BCH CODES AND ITS APPLICATION BY POLYNOMIAL

Mohammad Hussain Farahi
Abdul Razeq Rahmani
Mathematics department, Education Faculty, Farah Institute of Higher Education, Farah Afghanistan

ABSTRACT

The paper presents the result of the research BCH Codes and its Application by polynomial presented. In the research work we used foreign reliable sources and materials. The BCH Codes and its Application by polynomial is very useful and usable in human life. Coding theory deals with the fast and accurate transmission of massages information over an electronic channel (telephone, telegraph, radio, TV, satellite, computer rely, etc.) that is affected by noise. The atmospheric conditions, interference from nearby electronic devices equipment failures. A variety of algebraic concepts can be used to describe BCH codes. In this research paper we discuss a class of codes called BCH codes that are linear and can be constructed to be multiple-error correcting. BCH codes are named for their creators Bose, Chaudhary, and Hocquenghem also we clarified that with some useful examples.

Keywords: BCH codes, code words, polynomials, error-correcting codes.

1. Introduction

Some of the most important codes, discovered independently by A.

Hocquenghem in 1959 and by R. C. Bose and D. V. Ray-Chaudhary in 1960, are BCH codes. The European and transatlantic communication systems both use BCH codes. Information words to be encoded are of length 231, and a polynomial of degree 24 is used to generate the code. Since $231 + 24 = 255 = 2^8 - 1$, we are dealing with a (255,231)-block code. This BCH code will detect six errors and has a failure rate of 1 in 16 million. One advantage of BCH codes is that efficient error correction algorithms exist for them. The idea behind BCH codes is to choose a generator polynomial of smallest degree that has the largest error detection and error correction capabilities. Let $d = 2r + 1$ for some $r \geq 0$. Suppose that ω is a primitive nth root of unity over Z_2, and let $m_i(x)$ be the minimal polynomial over Z_2 of ω^i. If

$$g(x) = 1cm[m_1(x), m_2(x), \dots, m_{2r}(x)],$$

Then the cyclic code $hg(t)i$ in Rn is called the BCH code of length n and distance d. The minimum distance of C is at least d.

Theorem 1. Let $C =< g(t) > be$ be a cyclic code in R_n. The following statements are equivalent.

1. The code C is a BCH code whose minimum distance is at least d.

2. A code polynomial $f(t)$ is in C if and only if $f(\omega^i) = 0 \; for \;\; 1 \leq i < d.$

3. The matrix

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{n-(2)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{n-1(3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2r} & \omega^{4r} & & \omega^{(n-1)(2r)} \end{pmatrix}$$

Is a parity-check matrix for C.

Proof. (1) $\Rightarrow$ (2). If $f(t)$ is in C, then $g(x)/f(x) in\, Z_2[x]$. Hence, for $i = 1, \dots, 2r, f(\omega^i) = 0.$ since $g(\omega^i) = 0$ Conversely, suppose that $f(\omega^i)$ for $1 \leq i \leq d$. Then $f(x)$ is divisible by each $m_i(x)$ since $m_i(x)$ is the minimal polynomial of ω^i. Therefore, $g(x)/f(x)$ by the Definition of $g(x)$. Consequently, $f(x)$ is a codeword.

2) $\Rightarrow$ (3). Let $f(t) = a_0 + a_1 t + \cdots + a_{n-1} v t^{n-1}$ be in R_n. The corresponding n-tuple in Z_2^n is $x = (a_0 a_1 \dots a_{n-1})^t$ By (2),

$$Hx = \begin{pmatrix} a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} \\ a_0 + a_1\omega^2 + \cdots + a_{n-1}(\omega^2)^{n-1} \\ \vdots \\ a_0 + a_1\omega^{2r} + \cdots + a_{n-1}(\omega^2)^{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} f(\omega) \\ f(\omega^2) \\ \vdots \\ f(\omega^{2r}) \end{pmatrix} =$$

Exactly when $f(t)$is in C. Thus, H is a parity-check matrix for C.

(3) $\Rightarrow$ (1). By (3), a code polynomial $f(t) = \; a_0 + a_1 t + \cdots + a_{n-1} t^{n-1}$ is in C exactly when$f(\omega^i) = 0 \;\; for\, i = 1, \dots, 2r.$ Thesmallest such polynomial is $g(t) = 1cm[m_1(t), m_2(t)], = 1cm[m_1(t), \dots, m_{2r}(t)]$. therefore, $C =< g(t)$.

Example 1. It is easy to verify that $x^{15} - 1 \in Z_2[x]$. has a factorization

$x^{15} - 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 x + 1),$ Where each of the factors is an irreducible polynomial. Let ω be a root of $1 + x + x^4$. The Galois field GF (2^4) is

$$\{a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 : a_i \in Z_2 \quad and \;\; 1 + \omega + \omega^4\}.$$

ω is a primitive 15th root of unity. The minimal polynomial of ω is

$m_1(x) = 1 + \omega + \omega^4$. It is easy to see that ω^2 and ω^4 are also roots of $m_1(x)$. the minimal polynomial of ω^3 is $1 + x + x^2 + x^3 + x^4$. Therefore,

$$g(x) = m_1(x)m_2(x) = 1 + x^4 + x^6 + x^7 + x^8$$

has roots $\omega, \omega^2, \omega^3, \omega^4$. Since both $m_1(x)$ and $m_2(x)$ divide $x^{15} - 1$, the BCH code is a $(15, 7)$ −code. If $x^{15} - 1 = g(x)h(x), then\ h(x) = 1 + x^4 + x^6 + x^7$; therefore, a parity-check matrix for this code is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. Construction of BCH Codes

One way that BCH codes differ from the codes which we will discuss on here. BCH codewords are polynomials rather than vectors. To construct a BCH code, we begin by letting $f(x) = x^{m-1} \in Z_2[x]$ for some positive integer m. Then $R = Z_2[x]/(f(x))$ is a ring that can be represented by all polynomials in $Z_2[x]$ of degree less than m. Suppose $g(x) \in Z_2[x]$ divides $f(x)$. Then $C = \{multiples\ of\ g(x)\ in\ Z_2[x]$ of degree less than m$\}$ is a vector space in R with dimension m – deg $g(x)$. Hence, the polynomials in C form codewords in an $[m, m - deg\ g(x)]$ linear code in R with $2^{m-\deg g(x)}$ codewords. The polynomial $g(x)$ is called a generator polynomial for the code. We consider the codewords in this code to have length m positions because we view each term in a polynomial codeword as a codeword position. A codeword $c(x) \in Z_2[x]$ with m terms can naturally be expressed as a unique vector in Z_2^m by listing the coefficients of c(x) in order (including coefficients of zero). In this book we will assume BCH codewords are transmitted this way with increasing powers of x.

Example 2. Let $f(x) = x^7 - 1$ and $g(x) = x^3 + x + 1\ in\ Z_2[x]$. Then the code C of multiples of $g(x)$ in $Z_2[x]$ of degree less than 7 has basis $\{x^3 + x + 1,\ \ x^4 + x^2 + x,\ x^5 + x^3 + x^2,\ x^6 + x^4 + x^3\}$ Hence, C is a [7,4] code with 16 codewords consisting of all linear combinations of these basis polynomials in $Z_2[x]$. In this code, we will assume that the codeword $x^5 + x^4 + x^3 + x$ would be transmitted as the vector $0 + 1x + 0x^2 + 1x^3 +$

$1x^4 + 1x^5 + 0x^6 = (0101110) \in Z_2^7$. ■

For a code constructed as described above to be a BCH code, the generator polynomial g(x) must be chosen as follows. Let $a_1, a_2, \dots, a_s$ for $s < m$ be roots of $f(x)$ with minimum polynomials $m_1(x), m_2(x), \dots, m_s(x)$ in $Z_2(x)$ respectively, and let g(x) be the least common multiple of the polynomials $m_i(x)$ in $Z_2[x]$ .Note that g(x) divides $f(x)$, so g(x) can be used as the generator polynomial for a code. Choosing g(x) in this manner is useful because of how it allows errors to be corrected in the resulting code. We will discuss BCH error correction in Section 2. Actually, choosing a generator polynomial as just described still does not necessarily yield a BCH code. For the resulting code to be a BCH code, the values of m and the roots a_i must be chosen in a special way. We describe this next.

Let $m = 2^m - 11$ for some positive integer n, and let $f(x) = x^m - 1$ in $Z_2[x]$ .Suppose $p(x)$ is a primitive polynomial of degree n in $Z_2[x]$. Then $Z_2[x]/(p(x))$ is a field of order 2^n whose nonzero elements are generated by the field element x. We will denote the element x in this field by a. Then, for the roots a_i described in the previous paragraph, we let $a_i = a^i \; for \; i = 1, \dots, s.$ Choosing the a_i in this manner is useful because of how it allows the generator polynomial g(x) to be determined. The polynomials $m_i(x)$ described in the previous paragraph are then the minimum polynomials of a^i for $i = 1, \dots, s.$ .Thus, we can determine g(x) by forming the product that includes a single factor of each unique $m_i(x)$ As a consequence of Lagrange's Theorem (Theorem 1.), a^i will be a root of $f(x)$ for all i. Hence, g(x) will divide $f(x)$.

Because BCH codewords are in $Z_2[x]$, some of the computations that are necessary for constructing BCH codes can be done very easily. Specifically, note that $(x_1 + x_2 + \cdots + x_r^2)^2 = x_1^2 + x_2^2 + \cdots + x_r^2$ over Z_2 since all cross terms will contain a factor of 2. Therefore, for a polynomial $h(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_r} \in Z_2[x]$, it follows that $h(a^2) = (a^2)^{i_1} + (a^2)^{i_2} + \cdots + (a^2)^{i_r} = \left(a^{i_1} + a^{i_2} + \cdots + a^{i_r}\right)^2 = h(a^2)$. Similarly, it can be seen that $h(a^{2k}) = h(a^k)^2$ for any positive integer k. Thus, for example, $h(a^{12}) = h(a^6)^2 = h(a^3)^4$. The utility of this will be clear in the following examples.

Example 3. Let $f(x) = x^7 - 1$, and choose the primitive polynomial $p(x) = x^3 + x + 1$ in $Z_2[x]$ Then for the element $a = x$ in the field $Z_2[x]/p(x)$ of order 8, we list the field elements that correspond to the first seven powers of a in the following table.

power Field Element

a^1	a
a^2	a^2
a^3	$a+1$
a^4	a^2+a
a^5	a^2+a+1
a^6	a^2+1
a^7	1

Let C be the BCH code that results from considering the first four powers of a. To determine the generator polynomial g(x) for C, we must find the minimum polynomials $m_1(x)$, $m_2(x)$, $m_3(x)$ and $m_4(x)$. But since $p(x)$ is primitive and $a = x$, it follows that $p(a) = 0$. Furthermore, $p(a^2) = p(a)^2 = 0$ and $p(a^4) = p(a)^4 = 0$, since $p(x) \in Z_2[x]$. Thus $m_1(x) = m_2(x) = m_3(x) = m_4(x) = p(x)$. Now, since a^3 is a root of $f(x)$ the minimum polynomial $m_3(x)$ of a^3 must be one of the irreducible factors of $x^7 - 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$. By substituting a^3 into each of these irreducible factors, we can find that $x^3 + x^2 + 1$ is equal to zero when evaluated at a^3. Hence, $m_3(x) = x^3 + x^2 + 1$. Thus, g(x) = $m_1(x)m_3(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ The code that results from this generator polynomial is a [7,1] BCH code with basis {g(x)} and two codewords.

Example 4. a. if $n = 1$ it is clear, if n =2

$$(f_1 + f_2)^2 = f_1^2 + 2f_1f_2 + f_2^2 = f_1^2 + f_2^2. \quad in\ general$$

$$(f_1 + \cdots + f_{n+1})^2 = (f_1 + \cdots + f_n)^2 + f_{n+1}^2 = f_1^2 + \cdots + f_n^2 + f_{n+1}^2.$$

$$b.If \quad f = a_0 + a_1x + \cdots \ then \ f' = a_1x + a_3x^2 + a_5x^4 + \cdots = g(x^2) \quad where$$

$$g = a_1 + a_3x + \cdots .conversely, \quad f = g(x^2) = b_0 + b_1x^2 + b_2x^4 + \cdots clearly$$

$$implies\ that\ f = 0(as\ 2 = 0\ in\ Z_2).$$

$$if \quad n = 2^k\ then$$

$$1 - x^4 = (1 - x^2)(1 + x^2) = (1 + x^4),$$

$$1 - x^8 = (1 - x^4)(1 + x^4) = (1 + x^8)$$

$$and, by\ induction, \ 1 - x^{2^k} = (1 + x)^{2^k}; \ that\ is\ 1 - x^n = (1 + x)^n.$$

So the divisors of $1 - x^n$ are 1, $(1 + x), (1 + x)^2, \ldots, (1 + x)^n$, and there are a chain under divisibility. Conversely, if $1 - x^n = (1 + x)^k p^m$ ... where p is irreducible and $p \neq (1 + x)$, then neither $1 + t\ nor\ (p(t))$ contain the other in B_n.

d. If $n = 2^k m$ the, m odd, then

$$1 + x^n = \left(1 + x^{2^k}\right)^m = 1 + mx^{2^k} + \cdots + x^n$$ a

contradiction as $m = 1 \quad in\ Z_2$.

E. In B_4: $1+t,\ t+t^2=t(1+t),\ t^2+t^3=t^2(1+t)\ and\ 1+t^3=t^3(1+t)$.

The other members $0, 1+t^2,\ t+t^2\ and\ 1+t+t^2+t^3$ all lie in smaller ideals.

3. Error Correction in BCH Codes

The generator polynomial for a BCH code is chosen in a special way because of how it allows errors to be corrected in the code. Before discussing the BCH error correction scheme, we first note the following theorem.

Theorem 2. Let C if be a BCH code that results from a primitive polynomial of degree n by considering the first s powers of a, and suppose $c(x) \in Z_2[x]$ has degree less than 2^n-1. Then $c(x) \in c$ if and only if $c < a^i >= 0$. For $i = 1, \dots, s$.

Proof. Let $m_i(x)$ be the minimum polynomial of a^i in $Z_2[x]$ for $i = 1, \dots, s$, and let $g(x)$ if be the least common multiple of the polynomials $m_i(x)$ in $Z_2[x]$. If $c(x) \in C, \in$ then $c(x) = g(x)h(x)$ for some $h(x) \in Z_2[x]$. Thus,$c(a^i)h(a^i) = 0h(a^i) = 0 \quad for\ i = 1, \dots, s$. Conversely, if $c(a^i = 0\ for\ i = 1, \dots, s$, then $m_i(x)$divides $c(x)$ for $i = 1, \dots, s$. Hence, $g(x)$ divides $c(x)$ and $c(x) \in C$.

Example 5. We may construct all binary BCH codes of block length 31. Minimal polynomials of elements in $GC(2^5)$. the codes of these generator polynomials

$$t = 1 \qquad g(x) = m_1(x)m_2(x)$$
$$= 1 + x^3 + x^5 + x^6 + x^8 + x^9 + x^{10} \quad or\ g = 10010110111$$
$$t = 3 \quad g(x) = m_1(x)m_3(x)m_5(x)$$
$$g = 101010110110010001101$$
$$t = 6 \quad or \quad t = 7 \quad g(x) = m_1(x)m_3(x)m_5(x)m_7(x)m_{11}(x)$$
$$g = 11100100010101111011010011$$
$$t = 8,9, \dots, or\ 15$$
$$g(x) = m_1(x)m_3(x)m_5(x)m_7(x)m_{11}(x)m_{15}(x)$$
$$g = 1111111111111111111111111111111$$

The single-error-correcting code has 5 cheek digits, 26 message digits, and rate 26⁄31.

4. Polynomial BCH Codes

With knowledge of polynomial rings and finite fields, it is now possible to derive more sophisticated codes. First let us recall that an (n,k) −block code consists of a one-to-one encoding function $E: Z_2^k \to Z_2^n$ and a decoding function $D: Z_2^k \to Z_2^n$. The code is error-correcting if D is onto. A

code is a linear code if it is the null space of a matrix $H \in M_{k\times n}(Z_2)$.

We are interested in a class of codes known as cyclic codes. Let $\varphi: Z_2^k \to Z_2^n$ φ: be a binary (n,k) −block code. Then φ is a cyclic code if for every codeword $(a_1, a_2, \dots, a_n)$ the cyclically shifted n-tuple $(a_n,\ a_1,\ a_2, \dots, a_{n-1})$ is also a codeword. Cyclic codes are particularly easy to implement on a computer using shift registers.

Example 6. Consider the $(6,3)$ −linear codes generated by the two matrices

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad and \quad G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Messages in the first code are encoded as follows:)

$(000) \mapsto (000000)$ $(100) \mapsto (100100)$
$(001) \mapsto (001001)$ $(101) \mapsto (101101)$
$(010) \mapsto (010010)$ $(110) \mapsto (110110)$
$(011) \mapsto (011011)$ $(111) \mapsto (111111)$

It is easy to see that the codewords form a cyclic code. In the second code, 3-tuples are encoded in the following manner:

$(000) \mapsto (000000)$ $(100) \mapsto (111100)$
$(001) \mapsto (001111)$ $(101) \mapsto (110011)$
$(010) \mapsto (011110)$ $(110) \mapsto (100010)$
$(011) \mapsto (010001)$ $(111) \mapsto (101101)$

This code cannot be cyclic, since (101101) is a codeword but (011011) is not a codeword. We would like to find an easy method of obtaining cyclic linear codes. To accomplish this, we can use our knowledge of finite fields and polynomial rings over Z_2 Any binary n-tuple can be interpreted as a polynomial in $Z_2[x]$. Stated another way, the n-tuple $(a_0 + a_1x + \cdots, a_{n-1})$, corresponds to the polynomial

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

where the degree of $f(x)$ is at most $n-1$. For example, the polynomial corresponding to the 5-tuple (10011) is.

$$1 + 0x + 0x^2 + 1x^3 + 1x^4 = 1 + x^3 + x^4$$

Conversely, with any polynomial $f(x) \in Z_2[x]$. with deg $f(x) < n$ we can associate a binary n-tuple. The polynomial $x + x^2 + x^4$ corresponds to the 5-tuple (01101). Let us fix a nonconstant polynomial $g(x)$. in $Z_2[x]$. of degree $n - k$. We can define an (n,k) −code C in the following

manner. If $a_0+, \dots, a_{k-1}$ is a k- tuple to be encoded, then

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$$

is the corresponding polynomial in $Z_2[x]$. To encode $f(x)$, we multiply by $g(x)$. The codewords in C are all those polynomials in $Z_2[x]$. of degree less than n that are divisible by $g(x)$. Codes obtained in this manner are called polynomial codes.

Example 7. If we let $g(x) = 1 + x^3$, we can define a $(6,3)-$code C as follows. To encode a 3-tuple $(a_0,\ a_1,\ a_2)$ we multiply the corresponding polynomial $f(x) = a_0 + a_1x + a_2x^2$ by $1 + x^3$ we are defining a map $\varphi: Z_2^3 \to Z_2^6$ by $\phi: f(x) \mapsto g(x)f(x)$. It is easy to check that this map is a group homomorphism. In fact, if we regard Z_2^n as a vector space over Z_2 $\emptyset$ is a linear transformation of vector spaces. Let us compute the kernel of φ. Observe that $\emptyset(a_0,\ a_1,\ a_2) = (000000)$ exactly when

$$0 + 0x + 0x^2 + 0x^3 + 0x^4 = (1 + x^3)(a_0 + a_1x + a_2x^2 =$$
$$= a_0 + a_1x + a_2x^2 + a_0x^3 + a_1x^4 + a_2x^5$$

Since the polynomials over a field form an integral domain, $a_0 + a_1x + a_2x^2$ must be the zero polynomial. Therefore, ker $\varphi = \{(000)\}$ and φ is one-to-one.

To calculate a generator matrix for C, we merely need to examine the way the polynomials $1, x$ and x^2 are encoded:

$$(1 + x^3)\,.1 = 1 + x^3$$
$$(1 + x^3)x = x + x^4$$
$$(1 + x^3)x^2 = x^2 + x^5.$$

We obtain the code corresponding to the generator matrix G_1 in Example 4. The parity-check matrix for this code is

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Since the smallest weight of any nonzero codeword is 2, this code has the ability to detect all single errors.

5. BCH Decoding. Let v be a codeword and suppose that at most t errors occur in transmitting it by using a BCH code of designed distance $d \geq 2t + 1$. For decoding a received word w, the following steps are executed:

Step 1. Determine the syndrome of ω, where

$$G(x) = (G_{cr}G_{c+1}, \dots, G_{c+d-2})^T$$

Step 2. Determine the maximum number $r \leq t$ of equations of the form

$$G_j g_0 + G_{j+1} g_1 + \cdots + G_{j+r} = 0, \qquad c \leq j \leq c + r - 1,$$

such that the coefficient matrix of the g_i is nonsingular and thus obtain the number r of errors that have occurred. Solve this maximal system and form the error-locator polynomial

$$g = \sum_{i=0}^{i} g_i x_i \qquad with \;\; g_0 := 1$$

Step 3. Find the zeros of s by trying $x^0, x^1, \ldots$

Step 4. For binary codes, the zeros $x^{i_1}, \ldots, x^{i_r}$ determine e already.

Otherwise, the e_i can be obtained from the equations $\sum_{i \in I} e_i \, x^{ij} = 0 \; for \; j \in \{c, c+1, \ldots, c+d-2\}$ (since I is known now).

Conclusion

Human minds are designed for pattern recognition and we can find algebraic structures and applications in common objects and things around us BCH Codes and its Application by polynomial is an application of algebra that has become increasingly mportant over the last several decades. When we transmit data, we are concerned about sending a message over a channel that could be affected by "noise." We wish to be able to encode and decode the information in a manner that will allow the detection, and possibly the correction, of errors caused by noise. This situation arises in many areas of communications, including radio, telephone, television, computer communications, and even compact disc player technology. BCH Codes and its Application by polynomial, which is the main part of the paper, here we clarified that and its components like coding, encoding, decoding, in $Z_2[x]$ and decoding techniques. For more clarity, we used some of important theorems and useful examples.

REFERENCES

[1] Abramson, N. M., A Class of Systematic Code for Non-Independent Errors, IEEE Trans. Inform. Theory, 1950; 150-157.

[2] Berlecamp, E. R., A Cass of convolution codes, 1963; 1-13.

[3] Cohen, E. L., A note on perfect double error-correcting codes on q symbols, 1964; 381-384.

[4] Epstein, M. A., Algebraic decoding for a binary erasure channel, M. I. T. Res. Lab. Electron, 1958; 341.

[5] Elwyn Berlekamp; Algebraic coding theory. Revised Edition by World Scientific publishing Co. Ptc.Ltd, 2015; 176-177.
[6] Klima, Richard E. Applications of abstract algebra with Maple / Richard E. Klima, Neil P. Sigmon, Ernest Stitzinger,1999; 76-79.
[7] Nicholson, W. Keith. Introduction to abstract algebra, University of Calgary, Canada - 4th ed 2012; 160.
[8] Rudolf Lidl. Gunter Pilz. Applied Abstract Algebra. Second Edition. Springer-Verlag New York, 1998; 233.
[9] Thomas W. Hungerford. Abstract algebra an introduction. Third addition, Saint Louis University, Brooks/Close. Cengage Learning, 2014.
[10] Thomas W. Judson Stephen F. Abstract Algebra Theory and Applications. Austin State University August 11, 2012; 363-372.
[11] Ю. И. Журавлёв, Ю. А. Флёров, М. Н. Вялый. Основы высшей алгебры и теории кодирования Учебные материалы к курсу. Вариант от 28 апреля 2019 г.