AIMS Mathematics, 8(12): 29453–29473.
DOI: 10.3934/math.20231508
Received: 26 July 2023
Revised: 14 September 2023
Accepted: 18 September 2023
Published: 31 October 2023

http://www.aimspress.com/journal/Math

Research article

Eisenstein field BCH codes construction and decoding

Muhammad Sajjad[1,*], Tariq Shah[1], Qin Xin[2] and Bander Almutairi[3]

[1] Department of Mathematics, Quaid-I-Azam University, Islamabad 45320, Pakistan
[2] Faculty of Science and Technology, University of the Faroe Islands, Faroe Islands, Denmark
[3] Department of Mathematics, College of Sciences, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia

*** Correspondence:** Email: m.sajjad@math.qau.edu.pk; Tel: +923067759056.

Abstract: First, we will go through the theory behind the Eisenstein field (EF) and its extension field. In contrast, we provide a detailed framework for building BCH codes over the EF in the second stage. BCH codes over the EF are decoded using the Berlekamp-Massey algorithm (BMA) in this article. We investigate the error-correcting capabilities of these codes and provide expressions for minimal distance. We provide researchers and engineers creating and implementing robust error-correcting codes for digital communication systems with detailed information on building, decoding and performance assessment.

Keywords: Eisenstein integers; Eisenstein field; BCH codes over Eisenstein field; Berlekamp-Massey algorithm
Mathematics Subject Classification: 11T71, 81P73, 94Bxx

1. Introduction

Algebraic coding theory is a subset of coding theory that uses algebraic structures, especially finite fields, and linear algebra to make error-correcting codes and study how they work. The theory is based on linear codes, in which code words are shown as linear combinations of a given set of vectors called “basis vectors”. These codes' minimal distance and error correction capabilities may be studied and enhanced using algebraic methods. The field is important for telephony, data storage and information security, which makes it a key part of current code theory. “Algebraic Codes for Data Transmission” by Richard [1] is a complete introduction to algebraic coding theory. It covers the basics of finite fields, linear codes and decoding methods. It is good for both newbies and more

experiencecoders who want to learn more about algebra. “Modern Coding Theory” by Tom and Urbanke [2] is a book about advanced topics in coding theory, such as algebraic codes and iterative decoding methods. It shows how mathematical methods and current ways of coding are related, which makes it an important resource for experts in the field. Algebraic coding theory is a key part of designing and analyzing error-correcting codes, which makes it possible to make communication systems that work well and are reliable. Using algebraic structures, researchers can come up with strong coding schemes and build the theoretical frameworks needed for error correction in channels that are busy and not very reliable.

Ring-linear coding theory employs finite rings or modules as the basic alphabet. This field has grown tremendously. Assmus and Mattson (1963) [3] were among the first to suggest using ring elements for linear codes in their landmark book. An excellent starting point for learning about linear and cyclic codes-based fields is Augot et al. [4]. The Ring-linear coding theory was advanced by Blake [5, 6]. He started linear codes based on some special rings and moved on to the main integer residue rings. Blake also introduced Hamming, Reed-Solomon and BCH code analogs. Using group algebra, Spiegel [7, 8] linear codes over the integer ring modulo n. With the use of the Chinese Remainder Theorem, Blake was able to use these rings for BCH. In 1958, BCH codes over Galois fields existed. Shah et al. [9] utilized the semigroup ring to encode. In [10–12], the authors introduced DNA cyclic codes over $F_2[u]/(u^4 - 1)$. Kim et al. In [13], the authors defined quasi-cyclic self-orthogonal codes that can go on forever. Recently, Zullo [14] developed another type of cyclic code. The fundamental binary and ternary BCH code hulls were investigated by Lei et al. [15]. In [16], Liu et al. constructed $2^m + 1$ binary BCH codes.

Eisenstein integers, named after the German mathematician Ferdinand Eisenstein [17], are a special subset of complex numbers that have a significant impact on algebraic number theory. They are expressed as $a + b\omega$, where a and b are integers, and ω is a complex number known as the cube root of unity. The cube root of unity, ω, satisfies the equation $\omega^3 = 1$. Eisenstein integers exhibit intriguing properties, including a hexagonal lattice structure when represented on the complex plane. They are closely related to triangular numbers and have applications in various mathematical areas, such as elliptic curves and modular forms. The unique factorization of Eisenstein integers is also of great interest in algebraic number theory, making them a crucial element in studying and understanding number theory concepts.

Error-correcting codes are an essential component of today's sophisticated communication systems because they enable the detection and correction of errors that may occur while data is being sent. BCH codes, which are circular codes, have been studied extensively and are used in real life. BCH codes are made to handle random errors, which makes them good for busy lines of communication. Research on BCH codes has usually been about making and studying codes over limited Galois fields [18]. The authors have created codes using Vectorial Algebra and have also utilized these codes in cryptography [19–23]. Huber [24] presented a two-dimensional modular distance and associated codes. These codes, known as consta-cyclic codes, feature simple constructions and can be classified as a subset of I-cyclic (Ideal cyclic) codes. Notably, I-cyclic codes include error-correcting Mannheim codes. In addition, Eisenstein fields offer a generalized concept of finite Galois fields with a more intricate structure. Eisenstein's fields have numerous applications, including cryptography, error-correcting codes, communications, etc.

BCH codes are extremely valuable for securing data and providing efficient error correction capabilities. Important ideas for decoding BCH codes center on the polynomials used to find errors and evaluate their severity, as well as the critical key equation that these polynomials meet. There are numerous methods for solving the key equation, each of which provides a decoding algorithm. The

Euclidean algorithm [25], BMA [26] and Sugiyama's algorithm (SA) [27] are three of the most effective algorithms. Authors in [28–31] defined some algebraic structures and its applications in algebraic coding theory and algebraic cryptography. Sajjad et al. [32], constructed Gaussian field-based BCH codes decoding. In this situation, we will use a tweaked version of the Berlekamp-Massey method to fix errors in BCH codes. Due to their superior performance, the EF-based BCH is an area of study.

We have dual objectives. To answer the question, what is Eisenstein's field? To construct BCH codes that operate over the Eisenstein field. BMA-modified BCH codes decoding over the Eisenstein field. Then, we compare the BCH codes' Eisenstein and Galois field findings.

2. Eisenstein field and the extensions of Eisenstein field

2.1. Eisenstein field

Let ω be the cube root of unity$(\omega^3 = 1)$ and $1 + \omega + \omega^2 = 0$. Let $\mathbb{Z}[\omega] = \{u + v\omega : u, v \in \mathbb{Z}\}$ be the Euclidean domain (ED) of the Eisenstein integers (EI) [17, Section 1]. Accordingly, $\mathbb{Z}_p[\omega] = \{u + v\omega : u, v \in \mathbb{Z}_p\}$ is a commutative ring with identity. $\mathbb{Z}_p[\omega]$ is the Eisenstein field (EF) if $p \equiv 2(mod\ 3)$ [17, Corollary 14].

Illustration 1. Let $\mathbb{Z}_2[\omega] = \{0,1, \omega, 1 + \omega\}$ be the Eisenstein field because every nonzero element of $\mathbb{Z}_2[\omega]$ is a unit element and the cardinality of $\mathbb{Z}_2[\omega]$ is $2^2 = 4$. Elements of $\mathbb{Z}_2[\omega]$ are given in Figure 1.

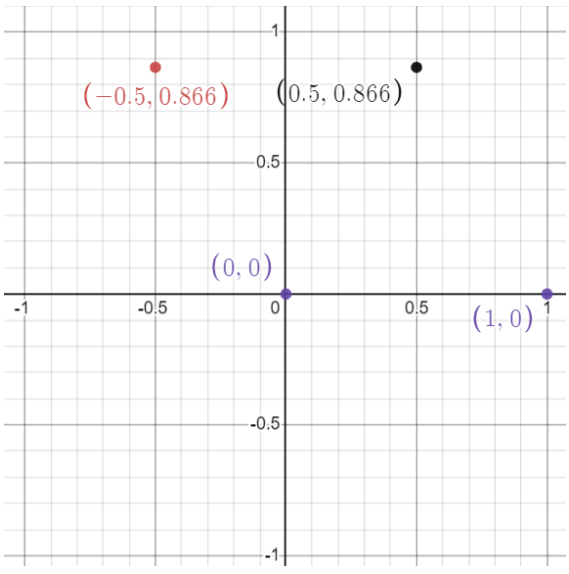

Figure 1. Eisenstein field $\mathbb{Z}_2[\omega]$.

Illustration 2. Let

$$\mathbb{Z}_5[\omega] = \{0, 1, 2, 3, 4, 4\omega, 4 + \omega, \omega, 2\omega, 3\omega, 1 + 2\omega, 1 + 3\omega, 1 + \omega, 1 + 4\omega, 2 + \omega, 2 + 2\omega, 2 + 4\omega, 2 + 3\omega, 3 + \omega, 3 + 2\omega, 3 + 3\omega, 3 + 4\omega, 4 + 2\omega, 4 + 3\omega, 4 + 4\omega\}$$

be an Eisenstein field, because every nonzero element of $\mathbb{Z}_5[\omega]$ is unit element and the cardinality of $\mathbb{Z}_5[\omega]$ is $5^2 = 25$. Elements of $\mathbb{Z}_5[\omega]$ are shown in Figure 2.

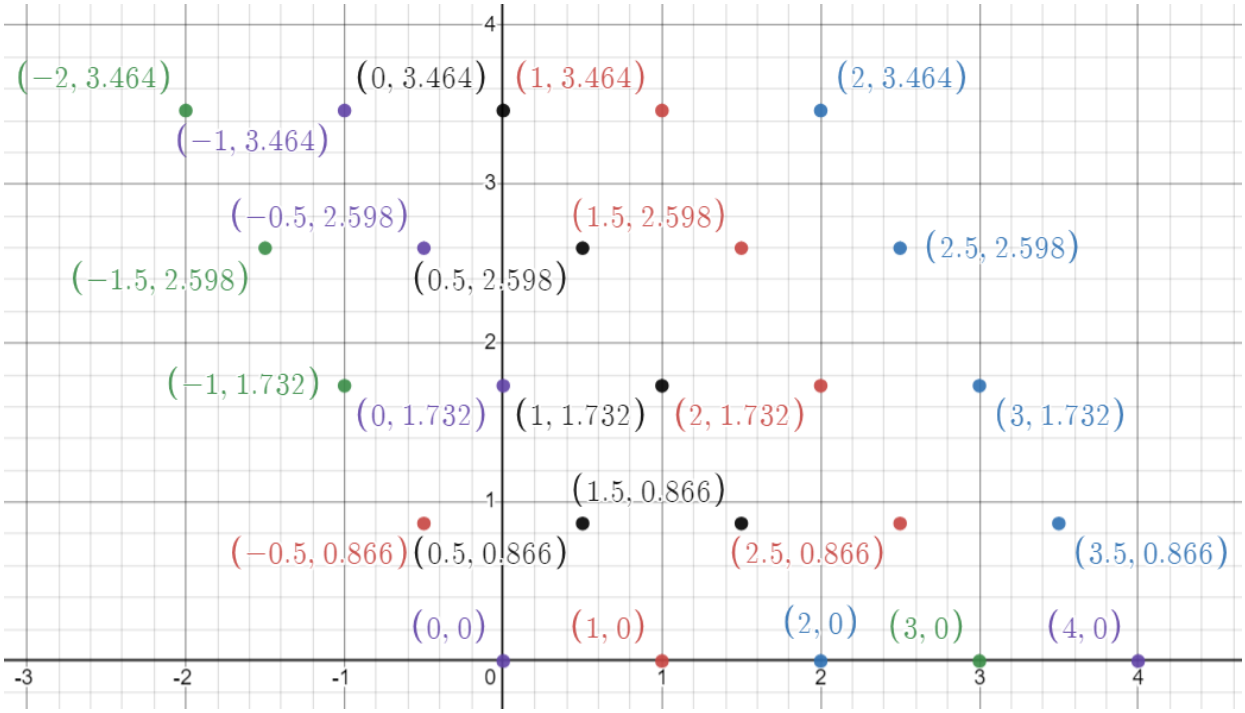

Figure 2. Eisenstein field $\mathbb{Z}_5[\omega]$.

Remark 1. $\mathbb{Z}_p[\omega]$ has p^2 elements if $p \equiv 2(mod\ 3)$.

Remark 2. Let $\mathbb{Z}_p[\omega]^*$ denote the units in $\mathbb{Z}_p[\omega]$ if $p \equiv 2(mod\ 3)$ with cardinality $p^2 - 1$.

2.2. Eisenstein field extension

Let $\mathbb{Z}_2[\omega]$ be the Eisenstein field. While $\mathbb{Z}_2[\omega][x]$ is an ED.

2.2.1. The Eisenstein field extension $\mathbb{Z}_2[\omega]^2$

For the extension of EF $\mathbb{Z}_2[\omega]^2$, the quotient ring (QR)

$$\mathbb{Z}_2[\omega][x]/< H(x) > \cong GF(2^4),$$

where $< H(x) >$ is the maximal ideal generated by an irreducible polynomial (IP) $H(x)$ of degree 2 in $\mathbb{Z}_2[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_2[\omega]^2 = \{u_0 + u_1\gamma : \forall u_0, u_1 \in \mathbb{Z}_2[\omega]\}.$$

Hence $\mathbb{Z}_2[\omega]^2$ is a 2-degree extension field of the EF $\mathbb{Z}_2[\omega]$, and $\mathbb{Z}_2[\omega]^{*2} = \mathbb{Z}_2[\omega]^2 \backslash \{0\}$ is a cyclic group (CG) of order $2^4 - 1 = 15$.

Illustration 3. Let the ideal

$$\mathbb{Z}_2[\omega][x]/< x^2 + x + \omega >= \{u_0 + u_1 x : \forall u_0, u_1 \in \mathbb{Z}_2[\omega]\}$$

generated by the primitive IP $H(x) = x^2 + x + \omega$ over $\mathbb{Z}_2[\omega]$ and γ be the root of $H(x)$ in extension field $\mathbb{Z}_2[\omega][x]$, then $H(\gamma) = 0$ as $\gamma^2 + \gamma + \omega = 0$. Thus, $\gamma^2 = \gamma + \omega$ and $\mathbb{Z}_2[\omega]^{*^2} = \mathbb{Z}_2[\omega]^2 \backslash \{0\}$ is a CG of order $2^{2(2)} - 1 = 15$ in Table 1.

Table 1. Cyclic group $\mathbb{Z}_2[\omega]^{*^2}$.

i	γ^i
1	γ
2	$\gamma + \omega$
3	$\gamma + \omega + \gamma\omega$
4	$\gamma + 1$
5	ω
6	$\gamma\omega$
7	$\gamma\omega + 1 + \omega$
8	$1 + \gamma + \omega$
9	$\omega + \gamma\omega$
10	$1 + \omega$
11	$\gamma + \gamma\omega$
12	$1 + \gamma + \gamma\omega$
13	$1 + \gamma\omega$
14	$1 + \gamma + \omega + \gamma\omega$
15	1

2.2.2. The Eisenstein field extension $\mathbb{Z}_2[\omega]^3$

For the extension of EF $\mathbb{Z}_2[\omega]^3$, the QR

$$\mathbb{Z}_2[\omega][x]/< H(x) > \cong GF(2^6),$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree 3 in $\mathbb{Z}_2[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_2[\omega]^3 = \{u_0 + u_1\gamma + u_2\gamma^2 : \forall u_0, u_1, u_2 \in \mathbb{Z}_2[\omega]\}.$$

Hence $\mathbb{Z}_2[\omega]^3$ is a 3-degree extension field of the EF $\mathbb{Z}_2[\omega]$, and $\mathbb{Z}_2[\omega]^{*^3} = \mathbb{Z}_2[\omega]^3 \backslash \{0\}$ is a CG of order $2^6 - 1 = 63$.

Illustration 4. Let the ideal

$$\mathbb{Z}_2[\omega][x]/< x^3 + x^2 + x + \omega >= \{u_0 + u_1 x + u_2 x^2 : \forall u_0, u_1, u_2 \in \mathbb{Z}_2[\omega]\}$$

generated by the primitive IP $H(x) = x^3 + x^2 + x + \omega$ over $\mathbb{Z}_2[\omega]$ and γ be the root of $H(x)$ in extension field $\mathbb{Z}_2[\omega][x]$, then $H(\gamma) = 0$ as $\gamma^3 + \gamma^2 + \gamma + \omega = 0$. Thus, $\gamma^3 = \gamma^2 + \gamma + \omega$ and $\mathbb{Z}_2[\omega]^{*^3} = \mathbb{Z}_2[\omega]^3 \backslash \{0\}$ is a CG of order $2^6 - 1 = 63$ in Table 2.

Table 2. Cyclic group $\mathbb{Z}_2[\omega]^{*3}$.

s	γ^s	s	γ^s
1	γ	33	$\omega\gamma^2+1+\gamma+\gamma^2$
2	γ^2	34	$\omega\gamma^2+\omega\gamma+1$
3	$\gamma^2+\omega+\gamma$	35	$\omega\gamma+1+\omega+\gamma$
4	$\omega+\gamma+\omega\gamma$	36	$\omega\gamma^2+\omega\gamma+\gamma+\gamma^2$
5	$\gamma^2+\omega\gamma+\gamma^2\omega$	37	$\omega\gamma+1+\gamma$
6	$\gamma^2+\omega\gamma+\gamma+1$	38	$\omega\gamma^2+\gamma+\gamma^2$
7	$\omega+\omega\gamma^2$	39	$\omega\gamma^2+\omega\gamma+1+\gamma$
8	$\omega\gamma^2+\omega+1$	40	$\omega\gamma+1+\omega+\gamma+\gamma^2$
9	$\omega\gamma^2+\omega+\gamma+1$	41	$\omega\gamma^2+\omega\gamma+\omega$
10	$\omega+\gamma+1+\omega\gamma^2+\gamma^2$	42	$\omega+1$
11	$1+\gamma^2\omega$	43	$\omega\gamma+\gamma$
12	$\gamma+1+\omega\gamma^2+\omega+\omega\gamma$	44	$\omega\gamma^2+\gamma^2$
13	$\gamma^2+\omega+1+\gamma$	45	$\omega\gamma+1+\omega\gamma^2+\gamma+\gamma^2$
14	$\omega\gamma+\omega$	46	$\omega\gamma+1$
15	$\omega\gamma+\omega\gamma^2$	47	$\omega\gamma^2+\gamma$
16	$\omega\gamma+1+\omega$	48	$\gamma^2+\omega\gamma^2+\omega\gamma+1+\omega$
17	$\omega\gamma^2+\omega\gamma+\gamma$	49	γ^2+1
18	$\omega\gamma+1+\omega+\gamma^2$	50	$\gamma^2+\omega$
19	$\omega\gamma^2+\omega\gamma+\gamma^2+\omega$	51	$\omega\gamma+\omega+\gamma+\gamma^2$
20	$\gamma^2+\gamma+1$	52	$\omega+\gamma+\omega\gamma+\omega\gamma^2$
21	ω	53	$\gamma^2+1+\omega$
22	$\omega\gamma$	54	$\omega\gamma+\omega+\gamma^2$
23	$\omega\gamma^2$	55	$\gamma^2+\omega+\gamma+\omega\gamma+\omega\gamma^2$
24	$\omega\gamma^2+\omega\gamma+1+\omega$	56	$1+\gamma$
25	$\omega+\gamma+1$	57	$\gamma^2+\gamma$
26	$\omega\gamma+\gamma^2+\gamma$	58	$\omega+\gamma$
27	$\omega\gamma^2+\omega+\gamma$	59	$\omega\gamma+\gamma^2$
28	$\omega\gamma^2+1+\omega+\gamma^2$	60	$\gamma^2+\gamma+\omega+\omega\gamma^2$
29	$\omega\gamma^2+1+\gamma^2$	61	$\gamma+\omega\gamma^2+1$
30	$\omega\gamma+\omega\gamma^2+1+\gamma^2$	62	$\gamma^2+\omega\gamma^2+\omega\gamma+1+\omega+\gamma$
31	$\omega\gamma+1+\gamma^2$	63	1
32	$\omega\gamma^2+\omega+\gamma^2$		

2.2.3. The Eisenstein field extension $\mathbb{Z}_2[\omega]^{\mathrm{m}}$

For the extension of EF $\mathbb{Z}_2[\omega]^m$, the QR

$$\mathbb{Z}_2[\omega][x]/<H(x)>\cong GF(2^{2m}),$$

where $<H(x)>$ is the maximal ideal generated by an IP $H(x)$ of degree m in $\mathbb{Z}_2[\omega][x]$. Let γ is the coset $x+(H(x))$, then $H(\gamma)=0$ and

$$\mathbb{Z}_2[\omega]^m=\{u_0+u_1\gamma+u_2\gamma^2+\cdots+u_{m-1}\gamma^{m-1}:\forall u_0,u_1,u_2,\ldots,u_{m-1}\in\mathbb{Z}_2[\omega]\}.$$

$\mathbb{Z}_2[\omega]^m$ is a m degree extension field of the EF $\mathbb{Z}_2[\omega]$, and $\mathbb{Z}_2[\omega]^{*m}=\mathbb{Z}_2[\omega]^m\backslash\{0\}$ is a cyclic group of order $2^{2m}-1$.

Furthermore, let $\mathbb{Z}_5[\omega]$ be an Eisenstein field. In fact, $\mathbb{Z}_5[\omega][x]$ is an ED and the EF extension is given below.

2.2.4. The Eisenstein field extension $\mathbb{Z}_5[\omega]^2$

For the extension of EF $\mathbb{Z}_5[\omega]^2$, the QR

$$\mathbb{Z}_5[\omega][x]/< H(x) >\cong GF(5^4),$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree 2 in $\mathbb{Z}_5[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and $\mathbb{Z}_5[\omega]^2 = \{u_0 + u_1\gamma : \forall u_0, u_1 \in \mathbb{Z}_5[\omega]\}$. Hence $\mathbb{Z}_5[\omega]^2$ is a 2-degree extension field of the EF $\mathbb{Z}_5[\omega]$, and $\mathbb{Z}_5[\omega]^{*^2} = \mathbb{Z}_5[\omega]^2\backslash\{0\}$ is a CG of order $5^4 - 1 = 624$.

2.2.5. The Eisenstein field extension $\mathbb{Z}_5[\omega]^3$

For the extension of EF $\mathbb{Z}_5[\omega]^3$, the QR

$$\mathbb{Z}_5[\omega][x]/< H(x) >\cong GF(5^6)$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree 3 in $\mathbb{Z}_5[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_5[\omega]^3 = \{u_0 + u_1\gamma + u_2\gamma^2 : \forall u_0, u_1, u_2 \in \mathbb{Z}_5[\omega]\}.$$

Hence, $\mathbb{Z}_5[\omega]^3$ is a 3-degree extension field of the EF $\mathbb{Z}_5[\omega]$, and $\mathbb{Z}_5[\omega]^{*^3} = \mathbb{Z}_5[\omega]^3\backslash\{0\}$ is a CG of order $5^6 - 1 = 15625$.

2.2.6. The Eisenstein field extension $\mathbb{Z}_5[\omega]^{\mathrm{m}}$

For the extension of EF $\mathbb{Z}_5[\omega]^m$, the QR

$$\mathbb{Z}_5[\omega][x]/< H(x) >\cong GF(5^{2m})$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree m in $\mathbb{Z}_5[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_5[\omega]^m = \{u_0 + u_1\gamma + u_2\gamma^2 + \cdots + u_{m-1}\gamma^{m-1} : \forall u_0, u_1, u_2, \ldots, u_{m-1} \in \mathbb{Z}_5[\omega]\}.$$

Hence, $\mathbb{Z}_5[\omega]^m$ is a m-degree extension field of the EF $\mathbb{Z}_5[\omega]$, and $\mathbb{Z}_5[\omega]^{*^m} = \mathbb{Z}_5[\omega]^m\backslash\{0\}$ is a CG of order $5^{2m} - 1$.

In a similar way, Eisenstein field extension $\mathbb{Z}_p[\omega]$, if $p \equiv 2(mod\ 3)$ is given below.

2.2.7. The Eisenstein field extension $\mathbb{Z}_{\mathrm{p}}[\omega]^2$ if $\mathrm{p} \equiv 2(\mathrm{mod}\ 3)$

For the extension of EF $\mathbb{Z}_p[\omega]^2$, the QR

$$\mathbb{Z}_p[\omega][x]/< H(x) >\cong GF(p^4)$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree 2 in $\mathbb{Z}_p[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_p[\omega]^2 = \{u_0 + u_1\gamma : \forall u_0, u_1 \in \mathbb{Z}_p[\omega]\}.$$

Hence, $\mathbb{Z}_p[\omega]^2$ is a 2-degree extension field of the EF $\mathbb{Z}_p[\omega]$, and $\mathbb{Z}_p[\omega]^{*^2} = \mathbb{Z}_p[\omega]^2 \backslash \{0\}$ is a CG of order $p^4 - 1$.

2.2.8. The Eisenstein field extension $\mathbb{Z}_p[\omega]^3$ if $p \equiv 2 (\mathrm{mod}\ 3)$

For the extension of EF $\mathbb{Z}_p[\omega]^3$, the QR

$$\mathbb{Z}_p[\omega][x]/< H(x) > \cong GF(p^6),$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree 3 in $\mathbb{Z}_p[\omega][x]$. Let γ is the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_p[\omega]^3 = \{u_0 + u_1\gamma + u_2\gamma^2 : \forall u_0, u_1, u_2 \in \mathbb{Z}_p[\omega]\}.$$

Hence, $\mathbb{Z}_p[\omega]^3$ is a 3-degree extension field of the EF $\mathbb{Z}_p[\omega]$, and $\mathbb{Z}_p[\omega]^{*^3} = \mathbb{Z}_p[\omega]^3 \backslash \{0\}$ is a CG of order $p^6 - 1$.

2.2.9. The Eisenstein field extension $\mathbb{Z}_p[\omega]^m$ if $p \equiv 2 (\mathrm{mod}\ 3)$

For the extension of EF $\mathbb{Z}_p[\omega]^m$, the QR

$$\mathbb{Z}_p[\omega][x]/< H(x) > \cong GF(p^{2m})$$

where $< H(x) >$ is the maximal ideal generated by an IP $H(x)$ of degree m in $\mathbb{Z}_p[\omega][x]$. Let γ be the coset $x + (H(x))$, then $H(\gamma) = 0$ and

$$\mathbb{Z}_p[\omega]^m = \{u_0 + u_1\gamma + u_2\gamma^2 + \cdots + u_{m-1}\gamma^{m-1} : \forall u_0, u_1, u_2, \ldots, u_{m-1} \in \mathbb{Z}_p[\omega]\}.$$

$\mathbb{Z}_p[\omega]^m$ is an m-degree extension field of the EF $\mathbb{Z}_p[\omega]$, and $\mathbb{Z}_p[\omega]^{*^m} = \mathbb{Z}_p[\omega]^m \backslash \{0\}$ is a CG of order $p^{2m} - 1$.

Remark 3. The cardinality of $\mathbb{Z}_p[\omega]^m$ *is* p^{2m}.

Theorem 1. Let γ be the element of the extension field $\mathbb{Z}_p[\omega]^m$ if $p \equiv 2 (mod\ 3)$, then $\gamma, \gamma^{p^2}, \gamma^{p^4}$, ..., have the same minimal polynomial over the EF $\mathbb{Z}_p[\omega]$.

Proof. Straightforward [18, Theorem 4.4.2].

In this section, we will construct BCH codes over the EF by following [16, Section 4.4].

3. Encoding of BCH codes over Eisenstein field

Let $c, n, q, d > 0$, such that q is a some prime power, $2 \leq d \leq n-1$, and $gcd(n, q) = 1$. Let a least positive integer m such that $p^{2m} \equiv 1(mod\ n)$ [By Euler's theorem, $p^{2\varphi(n)} \equiv 1(mod\ n)$, then m divides $\varphi(n)$]. Thus n divides $p^{2m} - 1$.

Let γ be the element of the extension field $\mathbb{Z}_p[\omega]^m$. Consider the minimal polynomials $m_i(X) \in \mathbb{Z}_p[\omega][X]$ of γ^i. The least common multiple (lcm) of all distinict minimal polynomials $m_i(X), i = c, c+1, \ldots, c+d-2$ is known as the generator polynomial $g(X)$ that is,

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

Since all minimal polynomials divides $X^n - 1$, So generator polynomial divides $X^n - 1$. Let C be the cyclic code generated by $g(X)$ in the ring $\mathbb{Z}_p[\omega][X]_n$. Then C is called a BCH code of length n over EF $\mathbb{Z}_p[\omega]$ with designed distance d.

Remark 4. If the code is full length $n = p^{2m} - 1$ then it is primitive.

Remark 5. If the code is narrow sense, then $c = 1$.

Remark 6. The cardinality of the code C over EF is p^{2k}.

Illustration 5. Construct a $(15, k, 3)$ BCH code over the EF $\mathbb{Z}_2[\omega]$.

Let $\gamma \in \mathbb{Z}_2[\omega]^2$ then by Theorem 1, γ, γ^{2^2} have the same minimal polynomial

$$m_1(X) = X^2 + X + \omega = f(X).$$

Let $\gamma^2 \in \mathbb{Z}_2[\omega]^2$ then $m_2(X)$ can be found by γ^2, γ^8,

$$m_2(X) = (X - \gamma^2)(X - \gamma^8) = X^2 - (\gamma^2 + \gamma^8)X + \gamma^{10} = X^2 + X + (1 + \omega).$$

The generator polynomial $g(X)$ is,

$$g(X) = m_1(X).m_2(X) = (X^2 + X + \omega)(X^2 + X + (1 + \omega)) = X^4 + X + 1.$$

The degree of $g(X)$ is 4, and the dimension k is 11. Hence, we get $(15, 11, 3)$ BCH code over EF $\mathbb{Z}_2[\omega]$.

Illustration 6. Construct a $(15, k, 5)$ BCH code over the EF $\mathbb{Z}_2[\omega]$.

Let $\gamma \in \mathbb{Z}_2[\omega]^2$ then by Theorem 1, γ, γ^{2^2} have the same minimal polynomial

$$m_1(X) = X^2 + X + \omega = f(X).$$

Let $\gamma^2 \in \mathbb{Z}_2[\omega]^2$ then $m_2(X)$ can be found by γ^2 and γ^8,

$$m_2(X) = (X - \gamma^2)(X - \gamma^8) = X^2 - (\gamma^2 + \gamma^8)X + \gamma^{10} = X^2 + X + (1 + \omega).$$

Let $\gamma^3 \in \mathbb{Z}_2[\omega]^2$ then $m_3(X)$ can be found by γ^3 and γ^{12},

$$m_3(X) = (X - \gamma^3)(X - \gamma^{12}) = X^2 - (\gamma^3 + \gamma^{12})X + \alpha^{15} = X^2 + (1 + \omega)X + 1.$$

Let $\gamma^4 \in \mathbb{Z}_2[\omega]^2$ then $m_4(X)$ can be found by γ^4 and γ^1,

$$m_4(X) = (X - \gamma^4)(X - \gamma) = X^2 + X + \omega = m_1(X).$$

The generator polynomial $g(X)$ is,

$$g(X) = m_1(X).m_2(X).m_3(X)$$

$$= (X^2 + X + \omega)\big(X^2 + X + (1 + \omega)\big)(X^2 + (1 + \omega)X + 1)$$

$$= X^6 + (1 + \omega)X^5 + X^4 + X^3 + \omega X^2 + \omega X + 1.$$

The degree of $g(X)$ is 6, and the dimension k is 9. Hence, we get $(15, 9, 5)$ BCH codes over EF $\mathbb{Z}_2[\omega]$.

Illustration 7. Construct a $(15, k, 7)$ BCH code over the EF $\mathbb{Z}_2[\omega]$.

Let $\gamma \in \mathbb{Z}_2[\omega]^2$ then by Theorem 1, γ, γ^{2^2} have the same minimal polynomial

$$m_1(X) = X^2 + X + \omega = f(X).$$

Let $\gamma^2 \in \mathbb{Z}_2[\omega]^2$ then $m_2(X)$ can be found by γ^2 and γ^8,

$$m_2(X) = (X - \gamma^2)(X - \gamma^8) = X^2 - (\gamma^2 + \gamma^8)X + \gamma^{10} = X^2 + X + (1 + \omega).$$

Let $\gamma^3 \in \mathbb{Z}_2[\omega]^2$ then $m_3(X)$ can be found by γ^3 and γ^{12},

$$m_3(X) = (X - \gamma^3)(X - \gamma^{12}) = X^2 - (\gamma^3 + \gamma^{12})X + \alpha^{15} = X^2 + (1 + \omega)X + 1.$$

Let $\gamma^4 \in \mathbb{Z}_2[\omega]^2$ then $m_4(X)$ can be found by γ^4 and γ^1,

$$m_4(X) = (X - \gamma^4)(X - \gamma) = X^2 + X + \omega = m_1(X).$$

Let $\gamma^5 \in \mathbb{Z}_2[\omega]^2$ then $m_5(X)$ can be found by γ^5,

$$m_5(X) = X - \gamma^5 = X + \omega.$$

Let $\gamma^6 \in \mathbb{Z}_2[\omega]^2$ then $m_6(X)$ can be found by γ^6 and γ^9,

$$m_6(X) = (X - \gamma^6)(X - \gamma^9) = X^2 - (\gamma^6 + \gamma^9)X + \alpha^{15} = X^2 + \omega X + 1.$$

The generator polynomial $g(X)$ is,

$$g(X) = m_1(X).m_2(X).m_3(X).m_5(X).m_6(X)$$

$$= (X^2 + X + \omega)\big(X^2 + X + (1 + \omega)\big)(X^2 + (1 + \omega)X + 1)(X + \omega)(X^2 + \omega X + 1)$$

$$= X^9 + (1 + \ \omega)X^8 + \omega^2 X^7 + \omega X^6 + X^5 + \omega X^4 + X + \omega.$$

The degree of $g(X)$ is 9, and the dimension k is 6. Hence, we get $(15, 6, 7)$ BCH codes over EF $\mathbb{Z}_2[\omega]$.

Illustration 8. Construct a $(15, k, 9)$ BCH code over the EF $\mathbb{Z}_2[\omega]$.

Let $\gamma \in \mathbb{Z}_2[\omega]^2$ then by Theorem 1, γ, γ^{2^2} have the same minimal polynomial

$$m_1(X) = X^2 + X + \omega = f(X).$$

Let $\gamma^2 \in \mathbb{Z}_2[\omega]^2$ then $m_2(X)$ can be found by γ^2 and γ^8,

$$m_2(X) = (X - \gamma^2)(X - \gamma^8) = X^2 - (\gamma^2 + \gamma^8)X + \gamma^{10} = X^2 + X + (1 + \omega).$$

Let $\gamma^3 \in \mathbb{Z}_2[\omega]^2$ then $m_3(X)$ can be found by γ^3 and γ^{12},

$$m_3(X) = (X - \gamma^3)(X - \gamma^{12}) = X^2 - (\gamma^3 + \gamma^{12})X + \alpha^{15} = X^2 + (1 + \omega)X + 1.$$

Let $\gamma^4 \in \mathbb{Z}_2[\omega]^2$ then $m_4(X)$ can be found by γ^4 and γ^1,

$$m_4(X) = (X - \gamma^4)(X - \gamma) = X^2 + X + \omega = m_1(X).$$

Let $\gamma^5 \in \mathbb{Z}_2[\omega]^2$ then $m_5(X)$ can be found by γ^5,

$$m_5(X) = X - \gamma^5 = X + \omega.$$

Let $\gamma^6 \in \mathbb{Z}_2[\omega]^2$ then $m_6(X)$ can be found by γ^6 and γ^9,

$$m_6(X) = (X - \gamma^6)(X - \gamma^9) = X^2 - (\gamma^6 + \gamma^9)X + \alpha^{15} = X^2 + \omega X + 1.$$

Let $\gamma^7 \in \mathbb{Z}_2[\omega]^2$ then $m_7(X)$ can be found by γ^7 and γ^{13},

$$m_7(X) = (x - \gamma^7)(x - \gamma^{13}) = x^2 - (\gamma^7 + \gamma^{13})x + \gamma^{20} = x^2 + \gamma x + \omega.$$

Let $\gamma^8 \in \mathbb{Z}_2[\omega]^2$ then $m_8(X)$ can be found by γ^8 and γ^2,

$$m_8(X) = (X - \gamma^2)(X - \gamma^8) = X^2 - (\gamma^2 + \gamma^8)X + \gamma^{10} = X^2 + X + (1 + \omega) = m_2(X).$$

The generator polynomial $g(X)$ is,

$$g(X) = m_1(X).m_2(X).m_3(X).m_5(X).m_6(X).m_7(X)$$

$$= (x^2 + x + \omega)\big(x^2 + x + (1 + \omega)\big)(x^2 + (1 + \omega)x + 1)(x + \omega)(x^2 + \omega x + 1)(x^2 + \gamma x + \omega)$$

$$= x^{11} + (1 + \gamma + \omega)x^{10} + (1 + \gamma + \gamma\omega)x^9 + (1 + \gamma + \omega + \gamma\omega)x^8 + \gamma\omega x^7 + (1 + \gamma)x^6 + (\omega + \gamma\omega)x^5 + (1 + \omega)x^4 + x^3 + (\gamma + \omega)x^2 + (\omega + \gamma\omega)x + (1 + \omega).$$

The degree of $g(X)$ is 11, and the dimension k is 4. Hence, we get $(15, 4, 9)$ BCH codes over EF $\mathbb{Z}_2[\omega]$.

4. Decoding algorithm-based EF

This section is for the comprehensive decoding procedure of BCH codes based that are superimposed on an EF with length n using modified BMA.

The subsequent theorem is a merely restatement of [27, Section V, Theorem 2].

Theorem 2. Let C be a n length BCH code that is superimposed over a GF $\mathbb{Z}_p[\omega]$ if $(p \equiv 2)(mod\ 3)$ with a distance d that has been created. Then the code C is the null space of the matrix H.

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

Proof. Straightforward [28].

Let c be a code word of the (n, k, d) narrow sense BCH code, received word r and design

distance d. Then the error corrections of the BCH codes have the following steps.

Step 1: Let S_i for $i = c, c+1, \ldots, c+d-2$ be the syndromes with the help of H and r as;

$$S_i = rH^{\mathrm{T}}(\mathrm{mod}\, p) = (S_c \;\; S_{c+1} \;\; \ldots \;\; S_{c+d-2}).$$

OR $S_i = r(\gamma^i) = a_0 + a_1\gamma^i + \cdots + a_{n-1}\gamma^{(n-1)i}$ for $i = c, c+1, \ldots, c+d-2$.

If all S_i are zeros then $c = r$. However, if at least one S_i is nonzero then the error occurs. So, we will move to the next step.

Step 2: Apply modified BMP to find $\Delta^n(y)$.

Table 3. Modified BMA.

Iterations	$\Delta^n(y)$	ϑ_n	u_n	$n-u_n$
-1	1	1	0	-1
0	1	F*irst non-zero syndrome*	0	0
1				
⋮				
$2t$				

Where ϑ_n is the discrepancy, degree $\left(\Delta^n(y)\right) = u_n$ and t is the upper bound of the number of errors. There are two cases for Δ^n(y);

Case 1: If $\vartheta_n = 0$, then Δ^{n+1}(y) = Δ^n(y) and $u_n = u_{n+1}$.

Case 2: If $\vartheta_n \neq 0$, then for $m \leq n-1$ and $n-u_m$ have the largest value in $n-u_n$. So, from $\vartheta_n - z\vartheta_m = 0$, we get z. Thus, $\Delta^{n+1}(y) = \Delta^n(y) - zy^{n-m}\,\Delta^m(y)$. Then,

$$\vartheta_{n+1} = \mathrm{S}_{n+2} + \Delta_1^{(n+1)}(\mathrm{y})\mathrm{S}_{n+1} + \Delta_2^{(n+1)}(\mathrm{y})\mathrm{S}_n + \ldots + \Delta_{u_{n+1}}^{(n+1)}(\mathrm{y})\mathrm{S}_{n+2-u_{n+1}}.$$

Step 3: Find the reciprocal function g(y) of Δ^n(y), then y_j represents the roots of g(y). Let $x_j = \rho^j$ are error locations if it satisfies the $(x_j - y_j) = 0$, where $1 \leq j \leq n-1$.

Step 4: Find an elementary symmetric function (ESF) for the possible errors that occur in the received word.

$$(y-x_1)(y-x_2)\ldots(y-x_v) = \Delta_0 y^v + \Delta_1 y^{v-1} + \cdots + \Delta_v,$$

where x_{j}, $j = 1,2, \ldots, v$ and v is the total number of the roots of $g(y)$.

Step 5: The magnitude of the errors can be found by Forney's procedure [29] as;

$$z_i = \frac{\sum_{l=0}^{v-1} \Delta_{i,j} S_{v-l}}{\sum_{l=0}^{v-1} \delta_{i,j} x_i^{v-l}}.$$

Start with $\Delta_0 = \Delta_{i,0} = 1$. Where $\Delta_{i,j} = \Delta_j + x_i.\Delta_{i,j-1}; j = 1, 2, 3, \ldots, v-1$ and $i = 1, 2, \ldots, v$.

Step 6: The cord word c can be corrected by $c = r - e$, where e is the error vector.

Illustration 9. Let $(15, 11, 3)$ BCH code over the EF $\mathbb{Z}_2[\omega]$ and the received vector $r = (0,0,\omega, \ldots, 0)_{1\times 15}$. Find the corrected cord word if possible.

Let

$$S = rH^T = (0\ \ 0\ \ \omega\ \ \ldots 0)\begin{pmatrix} 1\ \gamma\ \ \gamma^2\ \ \cdots\ \ \gamma^{14} \\ 1\ \gamma^2\ \gamma^4\ \ \cdots\ \ \gamma^{28} \end{pmatrix}^T = \begin{pmatrix} \omega\gamma^2 \\ \omega\gamma^4 \end{pmatrix} = \begin{pmatrix} 1+\omega+\gamma\omega \\ \omega+\gamma\omega \end{pmatrix} = \begin{pmatrix} \gamma^7 \\ \gamma^9 \end{pmatrix}.$$

Where $S_1 = \gamma^7$ and $S_2 = \gamma^9$ are two syndromes. Find $\Delta^2(y)$ by modified BMA by the following iterations.

Iteration 1. The first nonzero syndrome is $1 + \omega + \gamma\omega$. Apply step 2 (case II) of the BMA because $\vartheta_0 \neq 0$, $-1 = -1$, and $0 - u_{-1} = 0$ is the higher value of the last column. Then, $\vartheta_0 - z\vartheta_{-1} = 0$, then

$$z = \frac{\vartheta_0}{\vartheta_{-1}} = \frac{1+\omega+\gamma\omega}{1} = 1 + \omega + \gamma\omega.$$

So the polynomial

$$\begin{aligned} \Delta^1(y) &= \Delta^0(y) - (1 + \omega + \gamma\omega)y^{0+1}\Delta^{-1}(y) \\ &= 1 + (1 + \omega + \gamma\omega)y = 1 + (1 + \omega + \gamma\omega)\mathrm{y} = 1 + \gamma^7 y. \end{aligned}$$

$$\vartheta_1 = S_2 + \Delta_1^{(1)}(\mathrm{y})S_1 = \omega + \gamma\omega + (1 + \omega + \gamma\omega)(1 + \omega + \gamma\omega) = 1 + \gamma = \gamma^4.$$

Iteration 2. $\vartheta_1 \neq 0$ in Iteration 1, $0 = 1 - 1$ and $1 - u_0 = 1 - 0 = 1$ is the higher value of the last column. Thus, $\vartheta_1 - z\vartheta_0 = 0$, then

$$z = \frac{\vartheta_1}{\vartheta_0} = \frac{1+\gamma}{1+\omega+\gamma\omega} = 1 + \gamma + \gamma\omega = \gamma^{12}.$$

So, the polynomial

$$\begin{aligned} \Delta^2(y) &= \Delta^1(y) - (1 + \gamma + \gamma\omega)y^{1-0}\Delta^0(y) \\ &= 1 + \gamma^7 y + (1 + \gamma + \gamma\omega)y(1) \\ &= 1 + (\gamma + \omega)\mathrm{y} = 1 + \gamma^2 y. \end{aligned}$$

The results of the iterations are given in Table 4.

Table 4. Linear polynomial by modified BMA.

Iterations	$\Delta^n(y)$	ϑ_n	u_n	$n - u_n$
-1	1	1	0	-1
0	1	$\gamma^7 = 1 + \omega + \gamma\omega$	0	0
1	$1 + \gamma^7 y$	$\gamma^4 = 1 + \gamma$	1	0
2	$1 + \gamma^2 y$			

The reciprocal function of $\Delta^2(y) = 1 + \gamma^2 y$ is $g(y) = \gamma^2 + y.\gamma^2$ is the root of $g(y)$. Hence $y_1 = \gamma^2$, so an error occurred in second place of $r.\Delta_0\mathrm{y}^v + \Delta_1 = \mathrm{y} - \gamma^2$ is an ESF. The error magnitude is

$$z_1 = \frac{\Delta_{1,0}S_1}{\Delta_{1,0}x_1} = \frac{S_1}{x_1} = \frac{1+\omega+\gamma\omega}{\omega+\gamma} = \frac{\gamma^7}{\gamma^2} = \gamma^5 = \omega,$$

where $\Delta_0 = 1, \Delta_1 = \gamma^2$ and $v = 1$. Corrected code word $c = a - e = (0, 0, 0, \ldots, 0)_{1\times 15}$. Hence c is

the corrected code word of the $(15, 11, 3)$ BCH code C.

Illustration 10. Let $(15, 11, 3)$ BCH code over the EF $\mathbb{Z}_2[\omega]$ and the received vector $r = r = (1,1,\omega,0,1,0,\ldots,0)_{1\times 15}$. Find the corrected cord word if possible.

Let

$$S = rH^T = (1,1,\omega,0,1,0,\ldots,0)\begin{pmatrix} 1 & \gamma & \gamma^2 & \cdots & \gamma^{14} \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{28} \end{pmatrix}^T = \begin{pmatrix} \omega\gamma^2 \\ \omega\gamma^4 \end{pmatrix} = \begin{pmatrix} 1+\omega+\gamma\omega \\ \omega+\gamma\omega \end{pmatrix} = \begin{pmatrix} \gamma^7 \\ \gamma^9 \end{pmatrix}.$$

Where $S_1 = \gamma^7$ and $S_2 = \gamma^9$ are two syndromes. Find $\Delta^2(y)$ by modified BMA by the following iterations.

Iteration 1. The first nonzero syndrome is $1 + \omega + \gamma\omega$. Apply step 2 (case II) of the BMA because $\vartheta_0 \neq 0, -1 = -1$ and $0 - u_{-1} = 0$ is the higher value of the last column. Thus, $\vartheta_0 - z\vartheta_{-1} = 0$, then

$$z = \frac{\vartheta_0}{\vartheta_{-1}} = \frac{1+\omega+\gamma\omega}{1} = 1 + \omega + \gamma\omega.$$

So, the polynomial

$$\begin{aligned} \Delta^1(y) &= \Delta^0(y) - (1+\omega+\gamma\omega)y^{0+1}\Delta^{-1}(y) \\ &= 1 + (1+\omega+\gamma\omega)y = 1 + (1+\omega+\gamma\omega)\mathrm{y} = 1 + \gamma^7 y. \end{aligned}$$

$$\vartheta_1 = S_2 + \Delta_1^{(1)}(\mathrm{y})\mathrm{S}_1 = \omega + \gamma\omega + (1+\omega+\gamma\omega)(1+\omega+\gamma\omega) = 1 + \gamma = \gamma^4.$$

Iteration 2. $\vartheta_1 \neq 0$ in Iteration 1, $0 = 1 - 1$ and $1 - u_0 = 1 - 0 = 1$ is the higher value of the last column. Thus, $\vartheta_1 - z\vartheta_0 = 0$, then $z = \frac{\vartheta_1}{\vartheta_0} = \frac{1+\gamma}{1+\omega+\gamma\omega} = 1 + \gamma + \gamma\omega = \gamma^{12}$. So, the polynomial

$$\begin{aligned} \Delta^2(y) &= \Delta^1(y) - (1+\gamma+\gamma\omega)y^{1-0}\Delta^0(y) \\ &= 1 + \gamma^7 y + (1+\gamma+\gamma\omega)y(1) = 1 + (\gamma+\omega)\mathrm{y} = 1 + \gamma^2 y. \end{aligned}$$

The results of the iterations are given in Table 5.

Table 5. Linear polynomial by modified BMA.

Iterations	$\Delta^n(y)$	ϑ_n	u_n	$n - u_n$
-1	1	1	0	-1
0	1	$\gamma^7 = 1 + \omega + \gamma\omega$	0	0
1	$1 + \gamma^7 y$	$\gamma^4 = 1 + \gamma$	1	0
2	$1 + \gamma^2 y$			

The reciprocal function of $\Delta^2(y) = 1 + \gamma^2 y$ is $g(y) = \gamma^2 + y.\gamma^2$ is the root of $g(y)$. Hence $y_1 = \gamma^2$, so an error occurred in second place of $r.\Delta_0\mathrm{y}^v + \Delta_1 = \mathrm{y} - \gamma^2$ is an ESF. The error magnitude is

$$z_1 = \frac{\Delta_{1,0}S_1}{\Delta_{1,0}x_1} = \frac{S_1}{x_1} = \frac{1+\omega+\gamma\omega}{\omega+\gamma} = \frac{\gamma^7}{\gamma^2} = \gamma^5 = \omega,$$

where $\Delta_0 = 1, \Delta_1 = \gamma^2$ and $v = 1$. Corrected code word $c = a - e = (0, 0, 0, \ldots, 0)_{1\times 15}$. Hence c is the corrected code word of the $(15, 11, 3)$ BCH code C.

Illustration 10. Let $(15, 11, 5)$ BCH code over the EF $\mathbb{Z}_2[\omega]$ and the received vector $r = (1\ \omega\ \omega\ 1\ 1\ 0\ 0\ \ldots\ 0)_{1\times 15}$. Find the corrected cord word if possible.

Let

$$S = rH^T = (1\ \ \omega\ \ \omega\ \ 1\ \ 1\ \ 0\ \ 0 \ldots 0)\begin{pmatrix} 1\ \gamma\ \ \gamma^2\ \cdots\ \gamma^{14} \\ 1\ \gamma^2\ \ \gamma^4\ \cdots\ \gamma^{28} \\ 1\ \gamma^3\ \ \gamma^6\ \cdots\ \gamma^{42} \\ 1\ \gamma^4\ \gamma^8\ \cdots\ \gamma^{56} \end{pmatrix}^T$$

$$= \begin{pmatrix} 1+\gamma+\gamma\omega \\ 1+\gamma+\omega+\gamma\omega \\ 1+\gamma+\gamma\omega \\ 1+\omega+\gamma\omega \end{pmatrix} = \begin{pmatrix} \gamma^{12} \\ \gamma^{14} \\ \gamma^{12} \\ \gamma^{7} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix}.$$

Let$S_1 = 1+\gamma+\gamma\omega = \gamma^{12}, S_2 = 1+\gamma+\omega+\gamma\omega = \gamma^{14}, S_3 = 1+\gamma+\gamma\omega = \gamma^{12}$ and $S_4 = 1+\omega+\gamma\omega = \gamma^7$. Find $\Delta^4(y)$ by modified BMA by the following iterations.

Iteration 1. The first nonzero syndrome is $1+\gamma+\gamma\omega$. Apply step 2 (case II) of the BMA because $\vartheta_0 \neq 0, -1 = -1$ and $0 - u_{-1} = 0$ is the higher value of the last column. Thus, $\vartheta_0 - z\vartheta_{-1} = 0$, then

$$z = \frac{\vartheta_0}{\vartheta_{-1}} = \frac{1+\gamma+\gamma\omega}{1} = 1+\gamma+\gamma\omega = \gamma^{12}.$$

So, the polynomial

$$\Delta^1(y) = \Delta^0(y) - (1+\gamma+\gamma\omega)y^{0+1}\Delta^{-1}(y) = 1 + (1+\gamma+\gamma\omega)y = 1+\gamma^{12}y.$$

$$\vartheta_1 = S_2 + \Delta_1^{(1)}(\mathrm{y})\mathrm{S}_1 = (1+\gamma+\omega+\gamma\omega) + (1+\gamma+\gamma\omega)(1+\gamma+\gamma\omega) = 1+\gamma = \gamma^4.$$

Iteration 2. $\vartheta_1 \neq 0$ in Iteration 1, $0 = 1 - 1$ and $1 - u_0 = 1 - 0 = 1$ is the higher value of the last column. Thus, $\vartheta_1 - z\vartheta_0 = 0$, then

$$z = \frac{\vartheta_1}{\vartheta_0} = \frac{1+\gamma}{1+\gamma+\gamma\omega} = \gamma\omega + 1 + \omega = \gamma^7.$$

So, the polynomial

$$\begin{aligned}\Delta^2(y) &= \Delta^1(y) - (\gamma\omega + 1 + \omega)y^{1-0}\,\Delta^0(y) \\ &= 1 + \gamma^7 y + (1+\gamma+\gamma\omega)y(1) = 1 + (\gamma+\omega)\mathrm{y} = 1+\gamma^2 y. \\ \vartheta_2 &= S_3 + S_2\Delta_1^{(2)}(\mathrm{y}) + \Delta_2^{(2)}(\mathrm{y})\mathrm{S}_1 \\ &= (1+\gamma+\gamma\omega) + (\gamma+\omega)(1+\gamma+\omega+\gamma\omega) + 0 = 1+\gamma\omega = \gamma^{13}.\end{aligned}$$

Iteration 3. $\vartheta_2 \neq 0$ in Iteration 2, $1 = 2 - 1$ and $2 - u_1 = 2 - 1 = 1$ is the higher value of the last column. Thus, $\vartheta_2 - z\vartheta_1 = 0$, then

$$z = \frac{\vartheta_2}{\vartheta_1} = \frac{1+\gamma\omega}{1+\gamma} = \gamma\omega + \omega = \gamma^9.$$

So, the polynomial

$$\begin{aligned}\Delta^3(y) &= \Delta^2(y) - (\gamma\omega+\omega)y^{2-1}\Delta^1(y) = 1 + \gamma^2 y + (\omega+\gamma\omega)y(1+\gamma^{12}y)\\ &= 1 + (\gamma+\gamma\omega)y + (\gamma\omega)y^2 = 1 + \gamma^{11}y + \gamma^6 y^2.\\ \vartheta_3 &= S_4 + S_3\Delta_1^{(3)}(\mathrm{y}) + \Delta_2^{(3)}(\mathrm{y})\mathrm{S}_2 + \Delta_3^{(3)}(\mathrm{y})\mathrm{S}_1\\ &= (1+\omega+\gamma\omega) + (\gamma+\gamma\omega)(1+\gamma+\gamma\omega) + (\gamma\omega)(1+\gamma+\omega+\gamma\omega) + 0\\ &= \gamma + \omega + \gamma\omega = \gamma^3.\end{aligned}$$

Iteration 4. $\vartheta_3 \neq 0$ in Iteration 3, $2 = 3-1$ and $3 - u_2 = 3 - 1 = 2$ is the higher value of the last column. Thus, $\vartheta_3 - z\vartheta_2 = 0$, then $z = \frac{\vartheta_3}{\vartheta_2} = \frac{\gamma+\omega+\gamma\omega}{1+\gamma\omega} = \omega = \gamma^5$. So, the polynomial

$$\begin{aligned}\Delta^4(y) &= \Delta^3(y) - (\omega)y^{3-2}\Delta^2(y) = 1 + \gamma^{11}y + \gamma^6 y^2 + (\omega)y(1+\gamma^2 y)\\ &= 1 + (\gamma+\omega+\gamma\omega)y + (1+\omega)y^2 = 1 + \gamma^3 y + \gamma^{10}y^2.\end{aligned}$$

The results of the iterations are given in Table 6.

Table 6. Quadratic polynomial by modified BMA.

Iterations	$\Delta^n(y)$	ϑ_n	u_n	$n-u_n$
-1	1	1	0	-1
0	1	$1+\gamma+\gamma\omega = \gamma^{12}$	0	0
1	$1+\gamma^{12}y$	$\gamma^4 = 1+\gamma$	1	0
2	$1+\gamma^2 y$	$\gamma^{13} = 1+\gamma\omega$	1	1
3	$1+\gamma^{11}y+\gamma^6 y^2$	$\gamma^3 = \gamma+\omega+\gamma\omega$	2	1
4	$1+\gamma^3 y+\gamma^{10}y^2$			

The reciprocal function of $\Delta^4(y) = 1+\gamma^3 y+\gamma^{10}y^2$ is $g(y) = y^2+\gamma^3 y+\gamma^{10}$. γ and γ^9 are the roots of $g(y)$. Hence $y_1 = \gamma$ and $y_2 = \gamma^9$, so the errors appeared in first and ninth place in

$$r.\Delta_0\mathrm{y}^2 + \Delta_1\mathrm{y} + \Delta_2 = (\mathrm{y}-\gamma)(y-\gamma^9) = y^2+\gamma^3 y+\gamma^{10}$$

is an ESF. The error magnitudes are as;

$$\mathrm{z}_1 = \frac{\Delta_{1,0}.\mathrm{S}_2 + \Delta_{1,1}.\mathrm{S}_1}{\Delta_{1,0}.\mathrm{z}_1^2 + \Delta_{1,1}.\mathrm{x}_1} = 1+\gamma = \gamma^4.$$

As $\Delta_{1,1} = \Delta_1 + \Delta_{1,0}.y_1 = \gamma^9$, therefore

$$\Delta_{2,1} = \Delta_1 + \Delta_{2,0}.y_2 = \gamma.$$

$$\mathrm{z}_2 = \frac{\Delta_{2,0}.\mathrm{S}_2 + \Delta_{2,1}.\mathrm{S}_1}{\Delta_{2,0}.\mathrm{y}_2^2 + \Delta_{2,1}.\mathrm{y}_2} = \gamma\omega = \gamma^6.$$

Corrected code word

$$c = a - e = (1, 1 + \omega + \gamma, 0, 0, 0, 0, 0, 0, 0, \gamma\omega, 0, 0, 0, 0, 0)_{1\times 15}.$$

Hence c is the corrected code word of the $(15, 11, 5)$ BCH code C.

5. Comparison

We compare the narrow sense BCH code and decoding method on a GF and an EF. BCH-codes base $GF(p^m)$ are defined with detail in [7, Section 4.4], including their length $(n = p^m - 1)$, design distances (d), dimension (k_1), code rates $(R_1 = k_1/(p^m - 1)$ and words of C (p^{k_1}). Here, the authors provide BCH codes of length $(n = p^{2m} - 1)$, design distance (d), dimension k_2, code rate $(R_2 = k_2/(p^{2m} - 1)$ and the words of C over the EF $\mathbb{Z}_p[\omega]$ are p^{2k_2}, and their decoding technique. Comparisons between BCH codes based on GF and EF are given in Tables 7 and 8.

For comparison we take a one GF and one EF. Based on the results of [9, Exercise 4.4 (10)], length of the code n is $p^m - 1 = 2^4 - 1$, design distance$d$, dimension k_1, coding rate R_1 and the code words p^{k_1} are given in Table 7.

Table 7. Results of BCH codes-based GF.

n	d	k_1	R_1	p^{k_1}
15	3	11	0.7333	2^{11}
15	5	7	0.4667	2^7
15	7	5	0.3333	2^5
15	9	1	0.0667	2^1

In a similar way, the length of the code $n = p^{2m} - 1 = 2^4 - 1 = 15$, dimension k_2, designed distance d, code rate R_2 and the words of C are p^{2k_2} over the EF $\mathbb{Z}_p[\omega] = \mathbb{Z}_2[\omega]$ given in Table 8.

Table 8. Results of BCH codes-based EF.

n	d	k_2	R_2	q^{k_2}
15	3	11	0.7333	2^{11}
15	5	9	0.6	2^9
15	7	6	0.4	2^6
15	9	4	0.2667	2^4

Figure 3 shows the BCH coding rate R_1 over a Galois field (GF) and R_2 over the Eisenstein field with designed distance d from Tables 7 and 8. Figure 4 shows the BCH code dimension k_1 over a Galois field and k_2 over an Eisenstein field with designed distance d.

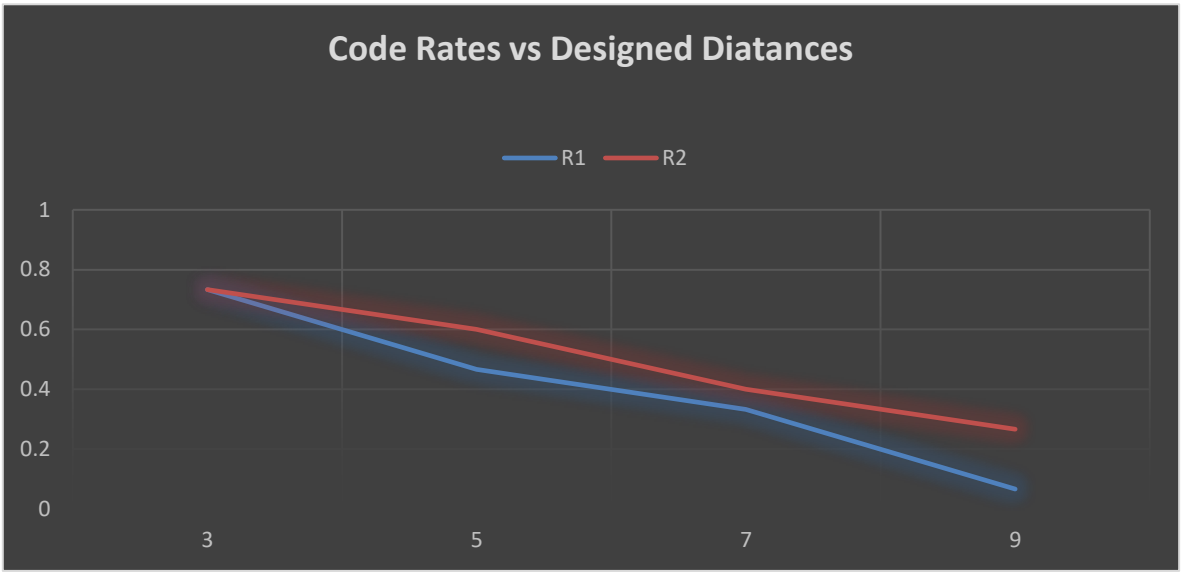

Figure 3. GF and EF code rates and designed distances.

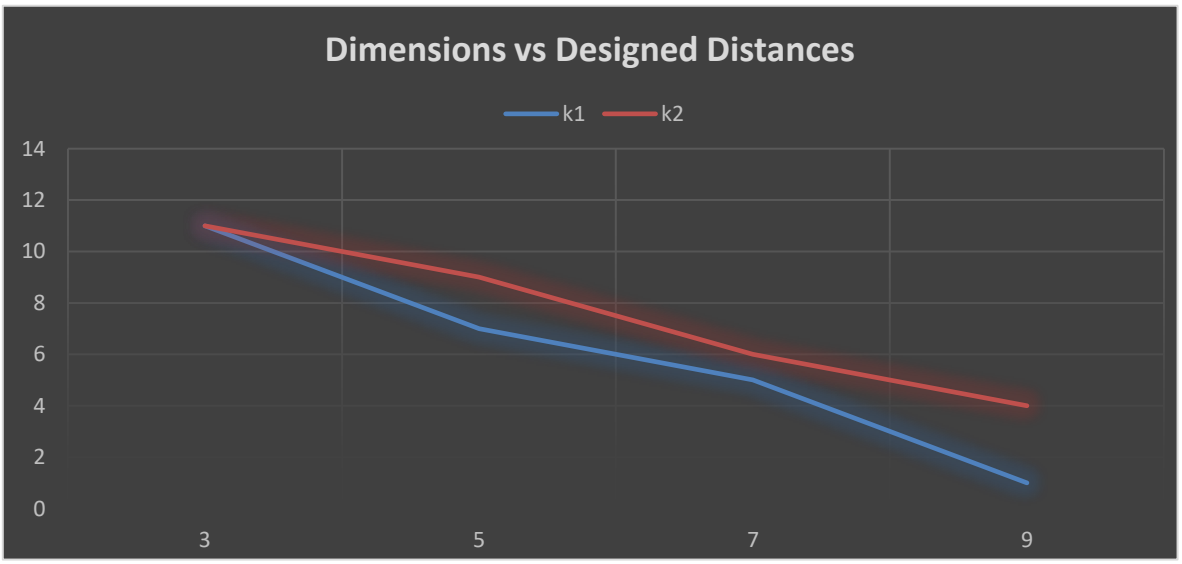

Figure 4. GF and EF dimensions and designed distances.

6. Discussion for shortcoming

When the BCH codes-based GF and their decoding algorithm are compared with the EF and their decoding method for the same length and designed distance, the following observations are achieved. In the Eisenstein field, the code rates and dimensions are greater than in the Galois field. The BCH code over the Eisenstein field has a lot number of code words than the Galois field. The decoding algorithm over the GF is a specific algorithm for error correction, whereas the Eisenstein field decoding algorithm is a general algorithm for error correction.

7. Conclusions and future direction

The Eisenstein field and its extension are covered in this article. Additionally, the construction of BCH codes based on the EF $\mathbb{Z}_p[\omega]$, for $p \equiv 2(mod\ 3)$ has been provided. Furthermore, a slightly modified version of the BMA was used to decode these codes. It has been demonstrated that the performance of the BCH codes over the EF $\mathbb{Z}_p[\omega]$ for $p \equiv 2(mod\ 3)$ and their decoding technique is superior to that of the BCH codes over the $GF(p^m)$.

In future directions, BCH codes based on EF $\mathbb{Z}_p[\omega]$ and its decoding technique may extend across Eisenstein local rings $\mathbb{Z}_{p^k}[\omega]$, for $p \equiv 2(mod\ 3)$, which may improve performance of the BCH codes using symbols from $\mathbb{Z}_p[\omega]$.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

Researchers Supporting Project number: RSPD 2023R650, King Saud University, Riyadh, Saudi Arabia.

Conflict of interest

The authors declared that they had no conflicts of interest.

References

1. R. E. Blahut, *Algebraic codes for data transmission*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511800467
2. T. Richardson, R. Urbanke, *Modern coding theory*, Cambridge University Press, 2008. https://doi.org/10.1017/CBO9780511791338
3. J. E. F. Assmus, H. F. Mattson, Error-correcting codes: an axiomatic approach, *Inf. Control*, **6** (1963), 315–330. https://doi.org/10.1016/S0019-9958(63)80010-8
4. D. Augot, E. Betti, E. Orsini, An introduction to linear and cyclic codes, In: M. Sala, S. Sakata, T. Mora, C. Traverso, L. Perret, *Gröbner bases, coding, and cryptography*, Springer, 2009, 47–68. https://doi.org/10.1007/978-3-540-93806-4_4
5. I. F. Blake, Codes over certain rings, *Inf. Control*, **20** (1972), 396–404. https://doi.org/10.1016/S0019-9958(72)90223-9
6. I. F. Blake, Codes over integer residue rings, *Inf. Control*, **29** (1975), 295–300. https://doi.org/10.1016/S0019-9958(75)80001-5
7. E. Spiegel, Codes over $\mathbb{Z}m$, *Inf. Control*, **35** (1977), 48–51. https://doi.org/10.1016/S0019-9958(77)90526-5
8. E. Spiegel, Codes over $\mathbb{Z}m$, revisited, *Inf. Control*, **37** (1978), 100–104. https://doi.org/10.1016/S0019-9958(78)90461-8

9. T. Shah, A. Khan, A. A. de Andrade, Constructions of codes through the semigroup ring B [X; $\frac{1}{2^2}$ $\mathbb{Z}_0$] and encoding, *Comput. Math. Appl.*, **62** (2011), 1645–1654. https://doi.org/10.1016/j.camwa.2011.05.056
10. B. Yildiz, I. Siap, Cyclic codes over F_2 [u]/(u^4−1) and applications to DNA codes, *Comput. Math. Appl.*, **63** (2012), 1169–1176. https://doi.org/10.1016/j.camwa.2011.12.029
11. G. Weil, K. Heus, T. Faraut, J. Demongeot, The cyclic genetic code as a constraint satisfaction problem, *Theor. Comput. Sci.*, **322** (2004), 313–334. https://doi.org/10.1016/j.tcs.2004.03.015
12. H. Q. Dinh, A. K. Singh, S. Pattanayak, S. Sriboonchitta, Construction of cyclic DNA codes over the ring $\mathbb{Z}_4$ [u]/<u^2−1> based on the deletion distance, *Theor. Comput. Sci.*, **773** (2019), 27–42. https://doi.org/10.1016/j.tcs.2018.06.002
13. B. Kim, Y. Lee, J. Yoo, An infinite family of Griesmer quasi-cyclic self-orthogonal codes, *Finite Fields Appl.*, **76** (2021), 1019–1023. https://doi.org/10.1016/j.ffa.2021.101923
14. F. Zullo, Multi-orbit cyclic subspace codes and linear sets, *Finite Fields Appl.*, **87** (2023), 102153. https://doi.org/10.1016/j.ffa.2022.102153
15. Y. Lei, C. Li, Y. Wu, P. Zeng, More results on hulls of some primitive binary and ternary BCH codes, *Finite Fields Appl.*, **82** (2022), 102066. https://doi.org/10.1016/j.ffa.2022.102066
16. Y. Liu, R. Li, Q. Fu, L. Lu, Y. Rao, Some binary BCH codes with length n=2^m+1, *Finite Fields Appl.*, **55** (2019), 109–133. https://doi.org/10.1016/j.ffa.2018.09.005
17. O. Alkam, E. A. Osba, On Eisenstein integers modulo *n*, *Int. Math. Forum*, **5** (2010), 1075–1082.
18. S. R. Nagpaul, S. K. Jain, *Topics in applied abstract algebra*, American Mathematical Society, 2005.
19. M. Sajjad, T. Shah, R. J. Serna, Designing pair of nonlinear components of a block cipher over Gaussian integers, *Comput. Mater. Cont.*, **75** (2023), 5287–5305. https://doi.org/10.32604/cmc.2023.035347
20. 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*, **10** (2022), 219. https://doi.org/10.3390/computation10120219
21. M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi, I. Hussain, Quaternion integers based higher length cyclic codes and their decoding algorithm, *Comput. Mater. Cont.*, **73** (2022), 1177–1194. https://doi.org/10.32604/cmc.2022.025245
22. M. Sajjad, T. Shah, M. Alammari, H. Alsaud, Construction and decoding of BCH-codes over the Gaussian field, *IEEE Access*, **11** (2023), 71972–71980. https://doi.org/10.1109/ACCESS.2023.3293007
23. M. Sajjad, T. Shah, H. Alsaud, M. Alammari, Designing pair of nonlinear components of a block cipher over quaternion integers, *AIMS Math.*, **8** (2023), 21089–21105. https://doi.org/10.3934/math.20231074
24. K. Huber, Codes over Eisenstein-Jacobi integers, *Contemp. Math.*, **168** (1994), 165–179. https://doi.org/10.1090/conm/168/01696
25. J. H, Baek, M. H. Sunwoo, New degree computationless modified Euclid algorithm and architecture for Reed-Solomon decoder, *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, **14** (2006), 915–920. https://doi.org/10.1109/TVLSI.2006.878484
26. A. A. D. Andrade, T. Shah, A. Khan, Decoding procedure for BCH, alternant and Goppa codes defined over semigroup ring, *TEMA*, **12** (2011), 8–14.

27. M. Eiglsperger, M. Siebenhaller, M. Kaufmann, An efficient implementation of Sugiyama's algorithm for layered graph drawing, In: J. Pach, *Graph Drawing*, GD 2004. Lecture Notes in Computer Science, Springer, **3383** (2004), 155–166. https://doi.org/10.1007/978-3-540-31843-9_17
28. M. Sajjad, T. Shah, M. Alammari, H. Alsaud, Construction and decoding of BCH-codes over the Gaussian field, *IEEE Access*, **11** (2023), 71972–71981. https://doi.org/10.1109/ACCESS.2023.3293007
29. G. Forney, On decoding BCH codes, *IEEE Trans. Inf. Theory*, **11** (1965), 549–557. https://doi.org/10.1109/TIT.1965.1053825
30. T. Shah, A note on ascend and descend of factorization properties, *Bull. Korean Math. Soc.*, **43** (2006), 419–424.
31. A. C. Canto, M. M. Kermani, R. Azarderakhsh, Reliable architectures for composite-field-oriented constructions of McEliece post-quantum cryptography on FPGA, *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, **40** (2020), 999–1003. https://doi.org/10.1109/TCAD.2020.3019987
32. A. C. Canto, M. M. Kermani, R. Azarderakhsh, Reliable CRC-based error detection constructions for finite field multipliers with applications in cryptography, *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, **29** (2020), 232–236. https://doi.org/10.1109/TVLSI.2020.3031170

AIMS Press