УДК 621.391.(075.8)

ДЕКОДИРОВАНИЕ КРАТНЫХ ОШИБОК НА ОСНОВЕ ЦИКЛОТОМИЧЕСКОГО СЖАТИЯ НОРМ СИНДРОМОВ

А.В.КУРИЛОВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Работа посвящена совершенствованию норменных методов коррекции ошибок для семейства БЧХ-кодов. Разрабатывается метод сжатия норм синдромов с помощью циклотомических подстановок. Переход к G-орбитам в примитивных БЧХ-кодах позволяет дополнительно сократить в $Log_2 n$ раз количество селектируемых Г-орбит.

Ключевые слова: синдром ошибок, норма синдрома, автоморфизм кода, циклическая подстановка, циклотомическая подстановка, БЧХ-код, декодер.

Введение

На рубеже 20 – 21 веков белорусской школой кодировщиков разработана теория норм синдромов – новое направление в теории и практике помехоустойчивого кодирования. Основным ее практическим результатом явилась серия норменных перестановочных методов коррекции кратных ошибок для широкого семейства циклических кодов, в частности, для семейства кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов) [1, 2]. Норменные методы отличают сокращение в n раз (n – длина кода) количества селектируемых комбинаций, конструктивная возможность исчерпания избыточности кодов, однородность структуры декодирующих схем.

Интенсивный рост объемов информации в современных инфокоммуникационных системах предъявляет жесткие требования к декодерам, прямым следствием которых является необходимость увеличения длин помехоустойчивых кодов и кратностей корректируемых ошибок. Эти требования приводят к необходимости дальнейшей работы по развитию теории норм синдромов и норменных методов коррекции ошибок. В [3] предложен оригинальный метод сжатия норм синдромов путем отображения векторов-ошибок в класс векторов-ошибок большей кратности. В данной работе рассматривается сжатие норм синдромов последовательным применением циклотомических подстановок.

Циклические и циклотомические подстановки принадлежат группам автоморфизмов многих циклических кодов, в том числе кодов семейства БЧХ [2, 4]. В данной работе на основе изученного влияния циклотомических подстановок на синдромы ошибок и нормы синдромов предложен альтернативный метод сжатия норм синдромов. Совместная группа G циклических и циклотомических подстановок разбивает корректируемую совокупность векторов-ошибок на непересекающиеся классы – G-орбиты. При этом G-орбиты состоят из Г-орбит. В примитивных БЧХ-кодах в подавляющем большинстве случаев G-орбита содержит $Log_2 n$ Г-орбит. Традиционные норменные методы требуют селекции всего многообразия Г-орбит корректируемой совокупности (что как известно в n раз меньше количества синдромов исправляемых векторов-ошибок). Предлагается модификация норменного метода, согласно которой следует селектировать только образующие G-орбит. В таком случае по вычисленным синдрому и норме синдрома определяем G-орбиту, содержащую искомую вектор-ошибку, затем осуществляем поиск вектора-ошибки внутри G-орбиты. Такой метод дополнительно

сокращает в $Log_2 n$ раз мощность селектируемой совокупности норм синдромов, что в конечном итоге соответственно уменьшает сложность декодирующих устройств.

Действие циклотомических подстановок на пространстве векторов-ошибок двоичных кодов

Определим на множестве $T=\{0,1,2,...,n-1\}$ преобразование φ по следующему правилу: для каждого $i \in T$ $\varphi(i)=\overline{2i}$ – элемент множества T, равный $2i$, если $2i<n$, и равный $2i-n$, если $2i \geq n$. Известно [2], что отображение φ является биекцией множества T тогда и только тогда, когда n нечетно. В дальнейшем $n=2l+1$ – нечётно. Существует наименьшее натуральное m с условием: $2^m-1=nq$, то есть n делит 2^m-1. Тогда циклическая группа Ф, порожденная степенями φ, конечна и имеет порядок m.

Группа Ф действует на пространстве ошибок E_n любого двоичного линейного кода, переставляя координаты векторов-ошибок в соответствии с указанным выше правилом действия на их номера, образующие множество T. Действия φ и ее степеней на i – элемент множества T – образуют циклотомический класс $i, 2i, 2^2 i, \cdots, 2^{m-1} i$ по модулю n [3]. Поэтому подстановки $\varphi, \varphi^2, \cdots, \varphi^m$ – называются циклотомическими. Действие подстановок $\varphi, \varphi^2, \cdots, \varphi^m$ на векторы пространства E_7 иллюстрирует рис. 1.

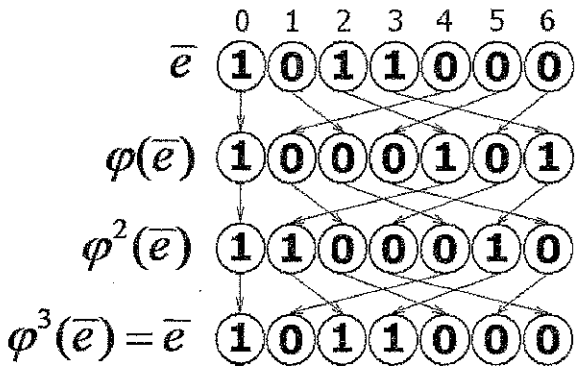

Рис. 1. Действие циклотомической подстановки φ и ее степеней в пространстве E_7 на вектор $\overline{e}=(1011000)$

Подстановки $\varphi, \sigma \in S_n$ для циклической подстановки σ на множестве T взаимосвязаны: для произвольного $\overline{e} \in E_n$ $\varphi\left(\sigma\left(\overline{e}\right)\right)=\sigma^2\left(\varphi\left(\overline{e}\right)\right)$ [2]. Они порождают некоммутативную группу G подстановок порядка mn.

Два вектора $\overline{f}$ и $\overline{g}$ из E_n называются G – эквивалентными, если найдется подстановка $\tau=\varphi^j\sigma^i \in \mathrm{G}$, такая, что $\overline{g}=\tau\left(\overline{f}\right)$. G – орбитой называется совокупность всех попарно G-эквивалентных между собой векторов-ошибок из E_n. Если $\overline{e}$ – фиксированный вектор данной G – орбиты, то G – орбиту с вектором $\overline{e}$ будем обозначать через $<\overline{e}>_G$.

Пусть $<\overline{e}>$ – Г-орбита, порожденная вектором $\overline{e} \in E_n$ [2]. Тогда $\varphi<\overline{e}>$ также является Г-орбитой. Поэтому всякая G-орбита имеет следующую структуру: $<\overline{e}>_G=\left\{<\overline{e}>, \varphi<\overline{e}>, \varphi^2<\overline{e}>, \ldots, \varphi^{\mu-1}<\overline{e}>\right\}$, где $\varphi^\mu<\overline{e}>=<\overline{e}>$, $\mu=m$ или делит m.

В табл. 1 приведены значения количества векторов-ошибок весом 2 – 4, их Г-орбит и G-орбит в примитивных БЧХ-кодах длиной в диапазоне от 15 до 1023.

Таблица 1. **Количество ошибок данного веса, их Г-орбит и G-орбит в зависимости от n**

Вес ω	Количество	Длина кода, n						
		15	31	63	127	255	511	1023
2	Ошибок	105	465	1 953	8 001	32 385	130 305	522 753
	Г-орбит	7	15	31	63	127	255	511
	G-орбит	3	3	7	9	16	29	52
3	Ошибок	455	4495	3 9711	333375	2731135	22108415	177910271
	Г-орбит	31	145	631	2625	10712	43265	173911
	G-орбит	10	29	106	375	214	4808	17395
4	Ошибок	13655	31465	595665	10334625	1,72E+08	2,81E+09	4,54E+10
	Г-орбит	91	1015	9455	81375	674751	5494655	44347135
	G-орбит	24	203	1577	11625	84345	610519	443474

Табл. 1 демонстрирует, что количество Г-орбит в n раз меньше количества векторов-ошибок данного веса, а количество G-орбит в $Log_2 n$ раз меньше числа составляющих их Г-орбит.

Влияние циклотомических подстановок на синдромы и нормы синдромов векторов-ошибок

Пусть $S(\overline{e}) = (s_1, s_2, ..., s_{\delta-1})$ - синдром вектора-ошибки $\overline{e}$ в БЧХ коде С с проверочной матрицей $H = [\alpha^{bi}, \alpha^{(b+1)i}, ..., \beta^{(b+\delta-2)i}]^T$. Тогда синдром $S(\varphi(\overline{e})) = (s_1^2, s_2^2, ..., s_{\delta-1}^2)$ [2]. Отсюда и из определения компонент нормы синдрома [2] вытекает, что компоненты нормы синдрома $N(S(\varphi(\overline{e})))$, преобразуются аналогично – возводятся в квадрат как элементы поля Галуа.

В табл. 2 приведен список G-орбит и составляющих их Г-орбит векторов-ошибок весом 2 в пространстве E_{31}, синдромов образующих и норм синдромов в БЧХ-коде C_5 над полем $GF(32)$ с примитивным элементом α – корнем полинома $x^5 + x^2 + 1$.

Каждая G-орбита в табл. 2 является полной – содержит максимально возможное количество Г-орбит, при этом построена из Г-орбит по циклу: следующая Г-орбита есть образ предыдущей под действием φ, последняя при этом переходит в первую. Аналогично выбраны и образующие Г-орбит. Поэтому компоненты синдрома каждой следующей образующей являются квадратами соответствующих компонент синдрома предыдущей образующей. Такая же взаимосвязь и норм синдромов внутри G-орбит.

Таким образом, зная образующую G-орбиты, а также ее синдром, можно однозначно восстановить элементы всей G-орбиты и синдромы всех ее векторов-ошибок.

Таблица 2. **Структура G-орбит векторов-ошибок весом 2 в пространстве** E_{31}

№ п/п G-орбиты	G-орбита $<\bar{e}>_G$	Образующая Г-орбиты $<\bar{e}>$	Показатели ($\deg s_1$, $\deg s_2$) компонент синдрома $S(\bar{e})=(s_1,s_2)$	Показатель нормы degN(S($\bar{e}$))
1	$<(0,1)>_G$	(0,1)	(18,29)	6
		(0,2)	(5,27)	12
		(0,4)	(10,23)	24
		(0,8)	(20,15)	17
		(0,16)	(9,30)	3
2	$<(0,3)>_G$	(0,3)	(29,16)	22
		(0,6)	(27,1)	13
		(0,12)	(23,2)	26
		(0,24)	(15,4)	21
		(0,17)	(30,8)	11
3	$<(0,5)>_G$	(0,5)	(2,24)	18
		(0,10)	(4,17)	5
		(0,20)	(8,3)	10
		(0,9)	(16,6)	20
		(0,13)	(14,20)	9

Норменный метод коррекции ошибок на основе циклотомических подстановок

Предложенная классификация векторов-ошибок позволяет сформулировать норменный перестановочный метод коррекции ошибок в БЧХ-кодах на основе циклотомических подстановок.

Предварительно составляем список 1 образующих $\bar{g}_i$ из совокупности $K=\{G_1,\ldots,G_t\}$ G-орбит корректируемых векторов-ошибок, список 2 синдромов $S(\bar{g}_i)$ и список 3 норм синдромов $\bar{N}_i=N(S(\bar{g}_i))$ или показателей $d_i=\deg N_i$.

Предлагаемый метод можно сформулировать следующим образом.

Приняв сообщение $\bar{x}_i$, вычисляем его синдром ошибок $S(\bar{x})=\alpha^i$.

Вычисляем текущую норму $\bar{N}_{\text{òåê}}=N(S(\bar{x}))$ (или показатель $\deg(N(S(\bar{x})))$.

В счётчике итераций алгоритма записываем «0».

Текущую норму сравниваем с множеством $\{\bar{N}_1,\ldots,\bar{N}_t\}$ третьего списка. Если $N=\bar{N}_i$, то переходим к этапу 4. Если же $N\notin\{\bar{N}_1,\ldots,\bar{N}_t\}$,, то переходим к этапу 5.

По текущему значению синдрома в Г-орбите $<g_i>$ с нормой $\bar{N}_i$ по одному из вариантов известного норменного алгоритма (см. [2], раздел 5.1) находим вектор-ошибку $\bar{e}_{\text{òåê}}$. Если в счётчике записано значение «0», то переходим к последнему - седьмому этапу алгоритма. Если в счётчике записано ненулевое значение, то переходим к шестому этапу.

Вычисляем квадрат текущей нормы, а с ним и квадраты компонент синдрома. Значение счётчика итераций увеличиваем на 1. С полученными текущими значениями нормы и синдрома возвращаемся к этапу 3.

Если в счётчике записано число k, $1\le k\le m-1$, то находим истинный вектор ошибок по формуле $\bar{e}=\varphi^{m-k}(\bar{e}_{\text{òåê}})$ и переходим к седьмому этапу алгоритма.

Находим истинное сообщение $\bar{c}=\bar{x}+\bar{e}$.

Техническая реализация данного метода может иметь различные варианты в зависимости от применяемых средств и схем декодеров. Наиболее естественной, является схема декодера, представленная на рис. 2 для коррекции ошибок в (21, 31)-БЧХ-коде C_5, исправляющем двойные ошибки. Необходимые данные представлены в табл. 2. Здесь синдром S поступает через мультиплексоры M_i, M_j на логическую матрицу ЛМ1, выделяющую только три фиксированные нормы синдрома N_1, N_2, N_3. Если на выходе ЛМ1 присутствует логический "0", то счетчик Cr переходит из состояния (0,0,...,0) в состояние (1,0,...,0). Далее, декодер переходит к реализации п. 4 алгоритма. При наличии логической "1" на выходе ЛМ1 – к п. 5 алгоритма.

В двух блоках умножения БУ1, БУ2 последовательно производится параллельное возведение в квадрат компонент синдрома s_1 и s_2 как элементов поля Галуа. Полученные значения квадратов поочередно опрашиваются через мультиплексоры M_i, M_j под управлением выходного кода счетчика. Данная операция по сути дела осуществляет последовательную перестановку образующих векторов Г-орбит ошибок.

При логическом "1" на выходе ЛМ1 счетчик останавливается, фиксируя тем самым код перестановки текущей нормы синдрома до одной из выбранных норм N_1, N_2, N_3. Компоненты вычисленного синдрома $S^* = (s_1^2, s_2^2)$ поступают на ЛМ2. На выходе ЛМ2 будет находиться вектор ошибок $\overline{e}_i^*$ из Г-орбиты J_i с нормой N_i, синдром которого равен S^*.

На седьмом этапе найденный вектор $\overline{e}_i^*$ поступает на блок обратной перестановки вектора ошибок (БОПВО) для нахождения истинного вектора ошибок $\overline{e}$. Это можно осуществить под управлением кода перестановки, хранимого в счетчике.

Реализация БОПВО сопряжена с определенными трудностями, поскольку необходимо реализовать не циклическую перестановку для вектора ошибок данной нормы N_i, а преобразование с изменением диаметра, полученного с ЛМ1 с нормой синдрома N_i. Зная степени i_T и i_0 синдромов можно определить, код сдвига $L_{сдв} = i_T - i_0$ для нормы N_i. В Величина сдвига не меняется под действием преобразований этапа 4 и, следовательно, остается одинаковой для всех рассматриваемых алгоритмом Г-орбит. Тогда по известному коду перестановки (а, значит, и по известной норме) можно сформировать образующий вектор ошибок и сдвинуть его в регистре сдвига на соответствующее число тактов, или же по адресу не сдвинутого вектора ошибок находить адреса текущего вектора ошибок.

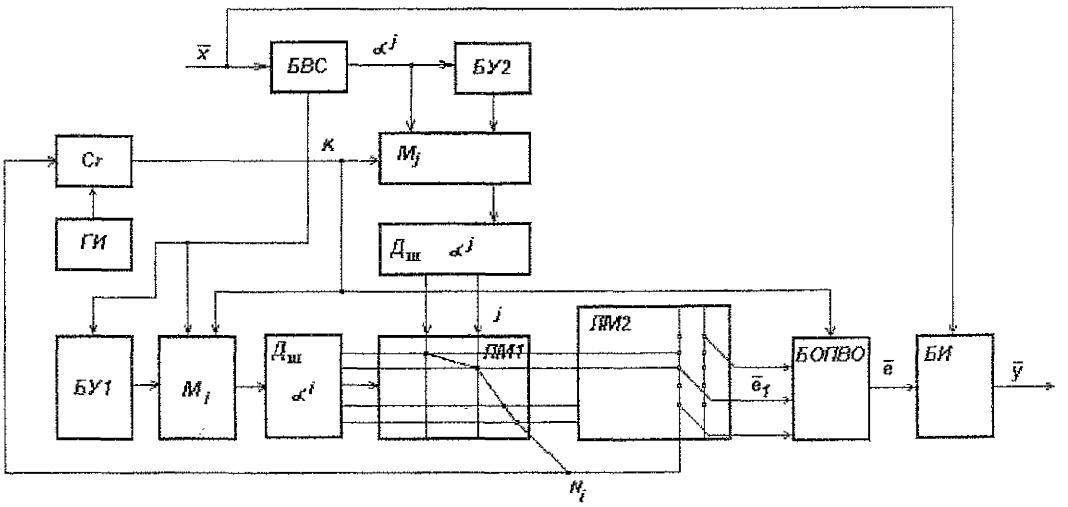

Рис. 2. Структурная схема декодера, реализующего метод циклотомического сдвига для t=3

Анализ затрат на реализацию метода показывает, что резкое сокращение аппаратурных затрат (например, для t=3 емкость ЛМ1 равна 3n, а ЛМ2 – 6n, то есть суммарная сложность равняется 9n) связано с увеличением числа тактов на перебор всех норм синдромов. Так при длине кода n=31 при t=3 в худшем случае требуется 161 такт (примерно 5n тактов) на декодирование.

Заключение

В работе исследован норменный метод коррекции ошибок БЧХ-кодами на основе циклотомических перестановок. Этот метод позволяет существенно сократить множество селектируемых норм синдромов (в $Log_2 n$ раз для примитивных БЧХ-кодов, где n – длина кода). Предложена реализация метода декодером на логических матрицах или на программируемых логических интегральных схемах.

DECODING OF MULTIPLE ERRORS ON THE BASIS OF CYCLOTOMIC COMPRESSION OF NORMS OF SYNDROMES

A.V. KURYLOVICH

Abstract

Work is devoted perfection norm methods of correction of errors for family of BCHH-CODES. The method of compression of norms of syndromes with the help cyclotomic substitutions is developed. Transition to G-orbits in primitive BCHH-CODES allows to reduce in addition in $Log_2 n$ time quantity selected G-orbits.

Литература

1. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М, 2004.
2. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
3. *Курилович А.В., Конопелько В.К., Липницкий В.А.* // Докл. БГУИР, 2005. № 6. 28 – 30.
4. *Мак-Вильямс, Ф.Дж.* Теория кодов, исправляющих ошибки. М., 1979.