

ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ ТЕОРИИ ПОЛЕЙ ГАЛУА ДЛЯ ОБРАБОТКИ КОДОВ РИДА-СОЛОМОНА

Военная академия Республики Беларусь
г. Минск, Республика Беларусь

Семёнов С.И.

Липницкий В.Н. – д.т.н., профессор

В докладе проведен обзор и критический анализ классических методов обработки кодов Рида-Соломона, установлены достоинства и недостатки этих методов, констатирована необходимость развития матричных методов обработки кодов Рида-Соломона на основе теории полей Галуа.

Цифровые системы передачи играют подавляющую роль в современной информационной эпохе. Инфокоммуникационные системы (ИКС) на их основе обеспечивают надежность и достоверность передачи информации благодаря использованию помехоустойчивого кодирования. Суть его заключается во введении избыточной информации в передаваемую с тем, чтобы в последующем, при передаче закодированного сообщения в каналах с шумами, ИКС могла бороться с возможными возникающими ошибками. Среди многообразия применяемых помехоустойчивых кодов значительную роль играют коды Рида-Соломона (РС-коды) [1–5]. Специфической особенностью РС-кодов является их работа с недвоичным алфавитом. Коды Рида-Соломона были созданы в 1960 году [6], однако только с появлением техники с большими вычислительными ресурсами стало возможным эффективно реализовать на их основе устройства в высокоскоростных цифровых системах передачи и обработки информации реального времени. Они активно применяются в самых различных цифровых системах передачи и обработки данных: в сетях ЭВМ; в оптических системах; при передаче информации в сети WiMax; в спутниковой, радиорелейной связи; в системах хранения данных (RAID 6) и т.д. [1].

Для декодирования ошибок РС-кодами разработана система различных методов: алгоритм Питерсона-Горенштейна-Цирлера, алгоритм Берлекэмп-Месси, алгоритм Форни [1,2], а также более новые – алгоритм Судана [7] и другие.

Особенно эффективно РС-коды проявили себя при коррекции ошибок весом 1. Однако как показывают проведенные исследования, коррекция ошибок кратностью $\omega \geq 2$ требует определенной осторожности. Так, например, трехзначная ошибка может быть декодирована как двухзначная при использовании алгоритма декодирования для двухзначной ошибки, и наоборот – двухзначная может быть интерпретирована как трехзначная, что в результате может привести к еще большему искажению принятого сообщения. Поэтому требуется проводить дополнительную проверку на правильность полученного кодового слова, что недопустимо в высокоскоростных системах передачи информации. В этих случаях работа декодера с РС-кодами требует уверенного знания кратности исправляемых ошибок.

Определение РС-кодов близко к определению БЧХ-кодов, для которых разработана теория норм синдромов (ТНС) [8], позволившая эффективно использовать теорию полей Галуа и теорию автоморфизмов кодов для их обработки. На основе ТНС предложен ряд перестановочных нормальных методов коррекции ошибок БЧХ-кодами, на порядок снижающих проблемы «селектора», напрямую не зависящих от веса исправляемых ошибок.

Несомненно, развитие ТНС на класс РС-кодов позволит предложить такие же эффективные методы их обработки. Следует заметить, что реализация этой идеи требует последовательного изложения теории РС-кодов на матричном языке с максимальным упором на теорию полей Галуа, роль которой еще недостаточно проявилась в теории и практике РС-кодов, поэтому перенос основных положений ТНС на семейства РС-кодов должны принести новые эффективные методы обработки этих кодов

Список использованных источников:

1. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр : – пер. с англ. – Изд. 2-е, испр. – М. : Вильямс, 2003. – 1104 с.
2. Кудряшов, Б. Д. Основы теории кодирования : учеб. пособие. – СПб. : БХВ-Петербург, 2016. – 400 с.
3. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн : Пер. с англ. – М. : Связь, 1979. – 744 с.
4. Блейхут, Р. Теория и практика кодов, контролирующих ошибки : Пер. с англ. – М. : Мир, 1986. – 576 с.
5. Сидельников, В. М. Теория кодирования. – М. : ФИЗМАТЛИТ, 2008. – 324 с.
6. Reed I. S., Solomon G. Polynomial codes over certain finite fields. Journal of the Society for Industrial & Applied Mathematics, 1960, 8(3). – Pp. 300 – 304.
7. V. Guruswami and M. Sudan, «Improved decoding of Reed-Solomon and algebraic-geometric codes», IEEE Transactions on Information Theory, September 1999, 45(7). – Pp. 1757–1767.
8. Липницкий, В. А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения : монография / В. А. Липницкий, В. К. Конопелько. – Минск : Изд. центр БГУ, 2007 – 239 с.