УДК 004.056.55

УНИВЕРСАЛЬНЫЙ АЛГОРИТМ КОРРЕКЦИИ ОШИБОК ДЛЯ НЕ ПРИМИТИВНЫХ БЧХ-КОДОВ В ДИАПАЗОНЕ ДЛИН ОТ 0 ДО 99

А.О. ОЛЕКСЮК, В.А. ЛИПНИЦКИЙ

Военная академия Республики Беларусь, Республика Беларусь

Поступила в редакцию 30 марта 2020

Аннотация. Предложен алгоритм обнаружения и коррекции ошибок для не примитивных БЧХ-кодов в диапазоне длин от 9 до 99. Метод базируется на теории норм синдромов, с применением алгоритмов группирования норм, обнуления первых синдромов и приведению к исходному виду второго синдрома ошибки. Показано, что алгоритм работает значительно быстрее, чем ранее известные алгоритмы обнаружения и исправления ошибок.

Ключевые слова: линейный циклический код, не примитивный БЧХ-код, автоморфизмы кодов, устройство коррекции ошибок.

Введение

Современные системы передачи данных функционируют, как правило, в каналах с разного рода шумами и помехами. Для защиты информации, передаваемой в зашумленных каналах, от искажений и ошибок общепринято применять помехоустойчивое кодирование. Сущность кодирования заключается во введении специальным образом избыточных символов в каждую передаваемую информационную комбинацию [1].

В цифровых системах передачи данных наибольшей популярностью пользуются коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) и их разнообразные модификации, данные коды широко используются в современной радиосвязи [2-4].

Тем не менее, многие вопросы, связанные со свойствами и применением БЧХ-кодов, требуют дальнейших исследований. Сказанное наиболее характерно для популярнейшего на практике класса кодов Боуза-Чоудхури-Хоквингема, особенно не примитивных БЧХ-кодов [2, 5], нередко имеющих корректирующие параметры, существенно превосходящие конструктивные [10]. Для реализации названного потенциала стандартные средства неприменимы. Здесь требуется разработка принципиально новых подходов, применение новых идей. Статья посвящена универсальным алгоритмам коррекции и поиска ошибок в данных кодах.

Перспективность не примитивных БЧХ-кодов

Наиболее популярными на практике из общего семейства БЧХ-кодов являются коды, задаваемые проверочной матрицей вида

$$\bar{\mathbf{H}} = \left(\beta^{i}, \beta^{3i}, \ \ldots \ , \beta^{(2\delta-1)i}\right)^{T} \qquad (1)$$

над полем Галуа $GF(2^m)$ из 2^m элементов, где β – элемент этого поля, имеющий порядок $n = (2^m - 1)/\tau$ для некоторого делителя τ числа $2^m - 1$, $0 < i < n$. При $\tau = 1$ элемент $\beta = \alpha$ – является примитивным элементом поля Галуа $GF(2^m)$, а поэтому соответствующий БЧХ-код называется примитивным. В случае, когда значение параметра τ больше 1, длина БЧХ-кода

$n < 2^m - 1$, элемент $\beta = \alpha^\tau$ перестает быть примитивным, поэтому БЧХ-код называется не примитивным [5, 6].

Попытки усовершенствования БЧХ-кодов приводят к увеличению их длины. Как известно длина примитивных кодов изменяется скачкообразно: $n = 2^m - 1$. Резкое увеличение длины меняет статистику возникающих в канале ошибок, растет количество ошибок большей кратности, для их исправления мы должны увеличивать δ и, следовательно, размеры проверочной матрицы, что, в свою очередь, значительно сказывается на сложности декодера, скорости и эффективности его работы.

В отличие от примитивных, не примитивные БЧХ-коды обладают целым рядом эффективных свойств и, следовательно, перспективны для применения [5–9]. Дальнейшие обсуждения проводимых исследований ограничим не примитивными БЧХ-кодами с конструктивным расстоянием пять, проверочная матрица которых является частным случаем матрицы (1) и имеет вид:

$$\overline{\mathbf{H}} = \left(\beta^i, \beta^{3i}\right)^T. \qquad (2)$$

Фактически, не примитивные БЧХ-коды получаются укорочением примитивных кодов длиной $n = 2^m - 1$, то есть выбрасыванием ряда столбцов проверочной матрицы примитивного БЧХ-кода. С различных точек зрения важно, чтобы укороченный БЧХ-код сохранял свойство цикличности, иными словами, чтобы из проверочной матрицы $\overline{\mathbf{H}} = \left(\alpha^i, \alpha^{3i}\right)^T$ примитивного кода получалась матрица (2) укороченного циклического не примитивного БЧХ-кода. Процедура выбрасывания может только увеличить минимальное расстояние получаемого кода. И действительно, проведенные расчеты при анализе не примитивных кодов на длинах в диапазоне от 9 до 99 показали [8, 10], что около 30% из них имеют минимальное расстояние $d_{\text{реал}}$, существенно превышающее их конструктивное расстояние $d_{\text{констр}} = 5$. Примеры некоторых перспективных БЧХ-кодов с проверочной матрицей (2) представлены в табл.1, данные для которой взяты из [7, 10]. В табл.1 $K_{\text{констр}} = C_n^1 + C_n^2$ количество векторов-ошибок весом 1, 2, исправление которых гарантировано конструктивным расстоянием, $K_{\text{дек}}$ – количество реально корректируемых векторов-ошибок весом $1, 2, \ldots, t$, где $t = (d_{\text{реал}} - 1)/2$ для нечетных $d_{\text{реал}}$ (для четных $t = (d_{\text{реал}} - 2)/2$). $\Gamma_{\text{дек}}$ -количество Г-орбит, на которые разбивается $K_{\text{дек}}$.

Таблица 1. **Не примитивные БЧХ-коды C_5 над полями $GF(2^m)$ в диапазоне длин от 9 до 99, размерность которых $k > 1$ и $d_{\text{реал}} > d_{\text{констр}}$**

n	m	$d_{\text{реал.}}$	$K_{\text{констр}}$	$K_{\text{дек}}$	$\Gamma_{\text{дек}}$
33	10	9	561	46937	1423
39	12	10	780	92170	2364
43	14	13	946	7195749	167343
49	21	7	1225	19649	401
57	18	9	1653	425923	7473
69	22	7	2415	54809	795
73	9	7	2701	64897	889
77	30	7	3003	76153	989
87	28	9	3828	2335718	26847
89	11	9	4005	2559195	28755
91	12	7	4186	125671	1381
99	30	9	4950	3926175	39659

Данные табл.1 демонстрируют многократное количественное превосходство допустимых к исправлению ошибок над конструктивно допустимыми ошибками – явление, ранее не наблюдавшееся в практике помехоустойчивого кодирования (см. также [10]). Именно такие коды – не примитивные БЧХ-коды с конструктивным расстоянием пять, способные

корректировать ошибки кратностью $\omega \geq 3$, представляют наибольший интерес и являются предметом исследований в данной работе.

Методы декодирования

Самый популярный метод, применяемый в БЧХ-кодах для коррекции ошибок, это синдромный метод. Он базируется на взаимно-однозначном соответствии между многообразием корректируемых ошибок и множеством их синдромов. Прямой путь – «синдром – ошибка» – реализован в исторически первых декодерах. В нашей ситуации он невозможен из-за огромного количества корректируемых ошибок.

Весьма популярна реализация синдромного метода коррекции t – кратных случайных ошибок, сводящаяся к решению алгебраических уравнений степени t над полем $GF(2^m)$ [10]. К сожалению, в кодах с проверочной матрицей (2) метод уравнений конструктивно невозможен для коррекции ошибок кратностью $\omega \geq 3$.

Эффективным синдромным методом коррекции ошибок, в том числе выходящих за конструктивные пределы, является перестановочный норменный метод [5]. Он существенно опирается на цикличность БЧХ-кодов с проверочной матрицей (1), на принадлежность группе автоморфизмов этих кодов подгруппы Г циклических сдвигов координат кодовых слов. Группа Г позволяет разбить векторы ошибок на попарно непересекающиеся Г-орбиты, как правило, мощностью n, где n – длина кода. Синдромы ошибок каждой отдельно взятой Г-орбиты имеют четкую взаимосвязь, что позволяет ввести в рассмотрение нормы синдромов – одинаковые для всех векторов каждой Г-орбиты. Теория норм синдромов [5] описывает свойства нового параметра, дает новый – перестановочный норменный метод коррекции ошибок, на порядок снижающий влияние «проблемы селектора».

Общий метод перестановочного норменного декодирования БЧХ-кодов заключается в следующем. Предварительно составляется список образующих $\overline{e}_i$ Г-орбит декодируемой совокупности $K_{\text{дек}}$, синдромов $S(\overline{e}_i) = (s_1^i, s_2^i)$ образующих и совокупность $NK_{\text{дек}}$ норм $N_i = N(S(\overline{e}_i))$ синдромов образующих. Действующая на основе выбранного БЧХ-кода ТКС, приняв очередное сообщение $\overline{x}$, вычисляет его синдром ошибок $S(\overline{x})$. Если $S(\overline{x}) = 0$, то сообщение не содержит ошибок и является правильным. Если же $S(\overline{x}) \neq 0$, то $\overline{x}$ подлежит коррекции, так как содержит неизвестную вектор-ошибку $\overline{e}$. Для нахождения этой вектор-ошибки вычисляется норма синдрома $N = N(S(\overline{x}))$, данная норма сравнивается со списком $NK_{\text{дек}}$. Пусть $N = N^* \in NK_{\text{дек}}$. Это означает, что искомая вектор-ошибка $\overline{e}$ принадлежит Г-орбите, порожденной вектором $\overline{e}^*$ из списка образующих Г-орбит декодируемой совокупности $K_{\text{дек}}$. Сравнивая синдромы ошибок векторов $\overline{x}$ и $\overline{e}^*$, однозначно определяем вектор $\overline{e}$ [5]. Именно этот перестановочный метод будет адаптирован для коррекции ошибок не примитивными БЧХ-кодами.

Универсальный алгоритм поиска и коррекции ошибок для не примитивных БЧХ-кодов

В монографии [3], глава 5, предложен ряд норменных перестановочных методов коррекции ошибок БЧХ-кодами. Некоторые из названных методов получили дальнейшее развитие в теоретических исследованиях и на практике. Особое внимание получил метод коррекции на интегральных схемах (см. рис.5.5, глава 5, [3]).

Задача коррекции ошибок не примитивными БЧХ-кодами с $\delta = 5$ и $\omega > 2$ похожа на задачу коррекции ошибок, рассмотренную в [3]. Однако, прямое применение названных методов к коррекции многократных ошибок в рассматриваемом нами случае невозможно.

Основная причина – количество $\Gamma_{\text{дек}}$ орбит корректируемой совокупности, как минимум, на порядок превосходит количество их, допустимое декодерами из [3].

Разработана обобщенная структурная схема устройства декодирования кратных ошибок БЧХ-кодами с проверочной матрицей (2), [10].Схема включает в себя следующие блоки: блок вычисления синдрома (БВС), блок перестановочного нахождения вектора ошибки (БПНВО), блок корректирующих сумматоров по модулю два. Особенности работы БВС и корректирующих сумматором по модулю два нам уже известны, основной задачей является построение алгоритма работы для БПНВО, свозможностью работать с численными значениями синдромов ошибок и вариантами, когда значения синдромов равны бесконечности.

Основной принцип работы блока БПНВО заключается в следующем.Все многообразие Г $K_{\text{дек}}$ орбит корректируемой совокупности разбивается на $\tau \le (2^m - 1)/n + 1$ групп. В силу предложения 3.10 [5], если образующая $\overline{e}$ Г-орбиты J имеет синдром $S(\overline{e}) = (s_1, s_2)$, $s_1, s_2 \in GF(2^m)$, то синдромы остальных векторов этой орбиты имеют вид: $(\alpha^{\lambda} s_1, \alpha^{3\lambda} s_2)$, $0 < \lambda \le n - 1$. Среди этих синдромов обязательно найдется синдром (s_1^*, s_2^*), у которого $0 \le \deg(s_1^*) < (2^m - 1)/n$, если $s_1 \ne 0$, и $0 \le \deg(s_2^*) < 3 \times (2^m - 1)/n$, если $s_1 = 0$. Тогда вектор $\overline{e}^*$ с синдромами $S(\overline{e}^*) = (s_1^*, s_2^*)$ фиксируем в качестве образующего Г-орбиту J. Такой выбор образующих Г-орбит естественным образом разбивает Г $K_{\text{дек}}$ на части или группы, в одну группу T_i попадают Г-орбиты с одинаковым значением $s_1^* = \alpha^{i-1}$. Априори предполагаем, что число таких групп максимально возможное: $\tau = (2^m - 1)/n + 1$. Тогда Г $K_{\text{дек}}$ есть непересекающееся объединение $T_1 \cup T_2 \cup ... \cup T_{\tau}$, для $\tau = (2^m - 1)/n + 1$. Для целых i, $1 \le i < \tau$, в группе T_i содержатся Г-орбиты $< \overline{e}_{ij}^* >$, у которых первая компонента синдрома $S(\overline{e}_{ij}^*) = (s_1^{ij*}, s_2^{ij*})$ имеет показатель $\deg(s_1^{i*}) = \alpha^{i-1}$; $s_1^{\tau*} = 0$ для Г-орбит группы T_{τ}.

На базе этого принципа разработан универсальный алгоритм коррекции и поиска ошибок представленный в блок-схеме на рис.1.

Работает алгоритм следующим образом:

1. Поступившие на входы БПНВОзначения синдромов $\deg(s_1)$ и $\deg(s_2)$ в бинарном виде, преобразуются к десятичному виду. Значение степени синдрома $\deg(s_1)$ преобразуется по модулю $(2^m - 1)/n$, а из значения степени синдрома $\deg(s_2)$ вычитается число $3 \times t \times (2^m - 1)/n$ по модулю 2^m, где t – количество циклов, в течение которых, $\deg(s_1)$ преобразуется к исходному значению r. Преобразованное $\deg(s_1)^*$ примет некое значение r, $0 \le r \le \tau - 1$, а $\deg(s_2)^*$ будет равняться некоторому z, $0 \le z < 2^m$. В группе T_{r+1} обязательно найдется Г-орбита $< \overline{e}_{(r+1)j}^* >$, у которой компоненты синдрома $S(\overline{e}_{(r+1)j}^*) = (s_1^{(r+1)j*}, s_2^{(r+1)j*})$ имеют показатели $\deg(s_1^{(r+1)j*}) = \deg(s_1)^*$ и $\deg(s_2^{(r+1)j*}) = \deg(s_2)^*$.

2. Полученное значение начального вектора ошибки $\overline{e}_0 = \overline{e}_{(r+1)j}^*$ сдвигается на t позиций вперед.

В случае $\deg(s_2) = 2^m$ – происходит только операция по преобразованию $\deg(s_1)$, $\deg(s_2)$ – остается неизменным.

В случае $\deg(s_1) = 2^m$, как правило, данный случай применим для неполных Г-орбит ошибок – преобразований $\deg(s_1)$ не происходит, происходит только операция преобразования $\deg(s_2)$ по модулю $3 \times (2^m - 1)/n$, в процессе преобразования производится подсчет p - количество циклов, в течение которых, $\deg(s_2)$ преобразуется к исходному значению y, $0 \le y \le 3 \times (\tau - 1)$. Полученное значение вектора ошибки сдвигается на p позиций вперед.

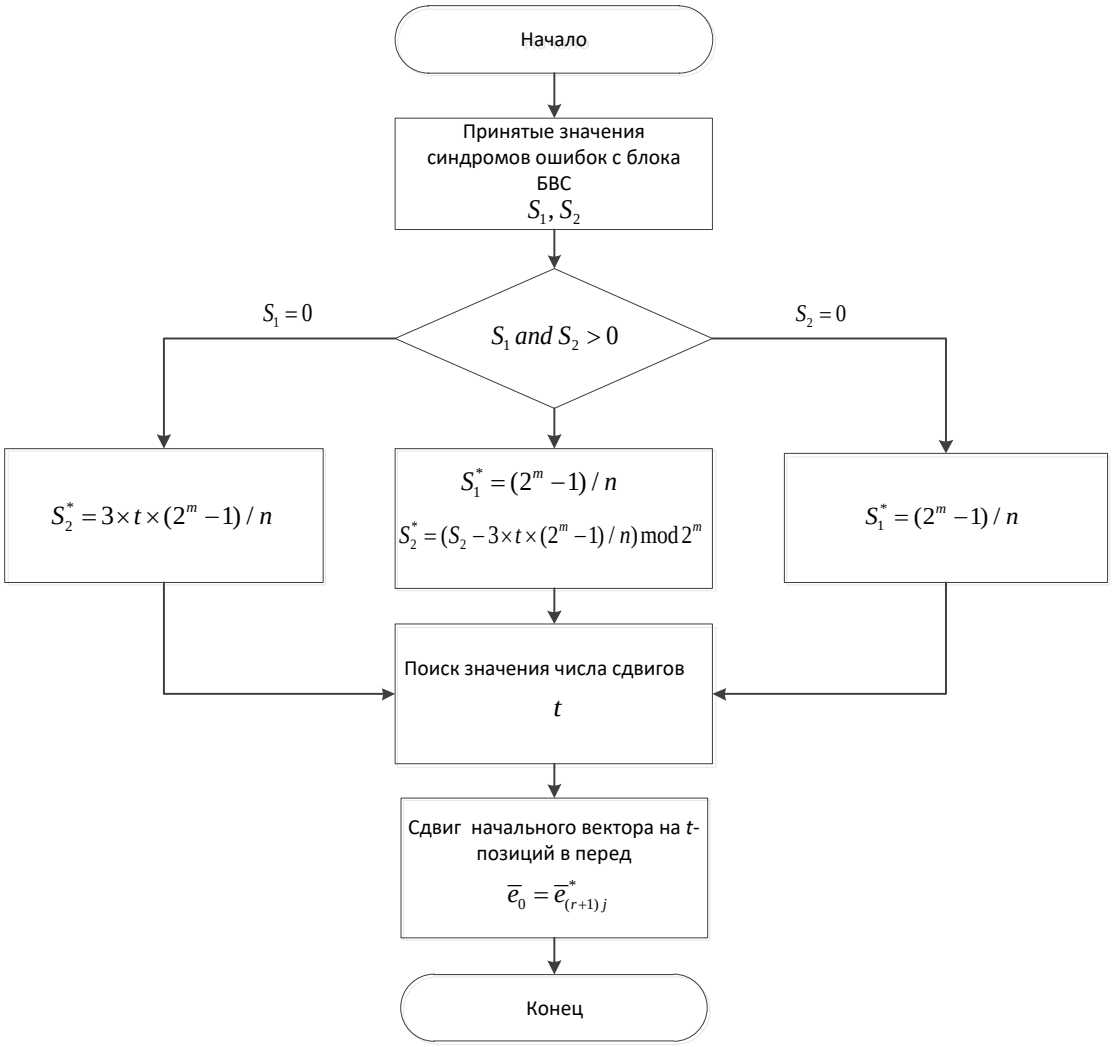

Рис. 1. Блок-схема универсального алгоритма коррекции и исправления ошибок

Заключение

Проведенные исследования показывают, что не примитивные БЧХ-коды обладают хорошими корректирующими возможностями, выходящими за пределы конструктивных. Предложенный универсальный алгоритмобнаружения и коррекции ошибок для не примитивных БЧХ-кодов в диапазоне длин от 9 до 99может найти достойное место в разрабатываемых и применяемых на практике системах передачи данных.

UNIVERSAL ERROR CORRECTION ALGORITHM FOR NON-SIMPLE BCH CODES IN THE RANGE OF LENGTHS FROM 0 TO 99

A.O. ALIAKSIUK, V.A. LIPNITSKI

Abstract. An algorithm for detecting and correcting errors for non-primitive BCH codes in the range of lengths from 9 to 99 is proposed. The method is based on the theory of norms of syndromes, using algorithms for grouping norms, zeroing the first syndromes and bringing the second syndrome of the error back to its original form. It is shown that the algorithm works much faster than previously known error detection and correction algorithms.

*Keywords:*linear cyclic code, non-primitive BCH code, automorphisms of codes, error correction device.

Списоклитературы

1. Шеннон К. Работа по теории информации и кибернетике. М.: ИЛ, 1963.
2. Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь. 1979.
3. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн.: Издательский центр БГУ, 2007.
4. Вернер Р. Основы кодирования. М.: Техносфера. 2006.
5. Липницкий В.А.,[и др.] Прикладная математика и теория норм синдромов: методич. пособие.Минск: М-во образования РБ, БГУИР. 2011.
6. Курилович А.В., Липницкий В.А., Михайловская Л.В. // Сб. науч. статей. / Ин-т технологий нформатизации и управления БГУ. Вып. 2: Технологии информатизации и управления. Минск.: 2011. С. 43–49.
7. Липницкий В.А., Олексюк А.О. //Доклады БГУИР.2014.№8 (86). С. 72–78.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир. 1986.
9. Олексюк А.О.,Липницкий В.А. Устройство коррекции ошибок кратность четыре № A20130054 от 16 января 2013г.
10. Липницкий, В.А. Олексюк А.О.// Доклады БГУИР. 2015. №3(89). С.117–123.