

# **ОБ ОПРЕДЕЛЕНИИ МИНИМАЛЬНОГО РАССТОЯНИЯ НЕПРИМИТИВНЫХ КОДОВ ХЭММИНГА**

Л.В. Михайловская, Е.В. Валаханович

Современная информационная эпоха характеризуется всеобщей компьютеризацией и стремительным развитием телекоммуникационных средств.

Современные компьютерные технологии позволяют решать задачи, недоступные для решения ранее. Созданы пакеты MathCAD, MATLAB, Maple, Mathematica, разрабатываются современные их версии, рассчитанные на преодоление растущих объемов вычислений. Современные физика, генетика, средства защиты информации требуют освоения новых вычислительных сред, в частности, успешного проведения вычисления не только в рамках нулевой характеристики, но и переход к вычислениям в полях, характеристика которых конечна. Лишь новые версии пакета Mathematica содержат разделы, посвященные некоторым видам вычислений в полях положительной характеристики [1]. Однако потребности практики требуют существенного расширения этих вычислительных возможностей.

В докладе излагается опыт компьютерного формирования больших полей Галуа с предельно широким варьированием формирующих примитивных полиномов, практической организации вычислений в этих полях для решения различных задач помехоустойчивого кодирования.

В помехоустойчивом кодировании важное место занимают коды Хэмминга – циклические совершенные коды из класса BCH-кодов [2]. НепрIMITивные коды Хэмминга потенциально могут иметь минимальное расстояние больше трех. Конкретное определение расстояния связано с решением громоздкой переборной задачи и сопряжено с определенными проблемами организации компьютерных вычислений.

В докладе подводятся итоги систематического исследования непрIMITивных кодов Хэмминга на длинах от 9 до 99. Известно, что минимальное расстояние кода зависит от количества линейно-зависимых и линейно-независимых столбцов в проверочной матрице кода. Точное значение расстояния каждого рассматриваемого кода устанавливалось построением проверочной матрицы кода и исследованием систем ее столбцов на линейную зависимость.

Наиболее же удачным среди исследованных авторов кодов следует считать код Хэмминга  $C_x$ , задаваемый над полем  $GF(2)$ . Для этого кода точное значение минимального расстояния равно 15. Следовательно, данный код способен корректировать не только одиночные, но и любые ошибки кратностью до 7 включительно; всего 3200838655 ошибок, что в 40516945 раз больше количества корректируемых одиночных ошибок, исправление которых гарантировано конструктивным расстоянием кода Хэмминга  $C_x$ .

## Литература

1. Wolfram Research, Inc., System Modeler, Version 13.0.0. Champaign, IL. 2021.
2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск: Издательский центр БГУ, 2007. 240 с.