УДК 621.391

# ПРОЕКТИРОВАНИЕ УСТРОЙСТВ ОБРАБОТКИ МОДИФИКАЦИЙ КОДОВ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА НА ОСНОВЕ РАЗДЕЛЕНИЯ ОШИБОК НА КЛАССЫ

Власова Г.А.

Белорусский государственный университет информатики и радиоэлектроники,
Минск, Республика Беларусь, g.vlasova@bsuir.by

Аннотация: рассмотрены алгоритмы и устройства пошаговой и параллельной обработки модификаций кодов Боуза-Чоудхури-Хоквингема. На примере кодов, корректирующих одиночные и двойные независимые ошибки, показано, что разделение ошибок на классы позволяет уменьшить сложность селектора: пропорционально кратности корректируемых ошибок при пошаговом декодировании и пропорционально длине кода при параллельном декодировании. На основе разделения ошибок на классы с использованием программного обеспечения Logisim разработаны устройства декодирования, оценены их сложность и быстродействие.

Ключевые коды Боуза-Чоудхури-Хоквингема, классы ошибок, параметры идентификации, устройства декодирования.

## I. ВВЕДЕНИЕ

Увеличение объемов и скоростей передаваемой информации приводит к усложнению помеховой обстановки. В этой связи растет запрос на обнаружение, идентификацию и коррекцию ошибок в сообщениях, передаваемых в пространстве (связь) и во времени (хранение). Эффективным средством борьбы с помехами и обеспечения сохранности информации является помехоустойчивое кодирование [1,2]. При этом требуется обеспечить контроль ошибок все большей кратности с приемлемыми аппаратными и временными затратами.

## II. РАЗДЕЛЕНИЕ ОШИБОК НА КЛАССЫ

Среди всего многообразия известных кодов, контролирующих ошибки, широкое применение находят коды Боуза-Чоудхури-Хоквингема (БЧХ) [1,2]. Данные коды исправляют кратные ошибки и относятся к циклическим. Линейный код называется циклическим, если циклический сдвиг кодового слова также принадлежит коду [1,2]. В [3,4] было показано, что все ошибки можно разделить на классы, характеризующиеся весом ошибок (количеством ошибочных разрядов в кодовой последовательности) и расстоянием между ошибочными разрядами. Например, ошибки в разрядах $(0,1)$, $(1,2)$, $(2,3)$, …, $((n-1),0)$, где $n$ – длина слова, относятся к одному классу двойных ошибок. Таким образом, все множество двойных ошибок объемом $n(n-1)/2$ можно разделить на $(n-1)/2$ не пересекающихся класса. Очевидно, что одиночные ошибки образуют один класс. Для тройных ошибок количество классов равно $(n-1)(n-2)/6$ и т.д. Ниже будет показано, какие преимущества дает разделение ошибок на классы при проектировании устройств обработки БЧХ-кодов.

Поскольку рассматриваемые коды относятся к циклическим, алгоритмы их обработки можно разделить на параллельные (в том числе прямые табличные) и пошаговые [2].

## III. УСТРОЙСТВА ПОШАГОВОГО ДЕКОДИРОВАНИЯ КОДОВ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

Согласно [2] обобщенная структурная схема декодера циклического кода содержит буферный регистр, в который за $n$ тактов записывается анализируемая последовательность. Одновременно кодовое слово поступает в контрольное устройство, представляющее собой устройство деления на порождающий полином кода. За $n$ тактов в контрольном устройстве происходит вычисление синдрома (т. е. остатка от деления принятой последовательности на порождающий полином). Ненулевой синдром является признаком ошибки, по виду синдрома можно идентифицировать ошибку. Селектор выдает корректирующий сигнал в тот момент, когда ошибочный символ покидает буферный регистр. Коррекция ошибок происходит за $2n$ тактов. Сложность реализации устройства определяется сложностью селектора, который должен обеспечить коррекцию всех возможных ошибок. Так, для коррекции одиночных и двойных независимых ошибок необходимо селектировать $n+n(n-1)/2$ синдромов. Используя теорему Меггитта, можно в качестве селектируемых использовать только синдромы тех ошибок, в которых один из ошибочных символов расположен в старшем разряде [2]. Число таких комбинаций для одиночных и двойных ошибок составляет $1+(n-1)$. Декодирование по-прежнему происходит за $2n$ тактов. В схеме декодера Меггитта с модификацией синдрома (с вылавливанием ошибок) достаточно селектировать в два раза меньше синдромов двойных ошибок,

однако, коррекция ошибок при этом занимает $3n$ тактов [2]. Кроме того, метод вылавливания ошибок применим только к низкоскоростным кодам, а подобные коды редко применяются на практике.

Разделение ошибок на классы и использование модификации синдрома позволяет реализовать исправление двойных ошибок не более чем за $2{,}5n$ тактов при сокращенном числе селектируемых комбинаций [3]. Достаточно селектировать синдромы образующих классов ошибок, число которых при исправлении одиночных и двойных ошибок совпадает с числом комбинаций, селектируемых в декодере Меггитта с вылавливанием ошибок. Дополнительно уменьшить время декодирования позволит использование реверсивных однородных кодов, которые относятся к модифицированным кодам БЧХ. Однако при этом возрастут аппаратные затраты поскольку устройство должно состоять из двух каналов [5].

Разработана схема одноканального устройства декодирования реверсивного БЧХ-кода длины 31, корректирующего одиночные и двойные ошибки, с использованием разделения ошибок на классы [5]. Сложность одноканального устройства составляет не более 835 условных логических элементов GE (Gate Equivalent, единица измерения для определения размеров микросхем; площадь, занимаемая универсальным двухвходовым логическим элементом – элементом NAND с двумя входами [6]). Такая реализация устройства называется «ультралегкой», поскольку требует менее 1000 GE. Моделирование работы схемы с использованием программного обеспечения Logisim подтвердило, что коррекция всех возможных одиночных и двойных ошибок происходит не более, чем за $2{,}5n$ тактов.

## IV. УСТРОЙСТВА ПАРАЛЛЕЛЬНОГО ДЕКОДИРОВАНИЯ КОДОВ БОУЗА-ЧОУДХУРИ-ХОКВИНГЕМА

При необходимости минимизации временных затрат на исправление ошибок, декодирование реализуется по параллельным алгоритмам. В этом случае синдром определяется как произведение принятого кодового слова $X$ на проверочную матрицу $H^T$. Затем селектор по виду синдрома определяет вид ошибки. Коррекция поступившего сообщения реализуется путем суммирования по модулю два вектора ошибки с декодируемым словом [1,2]. Основные аппаратные затраты приходятся на селектор, реализуемый на запоминающем устройстве.

Разделение ошибок на классы позволяет в $n$ раз сократить количество хранимых векторов одиночных и двойных ошибок. Можно показать, что каждый класс характеризуется не только весом ошибки и расстоянием между ошибочными разрядами, но и параметром идентификации $N$, определяемым видом проверочной матрицы кода [3]. Например, реверсивный БЧХ-код, корректирующий две независимые ошибки, задается проверочной матрицей вида $H = (\alpha^i, \alpha^{-i})^T$ , где $\alpha$ – примитивный элемент поля Галуа $GF(2^m)$, $m \geq 3$, $0 \leq i \leq (n-1)$, $n = (2^m - 1)$ [8]. При декодировании вычисляется значение синдрома $S = XH^T = (\alpha^p, \alpha^q)$ и параметр идентификации $N = (p+q) mod (2^m - 1)$ [3,7]. По значению параметра идентификации определяется образующий класса, которому соответствует синдром $S_0 = X_0 H^T = (\alpha^{p0}, \alpha^{q0})$. По значению сдвига $(p - p0) mod (2^m - 1)$ определяется фактическая ошибка [7]. Данный алгоритм декодирования можно применить к модифицированным БЧХ-кодам, предложенным в [9]. В данной работе показано, что перестановка в лексикографическом порядке столбцов проверочной матрицы реверсивного БЧХ-кода позволяет дополнительно к одиночным и двойным независимым ошибкам корректировать одиночные модули ошибок длины четыре и пакеты ошибок длины три.

Разработано устройство декодирования модифицированного БЧХ-кода длины 128 с дополнительными корректирующими возможностями по контролю модульных и пакетных ошибок. Сложность устройства составляет 9500 GE. Быстродействие определяется максимальным числом последовательно соединенных элементов схемы и составляет 31. Максимальную задержку вносит идентификация и коррекция двойной независимой ошибки. Схема, реализующая данный алгоритм, представлена на рисунке 1.

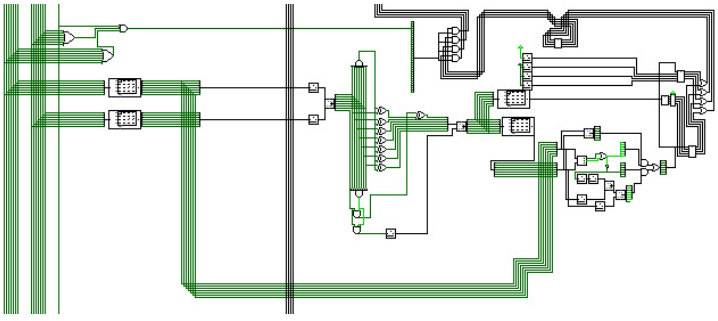

Рисунок 1. Идентификация и коррекция двойной ошибки модифицированным (128; 113)-кодом БЧХ

## V. ЗАКЛЮЧЕНИЕ

Разделение ошибок на классы позволяет значительно снизить аппаратные затраты при проектировании устройств обработки циклических помехоустойчивых кодов. Для БЧХ-кодов, корректирующих одиночные и двойные независимые ошибки, сложность селектора уменьшается в два раза при пошаговой обработке, при этом на 16% снижаются временные затраты на декодирование. Кроме того, данный алгоритм применим не только к низкоскоростным кодам. При параллельном декодировании сложность селектора может быть уменьшена пропорционально длине кода. Кроме того, алгоритм декодирования, основанный на вычислении и анализе параметра идентификации класса ошибок, позволяет применить в схеме запоминающие устройства с меньшей разрядностью адреса и данных, что также повышает быстродействие. Данный алгоритм можно использовать при разработке устройств обработки модифицированных БЧХ-кодов с дополнительными корректирующими возможностями. Следует отметить, что метод разделения на классы может быть применен при проектировании устройств коррекции независимых ошибок кратности больше двух.

## ЛИТЕРАТУРА

[1] Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования: методы, алгоритмы, применение / Р. Морелос-Сарагоса. М.: Техносфера, 2005. 320 с.

[2] Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. М.: Мир, 1986. 576 с.

[3] Власова, Г. А. Разработка методов и устройств идентификации и коррекции ошибок кодами Боуза – Чоудхури – Хоквингема: автореф. дис. … канд. техн. наук : 05.12.21 / Г. А. Власова; Белор. гос. ун-т информатики и радиоэлектроники. Минск, 1996. 18 с.

[4] Устройство декодирования для коррекции двойных ошибок : пат. Респ. Беларусь 3907 / В. К. Конопелько, Г. А. Власова. – Опубл. 14.12.2000

[5] Власова, Г.А. Устройства пошагового декодирования кодов Боуза-Чоудхури-Хоквингема / Г. А. Власова // Материалы Восьмого Белорусского космического конгресса: в 2 т. Минск: ОИПИ НАН Беларуси, 2022. Том 1. с.141-144.

[6] Жуков, А.Е. Легковесная криптография. Часть 1. / А.Е. Жуков // Вопросы кибербезопасности. 2010. №1(9). С. 26-46.

[7] Власова, Г.А. Устройство декодирования реверсивных кодов Боуза-Чоудхури-Хоквингема с дополнительными корректирующими возможностями для контроля целостности информации / Г. А. Власова // Материалы XXVI научно-практической конференции «Комплексная защита информации». Минск: Издатель Владимир Сивчиков, 2021. с.240-242.

[8] Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. М.: Связь, 1979. 744с.

[9] Липницкий, В. А. Двоичные реверсивные коды для контроля байтовых ошибок / В. А. Липницкий, В. К. Конопелько, Г. А. Власова, А. Н. Осипов // Известия национальной академии наук Беларуси. Серия физико- математических наук. 2000. №1. С. 127-131.

## DESIGN OF DEVICES FOR PROCESSING BOSE-CHAUDHURI-HOCQUENGHEM CODES MODIFICATIONS BASED ON DIVIDING ERRORS INTO CLASSES

G. Vlasova

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus,
g.vlasova@bsuir.by

Abstract: algorithms and devices for step-by-step and parallel processing of Bose-Chaudhuri-Hocquenghem codes modifications are considered. Using the example of codes that correct single and double independent errors, it is shown that dividing errors into classes can reduce the complexity of the selector: proportional to the multiplicity of corrected errors during step-by-step decoding and proportional to the code length during parallel decoding. Based on the division of errors into classes using Logisim software, decoding devices were developed, their complexity and performance were assessed.

Keywords: Bose-Chaudhuri-Hocquenghem codes, error classes, identification parameters, decoding devices.