, а имеющиеся трудоемки в реализации (см., к примеру, [2, п. 9.2; 3, п. 2.9; 7, гл. 5]).

Перспективной альтернативой синдромному методу алгебраических уравнений является применение автоморфизмов кодов [1–3]. Перейдем к рассмотрению сути метода автоморфизмов применительно к примитивным циклическим БЧХ-кодам.

**Г-орбиты ошибок, их спектры и нормы синдромов.** Группа  $\Gamma$  состоит из степеней циклической подстановки  $\sigma$ , действующей на каждый вектор  $\bar{x} = (x_1, x_2, \dots, x_n)$  по правилу

$$\sigma(\bar{x}) = (x_n, x_1, x_2, \dots, x_{n-1}). \quad (2)$$

Таким образом, группа  $\Gamma$  является коммутативной циклической группой порядка  $n$ . Она принадлежит группе автоморфизмов любого циклического кода длиной  $n$ , в частности БЧХ-кода с проверочной матрицей (1).

Для всякой вектор-ошибки  $\bar{e} = (e_1, e_2, \dots, e_n)$  ее  $\Gamma$ -орбита описывается выражением

$$\langle \bar{e} \rangle_\Gamma = \langle \bar{e} \rangle = \{ \bar{e}, \sigma(\bar{e}), \dots, \sigma^{v-1}(\bar{e}) \}, \quad (3)$$

где  $v$  – наименьшее натуральное число с условием:  $\sigma^v(\bar{e}) = \bar{e}$ . При этом  $v$  делит  $n$  или же  $v = n$ . Во втором случае  $\Gamma$ -орбита  $\langle \bar{e} \rangle$  имеет максимально возможную мощность и потому называется полной.

Действие  $\sigma$  на вектор  $\bar{e}$  по формуле (2) в БЧХ-коде  $C$  с проверочной матрицей (1) синхронно сопровождается столь же четким изменением синдрома [1–3]: если  $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2, s_3)^T$ , то

$$S(\sigma(\bar{e})) = H \cdot (\sigma(\bar{e}))^T = (\alpha \cdot s_1, \alpha^3 \cdot s_2, \alpha^5 \cdot s_3)^T. \quad (4)$$

Равенство (4) послужило основой для определения нормы синдрома в БЧХ-коде  $C_7$  как вектора  $\bar{N} = \bar{N}(S(\bar{e})) = (N_1, N_2, N_3)$  с тремя координатами, задаваемыми следующими формулами:

$$N_1 = s_2/s_1^3; \quad N_2 = s_3/s_1^5; \quad N_3 = s_3^3/s_2^5. \quad (5)$$

При  $N_1 \neq 0$  (что возможно лишь при условиях:  $s_1 \neq 0, s_2 \neq 0$ ) компонента  $N_3$  однозначно выражается через первые две компоненты:  $N_3 = N_2^3/N_1^5$  и, следовательно, ее можно не принимать в расчет. Если же  $s_1 = 0$ , то компоненты  $N_1$  и  $N_2$  вектора  $\bar{N}$  становятся вырожденными и информационную нагрузку начинает нести только компонента  $N_3$ . Вычисленная по формулам (5) норма  $\bar{N}$  не меняется при действии подстановки  $\sigma$ , является инвариантом для векторов-ошибок каждой отдельно взятой  $\Gamma$ -орбиты, а потому называется нормой самой  $\Gamma$ -орбиты векторов-ошибок.

Достаточно стройная система свойств норм синдромов (см. [1–3]), в частности предложение 5.4 [3] о попарном различии норм  $\Gamma$ -орбит ошибок весом 1, 2, 3 и предложение 5.2 [3] о том, что в примитивном БЧХ-коде из равенства норм двух полных  $\Gamma$ -орбит ошибок следует совпадение их спектров синдромов, послужила основой перестановочных норменных методов коррекции ошибок в рассматриваемых и более широких классах БЧХ-кодов. Специфика этих методов в том, что вместо поиска ошибки с вычисленным синдромом во множестве всех исправляемых ошибок проводится поиск вычисленной нормы в более узком списке норм декодируемых  $\Gamma$ -орбит ошибок. Таким образом, поисковые процедуры в норменном декодере сокращаются, как минимум, в  $n$  раз.

Стимулируемое потребностями приложений увеличение хотя бы на единицу параметра  $m$  практически удваивает основной параметр  $n$ , что тянет за собой рост остальных параметров кода, включая и количество декодируемых  $\Gamma$ -орбит ошибок. Через несколько подобных итераций приходим к невероятному росту всех данных о применяемом коде. Выход – в разумном ограничении параметров применяемых кодов и в применении для декодирования более крупных объединений ошибок –  $G$ -орбит векторов-ошибок.

**Специфика синдромов и  $\Gamma$ -орбит тройных ошибок.** У двойных ошибок первая компонента синдрома всегда отлична от нуля. У тройных же ошибок любая из трех компонент синдрома может принимать любое значение из поля  $GF(2^m)$ , в частности может быть равной нулю. Случаи, когда две компоненты синдрома одновременно равны нулю, исследованы в [2, предложение 3.15]: если  $s_1 = 0$ , то  $s_2 \neq 0$ ;

равенство  $S(\bar{e}) = (0, s_2, 0)$ ,  $s_2 \neq 0$ , возможно только в случае  $n = 3l$  для единственной  $\Gamma$ -орбиты ошибок  $\langle (1, l+1, 2l+1) \rangle$  мощностью  $l$ , порожденной вектором-ошибкой с единицами на указанных позициях;

синдром  $S(\bar{e}) = (s_1, 0, 0)$ ,  $s_1 \neq 0$ , возможен только при  $m = 3l$  и в этом случае только для векторов-ошибок единственной полной  $\Gamma$ -орбиты ошибок  $\langle (1, 2a+1, 2b+1) \rangle$ , где  $\alpha^a = t_1$  – корень уравнения  $t^3 + t^2 + 1 = 0$ ,  $\alpha^b = t_2$  для  $t_2 = t_1 + t_1^2$ ; здесь  $\bar{s} = s$  для целых  $s$ ,  $1 \leq s \leq n$ ,  $\bar{s} = s - n$  для целых  $s$ ,  $n+1 \leq s \leq 2n$ .

Как и для двойных ошибок, все  $\Gamma$ -орбиты тройных ошибок полные, за исключением единственного отмеченного выше случая  $\Gamma$ -орбиты  $J = \langle (1, l+1, 2l+1) \rangle$  при  $n = 3l$ , то есть при  $m = 2\mu$  – четном. Все  $\Gamma$ -орбиты должны иметь попарно различные спектры синдромов, одинаковые с орбитами по мощности благодаря условию  $d = 7$ . В силу отмеченных свойств нормы всех  $\Gamma$ -орбит ошибок весом 1–3 также должны быть попарно-различными.

Таким образом, в примитивном БЧХ-коде  $C_7$  имеется  $\lambda_\Gamma = C_n^3/n = (n-1)(n-2)/6$  полных  $\Gamma$ -орбит тройных ошибок для  $n = 3l+1$  и  $n = 3l+2$ ; в случае  $n = 3l$  имеется  $[C_n^3/n]$  полных  $\Gamma$ -орбит плюс одна  $\Gamma$ -орбита  $J = \langle (1, l+1, 2l+1) \rangle$  мощностью  $l$ . Здесь  $[a/b]$  – целая часть рационального числа  $a/b$ .

**G-орбиты тройных ошибок и их полиномиальные инварианты.** Группа  $G$  некоммутативна, имеет порядок  $mn$ , получается присоединением к группе  $\Gamma$  циклотомической подстановки  $\varphi$ , переставляющей координаты векторов  $n$ -мерного ( $n$  нечетно) пространства по правилу  $\varphi(i) = \begin{cases} 2i-1, & 2i-1 \leq n, \\ 2i-1-n, & 2i-1 > n. \end{cases}$  При этом подстановка  $\varphi$  имеет порядок  $m$ ,  $\varphi\sigma = \sigma^2\varphi$ , всякую  $\Gamma$ -орбиту

$\langle \bar{e} \rangle$  подстановка  $\varphi$  преобразует в  $\Gamma$ -орбиту, поэтому для каждого вектора-ошибки  $\bar{e}$  БЧХ-кода  $C_7$  ее  $G$ -орбита имеет вид

$$\langle \bar{e} \rangle_G = \{ \langle \bar{e} \rangle_\Gamma, \varphi(\langle \bar{e} \rangle_\Gamma), \dots, \varphi^{\mu-1}(\langle \bar{e} \rangle_\Gamma) \}, \tag{6}$$

где  $\mu$  – наименьшее натуральное число с условием:  $\varphi^\mu(\langle \bar{e} \rangle_\Gamma) = \langle \bar{e} \rangle_\Gamma$ . При этом  $\mu$  делит  $m$  или же  $\mu = m$ . При условии  $\mu = m$   $G$ -орбита  $\langle \bar{e} \rangle_G$  называется полной при условии, что и  $\Gamma$ -орбита  $\langle \bar{e} \rangle_\Gamma$  – полная. Циклотомическая подстановка замечательна следующим свойством: если синдром  $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2, s_3)^T$ , то  $S(\varphi(\bar{e})) = (s_1^2, s_2^2, s_3^2)^T$ . Аналогично преобразуется и норма синдрома:  $\bar{N}(S(\varphi(\bar{e}))) = (N_1^2, N_2^2, N_3^2)$  (детали см. в [2, гл. 3, 4; 3, гл. 4, 5]). Повторное применение подстановки  $\varphi$  к вектору-ошибке приведет к повторному возведению в квадрат компонент ее синдрома и компонент нормы синдрома. Таким образом, вся  $G$ -орбита  $\langle \bar{e} \rangle_G$ , построенная по формуле (6) как цикл, «круг» переходящих друг в друга  $\Gamma$ -орбит, имеет синхронный и адекватный образ в спектре норм этих  $\Gamma$ -орбит в виде трех 2-примарных последовательностей компонент этих норм:

$$\{ (N_1, N_2, N_3); (N_1^2, N_2^2, N_3^2), \dots, (N_1^{2^{\mu-1}}, N_2^{2^{\mu-1}}, N_3^{2^{\mu-1}}) \}, \text{ где } N_i^{2^\mu} = N_i. \tag{7}$$

Отображение  $f: x \rightarrow x^2$  в любом поле Галуа  $GF(2^m)$  характеристики 2 есть автоморфизм Фробениуса этого поля. Поэтому для каждого  $i = 1, 2, 3$  взятое из (7) множество

$$\{ N_i, N_i^2, \dots, N_i^{2^{\mu-1}} \} \tag{8}$$

при наименьшем натуральном  $\mu$  с условием  $N_i^{2^\mu} = N_i$  является полной системой элементов, сопряженных с  $N_i$ . Тогда три полинома

$$p_\mu(N_i, x) = p(x) = (x - N_i)(x - N_i^2) \dots (x - N_i^{2^{\mu-1}}) \tag{9}$$

имеют, согласно теореме Виета, коэффициенты, принадлежащие  $Z/2Z$ ; они являются неприводимыми над  $Z/2Z$  полиномами и каждый из них – единственный полином степени  $\mu$ , содержащий все корни множества (8) [7, гл. 4; 8]. По традиции, начатой в [5, 6], введем следующее

*Определение 1.* Тройка  $P(\langle \bar{e} \rangle_G)$  полиномов (9) называется векторным полиномиальным инвариантом  $G$ -орбиты (6) в коде  $C_7$ .

Перечисленные свойства названной тройки полиномов служат полным оправданием и обоснованием такого определения. Множество этих троек совпадает с количеством  $G$ -орбит и примерно в  $m$  раз меньше числа  $\lambda_\Gamma = C_n^3/n = (n-1)(n-2)/6$ . Если все три компоненты нормы  $\bar{N}$  являются ненулевыми элементами поля  $GF(2^m)$ , что чаще всего и бывает, то третья компонента  $N_3$  однозначно алгебраически выражается через первые две компоненты нормы  $\bar{N}$ , как уже отмечено. Следовательно, в данном случае в тройке  $P(\langle \bar{e} \rangle_G)$  третий полином можно не учитывать. Если же у синдрома  $S(\bar{e})$  компонента  $s_1 = 0$ , то в тройке  $P(\langle \bar{e} \rangle_G)$  третий полином становится единственным информативным полиномом. Отметим также, что привычная нам запись полинома  $p(x) = c_\mu x^\mu + c_{\mu-1} x^{\mu-1} + \dots + c_0$  в компьютере выражается набором  $(c_\mu, c_{\mu-1}, \dots, c_0)$  из  $\mu+1$  коэффициентов этого полинома, в данном случае из элементов 0, 1. Очевидно,  $c_\mu = 1$  в силу неприводимости полинома  $c_0 = 1$ , и количество единиц в наборе должно быть нечетным.

Каждый элемент поля  $GF(2^m)$  является алгебраическим над  $Z/2Z$ . Следовательно, еще на фазе формирования поля можно составить списки неприводимых полиномов для каждого из элементов этого поля.

*Пример 1.* В БЧХ-коде  $C_7$  длиной 31 имеется  $\lambda_\Gamma = C_{31}^3/31 = 30 \cdot 29/6 = 145$   $\Gamma$ -орбит тройных ошибок, что составляет  $145/5 = 29$  полных  $G$ -орбит ошибок. В табл. 1 приведен список образующих  $\bar{e}_i$  всех 29 названных  $G$ -орбит, синдромов образующих  $S(\bar{e}_i)$  в БЧХ-коде  $C_7$  с проверочной матрицей (1) для  $\alpha$  – корня полинома  $x^5 + x^2 + 1$ , норм синдромов  $\bar{N}_i = \bar{N}(S(\bar{e}_i))$ , а также полиномиальных инвариантов  $P(\langle \bar{e} \rangle_G)$ .

Т а б л и ц а 1. Список  $G$ -орбит тройных ошибок в БЧХ-коде длиной 31 с проверочной матрицей

$H = [\alpha^i, \alpha^{3i}, \alpha^{5i}]^T$ , где  $\alpha$  – корень полинома  $x^5 + x^2 + 1$ , их образующих  $\bar{e}_i$ , синдромов  $S(\bar{e}_i)$  и норм  $\bar{N}_i = \bar{N}(S(\bar{e}_i))$

T a b l e 1. A list of  $G$ -orbits of triple errors in the BCH code of length 31 with a check matrix

$H = [\alpha^i, \alpha^{3i}, \alpha^{5i}]^T$ , where  $\alpha$  is the root of the  $x^5 + x^2 + 1$  polynomial, its generators  $\bar{e}_i$ , the syndromes  $S(\bar{e}_i)$  and the norms  $\bar{N}_i = \bar{N}(S(\bar{e}_i))$

№ п/п	Образующая $\bar{e}_i$ Г-орбиты	Синдром $S(\bar{e}_i)$	Норма $\bar{N}$ Г-орбиты	$p_\mu(N_1, x)$	$p_\mu(N_2, x)$	$p_\mu(N_3, x)$
1	(1, 2, 3)	$(\alpha^{11}, \alpha^{18}, \alpha^{22})$	$(\alpha^{16}, \alpha^{29}, \alpha^7)$	$x^5 + x^2 + 1$	$x^5 + x^3 + 1$	$x^5 + x^3 + x^2 + x + 1$
2	(1, 2, 12)	$(\alpha^2, \alpha^8, \alpha^9)$	$(\alpha^2, \alpha^{30}, \alpha^{18})$	$x^5 + x^2 + 1$	$x^5 + x^3 + 1$	$x^5 + x^4 + x^2 + x + 1$
3	(1, 2, 15)	$(\alpha^{24}, \alpha^{12}, \alpha^{29})$	$(\alpha^2, \alpha^2, )$	$x^5 + x^2 + 1$	$x^5 + x^2 + 1$	
4	(1, 2, 6)	$(\alpha^{19}, \alpha^{28}, \alpha^{14})$	$(\alpha^2, \alpha^{12}, )$	$x^5 + x^2 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$	
5	(1, 6, 11)	$(\alpha^{22}, \alpha^{20}, \alpha^{24})$	$(\alpha^{16}, \alpha^7, )$	$x^5 + x^2 + 1$	$x^5 + x^3 + x^2 + x + 1$	
6	(1, 2, 4)	$(\alpha^{27}, \alpha^{17}, \alpha^{16})$	$(\alpha^{29}, \alpha^5, )$	$x^5 + x^3 + 1$	$x^5 + x^3 + x^2 + x + 1$	
7	(1, 2, 13)	$(\alpha^8, \alpha^{20}, \alpha^8)$	$(\alpha^{27}, \alpha^{30}, \alpha^{17})$	$x^5 + x^3 + 1$	$x^5 + x^3 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$
8	(1, 4, 10)	$(\alpha^{17}, \alpha^4, \alpha^{18})$	$(\alpha^{15}, \alpha^{26}, )$	$x^5 + x^3 + 1$	$x^5 + x^4 + x^3 + x + 1$	
9	(1, 7, 10)	$(\alpha^{10}, \alpha^{29}, \alpha^{12})$	$(\alpha^{30}, \alpha^{24}, )$	$x^5 + x^3 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$	
10	(1, 4, 7)	$(\alpha^{18}, \alpha^{21}, \alpha^{20})$	$(\alpha^{29}, \alpha^{23}, \alpha^{17})$	$x^5 + x^3 + 1$	$x^5 + x^3 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$
11	(1, 2, 5)	$(\alpha^{17}, \alpha^{11}, \alpha^3)$	$(\alpha^{22}, \alpha^{11}, )$	$x^5 + x^4 + x^3 + x + 1$	$x^5 + x^4 + x^3 + x + 1$	
12	(1, 8, 11)	$(\alpha^2, \alpha^{27}, \alpha^{26})$	$(\alpha^{21}, \alpha^{16}, \alpha^5)$	$x^5 + x^4 + x^3 + x + 1$	$x^5 + x^2 + 1$	$x^5 + x^4 + x^2 + x + 1$
13	(1, 5, 8)	$(\alpha^5, \alpha^{26}, \alpha^{14})$	$(\alpha^{11}, \alpha^{20}, )$	$x^5 + x^4 + x^3 + x + 1$	$x^5 + x^4 + x^2 + x + 1$	
14	(1, 7, 12)	$(\alpha^{20}, \alpha^{19}, \alpha^8)$	$(\alpha^{21}, \alpha, \alpha^{22})$	$x^5 + x^4 + x^3 + x + 1$	$x^5 + x^2 + 1$	$x^5 + x^4 + x^3 + x + 1$
15	(1, 2, 7)	$(\alpha^{29}, \alpha^6, \alpha^{28})$	$(\alpha^{12}, \alpha^7, )$	$x^5 + x^4 + x^3 + x^2 + 1$	$x^5 + x^3 + x^2 + x + 1$	
16	(1, 4, 14)	$(\alpha^{22}, \alpha^{28}, \alpha^{28})$	$(\alpha^{24}, \alpha^{11}, )$	$x^5 + x^4 + x^3 + x^2 + 1$	$x^5 + x^4 + x^3 + x + 1$	
17	(1, 3, 14)	$(\alpha^{25}, \alpha^{19}, \alpha^{21})$	$(\alpha^6, \alpha^{20}, )$	$x^5 + x^4 + x^3 + x^2 + 1$	$x^5 + x^4 + x^2 + x + 1$	
18	(1, 3, 4)	$(\alpha^8, \alpha^{10}, \alpha^8)$	$(\alpha^{17}, \alpha^{30}, )$	$x^5 + x^4 + x^3 + x^2 + 1$	$x^5 + x^3 + 1$	
19	(1, 2, 10)	$(\alpha^9, \alpha, \alpha^{21})$	$(\alpha^5, \alpha^7, \alpha^{27})$	$x^5 + x^4 + x^2 + x + 1$	$x^5 + x^3 + x^2 + x + 1$	$x^5 + x^3 + 1$
20	(1, 3, 12)	$(\alpha, \alpha^{23}, \alpha^{12})$	$(\alpha^{20}, \alpha^7, \alpha^{14})$	$x^5 + x^4 + x^2 + x + 1$	$x^5 + x^3 + x^2 + x + 1$	$x^5 + x^3 + x^2 + x + 1$
21	(1, 4, 5)	$(\alpha^{25}, \alpha^{22}, \alpha^{30})$	$(\alpha^9, \alpha^{29}, )$	$x^5 + x^4 + x^2 + x + 1$	$x^5 + x^3 + 1$	
22	(1, 10, 18)	$(\alpha^3, \alpha^{19}, \alpha^{17})$	$(\alpha^{10}, \alpha^2, )$	$x^5 + x^4 + x^2 + x + 1$	$x^5 + x^2 + 1$	
23	(1, 3, 8)	$(\alpha^{10}, \alpha^{17}, 0)$	$(\alpha^{18}, 0, )$	$x^5 + x^4 + x^2 + x + 1$	$x$	
24	(1, 3, 10)	$(\alpha^{15}, 0, \alpha^8)$	$(0, \alpha^{26}, )$	$x$	$x^5 + x^4 + x^3 + x + 1$	
25	(1, 2, 11)	$(\alpha^{30}, \alpha^{16}, \alpha)$	$(\alpha^{19}, \alpha^6, )$	$x^5 + x^3 + x^2 + x + 1$	$x^5 + x^4 + x^3 + x^2 + 1$	
26	(1, 4, 11)	$(\alpha^{21}, \alpha^{29}, \alpha^{26})$	$(\alpha^{28}, \alpha^{14}, )$	$x^5 + x^3 + x^2 + x + 1$	$x^5 + x^3 + x^2 + x + 1$	
27	(1, 2, 8)	$(\alpha^{26}, \alpha^{10}, \alpha^7)$	$(\alpha^{25}, \alpha, )$	$x^5 + x^3 + x^2 + x + 1$	$x^5 + x^2 + 1$	
28	(1, 3, 6)	$(0, \alpha^7, \alpha^{29})$	$(, , \alpha^{23})$			$x^5 + x^4 + x^3 + x + 1$
29	(1, 12, 20)	$(0, \alpha^{30}, \alpha^{16})$	$(, , \alpha^{16})$			$x^5 + x^2 + 1$

**Свойства полиномиальных инвариантов.** Изучение данных табл. 1 приводит к ряду интересных заключений. По значениям первого полинома  $p_\mu(N_1, x)$  множество всех  $G$ -орбит тройных ошибок разбилось на семь примерно равномоощных подмножеств. В большинстве случаев значения второго полинома  $p_\mu(N_2, x)$  определяют в подмножестве конкретную  $G$ -орбиту. Исключение составляют четыре пары  $G$ -орбит, в трех парах из них  $G$ -орбиты индивидуализируются по значениям третьего полинома  $p_\mu(N_3, x)$ . Вторая же пара  $G$ -орбит – 7-я и 10-я – имеет полностью одинаковые полиномиальные инварианты:  $P(\langle \bar{e}_7 \rangle_G) = P(\langle \bar{e}_{10} \rangle_G)$ . Приведенное наблюдение служит оправданием того, чтобы ввести следующее

*Определение 2.*  $G$ -орбиты называются орбитами-изомерами (полными изомерами), если у них одинаковы основные полиномиальные инварианты  $p_\mu(N_1, x)$  и  $p_\mu(N_2, x)$  или же  $p_\mu(N_3, x)$  при отсутствии первых двух (совпадают тройки полиномов  $P(\langle \bar{e} \rangle_G)$ ).

К примеру, анализируя табл. 4.3 из [2]  $G$ -орбит тройных ошибок в БЧХ-коде длиной 15, можно убедиться в наличии там двух пар полных орбит-изомеров. Существование  $G$ -орбит-изомеров нельзя считать чем-то исключительным. Оно определяется существованием  $G$ -орбит с нормами – различными парами корней заданных полиномов  $p_\mu(N_1, x)$  и  $p_\mu(N_2, x)$ . Поэтому максимальное количество  $G$ -орбит-изомеров с фиксированными полиномами  $p_\mu(N_1, x)$  и  $p_\mu(N_2, x)$  степеней  $\mu_1$  и  $\mu_2$  соответственно равно числу  $\mu_1 \cdot \mu_2$ . В реальной практике такое количество  $G$ -орбит-изомеров вряд ли достижимо.

Таким образом, в отличие от кодов  $C_5$ , где полиномиальные инварианты состоят из единственного полинома  $p_\mu(N_1, x)$  и однозначно характеризуют свою  $G$ -орбиту, векторные полиномиальные инварианты  $P(\langle \bar{e} \rangle_G)$  потеряли свойство однозначной характеристики и допускают наличие  $G$ -орбит-изомеров. Но главное назначение полиномиальных инвариантов – разделять  $G$ -орбиты на примерно равные подмножества – выполняется.

**Коррекция тройных ошибок в БЧХ-кодах  $C_7$  с помощью полиномиальных инвариантов.**

Для организации функционирования декодера необходимо провести подготовительную работу. Следует разбить образующие всех  $G$ -орбит корректируемой совокупности на группы с одинаковыми значениями полиномиального инварианта  $p_\mu(N_1, x)$ . Внутри каждой группы проводится более детальное деление по значениям инварианта  $p_\mu(N_2, x)$ . При наличии в группах ряда  $G$ -орбит с одинаковыми парами  $(p_\mu(N_1, x), p_\mu(N_2, x))$  проводится их дальнейшая сортировка по значениям третьего инварианта  $p_\mu(N_3, x)$ . Конечно, списки образующих должны быть дополнены синдромами образующих, нормами синдромов образующих и полиномиальными инвариантами, которым принадлежат компоненты норм синдромов. Табл. 1 иллюстрирует пример подобного списка.

В процессе работы декодера необходимо использовать полный список образующих  $G$ -орбит ошибок, входящих в ту или иную  $G$ -орбиту или группу  $G$ -орбит-изомеров, вместе с синдромами и нормами синдромов. Эти дополнительные списки (серия аналогов, табл. 2) либо заранее составляются и хранятся в памяти, либо составляются непосредственно по мере необходимости.

При получении очередного блока-сообщения  $\bar{x}$  работа декодера начинается с традиционного вычисления синдрома ошибок  $S(\bar{x}) = S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2, s_3)$ . При  $S(\bar{e}) \neq (0, 0, 0)$  вычисляется норма синдрома  $\bar{N}_{\text{выч}} = \bar{N}(S(\bar{e})) = (N_1, N_2, N_3)$ , для вычисленных компонент  $N_1, N_2, N_3$  находится тройка полиномов  $P(\langle \bar{e} \rangle_G)$ , содержащих каждую из компонент в качестве своих корней. Найденная тройка сравнивается с данными уже названного списка. Тем самым определяется  $G$ -орбита или группа  $G$ -орбит-изомеров, имеющая этот же полиномиальный инвариант.

Далее переходим к списку 2 образующих  $G$ -орбит ошибок, входящих в найденную  $G$ -орбиту или группу  $G$ -орбит-изомеров. В этом списке находим единственную  $G$ -орбиту  $\langle \bar{e}_i \rangle_G$  с нормой  $\bar{N}_{\text{выч}} = (N_1, N_2, N_3)$ . Сравнивая вычисленный синдром  $S(\bar{e}) = (s_1, s_2, s_3)$  с синдромом  $S(\bar{e}_i)$ , находим величину  $\nu$  циклического сдвига, такую, что  $\sigma^\nu(\bar{e}_i) = \bar{e}$ . Тогда вектор  $\bar{c} = \bar{x} + \bar{e}$  будет правильным переданным сообщением.

*Пример 2.* Пусть ИКС на основе БЧХ-кода  $C_7$  длиной 31 с данными из примера 1 приняла сообщение  $\bar{x}$  с синдромом ошибок  $S(\bar{x}) = S(\bar{e}) = (\alpha, \alpha^2, \alpha^{26})$ . Вычисляем норму полученного синдрома  $\bar{N}_{\text{выч}} = (\alpha^{23}, \alpha^{30}, \alpha^6)$ :

- норма  $N_1 = \alpha^{23}$  является корнем неприводимого над  $Z/2Z$  полинома  $p_5(N_1, x) = x^5 + x^3 + 1$ ;
- норма  $N_2 = \alpha^{30}$  является корнем того же неприводимого над  $Z/2Z$  полинома  $p_5(N_2, x) = x^5 + x^3 + 1$ ;
- норма  $N_3 = \alpha^6$  является корнем неприводимого над  $Z/2Z$  полинома  $p_5(N_3, x) = x^5 + x^4 + x^3 + x^2 + 1$ .

Сравнивая полученную тройку полиномов с данными табл. 1, видим, что данная тройка полиномов совпадает с тройкой полиномиальных инвариантов пары  $G$ -орбит-изомеров  $\langle (1, 2, 13) \rangle_G$  и  $\langle (1, 4, 7) \rangle_G$ . Составим табл. 2 образующих  $G$ -орбит данных  $G$ -орбит, синдромов и норм синдромов этих образующих.

Сравниваем с данными табл. 2 вычисленный норменный вектор  $\bar{N}_{\text{выч}} = (\alpha^{23}, \alpha^{30}, \alpha^6)$ . Он совпадает с данными восьмой  $G$ -орбиты. Вычисляем частное от деления первой компоненты

Таблица 2. **Образующие  $\Gamma$ -орбит из  $G$ -орбит  $\langle(1, 2, 13)\rangle_G$  и  $\langle(1, 4, 7)\rangle_G$ , синдромы и нормы синдромов образующих в БЧХ-коде из примера 1**  
 Table 2. **Generators of  $\Gamma$ -orbits from  $G$ -orbits  $\langle(1, 2, 13)\rangle_G$  and  $\langle(1, 4, 7)\rangle_G$ , the syndromes and the norms of syndromes of generators in BCH code from example 1**

№ п/п	Образующая $\bar{e}_i$ $\Gamma$ -орбиты	Синдром $S(\bar{e}_i)$	Норма $\bar{N}$ $\Gamma$ -орбиты
1	(1, 2, 13)	$(\alpha^8, \alpha^{20}, \alpha^8)$	$(\alpha^{27}, \alpha^{30}, \alpha^{17})$
2	(1, 3, 25)	$(\alpha^{16}, \alpha^9, \alpha^{16})$	$(\alpha^{23}, \alpha^{29}, \alpha^3)$
3	(1, 5, 18)	$(\alpha, \alpha^{18}, \alpha)$	$(\alpha^{15}, \alpha^{27}, \alpha^6)$
4	(1, 4, 9)	$(\alpha^2, \alpha^5, \alpha^2)$	$(\alpha^{30}, \alpha^{23}, \alpha^{23})$
5	(1, 7, 17)	$(\alpha^4, \alpha^{10}, \alpha^4)$	$(\alpha^{29}, \alpha^{15}, \alpha^{24})$
6	(1, 4, 7)	$(\alpha^{18}, \alpha^{21}, \alpha^{20})$	$(\alpha^{29}, \alpha^{23}, \alpha^{17})$
7	(1, 7, 13)	$(\alpha^5, \alpha^{11}, \alpha^9)$	$(\alpha^{27}, \alpha^{15}, \alpha^3)$
8	(1, 13, 25)	$(\alpha^{10}, \alpha^{22}, \alpha^{18})$	$(\alpha^{23}, \alpha^{30}, \alpha^6)$
9	(1, 17, 25)	$(\alpha^{20}, \alpha^{13}, \alpha^5)$	$(\alpha^{15}, \alpha^{29}, \alpha^{12})$
10	(1, 4, 18)	$(\alpha^9, \alpha^{26}, \alpha^{10})$	$(\alpha^{30}, \alpha^{27}, \alpha^{24})$

вычисленного синдрома на первую компоненту синдрома образующей восьмой  $\Gamma$ -орбиты:  $\alpha^{24}/\alpha^{10} = \alpha^{14}$ . Следовательно, искомый вектор-ошибок в сообщении  $\bar{x}$  получается циклическим сдвигом на 14 позиций координат вектора  $\bar{e}_7$ :  $\bar{e} = \sigma^{14}(\bar{e}_7) = \sigma^{14}((1, 13, 25)) = (8, 15, 27)$ .

Приведенный алгоритм сохранил вычисления, присущие норменным методам, а именно вычисление нормы синдрома, а также величины циклического сдвига образующей  $\Gamma$ -орбиты до получения искомой вектор-ошибки. Главное отличие данного алгоритма от норменного – в реструктуризации и сокращении однообразного поиска нужной нормы в длинном списке норм всех  $\Gamma$ -орбит корректируемой совокупности векторов-ошибок. Проводились переборный поиск лишь в небольшом списке норм  $\Gamma$ -орбит отдельного небольшого набора  $G$ -орбит-изомеров, а также усеченный последовательный покоординатный поиск во множестве векторных полиномиальных инвариантов.

**Заключение.** В работе развита теория полиномиальных инвариантов на БЧХ-коды, конструктивное расстояние которых равно семи. Как и нормы синдромов, полиномиальные инварианты в этих кодах приобретают векторный характер. Работа с полиномиальными инвариантами становится более громоздкой. Более того, они теряют свойство однозначной характеристики  $G$ -орбит. Но сохраняется их основное предназначение – закономерное разделение класса  $G$ -орбит декодируемой совокупности на примерно равномошные непересекающиеся классы.

Метод векторных полиномиальных инвариантов – весьма эффективное средство коррекции больших массивов ошибок. Он повторяет вычисления в полях Галуа, присущие норменным методам, не способствуя их увеличению. Этот метод сокращает переборные процедуры, разделяет их на два этапа: 1) последовательный покоординатный поиск вычисленного векторного полиномиального инварианта в упорядоченном списке таких инвариантов корректируемой совокупности  $G$ -орбит; 2) поиск вычисленной нормы в списке норм найденной  $G$ -орбиты или  $G$ -орбит-изомеров. Данный метод имеет все признаки на успешные приложения.

### Список использованных источников

1. Конопелько, В.К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В.К. Конопелько, В.А. Липницкий. – Изд. 2-е. – М.: Едиториал УРСС, 2004. – 176 с.
2. Липницкий, В.А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В.К. Конопелько, В.А. Липницкий. – Минск: Изд. центр БГУ, 2007. – 240 с.
3. Липницкий, В.А. Теория норм синдромов / В.А. Липницкий. – Минск: БГУИР, 2011. – 96 с.
4. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М.: Связь, 1979. – 744 с.
5. Липницкий, В.А. Полиномиальные инварианты  $G$ -орбит ошибок БЧХ-кодов и их применение / В.А. Липницкий, Е.В. Середа // Докл. БГУИР. – 2017. – № 5(107) – С. 62–69.
6. Липницкий, В.А. Полиномиальные инварианты автоморфизмов семейства БЧХ-кодов и их приложения / В.А. Липницкий, Е.В. Середа // Комплексная защита информации: материалы XXII Белорус.-Рос. науч.-практ. конф., Полоцк, 16–19 мая 2017 г. – Новополоцк, 2017. – С. 117–120.
7. Муттер, В.М. Основы помехоустойчивой телепередачи информации / В.М. Муттер. – Л.: Энергоатомиздат, 1990. – 286 с.

### References

1. Konopel'ko V. K., Lipnickij V. A. *The Norm of Syndrome Theory and Permutation Decoding of Noise-Immune Codes*. Second edition. Moscow, Editorial URSS Publ., 2004. 176 p. (in Russian).

2. Lipnickij V. A., Konopel'ko V. K. *Norm Decoding of Noise-Immune Codes and Algebraic Equations*. Minsk, Publishing Center of the Belarusian State University, 2007. 240 p. (in Russian).
3. Lipnickij V. A. *The Norm of Syndrome Theory*. Minsk, Belarusian State University of Informatics and Radioelectronics, 2011. 96 p. (in Russian).
4. Mak-Vil'jams F. Dzh., Slojen N. Dzh. A. *The Theory of Error-Correcting Codes*. Moscow, Svjaz' Publ., 1979. 744 p. (in Russian).
5. Lipnickij V. A., Sereda E. V. Polynomial invariants of errors'  $G$ -orbit of BCH codes and its application. *Doklady BGUIR = Doklady BSUIR*, 2017, no. 5 (107), pp. 62–69 (in Russian).
6. Lipnickij V. A., Sereda E. V. Polynomial invariant of automorphisms of BCH code family and its application. *Materialy XXII Belorussko-Rossijskoj nauchno-prakticheskoj konferencii "Kompleksnaja zashhita informacii"* [Proc. of the XXII Belarusian-Russian Scientific and Practical Conference "Complex information security"]. Novopolock, 2017, pp. 117–120 (in Russian).
7. Mutter V. M. *Fundamentals of Noise-Immune Telecasting of Information*. Leningrad, Energoatomizdat Publ., 1990. 286 p. (in Russian).

### Информация об авторах

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

*Серёда Елена Владимировна* – магистр, аспирант кафедры защиты информации, Белорусский государственный университет информатики и радиоэлектроники (ул. П. Бровки, 10, 220013, Минск, Республика Беларусь). E-mail: elen.vt@gmail.com

### Information about the authors

*Valery A. Lipnitski* – D. Sc. (Engineering), Professor, Head of the Department of Higher Mathematics, Military Academy of the Republic of Belarus (220, Nezavisimosti Ave., 220057, Minsk, Republic of Belarus). E-mail: valipnitski@yandex.ru

*Alena U. Serada* – Master of Engineering Science, Postgraduate Student at the Department of Information Security, Belarusian State University of Informatics and Radioelectronics (10, P. Brovka Str., 220013, Minsk, Republic of Belarus). E-mail: elen.vt@gmail.com