

УДК 004.056.55

## ПЕРЕСТАНОВОЧНЫЙ ДЕКОДЕР ДЛЯ КОРРЕКЦИИ МНОГОКРАТНЫХ ОШИБОК НЕПРИМИТИВНЫМИ БЧХ-КОДАМИ

В.А. ЛИПНИЦКИЙ, А.О. ОЛЕКСЮК

Военная академия Республики Беларусь  
Минск, 220057, Беларусь

Поступила в редакцию 17 февраля 2015

Доказано, что не примитивные БЧХ-коды с корректирующими возможностями, выходящими за пределы конструктивных, имеют эффективные микропроцессорные перестановочные алгоритмы коррекции ошибок и могут найти достойное место в разрабатываемых и применяемых на практике инфокоммуникационных системах.

*Ключевые слова:* теория норм синдромов, БЧХ-коды, не примитивные БЧХ-коды, конструктивное расстояние, минимальное расстояние кода, Г-орбита.

### Введение

Современные инфокоммуникационные системы (ИКС) вынуждены функционировать, 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 телекоммуникационных сетях наибольшей популярностью пользуются коды Боуза-Чоудхури-Хоквингема (БЧХ-коды) и их разнообразные модификации; данные коды широко используются в современной радиосвязи [2]. Тем не менее, многие вопросы, связанные со свойствами и применением БЧХ-кодов, требуют дальнейших исследований. Особенно сказанное относится к не примитивным БЧХ-кодам [3, 4], нередко имеющим корректирующие параметры, существенно превосходящие конструктивные. Данная статья посвящена алгоритмам декодирования подобных кодов и возможностям реализации предложенных алгоритмов на микропроцессорной технике.

### Не примитивные БЧХ-коды, их перспективность

Практический интерес из общего семейства БЧХ-кодов вызывают коды с наибольшей размерностью – циклические коды, задаваемые проверочной матрицей вида

$$\bar{H} = (\beta^i, \beta^{3i}, \dots, \beta^{(2^{\delta}-1)i})^T \quad (1)$$

над полем Галуа  $GF(2^m)$  из  $2^m$  элементов, где  $\beta$  – элемент этого поля, имеющий порядок  $n = (2^m - 1)/\tau$  для некоторого делителя  $\tau$  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  $\tau$  больше 1, длина БЧХ-кода  $n < 2^m - 1$ , элемент  $\beta = \alpha^\tau$  перестает быть примитивным, поэтому БЧХ-код называется не примитивным [3, 4].

К современным системам связи с каждым днем ужесточаются требования: к качеству передаваемой информации, к ее точности, к помехозащищенности, к скорости передачи информации. Попытки их усовершенствования приводят к увеличению длины применяемых

примитивных БЧХ-кодов. 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  $\delta$  и, следовательно, размеры проверочной матрицы, что, в свою очередь, значительно сказывается на сложности декодера, скорости и эффективности его работы.

### Перспективность не примитивных БЧХ-кодов

Новейшие исследования, проведенные в XXI веке белорусской школой помехоустойчивого кодирования показывают, что не примитивные БЧХ-коды обладают целым рядом эффективных свойств и, следовательно, перспективны для применения [3–7]. Дальнейшие обсуждения проводимых исследований ограничим не примитивными БЧХ-кодами с конструктивным расстоянием пять, проверочная матрица которых является частным случаем матрицы (1) и имеет вид

$$\bar{H} = (\beta^i, \beta^{3i})^T. \quad (2)$$

Фактически, не примитивные БЧХ-коды получаются укорочением примитивных кодов длиной  $n = 2^m - 1$ , т.е. 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  $\bar{H} = (\alpha^i, \alpha^{3i})^T$  примитивного кода получалась матрица (2) укороченного циклического не примитивного БЧХ-кода. Процедура выбрасывания может только увеличить минимальное расстояние получаемого кода. И действительно, компьютерные расчеты при анализе не примитивных кодов на длинах в диапазоне от 9 до 99 показали [6], 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]. 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, ...,  $t$ , где  $t = (d_{\text{реал}} - 1) / 2$  для нечетных  $d_{\text{реал}}$  (для четных  $t = (d_{\text{реал}} - 2) / 2$ ).  $\Gamma_{\text{дек}}$  – количество  $\Gamma$ -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 [7]). 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.

## Выбор метода 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  $GF(2^m)$  [8]. 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 [3]. Он существенно опирается на цикличность БЧХ-кодов с проверочной матрицей (1), на принадлежность группе автоморфизмов этих кодов подгруппы  $\Gamma$  циклических сдвигов координат кодовых слов. Группа  $\Gamma$  позволяет разбить векторы ошибок на попарно непересекающиеся  $\Gamma$ -орбиты, как правило, мощностью  $n$ , где  $n$  – длина кода. Синдромы ошибок каждой отдельно взятой  $\Gamma$ -орбиты имеют четкую взаимосвязь, что позволяет ввести в рассмотрение нормы синдромов – одинаковые для всех векторов каждой  $\Gamma$ -орбиты. Теория норм синдромов [3] 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  $\bar{e}_i$   $\Gamma$ -орбит декодируемой совокупности  $K_{\text{дек}}$ , синдромов  $S(\bar{e}_i) = (s_1^i, s_2^i)$  образующих и совокупность  $NK_{\text{дек}}$  норм  $N_i = N(S(\bar{e}_i))$  синдромов образующих. Действующая ТКС, приняв очередное сообщение  $\bar{x}$ , вычисляет его синдром ошибок  $S(\bar{x})$ . Если  $S(\bar{x}) = 0$ , то сообщение не содержит ошибок и является правильным. Если же  $S(\bar{x}) \neq 0$ , то  $\bar{x}$  подлежит коррекции, так как содержит неизвестную вектор-ошибку  $\bar{e}$ . Для нахождения этой вектор-ошибки вычисляется норма синдрома  $N = N(S(\bar{x}))$ , данная норма сравнивается со списком  $NK_{\text{дек}}$ . Пусть  $N = N^* \in NK_{\text{дек}}$ . Это означает, что искомая вектор-ошибка  $\bar{e}$  принадлежит  $\Gamma$ -орбите, порожденной вектором  $\bar{e}^*$  из списка образующих  $\Gamma$ -орбит декодируемой совокупности  $K_{\text{дек}}$ . Сравнивая синдромы ошибок векторов  $\bar{x}$  и  $\bar{e}^*$ , однозначно определяем вектор  $\bar{e}$  [3]. Именно этот перестановочный метод будет адаптирован для коррекции ошибок не примитивными БЧХ-кодами.

### Алгоритм перестановочного декодирования кратных ошибок для не примитивных БЧХ-кодов на микропроцессорной базе

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]).

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

Авторами разработана обобщенная структурная схема устройства декодирования кратных ошибок БЧХ-кодами с проверочной матрицей (2), представленная на рис. 1. Схема включает в себя следующие блоки: блок вычисления синдрома (БВС), блок перестановочного нахождения вектора ошибки (БПНВО), блок корректирующих сумматоров по модулю два. Особенности данной схемы отражают следующие четыре момента.

1. Непосредственно в алгоритме отсутствует вычисление норм  $\Gamma$ -орбит (так

необходимых при качественном исследовании качественных характеристик каждого не примитивного БЧХ-кода).

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

3. Почти в каждой группе  $T_i$  могут содержаться ошибки разного веса.

4. Предлагается применение микроконтроллеров в качестве своеобразной интеллектуальной оболочки всего алгоритма. Микроконтроллеры позволяют конструктивно уменьшить размеры устройства за счет того, что они содержат в своей оболочке набор таких необходимых элементов, как счетчики, дешифраторы и другие элементы, в отличие от аналогичных устройств (см. рис. 5.1–5.4, глава 5, [3]), которые требуют применения названных элементов. Микропроцессор конструктивно адаптирует перестановочный алгоритм на интегральных схемах (рис. 5.5, глава 5, [3]). Вычислительные возможности микропроцессора допускают практически мгновенный переход в нужную группу  $T_i$  на соответствующем этапе алгоритма.

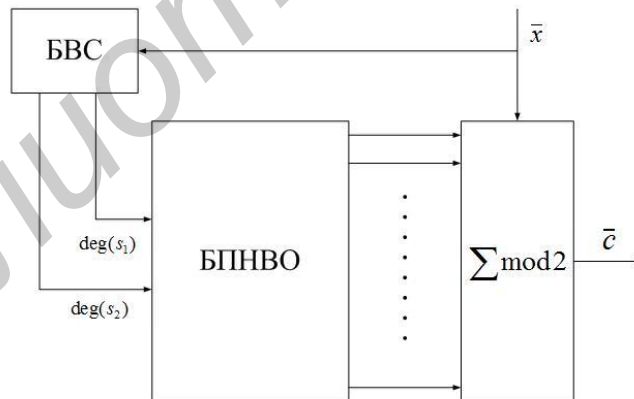


Рис. 1. Обобщенная структурная схема устройства декодирования кратных ошибок

Обобщенный микропроцессорный перестановочный алгоритм (МПА) работы данного устройства заключается в следующем.

1. Принятое сообщение  $\bar{x}$  поступает на входы блока вычисления синдрома, где формируются значения  $\deg(s_1)$  и  $\deg(s_2)$  показателей компонент  $s_1$  и  $s_2$  синдрома  $S(\bar{x})$ , которые в бинарном виде поступают на входы блока перестановочного нахождения вектора ошибки.

Блок перестановочного нахождения вектора ошибки работает следующим образом.

2. Поступившие на входы микроконтроллера значения  $\deg(s_1)$  и  $\deg(s_2)$  в бинарном

виде, преобразуются к десятичному виду. Значение степени синдрома  $\text{deg}(s_1)$  преобразуется по модулю  $(2^m - 1)/n$ , а из значения степени синдрома  $\text{deg}(s_2)$  вычитается число  $3 \times t \times (2^m - 1)/n$  по модулю  $2^m$ , где  $t$  – количество циклов, в течение которых,  $\text{deg}(s_1)$  преобразуется к исходному значению  $r$ . Преобразованное  $\text{deg}(s_1)^*$  примет некое значение  $r$ ,  $0 \leq r \leq \tau - 1$ , а  $\text{deg}(s_2)^*$  будет равняться некоторому  $z$ ,  $0 \leq z < 2^m$ . Микроконтроллер автоматически обеспечивает дальнейший поиск вектора ошибки только в группе  $T_{r+1}$ , следуя вычисленному значению  $\text{deg}(s_2)^*$ . В группе  $T_{r+1}$  обязательно найдется  $\Gamma$ -орбита  $\langle \bar{e}_{(r+1)j}^* \rangle$ , у которой компоненты синдрома  $S(\bar{e}_{(r+1)j}^*) = (s_1^{(r+1)j^*}, s_2^{(r+1)j^*})$  имеют показатели  $\text{deg}(s_1^{(r+1)j^*}) = \text{deg}(s_1)^*$  и  $\text{deg}(s_2^{(r+1)j^*}) = \text{deg}(s_2)^*$ .

3 Полученное значение начального вектора ошибки  $\bar{e}_0 = \bar{e}_{(r+1)j}^*$  сдвигается на  $t$  позиций вперед. Выходное значение вектора ошибки  $\bar{e}$  поступает на блок корректирующих сумматоров по модулю два, где и происходит сложение с ним по модулю два входного сигнала  $\bar{x}$ .

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

### Пример работы микропроцессорного перестановочного декодера

В качестве примера работоспособности выше описанного алгоритма коррекции многократных ошибок на базе микропроцессора разработано устройство, исправляющее ошибки весом  $\omega$ ,  $1 \leq \omega \leq 4$ . Устройство реализовано для не примитивного БЧХ-кода  $C_5$  длиной  $n = 33$ , имеющего  $d = 9$  согласно табл. 1, определенного над полем Галуа  $GF(2^{10})$ ; в качестве порождающего полинома этого поля взят примитивный полином  $x^{10} + x^3 + 1$ . Структурная схема устройства коррекции четырехкратных ошибок представлена на рис. 2 и включает в себя следующие блоки: 1 – блок вычисления синдрома, 3 – блок корректирующих сумматоров по модулю два, 6 – блок перестановочного нахождения вектора ошибки. Здесь  $\tau = 32$ .

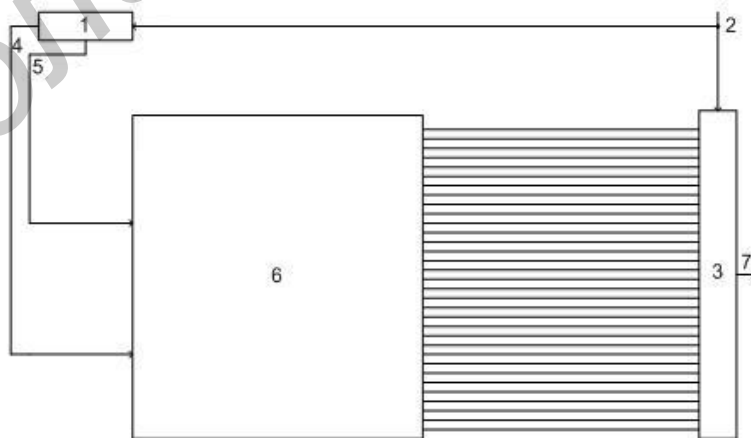


Рис. 2. Структурная схема декодера (33,13)-БЧХ-кода

Мощности групп  $T_i$ ,  $1 \leq i \leq 32$ , на которые разбивается множество  $\Gamma K_{\text{дек}}$  корректируемых  $\Gamma$ -орбит ошибок в рассматриваемом коде длиной 33 представлены в табл. 2.

Таблица 2. Мощности  $|T_\tau|$  групп  $T_i$  в коде  $C_5$  длиной 33

$\tau$	1	2	3	4	5	6
$ T_\tau $	37	51	51	41	51	48
$\tau$	7	8	9	10	11	12
$ T_\tau $	41	43	51	48	48	50
$\tau$	13	14	15	16	17	18
$ T_\tau $	40	51	43	44	51	40
$\tau$	19	20	21	22	23	24
$ T_\tau $	48	43	48	50	50	44
$\tau$	25	26	27	28	29	30
$ T_\tau $	41	43	50	44	43	43
$\tau$	31	32				
$ T_\tau $	44	1				

Рассмотрим работу декодера на конкретных примерах.

Пусть на входы 4, 5 блока перестановочного нахождения вектора ошибки (6) поступают синдромы ошибок со значениями  $\deg(\alpha^i)=77$ ,  $\deg(\alpha^j)=175$ . Так как ни одно из значений синдромов ошибок не равно бесконечности, то степень синдрома  $\deg(\alpha^i)=77$  преобразуется по модулю  $(2^m - 1)/n = 31$ , в результате чего  $\deg(\alpha^i)^* = 15$ . Из  $\deg(\alpha^j)=175$  число  $93 \times t$  по модулю 1024, где для данного случая  $t=2$ , преобразованное  $\deg(\alpha^j)^*$  будет равно 920. Полученные значения  $\deg(\alpha^i)^* = 15$  и  $\deg(\alpha^j)^* = 920$  будут являться синдромами, определяющими начальный вектор ошибки, а значение  $t=2$  – количество циклов, в течение которых  $\deg(s_1)$  преобразуется к значению 15. Следовательно, искомый вектор  $\bar{e}_0$  принадлежит группе  $T_{16}$ .

Составлена табл. 3 значений показателя  $\deg(s_2)$  второй компоненты синдрома образующих  $\bar{e}_{16,j}$   $\Gamma$ -орбит в группе  $T_{16}$ , т.е. образующих, у которых  $\deg(s_1)=15$ , а также самих образующих  $\bar{e}_{16,j}$ . Из табл. 3 следует, что группа  $T_{16}$  состоит из 44  $\Gamma$ -орбит (согласно табл. 2), из них: 1 состоит из двукратных векторов-ошибок; 5 – из трехкратных; 38 – из четырехкратных векторов-ошибок.

В табл. 3 под номером 10 находится  $\Gamma$ -орбита  $\langle \bar{e}_{16,10} \rangle = \langle (6, 9, 15, 16) \rangle$ , образующий вектор которой  $\bar{e}_{16,10} = (6, 9, 15, 16)$  – вектор весом 4 с единицами в 6-й, 9-й, 15-й, 16-й координатах, у которого компоненты синдрома  $S(\bar{e}_0) = (s_1^0, s_2^0)$  имеют показатели  $\deg(s_1^0)^* = 15$  и  $\deg(s_2^0)^* = 920$ .

Таблица 3. Значения показателя  $\deg(s_2)$  второй компоненты синдрома образующих  $\bar{e}_{16,j}$   $\Gamma$ -орбит в  $T_{16}$

$j$	$\deg(s_2)$	$\bar{e}_{16,j}$	$j$	$\deg(s_2)$	$\bar{e}_{16,j}$	$j$	$\deg(s_2)$	$\bar{e}_{16,j}$
0	375	(23,28)	15	805	(17,19,22,26)	30	337	(1,7,24,26)
1	784	(18,19,27)	16	771	(3,15,21,30)	31	327	(11,22,24,32)
2	558	(1,12,28)	17	756	(8,18,27,30)	32	306	(9,10,14,27)
3	177	(7,9,11)	18	723	(1,8,11,15)	33	291	(0,10,21,24)
4	164	(0,24,32)	19	697	(1,10,20,30)	34	285	(5,16,18,19)
5	93	(6,17,23)	20	662	(2,15,22,27)	35	258	(3,7,10,17)
6	1002	(0,18,25,26)	21	649	(6,24,25,31)	36	213	(4,8,9,24)
7	959	(12,20,26,27)	22	602	(0,5,30,31)	37	210	(7,11,20,31)
8	956	(14,15,20,29)	23	564	(0,2,13,32)	38	182	(11,17,25,27)
9	942	(0,7,9,22)	24	553	(3,4,22,31)	39	166	(0,1,14,16)
10	920	(6,9,15,16)	25	478	(13,18,20,21)	40	105	(9,11,18,29)
11	885	(7,19,27,29)	26	449	(8,17,21,31)	41	102	(7,13,25,30)
12	848	(2,4,17,18)	27	430	(2,5,8,14)	42	89	(4,10,13,16)
13	846	(5,11,21,26)	28	424	(2,3,9,12)	43	1024	(1,6,12,17)
14	836	(1,25,29,32)	29	352	(3,16,24,29)			

В силу проведенных выше вычислений полученный начальный вектор ошибки  $\bar{e}_0 = \bar{e}_{16,10}$  сдвигается на две позиции вперед. В результате получаем искомый вектор-ошибок  $\bar{e} = (9, 12, 18, 19)$ . Полученный вектор  $\bar{e}$  складываем по модулю 2 с принятым сообщением  $\bar{x}$  и получаем истинное сообщение  $\bar{c} = \bar{x} + \bar{e}$ .

Рассмотрим случай, когда  $\deg(s_1) = 2^m = 1024$ , т.е.  $s_1 = 0$ . Пусть, к примеру, на входы 4, 5 блока нахождения вектора ошибки (6) поступает сообщение  $\bar{x}$  с синдромом  $S(\bar{x}) = (s_1, s_2) = (\alpha^i, \alpha^j)$ , у которого:  $\deg(\alpha^i) = 1024$ ,  $\deg(\alpha^j) = 186$ . Согласно второму этапу алгоритма МПА преобразуется только  $\deg(s_2)$  к исходному значению  $y$ ,  $0 \leq y \leq 92$  по модулю 93. Очевидно,  $186 = 93 \times 2$ . Таким образом, при  $p = 2$  получаем начальный вектор ошибки  $\bar{e}_0$  с синдромом  $S(\bar{e}_0) = (s_1^0, s_2^0)$ , где  $\deg(s_1^0) = 1024$ ,  $\deg(s_2^0) = 0$ . Иными словами,  $S(\bar{e}_0) = (0, 1)$ . Согласно табл. 2 в группе  $T_{32}$  имеется единственная  $\Gamma$ -орбита  $\langle (\bar{e}_{32}) \rangle = \langle (1, 12, 23) \rangle$ , образующий вектор которой  $\bar{e}_{32} = (1, 12, 23)$  - вектор весом 3 с единицами в 1-й, 12-й, 23-й координатах. Вычисления показывают, что  $S(\bar{e}_{32}) = (0, 1)$  [9], что совпадает с  $S(\bar{e}_0)$ . Полученный начальный вектор ошибки сдвигается на две позиции вперед, в результате получаем искомый вектор  $\bar{e} = (3, 14, 25)$ . По результатам проведенных исследований подана заявка на изобретение устройства перестановочной коррекции ошибок не примитивными БЧХ-кодами на микропроцессорной основе [9].

### Заключение

Проведенные исследования показывают, что не примитивные БЧХ-коды обладают хорошими корректирующими возможностями, выходящими за пределы конструктивных, имеют эффективные микропроцессорные перестановочные алгоритмы коррекции ошибок, могут найти достойное место в разрабатываемых и применяемых на практике ИКС.

## CORRECTION COMMUTE DECODER FOR MULTIPLE ERRORS WITH NOT PRIMITIVE BCH-CODES

V.A. LIPNITSKI, A.O. ALIAKSIUK

### Abstract

It's proved that not primitive BCH codes with corrective opportunities that go beyond design, have effective microprocessor commutation algorithms error correction and can find its rightful place in developed and applied in practice ICS.

### Список литературы

1. Шеннон К. Работа по теории информации и кибернетике. М., 1963.
2. Мак-Вильямс Ф.Дж., Слоэн Н. Дж.А. Теория кодов, исправляющих ошибки. М., 1979.
3. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
4. Вернер Р. Основы кодирования. М., 2006.
5. Липницкий В.А., Спичкова Н.В. Прикладная математика и теория норм синдромов. Минск, 2011.
6. Курилович А.В., Липницкий В.А., Михайловская Л.В. // Технологии информатизации и управления. 2011. Вып. 2. С. 43–49.
7. Липницкий В.А., Олексюк А.О. // Докл. БГУИР. 2014. № 8 (86). С. 72–78.
8. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М., 1986.
9. Олексюк А.О., Липницкий В.А. Устройство декодирования для коррекции четырехкратных ошибок. Заявка на изобретение № А20130054.