Геометрия и алгебра

Geometry and algebra

УДК 004.6

СВОЙСТВА И ПРИМЕНЕНИЕ ПОЛИНОМИАЛЬНЫХ ИНВАРИАНТОВ *G*-ОРБИТ ОШИБОК В РЕВЕРСИВНЫХ КОДАХ

А. В. КУШНЕРОВ[1], ***В. А. ЛИПНИЦКИЙ***[1, 2]

[1]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*
[2]*Военная академия Республики Беларусь, пр. Независимости, 220, 220057, г. Минск, Беларусь*

Впервые описана двухступенчатая процедура полиномиально-норменной коррекции ошибок реверсивными помехоустойчивыми кодами, которые задаются проверочной матрицей $H_R = \left(\beta^i, \beta^{-i}\right)^{\mathrm{T}}$, $0 \le i \le n-1$, $\beta = \alpha^{\frac{2^m-1}{n}}$, где α – примитивный элемент поля $GF\left(2^m\right)$; n – длина кода. Такой подход позволяет существенно ускорить процесс обнаружения и исправления ошибок. Также представлен алгоритм нахождения и исправления ошибок в зашумленном сообщении. На примере реверсивного кода C_R длиной 89 с минимальным расстоянием 7 показана процедура исправления конкретных ошибок.

Ключевые слова: линейные помехоустойчивые коды; минимальное расстояние кода; реверсивные коды; БЧХ-коды; синдром ошибок; норменный метод декодирования.

Образец цитирования:
Кушнеров АВ, Липницкий ВА. Свойства и применение полиномиальных инвариантов *G*-орбит ошибок в реверсивных кодах. *Журнал Белорусского государственного университета. Математика. Информатика.* 2018;3:21–28.

For citation:
Kushnerov AV, Lipnitski VA. Properties and applications of *G*-orbits polynomial invariants of errors in reverse codes. *Journal of the Belarusian State University. Mathematics and Informatics*. 2018;3:21–28. Russian.

Авторы:
Александр Викторович Кушнеров – аспирант кафедры дифференциальных уравнений и системного анализа механико-математического факультета. Научный руководитель – В. А. Липницкий.
Валерий Антонович Липницкий – доктор технических наук, профессор; заведующий кафедрой высшей математики[2], профессор кафедры дифференциальных уравнений и системного анализа механико-математического факультета[1].

Authors:
Alexander V. Kushnerov, postgraduate student at the department of differential equations and system analyses, faculty of mechanics and mathematics.
al.v.kushnerov@gmail.com
Valery A. Lipnitski, doctor of science (engineering), full professor; head of the department of higher mathematics[b] and professor at the department of differential equations and systems analysis, faculty of mechanics and mathematics[a].
valipnitski@yandex.by

Журнал Белорусского государственного университета. Математика. Информатика. 2018;3:21–28
Journal of the Belarusian State University. Mathematics and Informatics. 2018;3:21–28

PROPERTIES AND APPLICATIONS OF *G*-ORBITS POLYNOMIAL INVARIANTS OF ERRORS IN REVERSE CODES

A. V. KUSHNEROV [a], ***V. A. LIPNITSKI*** [a, b]

[a] *Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*
[b] *Military Academy of the Republic of Belarus, 220 Niezaliežnasci Avenue, Minsk 220057, Belarus*
Corresponding author: A. V. Kushnerov (al.v.kushnerov@gmail.com)

In this paper is described a two-step procedure for polynomial-norm error correction with reverse error correcting codes. Such codes of length n traditionally are defined by check matrix $H_R = \left(\beta^i, \beta^{-i}\right)^{\mathrm{T}}$, $0 \le i \le n-1$, $\beta = \alpha^{\frac{2^m-1}{n}}$ and α is primitive element of $GF\left(2^m\right)$. Also in paper you can find a description of error correction algorithm and an example based on reverse code of length 89.

Key words: error correcting codes; code minimal distance; reverse codes; BCH codes; norm method of error correction.

1. Введение

Реверсивные коды примыкают к семейству БЧХ-кодов с конструктивным расстоянием 5 [1]. С 1990-х гг. проводятся систематические исследования класса реверсивных кодов, сначала примитивных, лексикографически упорядоченных, а также циклических [2, гл. 6; 3; 4], а затем и непримитивных [5; 6]. Установлены некоторые их общие свойства, в диапазоне длин от 7 до 507 найдены случаи, когда они совпадают с кодами Хемминга, БЧХ-кодами, а также когда минимальное расстояние непримитивных реверсивных кодов превышает конструктивное.

В данной работе развиваются исследования, начатые в [6]. Для перспективных непримитивных реверсивных кодов C_R (минимальное расстояние которых $d > 5$), следуя [7], вводятся полиномиальные инварианты G-орбит ошибок относительно группы G циклических и циклотомических автоморфизмов кода C_R, разрабатываются полиномиально-норменные методы коррекции ошибок весом 1–3 этими кодами.

2. Необходимые сведения о реверсивных кодах

Двоичный реверсивный код C_R определен над полем Галуа $GF\left(2^m\right)$ из 2^m элементов ($m > 2$), имеет нечетную длину n, являющуюся делителем числа $2^m - 1$, а также размерность $k = n - 2m$. Здесь следует помнить о минимальности m: для всех натуральных значений $\mu < m$ величина $2^\mu - 1$ не делится на n. Код C_R однозначно задается своей проверочной матрицей

$$H_R = \begin{pmatrix} \beta^0 & \beta^1 & \beta^2 & \dots & \beta^{n-1} \\ \beta^0 & \beta^{-1} & \beta^{-2} & \dots & \beta^{1-n} \end{pmatrix}, \tag{1}$$

$0 \le i \le n-1$, $2m < n$, $\beta = \alpha^z$ для примитивного элемента α поля Галуа $GF\left(2^m\right)$, $z = \dfrac{2^m-1}{n}$. При $n = 2^m - 1$ величина $\beta = \alpha$, и код C_R называется примитивным. В противном случае код называется непримитивным [1; 2].

Коды с проверочной матрицей (1), как и БЧХ-коды с проверочной матрицей $H_{BCH} = \left(\beta^i, \beta^{3i}\right)^{\mathrm{T}}$, создавались в расчете на исправление двойных ошибок, и потому их называют кодами с конструктивным расстоянием 5. У примитивных БЧХ-кодов эти расчеты действительно подтвердились [1, гл. 7]. Что же касается примитивных реверсивных кодов, то при четных значениях m (тогда $n = 2^m - 1$ делится на 3) они имеют минимальное расстояние $d = 3$, а при нечетных m (тогда $n = 2^m - 1$ не делится на 3) действительно имеют $d = 5$ [1; 6].

3. Проблема коррекции трехкратных ошибок реверсивными кодами C_R^+

Потенциальная возможность обнаружения и исправления трехкратной ошибки в коде C_R с минимальным расстоянием 7 представляет собой реальную проблему, не решаемую стандартными синдромными методами. Действительно, рассмотрим w – сообщение, принятое в некоторой информационно-коммуникационной системе (ИКС) с двоичным кодом C_R над полем $GF\left(2^m\right)$ с проверочной

матрицей H_R. Тогда синдром зашумленного сообщения представим в виде $S(w) = H_R w^{\mathrm{T}} = (s_1, s_2)$, где s_1, s_2 – элементы поля $GF(2^m)$; $w = c + e$ для передаваемого кодового слова c и вектора-ошибки e. По фундаментальному свойству проверочной матрицы кода $H_R c^{\mathrm{T}} = 0$, поэтому $S(w) = S(e)$, т. е. зависит только от вектора-ошибки e. Отметим также, что все синдромы ошибок корректируемой совокупности попарно различны. Названные обстоятельства являются основой всех синдромных методов коррекции ошибок. Для определения трех ошибочных позиций вектора-ошибки весом 3 необходимо отыскать решение системы из двух уравнений

$$\begin{cases} x + y + z = s_1, \\ x^{-1} + y^{-1} + z^{-1} = s_2 \end{cases}$$

относительно переменных x, y, z. Очевидно, что это решение не может быть однозначным в силу неопределенности системы.

Альтернативным методом коррекции таких ошибок является норменный.

4. Основы теории норм синдромов для непримитивных реверсивных кодов

В указанной теории базовым является понятие нормы синдрома. Пусть ИКС, функционирующая на основе двоичного реверсивного кода C_R длиной n над полем $GF(2^m)$, приняла сообщение w с синдромом $S(w) = H_R w^{\mathrm{T}} = (s_1, s_2) \neq 0$. Согласно [2] нормой синдрома $S(w)$ в коде C_R называется элемент поля $GF(2^m)$, который вычисляется через компоненты синдрома по формуле $N(S(w)) = s_1 s_2$.

Главная задача декодирования сообщения – найти вектор ошибки, приобретенной в процессе его передачи. Теория автоморфизмов кодов позволяет разбить множество исправляемых ошибок на непересекающиеся классы эквивалентности, называемые Г-орбитами. Циклические коды выделяются из класса линейных тем, что σ – оператор циклического сдвига координат векторов вправо на одну позицию по циклу – является автоморфизмом этих кодов. Коды C_R с проверочной матрицей (1) относятся к классу циклических [1–4]. Через Г обозначим циклическую подгруппу, порожденную автоморфизмом σ в группе $\mathrm{Aut}(C_R)$. Это коммутативная группа порядка n. Два вектора e_1, e_2 из пространства векторов-ошибок E_n называют эквивалентными, если выполнено соотношение $e_1 = \sigma^k(e_2)$. Это отношение эквивалентности разбивает все пространство возможных ошибок V_n над полем $\mathbb{Z}/2\mathbb{Z}$ на непересекающиеся классы, называемые Г-орбитами (детали в [2–4]).

Поскольку длина n у кодов C_R нечетна и при условии $d > 5$ не делится на 3 (см. разд. 2), то все ошибки весом 1–3 в этих кодах делятся на полные Г-орбиты, содержащие по n векторов-ошибок в каждой. Каждая Г-орбита J таких ошибок однозначно определяется любым своим представителем e, циклическим сдвигом координат которого могут быть получены все n ошибок Г-орбиты:

$$J = \left\{e, \sigma(e), \ldots, \sigma^{n-1}(e)\right\} = < e >_{\Gamma} = < e >.$$

Ясно, что $\sigma^n(e) = e$.

Как известно [2; 3], если $S(w) = (s_1, s_2)$, то

$$S(\sigma(w)) = (\beta s_1, \beta^{-1} s_2). \tag{2}$$

Благодаря свойству, выражаемому формулой (2), спектр синдромов, т. е. множество всех различных синдромов векторов-ошибок каждой Г-орбиты J, равномощен самой Г-орбите и взаимно однозначно соответствует ее циклической структуре: $\sigma^k(e) = e^*$ тогда и только тогда, когда показатели компонент синдромов $S(e) = (s_1, s_2)$ и $S(e^*) = (s_1^*, s_2^*)$ связаны равенствами

$$\deg s_1^* = \deg s_1 + kz, \ \deg s_2^* = \deg s_2 - kz. \tag{3}$$

Другими словами, два вектора-ошибки принадлежат одной Г-орбите тогда и только тогда, когда разность показателей одноименных компонент их синдромов делится на z.

Таким образом, вектор-ошибка по синдромам с помощью формул (3) однозначно определяется внутри каждой Г-орбиты. Более того, каждый вектор-ошибка принадлежит лишь одной Г-орбите, следовательно, разность показателей синдромов будет делиться на z в единственном случае, когда эти векторы лежат в одной Г-орбите.

Из формулы (2) следует, что норма синдрома $N\left(S\left(w\right)\right) = N\left(S\left(\sigma\left(w\right)\right)\right) = N$ постоянна на всех векторах каждой отдельно взятой Г-орбиты, и потому называется нормой самой Г-орбиты. Как у примитивных, так и у непримитивных кодов C_R нормы Г-орбит ошибок весом 1, 2 попарно различны и отличны от 0, что легко проверяется повторением доказательства теоремы 4.8 из [3]. Что же касается норм Г-орбит векторов-ошибок весом 3 у непримитивных кодов C_R^+, то здесь возможны отдельные совпадения. Не доказано (в отличие от двойных ошибок) отсутствие Г-орбит тройных ошибок с нормой, равной 1; среди них вполне могут найтись Г-орбиты, с нормой 0 или совпадающей с нормой какой-либо Г-орбиты двойных ошибок, с совпадающими между собой нормами.

Во-первых, число Г-орбит декодируемой совокупности K векторов-ошибок для реверсивного кода C_R длиной n с минимальным расстоянием 7 равно $\frac{1}{n}\left(C_n^1 + C_n^2 + C_n^3\right) = \frac{n^2+5}{6}$, что вполне может оказаться бóльшим 2^m – количества возможных значений норм синдромов. У всех перечисленных выше кодов C_R^+ эта величина не превосходит 2^m. Во-вторых, имеется более глубокая, внутренняя причина возможности таких совпадений. У примитивного кода C_R спектр синдромов $S\left(J\right)$ каждой Г-орбиты J в определенном смысле полный. А именно, если для вектора $\overline{e} \in J$ синдром $S\left(\overline{e}\right) = \left(s_1, s_2\right)$ таков, что $s_1 \neq 0$, то первые компоненты спектра $S\left(J\right)$ составляют в силу формулы (2) всю мультипликативную группу $GF\left(2^m\right)^*$ порядка $2^m - 1$. Аналогичная ситуация и для второй компоненты синдрома, если $s_2 \neq 0$. У непримитивного же кода C_R при $s_1 \neq 0$ первые компоненты спектра $S\left(J\right)$ составляют в силу формулы (2) смежный класс в группе $GF\left(2^m\right)^*$, порожденный элементом s_1 по циклической подгруппе $<\beta>$ порядка $n = \frac{2^m - 1}{z}$. Вполне может найтись вектор ошибок $\overline{e}^*$ с синдромом $S\left(\overline{e}^*\right) = \left(\alpha^i s_1, \alpha^{-i} s_2\right)$ для некоторого целого i, $1 \le i < z$. Несложно видеть, что нормы Г-орбит J и $<\overline{e}^*>_\Gamma$ совпадают, а спектры синдромов не пересекаются.

Таким образом, у непримитивных реверсивных кодов C_R может существовать до z попарно различных Г-орбит с одинаковыми нормами.

Пример 1. Реверсивный код C_R^+ длиной 89 определен над полем $GF\left(2^{11}\right)$. Он способен декодировать 117 569 векторов-ошибок весом 1–3, которые группируются в 1321 Г-орбиту: 1 Г-орбита ошибок весом 1 и нормой 1, 44 полные Г-орбиты ошибок весом 2 с попарно различными нормами, отличными от 0 и 1, и 1276 полных Г-орбит тройных ошибок. Среди последних 33 Г-орбиты имеют уникальные нормы, 924 Г-орбиты – по 2 одинаковые нормы, 33 Г-орбиты – по 3 одинаковые нормы, 244 Г-орбиты – по 4 одинаковые нормы, а также 22 Г-орбиты тройных ошибок имеют одинаковые нормы с 11 Г-орбитами двойных ошибок. Таким образом, 1321 Г-орбита распределяются на 614 групп по значениям своих норм, что по-прежнему составляет достаточно внушительное количество.

5. Норменный метод коррекции ошибок реверсивными кодами C_R^+

Метод заключается в следующем. Составляют список образующих e_i всех $\frac{n^2+5}{6}$ Г-орбит векторов-ошибок совокупности K, синдромов образующих $S\left(e_i\right)$ и их норм синдромов $N_i = N\left(S\left(e_i\right)\right)$. Естественно, Г-орбиты сортируют в группы с одинаковыми нормами. Для принятого сообщения w декодер ИКС в обязательном порядке вычисляет его синдром $S\left(w\right)$. Если $S\left(w\right) \neq 0$, находят $N = N\left(S\left(w\right)\right)$. Эту величину сравнивают со списком попарно различных норм N_i. Пусть $N = N_k$. Синдром $S\left(w\right) = \left(s_1, s_2\right)$ сравнивают с синдромами образующих Г-орбит с нормой N_k. В силу формул (3) найдется только одна орбита $<e_k>$ с образующей e_k и синдромом $S\left(e_k\right) = \left(s_1^k, s_2^k\right)$ такая, что разность показателей $\deg\left(s_1\right) - \deg\left(s_1^k\right)$ нацело делится на z. Если соответствующее частное равно τ, то искомый вектор-ошибка e в сообщении w вычисляется по формуле $e = \sigma^{\tau(\mathrm{mod}\, n)}\left(e_k\right)$.

Норменный метод достаточно успешно решает задачу нахождения вектора-ошибки. Однако число Г-орбит декодируемой совокупности для реверсивного кода C_R длиной n с минимальным расстоянием 7,

равное $\frac{n^2+5}{6}$, будет быстро увеличиваться с ростом n, что, естественно, затрудняет задачи эффективного поиска нужной информации в быстро растущих объемах хранения, замедляет работу декодера.

Определенного ускорения процесса декодирования можно добиться норменным методом с использованием полиномиальных инвариантов [7].

6. *G*-орбиты ошибок и их полиномиальные инварианты

Определим на множестве $T = \{1, 2, \ldots, n\}$, где n – нечетно, преобразование φ по правилу

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

Для нечетных n оператор φ является взаимно однозначным на множестве T. Применение данного оператора к вектору-ошибке подразумевает перестановку его координат по правилу φ. Ее называют циклотомической перестановкой на пространстве ошибок E_n и обычно по-прежнему обозначают через φ. Повторяя почти дословно доказательство предложения 3.17 из [3], можно убедиться, что она является автоморфизмом любого циклического кода C_R с проверочной матрицей (1), причем порядка m. Автоморфизмы σ и φ образуют некоммутативную группу G порядка mn [1; 2].

Два вектора $\bar{f}$, $\bar{g}$ из пространства ошибок E_n называются G-эквивалентными, если найдется такая подстановка $\tau = \varphi^i\sigma^j$, что $\bar{g} = \tau(\bar{f})$. Совокупность всех попарно G-эквивалентных векторов из пространства E_n называют G-орбитой. Для реверсивного кода C_R, определенного над полем $GF(2^m)$, любая G-орбита J_G имеет четкую структуру и состоит из всех векторов Г-орбит, определяемых следующим соотношением:

$$J_G = \{<\bar{e}>, \varphi<\bar{e}>, \varphi^2<\bar{e}>, \ldots, \varphi^{\mu-1}<\bar{e}>\}, \tag{4}$$

где $<\bar{e}>$ – Г-орбита, порожденная вектором-ошибкой e из пространства ошибок E_n; $\mu = m$ или μ делит m. Формула (4) определяет всю G-орбиту одним вектором-ошибкой, который называют ее образующим, и потому используют обозначение $J_G = <e>_G$ [2].

Циклотомическая подстановка замечательна следующими свойствами: если $S(\bar{e}) = (s_1, s_2)$, то

$$S(\varphi(\bar{e})) = (s_1^2, s_2^2),\ \left(N(S(\bar{e}))\right)^2 = N(S(\varphi(\bar{e}))). \tag{5}$$

Пусть $N_1 = N(<\bar{e}>)$ – норма Г-орбиты $<e>$, тогда нормы Г-орбит G-орбиты $<\bar{e}>_G$ имеют спектр $N(<e>_G) = \{N_1, N_1^2, N_1^4, \ldots, N_1^{2^{\mu-1}}\}$ в силу формул (4), (5). Возведение нормы в квадрат соответствует применению автоморфизма Фробениуса к элементу N_1 поля $GF(2^m)$. Построенный список норм Г-орбит, составляющих G-орбиту $<e>_G$, есть множество всех сопряженных друг другу под действием группы Галуа элементов поля. Такие элементы составляют полный список корней неприводимого полинома над минимальным подполем $GF(2)$ [5]. Этот полином называют минимальным полиномом элемента N_1 (а также любого элемента поля, сопряженного с ним) и обозначают $\mathrm{Irr}(N_1, x)$. Из теоремы Безу о корнях полиномов следует, что не существует иного неприводимого полинома, содержащего хотя бы один из корней полинома $\mathrm{Irr}(N_1, x)$. Отсюда получаем следующее определение.

Определение. Единственный неприводимый полином

$$\mathrm{Irr}(N_1, x) = (x - N_1)(x - N_1^2)\cdots(x - N_1^{2^{\mu-1}}), \tag{6}$$

множество корней которого совпадает с множеством норм в коде C_R Г-орбит, составляющих данную G-орбиту, называется полиномиальным инвариантом этой G-орбиты и обозначается $p(<e>_G, x)$ или $p(N_1, x)$ [6].

Важно отметить, что степень полинома $p(<e>_G, x)$ совпадает с количеством Г-орбит в соответствующей G-орбите. В частности, для простых значений m степень этого полинома равна 1 или, что чаще всего, m.

Конечно, $p(<e>_G, x)$ должен храниться не в форме (6), а в стандартной полиномиальной форме $x^\mu + c_{\mu-1}x^{\mu-1} + \ldots + c_1x + c_0$ с коэффициентами из $GF(2)$ или вовсе в виде двоичного вектора

$(1, c_{\mu-1}, \ldots, c_1, c_0)$. Для этого следует раскрыть скобки в формуле (6) и привести подобные. Полученные в результате коэффициенты c_i, $0 \le i < \mu$, будучи симметрическими полиномами от корней полинома в силу теоремы Виета, должны быть инвариантными относительно автоморфизма Фробениуса поля Галуа $GF(2^m)$ и, следовательно, принадлежать его минимальному подполю $GF(2)$.

Каждый элемент γ поля $GF(2^m)$ является алгебраическим над подполем $GF(2)$, т. е. есть корень некоторого единственного неприводимого полинома $\mathrm{Irr}(\gamma, x) \in \mathbb{Z}/2\mathbb{Z}[x]$. Если γ не принадлежит никакому подполю поля $GF(2^m)$, то $\deg \mathrm{Irr}(\gamma, x) = m$, в противном случае $\deg \mathrm{Irr}(\gamma, x) = \mu$ – делитель числа m (детали в [8] или [9]). Чтобы конкретная работа с полиномиальными инвариантами не создавала проблем со временем, не замедляла работу декодера, следует заранее, при построении конечного поля $GF(2^m)$, для каждого элемента γ найти его полином $\mathrm{Irr}(\gamma, x) \in GF(2)[x]$ и хранить эту пару в памяти в единой связке: $\gamma \leftrightarrow \mathrm{Irr}(\gamma, x)$.

В непримитивных кодах, как и в случае Г-орбит, один полиномиальный инвариант могут иметь до z различных G-орбит. Одиночные ошибки образуют одну G-орбиту из одной Г-орбиты с полиномиальным инвариантом $x+1$. Двойные ошибки делятся, как правило, на полные G-орбиты по m Г-орбит в каждой, но если число Г-орбит $\frac{1}{n}C_n^2 = \frac{n-1}{2}$ не делится на m, то среди G-орбит обязательно найдутся неполные, но содержащие более одной Г-орбиты. У G-орбит тройных ошибок трудно указать какие-либо общие закономерности.

Пример 2. Над полем $GF(2)$ имеется 186 различных неприводимых полиномов 11-й степени, по которым распределяются в качестве корней 2046 элементов поля $GF(2^{11})$ (два оставшихся принадлежат подполю $GF(2)$). В развитие примера 1 заметим, что в коде C_R^+ длиной 89 векторы двойных ошибок образуют 4 полные G-орбиты с уникальными полиномиальными инвариантами:

Полином	Образующая	Синдром образующей	Норма образующей
$1+x^2+x^3+x^4+x^5+x^6+x^8+x^9+x^{11}$	(1, 4)	$(\alpha^{1534}, \alpha^{1465})$	α^{952}
$1+x^3+x^5+x^6+x^7+x^{10}+x^{11}$	(1, 2)	$(\alpha^{527}, \alpha^{504})$	α^{1031}
$1+x^2+x^4+x^5+x^6+x^7+x^8+x^{10}+x^{11}$	(1, 6)	$(\alpha^{397}, \alpha^{282})$	α^{679}
$1+x^2+x^3+x^4+x^6+x^7+x^9+x^{10}+x^{11}$	(1, 14)	$(\alpha^{1041}, \alpha^{742})$	α^{1783}

В свою очередь, 1276 Г-орбит тройных ошибок делятся на 116 полных G-орбит, которым соответствуют 53 полиномиальных инварианта. Из них 3 инварианта соответствуют в точности одной G-орбите, 43 полинома – сразу двум G-орбитам, 1 полином – трем G-орбитам и 6 – четырем. Отметим также, что два инвариантных полинома для тройных ошибок совпадают с таковым для двойных.

7. Двухступенчатая процедура полиномиально-норменной коррекции ошибок реверсивными кодами C_R^+

Для работы декодера на основе полиномиальных инвариантов необходимо хранить в памяти ряд списков: $PG = \{p(<e_1>_G, x), p(<e_2>_G, x), \ldots, p(<e_s>_G, x)\}$ – список попарно различных полиномиальных инвариантов всех G-орбит векторов-ошибок весом 2 и 3; для каждого целого i ($1 \le i \le s$) – список $N_i\Gamma$ из μ ($\mu = m$ или μ – делитель m) попарно различных норм N_{ij} ($1 \le j \le \mu$) Г-орбит с полиномиальным инвариантом $p(<e_i>_G, x)$; для каждой нормы N_{ij} – список $N_{ij}OS = \{<\bar{e}_{ij1}>, S(\bar{e}_{ij1}); <\bar{e}_{ij2}>, S(\bar{e}_{ij2}); \ldots; <\bar{e}_{ij\varsigma}>, S(\bar{e}_{ij\varsigma})\}$ образующих Г-орбит и синдромов образующих с данной нормой N_{ij}.

Представим алгоритм исправления ошибки кодом C_R с проверочной матрицей (1). Пусть принято некоторое сообщение l. Вычисляем его синдром ошибки $Hl^{\mathrm{T}} = S(l)$. Если $S(l) = 0$, то сообщение не содержит ошибок. Алгоритм заканчивает работу. В противном случае переходим на выполнение следующих ниже шагов.

1. Пусть $S(l) \neq 0$. Тогда находим норму синдрома $S(l) = (s_1, s_2)$ по формуле $N_0 = N(S(l)) = s_1 s_2$. Если $N_0 = 1$ и $s_1 = s_2^{-1} = \beta^{t-1}$, то ошибка e_l однократная на t-й позиции и можно переходить к шагу 6.

2. Иначе по отмеченной выше связке элементов поля с их неприводимыми полиномами $\gamma \leftrightarrow \mathrm{Irr}(\gamma, x)$ определяем полиномиальный инвариант $p(N_0, x)$ и сравниваем его со списком PG. Пусть $p(N_0, x) = p(< e_i >_G, x)$ для некоторого целого i ($1 \le i \le s$). Это означает, что норма N_0 принадлежит короткому списку $N_i\Gamma$.

3. Сравниваем N_0 с этим списком, находим $N_0 = N_{ij_0} \in N_i\Gamma$. Следовательно, искомая вектор-ошибка находится среди ς Γ-орбит с нормой N_{ij_0}.

4. Для каждого целого k ($1 \le k \le \varsigma$) и вектора $\overline{e}_{ij_0k}$ из списка $N_{ij_0}OS = \left\{< \overline{e}_{ij_0 1} >, S(\overline{e}_{ij_0 1}) = (s_1^1, s_2^1); < \overline{e}_{ij2} >, S(\overline{e}_{ij_0 2}) = (s_1^2, s_2^2); \ldots; < \overline{e}_{ij_0\varsigma} >, S(\overline{e}_{ij_0\varsigma}) = (s_1^\varsigma, s_2^\varsigma)\right\}$ вычисляем величину $\tau_k = \dfrac{\deg(s_1) - \deg(s_1^k)}{z}$, если $s_1 \neq 0$, и величину $\tau'_k = \dfrac{\deg(s_2^k) - \deg(s_2)}{z}$, если $s_1 = 0$. Фиксируем то единственное, в силу сказанного выше, значение $k = \lambda$, для которого τ_λ или τ'_λ является целым числом.

5. Вычисляем искомую вектор-ошибку $e_l = \sigma^{\tau(\mathrm{mod}\, n)}(\overline{e}_{ij_0\lambda})$ в сообщении l.

6. Получаем верное сообщение $c = l + e_l$.

Пример 3. Работу декодера проследим на примере реверсивного кода длиной 89 над полем $GF(2^{11})$. Декодер данного кода содержит в себе, помимо проверочной матрицы, список PG из 57 полиномов и список SNO Γ-орбит, отсортированный по G-орбитам. Всего пространство ошибок содержит 121 G-орбиту: 4 орбиты двукратных ошибок, 116 – ошибок весом 3, а также 1 орбиту однократных ошибок.

Пусть ИКС приняла следующее сообщение:

$l = (01110111101110010010000000000000000000000000000011000000000000000000000000000100000000010010)$.

Находим синдром ошибки для сообщения $S(l) = Hl = (\alpha^{1687}, \alpha^{1835})$.

1. Вычисляем норму синдрома $N_0 = s_1 s_2 = \alpha^{1475}$. По связке элемент поля – полином определяем $p(N_0, x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{11}$.

2. В списке PG находим полином, равный найденному $p(N_0, x)$, $p(x) = 1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{11}$.

Сразу получаем и список норм, соответствующий инвариантному полиному: $N_i\Gamma = \{\alpha^{952}, \alpha^{476}, \alpha^{238}, \alpha^{119}, \alpha^{1083}, \alpha^{1565}, \alpha^{1806}, \alpha^{903}, \alpha^{1475}, \alpha^{1761}, \alpha^{1904}\}$.

3. В списке $N_i\Gamma$ легко отыщем нашу норму, а значит, искомая ошибка находится среди элементов Γ-орбит с нормой N_0. Переходим к списку $N_{ij_0}OS = \left\{< (1, 25) >, \{\alpha^{2037}, \alpha^{1485}\}; < (1, 2, 28) >, \{\alpha^{606}, \alpha^{869}\}; < (1, 27, 28) >, \{\alpha^{1490}, \alpha^{2032}\}\right\}$. Отметим, что данной норме соответствуют Γ-орбиты двойных и тройных ошибок одновременно.

4. Находим $\tau_k = \dfrac{\deg(s_1) - \deg(s_1^k)}{z}$, где $z = \dfrac{2^{11} - 1}{89} = 23$. Таким образом, имеем

$$\tau_1 = \frac{1687 - 2037}{23} = \frac{-350}{23},\ \tau_2 = \frac{1687 - 606}{23} = 47,\ \tau_3 = \frac{1687 - 1490}{23} = \frac{197}{23}.$$

Фиксируем $\tau_2 = 47$, так как оно является целым числом.

5. Вычисляем искомый вектор-ошибку $e_l = \sigma^{47(\mathrm{mod}\, n)}(1, 2, 28) = (48, 49, 75)$. Выпишем вектор e_l в полной форме:

$e_l = (00000000000000000000000000000000000000000000000011000000000000000000000000000100000000000000)$.

6. Получаем верное сообщение $c = l + e_l$:

$c = (01110111101110010010000000000000000000000000000000000000000000000000000000000000000010010)$.

8. Заключение

В работе развита теория полиномиальных инвариантов *G*-орбит ошибок на класс реверсивных кодов, как правило непримитивных, корректирующие возможности которых выходят за рамки конструктивных возможностей. Свойства этих инвариантов позволяют предложить усеченный двухступенчатый полиномиально-норменный метод декодирования ошибок реверсивными кодами. Классические синдромные методы коррекции ошибок так или иначе преодолевают полный перебор списка исправляемых ошибок, что неизбежно приводит к «проблеме селектора». Норменные методы на порядок сокращают этот перебор, ибо ему подвергаются нормы Г-орбит декодируемых ошибок (их инварианты). Когда идентифицирована Г-орбита, содержащая искомую ошибку, дальнейший ее поиск осуществляется детерминированными вычислениями с синдромами. Полиномиально-норменный метод выполняет еще более усеченный поиск в списке полиномиальных инвариантов *G*-орбит ошибок корректируемой совокупности с последующим минимальным поиском нужной Г-орбиты в узком списке *G*-орбит с найденным полиномиальным инвариантом. Предлагаемый метод коррекции ошибок, несомненно, должен найти свои приложения в практике.

Библиографические ссылки

1. Мак-Вильямс ФДж, Слоэн Н. *Теория кодов, исправляющих ошибки.* Москва: Связь; 1979.
2. Конопелько ВК, Липницкий ВА. *Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов.* Москва: Едиториал УРСС; 2004.
3. Конопелько ВК, Липницкий ВА. *Норменное декодирование помехоустойчивых кодов и алгебраические уравнения.* Минск: Издательский центр БГУ; 2007.
4. Липницкий ВА. *Теория норм синдромов.* Минск: БГУИР; 2010.
5. Липницкий ВА, Кушнеров АВ. Некоторые свойства реверсивных помехоустойчивых кодов. В: *Технологии информатизации и управления. Выпуск 3. В 2 книгах. Книга 1.* Кадан АМ, Свирский ЕА, редакторы. Минск: РИВШ; 2017. с. 47–54.
6. Липницкий ВА, Кушнеров АВ. Свойства и декодирование реверсивных кодов с конструктивным расстоянием 5. *Веснік Магілёўскага дзяржаўнага ўніверсітэта імя А. А. Куляшова. Серыя В.* 2016;2:30–44.
7. Липницкий ВА, Середа ЕВ. Полиномиальные инварианты *G*-орбит ошибок БЧХ-кодов и их применение. *Доклады БГУИР.* 2017;5(107):62–69.
8. Липницкий ВА. *Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа.* Минск: БГУИР; 2005. 88 с.
9. Лиддл Р, Нидеррайтер Г. *Конечные поля.* Москва: Мир; 1988.

References

1. MacWilliams FJ, Sloane N. *Teoriya kodov, ispravlyayushchikh oshibki* [The Theory of Error-Correcting Codes]. Moscow: Svyaz; 1979. Russian.
2. Konopel'ko VK, Lipnitskii VA. *Teoriya norm sindromov i perestanovochnoe dekodirovanie pomekhoustoichivykh kodov* [Theory of syndrome norms and permutation decoding of error-correcting codes]. Moscow: Editorial URSS; 2004. Russian.
3. Konopel'ko VK, Lipnitskii VA. *Normennoe dekodirovanie pomekhoustoichivykh kodov i algebraicheskie uravneniya* [Norm decoding of error-correcting codes and algebraic equations]. Minsk: Izdatel'skii tsentr BGU; 2007. Russian.
4. Lipnitskii VA. *Teoriya norm sindromov* [Theory of syndrome norms]. Minsk: BGUIR; 2010. Russian.
5. Lipnitskii VA, Kushnerov AV. [Some properties of reverse error-correcting codes]. In: *Tekhnologii informatizatsii i upravleniya. Vypusk 3. V 2 knigakh. Kniga 1.* Kadan AM, Svirskii EA, editors. Minsk: RIVSh; 2017. p. 47–54. Russian.
6. Lipnitskii VA, Kushnerov AV. [Properties and decoding of reverse codes with a code distance of 5]. *Vesnik Magilewskaga dzjarzhawnaga wniversitjeta imja A. A. Kuljashova. Seryja V.* 2016;2:30–44. Russian.
7. Lipnitskii VA, Sereda EV. [Polynomial invariants of *G*-orbits of BCH-code errors and their application]. *Doklady BGUIR.* 2017; 5(107):62–69. Russian.
8. Lipnitskii VA. *Sovremennaya prikladnaya algebra. Matematicheskie osnovy zashchity informatsii ot pomekh i nesanktsionirovannogo dostupa* [Modern applied algebra. Mathematical foundations of information protection from interference and unauthorized access]. Minsk: BGUIR; 2005. 88 p. Russian.
9. Liddle R, Niederreiter G. *Introduction to finite fields and their applications.* New York: Cambridge University Press; 1986. Russian edition: *Konechnye polya.* Moscow: Mir; 1988.

Статья поступила в редколлегию 23.03.2018.
Received by editorial board 23.03.2018.