УДК 519.725

Коды, исправляющие ошибки, и комбинаторные конструкции, основанные на полях Галуа.

Глухова М.Г., ГБОУ Лицей №64, г. СПб.

Научный руководитель – доктор технических наук, профессор кафедры автоматизированных систем специального назначения Военной академии связи им. С.М.Буденного г. СПб Чуднов Александр Михайлович

Поля Галуа играют важную роль как в фундаментальных разделах математики, так и в прикладных задачах, решение которых находит широкое применение в различных сферах практической деятельности людей. В настоящей работе излагаются свойства полей Галуа и принципы построения на их основе конечных геометрий, систем ортогональных латинских квадратов, а также кодов, корректирующих ошибки. Целью работы является изложение вопросов построения и использования полей Галуа на доступном языке для продвинутых учащихся старших классов и студентов, а также написание программ, моделирующих работу кодирующих и декодирующих устройств.

В настоящее время активно развивается вычислительная техника, поэтому появляются новые возможности по реализации алгоритмов для обработки информации. Новые алгоритмы повышают эффективность работы и улучшают функционирование систем. Развитие этого направления представляется весьма актуальным, так как является теоретической базой для совершенствования информационных систем. В настоящее время теория кодирования продолжает свое развитие, а методы теории кодирования широко используются во всех информационных системах и системах передачи информации.

Поле — это алгебраическая структура с операциями, которые аналогичны сложению и умножению. Эварист Галуа установил, что для любой степени простого числа существует поле порядка p^n, где n - натуральное. Поле порядка p строится как поле вычетов по модулю p, а p^n - как поле вычетов многочленов с коэффициентами из простого поля по модулю неприводимого многочлена.

Конечная геометрия — это геометрическая структура, содержащая конечное количество точек. Известные конечные геометрии построены на основе полей Галуа. Существует два вида конечных геометрий: аффинная и проективная. В аффинной используется Евклидово понятие параллельности прямых, а в проективной любые две прямые пересекаются в одной точке, и потому параллельных прямых нет. Для каждого вида имеются свои аксиомы.

На основе полей Галуа решаются задачи построения систем ортогональных латинских квадратов. Латинским квадратом порядка n называется (n×n) таблица (матрица), в которой каждая строка и столбец являются некоторыми перестановками чисел 1,2…n. Два латинских квадрата порядка n ортогональны, если при наложении одного из них на другой полученные ячейки все различны.

Коды, исправляющие ошибки в системах передачи информации, строятся над алфавитами, также являющимися полями Галуа. Кодом называется множество последовательностей длины M с компонентами из поля Галуа. Код может исправлять возникающие последовательности ошибки, если число этих ошибок менее половины расстояния Хемминга между ближайшими кодовыми последовательностями.

Наиболее важные результаты получены для алфавитов, являющимися конечными полями. В работе рассмотрены лишь двоичные случаи. Для пространств Хемминга над

полями Галуа получены эффективные код, исправляющие ошибки, широко применяемые в современных системах связи. Примером является совершенный код, исправляющий любую 1 ошибку в последовательности длины 7.

Из двоичных нетривиальных совершенных кодов, кроме кодов Хэмминга, известен лишь один совершенный код Голея, где передается последовательность длины 23 с числом информационных элементов 12, исправляющий до 3х ошибок.

Для иллюстрации применения кодов в работе составлены 2 программы, в каждой из которых представлены различные коды и методы декодирования, основанные на переборе множества возможных синдромов или всех информационных последовательностей.

Для кодов с хорошими исправляющими способностями известны аналоги в классе циклических кодов, где каждый циклический сдвиг снова является кодовым блоком. Для матрицы можно построить циклический аналог, содержащий одну первую строку, задаваемую так называемым проверочным многочленом кода. Остальные строки получены в результате циклических сдвигов данной строки.

В докладе рассмотрены два различных метода декодирования. Следует отметить, что наибольший эффект от кодирования достигается при использовании длинных кодов, для которых реализация переборных алгоритмов декодирования требует больших вычислительных ресурсов, что на практике не всегда возможно.

В работе показана важная роль полей Галуа в различных областях математики и их использование в прикладных научных сферах. Проанализировано значение этих вопросов для решения проблем конечных плоскостей, ортогональных латинских квадратов и кодов, исправляющих ошибки. Развитие этого направления представляется весьма актуальным, так как является теоретической базой для совершенствования информационных систем.

На настоящее время все приведенные в работе структуры построены только на основе конечных полей. При этом открытой в этой области остается проблема существования подобных конструкции над составными алфавитами, не являющимися полями Галуа.