УДК 512 (075.8)

В. А. ЛИПНИЦКИЙ[1], Е. В. СЕРЕДА[2]

СВОЙСТВА G-ОРБИТ ДВОЙНЫХ ОШИБОК И ИХ ИНВАРИАНТОВ В БЧХ-КОДАХ

[1]Военная академия Республики Беларусь
[2]Белорусский государственный университет информатики и радиоэлектроники

Цель работы – дальнейшее расширение сферы применения автоморфизмов кодов в методах и алгоритмах коррекции ошибок этими кодами. Эффективность данного подхода продемонстрировала разработанная на рубеже XX и XXI веков белорусской школой помехоустойчивого кодирования теория норм синдромов (ТНС). В основе теории лежит группа Г циклических сдвигов координат векторов. Под ее действием векторы-ошибок разбиваются на непересекающиеся Г-орбиты с четко очерченным спектром синдромов. Это позволило ввести в семействе БЧХ-кодов нормы синдромов, инвариантные относительно действия группы Г. Нормы синдромов явились однозначными характеристиками Г-орбит ошибок любой корректируемой совокупности, а потому стали основой перестановочных норменных методов коррекции ошибок. Перебирая не ошибки, а Г-орбиты ошибок, методы эти действуют на порядок быстрее классических синдромным методов коррекции ошибок, избавлены от громоздкой процедуры решения алгебраических уравнений в полях Галуа, легко реализуемы на ПЛИС.

В работе развивается подобная теория для группы G автоморфизмов БЧХ-кодов, получаемой добавлением к группе Г циклотомической подстановки. Проводится детальное исследование структуры G-орбит ошибок как объединения своих Г-орбит векторов-ошибок; взаимно-однозначного отражения этого строения на структуре спектра норм составляющих Г-орбит. Нормы эти, будучи связанными между собой автоморфизмом Фробениуса в поле Галуа – поле задания БЧХ-кода, составляют полный набор корней единственного неприводимого полинома. Он и является полиномиальным инвариантом своей G-орбиты. Основное внимание в работе сосредоточено на описании свойств и специфики G-орбит двойных ошибок и их полиномиальных инвариантов.

Ключевые слова: *БЧХ-коды, теория норм синдромов, автоморфизмы БЧХ-кодов, норма синдрома, синдром, полиномиальные инварианты норм синдромов.*

Введение

Белорусская алгебраическая школа в лице академиков Чунихина С. А., Супруненко Д. А., Платонова В. П. и их учеников заняла в последней четверти XX века одно из лидирующих мест в математических исследованиях, проводившихся в Советском Союзе. Весом непосредственный вклад этой школы в развитие теории групп, формаций групп, классических и алгебраических групп, ассоциативных колец и алгебр, коммутативных полей и алгебр с делением, алгебраической геометрии. Наработанный потенциал послужил побудительным мотивом для развития различных приложений алгебры, в частности, в помехоустойчивом кодировании.

Систематическое исследование в Республике Беларусь автоморфизмов линейных циклических кодов в 1996–2003 годах привело к:

- детальному описанию Г-орбит векторов-ошибок в названных кодах относительно группы Г циклических сдвигов координат векторов;
- построению адекватной картины в спектрах синдромов Г-орбит ошибок в реверсивных и БЧХ-кодах;
- разработке норм синдромов как инвариантов Г-орбит ошибок, описанию достаточно стройной системы свойств норм синдромов.

Созданная таким образом на рубеже XX и XXI веков теория норм синдромов [1–3] дала норменный метод декодирования ошибок в БЧХ-кодах, а также в реверсивных кодах, действующий на порядок быстрее иных синдромных методов, легко реализуемый на ПЛИС, отлича-

ющийся усеченностью процедуры поиска корректируемой ошибки, конструктивными возможностями расширения спектра корректируемых ошибок [2].

В семействе БЧХ-кодов нечетной длины автоморфизм Фробениуса поля Галуа – поля определения кода – порождает автоморфизмы, называемые циклотомическими подстановками. Они вместе с группой Г образуют некоммутативную группу G автоморфизмов БЧХ-кодов [2–4]. G-орбиты ошибок состоят из специальным образом взаимосвязанных Г-орбит векторов-ошибок [2, 3]. Открытие полиномиальных инвариантов G-орбит ошибок [5] создает хорошие перспективы к декодированию больших спектров ошибок. Продолжая [5], в данной работе исследуются дальнейшие свойства G-орбит ошибок и их полиномиальных инвариантов.

Немного о БЧХ-кодах. В данной работе мы имеем дело с циклическими примитивными двоичными БЧХ-кодами C длиной $n = 2^m - 1$, задаваемыми проверочными матрицами вида

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

где α – корень примитивного неприводимого над $Z/2Z$ полинома степени m, $m \ge 3$, [2–4]. Их минимальное расстояние d равно 5 [4], что позволяет данным кодам корректировать одиночные и двойные ошибки.

Пусть инфокоммуникационная система (ИКС), основанная на БЧХ-коде С, приняла сообщение $\overline{x}$. Приемное устройство ИКС в обязательном порядке вычисляет синдром ошибок $S(\overline{x}) = H\,\overline{x}^T$. В силу формулы (1) этот синдром имеет следующую структуру:

$$S(\overline{x}) = (s_1, s_2)^T,$$

где s_1, s_2 – элементы поля Галуа $GF(2^m)$ из 2^m элементов. Условие $d = 5$ влечет попарное различие синдромов векторов-ошибок весом 1, 2. Несложно заметить, что у всех этих векторов первая компонента синдрома $s_1 \ne 0$.

Неравенство $S(\overline{x}) \ne \overline{0}$ свидетельствует о наличии ошибок в принятом сообщении: $\overline{x} = \overline{c} + \overline{e}$, где $\overline{c}$ – истинное передаваемое сообщение, $\overline{e}$ – вектор ошибок, который наложился на сообщение в процессе передачи $\overline{c}$ в канале с шумами. Поскольку $H\,\overline{c}^T = \overline{0}$, то $S(\overline{x}) = S(\overline{e})$ – зависит только от вектора-ошибки $\overline{e}$. Традиционно, координаты вектора $\overline{e}$ весом 2 находятся решением системы алгебраических уравнений:

$$\begin{cases} x + y = s_1; \\ x^3 + y^3 = s_2. \end{cases}$$

Данная система несложно преобразуется к квадратному уравнению. К сожалению, над полями Галуа характеристики 2 не существует эффективных алгоритмов решения алгебраических уравнений, а имеющиеся весьма вязки в реализации (см. [3], п. 9.2; [5], п. 2.9; [6], гл. 5).

Еще в 70-х годах XX века эксперты говорили об эффективности применения для коррекции ошибок автоморфизмов кодов. Правда, предполагалось весьма специфическое их применение – для сдвига имеющихся ошибочных разрядов в проверочное поле, где их просто можно отбросить (см. [4], п. 16.9, стр. 496–497). Внешне прозрачная идея остается нереализованной и по сей день. Тем не менее, автоморфизмы кодов нашли свое применение в помехоустойчивом кодировании, прямое и весьма успешное.

Г-орбиты ошибок, их спектры и нормы синдромов.

Группа Г состоит из степеней циклической подстановки σ, действующей на каждый вектор $\overline{x} = (x_1, x_2, ..., x_n)$ по правилу:

$$\sigma(\overline{x}) = (x_n, x_1, x_2, ..., x_{n-1}). \qquad (2)$$

Таким образом, группа Г является коммутативной циклической группой порядка n. По определению, она принадлежит группе автоморфизмов любого циклического кода длиной n, в частности, БЧХ-кодов с проверочной матрицей (1).

Для всякой вектор-ошибки $\overline{e} = (e_1, e_2, ..., e_n)$ ее Г-орбита

$$<\overline{e}>_\Gamma = <\overline{e}> = \left\{\overline{e}, \sigma(\overline{e}), ..., \sigma^{\nu-1}(\overline{e})\right\}, \qquad (3)$$

где ν – наименьшее натуральное число с условием: $\sigma^\nu(\overline{e}) = \overline{e}$. При этом ν делит n или же $\nu = n$. Во втором случае Г-орбита $<\overline{e}>$ имеет максимально возможную мощность и потому называется полной. Очевидно, в любом циклическом коде длиной $n > 1$ одиночные ошибки в количестве $C_n^1 = n$ составляют одну полную Г-орбиту. Двойные ошибки в количестве $C_n^2 = n(n-1)/2$ в циклических кодах с нечетной длиной $n = 2\mu + 1$ распределяются по $(n-1)/2 = \mu$ полным Г-орбитам $<\overline{e}_{1,2}>, <\overline{e}_{1,3}>, ..., <\overline{e}_{1,\mu+1}>$. Здесь $\overline{e}_{1,i}$ – вектор-ошибка весом 2 с единицами на первой и i-й позициях, $2 \le i \le \mu + 1$, и с нулевыми остальными координатами (детали см. в [1–3]).

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

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

Неравенство $s_1 \neq 0$ у синдромов ошибок весом 1, 2 влечет тот факт, что спектр синдромов каждой Г-орбиты названных векторов-ошибок имеет ту же мощность, что и сама Г-орбита, а циклическая структура этого спектра, определяемая формулой (4), адекватно соответствует циклической, «кольцевой» структуре самой Г-орбиты (формула (3)).

Равенство (4) послужило основой для определения нормы синдрома в данном коде формулой:

$$N(S(\bar{e})) = s_2 / s_1^3. \quad (5)$$

Главное достоинство этой формулы – ее постоянство на всех векторах каждой отдельно взятой Г-орбиты векторов-ошибок. Таким образом, вычисленная норма становится инвариантом, называемым нормой самой Г-орбиты.

Стройная система свойств норм синдромов (см. [3], п. 5.2), в частности, теорема 5.2 о попарном различии норм Г-орбит ошибок весом 1, 2, теорема о том, что в примитивном БЧХ-коде из равенства норм двух Г-орбит ошибок следует совпадение их спектров синдромов, послужили основой перестановочных норменных методов коррекции ошибок в рассматриваемых и более широких классах БЧХ-кодах. Основная их особенность в том, что вместо поиска ошибки с вычисленным синдромом во множестве всех исправляемых ошибок проводится поиск вычисленной нормы в списке норм декодируемых Г-орбит ошибок. Таким образом, поисковые процедуры в норменном декодере сокращаются в *n* раз быстрее по сравнению с классическими синдромными методами.

Увеличение *m* на единицу практически удваивает *n* и остальные параметры кода, включая и количество декодируемых Г-орбит ошибок. Через несколько подобных итераций это приводит к невероятному росту всех данных в прямой аналогии со знаменитой притчей о вознаграждении изобретателю шахмат. Выход – в разумном ограничении длин применяемых кодов и в применении для процедур декодирования более крупных орбит – G-орбит ошибок.

G-орбиты ошибок и их полиномиальные инварианты. Группа *G* некоммутативна, имеет порядок *mn*, получается присоединением к группе Г циклотомической подстановки φ, переставляющей координаты векторов *n*-мерного (*n* нечетно) пространства по правилу:

$$\varphi(i) = \begin{cases} 2i-1, 2i-1 \le n, \\ 2i-1-n, 2i-1 > n. \end{cases}$$

При этом подстановка φ имеет порядок *m*, $\varphi\sigma = \sigma^2\varphi$, всякую Г-орбиту $<\bar{e}>$ подстановка φ преобразует в новую Г-орбиту, поэтому для каждого вектора-ошибки $\bar{e}$ БЧХ-кода C ее G-орбита имеет вид:

$$<\bar{e}>_G = \left\{<\bar{e}>_\Gamma, \varphi(<\bar{e}>_\Gamma), ..., \varphi^{\mu-1}(<\bar{e}>_\Gamma)\right\}, \quad (6)$$

где μ – наименьшее натуральное число с условием: $\varphi^\mu(<\bar{e}>_\Gamma) = <\bar{e}>_\Gamma$. При этом μ делит *m* или же $\mu = m$. Во втором случае *G*-орбита $<\bar{e}>_G$ называется полной при условии, что и Г-орбита $<\bar{e}>_\Gamma$ – полная. Циклотомическая подстановка замечательна следующим свойством: если синдром $S(\bar{e}) = H\bar{e}^T = (s_1, s_2)^T$, а норма синдрома $N(S(\bar{e})) = s_2/s_1^3 = N$, то $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$, $N(S(\varphi(\bar{e}))) = N^2$ (детали см. в [2], гл. 3, 4 или же в [3], гл. 4, 5). Повторное применение подстановки φ к вектору-ошибке приведет к повторному возведению в квадрат ее синдрома и нормы синдрома. Таким образом, вся *G*-орбита $<\bar{e}>_G$, построенная по формуле (6) как цикл, «круг» переходящих друг в друга Г-орбит, имеет синхронный и адекватный образ в спектре норм этих Г-орбит в виде 2-примарной последовательности норм:

$$\{N, N^2, ..., N^{2^{\mu-1}}\}, \text{ где } N^{2^\mu} = N. \quad (7)$$

Теорема 1. *Между циклом Г-орбит, составляющих G-орбиту* $<\bar{e}>_G$ *по формуле (6), и циклом их норм, составленном по формуле (7), существует взаимно однозначное соответствие. G-орбита* $<\bar{e}>_G$ *является неполной и состоит из* $\mu < m$ *Г-орбит тогда и только тогда, когда* $GF(2^\mu)$ *– наименьшее подполе поля* $GF(2^m)$, μ *делит m, содержащее норму N.*

Доказательство. Первая часть утверждения обоснована выше. Собственно, циклотомическая подстановка так и определяется, чтобы ее действие на вектор ошибок сопровождался возведением ее синдрома в квадрат. Как известно, отображение $f: x \to x^2$ в любом поле Галуа $GF(2^m)$ характеристики 2 есть не что иное, как автоморфизм Фробениуса в этом поле – образу-

ющая группы Галуа поля $GF(2^m)$ над своим подполем $Z/2Z$. Поэтому множество $N, N^2, ..., N^{2^{\mu-1}}$ при наименьшем натуральном μ с условием $N^{2^\mu} = N$ является полной системой элементов, сопряженных с N. Тогда полином $p_\mu(N, x) = p(x) = (x - N)(x - N^2)...(x - N^{2^{\mu-1}})$ имеет коэффициенты, определяемые теоремой Виета и, следовательно, инвариантные относительно действия автоморфизма Фробениуса, а потому принадлежащие минимальному подполю $Z/2Z$. Минимальное подполе поля $GF(2^m)$, содержащее N, по теории расширений Галуа [7], должно быть расширением $Z/2Z$ степени μ; в противном случае элемент N должен был бы иметь менее μ сопряженных. Теорема 1 полностью доказана.

Методом от противного доказывается, что $p_\mu(N, x)$ является неприводимым над $Z/2Z$ полиномом. Следовательно, это единственный полином степени μ, содержащий все корни множества (7). Полином $p_\mu(N, x)$ называют неприводимым полиномом любого из своих корней, потому его иногда обозначают через $Irr(N^{2^i}, x)$ [7, гл. 4, 8]. В [5] этот полином авторы назвали полиномиальным инвариантом G-орбиты (6). Теорема 1 и отмеченные свойства полинома $p_\mu(N, x)$ служат полным оправданием и обоснованием такого названия.

Наиболее характерные G-орбиты ошибок и их параметры. 1. В БЧХ-коде C любой длины Г-орбита J ошибок весом 1 имеет норму $N = 1$. G-орбита одиночных ошибок совпадает с J. Поэтому полиномиальный инвариант этой G-орбиты совпадает с полиномом $x+1$.

2. Пусть у БЧХ-кода C величина $m = 2s$ – четная. Тогда $2^m - 1 = 2^{2s} - 1 = (2^s - 1)(2^s + 1)$ – делится на три: $n = 3\nu$. Вектор-ошибка весом $2\ \overline{e}_{1,\nu+1} = (1, \nu+1)$ с единицами на 1-й и ν+1-й позициях и с нулями на остальных позициях имеет компоненты синдрома: $s_1 = 1 + \alpha^\nu \neq 0$; $s_2 = 1 + (\alpha^\nu)^3 = 1 + 1 = 0$. Следовательно, $N = N(S(1, \nu + 1)) = 0$. Поскольку $\varphi((1, \nu+1)) = (1, 2\nu+1) = \sigma^{2\nu}(1, \nu+1) \in <(1, \nu+1)>$, то G-орбита $<(1, \nu+1)>_G = <(1, \nu+1)>_J$. Поэтому полиномиальный инвариант этой G-орбиты совпадает с x.

Пусть $m = 2s+1$ – нечетное. В этом случае отсутствуют Г-орбиты двойных ошибок с нулевой нормой. Действительно, согласно лемме 3.2 [2] в этом случае $n = 2^{2s+1} - 1$ не делится на 3 и поэтому возведение в куб является автоморфизмом мультипликативной группы $GF(2^{2s+1})^*$. (детали см. в п. 2.12 [7]). Отсюда следует, что столбцы подматрицы (α^{3i}) проверочной матрицы $H = (\alpha^i, \alpha^{3i})^T$ БЧХ-кода C над рассматриваемым полем попарно различны и в целом составляют в этой подматрице перестановку столбцов подматрицы (α^i). Это означает, что для всех двойных ошибок $\overline{e}$ вторая компонента их синдрома $S(\overline{e})$ в рассматриваемом БЧХ-коде $s_2 \neq 0$ и $N(S(\overline{e})) \neq 0$.

3. Пусть $m = p$ – простое, $p > 2$. Тогда поле $Z / 2Z = GF(2)$ является единственным подполем поля $GF(2^p)$. Здесь G-орбита ошибок весом 1 – единственная G-орбита ошибок весом 1, 2, совпадающая со своей Г-орбитой и с полиномиальным инвариантом $x+1$. Согласно предыдущему примеру здесь отсутствуют Г-орбиты двойных ошибок с нулевой нормой. Значит, здесь любая Г-орбита двойных ошибок J имеет норму N, отличную от нуля и от 1. Тогда норма N должна порождать поле $GF(2^p)$, а полином $Irr(N, x)$ должен иметь степень p. А это означает, что G-орбита $< J >_G$ должна быть полной. Согласно малой теореме Ферма $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$, то есть $2^{p-1} - 1 = p\eta$ для подходящего целого η. Следовательно, в БЧХ-коде C над полем $GF(2^p)$ все множество из $(n - 1)/2 = (2^p - 1 - 1)/2 = 2^{p-1} - 1 = p\eta$ полных Г-орбит двойных ошибок делится на η полных G-орбит ошибок.

4. Пусть у БЧХ-кода C вновь величина $m = 2s$ – четная. Тогда поле Галуа $GF(2^m)$ содержит подполе $GF(2^2)$; в силу примера 2 величина n делится на 3; для $\nu = n/3$ и примитивного элемента $\alpha \in GF(2^m)$ степени α^ν и $\alpha^{2\nu}$ являются кубическими корнями из 1 и потому принадлежат подполю $GF(2^2)$. Если у БЧХ-кода C найдется двойная ошибка $\overline{e} = (1, i)$ с нормой синдрома $N(S(\overline{e})) = \alpha^\nu$, то тогда G-орбита $<\overline{e}>_G = \{<\overline{e}>_\Gamma, <\phi(\overline{e})>_\Gamma\}$ – состоит из двух Г-орбит со спектром норм $\{\alpha^\nu, \alpha^{2\nu}\}$. Причем такая G-орбита – единственная! Ее полиномиальным инвариантом является единственный неприводимый над $Z/2Z$ полином $x^2 + x + 1$.

Нормы Г-орбит двойных ошибок в каждом коде занимают $(n-1)/2$ значений из $n + 1$ всех возможных. Поэтому априори можно утверждать, что примерно в половине БЧХ-кодов с четным $m = 2s$ имеется одна единственная Г-орбита двойных ошибок с нормой синдрома $N(S(\overline{e})) = \alpha^\nu$, а во второй половине БЧХ-кодов таких двойных ошибок не имеется.

Непосредственные расчеты подтверждают данное предположение. При $m = 4$ и $n = 15$ такой является Г-орбита $<\overline{e}>_\Gamma = <(1, 7)>_\Gamma$. В БЧХ-коде над полем $GF(2^4)$ с примитивным элементом α-корнем полинома $x^4 + x + 1$ норма данной Г-орбиты равна $\alpha^5 = \alpha^{n/3}$. При $m = 8$ и $n = 255$ таковой является Г-орбита $<\overline{e}>_\Gamma = <(1, 52)>_\Gamma$. В БЧХ-коде над полем $GF(2^8)$ с примитивным элементом α-корнем полинома $p(x) = x^8 + x^4 + x^3 + x + 1$ норма данной Г-орбиты равна $\alpha^{85} = \alpha^{n/3}$. При $m = 12$ и $n = 4095$ таковой является Г-орбита $<\overline{e}>_\Gamma = <(1, 820)>_\Gamma$. В БЧХ-коде над полем $GF(2^{12})$ с примитивным элементом α-корнем полинома $p(x) = x^{12} + x^7 + x^4 + x^3 + 1$ норма данной Г-орбиты равна $\alpha^{1365} = \alpha^{n/3}$. При $n = 6$ и $n = 10$ таких Г-орбит не имеется.

5. В БЧХ-кодах C над полями $GF(2^m)$ с $m = 3\mu$ – делящимся на 3 и содержащими подполе $GF(2^3)$, которое определяется одним из двух неприводимых полиномов третьей степени: $x^3 + x + 1$ и $x^3 + x^2 + 1$, могут существовать одна, две или ни одной G-орбиты ошибок весом 2, состоящие в точности из трех Г-орбит. Так, при $m = 3$ и $n = 7$ все двойные ошибки укладываются в одну полную G-орбиту из трех Г-орбит; при $m = 6$ и $n = 63$ имеются в точности две G-орбиты двойных ошибок, содержащие по три Г-орбиты ошибок: $<(1, 8)>_\Gamma$ и $<(1, 10)>_\Gamma$; при $m = 9$ и $n = 511$ существует одна G-орбита, содержащая три Г-орбиты: $<(1, 74)>_\Gamma$; при $m = 12$ и $n = 4095$ таких G-орбит не имеется.

Заключение

Установлено взаимно-однозначное соответствие между строением G-орбит как строго фиксированного цикла Г-орбит и структурой спектра норм этих составляющих Г-орбит. Это соответствие усиливается синхронностью действия циклотомической подстановки на Г-орбиты и автоморфизма Фробениуса на нормы этих Г-орбит. Первая часть утверждения обоснована выше. Большинство G-орбит двойных ошибок являются полными, то есть содержат максимально возможное количество полных Г-орбит ошибок. Неполные G-орбиты двойных ошибок возможны только над полями Галуа $GF(2^m)$ с составным показателем m. В G-орбите может содержаться $\mu < m$ Г-орбит, только при μ делящем m, количество таких G-орбит не превосходит числа неприводимых над минимальным подполем полиномов степени μ. Наличие небольшого числа неполных G-орбит ошибок не сильно осложняет работу перестановочных декодеров на основе полиномиальных инвариантов.

ЛИТЕРАТУРА

1. **Конопелько В. К., Липницкий В. А.** Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Монография. – Мн.: БГУИР, 2000. – 242 с. Изд. 2-е. – М.: Едиториал, УРСС 2004. – 176 с.

2. **Липницкий В. А., Конопелько В. К.** Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. – Мн.: Издательский центр БГУ, 2007. – 240 с.

3. **Липницкий В. А.** Теория норм синдромов. – Мн.: БГУИР, 2011. – 96 с.

4. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. – 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 // Доклады БГУИР. – 2017. – № 5(107) – С. 62 – 69.

6. **Муттер В. М.** Основы помехоустойчивой телепередачи информации – Л.: Энергоатомиздат, 1990. – 286 с.

7. **Липницкий, В. А.** Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. – Мн.: БГУИР, 2006. – 88 с.

8. **Лиддл Р., Ниддеррайтер Г.** Конечные поля. Т.1, 2. – М.: Мир, 1988. – 882 с.

REFERENCES

1. **Konopel'ko V. K., Lipnickij V. A.** Teorija norm sindromov i perestanovochnoe dekodirovanie pomehoustojchivyh kodov. Monografija. – Mn.: BGUIR, 2000. – 242 s. Izd. 2-e. – M.: Editorial, URSS 2004. – 176 s.

2. **Lipnickij V. A., Konopel'ko V. K.** Normennoe dekodirovanie pomehoustojchivyh kodov i algebraicheskie uravnenija. – Mn.: Izdatel'skij centr BGU, 2007. – 240 s.

3. **Lipnickij V. A.** Teorija norm sindromov. – Mn.: BGUIR, 2011. – 96 s.

4. **Mak-Vil'jams F. Dzh., Slojen N. Dzh. A.** Teorija kodov, ispravljajushhih oshibki. – M.: Svjaz', 1979. – 744 s.

5. **Lipnickij, V. A.** Polinomial invariants of errors' G-orbit of BCH codes and its application / V. A. Lipnickij, E. V. Sereda // Doklady BGUIR. – 2017. – № 5(107) – S. 62–69.

6. **Mutter V. M.** Osnovy pomehoustojchivoj teleperedachi informacii – L.: Jenergoatomizdat, 1990. – 286 s.

7. **Lipnickij, V. A.** Sovremennaja prikladnaja algebra. Matematicheskie osnovy zashhity informacii ot pomeh i nesankcionirovannogo dostupa. – Mn.: BGUIR, 2006. – 88 s.

8. **Liddl R., Nidderrajter G.** Konechnye polja. T.1, 2. – M.: Mir, 1988. – 882 s.

Поступила *16.01.2018*
После доработки *10.03.2018*
Принята к печати *01.06.2018*

Lipnickij V.[1], Serada A.[2]

PROPERTIES OF GROUPS G OF DOUBLE ERRORS AND ITS INVARIANTS IN BCH CODES

[1] Military Academy of the Republic of Belarus
[2] Belarusian State University of Mathematics and Radioelectronics

The goal of the work is the further extending the scope of application of code automorthism in methods and algorithms of error correction by these codes. The effectiveness of such approach was demonstrated by norm of syndrome theory that was developed by Belarusian school of noiseless coding at the turn of the XX and XXI century. The group Γ of the cyclical shift of vector component lies at the core of the theory. Under its action The error vectors are divided into disjoint Γ-orbits with definite spectrum of syndromes. This allowed to introduce norms of syndrome of a family of BCH codes that are invariant over action of group Γ. Norms of syndrome are unique characteristic of error orbit Γ of any decoding set, hence it is the basis of permutation norm methods of error decoding. Looking over the Γ-orbits of errors not the errors these methods are faster than classic syndrome methods of error decoding, are avoided from the complex process of solving the algebraic equation in Galois field, are simply implemented.

A detailed theory for automorphism group G of BCH codes obtained by adding cyclotomic substitution to the group Γ develops in the article. The authors held a detailed study of structure of G-orbit of errors as union of orbits Γ of error vectors; one-to-one mapping of this structure on the norm structure of group Γ. These norms being interconnected by Frobenius automorphism in the Galois field – field of BCH code constitute the complete set of roots of the only irreducible polynomial. It is a polynomial invariant of its orbit G. The main focus of the work is on the description of properties and specific features of groups G of double errors and its polynomial invariants.

Keywords: *BCH code, norm of syndrome theory, BCH code automorphism, norm of syndrome, syndrome, polynomial invariants of norm of syndrome.*

Липницкий Валерий Антонович – кандидат физико-математических наук (1980), доктор технических наук (2003), профессор по кафедре математики (2004), заведующий кафедрой высшей математики УО «Военная академия Республики Беларусь». Ученик академика В. П. Платонова и профессора В. К. Конопелько. Совместно с последним разработал теорию норм синдромов – новое направление в теории и практике помехоустойчивого кодирования, развивающее эффективное применение автоморфизмов кодов для коррекции ими ошибок в телекоммуникационных системах. Автор более 300 научных работ, четырёх монографий, ряда патентов на изобретения. Область научных интересов – алгебра и ее приложения, защита информации от помех и несанкционированного доступа.

Lipnitski Valery – PhD of Physico-Mathematical Sciences (1980), Grand PhD of Engineering Sciences (2003), Full Professor (2004), Head of the Department of Higher Mathematics of the Military Academy of the Republic of Belarus, the apprentice of academician V. P. Platonov and professor V. K. Konopelko. Together with the latter was developed norm of syndrome theory – a new direction in the theory and practice of noise-immune coding, which develops an effective application of code automorphisms for correcting errors in telecommunication systems. The author of more than 300 scientific works, four monographs, a number of patents for inventions. The field of scientific interests is algebra and its applications, information security from interference and unauthorized access. valipnitski@yandex.ru

Середа Елена Владимировна – магистр технических наук (2013), аспирант кафедры защиты информации УО «Белорусский государственный университет информатики и радиоэлектроники». Область научных интересов – исследование групп автоморфизмов линейных кодов и применение автоморфизмов кодов к разработке перестановочный алгоритмов декодирования этих кодов.

Serada Alena – Master of Engineering sciences (2013), PhD student at the Department of Information Security of the Belarusian State University of Informatics and Radioelectronics. The field of scientific interests is the investigation of automorphism groups of linear codes and the application of automorphisms of codes to the development of permutational algorithms for decoding these codes. elen.vt@gmail.com