УДК 004.056.55

УСЕЧЕННЫЙ ПОЛИНОМИАЛЬНО-НОРМЕННЫЙ МЕТОД КОРРЕКЦИИ ОШИБОК В НЕПРИМИТИВНЫХ БЧХ-КОДАХ C_5

Е.В. СЕРЕДА[1], В.А. ЛИПНИЦКИЙ[2], В.К. КОНОПЕЛЬКО[1]

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

Поступила в редакцию 20 марта 2019

Аннотация. Рассмотрены полиномиальные инварианты *G*-орбит ошибок, которые создают хорошие перспективы для декодирования больших спектров ошибок. Приведена развернутая формулировка усеченного двухуровневого полиномиально-норменного метода коррекции всех допустимых реальным минимальным расстоянием ошибок непримитивными БЧХ-кодами. В цепочку «синдром-ошибка» норменные методы ввели промежуточный уровень идентификации Г-орбиты, которой принадлежит искомая ошибка, что сокращает поисковые процедуры. Данный метод вводит еще один уровень идентификации – определение узкой группы *G*-орбит, среди которых лежит искомый вектор ошибок.

Ключевые слова: БЧХ-код, автоморфизм кодов, группа циклических сдвигов координат векторов, циклотомические подстановки.

Введение

Теория норм синдромов [1–3] обосновала норменный метод декодирования ошибок в семействе БЧХ-кодов, который легко реализуется и действует на порядок быстрее иных синдромных методов. Данный метод может быть усовершенствован и ускорен с помощью полиномиальных инвариантов.

Рассмотрим циклические двоичные БЧХ-коды C длины $n=(2^m-1)/\tau$ для целых $\tau>1$, задаваемые проверочными матрицами вида $H=[\beta^i,\beta^{3i}]^T$, $0\le i\le n-1$, где $\beta^\tau=\alpha$ и α – корень примитивного неприводимого над $GF(2)$ полинома степени m, $m\ge 3$, α – примитивный элемент поля определения кода C, поля Галуа $GF(2^m)$ [2–4]. Из непримитивных БЧХ-кодов C_5 с проверочной матрицей H с практической точки зрения представляют интерес только те коды, минимальное расстояние которых больше конструктивного: $d>5$. Обозначим такие коды C_5^+.

Проблема декодирования в кодах C_5^+

Пусть инфокоммуникационная система (ИКС) на основе БЧХ-кода C_5^+ приняла сообщение $\bar{x}$. Вычисляем синдром ошибок $S(\bar{x})=H\cdot\bar{x}^T=(s_1,s_2)^T$, где s_1, s_2 – элементы поля Галуа $GF(2^m)$. Неравенство $S(\bar{x})\ne\bar{0}$ означает существование ошибок в принятом сообщении: $\bar{x}=\bar{c}+\bar{e}$, где $\bar{c}$ – истинное сообщение, $\bar{e}$ – вектор ошибок. Поскольку $H\cdot\bar{c}^T=\bar{0}$, то $S(\bar{x})=S(\bar{e})$ – зависит только от вектора-ошибки $\bar{e}$.

Группа Г – циклическая группа порядка n – состоит из степеней циклической подстановки σ, действующей на каждый вектор $\bar{x}=(x_1,x_2,...,x_n)$ по правилу: $\sigma(\bar{x})=(x_n,x_1,x_2,...,x_{n-1})$. Для всякой вектор-ошибки $\bar{e}=(e_1,e_2,...,e_n)$ ее Г-орбита $<\bar{e}>_\Gamma=<\bar{e}>=\{\bar{e},\sigma(\bar{e}),...,\sigma^{\nu-1}(\bar{e})\}$, где ν – наименьшее натуральное число с условием: $\sigma^\nu(\bar{e})=\bar{e}$. Известно, что при этом ν делит n или же $\nu=n$. При $\nu=n$ Г-орбита $<\bar{e}>$ называется полной. Действие σ на вектор $\bar{e}$

в БЧХ-коде C с проверочной матрицей H единовременно влечет изменение синдрома: если $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2)^T$, то $S(\sigma(\bar{e})) = H \cdot \sigma(\bar{e})^T = (\beta \cdot s_1, \beta^3 \cdot s_2)^T$ [1–3]. Из последнего равенства следует определение нормы синдрома: $N(S(\bar{e})) = s_2 / s_1^3$. Так как $N(S(\sigma(\bar{e}))) = N(S(\bar{e}))$, то вычисленная норма становится инвариантом – нормой Г-орбиты $J = <\bar{e}>_\Gamma$ – и обозначается $N(J) = N(<\bar{e}>_\Gamma)$.

Отметим также, что могут существовать ошибки $\bar{e}$ веса 3, первая компонента синдрома которых $s_1 = 0$. Тогда норма $N(<\bar{e}>_\Gamma) = \infty$ и не является элементом поля Галуа $GF(2^m)$.

Группа G некоммутативна, имеет порядок mn и 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: $<\bar{e}>_G = \left\{<\bar{e}>_\Gamma, \varphi(<\bar{e}>_\Gamma), ..., \varphi^{\mu-1}(<\bar{e}>_\Gamma)\right\}$, где μ – наименьшее натуральное число с условием: $\varphi^\mu(<\bar{e}>_\Gamma) = <\bar{e}>_\Gamma$. При этом μ делит m или же $\mu = m$. При $\mu = m$ G-орбита $<\bar{e}>_G$ называется полной при условии, что Г-орбита $<\bar{e}>_\Gamma$ – полная.

Циклотомическая подстановка определена таким образом, что, если синдром $S(\bar{e}) = H \cdot \bar{e}^T = (s_1, s_2)^T$, а норма синдрома $N(S(\bar{e})) = s_2 / s_1^3 = N$, то $S(\varphi(\bar{e})) = (s_1^2, s_2^2)^T$, $N(S(\varphi(\bar{e}))) = N^2$ [2, 3]. Повторное применение подстановки φ к вектору-ошибке приведет к повторному возведению в квадрат ее синдрома и нормы синдрома. Таким образом, вся G-орбита $<\bar{e}>_G$ имеет синхронный образ в спектре норм этих Г-орбит в виде последовательности норм $\{N, N^2, ..., N^{2^{\mu-1}}\}$, где $N^{2^\mu} = N$.

Полиномиально-норменный метод коррекции ошибок в непримитивных БЧХ-кодах C_5^+

Отображение $f: x \to x^2$ в любом поле Галуа $GF(2^m)$ – автоморфизм Фробениуса этого поля. 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 элементом N. Полином $p_\mu(N, x) = p(x) = (x-N)(x-N^2)\cdot...\cdot(x-N^{2^{\mu-1}})$ является неприводимым над $GF(2)$ и единственным полиномом степени μ, содержащим все корни множества $N, N^2, ..., N^{2^{\mu-1}}$. Назовем полином $p_\mu(N, x)$ полиномиальным инвариантом G-орбиты [5, 6].

Если $N \in GF(2^m)^*$, что соответствует большинству случаев, то $p(N, x)$ несет основную информацию о своей G-орбите, в частности, степень $p(N, x)$ совпадает с количеством принадлежащих ей Г-орбит. Если $N = 0$, а G-орбита состоит из μ Г-орбит, то полагаем $p(N, x) = x^\mu$. Если же $N = \infty$, то полагаем $p(N, x) = 0$.

На этапе формирования поля $GF(2^m)$ для задания конкретного БЧХ-кода в работающей ИКС, с каждым элементом γ поля $GF(2^m)$ необходимо связать минимальный неприводимый над $GF(2)$ полином $p(\gamma, x)$, одним из корней которого является γ. Затем составляется список PG попарно различных полиномиальных инвариантов $p_i(x)$ всех G-орбит ошибок. С каждым $p_i(x)$ должен быть связан соответствующий i-й список p_iG попарно-различных G-орбит G_{ij}, $1 \le j \le \tau_i \le \tau$. По построению каждая G-орбита G_{ij}, $1 \le j \le \tau_i \le \tau$, представляет собой набор $G_{ij}\Gamma$ Г-орбит $<\bar{e}_{ij\chi}>_\Gamma$, $1 \le \chi \le \mu$, с образующими $\bar{e}_{ij\chi}$, $1 \le \chi \le \mu$, синдромы которых

$S(\bar{e}_{ij\chi}) = (s_1^{\chi}, s_2^{\chi})$ таковы, что $N(S(\bar{e}_{ij\chi})) = N_i^{\chi}$ – различные корни полинома $p_i(x)$. Через $p_iG\Gamma$ обозначаем набор всех Г-орбит, формирующих набор всех G-орбит списка p_iG. Через $p_iG\Gamma N^*$ обозначаем срез, часть тех Г-орбит $J \in p_iG\Gamma$, которые имеют норму $N(J) = N^*$ – один из корней полинома $p_i(x)$ [7].

Пусть ИКС приняла сообщение $\bar{x}$. Вычисляем синдром $S(\bar{x}) = (s_1, s_2)^T$, норму синдрома $N = N(S(\bar{x}))$ и определяем полиномиальный инвариант $p(N, x)$. Найденный полином $p(N, x)$ сравниваем с полиномами списка PG. Пусть $p(N, x) = p_{i_0}(x)$ для какого-то конкретного значения $i = i_0$. Из всего списка G-орбит корректируемых ошибок выделяем коротенький список $G_{i_0 j}$, $1 \le j \le \tau_{i_0} \le \tau$, с полиномиальным инвариантом $p_{i_0}(x)$ и список $p_{i_0}G_{i_0 j}\Gamma$ составляющих их Г-орбит $<\bar{e}_{i_0 j\chi}>_{\Gamma}$, $1 \le \chi \le \mu$.

В каждой G-орбите $G_{i_0 j} \in p_iG$, $1 \le j \le \tau_{i_0} \le \tau$, найдется единственная Г-орбита $<\bar{e}_{i_0 j\chi^*}>_{\Gamma}$, $1 \le \chi^* \le \tau_{i_0}$, с образующей $\bar{e}_{i_0 j\chi^*}$, синдром которой $S(\bar{e}_{i_0 j\chi^*}) = (s_1^{\chi^*}, s_2^{\chi^*})$ таков, что равен вычисленному значению N. Искомая вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$ принадлежит одной из Г-орбит списка $p_{i_0}G_{i_0 j}\Gamma N$.

При условии $s_1 \neq 0$ у синдрома $S(\bar{x}) = (s_1, s_2)^T$ следует вычислять разности $\deg(s_1) - \deg(s_1^{\chi^*})$ и делить их на $\tau = (2^m - 1)/n$. Результатом будет единственное целое значение $\chi^* = \chi_0^*$. Если же $s_1 = 0, \chi^* = \chi_0^*, (\deg(s_2) - \deg(s_2^{\chi_0^*}))/3\tau = l\lambda$, находим то единственное λ, для которого целым является число l. В обоих случаях существует единственное целое l из множества $[0, n)$, удовлетворяющее сравнению $\lambda \equiv l (\mathrm{mod}\, n)$. Вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$ находится по формуле: $\sigma^{\lambda}(\bar{e}_{ij^*\chi_0}) = \bar{e}$. Тогда $\bar{c} = \bar{x} + \bar{e}$ – истинное сообщение.

Заключение

Полиномиально-норменный метод сохранил вычисления, присущие норменным методам, а именно вычисление нормы синдрома, а также величины циклического сдвига образующей Г-орбиты до получения искомой вектор-ошибки. Главное отличие данного алгоритма от норменного – в сокращении однообразного поиска нужной нормы в длинном списке норм всех Г-орбит. Следовательно, переборные процедуры сокращаются.

Полиномиально-норменный метод позволяет достаточно равномерно разделить многообразие Г-орбит корректируемой совокупности на небольшие группы G-орбит по значениям их полиномиальных инвариантов. Исходный поиск начинается в полном списке этих полиномов. Дальнейшие поиски и расчеты ведутся внутри достаточно узкой группы Г-орбит с вычисленным полиномиальным инвариантом. Подобная усеченная процедура коррекции ошибок должна найти применение в высокоскоростных системах передачи информации.

TRUNCATED POLYNOMIAL-NORM METHOD OF ERROR CORRECTION IN BCH-CODES C_5

E.V. SEREDA, V.A. LIPNITSKI, V.K. KONOPELKO

Abstract. Polynomial invariants of *G*-orbits of errors, which create good prospects for decoding large error spectra, are considered. A detailed formulation of the truncated two-level polynomial-norm correction method for all errors that are permissible by a minimum distance, by non-primitive BCH-codes is given. The norm methods in the «syndrome-error» chain introduced an intermediate level of identification of the Γ-orbits to which the sought error belongs. This level reduced the search procedures by an order of magnitude. This method introduces another level of identification – the definition of a narrow group of *G*-orbits, where is the sought error vector.

Keywords: BCH-code, code automorphism, group of cyclic shifts of the vector's coordinates, cyclotomic substitution.

Список литературы

1. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Монография.: Едиториал УРСС, 2004.
2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения.: Издательский центр БГУ, 2007.
3. Липницкий В.А. Теория норм синдромов. Мн.: БГУИР, 2011.
4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
5. Липницкий В.А., Середа Е.В. // Докл. БГУИР. 2017. № 5 (107). С. 62–69.
6. Липницкий В.А., Середа Е.В. // Материалы XXII Белорусско-Российской научн.-практ. конф. «Комплексная защита информации». Полоцк, 16 – 19 мая 2017 г. С. 117–120.
7. Липницкий В.А., Середа Е.В. // Веснік Гродзенскага дзяржаўнага ўніверсітэта імя Янкі Купалы. Серыя 2. Матэматыка. Фізіка. Інфарматыка, вылічальная тэхніка і кіраванне. 2019 Т. 9. № 1 (2019). С. 118–127.