УДК 004.722 *МРНТИ 50.39.15, 28.21.27, 49.37.33*

РЕАЛИЗАЦИЯ КОДОВ РИДА – СОЛОМОНА В МОДЕЛИРУЮЩИХ ПРОГРАММАХ

К. С. Сматов, д.ф.-м.н., ***Д. О. Туенбаев****

Казахский национальный технический университет им. К. И. Сатпаева

ТОО «Алатау-Софт»*

Осы мақалада Рид – Соломон кодының ақпаратты сақтайтын және жіберетін құрылғылардағы қолданылуы қарастырылған. Мақалада көп есептеу ресурстарын қажет етпейтін Рид – Соломон кодерін және декодерін модельдеу тәсілі сипатталған.
Түйінді сөздер: декодтау алгоритмі, ақпараттарды кодтау.

The article considers application of Reed – Solomon code in data storing and data transferring devices. It also describes the way of modeling the coder and decoder of Reed – Solomon, which does not demand many computing resources.
Key words: algorithm of decoding, coding of information.

С развитием компьютеров и компьютерных сетей в мире возрастает количество обрабатываемой, передаваемой и хранимой информации. Появляются новые способы записи и хранения информации, такие, как BlueRay DVD, HD DVD. Разрабатываются новые способы передачи информации, например WiMAX, вариации DSL; основанные на широко используемых WiFi, выделенные линии и других. В связи с необходимостью обеспечения сохранности данных необходимо применять различные способы увеличения надежности их хранения и передачи. Чаще всего используется кодирование или дублирование данных, а также более надежные устройства передачи и хранения данных.

В настоящей статье рассматривается один из популярных способов помехозащищенного кодирования информации: код Рида – Соломона (RS), и его моделирование в программе SystemView. Этот метод включен во многие стандарты записи и протоколы передачи данных. Он используется в технологиях записи данных CD-R, DVD-R, BlueRay DVD, HD DVD; в технологиях передачи данных WiFi, WiMAX, оптических линиях, сотовой, спутниковой, радиорелейной связях (FEC). Кроме того, код Рида – Соломона используется при записи в контроллерах оперативной памяти, при записи на жесткие диски (ECC) [3]. Фактически с момента изобретения кода Рида – Соломона в 1960 г. до его практического применения в больших масштабах прошло немало времени. Эффективный алгоритм декодирования был разработан в 1969 г. Элвином Берлекэмпом и Джэймсом Месси. Первое применение код Рида – Соломона получил в 1984 г. в серийном выпуске компакт-дисков [3]. Изначально его применение ограничивалось сложностью аппаратной реализации декодирующего устройства и большого количества необходимой вычислительной мощности. Теперь современные технологии позволяют с высокой скоростью декодировать и передавать большие объемы данных, например видео в формате Full HD.

Коды Рида – Соломона являются частным случаем кодов БЧХ (Боуза – Чоудхури – Хоквингема), корни порождающего полинома которого лежат в том же поле, над каким и строится код. Сам код является набором полиномов из элементов конечного поля (поле GF). Основная идея помехозащитного кодирования Рида – Соломона заключается в умножении информационного слова, представленного в виде полинома D, на неприводимый полином G (элемент поля GF), известный отправителю и получателю. В результате получается кодовое слово C, опять-таки представленное в виде полинома. Декодирование осуществляется с точностью до наоборот: если при делении кодового слова C на полином G декодер внезапно получает остаток, то он может рапортовать об ошибке. Соответственно, если кодовое слово разделилось нацело, его передача завершилась успешно. Если степень полинома G (называемого также порождающим полиномом) превосходит степень кодового слова по меньшей мере на две степени, то декодер может не только обнаруживать, но и исправлять одиночные ошибки. Если же превосходство степени порождающего полинома над кодо-

вым словом равно 4, то восстановлению поддаются и двойные ошибки. Короче говоря, степень полинома k связана с максимальным количеством исправляемых ошибок t следующим образом: $k = 2 \cdot t$. Следовательно, кодовое слово должно содержать 2 дополнительных символа на одну исправляемую ошибку. В то же время максимальное количество распознаваемых ошибок равно t, т. е. избыточность составляет 1 символ на каждую распознаваемую ошибку [1].

Для работы с кодами Рида – Соломона обычная арифметика не подходит. Кодирование предполагает вычисления по правилам действия над многочленами, с коэффициентами которых надо выполнять операции сложения, вычитания, умножения и деления. Причем все эти действия не должны сопровождаться каким-либо округлением промежуточных результатов (даже при делении!), чтобы не вносить неопределенность. При этом и промежуточные, и конечные результаты не имеют права выходить за пределы установленной разрядной сетки. Выполнение этих операций требует реализации сложной программы и не очень оптимально по количеству затрачиваемых машинных ресурсов.

Однако есть другой более удобный способ реализации кодера и декодера Рида – Соломона. Вместо умножения полиномов их можно делить, а остаток от деления брать как результат – контрольные биты. Тогда алгоритм кодировщика будет выглядеть следующим образом:

1) Добавляем к исходному информационному слову D справа k нулей, в результате у нас получается слово длины $n = m + r$ и полином $X^r \cdot D$, где m – длина информационного слова.

2) Делим полученный полином $X^r \cdot D$ на порождающий полином G и вычисляем остаток от деления R, такой что: $X^r \cdot D = G \cdot Q + R$, где Q – частное, которое мы игнорируем за ненадобностью – сейчас нас интересует только остаток.

3) Добавляем остаток R к информационному слову D. В результате получаем кодовое слово C, информационные биты которого хранятся отдельно от контрольных бит. Собственно, тот остаток, который мы получили в результате деления – и есть корректирующие коды Рида – Соломона. Способ кодирования, при котором информационные и контрольные символы хранятся раздельно, называется *систематическим кодированием* и такое кодирование весьма удобно с точки зрения аппаратной реализации.

4) Информационное слово + корректирующие коды можно записать так:

$$T = X^r \cdot D + R = GQ.$$

Декодирование полученного слова T осуществляется точно так же, как при кодировании. Если при делении T (которое в действительности является произведением G на Q) на порождающий полином G образуются остаток, то слово T искажено и соответственно, наоборот [2].

Исправление ошибок в полученном кодовом слове производится как при использовании обычного контроля четности битов. Позиции ненулевых битов в остатке от деления являются ошибочными, исправление ошибок осуществляется инвертированием в кодовом слове битов на этих позициях.

Все операции в кодере и декодере выполняются с применением арифметики конечных групп (поля Галуа).

Схема кодера и декодера. Используя программу SystemView , можно создавать модель, получающую на вход телемеханическую информацию и выдающую на выход вычисленные данные. Входящая информация может быть считана из входного файла, в котором записана последовательность битов информации. Выходной сигнал также может сохраняться в файл в виде значений последовательности битов.

На вход кодера поступают исходные данные, на выходе формируется набор из начальных данных и информации для восстановления – контрольные биты.

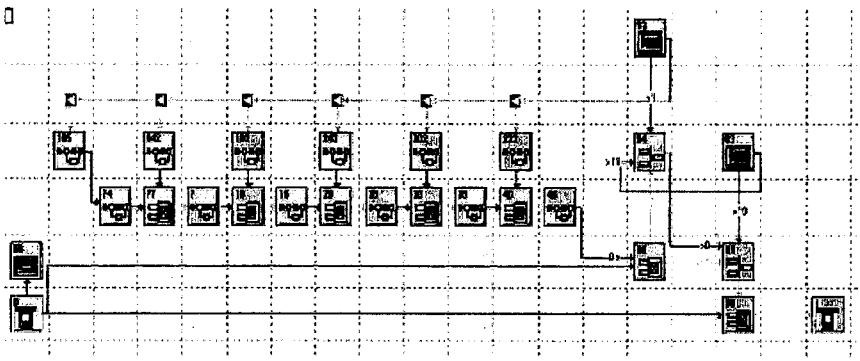

Рис. 1. Схема кодера

В схеме (рис. 1) каждое входное слово (регистр) умножается на образующий полином. Операция умножения одного регистра на другой является составной, в схеме кодера каждое такое умножение изображено в виде одного блока. Блок умножения приведен на рис. 2.

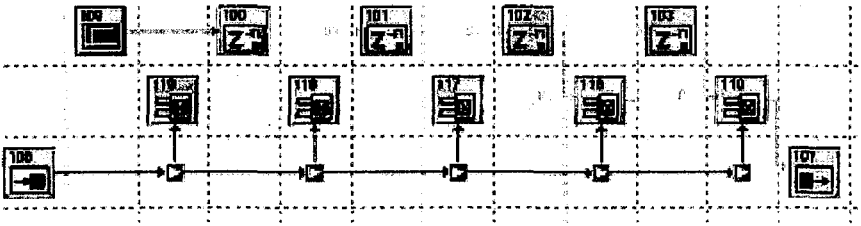

Рис. 2. Блок умножения

В схеме кодера регистр также изображен в виде составного блока, который состоит из блоков задержки (рис. 3).

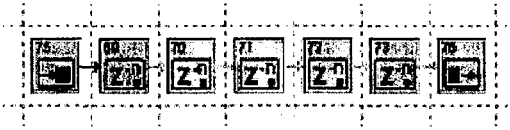

Рис. 3. Схема регистра

Декодер отличается от кодера наличием буферных регистров, которые временно хранят копию получаемых на вход данных. После получения всех входных данных вычисляются биты четности. Затем из буферных регистров данные поступают на выход, предварительно проходя через операцию умножения с результатом проверки четности (рис. 4).

Во многих современных моделирующих программах есть возможность экспорта созданных моделей в формат, который используется при печати компьютерных плат. Это означает, что смоделированный и протестированный алгоритм кодов Рида – Соломона гарантированно может быть аппаратно реализован.

В настоящее время существует несколько коммерческих реализаций и готовых схем кодирования и декодирования Рида – Соломона.

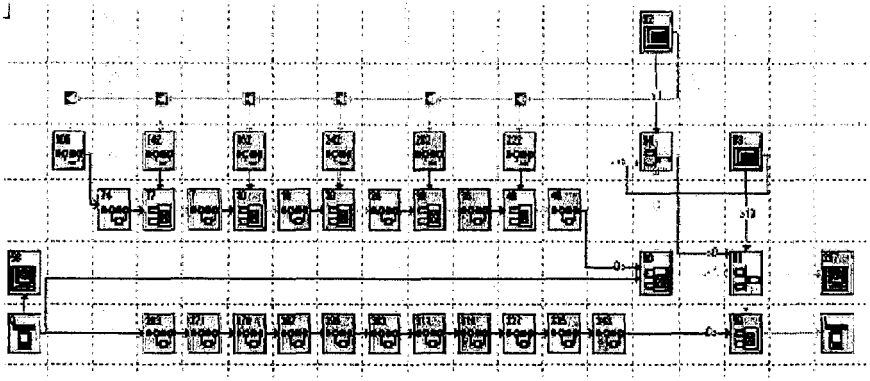

Рис. 4. Схема декодера

Однако на фоне всеобщей популяризации беспроводных технологий и повышения скорости Интернет-каналов разработка оптимальной аппаратной реализации кодера и декодера Рида – Соломона остается актуальной.

Литература

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. – Вильямс, 2004.
2. *Касперски К.* Могущество кодов Рида – Соломона или информация, воскресшая из пепла // Системный администратор. – 2008. – Вып. 5.
3. http://www.wikipedia.org