

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ КОДОВ РИДА-СОЛОМОНА

Юрьев И.В., Дяченко О.Н.

Донецкий национальный технический университет

При проектировании современных систем коммуникаций одной из важнейших является задача обеспечения высокой достоверности передачи информации, а также её хранение и обработка. Для обеспечения помехоустойчивости информации применяют коды, обнаруживающие и исправляющие ошибки, возникающие в ходе работы системы и её элементов.

Коды Рида-Соломона — циклические коды, позволяющие исправлять ошибки в блоках данных. Элементами кодового вектора являются не биты, а группы битов (блоки). В настоящее время широко используются коды Рида-Соломона для космической связи NASA, цифрового телевидения высокого разрешения (формат HDTV), в системах восстановления данных с компакт-дисков, в контроллерах оперативной памяти, в модемах, в жестких дисках, при создании архивов с информацией для восстановления в случае повреждений и т.д. [1-3]. Популярность этих кодов заключается в высоких корректирующих возможностях - исправление пакетов и множественных пакетов ошибок.

Данная работа посвящена рассмотрению вопросам определения оптимальных параметров кодов Рида-Соломона для одиночных пакетов ошибок.

1. Запись на CD-ROM

Возможные ошибки при чтении с диска появляются уже на этапе производства диска, так как сделать идеальный диск при современных технологиях невозможно. Кроме того, ошибки могут быть вызваны царапинами на поверхности диска, пылью и т.д. Поэтому при изготовлении читаемого компакт-диска используется система коррекции CIRC (Cross Interleaved Reed Solomon Code). Эта коррекция реализована во всех устройствах, позволяющих считывать данные с CD дисков, в виде чипа с прошивкой firmware. Нахождение и коррекция ошибок основана на избыточности и перемежении (redundancy & interleaving). Избыточность примерно 25 % от исходной информации.

При записи на цифровые аудиокомпакт-диски (Compact Disc Digital Audio — CD-DA) используется стандарт Red Book.

Название Red Book (красная книга) связано с вхождением стандарта в набор стандартов форматов компакт-дисков, известных как цветные книги. Первая редакция стандарта издана в июне 1980 года компаниями Philips и Sony, она была доработана организацией Digital Audio Disc Committee, а затем ратифицирована как стандарт IEC 908. Он не является свободно доступным и подлежит лицензированию у Philips. Стоимость формы заявки на лицензию составляет 5000 долларов США. Текст стандарта доступен для скачивания в формате PDF и стоит 240 долларов США.

Коррекция ошибок происходит на двух уровнях C1 и C2. При кодировании на первом этапе происходит добавление проверочных символов к исходным данным, на втором этапе информация снова кодируется. Кроме кодирования осуществляется также перемеживание (перемежение) байтов, чтобы при коррекции блоки ошибок распались на отдельные биты, которые легче исправляются. На первом уровне обнаруживаются и исправляются ошибочные блоки длиной один и два байта (один и два ошибочных

символа соответственно). Ошибочные блоки длиной три байта обнаруживаются и передаются на следующий уровень. На втором уровне обнаруживаются и исправляются ошибочные блоки, возникшие в С2.

2. Коды Рида-Соломона

Коды Рида-Соломона являются частным случаем кодов БЧХ. Главное отличие кодов Рида-Соломона заключается в том, что в качестве символа выступает не двоичный символ (один бит), а элемент поля Галуа (несколько битов).

Порождающий полином кода Рида-Соломона, исправляющего s ошибок, должен содержать $2s$ корней:

$$\{\alpha_0^j, \alpha_0^{j+1}, \alpha_0^{j+2}, \dots, \alpha_0^{j+2s-1}\},$$

где j_0 – конструктивный параметр.

Как правило, j_0 выбирают равным 1. Тогда множество корней полинома принимает вид $\{\alpha, \alpha^2, \alpha^3 \dots \alpha^{2s}\}$.

Для кода Рида-Соломона, исправляющего s ошибок, порождающий полином имеет следующий вид:

$$RS(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3) \dots (x - \alpha^{2s}),$$

При таком представлении порождающий полином имеет множество корней $\{\alpha, \alpha^2, \alpha^3 \dots \alpha^{2s}\}$.

Длина исправляемого пакета ошибок для последовательного кода без каких-либо ограничений равна $b' = j*b - (b - 1)$ для посимвольно перемеженного кода Рида-Соломона поля Галуа $GF(2^b)$ с параметром перемежения j .

Схему посимвольно перемеженного кода Рида-Соломона можно получить из схемы исходного кода, вставив дополнительно к каждому элементу памяти $j-1$ элементов. Например, для поля $GF(2^3)$ при перемежении с параметром $j=2$ каждую триаду элементов памяти нужно заменить двумя последовательно включенными триадами.

Чтобы из (n, k) -кода получить (jn, jk) -код, выберем из исходного кода j произвольных кодовых слов и укрупним кодовые слова, чередуя их символы. Если исходный код исправлял произвольный пакет ошибок длины t , то, очевидно, результирующий код будет исправлять все пакеты ошибок длины jt . Например, применяя метод перемежения к четырём копиям $(31,25)$ -кода, получаем $(124,100)$ -код. Так как каждый из четырёх исходных кодов исправлял пакет ошибок длины 2, то новый код будет исправлять любой пакет ошибок длины 8 [2].

Для циклических кодов метод перемежения приводит к циклическим кодам. Предположим, что исходный код порождается полиномом $g(x)$. Тогда порождающий полином получаемого перемежением кода равен $g(x^j)$. Чтобы установить это, заметим, что перемежение символов нескольких информационных полиномов с последующим умножением на $g(x^j)$ даёт то же самое кодовое слово, что и умножение каждого из исходных информационных полиномов на $g(x)$ с последующим перемежением этих слов (n, k) -кода [2].

3. Определение оптимальных параметров

Рассмотрим влияние параметров на длину исправляемого пакета ошибок для последовательного кода при $s=1$.

Таблица 1

Зависимость параметров кода и длины исправляемого пакета ошибок

j	b'(GF(2))	b'(GF(4))	b'(GF(8))	b'(GF(64))
1	1	1	1	1
2	2	3	4	7
3	3	5	7	13
4	4	7	10	19
5	5	9	13	25
6	6	11	16	31
7	7	13	19	37
8	8	15	22	43
9	9	17	25	49
10	10	19	28	55
11	11	21	31	61
12	12	23	34	67

Из таблицы видно, что чем больше поле Галуа и коэффициент перемежения, тем больше длина исправляемого пакета ошибок. Но при увеличении каждого из этих параметров увеличиваются аппаратные затраты и уменьшается скорость работы схемы.

Рассмотрим, как влияет каждый параметр в отдельности. Так как особенности реализации для кодеров и декодеров одинаковы, поэтому рассматривать их будем на примере декодеров с количеством ошибок $s=1$.

Из рисунков 1 и 2 видно, что параметр j влияет только на количество элементов памяти, в данном случае при $j=2$ количество элементов памяти удваивается.

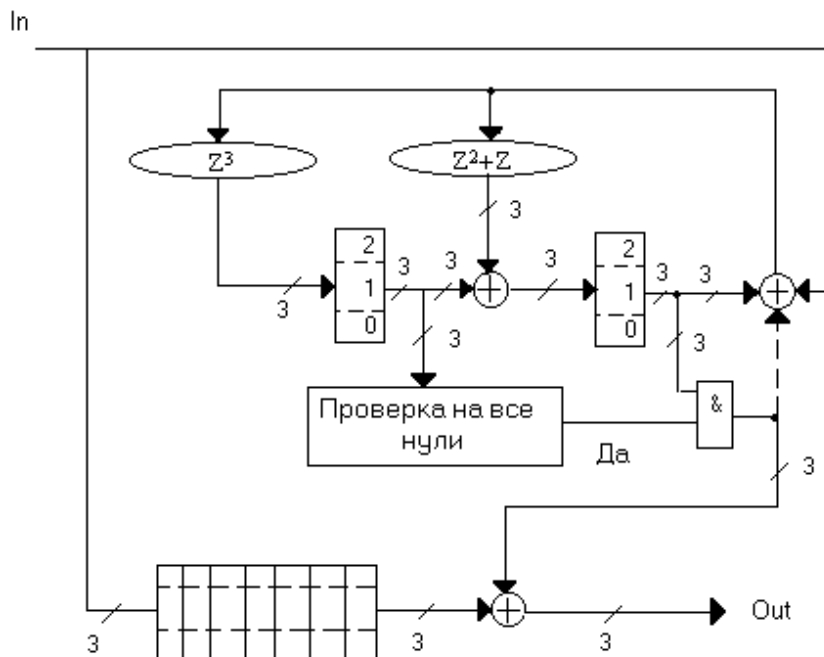


Рисунок 1 - Декодер кода Рида-Соломона для поля Галуа GF(8) и $j=1$

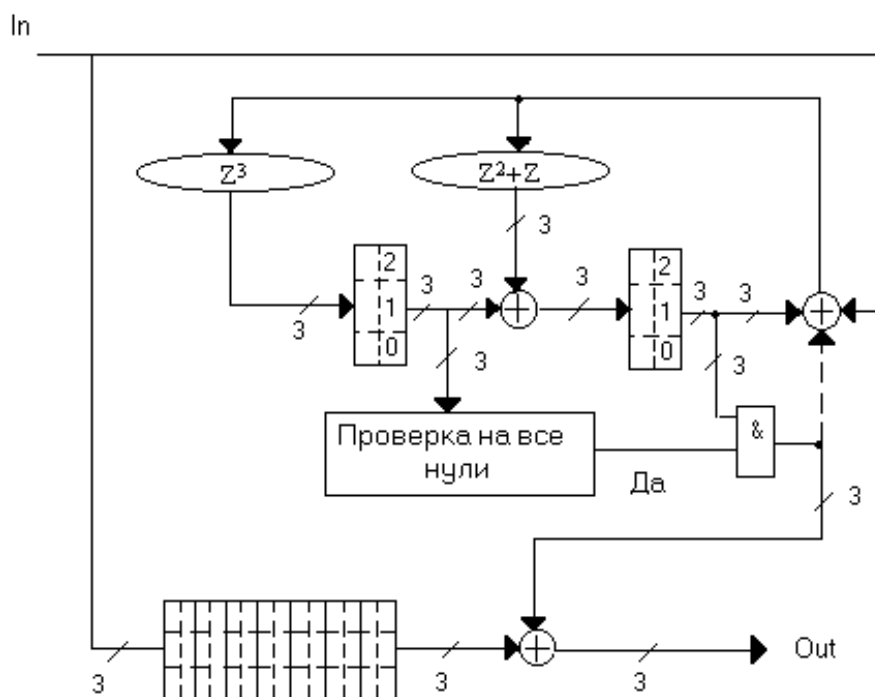


Рисунок 2 - Декодер кода Рида-Соломона для поля Галуа GF(8) и $j=2$

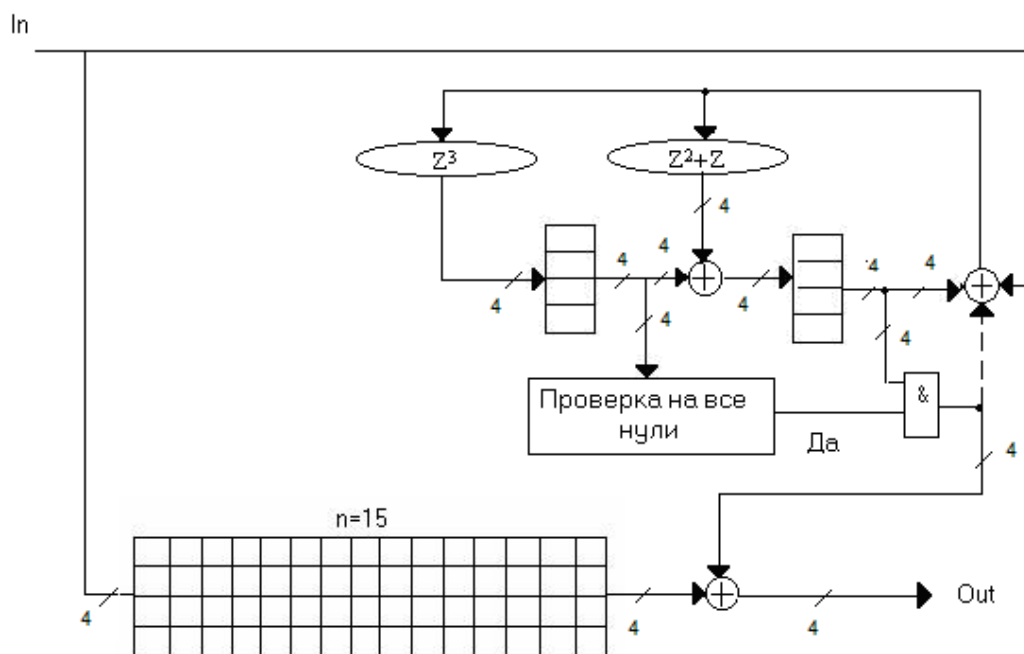


Рисунок 3 - Декодер кода Рида-Соломона для поля Галуа GF(16) и $j=1$

Из рисунка 3 видно, что при возрастании размерности поля Галуа увеличивается количество элементов памяти и разрядность шины, а вместе с ней и схемная реализация операций умножения.

Если из таблицы взять четыре поля Галуа: GF(2) с перемежением 7, GF(4) с перемежением 4, GF(8) с перемежением 3 и GF(64) с перемежением 2, у которых длина исправляемого пакета ошибок равна 7, то количество элементов памяти в соответствующих декодерах равно

$$\text{GF}(2): 2^*b^{*j+n*(n-k)}=2^*1^*7+1^*1=15,$$

$$\text{GF}(4): 2^*b^{*j+n*(n-k)}=2^*2^*4+3^*2=22,$$

$$\text{GF}(8): 2^*b^{*j+n*(n-k)}=2^*3^*3+7^*3=39,$$

$$\text{GF}(64): 2^*b^{*j+n*(n-k)}=2^*6^*2+63^*6=402.$$

Если учесть, что для приведенных выше полей Галуа также увеличивается количество элементов для реализации операции умножения, то отсюда следует, что по минимальным аппаратным затратам и максимальной скорости более оптимальным является способ с минимальным размером поля Галуа и максимальным перемежением.

Литература:

- [1] Robert H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. First Edition, John Wiley & Sons, 2002. – 221p.
- [2] Richard E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, Massachusetts, 1984. – 576p.
- [3] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. - М.:Мир,1976. - 595с.