УДК 004.056.55

ОСНОВНАЯ ИДЕЯ КОДОВ РИДА − СОЛОМОНА

Жуат Е.М.
Казахский университет бизнеса и технологий, г. Астана

Научный руководитель – к.ф.-м.н., доцент Ташатов Н.Н.

Цифровая связь – область техники, связанная с передачей цифровых данных на расстояние.

В настоящее время цифровая связь повсеместно используется также и для передачи аналоговых (непрерывных по уровню и времени, например, речь, изображение) сигналов, которые для этой цели оцифровываются (дискретизируются). Такое преобразование всегда связано с потерями, т.е. аналоговый сигнал представляется в цифровом виде с некоторой точностью.

Современные системы цифровой связи используют кабельные (в том числе и волоконно-оптические), спутниковые, радиорелейные и другие линии и каналы связи, в том числе и аналоговые.

Обнаружение ошибок в технике – действие, направленное на контроль целостности данных при записи/воспроизведении информации или при ее передаче по линиям связи. Исправление ошибок (коррекция ошибок) – процедура восстановления информации после чтения её из устройства хранения или канала связи.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления − корректирующие коды (коды, исправляющие ошибки, коды с коррекцией ошибок, помехоустойчивые коды).

Основная идея помехозащитного кодирования Рида − Соломона заключается в умножении информационного слова, представленного в виде полинома D, на неприводимый полином G, известный обеим сторонам, в результате чего 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 наверх об ошибке. Соответственно, если кодовое слово разделилось нацело, его передача завершилась успешно.

Если степень полинома G (называемого так же 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 кодовым словом равно четырем, то восстановлению поддаются и двойные ошибки. То есть, степень полинома k связана с максимальным количеством исправляемых ошибок t следующим образом: $k = 2t$.

Следовательно, кодовое слово должно содержать два дополнительных символа на одну исправляемую ошибку. В то же время максимальное количество распознаваемых ошибок равно t, т.е. избыточность составляет один символ на каждую распознаваемую ошибку.

В отличие от кодов Хемминга, коды Рида − Соломона могут исправлять любое разумное количество ошибок при вполне приемлемом уровне избыточности. В кодах Хемминга контрольные биты контролировали лишь те информационные биты, что находятся по правую сторону от них и игнорировали всех «левосторонних» товарищей. Обратимся к таблице 1: добавление восьмого контрольного бита D ничуть не улучшило помехозащищенность кодирования, поскольку контрольному биту D было некого контролировать.

В кодах же Рида − Соломона контрольные биты распространяют свое влияние на все информационные биты и потому с увеличением количества контрольных бит увеличивается и количество распознаваемых/устраняемых ошибок. Именно благодаря последнему обстоятельству, собственно, и вызвана ошеломляющая популярность корректирующих кодов Рида − Соломона [1].

Для работы с кодами Рида − Соломона обычная арифметика не подходит. Так как кодирование предполагает вычисления по правилам действия над полиномами, 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. Причем и промежуточные, и конечные результаты не имеют права выходить за пределы установленной разрядной сетки.

Умножать информационное слово на порождающий полином вовсе не обязательно, можно поступить иначе:

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

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

– Добавляем остаток R к информационному слову D, в результате чего получаем кодовое слово C, информационные биты которых хранятся отдельно от контрольных бит. Тот остаток, который получается 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.

– Корректирующие коды можно записать так: $T = X^r D + R = G*Q$.

Декодирование полученного слова T осуществляется точно так же, как уже и было описано ранее. 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.

Макет кодера/декодера Рида − Соломона сконструируем таким образом, который работает по правилам обычной целочисленной алгебры. Естественно, за счет неизбежного в этом случае расширения разрядной сетки такому кодеру/декодеру будет очень трудно найти практическое применение, но зато он нагляден и позволяет не только понять, но и почувствовать принцип работы корректирующих кодов Рида − Соломона.

Будем исходить из того, что если $g = 2^n + 1$, то для любого a из диапазона $0…2^n$, произведение $ag = c$ (где c – кодовое слово), будет представлять, по сути, полную мешанину битов обоих исходных чисел.

Допустим $n = 2$, тогда $g = 3$. Легко видеть: на что бы мы не умножали g – хоть на 0, хоть на 1, хоть на 2, хоть на – 3, полученный результат делится нацело на g в том и только том случае, если никакой из его бит не инвертирован (то есть, попросту говоря, одиночные ошибки отсутствуют).

Остаток от деления однозначно указывает на позицию ошибки (при условии, что ошибка одиночная, групповые же ошибки данный алгоритм исправлять не способен). Точнее, если ошибка произошла в позиции x, то остаток от деления k будет равен $k = 2^x$.

Для быстрого определения x по k можно воспользоваться тривиальным табличным алгоритмом. Впрочем, для восстановления сбойного бита знать его позицию совершенно необязательно, достаточно сделать $R = e \wedge k$, где e – искаженное кодовое слово, ^ – операция XOR, а R – восстановленное кодовое слово.

Коды Рида − Соломона широко используются в устройствах передачи и хранения данных для обнаружения и исправления как одиночных, так и групповых ошибок. Область их применения необычайно широка– кодеры/декодеры Рида − Соломона можно найти и в ленточных запоминающих устройствах, и в контроллерах оперативной памяти, и в модемах, и в жестких дисках, и в CD-ROM/DVD-приводах и т. д. Благодаря им некоторые архиваторы безболезненно переносят порчу нескольких секторов носителя, содержащего архив, а подчас и полное разрушение целого тома многотомного архива. Еще коды Рида − Соломона позволяют защитному механизму автоматически восстанавливать информацию, взломанную хакером и/или искаженные в результате сбоя программного/аппаратного обеспечения.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер. с англ. – Издательский дом «Вильямс», 2004. – 1104 с. ил.