

**Белорусский государственный университет
Механико-математический факультет
Кафедра дифференциальных уравнений и системного анализа**

**Аннотация к магистерской диссертации
“Теоретико-групповые методы в помехоустойчивом кодировании”**

Фомич Екатерина Александровна

руководитель Липницкий Валерий Антонович

2019

Диссертация состоит из 6 глав и 7 приложений.

В магистерской диссертации 96 страниц, 11 таблиц, 14 источников, 7 приложений.

Ключевые слова: ТЕОРИЯ ГРУПП, ПОМЕХОУСТОЙЧИВОЕ КОДИРОВАНИЕ, ЛИНЕЙНЫЙ КОД, МИНИМАЛЬНОЕ РАССТОЯНИЕ, АВТОМОРФИЗМЫ ЛИНЕЙНЫХ КОДОВ, КОДЫ ХЕММИНГА, БЧХ-КОДЫ, КВАДРАТИЧНО-ВЫЧЕТНЫЕ КОДЫ, ТЕОРИЯ НОРМ СИНДРОМОВ.

В магистерской диссертации изучается применение групп автоморфизмов кодов к коррекции ошибок этими кодами, основные свойства квадратично-вычетных кодов, взаимосвязь с обобщенными БЧХ-кодами, корректирующие возможности, развиваются норменный и полиномиально-норменный алгоритмы коррекции многократных ошибок квадратично-вычетными кодами.

Цель магистерской диссертации – изучить и применить теоретико-групповые методы для коррекции ошибок кодами Хемминга, БЧХ-кодами и квадратично-вычетными кодами.

В магистерской диссертации получены следующие результаты:

- 1) Описаны условия для параметров квадратично-вычетных кодов и способы их построения, дан ряд примеров
- 2) Раскрыта взаимосвязь КВ-кодов с кодами БЧХ
- 3) Проанализированы корректирующие возможности КВ-кодов по сравнению с кодами других типов с аналогичными параметрами
- 4) Изучены группы автоморфизмов кодов и показано, как они применяются для коррекции ошибок этими кодами
- 5) Изучена теория норм синдромов для БЧХ кодов и применена к квадратично-вычетным кодам

- 6) Разработан и реализован в пакете Mathematica алгоритм норменного декодирования для квадратично-вычетного кода длиной 31
- 7) Разработан алгоритм полиномиально-норменного декодирования многократных ошибок для квадратично-вычетного кода длиной 31
- 8) Продемонстрировано, как с помощью циклотомических классов находить полиномиальные инварианты, применяемые в полиномиально-норменном методе

Новизна результатов состоит в разработке и реализации норменного и полиномиально-норменного методов декодирования ошибок квадратично-вычетными кодами.

Магистерская диссертация носит практический характер. Ее результаты могут применяться при разработке средств защиты информации от помех.

Все результаты магистерской диссертации доказаны в соответствии с принятыми в математике правилами и обоснованы сформулированными в работе теоремами.

Магистерская диссертация выполнена автором самостоятельно.

The master thesis is presented in the form of an explanatory note of 96 pages, 11 tables, 14 references, 7 applications.

Keywords: GROUP THEORY, ERROR-CORRECTING CODING, LINER CODE, MINIMUM DISTANCE, LINER CODE AUTOMORPHISM, HAMMING CODES, BCH CODES, QUADRATIC-RESIDUE CODES, THEORY OF SYNDROME NORMS.

The research object is to study and apply the Group-Theoretic Methods for error correcting using Hamming codes, BCH codes and quadratic-residue codes.

The main results of the master thesis are as follows:

- 1) Conditions for the parameters of quadratic-residue codes and methods for their construction are described, and a number of examples are given
- 2) The relationship of QR-codes with BCH-codes is described
- 3) Correcting capabilities of QR-codes are analyzed in comparison with codes of other types with the same parameters
- 4) Automorphism groups of error-coding codes are studied and applied for error correction
- 5) The theory of syndrome norms for BCH-codes was studied and applied to quadratic-residue codes
- 6) The norm decoding algorithm for a quadratic-residue code of length 31 has been developed and implemented in the Mathematica package.
- 7) The polynomial-norm decoding algorithm for a quadratic-residue code of length 31 has been developed
- 8) Using of cyclotomic classes for finding polynomial invariants was demonstrated and explained

The novelty of the results consists in the development and implementation of the norm and polynomial-norm error decoding methods for quadratic-residue codes.

This master thesis is a practical one. Its results can be used for protecting information against noises.

All results of the master thesis are proved in accordance with the rules accepted in mathematics and are justified by the theorems formulated in the project.

The master thesis was done solely by the author.