An Enhanced (31,11,5) Binary BCH Encoder and Decoder for Data Transmission

P.Mozhiarasi, C.Gayathri, V.Deepan

Master of Engineering, VLSI design, Sri Eshwar College of Engineering, Coimbatore- 641 202, arasi.mozhi91@gmail.com
Assistant Professor, Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore- 641 202, gayathrichandran28@gmail.com
System administrator, Mahle Behr India Pvt. Ltd., Kancheepuram, Dist.-603002, deepan2100@yahoo.co.in

Abstract— This paper describes the design of (31,11,5) BCH encoder and decoder using mathematical derivation where 31, 11 and 5 represents the block length(n), data length(k) and maximum number of correctable errors(t) respectively. By the use of Galois Field GF(2^5) the encoding and decoding are carried out with an irreducible polynomial of x^5+x^2+1.The codeword is formed in encoder side by appending redundant bits(R(X)) with the message bit and transmitted through the channel to the decoder side. In the meanwhile, the Flash memory is used to store codeword, later for correction part in decoder side. Decoder involves 3 important steps: 1) The Syndrome calculation(SC), 2) Berlekamp Massey Algorithm (BMA), 3)The Chein Search(CS). The result shows that maximum of 5 errors in any position of 31 bits can be corrected effectively.

Keywords— Bose Chaudhuri Hocquenghem (BCH), BCH Encoder, BCH Decoder, Berlekamp Massey Algorithm (BMA), Chein Search(CS), Galois Field (GF), Syndrome Calculation(SC).

INTRODUCTION

A block of memory can store a sequence of 0's and 1's which, depending on the context, can represent a number, a fragment of text or a piece of graphics. The digital systems represents values using two voltage levels (usually 0V and +5V) .With two such levels one can represent exactly two different values. These could be any two different values, but by convention we use the values 0 and 1. These two values coincidently, correspond to the two digits used by binary numbering system. Bit is abbreviated for Binary Digit, which can hold either a 0 or a 1. Bits are combined to form some meaningful data[1]. When eight bits are grouped together they are represented as a byte. Code is a symbolic representation of an information transform. Bit combinations are referred to as "Code words". When binary information can be transmitted from one device to another by electric wires or other communication medium, the system cannot guarantee that the same data is received by device on other side[2]. Therefore, Error Correcting Techniques were introduces to avoid such bit reversal errors. Error Correcting Control is very important in modern communication systems. There are two correcting codes, that are BCH (*Bose, Chaudhuri, and Hocquenghem*), Turbo, LDPC and RS (*Reed-Solomon*) codes, are being widely used in satellite communications, computer networks, magnetic and optic storage systems.

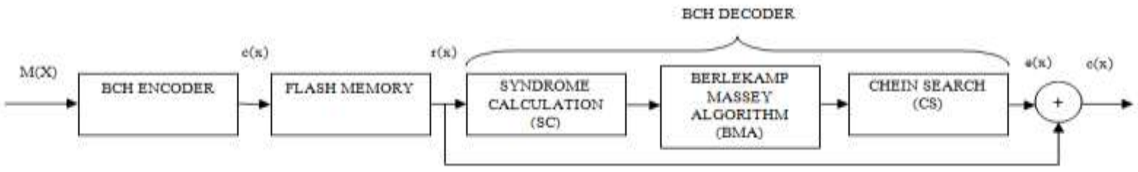


Figure 1 Block Diagram of BCH Encoder and Decoder

BCH codes are one of the most powerful random-error correcting cyclic codes. BCH codes can be defined by two parameters that are code size n and the number of errors to be corrected t [4]. BCH codes are polynomial codes that operate over Galois fields (or finite fields) [3]. In this paper, (31,11) BCH encoder and decoder are designed and they can detect and correct upto five errors In early stage, each character is a text message which is converted to a 11 bit binary data and is encoded to form 31 bit codeword. The BCH decoder is implemented with Berlekamp Massey Algorithm(BMA) and Chien Search (CS) Algorithm as shown in Fig. 1.

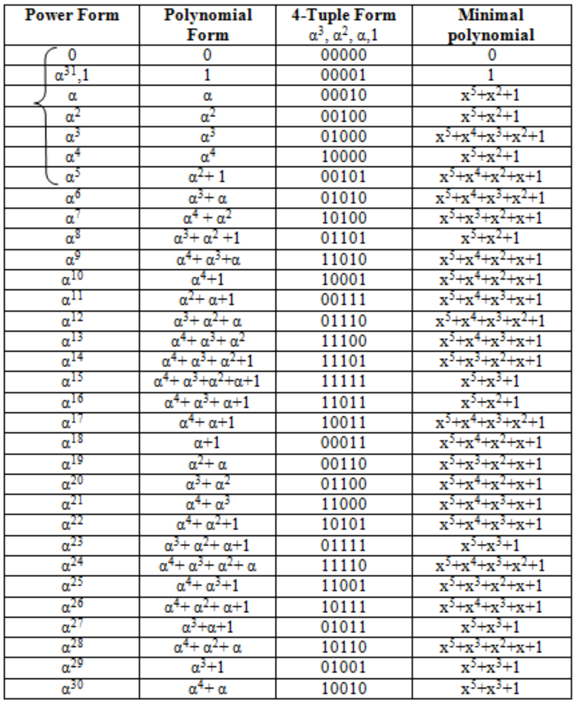
BCH CODES

The BCH abbreviation stands for the discoverers, Bose and Chaudhuri (1960), and independently Hocquenghem (1959). These codes are multiple error correcting codes and generalization of the Hamming codes. The most common binary BCH codes are characterized for any positive integers m (equal to or greater than 3) and the number of errors detected and corrected t by following parameters.

Codeword length, n = 2^m-1
Number of parity check bits, n-k ≤ mt
Minimum distance, $d_{min} \geq 2t+1$
where, m – primitive polynomial
k – data length
t – maximum number of correctable errors

Let us construct a generator polynomial for BCH (31,11) where, the code has 31 codeword bits, 20 redundant bits, corrects 5 errors (t=5).The generator polynomial of this code is generated using primitive polynomial x^5+x^2+1 over Galois Field GF(32)[3] as shown in Table 1.

Table I Field of 32 Elements Generated by x^5+x^2+1



Power Form	Polynomial Form	4-Tuple Form $\alpha^3, \alpha^2, \alpha, 1$	Minimal polynomial
0	0	00000	0
α^{31},1	1	00001	1
α	α	00010	x^5+x^2+1
α^2	α^2	00100	x^5+x^2+1
α^3	α^3	01000	$x^5+x^4+x^3+x^2+1$
α^4	α^4	10000	x^5+x^2+1
α^5	α^2+1	00101	$x^5+x^4+x^2+x+1$
α^6	$\alpha^3+\alpha$	01010	$x^5+x^4+x^3+x^2+1$
α^7	$\alpha^4+\alpha^2$	10100	$x^5+x^3+x^2+x+1$
α^8	$\alpha^3+\alpha^2+1$	01101	x^5+x^2+1
α^9	$\alpha^4+\alpha^3+\alpha$	11010	$x^5+x^4+x^2+x+1$
α^{10}	α^4+1	10001	$x^5+x^4+x^2+x+1$
α^{11}	$\alpha^2+\alpha+1$	00111	$x^5+x^4+x^3+x+1$
α^{12}	$\alpha^3+\alpha^2+\alpha$	01110	$x^5+x^4+x^3+x^2+1$
α^{13}	$\alpha^4+\alpha^3+\alpha^2$	11100	$x^5+x^4+x^3+x+1$
α^{14}	$\alpha^4+\alpha^3+\alpha^2+1$	11101	$x^5+x^3+x^2+x+1$
α^{15}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	11111	x^5+x^3+1
α^{16}	$\alpha^4+\alpha^3+\alpha+1$	11011	x^5+x^2+1
α^{17}	$\alpha^4+\alpha+1$	10011	$x^5+x^4+x^3+x^2+1$
α^{18}	$\alpha+1$	00011	$x^5+x^4+x^2+x+1$
α^{19}	$\alpha^2+\alpha$	00110	$x^5+x^3+x^2+x+1$
α^{20}	$\alpha^3+\alpha^2$	01100	$x^5+x^4+x^2+x+1$
α^{21}	$\alpha^4+\alpha^3$	11000	$x^5+x^4+x^3+x+1$
α^{22}	$\alpha^4+\alpha^2+1$	10101	$x^5+x^4+x^3+x+1$
α^{23}	$\alpha^3+\alpha^2+\alpha+1$	01111	x^5+x^3+1
α^{24}	$\alpha^4+\alpha^3+\alpha^2+\alpha$	11110	$x^5+x^4+x^3+x^2+1$
α^{25}	$\alpha^4+\alpha^3+1$	11001	$x^5+x^3+x^2+x+1$
α^{26}	$\alpha^4+\alpha^2+\alpha+1$	10111	$x^5+x^4+x^3+x+1$
α^{27}	$\alpha^3+\alpha+1$	01011	x^5+x^3+1
α^{28}	$\alpha^4+\alpha^2+\alpha$	10110	$x^5+x^3+x^2+x+1$
α^{29}	α^3+1	01001	x^5+x^3+1
α^{30}	$\alpha^4+\alpha$	10010	x^5+x^3+1

Let α be a primitive element in GF (2^m). The generator polynomial g(x) of the t error-correcting BCH code of length 2^m-1 is the lowest-degree polynomial over GF(2)[5] which has $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$ as its roots [i.e., g(α^i) = 0 for 1 ≤ i ≤ 2t].

Consider $f_i(x)$ be the minimal polynomial of α^i. Then g(x) must be the least common multiple of $f_1(x), f_2(x), \ldots, f_{2t}(x)$, that is, g(x) = LCM $\{f_1(x), f_2(x), \ldots, f_{2t}(x)\}$. But, *g(x)* is simplified to *g(x) = LCM* $\{f_1(x), f_3(x), \ldots, f_{2t-1}(x)\}$ because every even power of primitive element will have same minimal polynomial as some odd power of the elements having the number of factors in the polynomial.

Lin and Costello, Pless, and Rorabaugh exhibit algorithms for finding them using cyclotomic cosets[6]. From Lin and Costello, the first four odd power of α minimal polynomials are:

$\alpha : f_1(x) = x^5+x^2+1$
$\alpha_3 : f_3(x) = x^5+x^4+x^3+x^2+1$
$\alpha_5 : f_5(x) = x^5+x^4+x^2+x+1$
$\alpha_7 : f_7(x) = x^5+x^3+x^2+x+1$

Therefore, g(x) = LCM $\{f_1(x), f_3(x), f_5(x), f_7(x)\} = f_1(x)\, f_3(x)\, f_5(x)\, f_7(x)$ (since these are irreducible).So

$$g(x) = (x^5+x^2+1)\,(x^5+x^4+x^3+x^2+1)\,(x^5+x^4+x^2+x+1)\,(x^5+x^3+x^2+x+1)$$
$$= x^{20}+x^{18}+x^{17}+x^{13}+x^{10}+x^9+x^7+x^6+x^4+x^2+1$$
$$= 101100010011011010101$$

1. BCH ENCODER:

Let us consider a binary word 1000100 which represents "D" and it is placed in 11-bit information which is then appended with 20 bit sequence. Thus, 31 bit sequence is divided with generator polynomial to obtain a remainder.By combining the message sequence with the remainder sequence, the codeword is obtained (i.e., c(x) = X^{n-k} M(x) mod g(x) = X^{20}M(x) =0000100010011001100100001101101). This type of encoding is called systematic encoding where message bit and check bits were placed one after the other.

When the encoded data is transmitted through a noisy channel, errors are included into the codeword[10]. This is because the data which is transmitted in the form of electromagnetic signal over a channel whenever an electromagnetic signal flows from one point to another, it is subjected to unpredictable interference from heat, magnetism and other forms of electricity. This interference can change the shape or timing of signal. If the signal is carrying encoded binary data, such changes can alter the meaning of data[11].

Therefore, the codewords can be tested by dividing the codeword sequence by generator polynomial. If the remainder produced is zero then we confirm that there is no error in the codeword or else error is present[7].

2. BCH DECODER:

Five errors are introduced to the codeword for applying the error correcting algorithm to detect those errors and to correct them. The received sequence is represented by r(x) = 0**1**0**1**1000**0**001100110010**1**0011011**1**1 (bits in bold represents the error). The primitive polynomials are denoted as $f_1(x) = f_2(x)=f_4(x)=f_8(x)=100101$
$f_3(x) = f_6(x)= 111101$
$f_5(x) = f_{10}(x)=f_9(x)= 110111$
$f_7(x) =101111$

2.1 SYNDROME CALCULATION

The number of syndrome elements is 2*t = 10, to find t=5 errors[8]. Those syndrome elements are represented as $S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9, S_{10}$ and they can be calculated by

$S_1(x) = r(x) \bmod f_1(x) = r(x) \bmod f_1(x) = \alpha^{23}$
$S_2(x) = r(x) \bmod f_2(x) = r(x) \bmod f_1(x) = \alpha^{15}$
$S_3(x) = r(x) \bmod f_3(x) = r(x) \bmod f_3(x) = \alpha^{20}$
$S_4(x) = r(x) \bmod f_4(x) = r(x) \bmod f_1(x) = \alpha^{30}$
$S_5(x) = r(x) \bmod f_5(x) = r(x) \bmod f_5(x) = \alpha^{7}$
$S_6(x) = r(x) \bmod f_6(x) = r(x) \bmod f_3(x) = \alpha^{9}$
$S_7(x) = r(x) \bmod f_7(x) = r(x) \bmod f_7(x) = \alpha^{15}$
$S_8(x) = r(x) \bmod f_8(x) = r(x) \bmod f_1(x) = \alpha^{29}$
$S_9(x) = r(x) \bmod f_9(x) = r(x) \bmod f_5(x) = \alpha^{25}$
$S_{10}(x) = r(x) \bmod f_{10}(x) = r(x) \bmod f_5(x) = \alpha^{14}$

Each syndrome equation is a function only of the errors in the received codeword.

2.2 BERLEKAMP MASSEY ALGORITHM (BMA)

Error locator polynomial is calculated iteratively by Berlekamp. Using Lin and Costello, a table is formed.

The "Key Equation" is given by

$$\sigma^{(\mu+1)}(x) = \sigma^{\mu}(x) + d_\mu\, d_\rho^{-1} x^{2(\mu-\rho)} \sigma^{(\rho)}(x) \qquad \text{--------equation 1}$$

$$l_{\mu+1} = L = \deg(\sigma^{(\mu+1)}(x)) \qquad \text{--------equation 2}$$

$$d_{\mu+1} = S_{2\mu+3} + \sigma_1^{(\mu+1)} S_{2\mu+2} + \sigma_2^{(\mu+1)} S_{2\mu+1} + \cdots + \sigma_L^{(\mu+1)} S_{2\mu+3-L} \text{-------equation 3}$$

Steps:

(i) Initialize μ = 0, $d_\mu \neq 0$, $\rho =$ -1/2

(ii) Substitute $\sigma^{(\mu)}(x) = \sigma^{(0)}(x) = 1$, $d_\mu = d_0 = S_1$, $d_\rho^{-1} = d_{-\frac{1}{2}}^{-\frac{1}{2}}$=1, $\sigma^{(\rho)}(x) = \sigma^{\left(-\frac{1}{2}\right)}(x) = 1$ in equation 1

$$\sigma^{(1)}(x) = \sigma^0(x) + d_0\, d_{-1/2}^{-1} x^{2\left(\frac{1}{2}\right)} \sigma^{\left(\frac{-1}{2}\right)}(x)$$

$= 1 + \alpha^{23}(1)^{-1}x(1)$

$= \mathbf{\alpha^{23}x + 1}$

(iii) Substitute $\sigma^{(1)}(x) = \alpha^{23}x + 1$ in equation 2

$l_1 = \deg(\sigma^{(1)}(x))$

$= \deg(\alpha^{23}x + 1) = \mathbf{1}$

(iv) Substitute $S_3 = \alpha^{20}$, $S_2 = \alpha^{15}$, $\sigma_1^{(1)} = \alpha^{23}$ in equation 3

$d_1 = S_3 + \sigma_1^{(1)} S_2$

$= \alpha^{20} + (\alpha^{23})(\alpha^{15})$

$\mathbf{d_1 = \alpha^{21}}$

(v) In similar way, for μ = 1, $d_\mu \neq 0, \rho = 0$, $\boldsymbol{\sigma^{(2)}(x) = \alpha^{29}x^2 + \alpha^{23}x + 1, l_2 = 2}$**and** $\boldsymbol{d_2 = \alpha}$

for μ = 2, $d_\mu \neq 0, \rho = 1$, $\boldsymbol{\sigma^{(3)}(x) = \alpha^3x^3 + \alpha^{12}x^2 + \alpha^{23}x + 1, l_3 = 3}$ and $\boldsymbol{d_3 = \alpha^{15}}$

for μ = 3, $d_\mu \neq 0, \rho = 2$, $\boldsymbol{\sigma^{(4)}(x) = \alpha^{12}x^4 + \alpha x^3 + \alpha^{17}x^2 + \alpha^{23}x + 1,}$ $l_4 = \mathbf{4}$and $\boldsymbol{d_3 = \alpha^7}$

for μ = 4, $d_\mu \neq 0, \rho = 3$, $\boldsymbol{\sigma^{(5)}(x) = \alpha^{26}x^5 + \alpha^{24}x^4 + \alpha^{14}x^3 + \alpha^{13}x^2 + \alpha^{23}x + 1}$

The last polynomial $\boldsymbol{\sigma^{(5)}(x) = \alpha^{26}x^5 + \alpha^{24}x^4 + \alpha^{14}x^3 + \alpha^{13}x^2 + \alpha^{23}x + 1}$ represents the final error locator polynomial. The Lin and Costello, a table [9] is finally formed using above calculations as shown in Table II.

Table II Lin and Costello Table

μ	**$\sigma^{(\mu)}(x)$**	**d_μ**	**l_μ**	**$2\mu - l_\mu$**
-1/2	1	1	0	-1
0	1	α^{23}	0	0
1	$\alpha^{23}x+1$	α^{21}	1	1
2	$\alpha^{29}x^2+\alpha^{23}x+1$	α	2	2
3	$\alpha^3x^3+\alpha^{12}x^2+\alpha^{23}x+1$	α^{15}	3	3
4	$\alpha^{12}x^4+\alpha x^3+\alpha^{17}x^2+\alpha^{23}x+1$	α^7	4	4
5	$\alpha^{26}x^5+\alpha^{24}x^4+\alpha^{14}x^3+\alpha^{13}x^2+\alpha^{23}x+1$	-	-	-

Note: 1) Lin and Costello notations were used

2) d_μ represents discrepancy value

2.3 CHIEN SEARCH (CS) ALGORITHM

The roots of $\sigma^{(\mu)}(x)$ in GF (2^5) should be found out by trial and error substitution [12]. If $\sigma^{(\mu)}(x) = \sigma^{(5)}(x) = \alpha^{26}x^5+\alpha^{24}x^4+\alpha^{14}x^3+\alpha^{13}x^2+\alpha^{23}x+1 = 0$ is obtained by substituting $x = 0, 1, \alpha, \alpha^2, \ldots, \alpha^{30}$ then they are considered as roots.

Example: $\sigma^{(5)}(0) = \alpha^{26}(0)^5+\alpha^{24}(0)^4+\alpha^{14}(0)^3+\alpha^{13}(0)^2+\alpha^{23}(0)+1 = 1 \neq 0$

…

$\sigma^{(5)}(\alpha^2) = \alpha^{26}(\alpha^2)^5+\alpha^{24}(\alpha^2)^4+\alpha^{14}(\alpha^2)^3+\alpha^{13}(\alpha^2)^2+\alpha^{23}(\alpha^2)+1 = 0$

…

$\sigma^{(5)}(\alpha^4) = \alpha^{26}(\alpha^4)^5+\alpha^{24}(\alpha^4)^4+\alpha^{14}(\alpha^4)^3+\alpha^{13}(\alpha^4)^2+\alpha^{23}(\alpha^4)+1 = 0$

…

$$\sigma^{(5)}(\alpha^9) = \alpha^{26}(\alpha^9)^5+\alpha^{24}(\alpha^9)^4+\alpha^{14}(\alpha^9)^3+\alpha^{13}(\alpha^9)^2+\alpha^{23}(\alpha^9)+1= 0$$

$$\dots$$

Therefore, α^2, α^4, α^9, α^{22}, α^{30} are the roots. The bit position of error location will be the inverse of their roots (α^2, α^4, α^9, α^{22}, α^{30}) i.e., 0**1**0**1**0000**1**000000000000**1**0000000**1**0. Thus, the error pattern polynomial can be written as $e(x) = x^{29}+x^{27}+x^{22}+x^9+x$. As a result, the transmitted or original data is recovered by performing modulo-2 addition for r(x) and e(x).

$$\begin{aligned} c(x) &= r(x) + e(x) \\ &= 0101100000011001100101001101111 + 0101000010000000000001000000010 \\ &= \underbrace{0\mathbf{0}0\mathbf{0}1000\mathbf{1}}_{M(x)}\underbrace{001100110010\mathbf{0}0011011\mathbf{0}1}_{R(x)} \end{aligned}$$

CONCLUSION

The error correcting technique plays an important role in modern communication and digital storage systems. (31,11,5) BCH encoder and decoder are designed with mathematical derivations and upto 5 errors can be detected and corrected by using Berlekamp Massey Algorithm (BMA) and Chien Search (CS).

REFERENCES:

[1] Berlekamp.E.R, "Algebraic Coding Theory", Mc GrawHill, New York, 1968.

[2] Claude E. Shannon and Warren Weaver, "The Mathematical theory of Communication", Chicago: University of Illinois Press, p.71, 1963.

[3] Goresky, M. and Klapper, A.M. Fibonacci, "Galois representations of feedback-with-carry shift registers", *IEEE Transactions on Information Theory*, Volume: 48, p. 2826 –2836, Nov 2002.

[4] Hank Wallace, "Error Detection and Correction using BCH Codes", Copyright © 2001 Hank Wallace.

[5] Oliver Pretzel, "Error Correcting Codes and Finite Fields", Oxford: Oxford University Press, p. 77, 1992.

[6] P.Mozhiarasi , Ms.C.Gayathri, "A Mathematical Derivation for Error Correction and Detection in Communication using BCH Codes", IPASJ International Journal of Electronics & Communication, Vol. 2, Issue 10, p. 7-12, Oct. 2014.

[7] R.C.Bose, D.K.Ray-Chaudhuri, "On a class of error correcting binary group codes", Inf. Cntrl, 3, p. 68-79, March 1960.

[8] R.L. Miller,''Generalized BCH codes'', Information and Control, Vol.40, Issue 1, p. 61-75, Jan. 1979.

[9] Shu Lin and Daniel J. Costello, Jr., "Error Control Coding", Englewood Cliffs, New Jersy: Prentice Hall, Chapter 1, 1983.

[10] Simon Haykin, "Communication Systems", 4th Edition, John Wiley & Sons, Inc.

[11] W.W.Peterson, "Encoding and Error-Correction procedures for the Bose-Chaudhuri Codes", IRE Trans. Inf. Theory, IT-6, p. 459-470, Sep. 1960.

[12] Yunghsiang S. Han, "BCH Codes", Graduate Institute of Communication Engineering, National Taipei University Taiwan.