КОРРЕКТИРУЮЩИЕ СВОЙСТВА НЕПРИМИТИВНЫХ БЧХ-КОДОВ

Е. К. Аль-Хайдар, В. А. Липницкий

Современные цифровые системы передачи и хранения информации в большинстве своем опираются на линейные коды для борьбы с помехами и шумами. К числу наиболее популярных относятся коды Боуза-Чоудхури-Хоквингема (БЧХ-коды), открытые в начале 60-ых годов.

Для задания БЧХ-кода C следует зафиксировать следующие параметры: длину n кода C, поле $GF(q^m)$ – наименьшее конечное поле из q^m элементов такое, что длина n является делителем числа $q^m - 1$ (непримитивный БЧХ-код) или совпадать с ним (примитивный БЧХ-код), неприводимый полином над минимальным полем Галуа $GF(q)$–если $p(x)$ примитивен, то и БЧХ-код примитивен, если $p(x)$ непримитивен, то и БЧХ-код непримитивен. БЧХ-код составляет ядро своей проверочной матрицы $H = [\beta^{bi}, \beta^{(b+1)i}, \ldots, \beta^{(b+\delta-2)i}]^T$ [1], $0 \le i \le n$, β – корень неприводимого полинома $p(x)$, $b > 0$, не делящееся на n, δ – конструктивное расстояние.

Наиболее изучены и применимы на практике двоичные ($q = 2$) примитивные БЧХ-коды с проверочной матрицей

$$H = [\beta^{i}, \beta^{3i}, \ldots, \beta^{(2t-1)i}]^T, \qquad (1)$$

где $\delta = 2t + 1$, $t > 0$, имеющие при данном n и наибольшую размерность $k = n - rangH$ кода C. Однако остались практически не изученными непримитивные БЧХ-коды, чему и посвящена данная работа. К числу важнейших параметров кода относится d – минимальное или кодовое расстояние. У примитивных БЧХ-кодов обычно $d = \delta$. Как показывают вычисления (*табл.* 1), у непримитивных БЧХ-кодов ситуация более разнообразная.

Таблица 1

n	m(min)	2^m–1	t	k	δ	d
11	10	1023=3·11·31	1	1	3	11
13	12	4095=3·3·5·7·13	1	1	3	13
17	8	255=3·5·17	1	9	3	5
23	11	2047=23·89	1	12	3	7
			2	1	5	7
65	12	4095=3·3·5·7·13	1	53	3	5

Главное назначение линейных кодов – синхронное исправление ошибок, которые могут возникать в процессе передачи кодовых слов. Общепринятыми синдромные методы коррекции ошибок в кодовых словах.

Синдром – это вектор, свидетельствующий о наличии ошибок в принятом сообщении, вычисляемый по формуле:

$$S = H \cdot \bar{x}^T = H \cdot \bar{e}^T = S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1}) \in P_{n-k}, \qquad (2)$$

где $\bar{e} \in E_n$ – вектор-ошибка, наложенная на сообщение $\bar{c}$, $\bar{x} = \bar{c} + \bar{e}$ – принятое слово. Декодирующее устройство устанавливает взаимнооднозначное соответствие между синдромами и соответствующими ошибками. Однако при большом количестве ошибок и синдромов аппаратурно установить взаимнооднозначное соответствие между ними в реальном устройстве цифровой системы связи затруднительно. На помощь в такой ситуации приходит теория норм синдромов. Она предлагает разбиение ошибок на блоки или группы, по какому либо признаку, например на Г-орбиты [2].

Широко известно, что к автоморфизмам многих линейных кодов принадлежит группа циклических сдвигов $\Gamma = <\sigma> = \{\sigma, \sigma^2, \ldots, \sigma^n = e\}$, действие которых на произвольный вектор ошибок $\bar{e} = (e_1, e_2, \ldots, e_n)$ пространства $E_n = P_n$ осуществляется кратным применением следующего правила: $\sigma(e_1, e_2, \ldots, e_n) = (e_n, e_1, e_2, \ldots, e_{n-1})$. Совокупность же всех попарно различных векторов-ошибок $\sigma^k(\bar{e})$, $0 \le k < n$, называется Г-орбитой вектора-ошибки $\bar{e}$ в пространстве ошибок E_n и обозначается через $<\bar{e}>$. Векторы каждой Г-орбиты имеют тесную взаимосвязь – каждый из них можно получить циклическими сдвигами какого-нибудь фиксированного вектора Г-орбиты.

Норма синдрома – векторная характеристика векторов-ошибок, вычисляемая через координаты синдрома. Это вектор $N(S(\bar{e})) = (N_{12}, N_{13}, \ldots, N_{1(\delta-1)}, N_{23}, \ldots, N_{(\delta-2)(\delta-1)})$ с $C^2_{\delta-1}$ координатами N_{ij}, $1 \le i < j \le \delta - 1$, которые вычисляются по формулам [2]:

$$N_{ij} = \infty \text{ , если } s_j \ne 0,\ s_i = 0;\ N_{ij} = -(\text{не сущ.}), \text{ если } s_i = s_j = 0, \qquad (3)$$

$$N_{ij} = s_j^{(b+i-1)/h_{ij}} / s_i^{(b+j-1)/h_{ij}} \text{ , если } s_i \ne 0, \qquad (4).$$

Основное и наиболее важное свойство норм синдромов отражает

Теорема 1. Для всякого вектора ошибок $\bar{e}$ и его синдрома $S(\bar{e})$ в БЧХ-коде C справедливо равенство $N(S(\sigma(\bar{e}))) = N(S(\bar{e}))$ [2].

Теорема 1 показывает, что норма синдрома одинакова для всех векторов каждой Г-орбиты, то есть является инвариантом, индивидуальной характеристикой всякой Г-орбиты векторов-ошибок. Очевидно, Г-орбиты ошибок с различными нормами имеют непересекающиеся спектры синдромов. Установлено, что у примитивных БЧХ-кодов класс K_t Г-орбит векторов-ошибок весом ω, $1 \le \omega \le t$, имеет попарно различные нормы. Специфика непримитивных БЧХ-кодов в том, что здесь класс K_t может иметь до $c = (2^m - 1)/n$ различных Г-орбит с одинаковым значением нормы $\overline{N}$, но с попарно различными спектрами синдромов. А возможный спектр корректируемых непримитивным БЧХ-кодом ошибок очерчивает

Теорема 2. Пусть K – совокупность Г-орбит векторов-ошибок в БЧХ-коде C с полными и попарно непересекающимися спектрами синдромов. Если известно, что в принятом сообщении произошла ошибка из совокупности K, то код C ее однозначно декодирует [2].

Теорема 1, 2 составляют основу норменного перестановочного метода коррекции ошибок. Для его реализации следует составить таблицу образующих $\overline{e}_i$ Г-орбит $<\overline{e}_i>$ векторов ошибок декодируемой совокупности K, их синдромов $S(\overline{e}_i)$ и норм синдромов $\overline{N}_i = \overline{N}(S(\overline{e}_i))$.

Алгоритм норменного декодирования можно разбить на следующие этапы:

1. По принятому сообщению $\overline{x} = \overline{c} + \overline{e}$ вычисляем синдром $S = S(\overline{x}) = H \cdot (\overline{x})^T = (s_1, s_2, \ldots, s_t)^T$.

2. Вычисляем норму $\overline{N}^* = \overline{N}(S)$; находим в таблице $\overline{N}_k = \overline{N}^*$.

3. Если k-ая Г-орбита – единственная с условием $\overline{N}_k = \overline{N}^*$, то вычисляем $s_1 / s_1^k = \beta^\mu$ или $\mu = (\deg s_1 - \deg s_1^k)/c$.

4. Если с нормой $\overline{N}^*$ имеется θ Г-орбит, $1 < \theta \le 1$, а именно, $<e_{k1}>, \ldots, <e_{k\theta}>$, то вычисляем величины $\mu_i = (\deg s_1 - \deg s_1^{ki})/c$, $1 \le i \le \theta$. Найдется единственное i^*, $1 \le i^* \le \theta$, с условием $\mu = \mu_i^*$ – целое число.

5. Вычисляем вектор-ошибку $\overline{e} = \sigma^\mu(\overline{e}_{ki^*})$.

Пример. В поле $GF(2^6)$ величина $2^6 - 1 = 63 = 3 \cdot 3 \cdot 7$. Следовательно, над этим полем определен непримитивный (21,6) – БЧХ С с проверочной матрицей $H = (\beta^i, \beta^{3i})$, то есть с $\beta = \alpha^3$ для примитивного элемента α поля $GF(2^6)$. Возьмем в качестве α корень полинома $x^6 + x + 1$. Конструктивное расстояние кода $\sigma = 5$. Но код декодирует наряду с двойными ошибками и пакеты ошибок длиной 4 и весом $\omega = 3$. Об этом свидетельствует *табл.* 2.

Таблица 2

Образующие $\bar{e}_i$ Г-орбит ошибок весом 1, 2 и пакетов ошибок весом 3 и длиной 4, синдромы $S(\bar{e}_i)$ и нормы $\overline{N}_i = \overline{N}(S(\bar{e}_i))$

$\bar{e}_i$	(1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)
$S(\bar{e}_i)$	(1,1)	$(\alpha^{53},\alpha^{45})$	$(\alpha^{43},\alpha^{27})$	$(\alpha^{45},\alpha^{18})$	$(\alpha^{23},\alpha^{54})$	(α^{44},α^{9})	$(\alpha^{27},\alpha^{36})$
N_i	1	α^{12}	α^{24}	α^{9}	α^{48}	α^{3}	α^{18}
$\bar{e}_i$	(1,8)	(1,9)	(1,10)	(1,11)	(1,2,3)	(1,2,4)	(1,3,4)
$S(\bar{e}_i)$	$(\alpha^{42},0)$	$(\alpha^{46},\alpha^{45})$	$(\alpha^{18},\alpha^{27})$	$(\alpha^{25},\alpha^{18})$	$(\alpha^{55},\alpha^{36})$	$(\alpha^{24},\alpha^{54})$	$(\alpha^{28},0)$
N_i	0	α^{33}	α^{36}	α^{6}	α^{60}	α^{45}	0

В *табл*. 2 лишь две Г-орбиты имеют одинаковую – нулевую норму. Но спектры синдромов этих Г-орбит не пересекаются. Поэтому, согласно теореме 2, код С все перечисленные в табл. 2 векторы-ошибки может декодировать. Минимальное кодовое расстояние $d = 5$.

Пусть, к примеру, декодер с данным кодом принял сообщение – вектор $\bar{x} = (10101011001000001011) = (\bar{c} + \bar{e})$. Вычисляем его синдром $S(\bar{x}) = S(\bar{c} + \bar{e}) = S(\bar{e}) = H \cdot \bar{x}^T = (s_1, s_2)^T$, где

$$s_1 = 1 + \beta^2 + \beta^4 + \beta^7 + \beta^{10} + \beta^{17} + \beta^{20} + \beta^{21} = \alpha^{16};$$

$$s_2 = 1 + \beta^6 + \beta^{12} + \beta^{18} + \beta^{21} + \beta^{30} + \beta^{51} + \beta^{60} + \beta^{63} = 0.$$

Ясно, что $N(S(\bar{e})) = 0 = N_7 = N_{13}$. $\deg s_1 - \deg s_1^7 = 16 - 14 = 2$ не делится на 3; $\deg s_1 - \deg s_1^{13} = 16 - 28 = -12 = 63 - 12 = 51 = 3 \cdot 17$. Следовательно, $\mu = 17$ и $\bar{e} = \sigma^{17}(1,3,4) = (18,20,21)$ – пакетная ошибка длиной 4 и весом 3 на последних четырех позициях кодового слова, а правимое сообщения $\bar{c} = (1010101100\,10000000000)$.

Таким образом, непримитивные БЧХ-коды обладают хорошими корректирующими возможностями, а теория норм синдромов обеспечивает эффективный метод их декодирования.

Литература

1. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* // Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
2. *Конопелько В.К., Липницкий В.А.* // Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М.: УРСС,2004.–176 с.