IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2022.Doi Number

Construction and Decoding of BCH-Codes over the Gaussian Field

Muhammad Sajjad[1], Tariq Shah[1], Maha Alammari[2] and Huda Alsaud[2]

[1] Department of Mathematics, Quaid-I-Azam University, Islamabad 45320, Pakistan
[2] Department of Mathematics, College of Science, King Saud University, P.O. Box 22452 Riyadh 11495, Saudi Arabia

Corresponding authors: Muhammad Sajjad (m.sajjad@math.qau.edu.pk).

Acknowledgment: Researchers Supporting Project number (RSP 2023R472), King Saud University, Riyadh, Saudi Arabia.

ABSTRACT In this article, first we deliberate the theory of the Gaussian field and extension field of the Gaussian field. However, in the second phase, we provide a comprehensive construction scheme for BCH codes over the Gaussian field. The decoding of newly designed BCH codes is handled through a slightly amended modified Berlekamp-Massey algorithm. The coding gain is obtained by BCH codes over the Gaussian field. Accordingly, a better code rate and the number of code words are obtained as compared to the BCH codes over finite fields. Thus, this makes them a promising candidate for use in communication systems.

INDEX TERMS Gaussian integers, Gaussian field, BCH codes, and Berlekamp-Massey algorithm.

I. INTRODUCTION

T Regardless of the Field-linear coding theory, the Ring-linear coding theory is a discipline of algebraic coding theory where the primary alphabet transport the structure of a finite ring or, more generally, of a module. Such a setup was given much firmer than usually assumed: Assmus and Mattson (1963) [1] first reference the elements of rings as possible alphabets for linear codes in their contribution ‘Error-Correcting Codes: An Axiomatic Approach’. It took substantial time for ring-linear coding theory to cultivate from these origins to the contemporary. For an introduction to linear and cyclic codes over fields, see Augot et al. (2009) [2]. In the seventies of the 20th century, Blake (1972, 1975) [3,4] offered linear codes first over semi-simple, and later over primary integer residue rings. Analogs of Hamming, Reed–Solomon, and BCH Codes were also introduced. Spiegel (1977, 1978) [5, 6] pursued a group-algebraic approach to linear codes over $\mathbb{Z}_n$. Blake used the Chinese Remainder Theorem to examine BCH Codes over these rings. While the notion of BCH codes over Galois fields was established in 1958. Shah et al. constructed codes by the semigroup ring $B[X;1/2^2\mathbb{Z}_0]$ and encoding in [7]. The authors [8-10] presented cyclic codes over $\frac{F_2[u]}{u^4-1}$ and their applications to DNA codes. Kim et al. [11] constructed another infinite family of Griesmer quasi-cyclic self-orthogonal codes in this continuation. In the recent, Zullo [12] constructed multi-orbit cyclic subspace codes and linear sets. The authors have constructed codes and used these in cryptography by vectorial algebra [13-15]. Lei et al. [16] presented the results on hulls of some primitive binary and ternary BCH codes. Furthermore, Liu et al. [17] constructed binary BCH codes with length $n = 2^m + 1$.

Gaussian integers are a generalization of the usual concept of rational integers to the complex plane. They are defined as numbers of the form $a + bi$, where a and b are integers and i is the imaginary unit, which satisfies the equation $i^2 = -1$. These numbers can be added, subtracted, multiplied, and divided, like rational integers. The study of Gaussian integers falls in algebraic number theory, a branch of number theory. Error-correcting codes are essential in modern communication systems and allow for detecting and correcting errors that occur during data transmission. One class of error-correcting codes that has been widely studied and used in practice is BCH codes, a class of cyclic codes. These BCH codes are parameterized randomly error-correcting codes, making them suitable for use in noisy communication channels [18]. Usually, BCH codes have been studied and built over finite Galois fields [18]. Huber [19] defined a two-dimensional modular distance and proposed codes for it. Simple constructions of such codes are classified as consta-cyclic codes. Icyclic codes, as a special case, include perfect Mannheim error-correcting codes. While Gaussian fields generalize the notion of finite Galois fields and have a complex structure. The Gaussian fields have been used in various bids such as coding theory, cryptography, and wireless communications [20].

BCH codes are a wonderful tool to protect information. The main concepts for decoding are the error location, the error evaluation polynomials, and the so-called key equation they satisfy. There are many methods to solve the key equation. Any method for solving the key equation amounts to a decoding algorithm. The most effective algorithms are the Euclidean algorithm, the Berlekamp-Massey algorithm (1967), and, Sugiyama's algorithm (1975). Here we will use the modified Berlekamp-Massey algorithm for the error correction of BCH codes. The reason for the study of BCH codes over Gaussian fields is their better performance.

The aim of this correspondence is twofold. Initially, we present the notion of the Gaussian field and the extension of the Gaussian field. Then, we provide a complete construction method of BCH codes having symbols from the Gaussian field. Furthermore, design the decoding of BCH codes over the Gaussian field through a slightly amended modified Berlekamp-Massey algorithm. Finally, compare the results of the BCH codes over the Gaussian field with BCH codes over the finite field.

II. GAUSSIAN FIELD

Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ be the Euclidean domain of Gaussian integers. Accordingly $\mathbb{Z}_p[i] = \{a + bi : a, b \in \mathbb{Z}_p\}$ is a commutative ring with identity. The ring $\mathbb{Z}_p[i]$ is the Gaussian field if $p \equiv 3(mod\ 4)$.

A. ILLUSTRATION 1

Let $\mathbb{Z}_3[i] = \{0,1,2, i, 1 + i, 1 + 2i, 2i, 1 + 2i, 2 + 2i\}$ is a Gaussian field. The cardinality of $\mathbb{Z}_3[i]$ is $3^2 = 9$.

B. ILLUSTRATION 2

Let $\mathbb{Z}_7[i] = \{0,1,2,3,4,5,6, i, 1 + i, 2 + i, 3 + i, 4 + i, 5 + i, 6 + i, 2i, 1 + 2i, 2 + 2i, 3 + 2i, 4 + 2i, 5 + 2i, 6 + 2i, 3i, 1 + 3i, 2 + 3i, 3 + 3i, 4 + 3i, 5 + 3i, 6 + 3i, 4i, 1 + 4i, 2 + 4i, 3 + 4i, ,4 + 4i, 5 + 4i, 6 + 4i, 5i, 1 + 5i, 2 + 5i, 3 + 5i, 4 + 5i, 5 + 5i, 6 + 5i, 6i, 1 + 6i, 2 + 6i, 3 + 6i, 4 + 6i, 5 + 6i, 6 + 6i\}$ is a Gaussian field. The cardinality of $\mathbb{Z}_7[i]$ is $7^2 = 49$.

REMARK 1

The cardinality of $\mathbb{Z}_p[i]$ if $p \equiv 3(mod\ 4)$ is p^2.

III. THE EXTENSIONS OF THE GAUSSIAN FIELD

A. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_3[i]^2$

Let $\mathbb{Z}_3[i]$ be a Gaussian field. While $\mathbb{Z}_3[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_3[i]^2$, the quotient ring $\mathbb{Z}_3[i][X]/< f(X) > \equiv GF(3^4)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 2 in $\mathbb{Z}_3[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_3[i]^2 = \{a_0 + a_1\alpha : \forall\ a_0, a_1 \in \mathbb{Z}_3[i]\}$$

The field $\mathbb{Z}_3[i]^2$ is a two-degree extension field of the Gaussian field $\mathbb{Z}_3[i]$. And $\mathbb{Z}_3^*[i]^2 = \mathbb{Z}_3[i]^2 \backslash \{0\}$, be a multiplicative cyclic group of order $3^4 - 1 = 80$.

B. ILLUSTRATION 1

Let $\mathbb{Z}_3[i]$ be a Gaussian field. While $\mathbb{Z}_3[i][X]$ is a Euclidian Domain. The ideal generated by the polynomial $X^2 + X + (2 + i)$ over $\mathbb{Z}_3[i][X]$ is

$$\mathbb{Z}_3[i][X] \not< X^2 + X + (2 + i) >$$
$$= \{a_0 + a_1X : a_0, a_1 \in \mathbb{Z}_3[i]\}$$

The polynomial $f(X) = X^2 + X + (2 + i)$ is a primitive irreducible polynomial over $\mathbb{Z}_3[i]$, and α be the root of $f(X)$ in $\mathbb{Z}_3[i][X]$, then $f(\alpha) = 0$ as $\alpha^2 + \alpha + 2 + i = 0$. Thus, $\alpha^2 = 2\alpha + 1 + 2i$. And $\mathbb{Z}_3^*[i]^2 = \mathbb{Z}_3[i]^2 \backslash \{0\}$ is a multiplicative cyclic group of order $3^{2(2)} - 1 = 80$ given in Table 1.

TABLE 1
ELEMENTS OF THE MULTIPLICATIVE CYCLIC GROUP $\mathbb{Z}_3^*[\text{I}]^2$

α^j	VALUES	α^j	VALUES
1	α	41	2α
2	$2\ \alpha + 1 + 2i$	42	$\alpha + 2 + i$
3	$2\alpha + 2 + i + 2i\alpha$	43	$\alpha + 1 + 2i + i\alpha$
4	$2i\alpha + 1$	44	$i\alpha + 2$
5	$i\alpha + 2i + 2 + \alpha$	45	$2\alpha + 1 + i + 2i\alpha$
6	$i\alpha + \alpha + 2$	46	$2\alpha + 1 + 2i\alpha$
7	$2i\alpha + \alpha + 2$	47	$2\alpha + 1 + i\alpha$
8	$i\alpha + \alpha + i$	48	$2\alpha + 2i\alpha + 2i$
9	$2\alpha + 2$	49	$\alpha + 1$
10	$2 + i$	50	$1 + 2i$
11	$2\alpha + i\alpha$	51	$\alpha + 2i\alpha$
12	$\alpha + 2i + 2i\alpha$	52	$2\alpha + i + i\alpha$
13	$2\alpha + i$	53	$\alpha + 2i$
14	$\alpha + 2 + i + i\alpha$	54	$2\alpha + 1 + 2i + 2i\alpha$
15	$\alpha + 2$	55	$2\alpha + 1$
16	$\alpha + 1 + 2i$	56	$2\alpha + 2 + i$
17	$2i\alpha + 1 + 2i$	57	$i\alpha + i + 2$
18	$\alpha + 2 + 2i$	58	$2\alpha + i + 1$
19	$\alpha + 2i\alpha + 1 + 2i$	59	$2\alpha + 2 + i + i\alpha$
20	i	60	$2i$
21	$i\alpha$	61	$2i\alpha$
22	$2i\alpha + i + 1$	62	$i\alpha + 2i + 2$
23	$\alpha + 2 + 2i + 2i\alpha$	63	$2\alpha + 1 + i + i\alpha$
24	$\alpha + i$	64	$2\alpha + 2i$
25	$2\alpha + i\alpha + 1 + 2i$	65	$\alpha + 2 + i + 2i\alpha$
26	$2\alpha + i\alpha + 2i$	66	$\alpha + i + 2i\alpha$
27	$\alpha + i\alpha + 2i$	67	$2\alpha + i + 2i\alpha$
28	$2\alpha + i\alpha + 2$	68	$\alpha + 1 + 2i\alpha$
29	$2i\alpha + 2i$	69	$i\alpha + i$
30	$2i + 2$	70	$1 + i$
31	$2i\alpha + 2\alpha$	71	$\alpha + i\alpha$
32	$\alpha + 1 + i\alpha$	72	$2\alpha + 2 + 2i\alpha$
33	$2i\alpha + 2$	73	$i\alpha + 1$
34	$2\alpha + 2 + 2i + i\alpha$	74	$\alpha + 1 + i + 2i\alpha$
35	$i\alpha + 2i$	75	$2i\alpha + i$
36	$i\alpha + i + 1$	76	$2i\alpha + 2i + 2$
37	$\alpha + 1 + i$	77	$2\alpha + 2 + 2i$
38	$i\alpha + 1 + 2i$	78	$2i\alpha + 2 + i$

39	$\alpha + i + 1 + i\alpha$	79	$2\alpha + 2 + 2i + 2i\alpha$
40	2	80	1

C. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_3[i]^3$

Let $\mathbb{Z}_3[i]$ be a Gaussian field. While $\mathbb{Z}_3[i][X]$ is a Euclidian Domain. For the extension of the Gaussian field $\mathbb{Z}_3[i]^3$, the quotient ring $\mathbb{Z}_3[i][X]/< f(X) >\equiv GF(3^6)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 3 in $\mathbb{Z}_3[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_3[i]^3 = \{a_0 + a_1\alpha + a_2\alpha^2 : \forall\, a_0, a_1, a_2 \in \mathbb{Z}_3[i]\}$$

The field $\mathbb{Z}_3[i]^3$ is a three-degree extension field of the Gaussian field $\mathbb{Z}_3[i]$. And $\mathbb{Z}_3^*[i]^3 = \mathbb{Z}_3[i]^3\backslash\{0\}$, be a multiplicative cyclic group of order $3^6 - 1 = 728$.

Similarly, the field $\mathbb{Z}_3[i]^m$ is m degree extension field of the Gaussian field $\mathbb{Z}_3[i]$ is given below.

D. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_3[i]^m$

Let $\mathbb{Z}_3[i]$ be a Gaussian field. While $\mathbb{Z}_3[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_3[i]^m$, the quotient ring $\mathbb{Z}_3[i][X]/< f(X) >\equiv GF(3^{2m})$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree m in $\mathbb{Z}_3[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_3[i]^m = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} : \forall\, a_i, \in \mathbb{Z}_3[i], i = 0,1,\dots,m-1\}$$

The field $\mathbb{Z}_3[i]^m$ is m degree extension field of the Gaussian field $\mathbb{Z}_3[i]$. And $\mathbb{Z}_3^*[i]^m = \mathbb{Z}_3[i]^m\backslash\{0\}$, be a multiplicative cyclic group of order $3^{2m} - 1$.

E. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_7[i]^2$

Let $\mathbb{Z}_7[i]$ be a Gaussian field. While $\mathbb{Z}_7[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_7[i]^2$, the quotient ring $\mathbb{Z}_7[i][X]/< f(X) >\equiv GF(7^4)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 2 in $\mathbb{Z}_7[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_7[i]^2 = \{a_0 + a_1\alpha : \forall\, a_0, a_1 \in \mathbb{Z}_7[i]\}$$

The field $\mathbb{Z}_7[i]^2$ is a two-degree extension field of the Gaussian field $\mathbb{Z}_7[i]$. And $\mathbb{Z}_7^*[i]^2 = \mathbb{Z}_7[i]^2\backslash\{0\}$, be a multiplicative cyclic group of order $7^4 - 1 = 2400$.

F. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_7[i]^3$

Let $\mathbb{Z}_7[i]$ be a Gaussian field. While $\mathbb{Z}_7[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_7[i]^3$, the quotient ring $\mathbb{Z}_7[i][X]/< f(X) >\equiv GF(7^6)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 3 in $\mathbb{Z}_7[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_7[i]^3 = \{a_0 + a_1\alpha + a_2\alpha^2 : \forall\, a_0, a_1, a_2 \in \mathbb{Z}_7[i]\}$$

The field $\mathbb{Z}_7[i]^3$ is m degree extension field of the Gaussian field $\mathbb{Z}_7[i]$. And $\mathbb{Z}_7^*[i]^3 = \mathbb{Z}_7[i]^2\backslash\{0\}$, be a multiplicative cyclic group of order $7^6 - 1 = 117648$.

Similarly, the field $\mathbb{Z}_7[i]^m$ is m degree extension field of the Gaussian field $\mathbb{Z}_7[i]$ is given below.

G. THE GAUSSIAN FIELD EXTENSION $\mathbb{Z}_7[i]^m$

Let $\mathbb{Z}_7[i]$ be a Gaussian field. While $\mathbb{Z}_7[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_7[i]^m$, the quotient ring $\mathbb{Z}_7[i][X]/< f(X) >\equiv GF(7^{2m})$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree m in $\mathbb{Z}_7[i][X]$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_7[i]^m = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} : \forall\, a_i \in \mathbb{Z}_7[i], i = 0,1,\dots,m-1\}$$

The field $\mathbb{Z}_7[i]^m$ is the $m-$degree extension field of the Gaussian field $\mathbb{Z}_7[i]$. And $\mathbb{Z}_7^*[i]^m = \mathbb{Z}_7[i]^m\backslash\{0\}$, be a multiplicative cyclic group of order $7^{2m} - 1$.

H. The GAUSSIAN FIELD EXTENSION $\mathbb{Z}_p[i]^2$ $IF\ p \equiv 3(mod\ 4)$

Let $\mathbb{Z}_p[i]$ be a Gaussian field if $p \equiv 3(mod\ 4)$. While $\mathbb{Z}_p[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_p[i]^2$, the quotient ring $\mathbb{Z}_p[i][X]/< f(X) > \equiv GF(q^2)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 2 in $\mathbb{Z}_p[i][X]$ and $q = p^2$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_p[i]^2 = \{a_0 + a_1\alpha : \forall\, a_0, a_1 \in \mathbb{Z}_p[i]\}$$

The field $\mathbb{Z}_p[i]^2$ is a two-degree extension field of the Gaussian field $\mathbb{Z}_p[i]$. And $\mathbb{Z}_p^*[i]^2 = \mathbb{Z}_p[i]^2\backslash\{0\}$, be a multiplicative cyclic group of order $q^2 - 1$.

I. The GAUSSIAN FIELD EXTENSION $\mathbb{Z}_p[i]^3$ $IF\ p \equiv 3(mod\ 4)$

Let $\mathbb{Z}_p[i]$ be a Gaussian field if $p \equiv 3(mod\ 4)$. While $\mathbb{Z}_p[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_p[i]^3$, the quotient ring $\mathbb{Z}_p[i][X]/< f(X) > \equiv GF(q^3)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree 3 in $\mathbb{Z}_p[i][X]$ and $q = p^2$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_p[i]^3 = \{a_0 + a_1\alpha + a_2\alpha^2 : \forall\, a_0, a_1, a_2 \in \mathbb{Z}_p[i]\}$$

The field $\mathbb{Z}_p[i]^3$ is a three-degree extension field of the Gaussian field $\mathbb{Z}_p[i]$. And $\mathbb{Z}_p^*[i]^3 = \mathbb{Z}_p[i]^3\backslash\{0\}$, be a multiplicative cyclic group of order $q^3 - 1$.

Similarly, the field $\mathbb{Z}_p[i]^m$ is m degree extension field of the Gaussian field $\mathbb{Z}_p[i]$ if $p \equiv 3(mod\ 4)$ is given below.

J. The GAUSSIAN FIELD EXTENSION $\mathbb{Z}_p[i]^m$ $IF\ p \equiv 3(mod\ 4)$

Let $\mathbb{Z}_p[i]$ be a Gaussian field if $p \equiv 3(mod\ 4)$. While $\mathbb{Z}_p[i][X]$ is a Euclidian Domain. For the extension of Gaussian field $\mathbb{Z}_p[i]^m$, the quotient ring $\mathbb{Z}_p[i][X]/< f(X) >\equiv GF(q^m)$, where the maximal ideal $< f(X) >$ is generated by $f(X)$ an irreducible polynomial of degree m in $\mathbb{Z}_p[i][X]$ and $q = p^2$. If we write α to denote the coset $X + (f(X))$, then $f(\alpha) = 0$ and

$$\mathbb{Z}_p[i]^m = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1} : \forall\, a_i \in \mathbb{Z}_p[i], i = 0,1,2,\dots,m-1\}$$

The field $\mathbb{Z}_p[i]^m$ is m degree extension field of the Gaussian field $\mathbb{Z}_p[i]$.

REMARK 1

The order of $\mathbb{Z}_p[i]^m\ is\ q^m$.

REMARK 2

$\mathbb{Z}_p^*[i]^m = \mathbb{Z}_p[i]^m \backslash \{0\}$ is a multiplicative cyclic group of order $q^m - 1$.

The following theorem is just a restatement of [15, Theorem 4.4.2].

THEOREM 1

Let $\alpha \in \mathbb{Z}_p[i]^m$ if $p \equiv 3(mod\ 4)$is an extension field of Gaussian field $\mathbb{Z}_p[i]$. Then $\alpha, \alpha^q, \alpha^{q^2}, \ldots,$ have the same minimal polynomial over $\mathbb{Z}_p[i]$.

IV. ENCODING OF BCH CODES OVER GAUSSIAN FIELD

A. CONSTRUCTION OF BCH CODES

Let c, d, q, n be positive integers such that $2 \leq d \leq n - 1$, q is a prime power, and n is relatively prime to q. Let m be the least positive integer such that $q^m \equiv 1(mod\ n)$ [By Euler's theorem, $q^{\varphi(n)} \equiv 1(mod\ n)$, so m divides $\varphi(n)$]. Thus n divides $q^m - 1$. Let α be a primitive nth root of unity in $\mathbb{Z}_p[i]^m$.

Assume $m_j(X) \in \mathbb{Z}_p[i][X]$ denote the minimal polynomial of α^j. And $g(X)$ be the product of distinct polynomials among $m_j(X), j = c, c+1, \ldots, c+d-2$; that is,

$$g(X) = lcm\{m_j(X) | j = c, c+1, \ldots, c+d-2\}.$$

Since $m_j(X)$ divides $X^n - 1$ for each j, it follows that $g\ (X)$ divides $X^n - 1$. Let C be the cyclic code with generator polynomial $g(X)$ in the ring $\mathbb{Z}_p[i][X]_n$. Then C is called a BCH code of length n over $\mathbb{Z}_p[i]$ with designed distance d. If $n = q^m - 1$ in the foregoing definition, then the BCH code C is called primitive. If $c = 1$, then C is called a narrow sense BCH code.

REMARK 1

The number of code words in BCH-code C over the Gaussian field is q^k.

B. BCH CODES OF LENGTH 80 WITH A DESIGNED DISTANCE OF 3 OVER THE GAUSSIAN FIELD $\mathbb{Z}_3[i]$

Let $j = c, c+1, c+2, \ldots, c+d-2 = 1,2$. Apply the above encoding procedure of BCH codes over the Gaussian field $\mathbb{Z}_3[i]$.

Let $m_1(X)$ be the first minimal polynomial for $j = 1$.

$$m_1(X) = (X - \alpha)(X - \alpha^9) = X^2 - (\alpha + \alpha^9)X + \alpha^{10}$$
$$= X^2 + X + (2 + i).$$

Similarly, another minimal polynomial $m_2(X)$ for $j = 2$.

$$m_2(X) = (X - \alpha^2)(X - \alpha^{18}) = X^2 - (\alpha^2 + \alpha^{18})X + \alpha^{20}$$
$$= X^2 + 2iX + i.$$

The LCM of both minimal polynomials is known as generator polynomial $g(X)$ as:

$$g(X) = \left(X^2 + X + (2 + i)\right)(X^2 + 2iX + i)$$
$$g(X) = X^4 + (1 + 2i)X^3 + (2 + i)X^2 + (1 + 2i)X + (2 + 2i)$$

Degree $\left(g(X)\right) = 4,$ Dimension$= k = 80 - 4 = 76.$ Hence, $[80, 76, 3]$ narrow sense BCH code over the Gaussian field $\mathbb{Z}_3[i]$.

C. BCH CODES OF LENGTH 80 WITH A DESIGNED DISTANCE OF 5 OVER THE GAUSSIAN FIELD $\mathbb{Z}_3[i]$

Let $j = c, c+1, c+2, \ldots, c+d-2 = 1,2,3,4.$ Apply the above encoding procedure of BCH codes over the Gaussian field $\mathbb{Z}_3[i]$.

Let $m_1(X)$ be the first minimal polynomial for $j = 1$.

$$m_1(X) = (X - \alpha)(X - \alpha^9) = X^2 - (\alpha + \alpha^9)X + \alpha^{10}$$
$$= X^2 + X + (2 + i).$$

Similarly, the minimal polynomials for $j = 2,3,4$ are given as

$$m_2(X) = (X - \alpha^2)(X - \alpha^{18}) = X^2 - (\alpha^2 + \alpha^{18})X + \alpha^{20}$$
$$= X^2 + 2iX + i.$$
$$m_3(X) = (X - \alpha^3)(X - \alpha^{27}) = X^2 - (\alpha^3 + \alpha^{27})X + \alpha^{30}$$
$$= X^2 + X + (2 + i).$$
$$m_4(X) = (X - \alpha^4)(X - \alpha^{36}) = X^2 - (\alpha^4 + \alpha^{36})X + \alpha^{40}$$
$$= X^2 + (1 + 2i)X + 2.$$

The LCM of all minimal polynomials is known as generator polynomial $g(X)$ as:

$$g(X) = \left(X^2 + X + (2 + i)\right)(X^2 + 2iX + i)(X^2 + X + (2 + i))(X^2 + (1 + 2i)X + 2)$$
$$g(X) = X^8 + iX^7 + (2 + i)X^6 + (1 + 2i)X^5 + (1 + i)X^3 + 2X^2 + 1$$

Degree $\left(g(X)\right) = 8$, Dimension$= k = 80 - 8 = 72.$ Hence, $[80, 72, 5]$ narrow sense BCH code over the Gaussian field $\mathbb{Z}_3[i]$.

D. BCH CODES OF LENGTH 80 WITH A DESIGNED DISTANCE OF 7 OVER THE GAUSSIAN FIELD $\mathbb{Z}_3[i]$

Let $j = c, c+1, c+2, \ldots, c+d-2 = 1,2,3,4,5,6$ then apply the encoding procedure of BCH codes over the Gaussian field $\mathbb{Z}_3[i]$.

Let $m_1(X)$ be the first minimal polynomial for $j = 1$.

$$m_1(X) = (X - \alpha)(X - \alpha^9) = X^2 - (\alpha + \alpha^9)X + \alpha^{10}$$
$$= X^2 + X + (2 + i).$$

Similarly, the minimal polynomials for $j = 2,3,4,5,6$ are given as

$$m_2(X) = (X - \alpha^2)(X - \alpha^{18}) = X^2 - (\alpha^2 + \alpha^{18})X + \alpha^{20}$$
$$= X^2 + 2iX + i.$$
$$m_3(X) = (X - \alpha^3)(X - \alpha^{27}) = X^2 - (\alpha^3 + \alpha^{27})X + \alpha^{30}$$
$$= X^2 + X + (2 + i).$$
$$m_4(X) = (X - \alpha^4)(X - \alpha^{36}) = X^2 - (\alpha^4 + \alpha^{36})X + \alpha^{40}$$
$$= X^2 + (1 + 2i)X + 2.$$
$$m_5(X) = (X - \alpha^5)(X - \alpha^{45}) = X^2 - (\alpha^5 + \alpha^{45})X + \alpha^{50}$$
$$= X^2 + (1 + 2i).$$
$$m_6(X) = (X - \alpha^6)(X - \alpha^{54}) = X^2 - (\alpha^{54} + \alpha^6)X + \alpha^{60}$$
$$= X^2 + iX + 2i$$

The LCM of all minimal polynomials is known as generator polynomial $g(X)$ as:

$$g(X) = \big(X^2 + X + (2+i)\big)(X^2 + 2iX + i)(X^2 + X + (2 + i))(X^2 + (1+2i)X + 2)(X^2 + 1 + 2i)(X^2 + iX + 2i)$$

$$g(X) = X^{12} + 2iX^{11} + (2+2i)X^{10} + iX^8 + 2X^7 + (2+i)X^6 + (1+i)X^5 + iX^4 + (2+i)X^3 + (2+2i)X^2 + 1$$

Degree $\big(g(X)\big) = 12$, Dimension$= k = 80 - 12 = 68$. Hence, $[80, 68, 7]$ narrow sense BCH code over the Gaussian field $\mathbb{Z}_3[i]$.

E. BCH CODES OF LENGTH 80 WITH A DESIGNED DISTANCE OF 9 OVER THE GAUSSIAN FIELD $\mathbb{Z}_3[i]$

Let $j = c, c+1, c+2, \dots, c+d-2 = 1,2,3,4,5,6,7,8$ then apply the encoding procedure of BCH codes over the Gaussian field $\mathbb{Z}_3[i]$.

Let $m_1(X)$ be the first minimal polynomial for $j = 1$.

$$m_1(X) = (X-\alpha)(X-\alpha^9) = X^2 - (\alpha + \alpha^9)X + \alpha^{10} = X^2 + X + (2+i).$$

Similarly, the minimal polynomials for $j = 2,3,4,5,6,7,8$ are given as

$$m_2(X) = (X-\alpha^2)(X-\alpha^{18}) = X^2 - (\alpha^2 + \alpha^{18})X + \alpha^{20} = X^2 + 2iX + i.$$

$$m_3(X) = (X-\alpha^3)(X-\alpha^{27}) = X^2 - (\alpha^3 + \alpha^{27})X + \alpha^{30} = X^2 + X + (2+i).$$

$$m_4(X) = (X-\alpha^4)(X-\alpha^{36}) = X^2 - (\alpha^4 + \alpha^{36})X + \alpha^{40} = X^2 + (1+2i)X + 2.$$

$$m_5(X) = (X-\alpha^5)(X-\alpha^{45}) = X^2 - (\alpha^5 + \alpha^{45})X + \alpha^{50} = X^2 + (1+2i).$$

$$m_6(X) = (X-\alpha^6)(X-\alpha^{54}) = X^2 - (\alpha^{54} + \alpha^{6})X + \alpha^{60} = X^2 + iX + 2i$$

$$m_7(X) = (X-\alpha^7)(X-\alpha^{63}) = X^2 - (\alpha^7 + \alpha^{63})X + \alpha^{70} = X^2 + 2iX + (1+i)$$

$$m_8(X) = (X-\alpha^8)(X-\alpha^{72}) = X^2 - (\alpha^8 + \alpha^{72})X + \alpha^{80} = X^2 + (1+2i)X + 1$$

The LCM of all minimal polynomials is known as generator polynomial $g(X)$ as:

$$g(X) = \big(X^2 + X + (2+i)\big)(X^2 + 2iX + i)(X^2 + X + (2 + i))(X^2 + (1+2i)X + 2)(X^2 + 1 + 2i)(X^2 + iX + 2i)(X^2 + 2iX + (1 + i))(X^2 + (1+2i)X + 1)$$

$$g(X) = X^{16} + X^{15} + (1+i)X^{14} + (2+2i)X^{13} + (2+2i)X^{12} + (2+2i)X^{11} + (1+2i)X^{10} + 2X^9 + 2X^8 + 2iX^7 + (1+i)X^6 + X^4 + 2X^3 + (1+i)X^2 + (2+2i)X + 1 + i$$

Degree $\big(g(X)\big) = 16$, Dimension$= k = 80 - 16 = 64$. Hence, $[80, 64, 9]$ narrow sense BCH code over the Gaussian field $\mathbb{Z}_3[i]$.

V. DECODIN PROCEDURE OF GAUSSIAN FIELD-BASED BCH CODES

The main purpose of this section is to decode the BCH codes over the Gaussian field of length n by the modified Berlekamp-Massey algorithm.

The following theorem is just a restatement of [7, Theorem 4.4.3].

THEOREM 1

Let C be a BCH code of length n over Gaussian field $\mathbb{Z}_p[i]$ if $(p \equiv 3)(mod\ 4)$ with designed distance$d$. Then BCH code $C = \{c(x) \in \mathbb{Z}_p[i][x]_n \mid c(\alpha^i) = 0 \text{ for all } i = c, c+1, \dots, c+d-2\}$. Equivalently, the code C is the null space of the matrix

$$H = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \alpha^{c+d-2} & \alpha^{2(c+d-2)} & \cdots & \alpha^{(c+d-2)(n-1)} \end{pmatrix} \dots (1)$$

Proof: Let $c(x) \in C$. Then, $c(x) = q(x)g(x)$ for some $q(x)$, where $g(x)$ is the generator polynomial of C. Hence $c(\alpha^i) = 0$ for all $i = c, c+1, \dots, c+d-2$. Conversely, let $c(x) \in \mathbb{Z}_p[i][x]_n$such that $c(S^i) = 0$ for all $i = c, c+1, \dots, c+d-2$. Then $m(x)$ divides $c(x)$ for all $i = c, c+1, \dots, c+d-2$. Hence $g(x)$ divides $c(x)$, so $c(x) \in C$.

A. DECODING PROCEDURE

Let $c = (c_0\, c_1\, c_2 \dots c_{n-1})$ be a BCH code of length n, received vector r, and designed distance d. There are the following steps.

1. Find syndromes S with the help of parity check matrix H and the transpose of the received vector r.

$$S = Hr^T (\text{mod } p)$$

If all syndromes are zeros then no error occurs in the received vector r, hence $r = c$. The error will occur if at least one syndrome is non-zero, then go to the next step.

2. Use the Modified Berlekamp-Massey algorithm to find $\delta^n(z)$.

TABLE 2
ELEMENTS OF THE MULTIPLICATIVE CYCLIC GROUP $\mathbb{Z}_3^*[\text{I}]^2$

Iteration	$\Delta^n(\mathbf{z})$	d_n	l_n	$n - l_n$
-1				
0				
1				
.				
.				
.				
2t				

Let d_n be the discrepancy; l_n be the degree of $\delta^n(\text{z})$.

Suppose initial conditions: $\delta^{-1}(\text{z}) = 1; d_{-1} = 1;\ l_{-1} = 0; \delta^0(\text{z}) = 1;\ l_0 = 0$ and $d_0 =$ first non-zero syndrome.

If $d_n = 0$, then $\delta^{n+1}(\text{z}) = \delta^n(\text{z})$ and $l_{n+1} = l_n$.

If $d_n \neq 0$, then for $m \leq n-1$ and $n - l_m$ has the largest value in the last column. So, from $d_n - yd_m = 0$ and got y. Thus, $\delta^{n+1}(z) = \delta^n(z) - yz^{n-m}\,\delta^m(z)$ and $\text{d}_{n+1} = \text{S}_{n+2} + \delta_1^{(n+1)}(\text{z})\,\text{S}_{n+1} + \delta_2^{(n+1)}(\text{z})\,\text{S}_n + \dots + \delta_{l_{n+1}}^{(n+1)}(\text{z})\,\text{S}_{n+2-l_{n+1}}$ and δ^n (z) by the last row of TABLE 2.

3. The reciprocal function of $\delta^n(\text{z}) = g(\text{z})$ and find the roots of $g(\text{z})$ in the form of z_i.

4. Let x_i be the correct location of errors. Select those x_i's

such that $(x_i - z_i)$are zeros, where $1 \leq i \leq n-1$and $x_i = \rho^i$ are error locations.

5. The main purpose of the elementary symmetric function is how many possible errors occur in the received vector. It depends on the value of v. $(z-x_1)(z-x_2)\ldots(z-x_v) = \delta_0\, z^v + \delta_1 z^{v-1} + \cdots + \delta_v$, Where $x_1, \ldots, x_v$ represents the error locations.
6. By using Forney's procedure in [9], calculate the magnitude of errors as follows.

$$y_j = \frac{\sum_{l=0}^{v-1} \delta_{j,i}\, S_{v-l}}{\sum_{l=0}^{v-1}\ \delta_{j,i} x_j^{v-l}}$$

Start with $\delta_0 = \delta_{j,0} = 1$. Where $\delta_{j,i} = \delta_i + x_j . \delta_{j,i-1}$; $i = 1, 2, 3, \ldots, v-1$ and $j = 1, 2, \ldots, v$.
Error vector= $e = (e_0\ e_1\ \ e_2 \ldots e_{n-1})$.

7. The corrected code word of code C is c with the help of the received vector r and error vector e as

$$c = r - e$$

8. For the verification of the code word c of the BCH code by using Theorem 2.

$$Hc^T = [O].$$

B. ILLUSTRATION 1

Suppose the [80, 76, 3] BCH codes of Illustration 4 over the Gaussian field $\mathbb{Z}_3[i]$ and the vector $r = (0, i, 0,0, \ldots, 0)_{1\times 80}$ is the received vector. Find the error vector and correct code word of the BCH code.

$$S = Hr^T = \begin{pmatrix} 1\ \alpha\ \ \alpha^2\ \cdots\ \alpha^{11} \\ 1\ \alpha^2\ \alpha^4\ \cdots\ \alpha^{22} \end{pmatrix} (0\ i\ 0 \ldots 0)^T$$
$$= \begin{pmatrix} i\alpha \\ i\alpha^2 \end{pmatrix} = \begin{pmatrix} \alpha^{21} \\ \alpha^{22} \end{pmatrix}$$

Where syndromes are $S_1 = \alpha^{21}; S_2 = \alpha^{22}$. Find $\delta^n(x)$ by using the modified Berlekamp massay algorithm.

TABLE 3
ELEMENTS OF THE MULTIPLICATIVE CYCLIC GROUP $\mathbb{Z}_3^*[\mathrm{I}]^2$

Iteration	$\Delta^{\boldsymbol{n}}(\mathbf{z})$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	$\alpha^{21} = \mathrm{i}\alpha$	0	0
1	$1 + \alpha^{61}x$	$2\alpha + 2 + 2i\alpha$	1	0
2	$1 + \alpha^{41}\mathrm{x}$			

Thus, it follows that $\delta^2(x) = 1 + \alpha^{41}x$, and its reciprocal function is $g(x) = \alpha^{41} + x$. Hence α is the root of $g(x)$. Now select those of x_i's such that $(x_i - z_i)$ are zeros in $\mathbb{Z}_3^*[\mathrm{i}]^2$, $1 \leq i \leq 80$. Hence $z_1 = \alpha$. So the error appeared at position 2 in the received vector r. $\delta_0 \mathrm{z}^v + \delta_1 = \mathrm{z} - \alpha$ is a symmetric function. The error magnitude is $y_1 = \frac{\delta_{1,0}S_1}{\delta_{1,0}x_1} = \frac{S_1}{x_1} = \frac{\alpha^{21}}{\alpha} = \alpha^{20} = i$, where $\delta_0 = 1, \delta_1 = -\alpha = 2\alpha, v = 1$.

Error vector= $e = (0\ \mathrm{i}\ 0 \ldots\ 0)_{1\times 80}$.

Corrected code word= $c = r - e = (0, 0, 0, \ldots, 0)_{1\times 80}$.

For verification $Hc^T = [O]$.

Hence c is the corrected codeword of BCH code C.

C. ILLUSTRATION 2

Suppose the [80, 76, 3] BCH code of Illustration 4 over the Gaussian field $\mathbb{Z}_3[i]$ and the vector $r = (2+i, 1+2i, 2+i, 0,1, \ldots, 0)_{1\times 80}$ is the received vector. Find the error vector and correct codeword.

Let $S = Hr^T = \begin{pmatrix} 1\ \alpha\ \ \alpha^2\ \cdots\ \alpha^{79} \\ 1\ \alpha^2\ \alpha^4\ \cdots\ \alpha^{78} \end{pmatrix} (2+i\ 1+2i\ 2+i\ 0\ 0 \ldots 0)^T = \begin{pmatrix} 2\alpha \\ 1+i+\alpha \end{pmatrix} = \begin{pmatrix} \alpha^{41} \\ \alpha^{37} \end{pmatrix}$

Where syndromes are $S_1 = \alpha^{41}; S_2 = \alpha^{37}$. Find $\delta^n(x)$ by using the modified Berlekamp massay algorithm.

TABLE 4
ELEMENTS OF THE MULTIPLICATIVE CYCLIC GROUP $\mathbb{Z}_3^*[\mathrm{I}]^2$

Iteration	$\Delta^{\boldsymbol{n}}(\mathbf{z})$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	$\alpha^{41} = 2\alpha$	0	0
1	$1 + \alpha x$	$2\alpha + 2\mathrm{i}$	1	0
2	$1 + \alpha^{36}\mathrm{x}$			

Thus, it follows that $\delta^2(x) = 1 + \alpha^{36}x$, and its reciprocal function is $g(x) = \alpha^{36} + x$. Hence $2 + 2i + 2i\alpha = \alpha^{76}$ is the root of $g(x)$. Now select those of x_i's such that $(x_i - z_i)$ are zeros in $\mathbb{Z}_3^*[\mathrm{i}]^2$, $1 \leq i \leq 80$. Hence $z_1 = \alpha^{76}$. So the error appeared at position 77 in the received vector r. $\delta_0 \mathrm{z}^v + \delta_1 = \mathrm{z} - \alpha^{76}$ is a symmetric function. The error magnitude is $y_1 = \frac{\delta_{1,0}S_1}{\delta_{1,0}x_1} = \frac{S_1}{x_1} = \frac{\alpha^{41}}{\alpha^{76}} = \alpha^{45} = 1 + i + 2\alpha + 2i\alpha$, where $\delta_0 = 1, \delta_1 = -\alpha^{76}, v = 1$.

$$e = (0, 0, 0, \ldots, 0, 2 + 2\alpha + 2i\alpha, 0 \ldots\ \ 0)_{1\times 80}$$

$$c = r - e = (2+i, 1+2i, 2+i, 0,1, \ldots, 0, 2+2i+\alpha + i\alpha, \ldots, 0)_{1\times 80}$$

For verification $Hc^T = [O]$.

Hence c is the corrected codeword of BCH code C.

D. ILLUSTRATION 3

Suppose the [80, 72, 5] BCH code C of Illustration 5 over the Gaussian field $\mathbb{Z}_3[i]$ and the vector $r = (1, 0,0,1+i, 0, 1+2i, 2+i, 0, 1, 0,0, \ldots, 0)_{1\times 80}$ is the received vector. Find the error vector and correct codeword. Also, verify the corrected codeword c.

Let $S = Hr^T = \begin{pmatrix} 1\ \alpha\ \ \alpha^2\ \cdots\ \alpha^{79} \\ 1\ \alpha^2\ \ \alpha^4\ \cdots\ \alpha^{78} \\ 1\ \alpha^3\ \ \alpha^6\ \cdots\ \alpha^{77} \\ 1\ \alpha^4\ \alpha^8\ \cdots\ \alpha^{76} \end{pmatrix} (1, 0,0,1+i, 0, 1+2i, 2+i, 0, 1, 0,0, \ldots, 0)^T$

$$= \begin{pmatrix} 1+\alpha+2i\alpha \\ 2+i+\alpha+i\alpha \\ 1+i+2i\alpha \\ 2\alpha+2i+2i\alpha \end{pmatrix} = \begin{pmatrix} \alpha^{68} \\ \alpha^{14} \\ \alpha^{22} \\ \alpha^{48} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix}$$

Where syndromes are $S_1 = \alpha^{68}, S_2 = \alpha^{14}, S_3 = \alpha^{22}, S_4 = \alpha^{48}$ Find $\delta^n(x)$ by using the modified Berlekamp Massay algorithm.

TABLE 5
ELEMENTS OF THE MULTIPLICATIVE CYCLIC GROUP $\mathbb{Z}_3^*[\mathrm{I}]^2$

Iteration	$\Delta^{\boldsymbol{n}}(\mathbf{z})$	d_n	l_n	$n - l_n$
-1	1	1	0	-1
0	1	α^{68}	0	0
1	$1+\alpha^{28}x$	α^{11}	1	0
2	$1+\alpha^{66}\mathrm{x}$	α^{78}	1	1
3	$1+\alpha^{41}\mathrm{x}+\alpha^{55}\mathrm{x}^2$	α^{39}	2	1
4	$1+\alpha^{74}\mathrm{x}^2$			

Consider, $\delta^4(x) = 1+\alpha^{74}x^2$ and the reciprocal function of $\delta^4(x)$ is $g(x) = \mathrm{x}^2+\alpha^{74}$. Hence α^{17} and α^{57} are the roots of $g(x)$. Now select those of x_i's such that $(x_i - z_i)$ are zeros in $\mathbb{Z}_3^*[\mathrm{i}]^2$, $1 \le i \le 80$. Hence $z_1 = \alpha^{17}$and $z_2 = \alpha^{57}$. So the error appeared at positions 18 and 58 in the received vector r. Therefore the symmetric function $\delta_0 \mathrm{z}^v + \delta_1 \mathrm{z}^{v-1} + \delta_2 = (\mathrm{z}-\alpha^{17})(\mathrm{z}-\alpha^{57}) = z^2+0z+\alpha^{74}$ implies $\delta_0 = 1, \delta_1 = 0, \delta_2 = \alpha^{74}$ and $v = 2$. Hence two errors appeared in the received vector r. As $\delta_{1,1} = \delta_1 + \delta_{1,0}.x_1 = \alpha^{17}$, therefore

$$\mathrm{y}_1 = \frac{\delta_{1,0}.\mathrm{S}_2 + \delta_{1,1}.\mathrm{S}_1}{\delta_{1,0}.\mathrm{x}_1^2 + \delta_{1,1}.\mathrm{x}_1} = \alpha^7$$

$$\delta_{2,1} = \delta_1 + \delta_{2,0}.x_2 = \alpha^{57}$$

$$\mathrm{y}_2 = \frac{\delta_{2,0}.\mathrm{S}_2 + \delta_{2,1}.\mathrm{S}_1}{\delta_{2,0}.\mathrm{x}_2^2 + \delta_{2,1}.\mathrm{x}_2} = \alpha^{66}$$

Hence y_1, and y_2 are error magnitudes. So

$$e = (0,0,0,\dots,0,2+\alpha+2i\alpha,0\dots,0,\mathrm{i}+\alpha + 2i\alpha,0,\dots,0)_{1\times 80}$$

$$c = r - e = r = (1,0,0,1+i,0,1+2i,2 + i,0,1,0,0,\dots,0,1+\alpha+i\alpha,0,\dots,0,2i + 2\alpha+i\alpha,0,\dots,0)_{1\times 80}$$

Hence c is the corrected code word.

VI. COMPARISON OF THE RESULTS OF FINITE FIELD AND GAUSSIAN FIELD

Here we give a comparison between the narrow sense BCH code and their decoding algorithm over a finite field and Gaussian field. Length of code is $n = p^m - 1$, designed distances d, dimension k_1, code rates $R_1 = \frac{k_1}{n} = \frac{k_1}{p^m - 1}$, and the number of p^{k_1} code words of the narrow sense BCH-codes over the finite field $GF(p^m)$ and their decoding algorithm are given in [7, Section 4.4].

But in this article, the authors constructed BCH codes of length $n = q^m - 1 = p^{2m} - 1$, designed distance d, dimension k_2, code rates $R_2 = \frac{k_2}{n} = \frac{k_2}{p^{2m} - 1}$, and the number of $q^{k_2} = p^{2k_2}$ code words over the Gaussian field $\mathbb{Z}_p[i]$ and their decoding algorithm.

Comparison between the narrow sense BCH code over finite field and Gaussian field are given in Table 6 and Table 7. From [7, Excerises 4.4 (10)], length $n = p^m - 1 = 3^4 - 1 = 80$, designed distance d, dimension k_1, code rate R, and the number of p^{k_1} code words of the narrow sense BCH-codes over the finite field $GF(p^m) = GF(3^2)$ are given in Table 6.

TABLE 6
LENGTH, DESIGNED DISTANCE, DIMENSION, CODE RATE, AND CODE WORDS OF THE BCH CODES OVER FINITE FIELD $\mathrm{GF}(3^2)$

n	D	k_1	p^{k_1}	R_1
80	3	72	3^{72}	0.90
80	5	68	3^{68}	0.85
80	7	64	3^{64}	0.80
80	9	56	3^{64}	0.70

Similarly, length $n = q^m - 1 = (3^2)^2 - 1 = 80$, designed distance d, dimension k_2, code rate R_2, and the number of q^{k_2} code words of the narrow sense BCH-codes over the Gaussian field $\mathbb{Z}_p[i] = \mathbb{Z}_3[i]$ are given in Table 7.

TABLE 7
LENGTH, DESIGNED DISTANCE, DIMENSION, CODE RATE, AND CODE WORDS OF THE BCH CODES OVER GAUSSIAN FIELD $\mathbb{Z}_3[\mathrm{I}]$

n	D	k_2	p^{k_2}	R_2
80	3	76	3^{152}	0.95
80	5	72	3^{144}	0.90
80	7	68	3^{136}	0.85
80	9	64	3^{128}	0.80
…	…	…	…	…

The dimension k_1 of BCH codes over codes over a finite field, and the dimension k_2 of BCH codes over a Gaussian field with designed distance d are given in Figure 1.

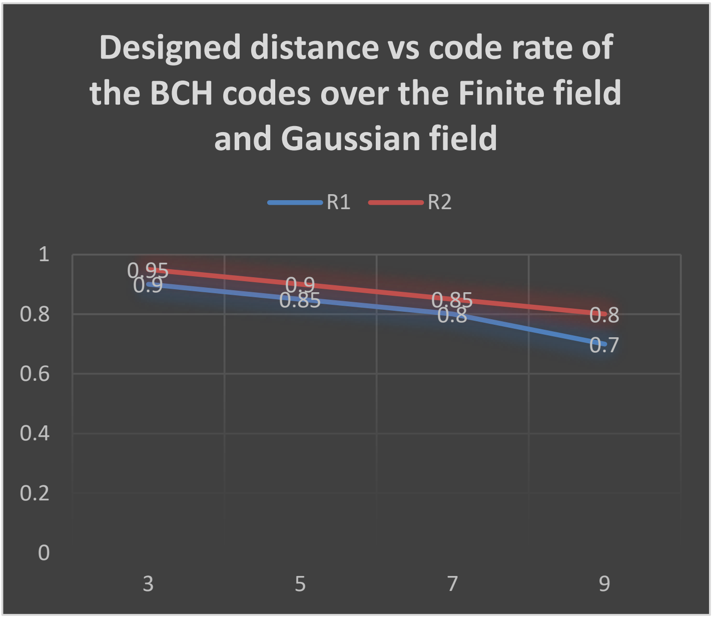

Figure 1: Designed Distance VS Code Rate of codes over finite field $GF(3^2)$ and Gaussian field $\mathbb{Z}_3[i]$

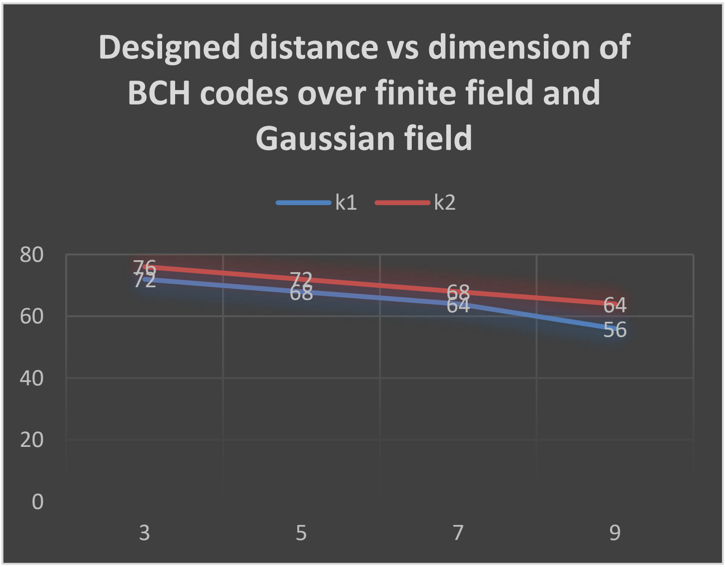

Figure 2: Designed Distance VS Dimension of BCH codes over finite field $GF(3^2)$ and Gaussian field $\mathbb{Z}_3[i]$

The code rate R_1 of BCH codes over codes over finite field, and the code rate R_2 of BCH codes over Gaussian field with designed distance d are given in Figure 2.

The following observations are obtained after comparing the BCH codes over finite field and their decoding algorithm with the BCH codes over Gaussian field and their decoding algorithm for the same length and the same designed distance. The dimension and code rate of the BCH code over the Gaussian field increased as compared to the dimension and code rate of the BCH code over the finite field.

The numbers of code words of the BCH code over the Gaussian field are much higher than the number of code words of the BCH code over the finite field.

The decoding algorithm of the BCH code over the finite field is a particular algorithm for the correction of errors, but the decoding of the BCH code by modified Berlekamp Massey algorithm over the Gaussian field is a generalized algorithm for the correction of errors.

VII. Conclusion

In this article, the Gaussian field and its extension have been presented. Further, the construction method for the BCH codes using the Gaussian field $\mathbb{Z}_p[i]$ has been provided. Also, designed the decoding of BCH codes over the Gaussian field through a slightly amended modified Berlekamp-Massey algorithm. It has been shown that the BCH codes over the Gaussian field $\mathbb{Z}_p[i]$ and their decoding algorithm have better performance than the BCH codes over the finite field $GF(p^m)$ and their decoding algorithm. The construction methods of BCH codes over Gaussian field $\mathbb{Z}_p[i]$ and their decoding algorithm may extend over the Gaussian rings $\mathbb{Z}_{p^k}[i]$, where $p \equiv 3(mod\ 4)$, which might give better performance than BCH codes having symbols from the Gaussian field $\mathbb{Z}_p[i]$.

REFERENCES

[1] Assmus J. E. F., Mattson H. F., “Error-correcting codes: An axiomatic approach”, *Information and Control*, pp. 315–330, 1963.

[2] Augot D., Betti E., Orsini E., “An Introduction to Linear and Cyclic Codes, Gröbner Bases, Coding, and Cryptography”, *Springer*, 2009, pp. 47–68, 2009.

[3] Blake I. F., “Codes over Certain Rings”, *Information and Control,* vol. 20, pp. 396–404, 1972.

[4] Blake I. F., “Codes over Integer Residue Rings”, *Information and Control*, vol. 29, pp. 295–300, 1975.

[5] Spiegel E., “Codes over Zm”, *Information and Control*, vol. 35, pp. 48–51, 1977.

[6] Spiegel E., “Codes over Zm, revisited”, *Information and Control*, vol. 37, pp. 100–104, 1978.

[7] Shah, T., Khan, A. and Andrade, A. A., “Constructions of codes through the semigroup ring B [X; 122Z0] and encoding”, *Computers & Mathematics with Applications*, vol. 62, pp. 1645-1654, 2011.

[8] Yildiz, B. and Siap, I., “Cyclic codes over F2 [u]/(u4− 1) and applications to DNA codes”, *Computers & Mathematics with Applications*, vol. 63, pp. 1169-1176, 2012.

[9] Weil, G., Heus, K., Faraut, T. and Demongeot, J., “The cyclic genetic code as a constraint satisfaction problem”, *Theoretical computer science*, vol. 322, pp. 313-334, 2004.

[10] Dinh, H. Q., Singh, A. K., Pattanayak, S. and Sriboonchitta, S., “Construction of cyclic DNA codes over the ring Z4 [u]/< u2− 1> based on the deletion distance”, *Theoretical Computer Science*, vol. 773, pp. 27-42, 2019.

[11] Kim, B., Lee, Y. and Yoo, J., “An infinite family of Griesmer quasi-cyclic self-orthogonal codes”, *Finite Fields and Their Applications*, vol. 76, pp. 1019-1023, 2021.

[12] Zullo, F., “Multi-orbit cyclic subspace codes and linear sets,” *Finite Fields and Their Applications*, vol. 87, pp. 1021-1053, 2023.

[13] M. Sajjad, T. Shah and R. J. Serna, "Designing Pair of Nonlinear Components of a Block Cipher Over Gaussian Integers", *Computers, Materials & Continua*, vol. 75, pp. 5287-5305, 2023.

[14] M. Sajjad, T. Shah, R. J. Serna, A. Z. E. Suarez, O. S. Delgado, "Fundamental Results of Cyclic Codes over Octonion Integers and Their Decoding Algorithm", *Computation*, vol. 10, pp. 1-12, 2022.

[15] M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi, I. Hussain, "Quaternion integers based higher length cyclic codes and their decoding algorithm", *Computers, Materials & Continua*, vol. 73, pp. 1177-1194, 2022.

[16] Y. Lei, C. Li, Y. Wu and P. Zeng, "More results on hulls of some primitive binary and ternary BCH codes", *Finite Fields and Their Applications*, vol. 82, pp. 1020-1066, 2022.

[17] Liu, Y., Li, R., Fu, Q., Lu, L., and Rao, Y., "Some binary BCH codes with length n= 2^m+ 1", *Finite Fields and Their Applications*, vol. 55, pp. 109-133, 2019.

[18] Nagpaul, S. R., "Topics in applied abstract algebra", *American Mathematical Soc,* vol. 15, pp. 183-207, 2005.

[19] Huber, K., "Codes over Gaussian integers", *IEEE Transactions on Information Theory*, vol. 40, pp. 207-216, 1994.

[20] Stillwell and Stillwell, J., "The Gaussian integers", *Elements of Number Theory*, pp. 101-116, 2003.

Muhammad Sajjad is a Ph.D. Research Scholar at Quaid-i-Azam University in Islamabad, Pakistan since 2020. Currently, he serves as a visiting lecture in the Department of Mathematics at National University of Modern Languages (NUML) Islamabad and Bahria University Islamabad, Pakistan. Since 2018, he has actively researched coding theory, cryptography, vectorial algebra, number theory, non-associative algebra, and elliptic curves. His work focuses on designing efficient error-correcting codes, enhancing data security through cryptographic techniques, exploring applications of vectorial algebra, studying properties of numbers, investigating non-associative algebra, aUniversind analyzing elliptic curves. His research contributions contribute to advancements in these diverse areas of mathematics.

Tariq Shah received his Ph.D. in mathematics from the University of Bucharest, Romania, in 2000. Currently, he serves as a Professor in the Department of Mathematics at Quaid-i-Azam University in Islamabad, Pakistan. Shah's research focuses on various areas, including commutative algebra, non-associative algebra, error-correcting codes, cryptography, number theory, and vectorial algebra. Within commutative algebra, he may explore properties of rings with commutative multiplication. In non-associative algebra, he may investigate algebras with non-associative multiplication structures. Shah's research in error-correcting codes and cryptography involves designing robust codes and encryption techniques. Furthermore, his interest in number theory and vectorial algebra showcases his exploration of number properties and applications of vectors in various mathematical contexts.

Maha Alammari is an Assistant Professor of Applied Mathematics at King Saud University in Riyadh, Saudi Arabia. Since 2011, she has researched matrix polynomials with a numerical computing aspect, the flow of bio-fluids and nano-material liquids with comprehensive graphical representation. Recently, she joined a research group on cryptography focusing on data security based on applications of number theory. Her research contributes to developments in such topics connecting physical, engineering, and computing problems to mathematical analysis.

Dr. Huda Alsaud is an Assistant Professor of Applied Mathematics at King Saud University in Riyadh, Saudi Arabia. She has research in applied mathematics, such as variational problems, Hankel Determinants, nanotechnology, and fractional derivatives with numerical computing aspects. Recently she considered another area of application, coding theory, and cryptography. Her work concentrates on data security as an application of algebra and number theory. Her participation in these areas of research contributes to the study and develop several fields through concepts of mathematics.