УДК 512 (075.8)

ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ *G*-ОРБИТ ОШИБОК БЧХ-КОДОВ И ИХ ПРИМЕНЕНИЕ

В.А. ЛИПНИЦКИЙ[1], Е.В. СЕРЕДА[2]

[1]*Военная академия Республики Беларусь, Республика Беларусь*

[2]*Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь*

Поступила в редакцию 5 июля 2017

Аннотация. В статье предсатавлено дальнейшее развитие норменных методов декодирования БЧХ-кодов. Авторы предлагают в теорию норм синдромов ввести новые синдромные инварианты – полиномиальные инварианты группы G всех автоморфизмов семейства БЧХ-кодов. Рассмотрены основные свойства полиномиальных инвариантов, а также методика коррекции ошибок, опирающаяся на итерационную двухступенчатую систему их идентификации. На конкретном примере демонстрируется эффективность метода коррекции ошибок на основе полиномиальных инвариантов.

Ключевые слова: БЧХ-коды, синдром ошибки, автоморфизмы БЧХ-кодов, Г-орбиты и G-орбиты ошибок, норма синдрома, теория норм синдромов, полиномиальные инварианты G-орбит ошибок.

Abstract. The article addresses the further development of methods of BCH codes norm decoding. The authors propose to use new syndrome invariants – polynomial invariants of automorphism group G of a family of BCH codes. The paper presents basic properties of polynomial invariants and errors correction technique considered on two-step iteration system of error identification. An efficiency of the method of decoding based on polynomial invariants of G-orbit is demonstrated by the example.

Keywords: BCH code, syndrome, automorphism of BCH code, error Г-orbits and G-orbits, norm of syndrome, norm of syndrome theory, polynomial invariants of error G-orbits.

Doklady BGUIR. 2017, Vol. 107, No. 5, pp. 62-69
Polynomial invariants of *G*-orbit errors of BCH codes and its application
V.A. Lipnitski, E.V. Sereda

Введение

В теории и практике помехоустойчивого кодирования наиболее популярным является семейство линейных кодов Боуза – Чоудхури – Хоквингема (БЧХ-кодов), особенно в высокоскоростных информационно-коммуникационных системах (ИКС) [1]. Свойства цикличности этих кодов, близость их к классу совершенных кодов, возможность представления компонент синдромов ошибок элементами поля Галуа инициировали развитие различных алгебраических методов их обработки. Наиболее известным и применимым на практике оказался метод коррекции ошибок в примитивных БЧХ-кодах с решением алгебраических уравнений в конечных полях, задающих эти коды [1, 2]. Однако данный метод в высокоскоростных ИКС применяется практически лишь для коррекции ошибок весом 2. Декодирование ошибок весом больше двух по одношаговому принципу «синдром – ошибка» сразу же наталкивается на проблему «селектора», то есть на проблему быстрого и надежного нахождения конкретной ошибки из весьма большого по количеству многообразия этих ошибок [3, 4].

В целях решения проблемы «селектора» на рубеже XX и XXI веков белорусской школой помехоустойчивого кодирования разработана теория норм синдромов (ТНС) – теория инвариантов Г-орбит ошибок относительно группы Г-циклических сдвигов координат векторов – подгруппы группы автоморфизмов семейства БЧХ-кодов [4, 5]. Важнейшим следствием ТНС явились перестановочные норменные методы коррекции ошибок. Эти методы отличаются итерационным трехшаговым принципом декодирования ошибок: «синдром – норма синдрома – Г-орбита ошибок – ошибка». Впервые в помехоустойчивом кодировании был введен промежуточный идентификационный шаг, определяющий по вычисленной норме синдрома Г-орбиту, которой принадлежит ошибка. Сравнением синдрома искомой ошибки с синдромом одной из фиксированных образующих данной Г-орбиты ошибок несложно устанавливается точное значение корректируемой ошибки. Перестановочные норменные методы оказались на порядок эффективнее классических синдромных методов [4 – 6].

Современные условия предъявляют высокие требования к ИКС, направленные, прежде всего, на увеличение объемов информации, передаваемых в единицу времени. Реализация этих требований приводит к росту длин применяемых кодов, что, в свою очередь, неизбежно приводит к необходимости увеличения кратности исправляемых ошибок и на новом витке актуализирует проблему «селектора».

Наиболее естественным выходом из данной ситуации авторы видят в применении группы G автоморфизмов всего семейства БЧХ-кодов, содержащую подгруппу Г, и соответствующих G-орбит векторов-ошибок, являющихся объединением ряда Г-орбит. В работе впервые вводятся полиномиальные инварианты G-орбит, рассматриваются их основные свойства, а также методика коррекции ошибок, опирающаяся на итерационную двухступенчатую систему идентификации ошибки по принципу: «синдром – норма синдрома – полином – G-орбита – Г-орбита ошибок – ошибка».

О полях Галуа

Как известно [7, 8], всякое конечное поле $GF(2^m)$ характеристики 2 состоит из 2^m элементов, при $m>1$ является m-мерным векторным пространством над своим минимальным подполем $GF(2)=Z/2Z$. Его мультипликативная группа $GF(2^m)^*$ – циклическая группа порядка 2^m-1. Образующие этой циклической группы называются примитивными элементами поля. Всякий ненулевой элемент $\gamma \in GF(2^m)$ является корнем некоторого полинома $f_\gamma(x)$ с коэффициентами из $Z/2Z$ степени m или ниже, потому что система из $m+1$ векторов $1,\gamma,\gamma^2,...,\gamma^m$ из m-мерного пространства $GF(2^m)$ обязательно будет линейно зависимой. В кольце полиномов $Z/2Z[x]$ полином $f_\gamma(x)$ однозначно раскладывается в произведение неприводимых сомножителей, в частности, может сам оказаться неприводимым. Во всяком случае, γ будет корнем одного из неприводимых сомножителей данного разложения. Обозначим его через $Irr(\gamma,x)$ и назовем минимальным полиномом элемента $\gamma \in GF(2^m)$. Несложно проверить, что если γ будет корнем какого-то другого полинома $g(x)$, то $g(x)$ должен делиться на $Irr(\gamma,x)$. Если $\deg Irr(\gamma,x)=\mu<m$, то γ принадлежит подполю $GF(2^\mu)$ поля $GF(2^m)$. В таком случае μ обязательно является делителем числа m [7, 8].

Итак, всякий элемент поля Галуа $GF(2^m)$ является корнем некоторого неприводимого полинома из кольца $Z/2Z[x]$. Степень этого полинома равна m тогда и только тогда, когда данный элемент принадлежит $GF(2^m)$ и не принадлежит никакому его подполю. В частности, примитивные элементы поля являются корнями неприводимых полиномов степени m из кольца $Z/2Z[x]$. Поэтому данные полиномы также называют примитивными, тем более, что если один корень является примитивным элементом поля, то и остальные корни обладают тем же свойством.

Для вычислений в конкретном поле Галуа, его следует сформировать. Для этого необходимо зафиксировать в кольце $Z/2Z[x]$ примитивный полином $p(x)$ степени m, его

корень α, тогда все 2^m-1 степени α фактически образуют мультипликативное задание поля $GF(2^m)$. Эти же степени можно задать как векторы пространства $GF(2^m)$, скажем, в базисе

$$\alpha^{m-1},\alpha^{m-2},...,1. \qquad (1)$$

Такое задание удобно для выполнения аддитивных операций. Таблица, связывающая степени α с их векторным заданием, по существу, является реальным заданием поля Галуа, наиболее удобным для практических применений.

Поле $GF(2^m)$ является расширением Галуа поля $GF(2)$, так как на нем действует $Z/2Z$ – автоморфизм Фробениуса $\varphi: x \to x^2$. Своими степенями он порождает циклическую группу автоморфизмов порядка m, то есть всю группу автоморфизмов названного расширения. Из теории расширения Галуа [7, 9] известно, что, зная один из корней неприводимого полинома, остальные можно получить с помощью автоморфизмов группы Галуа. Так, если известно, что степень $\deg Irr(\gamma,x)=m$, то сам полином $Irr(\gamma,x)=(x-\gamma)(x-\varphi(\gamma))\cdot...\cdot(x-\varphi^{m-1}(\gamma))=(x-\gamma)(x-\gamma^2)\cdot...\cdot(x-\gamma^{2^{m-1}})$. Раскрыв скобки непосредственно или с помощью формул Виета, мы получим полином $Irr(\gamma,x)\in Z/2Z[x]$ в стандартном виде. Впрочем, зная список всех неприводимых полиномов *m*-й степени из $Z/2Z[x]$, $Irr(\gamma,x)$ можно найти последовательной подстановкой γ в полиномы из этого списка.

БЧХ-коды с конструктивным расстоянием 5

Всякий двоичный БЧХ-код C определен над некоторым полем Галуа $GF(2^m)$, имеет конкретную длину n, где $n=2^m-1$ (и тогда БЧХ-код называется примитивным), или же n является делителем 2^m-1 (и тогда код называется не примитивным). БЧХ-код C_5 с конструктивным расстоянием 5 задается проверочной матрицей $H=\{\alpha^i,\alpha^{3i}\}^T$ в примитивном случае и матрицей $H=\{\beta^i,\beta^{3i}\}^T$ – для не примитивного кода; здесь $0\le i\le n-1$, $\beta=\alpha^\tau$, где $\tau=(2^m-1)/n$. Матрицы H предполагаются двоичными, каждая степень α^j – столбец с n координатами 0,1 – координатами α^j в базисе (1). Естественно, код C_5 существует при условии $2m<n$ (размерность кода C_5 есть величина $k=n-2m$). Известно [1], что в примитивном случае точное значение минимального расстояния кода C_5 совпадает с конструктивным расстоянием; в не примитивном случае практически треть кодов имеют минимального расстояния больше 5 [10]. Именно в случаях, когда $d>5$, не примитивные БЧХ-коды и представляют практический интерес.

Главное достоинство всякого помехоустойчивого кода состоит в его способности к исправлению тех или иных ошибок. Все линейные коды с минимальным расстоянием $d\ge 3$ способны исправлять ошибки весом 1, точно также как и коды Хемминга: исправляемая координата по номеру совпадает с номером того столбца проверочной матрицы, который равен синдрому этой ошибки. Линейные коды с $d=5$ исправляют все ошибки весом 2. Для примитивных БЧХ-кодов, чаще всего, это исправление осуществляется методом решения квадратных уравнений в полях Галуа [1, 11, 12].

Как правило, минимальное расстояние БЧХ-кода является нечетным числом: $d=2t+1$; тогда код способен исправлять ошибки весом $1,2,...,t$. Для не примитивных БЧХ-кодов C_5 с $d>5$ метод уравнений не применим в принципе. Реальным и эффективным выходом здесь является применение перестановочных методов на основе ТНС [4, 5, 12].

Некоторые сведения об автоморфизмах БЧХ-кодов

Согласно [1, 4, 5, 12] группа $AutC$ автоморфизмов всякого линейного кода C, в том числе и БЧХ-кода C_5, есть группа перестановок координат кодовых слов, преобразующих

кодовые слова в слова этого же кода. Группа $AutC_5$ достаточно обширна. Она содержит циклическую подгруппу Г, состоящую из степеней автоморфизма σ – автоморфизма циклического сдвига координат векторов: $\sigma(e_1, e_2, ..., e_n) = (e_n, e_1, e_2, ..., e_{n-1})$. Очевидно, $|\Gamma| = n$ в силу нечетности длины n. Каждый вектор ошибок $\bar{e}$ в БЧХ-коде C порождает свою Г-орбиту: $J = <\bar{e}_\Gamma> = \{\bar{e}, \sigma(\bar{e}), ..., \sigma^{\nu-1}(\bar{e})\}$, где ν – наименьшее натуральное число с условием: $\sigma^{\nu}(\bar{e}) = \bar{e}$. Известно, что ν в большинстве случаев совпадает с n (тогда Г-орбита называется полной), но, в отдельных случаях, является делителем n. Каждая Г-орбита имеет строгую циклическую структуру. Г-орбиты между собой не пересекаются.

Группа $AutC$ содержит также циклотомический автоморфизм φ [1, 5, 12], действующий на каждую координату $i \in \{1, 2, ..., n\}$ по правилу:

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

Преобразование φ, действующее по формуле (2), является автоморфизмом БЧХ-кодов для всех нечетных n. Этот автоморфизм имеет порядок m, при этом для любого вектора-ошибки $\bar{e}$:

$$\varphi\left(\sigma\left(\bar{e}\right)\right) = \sigma^2\left(\varphi\left(\bar{e}\right)\right). \quad (3)$$

Группа Г имеет порядок n, а минимальная группа G, содержащая σ и φ, – порядок mn в силу формулы (3). Каждая G-орбита состоит из Г-орбит и имеет следующую структуру: $I_G = \{J, \varphi(J), \varphi^2(J), ..., \varphi^{(\mu-1)}(J)\}$ для конкретной Г-орбиты J. Здесь μ – наименьший делитель числа m с условием: $\varphi^{\mu}(J) = J$. В большинстве случаев $\mu = m$, и G-орбиты имеют, как правило, мощность mn.

Нормы синдромов и норменные декодеры для БЧХ-кодов

Классический примитивный БЧХ-код длиной n, исправляющий двойные ошибки, задается проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^T$, $0 \le i \le 2^m - 2 = n - 1$, α – примитивный элемент поля $GF(2^m)$. Синдром ошибок в сообщении $\bar{x}$ вычисляется по формуле $S(\bar{x}) = H \cdot \bar{x}^T$. В соответствии со структурой проверочной матрицы здесь $S(\bar{x}) = (s_1, s_2)^T$, где s_1, s_2 – компоненты синдрома, элементы поля $GF(2^m)$.

Согласно предложению 3.1 [4]

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

Формула (4) устанавливает строгую однозначную взаимосвязь между синдромами векторов-ошибок каждой Г-орбиты, копирующую взаимосвязь векторов-ошибок внутри самой Г-орбиты. В силу формулы (4) норма $N(S(\bar{x}))$ синдрома $S(\bar{x})$ вычисляется по формуле (см. [4], гл. 4):

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

При заданном формулой (4) определении легко выясняется, что норма синдрома одинакова для всех векторов-ошибок каждой Г-орбиты J, то есть является инвариантом этой орбиты, а потому и называется нормой Г-орбиты J. Согласно теореме 4.1 [4] нормы множества T Г-орбит одиночных и двойных ошибок попарно различны. Составив список ET образующих $\bar{e}_i$ Г-орбит множества T, список ST синдромов образующих $S(\bar{e}_i)$ и список NST норм синдромов образующих $N(S(\bar{e}_i))$, можно реализовать работу норменного декодера (см. [4], гл. 4 и 5) следующим образом.

Декодер всякой ИКС, построенный на основе любого БЧХ-кода C_5, в обязательном порядке вычисляет синдром $S(\bar{x})$ каждого принятого блока-сообщения $\bar{x}$. Условие $S(\bar{x}) \ne 0$ означает наличие в сообщении $\bar{x}$ ненулевого вектора-ошибки $\bar{e}$, который декодер должен откорректировать. Путем вычисления $N(S(\bar{x}))$ по формуле (5) через компоненты синдрома

$S(\bar{x})$ идентифицируется Г-орбита *J*, которой принадлежит искомая ошибка $\bar{e}$ в сообщении $\bar{x}$. Не представляет особой сложности установить точное значение $\bar{e}$ внутри Г-орбиты *J*: сравнивая синдромы искомой ошибки и образующей Г-орбиты *J*, устанавливается величина циклического сдвига образующей для получения искомого корректируемого вектора-ошибки. Норменные методы оказались в *n* раз быстрее стандартных методов коррекции ошибок, где *n* – длина кода. Декодеры на их основе хорошо реализуются на БИС нейросетевого типа.

С ростом длины применяемых кодов, с увеличением кратности исправляемых векторов-ошибок (последнее особенно типично при применении не примитивных БЧХ-кодов, см., например, [5]) резко возрастают объемы ошибок, подлежащих исправлению, что существенно увеличивает названные выше списки и замедляет работу с ними. Для преодоления создавшейся проблемы предлагается перейти от Г-орбит к более крупным группам ошибок – *G*-орбитам.

G-орбиты и их полиномиальные инварианты

В силу предложения 3.17 в работе [5] $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$. Отсюда следует, что $N(S(\varphi(\bar{e}))) = (N(S(\bar{e})))^2$. Действие φ на координаты векторов-ошибок подробно изложено в [5], стр. 40 – 41, см. также [12, гл. 3]. Таким образом, почти автоматически строится селекция орбит множества *T* в *G*-орбиты, а также списков *ST* и *NST*. Список *EG* образующих *G*-орбит строится из списка *ET* и, практически, в *m* раз меньше списка *ET*.

Возьмём образующую $\bar{e}_i \in EG$. Ее норма $N_i = N(S(\bar{e}_i)) = \alpha^j$ – конкретный ненулевой элемент поля Галуа $GF(2^m)$. Как правило, *G*-орбита $<\bar{e}_i>_G$ состоит из *m* Г-орбит. Нормы этих Г-орбит получаются последовательным возведением в квадрат $N_i = \alpha^j$. Но возведение в квадрат элементов поля Галуа $GF(2^m)$ равносильно действию на $N_i = \alpha^j$ автоморфизма Фробениуса, образующей φ циклической группы Галуа этого поля. Таким образом, список норм Г-орбит *G*-орбиты $<\bar{e}_i>_G$ имеет вид: $N(<\bar{e}_i>_G) = \left\{N_i, \varphi(N_i), ..., \varphi^{m-1}(N_i)\right\} = \left\{\alpha^j, \alpha^{2j}, ..., \alpha^{2^{m-1}j}\right\}$. Аналогично строятся и синдромы образующих этих Г-орбит. Построенный список норм Г-орбит, составляющих *G*-орбиту $<\bar{e}_i>_G$, есть множество всех сопряженных друг другу под действием группы Галуа элементов поля. Такие элементы составляют полный список корней неприводимого полинома над минимальным подполем $Z/2Z = GF(2)$. Этот полином выше был назван минимальным полиномом любого из элементов названного списка; его, как правило, обозначают $Irr(\alpha^j, x)$ [7, 8]. Итак, полином

$$Irr(\alpha^j, x) = (x - \alpha^j)(x - \alpha^{2j}) \cdot ... \cdot (x - \alpha^{2^{m-1}i}) \qquad (6)$$

является однозначной характеристикой *G*-орбиты $<\bar{e}_i>_G$. А потому для него будем применять и иное обозначение: $p(\mathrm{G}, x) = p(<\bar{\mathrm{e}}_i>_G, \mathrm{x})$. *G*-орбита $<\bar{e}_i>_G$ содержит $\mu < m$ Г-орбит тогда и только тогда, когда α^j принадлежит подполю $GF(2^\mu)$ поля $GF(2^m)$.

Метод декодирования ошибок на основе *G*-орбит предполагает составление списка *PEG* неприводимых полиномов (6), норм синдромов образующих *G*-орбит, двухступенчатую систему идентификации ошибки: найдя ненулевой синдром ошибки, вычисляем ее норму, затем находим неприводимый полином этой нормы, данный полином сравниваем со списком *PEG*. Отождествив вычисленный полином с каким-то полиномом списка *PEG*, далее сравнивается вычисленная норма только со списком норм Г-орбит соответствующей *G*-орбиты. Дальнейшие действия с Г-орбитами уже описаны выше.

Пример

Рассмотрим БЧХ-код C_5 длиной 127 над полем $GF(2^7)$ с проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^T$, $0 \le i \le 30$, α – корень примитивного полинома $p(x) = x^7 + x + 1$. Здесь двойные

ошибки делятся на 63 Г-орбиты, а те на 9 *G*-орбит по 7 Г-орбит в каждой. Табл. 1 представляет список образующих $\overline{e}_i = \overline{e}_{1,\mathrm{j}}$ *G*-орбит двойных ошибок (с равными единице первой и j-й координатами), синдромов, норм синдромов и неприводимых полиномов этих G-орбит.

Пусть ИКС с данным кодом приняла блок-сообщение $\overline{x}$ с синдромом $S(\overline{x}) = (s_1, s_2)^T = (\alpha^{122}, \alpha^{48})^T$. Тогда в силу формулы (5) норма синдрома $N = N(S(\overline{x})) = \alpha^{63}$, а с помощью формулы (6) или таблиц устанавливается, что полином $p(N, x) = x^7 + x^6 + 1$. Он совпадает с третьим полиномом из табл. 1. Это означает, что вектор-ошибка $\overline{e}$ в принятом сообщении $\overline{x} = \overline{c} + \overline{e}$, где $\overline{c}$ – истинное сообщение, принадлежит третьей G-орбите из табл. 1.

Таблица 1. **Список образующих *G*-орбит двойных ошибок в БЧХ-коде C_5^{127}, синдромов образующих, норм синдромов и полиномиальных инвариантов этих орбит**

№ п/п	Образующая *G*-орбиты	Синдром $s_1(\overline{e}_{i,j})$	Синдром $s_2(\overline{e}_{i,j})$	Норма $N(S(\overline{e}_{i,j}))$	Неприводимый полином $p(x)$
1	$\overline{e}_{1,2}$	α^7	α^{63}	α^{42}	$x^7 + x^6 + x^3 + x + 1$
2	$\overline{e}_{1,4}$	α^{63}	α^{90}	α^{28}	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
3	$\overline{e}_{1,6}$	α^{54}	α^{31}	α^{123}	$x^7 + x^6 + 1$
4	$\overline{e}_{1,8}$	α	α^{57}	α^{54}	$x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$
5	$\overline{e}_{1,10}$	α^{90}	α^{31}	α^{50}	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
6	$\overline{e}_{1,12}$	α^{87}	α^{77}	α^{70}	$x^7 + x^6 + x^5 + x^2 + 1$
7	$\overline{e}_{1,14}$	α^{55}	α^{100}	α^{62}	$x^7 + x^6 + x^4 + x^2 + 1$
8	$\overline{e}_{1,20}$	α^{29}	α^{20}	α^{61}	$x^7 + x^6 + x^5 + x^4 + 1$
9	$\overline{e}_{1,22}$	α^{57}	α^3	α^{86}	$x^7 + x^6 + x^4 + x + 1$

В табл. 2 приведен список образующих $\overline{e}_{1,j}$ всех семи Г-орбит, составляющих названную *G*-орбиту, синдромов образующих и норм синдромов.

Таблица 2. **Образующая Г-орбит третьей *G*-орбиты из табл. 1, синдромы образующих и их нормы**

№ п/п	Образующая Г-орбиты	Синдром $s_1(\overline{e}_{i,j})$	Синдром $s_1(\overline{e}_{i,j})$	Норма $N(S(\overline{e}_{i,j}))$
1	$\overline{e}_{1,6}$	α^{54}	α^{31}	α^{123}
2	$\overline{e}_{1,11}$	α^{108}	α^{62}	α^{119}
3	$\overline{e}_{1,21}$	α^{89}	α^{124}	α^{111}
4	$\overline{e}_{1,41}$	α^{51}	α^{121}	α^{95}
5	$\overline{e}_{1,81}$	α^{102}	α^{115}	α^{63}
6	$\overline{e}_{1,34}$	α^{77}	α^{103}	α^{126}
7	$\overline{e}_{1,67}$	α^{27}	α^{79}	α^{125}

Сравниваем вычисленную норму N с нормами из табл. 2. Как видим, вычисленная норма N совпала с нормой образующей пятой Г-орбиты из табл. 2. Таким образом, искомая ошибка $\overline{e}$ принадлежит пятой Г-орбите из табл. 2 и находится циклическим сдвигом образующей $\overline{e}_{1,81}$ на величину, которая получается сравнением первых компонент s_1 синдрома $S(\overline{x})$ и синдрома $S(\overline{e}_{1,81})$: $\dfrac{s_1(\overline{x})}{s_1(\overline{e}_{1,81})} = \dfrac{\alpha^{122}}{\alpha^{102}} = \alpha^{20}$. Результаты вычислений показывают, что искомая ошибка $\overline{e}$ в принятом сообщении $\overline{x}$ получается циклическим сдвигом координат образующей $\overline{e}_{1,81}$ вправо на 20 позиций. Следовательно, $\overline{e} = \overline{e}_{21,101}$ – двойная ошибка с единичными координатами на позициях 21 и 101. Тогда истинное сообщение $\overline{c} = \overline{x} + \overline{e}_{21,101}$.

Заключение

Предложены полиномиальные инварианты G-орбит векторов-ошибок. Они обеспечивают трехэтапную итерационную процедуру декодирования ошибок кодами семейства БЧХ, примерно в mn раз более эффективную, чем стандартные синдромные методы. Особенность названной процедуры в последовательной уточняющей идентификации искомой ошибки: сначала с помощью полиномиального инварианта определяем G-орбиту, которой принадлежит искомая ошибка; затем с помощью норм Г-орбит, принадлежащих найденной G-орбите, определяем конкретную Г-орбиту, содержащую корректируемую ошибку; наконец, сравнивая синдромы образующей найденной Г-орбиты и декодируемой ошибки, определяем величину циклического сдвига образующей для получения точного значения искомой ошибки.

Предложенные полиномиальные инварианты эффективны в применении к не примитивным БЧХ-кодам и к любым БЧХ-кодам с конструктивным расстоянием, большим или равным пяти.

Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. М.: Техносфера, 2006. 320 с.
3. Колесник В.Д., Мирончиков Е.Т. Декодирование циклических сдвигов. М.: Связь, 1968. 251 с.
4. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск: БГУИР, 2000. 242 с.
5. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: БГУ, 2007. 239 с.
6. Липницкий В.А., Олексюк А.О. Устройство декодирования для коррекции четырехкратных ошибок / Патент Респ. Бел. № 19822.
7. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 430 с.
8. Липницкий В.А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. Минск: БГУИР, 2006. 88 с.
9. Ленг С. Алгебра. М.: Мир, 1968. 134 с.
10. Липницкий В.А., Олексюк А.О. Теория норм синдромов и плюс-декодирование // Докл. БГУИР. 2014. № 8. С. 71–78.
11. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
12. Липницкий В.А. Теория норм синдромов: курс лекций. Минск.: БГУИР, 2010.

References

1. Mak-Vil'jams F. Dzh., Slojen N. Dzh. A. Teorija kodov, ispravljajushhih oshibki. M.: Svjaz', 1979. 744 s. (in Russ.)
2. Morelos-Saragosa R. Iskusstvo pomehoustojchivogo kodirovanija. M.: Tehnosfera, 2006. 320 s. (in Russ.)
3. Kolesnik V.D., Mironchikov E.T. Dekodirovanie ciklicheskih sdvigov. M.: Svjaz', 1968. 251 s. (in Russ.)
4. Konopel'ko V.K., Lipnickij V.A. Teorija norm sindromov i perestanovochnoe dekodirovanie pomehoustojchivyh kodov. Minsk: BGUIR, 2000. 242 s. (in Russ.)
5. Lipnickij V.A., Konopel'ko V.K. Normennoe dekodirovanie pomehoustojchivyh kodov i algebraicheskie uravnenija. Minsk: BGU, 2007. 239 s. (in Russ.)
6. Lipnickij V.A., Oleksjuk A.O. Ustrojstvo dekodirovanija dlja korrekcii chetyrehkratnyh oshibok / Patent Resp. Bel. № 19822. (in Russ.)
7. Lidl R., Niderrajter G. Konechnye polja. M.: Mir, 1988. 430 s. (in Russ.)
8. Lipnickij V.A. Sovremennaja prikladnaja algebra. Matematicheskie osnovy zashhity informacii ot pomeh i nesankcionirovannogo dostupa. Minsk: BGUIR, 2006. 88 s. (in Russ.)
9. Leng S. Algebra. M.: Mir, 1968. 134 s. (in Russ.)
10. Lipnickij V.A., Oleksjuk A.O. Teorija norm sindromov i pljus-dekodirovanie // Dokl. BGUIR. 2014. № 8. S. 71–78. (in Russ.)
11. Blejhut R. Teorija i praktika kodov, kontrolirujushhih oshibki. M.: Mir, 1986. 576 s. (in Russ.)
12. Lipnickij V.A. Teorija norm sindromov: kurs lekcij. Minsk.: BGUIR, 2010. (in Russ.)

Сведения об авторах

Липницкий В.А., д.т.н., профессор, заведующий кафедрой высшей математики Военной академии Республики Беларусь.

Середа Е.В., м.т.н., аспирант кафедры защиты информации Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220057, Республика Беларусь,
г. Минск, пр-т Независимости, д. 220,
Военная академия Республики Беларусь,
тел.: +375 17 287-42-82;
e-mail: valipnitski@yandex.ru
Липницкий Валерий Антонович

Information about the authors

Lipnickij V.A., D.Sci., professor, head of the department of higher mathematics of Military academy of Republic of Belarus.

Sereda E.V., master of technical sciences, PG student of information security department of Belarusian state university of informatics and radioelectronics.

Address for correspondence

220057 Republic of Belarus,
Minsk, Nezavisimosti ave., 220,
Military academy of Republic of Belarus,
tel. +375-17-287-42-82;
e-mail: valipnitski@yandex.ru
Lipnickij Valery Antonovich