

Декодирование алгеброгеометрических кодов над гиперэллиптическими кривыми

Ширяев Пётр

ключевые слова: исправление ошибок, гиперэллиптическая кривая, пространство Римана–Роха

Одним из интересов теории передачи информации являются короткие помехоустойчивые коды над конечными полями характеристики 2. Алгеброгеометрические конструкции ([1], стр. 262-269) позволяют строить коды над гиперэллиптическими кривыми, которые имеют большую верхнюю границу длины кода, чем коды Рида–Соломона. Алгоритм декодирования, требующий знания базиса пространства Римана–Роха, был сформулирован и доказан С.Г. Влэдуцем и А.Н. Скоробогатовым в 1990 году [2]. В 2005г. Семеновых Д.Н. получил явный вид базиса пространства Римана–Роха приведённого дивизора ([3], Теорема 5), что позволяет рассматривать возможность практического применения алгеброгеометрических кодов.

В докладе будет изложен результат Семеновых о базисе пространства Римана–Роха, рассказан алгоритм декодирования и вычислена его сложность. Поскольку сложность значительно выше (при равных параметрах), чем для кодов Рида–Соломона, будут также изложены соображения о возможных оптимизациях алгоритма декодирования.

Список литературы

- [1] С.Г. Влэдуц, Д.Ю. Ногин, М.А. Цфасман “Алгеброгеометрические коды. Основные понятия”, МЦНМО, 2002
- [2] Alexei N. Skorobogatov, Serge G. Vladut: On the decoding of algebraic-geometric codes. IEEE Transactions on Information Theory 36(5): 1051-1060 (1990)
- [3] Д.Н. Семеновых “О теоретико-числовых вопросах в теории кодирования”, автореферат, 2006.