



Design and Implementation of (15,7) BCH Encoder Using labVIEW and its Transmission using NI USRP

Prof. M. D. Bobade¹, Ashru Jadhav², Rachana Khamamkar²

Assistant Professor, Dept. of E&TC, Pune Institute of Computer Technology, Pune, India.¹

B.E Student, Dept. of E&TC, Pune Institute of Computer Technology, Pune, India.²

ABSTRACT: This paper cites the design and implementation of (15,7) BCH encoder using NI labVIEW platform for reliable transfers in AWGN channel with multiple error correction control. The error correcting (15,7) BCH code of block length $n=15$ and message length $k=7$ is evaluated over $GF(2^4)$ with irreducible primitive polynomial x^4+x+1 . Subsequently, the minimal polynomial followed by generator polynomial are computed for (15,7). The designed system is capable of accepting any binary message of length 7 from the user, encode that message into BCH code word using either systematic or non-systematic BCH encoding schemes as per the preference of the user. The thus evaluated coding scheme is proficient enough to correct up to 2 errors that might be introduced over the transmission channel. Each code word comprises of 15 bits with 7 bits of message and 8 (15-7) bits of parity. The BCH encoded message is now all set to be transmitted over a wireless channel with the help of NI USRP (2922) kit after modulation. The main aim of this system is to obtain an error free message at the receiver end after demodulation and decoding.

KEYWORDS: BCH, NI labVIEW, NI USRP (2922), AWGN, error correction, irreducible primitive polynomial, $GF(2^4)$, minimal polynomial, generator polynomial, systematic BCH coding, non-systematic BCH coding.

I. INTRODUCTION

In recent years, there has been an increasing demand for efficient and reliable data transmission and storage systems. This demand has been accelerated by the emergence of large-scale, high-speed data networks for the exchange, processing and storage of digital information in the military, governmental and private spheres. A merging of communications and computer technology is required in the design of these systems. A major concern of the designers is the control of errors so that the reliable reproduction of data can be obtained. Recent developments have contributed towards achieving the reliability required by today's high-speed digital systems and the use of coding for error control has become an integral part in the design of modern communication systems and digital computers.[4]

In a digital communication system, the source encoder removes redundant information from the message signal and is responsible for efficient use of the channel. This data stream is processed by the channel encoder, which produces a new sequence of symbols called the channel code word. The channel code word is longer than the source code word by the virtue of the controlled redundancy built into its construction.[6] The design and implementation of channel encoders is done to combat the noisy environment in which code words must be transmitted or stored.[4]

One of the many channel coding techniques is by using BCH codes. The Bose, Chaudhary and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes. This class of codes is a remarkable generalization of the Hamming codes for multiple-error correction.[5]

Binary BCH codes were discovered by Hocquenghem in 1959 [1] and independently by Bose and Chaudhary in 1960 [2]. The cyclic structure of these codes was proved by Peterson in 1960. [3][5] Error-correcting block codes are widely used to improve the system-level reliability of computer main storage or control storage.[7]



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

II. LITERATURE SURVEY

In [10], they have discussed FPGA implementation of (15, 7) BCH Encoder and Decoder for text message using Verilog Hardware Description Language. Initially they converted each character in a text message is into binary data of 7 bits. These 7 bits are encoded into 15 bit code word using (15, 7) BCH encoder. The thus designed system is capable of detecting and correcting any 2 bit error at any position of 15 bit code word. This corrected data is converted back into an ASCII character. The decoder is implemented using the Peterson algorithm and Chine's search algorithm. It was simulated using Xilinx 12.1 ISE simulator, synthesized using the RTL compiler and finally the design is implemented on Spartan 3E FPGA.

In [9], they have designed and implemented (15, k) a BCH Encoder on FPGA using VHDL with multiple error correction control. Using the cyclic codes, the remainder b(x) is obtained in a linear (15-k) stage shift register with feedback connections corresponding to the coefficients of the generated polynomial. Three encoder are designed using VHDL to encode the single, double and triple error correcting BCH code (15, k) corresponding to the coefficient of generated polynomial. Here we have implemented (15, 5, 3), (15, 7, 2) and (15, 11, 1) BCH code encoder on Xilinx Spartan 3 FPGA using VHDL and the simulation & synthesis are done using Xilinx ISE 13.3.

III. METHODOLOGY

1. CALCULATION OF GENERATOR POLYNOMIAL:

For any positive integers m ($m \geq 3$) and t ($t < 2^{m-1}$), there exists a binary BCH code with the following parameters:

Block length:	$n=2^m - 1$
Number of parity check digits:	$n-k \leq mt$
Minimum distance:	$d_{min} \geq 2t+1$

Clearly this code is capable of correcting any combination of t or fewer errors in a block of n digits. We call this code a t-error-correcting BCH code. In our case, $n=15, k=7$. So, $m=4$ and $2 \leq t$ i.e. this code can correct up to 2 errors.

The generator polynomial of this code is specified in terms of its roots from the Galois field $GF(2^4)$.

Let α be a primitive element in $GF(2^4)$.

The generator polynomial $g(X)$ of the t-error-correcting BCH code of length $2^m - 1$ is the lowest-degree polynomial over $GF(2^m)$ which has $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ as its roots. According to the following theorem,

Theorem: Let $f(X)$ be a polynomial with co-efficients from $GF(2)$. Let β be an element in an extension field of $GF(2)$. If β is a root of $f(X)$, then for any $l \geq 0, \beta^{2^l}$ is also a root of $f(X)$.

The element β^{2^l} is called a conjugate of β . Thus, it can be said that $g(X)$ has $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{2t}$ and its conjugates as its roots. Minimal polynomials of α, α^3 and α^5 can be evaluated respectively as, [4]

$$\phi_1(X)=1+X+X^4, \quad \phi_3(X)=1+X+X^2+X^3+X^4, \quad \phi_5(X)=1+X+X^2.$$

$G(X)$ must be the least common multiple of $\phi_1(X), \phi_2(X), \dots, \phi_{2t}(X)$.

$$g(X)=LCM\{ \phi_1(X), \phi_2(X), \dots, \phi_{2t}(X) \} \quad \dots (1.)$$

But, from the theorem stated above, every power of α in the sequence of (1.) has the same minimal polynomial as some preceding odd power of α in the sequence.

$$g(X)=LCM\{ \phi_1(X), \phi_3(X), \dots, \phi_{2t-1}(X) \} \quad \dots (2.)$$

In our case, $t=2$ and so, $g(X)=LCM\{ \phi_1(X), \phi_3(X) \}$. Since $\phi_1(X)$ and $\phi_3(X)$ are two distinct primitive polynomials,

$$g(X)= \phi_1(X) \cdot \phi_3(X) = (1+X+X^4)(1+X+X^2+X^3+X^4) = 1+X^4+X^6+X^7+X^8. \quad \dots (3.)$$

2. EVALUATING THE CODE WORD:

Cyclic codes have the property that the code vectors are generated by multiplying the message polynomial $m(X)$ by generator polynomial $g(X)$. In fact, in the non-systematic form, the message polynomial $m(X)$ is multiplied by



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

generator polynomial $g(X)$, and in the systematic form there is an equivalent polynomial $q(X)$ that is multiplied by generator polynomial $g(X)$. Let $m=[1010101]$ i.e. $m(X)=1+X^2+X^4+X^6$.

a.) Non-systematic code word:

$$c(X) = m(X) \cdot g(X) = (1+X^2+X^4+X^6) \cdot (1+X^4+X^6+X^7+X^8) = 1+X^2+X^6+X^7+X^8+X^9+X^{10}+X^{11}+X^{13}+X^{14}$$
$$c=[110111111000101]$$

b.) Systematic code word:

$$c(X) = X^{n-k} \cdot m(X) + \text{rem}[X^{n-k} \cdot m(X)/g(X)]$$
$$= (X^8+X^{10}+X^{12}+X^{14}) + \text{rem}[(X^8+X^{10}+X^{12}+X^{14}) / (1+X^4+X^6+X^7+X^8)]$$
$$= 1+X^2+X^5+X^6+X^7+X^8+X^{10}+X^{12}+X^{14}$$
$$c=[101010111100101]$$

IV. PROPOSED ALGORITHM

A. Evaluate systematic and non-systematic code words.

a. Systematic code word

1. for($i=1$ to 7)
 - if (message bit is $\neq 0$)
 - $[ones]_{1 \times 15}$ and
 - $((X^{n-k} \lll 7)$ right rotated i times)
 - else($[zeros]_{1 \times 15}$)
2. Exor elements of each column of above matrix. Let this be matrix $[S]_{1 \times 15}$.
3. Calculate remainder of $\{[S]/[G]\}$.
4. Exor $[S]$ and matrix obtained from step 3. This is the systematic code word.

b. Non-systematic code word

1. for($i=1$ to 7)
 - if (message bit is $\neq 0$)
 - $[ones]_{1 \times 15}$ and
 - $([G] \lll 6)$ right rotated i times)
 - else($[zeros]_{1 \times 15}$)
2. Exor elements of each column of above matrix. This is the non-systematic code word.

B. If (Boolean = false), select systematic code word else send non-systematic code word.

C. Perform modulation wrt selected code word.

D. Transmit signal using USRP transmitting antenna from a computer.

E. Receive the signal using USRP receiving antenna on another computer.

F. Demodulate and decode the signal to obtain an errorless message.

For instance,

Consider message signal $[m]=[1010101]$,

For non-systematic encoding, $[G]=[111010001]$ and therefore, $([G] \lll 6) = [111010001000000]$

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

So, from step 1 of non-systematic code word evaluation, we get,

$$i/p : \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

7x15

step 2. \Rightarrow 1 1 0 1 1 1 1 1 1 0 0 0 1 0 1

We get the same result even by simple multiplication:

$$\begin{array}{r} 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1 \\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \\ \hline 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ * \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ * \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ * \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ * \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ * \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ * \\ \hline 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1 \end{array}$$

V. ARCHITECTURE OF BCH ENCODER

Circuit for BCH encoder (Block diagram):

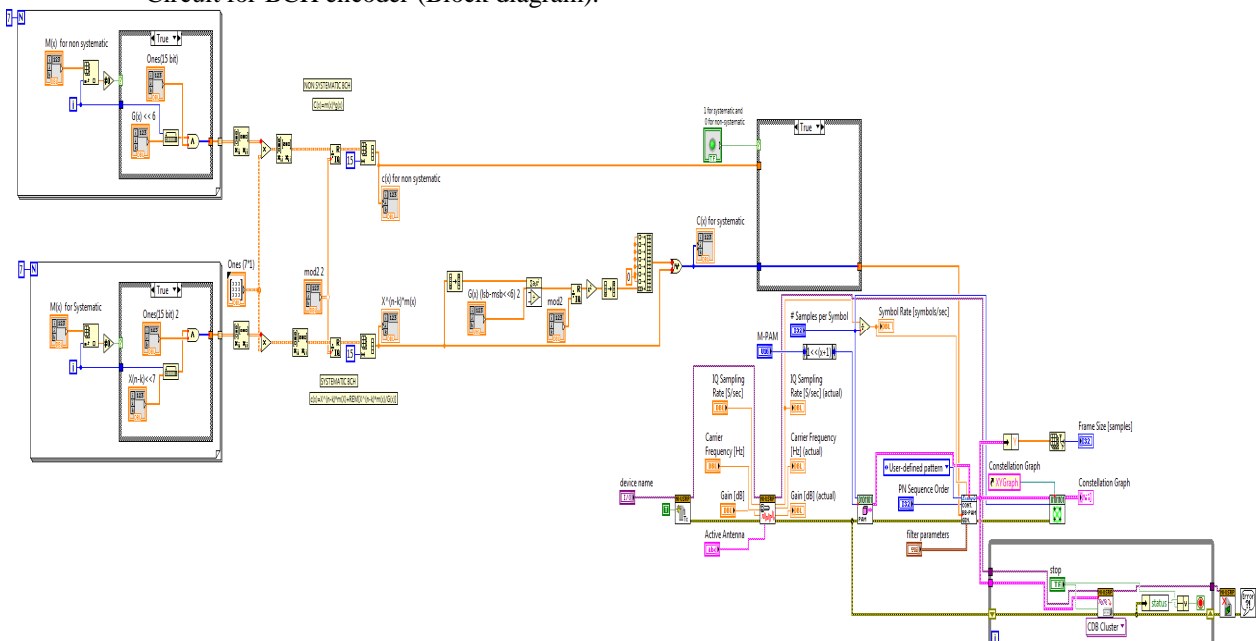


Figure 1. Block diagram of BCH encoder at transmitter end.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

VI. SIMULATION RESULTS

Transmitter (front panel):

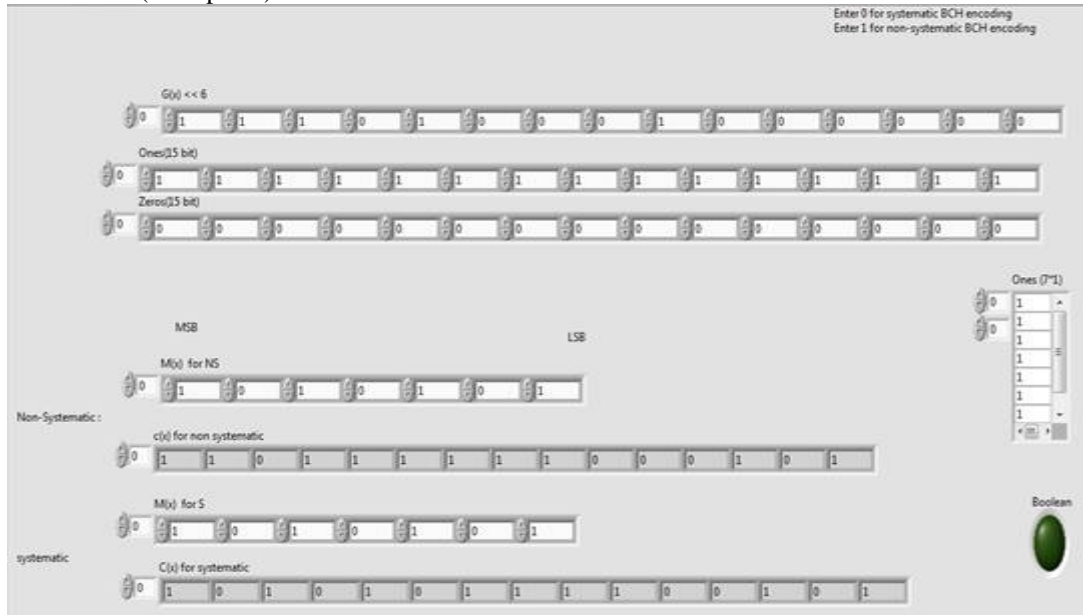


Figure 2. Front panel of BCH encoder at transmitter end.

Receiver (front panel):

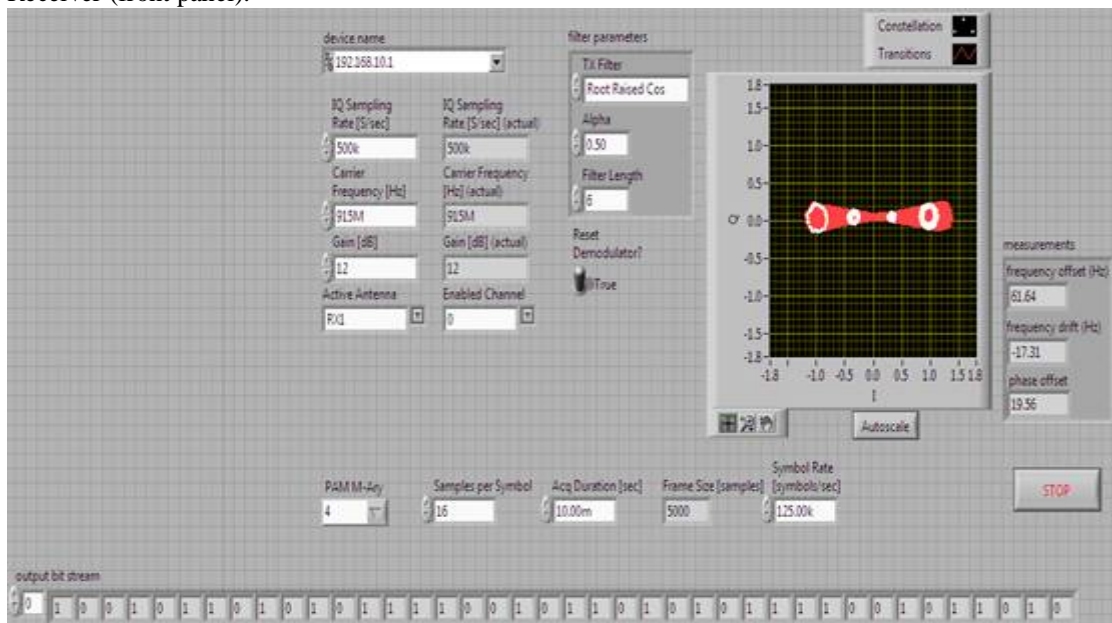


Figure 3. Front panel of BCH encoder at receiver end.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 6, June 2017

Result table:

Coding scheme	Message	Transmitted bits		Decoded message
		Message bits	Parity bits	
Systematic	1010101	1010101	11100101	1010101
Non-systematic	1010101	110111111000101		1010101

VII. CONCLUSION

In a nutshell, the role of error correcting BCH code is extremely vital in order to obtain an error-free message at the receiver. In this paper, we have discussed the design and implementation of (15, 7) BCH encoder which can correct up to two errors. The 7 bit pattern entered by the user is encoded systematically as well as non-systematically using labVIEW. The encoded message is modulated and transmitted with the help of NI USRP (2922) kit. Another NI USRP receiver kit, receives that signal on some other computer. Down the line, the results can evidently be verified by decoding the received code word. Decoding the erroneous received code word too, yields the same 7 bit pattern that was entered by the user.

REFERENCES

- [1]. A. Hocquenghem, "Codes correcteurs d'erreurs," *chiffers*, 2, pp. 147-156, 1959.
- [2]. R. C. Bose and D. K. Ray-Chaudhary, "On a Class of Error Correcting Binary Group Codes," *Inf. Control*, 3, pp. 68-79, March 1960.
- [3]. W.W. Peterson, "Encoding and Error Correcting Procedures for the Bose-Chaudhary codes," *IRE Trans. Inf. Theory*, IT-6, pp. 459-470, September 1960.
- [4]. S. Lin, and D.J. Costello Jr. - "Error Control Coding", Prentice-Hall, New Jersey, 1983, page 1-38.s
- [5]. S. Lin, and D.J. Costello Jr. - "Error Control Coding", Prentice-Hall, New Jersey, 1983, page 141-151.
- [6]. Simon Hykin - "Digital Communication Systems", Wiley, USA.
- [7]. S. Lin, and D.J. Costello Jr. - "Error Control Coding", Prentice-Hall, New Jersey, 1983, page 498.
- [8]. J. C. Moreira and Patrick Guy Farrell - "Essentials of Error- Control Coding", Wiley, England.
- [9]. M. Divya, K. Vinodalakshmi, G. Sumalatha, Shahbazsarik, Abhishek Awasthi, "Design and Implementation of Encoder for (15, k) Binary BCH Code Using VHDL and eliminating the fan-out"-IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), vol:7, issue:6, Sept-Oct (2013).
- [10]. Rohith S, Pavithra S, " FPGA Implementation of (15,7) BCH encoder and decoder for text message"-International Journal of Research in Engineering and Technology, vol:02, Issue: 09, page no.-209-214, Sept-2013.