International Journal of Mathematical Archive-11(4), 2020, 10-13
Available online through www.ijma.info ISSN 2229 – 5046

PERFORMANCE EVALUATION OF BCH CODES ON AWGN CHANNELS

AMAR PANDEY*

**Department of Mathematics,
University of Allahabad, Allahabad-211002, (U. P.), India.**

(Received On: 04-02-20; Revised & Accepted On: 28-02-20)

ABSTRACT

The Bose-Chaudhuri-Hocquenghem (BCH) codes are a class of widely studied error-correcting codes. These are powerful error-correcting codes suitable for the mobile channel environment where they can correct both random and burst errors. The impressive algebraic structure of BCH codes facilitates their design and implementation. Out of the three main decoding algorithms of BCH codes, the Berlekamp-Massey algorithm, the Peterson's algorithm and the Euclidean algorithm, the Berlekamp-Massey is the most efficient one and is widely used in simulations and software applications. In this paper, the BCH encoder and its decoder are implemented in a systematic manner. The Berlekamp-Massey algorithm is chosen as the decoding algorithms for (63, 30, 6) BCH codes. Further, simulation results for the bit error rate performance of (15, 5, 3), (31, 11, 5) and (63, 30, 6) BCH coded messages with BPSK modulation on AWGN channel have been obtained.

Keywords: *BCH Codes, AWGN Channel, Berlekamp-Massey Algorithm, BPSK.*

1. INTRODUCTION

A binary BCH codes that can correct upto t errors requires three decoding steps:

i. Computation of a syndrome vector whose $2t$ components belong to $GF(2^m)$, where m is a positive integer.
ii. Conversion of syndrome to an error location polynomial of degree t or less over the same field.
iii. Finding the roots of polynomial which correspond to bit error locations in the received vector.

Peterson [1] first outlined the method which was considerably refined by Berlekamp and others [2-4]. The discovery of the binary codes of Bose and Ray-Chaudhury [5, 6] and Hocquenghem [7] has been perhaps, the outstanding success of the search for codes based on algebraic structures. BCH codes are often used in communication systems because they provide good error correcting performance in most channels and their structure allows for algebraic decoding upto a designed distance.

In fact, the strategy which is used in Berlekamp's algorithm, and for specific practical examples, is to correct errors recursively. Syndrome vector computation is a transform over $GF(2^m)$ of the received data vector which was shown by Blahut [8] to be equivalent to a Fourier transform on the finite field. The computed syndrome vector must be converted into an error location polynomial by solving system of nonlinear equations. The main subject of this paper is to find the error location polynomial and analysis of decoding procedures and also to investigate error rate performance of different BCH codes with BPSK modulation on AWGN channel.

2. ENCODING

There are two methods to generate the BCH code words: Systematic manner and non-systematic manner. In the non-systematic manner, the encoding procedure is quite simple. Let V be the $n \times 1$ code word, M be the $k \times 1$ information bits and matrix G be generated by $g(x)$ such that

$$V = M \times G \tag{1}$$

where,

$$G^T = [g(x), xg(x), \dots\dots\dots, x^{k-1}g(x)]_{(n\times k)}$$
$$g(x) = LCM\big(\Phi(x), \Phi_{b+1}(x), \dots\dots\dots, \Phi_{b+2t-1}(x)\big) \tag{2}$$

Corresponding Author: Amar Pandey*
Department of Mathematics, University of Allahabad, Allahabad-211002, (U. P.), India.

For designing a systematic form encoder, let $u(x)$ be polynomial of degree less than k corresponding to the information vector, then we form $m(x) = X^{n-k}u(x)$ by remainder theorem, we get

$$m(x) = X^{n-k}u(x)$$
$$= q(x)g(x) + r(x); \quad \deg r(x) < \deg g(x),\ r(x) = 0 \tag{3}$$

or $$X^{n-k}u(x) - r(x) = q(x)g(x) \tag{4}$$

or $$m(x) - r(x) = q(x)g(x) \tag{5}$$

Thus, the code words are multiple of the generator polynomial $g(x)$. To find $g(x)$ for BCH (63, 30, 6) codes, we obtain all the elements of $GF(2^6)$. These are obtained by the primitive polynomial $p(x) = x^6 + x + 1$,
or $p(\alpha) = \alpha^6 + \alpha + 1 = 0$.
All elements of $GF(2^6)$ are shown in Table-1 and the generator polynomial is obtained to be:

$$g(x) = 1 + x + x^2 + x^5 + x^6 + x^8 + x^9 + x^{11} + x^{13}$$
$$+x^{14} + x^{15} + x^{20} + x^{22} + x^{23} + x^{27} + x^{28}$$
$$+x^{29} + x^{30} + x^{32} + x^{33}$$

Power	0	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}
Vector	000000	000001	000010	000100	001000	010000	100000	000011	000110	001100	011000	110000	100011
	α^{12}	α^{13}	α^{14}	α^{15}	α^{16}	α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}
	000101	001010	010100	101000	010011	100110	001111	011110	111100	111011	110101	101001	010001
	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}	α^{31}	α^{32}	α^{33}	α^{34}	α^{35}	α^{36}	α^{37}
	100010	000111	001110	011100	111000	110011	100101	001001	010010	100100	001011	010110	101100
	α^{38}	α^{39}	α^{40}	α^{41}	α^{42}	α^{43}	α^{44}	α^{45}	α^{46}	α^{47}	α^{48}	α^{49}	α^{50}
	011011	110110	101111	011101	111010	110111	101101	011001	110010	100111	001101	011010	110100
	α^{51}	α^{52}	α^{53}	α^{54}	α^{55}	α^{56}	α^{57}	α^{58}	α^{59}	α^{60}	α^{61}	α^{62}	
	101011	010101	101010	010111	101110	011111	111110	111111	111101	111001	110001	100001	

Table-1: Elements of $GF(2^6)$

3. BERLEKAMP - MASSEY DECODING

The objective of decoding is to obtain correct messages from the received encoded data, even if, certain errors have occurred in the transmission channel. The Berlekamp-Massey algorithm uses Lin's iterative method [9]. The decoding is performed by first obtaining the syndrome corresponding to the received blocks of data and then the error locator polynomial is obtained by Lin's algorithm as given below:

a) $\mu = 0$
b) If $d_\mu = 0$ then: $\sigma^{\mu+1}(x) = \sigma^\mu(x)$
   Else: Find a row, say $\rho < \mu$ and $d_\rho \neq 0$ where $2\rho - l_\rho$ is maximum.
   Then: $\sigma^{\mu+1}(x) = \sigma^\mu(x) + d\mu\, d\rho^{-1} x^{2(\mu-\rho)}\sigma^\rho(x)$.
c) In any case,
   $d_{\mu+1} = S_{2\mu+3} + \sigma_1^{\mu+1} S_{2\mu+2} + \cdots \ldots \ldots + \sigma_{l_{\mu+1}}^{\mu+1}\ S_{2\mu+3-l_{\mu+1}}$.
d) $l_{\mu+1} = DEGREE\big(\sigma^{\mu+1}(X)\big)$.
e) Increment μ.
f) If $\mu \leq t$ go to step b), Else quit: $\sigma^t(x)$ is the error location polynomial.

The initial conditions of the algorithm are

$$2\mu - l_\mu = -1, \qquad \sigma^{(-1/2)}(x) = 1, \qquad l_{-1/2} = 0, \qquad d_{-1/2} = 1$$
$$2\mu - l_\mu = 0, \qquad \sigma^{(0)}(x) = 1, \qquad l_0 = 0, \qquad d_0 = S_1$$

The last step is to find the error location numbers which are the reciprocal of the roots of $\sigma(x)$. The roots of $\sigma(x)$ can be found simply by substituting $1, \alpha, \alpha^2 \ldots \ldots, \alpha^{n-1} (n = 2^m - 1)$ in to $\sigma(x)$. Since $\alpha^n = 1$, $\alpha^{-l} = \alpha^{n-l}$, therefore α^l is the root of $\sigma(x)$, α^{n-l} is an error location number and received digit r_{n-l} is an erroneous digit. The decoding of binary BCH code is completed adding $(modulo - 2)e(x)$ to the received vector $r(x)$. After locating the error position, the correction is made accordingly to get correct polynomial.

4. ANALYSIS OF THE SIMULATION RESULT

An experimental setup to investigate BER of different BCH codes on AWGN channel is shown in Figure-1:

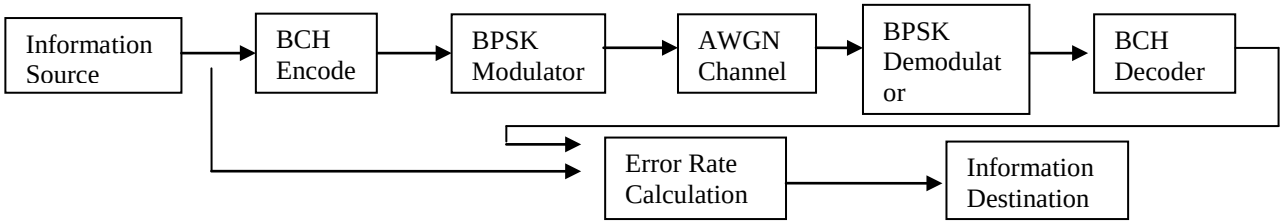

Figure-1: A setup for finding BER

The combination of modulator, channel and demodulator blocks can be replaced by a binary symmetric channel (BSC). The flip probabilities for BSC as calculated by Equation (6) are shown in Table-2.

$$P_b(R) = Q\left(\sqrt{(E_b/N_0)R}\right) \tag{6}$$

$E_b/N_0\,(dB)$	0	1	2	3	4	5	6	7	8
$P_b(R=1)$	0.0786	0.0563	0.0375	0.0229	0.0125	0.0060	0.0024	0.0008	0.0002
$P_b(R=30/63)$	0.1611	0.1366	0.1081	0.0841	0.0598	0.0416	0.0259	0.0141	0.0073
$P_b(R=11/31)$	0.1998	0.1723	0.1444	0.1170	0.0909	0.0671	0.0464	0.0297	0.0172
$P_b(R=5/15)$	0.2071	0.1798	0.1520	0.1244	0.0978	0.0733	0.0516	0.0338	0.0201

Table-2: Flip probabilities of BSC for un-coded and (63, 30, 6), (31, 11, 5) and (15, 5, 3) BCH coded data

The system has been simulated on Simulink 7.1. The number of samples taken for each observation is 10^7. The graph for BER data obtained for each case is shown in Figure-2.

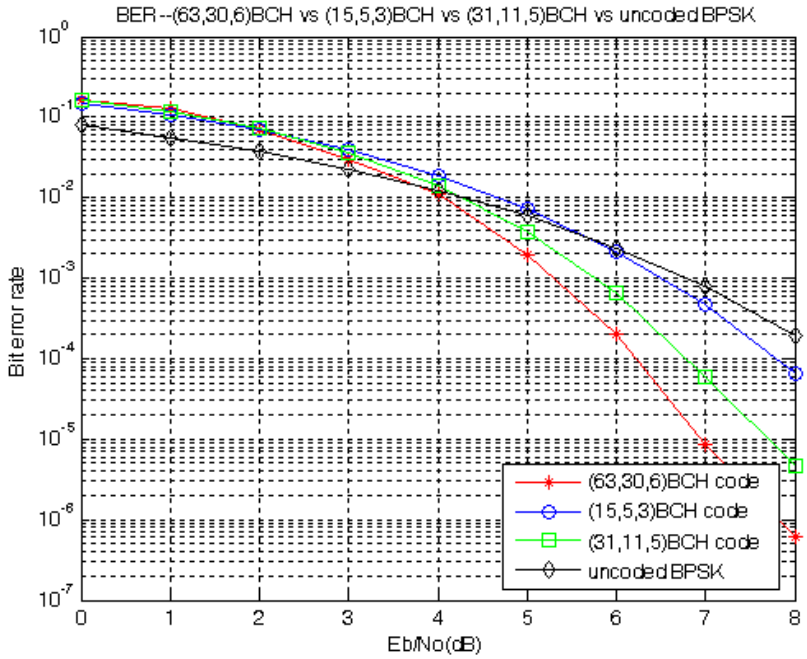

Figure-2: BER for (63, 30, 6), (31, 11, 5) and (15, 5, 3) BCH coded and un-coded data

5. CONCLUSION

There is no improvement by coding in BER below (E_b/N_0) equal to 4dB. Also, for 8dB of (E_b/N_0) the (63, 30, 6) BCH coding provides a gain of 5dB in BER with respect to (31, 11, 5) BCH coding. In general, the higher order of coding provides better performance for (E_b/N_0) from 3dB to 8dB.

REFERENCES

1. W. W. Peterson, "Encoding and error correction procedures for the Bose-Chaudhuri codes", IRE Trans. Inform. Theory, vol. IT-6, pp. 459-470, Sept. 1960.
2. E. R. Berlekamp, "On decoding Bose-Chaudhuri-Hocquenghem codes", IEEE Trans. Inform. Theory, vol. IT-11, pp. 577-580, Oct. 1965.
3. G. D. Forney, "On decoding Bose-Chaudhuri-Hocquenghem codes", IEEE Trans. Inform. Theory, vol. IT-11, pp. 549-557, Oct. 1965.
4. J. L. Massey, Jr., "Shift –register synthesis and BCH decoding", IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, 1969.
5. R. C. Bose, and D. K. Ray-Chaudhuri, "On a class of error correcting binary group Codes", Inform. and Contr., vol.3, pp. 68-79, March 1960.
6. R.C. Bose, and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes", Inform. and Contr., vol.3, pp. 279-290, Sept. 1960.
7. A. Hocquenghem, "Codes correctors d'erreurs" Chiffres, vol.2, pp. 147-156, Sept. 1959.
8. R.E. Blahut, "Transform Technique for error control codes", IBM J. Res. Develop, vol. 23, no.3, pp. 299-315, May 1979.
9. S. Lin, An Introduction to Error-Correcting codes, Prentice Hall, Englewood Cliffs, N. J., 1970.

Source of support: Nil, Conflict of interest: None Declared.