Секция «Математика и механика»

Построение быстрых эффективных кодов на эллиптических кривых

Ширяев Пётр Михайлович
Студент
Московский государственный университет имени М.В. Ломоносова,
Механико-математический факультет, Москва, Россия
E-mail: shiryaev.petr@gmail.com

Построение над полем характеристики 2 [15,7,8]-кода, исправляющего 3 ошибки.[5]
Алгоритм исправления ошибок и проверка его корректности для данного кода.[2,3,4]
Оценка количества арифметических операций для исправления ошибок.
Сравнение с БЧХ-кодами длины 15.[1,2]

Литература

1. Ричард Э. Блэйхут, “Быстрые алгоритмы цифровой обработки сигналов”, Л., 1988
2. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.. “Алгеброгеометрические коды. Основные понятия”, М.,2002.
3. Семеновых Д.Н. “О теоретико-числовых вопросах в теории кодирования”, диссертация, 59 стр., М., 2005.
4. Павлов Ю.М., “Декодирование алгеброгеометрических кодов”, дипломная работа, 13 стр., М., 2010.
5. Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato, “An elementary introduction to hyperelliptic curves”, Technical Report CORR 96-19, department of CO, University of Waterloo, Ontario, November 1996.