International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 2 Issue 11, November-2013, pp: (105-108), Available online at: **www.erpublications.com**

Decoding of BCH Codes and RS Codes

Amit K Dutta[1], Manasi Dey A Dutta[2]
JIS College of Engineering, Kalyani, WB, India

Abstract: A very high speed data communication in the range of 1Gb/s is required for next generation communication systems. The Error Correcting Codes should be decoded so that it does not hinder the speed. This paper addresses the hardware solutions associated with that need for BCH and RS Codes decoding. This technique is developed such that it allows the decoding to be done in real time.

Keywords: BCH Codes, RS Codes, Gigabit, Wireless and Line Communication.

I. INTRODUCTION

In this age of information super highway, there is increasing importance not only of speed [1], but also of accuracy in the transmission of data and in the storage/retrieval of data in mass storage. Error Correcting Codes are used extensively in communication and data storage to protect the data. In communication, channels are imperfect and susceptible to various noises and fading. The basic idea behind Error Correcting Codes is to add a certain amount of redundancy to the data prior to its transmission through noisy channel. At the receiver, the original message is recovered from the corrupted one. By adding redundancy and using some intelligent strategy, we can reduce the effect of noisy or fading channel.

The Bose, Chaudhuri and Hocquenghem (BCH) codes are sub class of cyclic codes. Some of these codes are optimum and they are capable of correcting multiple errors for which it is designed. They have well understood mathematical properties. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960. Encoding and decoding operations for the BCH codes are easy. Peterson devised the first decoding algorithm for binary BCH codes. The algorithm was later generalized and refined by Gorenstein and Zierler and this improved method goes by the name of Peterson-Gorenstein-Zierler decoding algorithm. Both binary and non binary BCH codes exist. A popular non binary class of BCH codes is the Reed-Solomon Codes. The Reed-Solomon Codes were introduced by IS Reed and G Solomon in 1960. Both of this codes are linear block codes and extensively used in digital communication and data storage.

The organization of the paper is as follows. Section II introduces the BCH Coding [2][3] and in the Section III the existing decoding techniques are described. In Section IV we discuss about the new decoding technique with an example for BCH Code. Section V introduces the RS Coding and decoding technique with an example [3]. We conclude the paper in the next Section.

II. BCH CODING

We know that the generator polynomial for Cyclic Codes of Block length n is formed out of the factors of $(x^n – 1)$, that is $(x^n – 1)=f_1(x)*f_2(x)*f_3(x)*……*f_p(x)$ and $g(x)=f_1(x)*f_2(x)*f_3(x)$ for example. For Bose-Chaudhuri-Hocquenghem Code, we choose a primitive polynomial of degree m for the extension field $GF(q^m)$ of GF(q) and find the minimal polynomials of $GF(q^m)$ by factoring $(x\hat{}(q^m-1) -1)$. Once the minimal polynomials are known we form the Generator Polynomial for t error correcting code by $g(x)=LCM[f_1(x), f_2(x), f_3(x),…….. f_{2t}(x)]$.

III. DECODING OF BCH CODE

BCH Codes are subclass of Cyclic Codes. So we can use all the decoding methods normally used for Cyclic Codes. There are some other decoding techniques, specially named after Peterson. The Peterson decoding algorithm is given below.

The received signal is r(x)=c(x) + e(x). But if we evaluate at zeros of g(x), then the Syndrome is given by

$S_j=r(□^j) = c(□^j) + e(□^j)= e(□^j) =\sum_{k=0}^{n-1} e_k(\alpha^j)^k$ for j=1,2,……,2t

Thus a series of 2t Syndromes are calculated at 2t zeros. Now, assume that the received word r(x) have v errors in position $i_1, i_2, \ldots\ldots i_v$ and the error magnitude is binary that is 0/1,

So, $S_j = \sum_{l=1}^{v} e_{i_l} (\alpha^j)^{i_l} = \sum_{l=1}^{v} (\alpha^{i_l})^j = \sum_{l=1}^{v} X_l^j$

$\{X_l\}$ are error location. Then,

$$S_1 = X_1 + X_2 + X_3 + \cdots .. + X_v$$

$$S_2 = {X_1}^2 + {X_2}^2 + {X_3}^2 + \cdots .. + {X_v}^2$$

$$S_{2t} = {X_1}^{2t} + {X_2}^{2t} + {X_3}^{2t} + \cdots .. + {X_v}^{2t}$$

Let $\Lambda(x)$ be the error locator polynomial such that

$$\Lambda(x) = \prod_{l=1}^{v} (1 - X_l x) = \Lambda_v x^v + \Lambda_{v-1} x^{v-1} + \cdots \ldots + \Lambda_1 x + 1$$

Where,

$$\Lambda_1 = \sum_{i=1}^{v} X_i$$

$$\Lambda_2 = \sum_{i<j}^{v} X_i \, X_j$$

$$\Lambda_2 = \sum_{i<j<k}^{v} X_i \, X_j X_k$$

and

$$\Lambda_v = X_1 X_2 \ldots \ldots X_v$$

So,

$$S_1 + \Lambda_1 = 0$$

$$S_2 + \Lambda_1 S_1 + 2\Lambda_2 = 0$$

$$S_{2t} + \Lambda_1 S_{2t-1} + \cdots \ldots .. + \Lambda_v S_{2t-v} = 0$$

So in Matrix form, where t=v,

$$\begin{bmatrix} 1 & 0 & \ldots \ldots & 0 \\ S_1 & 2 & \ldots .. & 0 \\ S_{2t-1} & S_{2t-2} & \ldots \; \ldots .. & S_{2t-v} \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \Lambda_t \end{bmatrix} = \begin{bmatrix} -S_1 \\ -S_2 \\ -S_{2t} \end{bmatrix}$$

If the Syndrome matrix is non-singular we get the location of errors.

IV. NEW METHOD FOR BCH DECODING

Let the transmitted code symbol be c(x) and the error polynomial be e(x). So the received symbols are r(x)=c(x)+e(x)= i(x)g(x)+e(x), where i(x) is the information bits. We calculate the Syndrome of it by multiplying r(x) by h(x), the parity check polynomial.

So, $r(x)h(x)=i(x)g(x)h(x)+e(x)h(x)=(x^n - 1)i(x) + e(x)h(x)$, where the n is the block length.

If i(x) is of length k (as it is a (n,k) BCH Codes), then the first term has three parts. 1) $x^n i(x)$ (for bits greater than n-1), 2) Null (for bits k+1 to n-1) and 3) i(x) (for bits 0 to k).

The second part of r(x)h(x) is e(x)h(x) also can be divided into three parts. The middle one between k+1 to n-1 is of interest. We map the these bits with the error into a table which has one is to one mapping. We get these middle bits, find the error by look up table and correct the error. This will be possible for code (31,21) or (15,7) BCH Codes two error correcting codes. This is possible for h(x) of length k. We explain this method by an example (15,7) BCH Code.

(15,7) BCH Code is a two error correcting Code, $g(x)=x^8+x^7+x^6+x^4+1$ and $h(x)=x^7+x^6+x^4+1$ and $g(x)h(x)=x^{15}+1$. Assume $i(x)=0000111=x^2+x+1$ and $e(x)=x^8+x^6$. The middle part of $r(x)h(x)=x^{14}+x^{13}+x^{10}$. So we get the error at bit 8th and 6th.

The look up table is done like the memory look up table (ROM, diode connected) and the syndrome gives the addresses.

V. REED-SOLOMON CODE

Reed-Solomon (RS) Code is an important subset of the non-binary BCH Codes with a wide range of application in digital communications and data storage. Here, the coding is done based on group of bits, such as byte, rather than individual 0's and 1's. This feature makes Reed-Solomon Codes particularly good at dealing the bursts error.

We take an example to construct the Reed-Solomon (RS) Codes. WE take GF(7). We get the primitive element by forming the table. GF(7)={0,1,2,3,4,5,6}

i	5^i/mod(7)
0	1
1	5
2	4
3	6
4	2
5	3
6	1

So, 5 is the primitive element.

Now for two error correcting code, the $g(x)=(x-5)(x-5^2)(x-5^3)(x-5^4)$ and $h(x)=(x-5^5)(x-5^6)$;

So, $g(x)=x^4+4x^3+6x^2+5x+2$ and $h(x)=x^2+3x+3$. So, $g(x)*h(x)=x^6-1=x^6+6$

The transmitted signal is i(x)g(x), where the g(x) is the generating polynomial.

The received signal is r(x)=i(x)*g(x)+e(x), where e(x) is the error polynomial. In the receiver we multiply by h(x), $r(x)*h(x)=i(x)*g(x)*h(x)+e(x)*h(x)=i(x)*(x^6-1)+e(x)*h(x)$;

Let, $e(x)=e_1(x)+e_2(x)$;

0-bits=$r(x)*h(x)=3*e_1(x)$;

1-2bits=$r(x)*h(x)=i(x)+h(x)*e_1(x)$

3-6bits=$r(x)*h(x)=h(x)*e_1(x)+h(x)*e_2(x)$;

Infinity-7bits=$r(x)*h(x)=i(x)+h(x)*e_2(x)$=shifted 7 bit to right

From the 3-6bits parts we can find the error. This we do by finding a mapping between errors and syndromes in 3-6 bits similar to the BCH decoding.

We find the r(x)h(x) using a hardware as shown in Figure. 1

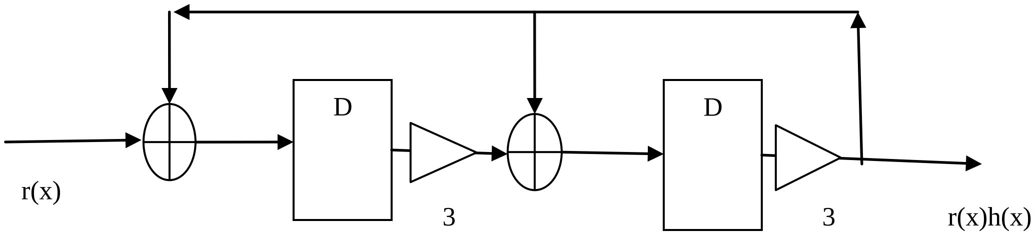

Figure. 1: The hardware for getting r(x)h(x). Here the adders are mod-7 adder and the lines are in parallel.

VI. CONCLUSION

Here, we discussed the basics of BCH codes and the non-binary Reed-Solomon Codes and their decoding methods. The BCH Codes constitute one of the most important and powerful classes of linear Codes which are cyclic. The decoding methods described here are simple to implement and very fast (comparable to memory fetch in Microcontroller).

VII. REFERENCES

[1]. A. K. Dutta, “High Speed Transmission by QAM-WCDMA Modulation,” International Journal of Enhanced Research in Science Technology & Engineering, ISSN 2319-7463 Vol. 2 Issue 10, October-2013 pp. 85-89.

[2]. R. Bose, “Information Theory, Coding and Cryptography,” 2nd Edition, Tata McGraw-Hill, 2008.

[3]. S.B. Wicker, “Error Control Systems for Digital Communication and Storage,” 1994.