УДК 512 (075.8)

ПОЛИНОМИАЛЬНЫЕ ИНВАРИАНТЫ В НОРМЕННОЙ ОБРАБОТКЕ ПОМЕХОУСТОЙЧИВЫХ КОДОВ

[1]В.А. ЛИПНИЦКИЙ, [2]Е.В. СЕРЕДА

[1]*Военная академия Республики Беларусь*
Минск-57, 220057, Беларусь

[2]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

Предлагается использование полиномиальных инвариантов при норменной коррекции многократных ошибок БЧХ-кодами.

Ключевые слова: норменная коррекция, ошибка, полиномиальный инвариант.

Классическое в теории помехоустойчивого кодирования семейство кодов Боуза–Чоудхури–Хоквингема (БЧХ-кодов) является наиболее популярным в приложениях, особенно в высокоскоростных системах передачи информации [1]. Определенная однородность этих кодов, возможность представления компонентов синдромов ошибок элементами конечного поля позволили развить различные алгебраические методы их обработки. К наиболее известным и применимым относится метод коррекции ошибок примитивными БЧХ-кодами путем решения уравнений в полях Галуа. На рубеже XX и XXI веков учеными белорусской школы помехоустойчивого кодирования разработана теория норм синдромов (ТНС) [2, 3]. Нормы синдромов – синдромные инварианты группы Г циклических сдвигов – подгруппы группы AutC автоморфизмов всякого циклического БЧХ-кода С, кодов Хемминга, реверсивных кодов, – являются своеобразными индикаторами Г-орбит. Установлено, что нормы синдромов Г-орбит ошибок декодируемой совокупности попарно различны. Таким образом, ТНС предоставляет новые эффективные норменные методы коррекции ошибок кодами семейства БЧХ. Декодер всякой инфокоммуникационной системы (ИКС), построенный на основе любого БЧХ-кода, в обязательном порядке вычисляет синдром $S(\bar{x})$ каждого принятого блока-сообщения $\bar{x}$. Условие $S(\bar{x}) \neq 0$ означает наличие в сообщении $\bar{x}$ ненулевого вектора-ошибки $\bar{e}$, которую декодер должен откорректировать. Вычислив $N(S(\bar{x})$ по установленным в [2, 3] формулам через компоненты синдрома $S(\bar{x})$, можно идентифицировать Г-орбиту *J*, которой принадлежит искомая ошибка $\bar{e}$ в сообщении $\bar{x}$. Не представляет особой сложности установить точное значение $\bar{e}$ внутри Г-орбиты *J* [2, 3]. Норменные методы оказались не только в *n* раз быстрее стандартных методов коррекции ошибок (*n* – длина кода), но и существенно проще в реализации, а декодеры на их основе хорошо реализуются на БИС нейросетевого типа.

Ниже предлагается дальнейшее развитие ТНС путем введения новых синдромных инвариантов – полиномиальных. Демонстрируется действенность этих инвариантов на конкретном примере.

Автоморфизмы БЧХ-кодов. Для всякого БЧХ-кода С его группа автоморфизмов AutC содержит некоммутативную подгруппу G, порожденную подгруппой Г и циклотомическим автоморфизмом φ [1, 3], порожденным автоморфизмом Фробениуса поля Галуа $GF(2^m)$ – поля определения кода С. Группа Г имеет порядок *n*, а группа *G* – порядок mn. Подавляющее большинство Г-орбит имеет мощность *n*, а *G*-орбиты имеют, как правило, мощность mn.

Каждая *G*-орбита состоит из Г-орбит и имеет следующую структуру: $I_G = \{J, \varphi(J), \varphi^2(J), \ldots, \varphi^{\mu-1}(J)\}$ для конкретной Г-орбиты *J*. Здесь μ – наименьший делитель m с условием: $\varphi^{\mu}(J) = J$. В большинстве случаев $\mu = m$.

Всякая Г-орбита *J* имеет похожую структуру: для автоморфизма σ циклического сдвига координат векторов: $\sigma(e_1, e_2, \ldots, e_n) = (e_n, e_1, e_2, \ldots, e_{n-1})$, и для любой своей вектор-ошибки $\bar{e}$: $J = \{\bar{e}, \sigma(\bar{e}), ..., \sigma^{\nu-1}(\bar{e})\}$, где ν – наименьшее натуральное число с условием: $\sigma^{\nu}(\bar{e}) = \bar{e}$. Известно, что мощность Г-орбиты делит *n* и, как правило, совпадает с *n*. В силу сказанного часто используются обозначения: $J = \langle \bar{e} \rangle$ или $J = \langle \bar{e}_{\Gamma} \rangle$.

Нормы синдромов и норменные декодеры для БЧХ-кодов. Классический примитивный БЧХ-код длиной n, исправляющий двойные ошибки, задается проверочной матрицей $H = \{\alpha^i, \alpha^{3i}\}^{\mathrm{T}}$, $0 \le i \le 2^m - 2 = n - 1$, 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 согласии со структурой проверочной матрицы $S(\bar{x}) = (s_1, s_2)^T$, где s_1, s_2 – компоненты синдрома, элементы поля $GF(2^m)$. Согласно предложению 3.1 [2], $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2)^T$. В силу этой формулы норма $N(S(\bar{x}))$ синдрома $(S(\bar{x}))$ вычисляется по формуле (см. [2], глава 4): $N(S(\bar{x})) = \frac{s_2}{s_1^3}$.

При таком определении норма синдрома одинакова для всех ошибок Г-орбиты $J = \langle \bar{e}_{\Gamma} \rangle$, т.е. является инвариантом этой орбиты, а потому и называется нормой этой Г-орбиты. Согласно теореме 4.1 [2], 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 можно реализовать работу норменного декодера по отмеченному во введении алгоритму.

Современные условия предъявляют высокие требования к инфокоммуникационным системам, прежде всего, к росту объемов информации, передаваемой в единицу времени. Это приводит к увеличению длин применяемых кодов, что, в свою очередь, отражается в увеличении названных выше списков и замедляет работу норменных декодеров. Один из выходов из сложившейся ситуации состоит в применении *G*-орбит и их полиномиальных инвариантов.

G-орбиты и их полиномиальные инварианты. В силу [3], $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$. Отсюда следует, что $N(S(\varphi(\bar{e}))) = (N(S(\bar{e})))^2$. Действие φ на координаты векторов-ошибок подробно изложено в [3, с. 40–41]. 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*.

Возьмем 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 автоморфизм Фробениуса, образующей φ циклической группы Галуа этого поля. Таким образом, список норм Г-орбит *G*-орбиты $<\bar{e}_i>_G$ имеет вид: $N(<\bar{e}_i>_G) = \{N_i, \varphi(N_i), ..., \varphi^{m-1}(N_i)\} = \{\alpha^j, \alpha^{2j}, ..., \alpha^{2^{m-1}j}\}$. Аналогично строятся и синдромы образующих этих Г-орбит. Построенный список норм Г-орбит, составляющих *G*-орбиту $<\bar{e}_i>_G$ есть множество всех элементов поля, сопряженных друг другу под действием группы Галуа. Такие элементы составляют полный список корней

неприводимого полинома над минимальным подполем $Z/2Z = GF(2)$. Этот полином называют минимальным полиномом любого из элементов названного списка и, как правило, обозначают $p(\alpha^j, x)$ [4, 5]. Полином $p(\alpha^j, x) = (x-\alpha^j)(x-\alpha^{2j})\cdot\ldots\cdot(x-\alpha^{2^{m-1}i}) = p(<\bar{e}_i>_G, x)$, очевидно, является однозначной характеристикой *G*-орбиты $<\bar{e}_i>_G$. *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 норм синдромов образующих *G*-орбит и двухступенчатую систему идентификации ошибки: найдя ненулевой синдром ошибки, можно вычислить ее норму, затем найти неприводимый полином этой нормы, данный полином сравнить со списком *PEG*. Отождествив вычисленный полином с каким-то полиномом списка *PEG*, далее можно сравнить вычисленную норму только со списком норм Г-орбит соответствующей *G*-орбиты и провести дальнейшие действия по коррекции, описанные 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. В табл. 1 представлен список образующих $\bar{e}_i = \bar{e}_{1,\mathrm{j}}$ *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 $\bar{x}$ с синдромом $S(\bar{x}) = (s_1, s_2)^{\mathrm{T}} = (\alpha^{122}, \alpha^{48})^{\mathrm{T}}$. Тогда норма синдрома $N = N(S(\bar{x})) = \alpha^{63}$, а полином $p(N, x) = x^7 + x^6 + 1$, который совпадает с третьим полиномом 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 $s_1(\bar{e}_{i,j})$	Синдром $s_2(\bar{e}_{i,j})$	Норма $N(S(\bar{e}_{i,j}))$	Неприводимый полином $p(x)$
1	$\bar{e}_{1,2}$	α^7	α^{63}	α^{42}	$x^7 + x^6 + x^3 + x + 1$
2	$\bar{e}_{1,4}$	α^{63}	α^{90}	α^{28}	$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$
3	$\bar{e}_{1,6}$	α^{54}	α^{31}	α^{123}	$x^7 + x^6 + 1$
4	$\bar{e}_{1,8}$	α	α^{57}	α^{54}	$x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$
5	$\bar{e}_{1,10}$	α^{90}	α^{31}	α^{50}	$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$
6	$\bar{e}_{1,12}$	α^{87}	α^{77}	α^{70}	$x^7 + x^6 + x^5 + x^2 + 1$
7	$\bar{e}_{1,14}$	α^{55}	α^{100}	α^{62}	$x^7 + x^6 + x^4 + x^2 + 1$
8	$\bar{e}_{1,20}$	α^{29}	α^{20}	α^{61}	$x^7 + x^6 + x^5 + x^4 + 1$
9	$\bar{e}_{1,22}$	α^{57}	α^3	α^{86}	$x^7 + x^6 + x^4 + x + 1$

Вычисленная норма N совпала с нормой образующей пятой Г-орбиты из табл. 2, в которой приведен список образующих $\bar{e}_{1,j}$ всех семи Г-орбит, составляющих названную *G*-орбиту, синдромов образующих и норм синдромов.

Результат сравнения синдрома $S(\bar{x})$ с синдромом $S(\bar{e}_{1,81})$: $\dfrac{s_1(\bar{x})}{s_1(\bar{e}_{1,81})} = \dfrac{\alpha^{122}}{\alpha^{102}} = \alpha^{20}$. Таким образом, искомый вектор в принятом сообщении $\bar{x}$ получается путем циклического сдвига вправо на 20 позиций координат образующей $\bar{e}_{1,81}$. Следовательно, $\bar{e} = \bar{e}_{21,101}$ – двойная ошибка с единичными координатами на позициях 21 и 101. Тогда истинное сообщение $\bar{c} = \bar{x} + \bar{e}_{21,101}$.

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}

POLYNOMIAL INVARIANTS IN NORMAL PROCESSING OF INTERMEDIATE CODES

V.A. LIPNYTSKI, E.V. SEREDA

Abstract

The use of polynomial invariants under the normal correction of multiple errors by BCH-codes is proposed.

Keywords: norm correction, error, polynomial invariant.

Список литературы

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М.: УРСС, 2004.
3. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: БГУ, 2007.
4. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
5. *Липницкий В.А.* Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск: БГУИР, 2006.