УДК 621.391.14

ЦИКЛОТОМИЧЕСКИЕ КЛАССЫ В НОРМЕННОМ ДЕКОДИРОВАНИИ БЧХ-КОДОВ

З.Н. ХОАНГ, В.К. КОНОПЕЛЬКО

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

Поступила в редакцию 5 февраля 2013

Рассмотрено норменное декодирование БЧХ-кодов, корректирующих многократные ошибки на основе циклотомических классов с основными, зависимыми и дополняющими нормами синдромов. Установлено, что все нормы входят в полные циклотомические классы. Рассматривается применение последовательной и параллельно-последовательной обработки объединенных циклотомических классов для идентификации образующих векторов ошибок.

Ключевые слова: образующий вектор ошибок $E_{\text{обр}}$, норма синдромов *N*, объединенные циклотомические классы норм.

Введение

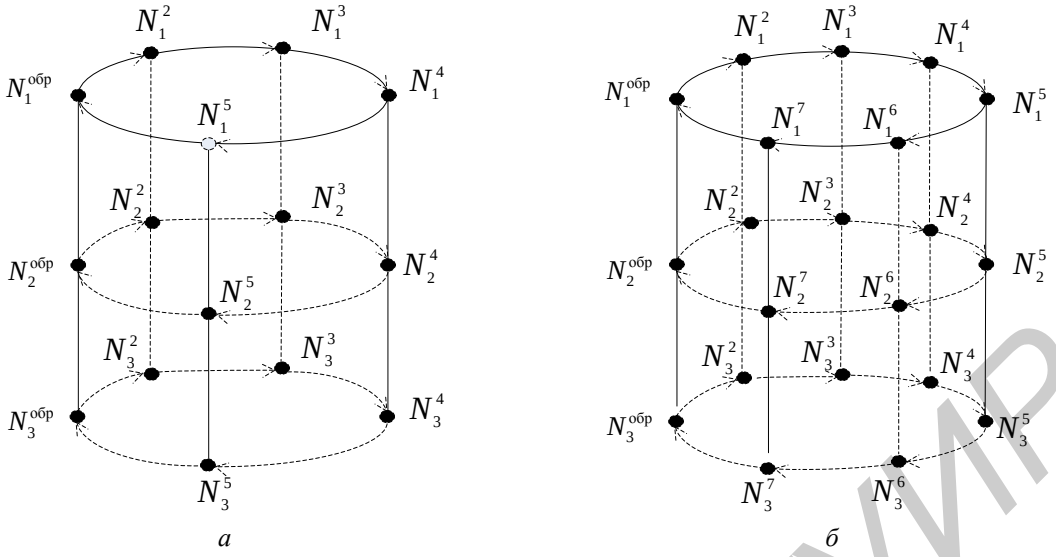
За последнее десятилетние в теории кодирования успешно развивается новое направление – норменное декодирование, благодаря которому снижаются затраты на реализацию селектора при коррекции многократных ошибок [1–3]. В [3, 4] для уменьшения сложности селектора при коррекции ошибок кратности $t = 2$ предлагается использование циклотомических классов норм. В данной статье исследуется множество норм синдромов ошибок кратности $t = 3 \div 7$ и их применение для идентификации образующих векторов ошибок на основе циклотомических перестановок норм синдромов.

Норменное декодирование на основе циклотомических классов с основными и зависимыми нормами

Определение 1. Объединенный циклотомический класс (ОЦКК) – множество, содержащее два или более элементов (норм синдромов), каждое из которых относится к множеству циклотомических перестановок.

Множество норм синдромов (1; 1; 29), (2; 2; 27), (4; 4; 23), (8; 8; 15), (16; 16; 30) является ОЦКК, где первый, второй элементы принадлежат циклотомическому классу (1; 2; 4; 8; 16), а третий элемент – классу (29; 27; 23; 15; 30) на длине $n = 31$. На рис. 1 представлены ОЦКК для норм синдромов БЧХ-кодов (31; 16) и (127; 106), корректирующих ошибки кратности $t = 3$.

Для того, чтобы выяснить, что все нормы БЧХ-кодов входят в ОЦКК был приведен вычислительный эксперимент, который включает следующие этапы: выбор первого образующего вектора ошибок с координатами $E = (x, y, ..., z)$ и соответствующими нормами $(N_1, N_2, ..., N_i)$; формирование первого ОЦКК (состоящего из 5 или 7 элементов для кодов $n = 31; 127$ и соответствующими образующими векторами ошибок); нахождение аналогичным образом других ОЦКК путем нахождения 2-ого (и следующих) образующего вектора ошибок, не принадлежащих предыдущим векторам ошибок 1-ого (предыдущих) класса, и соответствующие им нормы, до тех пор пока не исчерпается все множество образующих векторов ошибок.



а *б*

Рис. 1 Объединенные циклотомические классы для норм синдромов с $t = 3$
а – БЧХ-кода $(31;16)$; *б* – БЧХ-кода $(127;106)$

На рис. 2 приведен алгоритм нахождения объединенных циклотомических классов, где L – число образующих векторов ошибок, m – число элементов в циклотомическом классе.

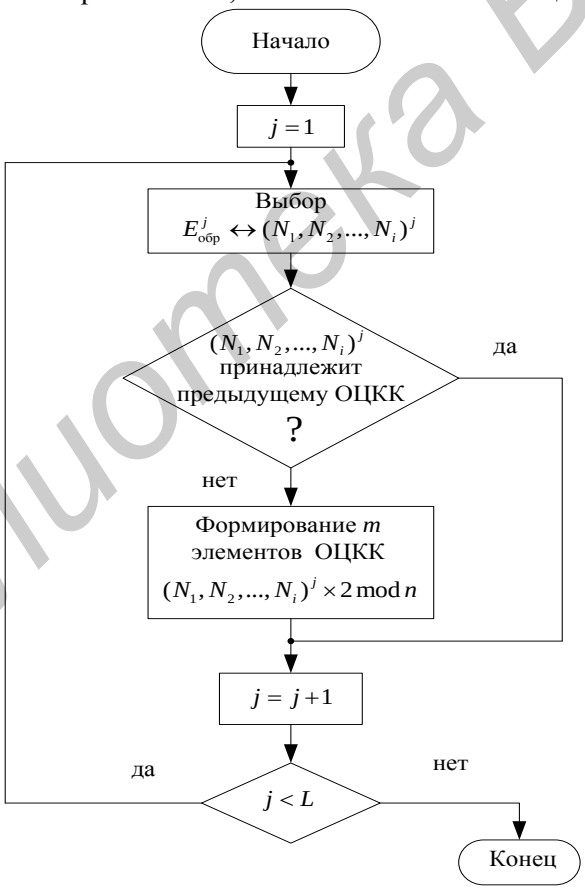


Рис. 2 Алгоритм нахождения объединенных циклотомических классов норм синдромов

Анализ данных результатов вычислительных экспериментов для БЧХ-кодов, корректирующих ошибок кратности $t = 3; 4; 5; 6; 7$ показал, что объединенные циклотомические классы охватывают все множество образующих векторов ошибок и удовлетворяют *определению* 1. Например, для БЧХ-кода с длиной $n = 31$, корректирующего ошибки кратности $t = 3$ имеется 29 объединенных циклотомических классов, каждый из которых содержит по 5 элементов

(каждый из 26 элементов содержит 2 основные (N_1, N_2) нормы и одну зависимую N_3 норму, а три циклотомических класса определяются только одной нормой N_1, N_2, N_3).

На рис. 3 для БЧХ-кода $(31;16)$, корректирующего ошибки кратности $t=3$, приведено распределение норм синдромов по ОЦКК.

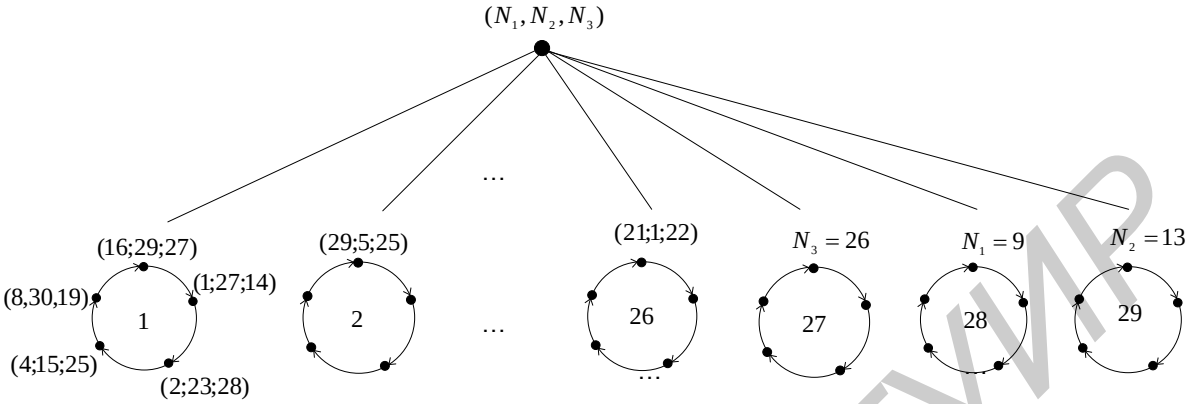


Рис. 3 Распределение норм синдромов по объединенным циклотомическим классам для БЧХ-кода $(31;16)$, корректирующего ошибки кратности $t=3$

При коррекции ошибок кратности $t=4$ БЧХ-кодом с длиной $n=31$ имеется 203 объединенных циклотомических класса, содержащих по 5 элементов (каждый из 175 содержит 3 основные (N_1, N_2, N_3) нормы и три зависимые нормы (N_4, N_5, N_6), и по 7 классов, содержащих нормы (N_4, N_5, N_6), (N_2, N_3, N_5), (N_1, N_3, N_6), (N_1, N_2, N_4) соответственно).

На рис. 4 приведены результаты исследований по распределению норм синдромов для БЧХ-кода, корректирующего ошибки кратности $t=5$ ($N_1 - N_4$ – основные нормы, $N_5 - N_{10}$ – зависимые нормы).

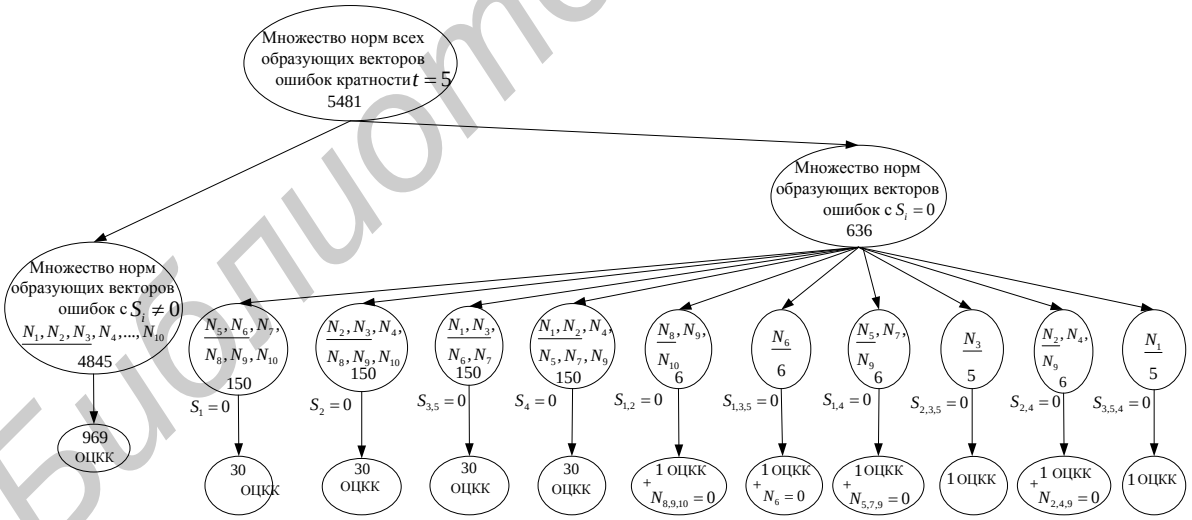


Рис. 4 Распределение норм в ОЦКК для кода длины $n=31$, корректирующего ошибки кратности $t=5$

Следует отметить, что в качестве образующих норм ОЦКК можно выбирать любой из элементов данного класса, позволяющих получить нужные свойства для синтеза селектора.

Идентификация образующих векторов ошибок с помощью объединенных циклотомических классов

Известно, что если занести элементы циклотомического класса в регистр сдвига с обратной связью, то в процессе осуществления сдвигов в нем формируются все элементы цик-

лотомического класса. Если проводить сравнение вычисленных норм синдромов со значениями всех образующих нормы ОЦКК, а затем с их сдвигами, то можно установить образующий вектор ошибок $E_{\text{обр}}$. Это свойство и используется в последовательном методе обработки ОЦКК, основанном на нижеследующем правиле декодирования.

1. Вычисленные значения норм синдромов $(N_1, N_2, ..., N_i)$ сравниваются со значениями первого элемента (образующего) ОЦКК ($(N_1, N_2, ..., N_i)^{\text{выч}} \equiv (N_1, N_2, ..., N_i)^1$). Если эти значения совпали, то это указывает на образующий вектор ошибок $E_{\text{обр}}$ данного ОЦКК. Тогда из ПЗУ-2 образующих векторов ошибок извлекается соответствующий вектор $E_{\text{обр}}$.

2. Если совпадения не произошло, то нормы в регистрах сдвига с обратной связью сдвигаются и повторяется п. 1 правила.

3. Если элементы норм не принадлежат первому ОЦКК, то переходим ко второму ОЦКК и повторяем п. 1, 2 правила и т.д., пока в блоке сравнения не произойдет совпадения.

На рис. 5 приведена структурная схема идентификатора образующих векторов ошибок $E_{\text{обр}}$, реализующего приведенное выше правило для $t = 3$.

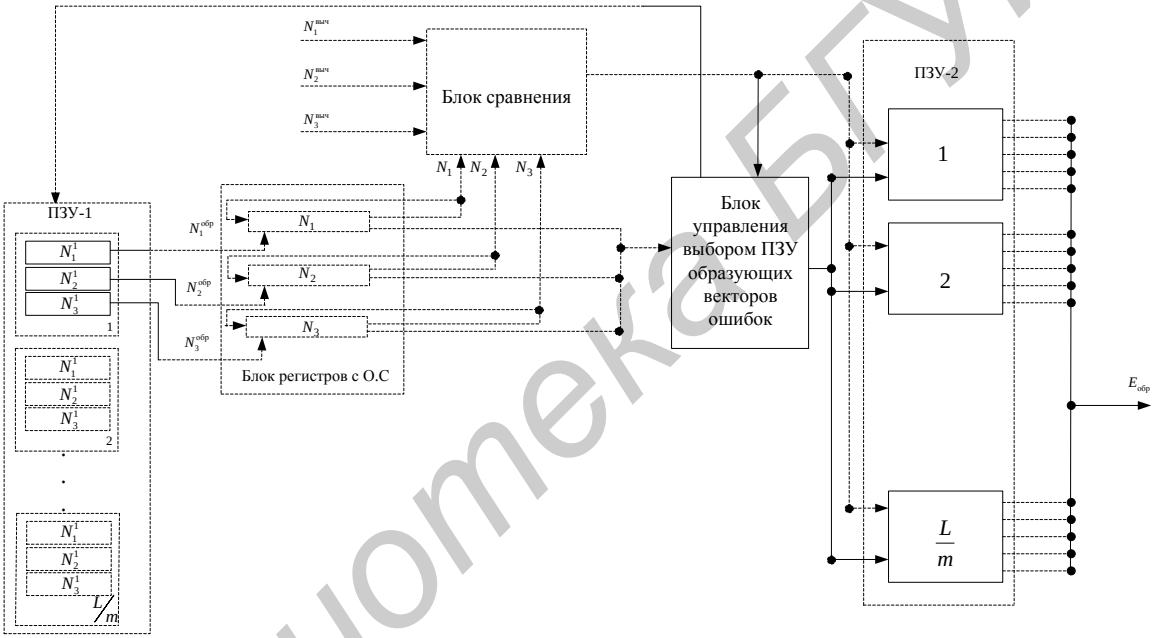


Рис. 5 Структурная схема последовательного идентификатора образующих векторов ошибок $E_{\text{îáð}}$ при коррекции ошибок кратности $t = 3$

Идентификатор состоит из двух ПЗУ (в ПЗУ-1 хранятся образующие нормы ОЦКК $(N_1, N_2, ..., N_i)$, в ПЗУ-2 хранятся образующие вектора ошибок $E_{\text{обр}}$), блока регистров с обратными связями (где формируются все элементы выбранного ОЦКК), блока сравнения вычисленных норм $(N_1, N_2, ..., N_i)^{\text{выч}}$ с нормами выбранного ОЦКК $(N_1, N_2, ..., N_i)^j$, $j = 1, 2, ..., L/m$, где L - число образующих векторов ошибок, m – число элементов в циклотомическом классе (для $n = 31, t = 3$, $L = 145$, $m = \lfloor \log_2 n \rfloor = 5$) и блока управления для выбора соответствующих кодов в ПЗУ-1 и ПЗУ-2 и сдвигов информации в блоке регистров (данный блок может состоять из счетчика, дешифратора и других логических элементов).

Идентификатор работает следующим образом. Из ПЗУ-1 в блок регистров загружаются образующие нормы синдромов $(N_1, N_2, ..., N_i)^1$ первого ОЦКК, которые сравниваются в блоке сравнения с вычисленными нормами $(N_1, N_2, ..., N_i)^{\text{выч}}$. При совпадении этих норм выбирается первое слово $E_{\text{обр}}$ из первого блока ПЗУ-2. Если совпадения не произошло, то в блоке управления значение счетчика увеличивается на единицу и происходит сдвиг норм в блоке реги-

стров. Благодаря этому формируются следующие элементы ОЦКК, которые вновь сравниваются с вычисленными нормами. Если через m тактов (для кода $n=31$, $m=5$) совпадения не произошло, то из ПЗУ-1 в блок регистров загружаются образующие нормы для второго ОЦКК (3-его и т.д.,), происходит сравнение с вычисленными нормами и т.д., пока не произойдет совпадения вычисленных норм с нормами ОЦКК. Очевидно, что последовательная обработка ОЦКК по сравнению с последовательной обработкой всего множества образующих норм уменьшает емкость ПЗУ-1 примерно в m раз. Например, при применении кода с $n=31$, $t=3$, исходная емкость ПЗУ-1 состоит из $t\times m\cdot L=3\cdot 5\cdot 145=2175$ ячеек памяти, а при применении ОЦКК - $t\times m=3\times 145=435$ ячеек.

В таблице приведена зависимость емкости ПЗУ-1 от длины кода n и числа корректируемых ошибок t при использовании последовательной обработки множества ОЦКК – Q^*. Для сравнения приведена сложность последовательного идентификатора Q [3, 4].

Таблица 1. **Зависимость емкости ПЗУ-1 от длины кода *n* и числа корректируемых ошибок *t***

Кратность ошибок t / Длина кода n		3	4	5	6	7
$n=31$	Q^*_{31}	435	6090	54810	356265	1781325
	Q_{31}	2175	30450	274050	1781325	8906625
$n=127$	Q^*_{127}	7875	488250	≈ 20 Мб	≈ 610 Мб	≈ 14,7 Гб
	Q_{127}	55125	3417750	≈ 140 Мб	≈ 4,2 Гб	≈ 102 Тб
$n=511$	Q^*_{511}	129795	≈ 33 Мб	≈5,5 Гб	≈ 704 Гб	≈ 71 Тб
	Q_{511}	1168155	≈ 296 Мб	≈ 50 Гб	≈ 6,3 Тб	≈ 640 Тб

Анализ данных таблицы показывает, что емкость ПЗУ-1 при реализации известным методом велика уже при $n\geq 128, t\geq 5$. Например, при $n=511$, $t=5$ емкость ПЗУ-1 примерно равна ≈ 50 Гб, а при $t=6$ ≈ 6,3 Тб. При применении декодирования с ОЦКК сложность ПЗУ-1 уменьшается в 9 раз до ≈ 5,5Гб и ≈ 704 Гб для $t=5,6$ соответственно.

Последовательная обработка ОЦКК, очевидно, приводит к низкому быстродействию устройства декодирования. Для увеличения быстродействия можно использовать параллельно-последовательную обработку ОЦКК. В этом случае происходит одновременное сравнение вычисленных норм со всеми образующими нормами ОЦКК. Для этого необходимо введение L блоков регистров с обратной связью. В отличие от вышеприведенной схемы последовательного декодирования в ПЗУ-1 хранятся только образующие нормы каждого ОЦКК (при этом происходит увеличение в *L/m* числа блоков сравнения при увеличении быстродействии в *L/m* раз, т.е., наблюдается обменный характер – увеличение числа блоков сравнения на соответствующий рост быстродействия за счет уменьшения числа тактов для обработки информации.

Норменное декодирование на основе циклотомических классов с основными и дополняющими нормами

В вышерассмотренных разделах проведен анализ основных и зависимых норм на предмет их разбиении в ОЦКК. Однако поскольку их число значительно больше числа основных и дополняющих (при одинаковом числе образующих векторов $E_{\text{обр}}$) [5, 6], то были проведены исследования на предмет вхождения этих норм в ОЦКК, а также являются ли они полными (к неполным ОЦКК относят циклотомические классы, содержащие не все элементы). Результаты исследований, проведенные на основе алгоритма рис. 2 показали, что для БЧХ-кода с $t=3\div 7$, $n=31,127$ в ОЦКК входят все множества основных и дополняющих норм. Так, например, при коррекции трехкратных ошибок БЧХ-кодом $(31;16;7)$ используются 130 основных (N_1,N_2) и 5 (N_1), 5 (N_2), 5 (N_3) дополняющих норм, которые разделяются на 26 (N_1,N_2) и по одному для (N_1), (N_2), (N_3) ОЦКК соответственно. При коррекции четырехкратных ошибок БЧХ-кодом $(31;11;9)$ используются 875 основных норм (N_1,N_2,N_3), и 35 (N_4,N_5), 35 (N_2,N_3),

35 (N_1, N_3), 35 (N_1, N_2) дополняющих норм, которые разделяются на 175, 7, 7, 7, 7 ОЦКК соответственно. Аналогично при коррекции ошибок кратности $t = 5$ БЧХ-кодом $(31;11)$, корректирующим ошибки кратности $t = 5$, множество основных и дополняющих норм разделяются на 969 основных (N_1, N_2, N_3), по 30 циклотомических классов (N_2, N_3), (N_1, N_3), (N_1, N_2), (N_5, N_6) ОЦКК и по одному ОЦКК N_8, N_6, N_5, N_3, N_2, N_1 (подчеркнутые нормы из рис. 4). Основные и дополняющие нормы при коррекции ошибок кратности $t = 6;7$ также разделяются на полные ОЦКК.

Анализ данных результатов показывает, что число ОЦКК остается одним и тем же при меньшем числе вычисляемых норм для $t \geq 4$. Однако для идентификации не используется часть норм, и кроме того, при данном выборе норм при $S_i = 0$ не требуется вычислять нормы (N_4, N_7, N_9, N_{10}). Это позволяет примерно в 2 раза уменьшить число идентификационных параметров (норм).

При построении идентификаторов $E_{\text{обр}}$ на основе ОЦКК с основными и дополняющими нормами также могут быть использованы последовательный и параллельно-последовательный методы декодирования, дополненные блоком анализа синдромов $(S_1, S_2, ..., S_i)$ на нуль $(S_1 = 0, S_2 = 0, ..., S_i = 0)$. Если значения вычисленных норм совпадают со значениями норм при $S_1 = S_2 =, .., S_i \neq 0$, то по значению основных норм, аналогично алгоритму, представленному на рис. 5, происходит нахождение образующего вектора ошибок $E_{\text{обр}}$; в противном случае, когда $S_i = 0$, $E_{\text{обр}}$ находится по значению основных и дополняющих норм, используемых для идентификации в меньшем количестве.

Поскольку для нахождения $E_{\text{обр}}$ в ОЦКК используется меньшее число объединенных норм, это приводит к уменьшению разрядности хранимых в ПЗУ-1 слов. Это приводит к уменьшению сложности ПЗУ-1, блока регистров и блоков сравнения.

В таблице приведена зависимость емкости ПЗУ-1 Q^{**} от кратности корректируемых ошибок t и длины кода n (Q^{*} – сложность последовательного циклотомического идентификатора при использовании основных и зависимых норм).

Таблица 2. **Зависимость емкости ПЗУ-1 от длины кода *n* и числа корректируемых ошибок *t* при последовательной обработке ОЦКК**

Кратность ошибок t / Длина кода n		3	4	5	6	7
$n = 31$	Q^{*}_{31}	435	6090	54810	356265	1781325
	Q^{**}_{31}	275	3445	15801	91309	325795
$n = 127$	Q^{*}_{127}	7875	488250	≈ 20 Мб	≈ 610 Мб	≈ 14,7 Гб
	Q^{**}_{127}	5187	241464	≈8 Мб	≈ 200 Мб	≈ 4,2 Мб
$n = 511$	Q^{*}_{511}	129795	≈ 33 Мб	≈5,5 Гб	≈ 704 Гб	≈ 71 Тб
	Q^{**}_{511}	86530	≈ 15 Мб	≈ 2 Гб	≈ 234 Гб	≈ 17 Тб

Анализ данных табл. 2 показывает, что при использовании основных и дополняющих норм ОЦКК сложность последовательного циклотомического идентификатора, которая в основном определяется емкостью ПЗУ-1, в более чем 2 и 4 раз меньше сложности норменного последовательного циклотомического идентификатора на основе основных и зависимых норм при идентификации образующих векторов ошибок кратности $t = 4$ и $t = 7$ БЧХ-кодом с $n = 511$ соответственно.

Заключение

Дано определение объединенных циклотомических классов. Показано, что все нормы БЧХ-кодов входят в полные объединенные циклотомические классы. Предложена идентификация с последовательной обработкой объединенных циклотомических классов, позволяющая

в m раз уменьшить сложность идентификатора по сравнению с последовательной норменной обработкой (m – число элементов в циклотомическом классе). Рассмотрена параллельно-последовательная идентификация на основе объединенных циклотомических классов, обеспечивающая в L/m раз увеличить быстродействие работы идентификатора (L -число образующих векторов ошибок). Показано, что идентификация с использованием основных и дополняющих норм позволяет в разы уменьшить сложность идентификатора по сравнению с идентификацией на основе основных и зависимых норм БЧХ-кодом для $n = 511$ при коррекции $t = 4$ и $t = 7$ соответственно.

CYCLOTOMIC CLASSES IN THE NORMING DECODING BCH-CODES

D.N. HOANG, V.K. KONOPELKO

Abstract

Norming decoding based on cyclotomic classes with main and subordinate norms is exanimated. It was found that all the norms of BCH codes and their error vector generators are the parts of complete cyclotomic classes. Identification of the error vectors generators with serial and parallel-serial processing of combined cyclotomic classes is proposed.

Список литературы

1. *Колесник. В. Д, Мирончиков Е.Т.* Декодирование циклических кодов М., 1968.
2. *Питерсон, У., Уэлдон, Э.* Коды, исправляющие ошибки. М., 1976
3. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск, 2004.
4. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
5. *Конопелько В.К., Хоанг Н.З.* // Докл. БГУИР. 2012. № 8 (70). С. 69–74.
6. *Хоанг З.Н., Конопелько В.К. , Макейчик Е.Г.* // Матер. Междунар. науч.-техн. семинара «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных». Минск, январь – декабрь 2012 г. С. 27–31.