EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6275
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Design and Analysis of Shortened Bose-Chaudhuri-Hocquenghem Codes for Efficient Data Transmission over the Eisenstein Fields

Muhammad Sajjad[1,*], Rida Asghar[2], Mushtaq K. Abdalrahem[3], Adnan Burhan Rajab[4], Mahesha Narayana[5], Moin-ud-Din Junjua[6,*], Salman A. AlQahtani[7]

[1] *NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad, 44000, Pakistan*
[2] *Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan*
[3] *College of Pharmacy, University of Al-Ameed*
[4] *Department of Computer Engineering, College of Engineering, Knowledge University, Erbil 44001, Iraq*
[5] *Department of Mathematics, The University of the West Indies, Kingston 7, Jamaica*
[6] *School of Mathematical Sciences, Zhejiang Normal University, Jinhua 321004, China*
[7] *New Emerging Technologies and 5G Network and Beyond Research Chair, Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia*

Abstract. This article focuses on the constructing and decoding of Shortened Bose-Chaudhuri-Hocquenghem (BCH) codes over the Eisenstein fields, based on the Berlekamp-Massey Algorithm (BMA) with improved decoding performance. Thus, Eisenstein fields, being a natural generalization of Gaussian fields, form a well-devised algebraic structure for error-correcting codes and have better parameters for transmission of information in noisy channels. The work starts with the definition of shortened BCH codes over the Eisenstein fields with the mention of generator polynomials and the study of certain algebraic characteristics. These codes are designed to provide the best balance between the word's length and the ability to cope with error detection and correction in a variety of high-efficiency applications. The modified BMA is presented as a decoding mechanism that is equipped for the translation of Eisenstein field arithmetic, which is different in nature. The modification concerns an improved approach to the residual terms defined by the classes of higher level, which leads to the efficiency of convergence and the reduction of numerical complexity in contrast to the BMA. The imitations show that the proposed codes offer a higher error-correcting capability and faster computation compared to the traditional BCH codes over finite fields when reliability and low latency are desired.

2020 Mathematics Subject Classifications: 94B75, 11T71, 94A24, 68P30, 14G50, 94A05
Key Words and Phrases: Eisenstein field, Shortened BCH codes, Modified BMA

*Corresponding author.
*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6275

Email addresses: muhammad.sajjad@nutech.edu.pk (M. Sajjad), moinuddin@zjnu.edu.cn (M. Junjua)

1. Introduction

Nowadays transmission of data is necessary, and error-correcting hyphenate codes are critically important for realizing reliable data transmission via noisy channels. Of them, BCH codes are being widely studied because of their algebraic nature and superlative error correction capability. Originally built over finite fields, BCH codes are widely used in storage equipment, wireless communication, and other data-applying fields. However, as the requirement for higher reliability and system efficiency increases in the next generation of communication systems, researchers are considering different algebraic contexts that will help improve these codes. Such field-based approaches are also possible, and Eisenstein fields appear to be logical extensions of Gaussian fields. Several algebraic characteristics of Eisenstein fields, including unique factorization and extended residue classes, can be critically exploited for efficient codes as well as being resilient to errors. Nonetheless, the use of the Eisenstein fields in coding theory has not been fully researched until now, especially in the construction and decoding of shortened BCH codes. This is especially due to the fact that shortened codes are renowned for their capability to sustain relatively short codes with good error correction capabilities. Shortened codes are well suited for any application that requires concise and efficient communication code. Other components of error-correcting codes as a standard are decoding algorithms. In a number of situations, the Berlekamp-Massey Algorithm (BMA) has been a standard tool in the decoding of BCH codes. Nevertheless, its use in Eisenstein fields may be problematic due to the fact that the residue classes are extended and the computations are more cumbersome. Overcoming these challenges calls for propositions on the classical BMA for faster and more accurate decoding for codes over Eisenstein fields [1–6].

Among the coding techniques, the error-correcting code, especially the shortened BCH code of a given order, has been an important topic in coding theory because of its random error-correcting capability and use in high-reliability communication systems. The theoretical characteristics of shortened cyclic codes and their uses, especially for burst-error correction, were investigated by Kasami and Hsu. Further, they pointed out that, while optimizing code length, it is necessary to balance the amount of correction capacity [7, 8]. Helgert and Stinaff extended the construction and decoding of shortened BCH codes and the fact that these codes are well suited to any narrow bandwidth systems [9]. Traditionally linear codes have been discussed in numerous algebraic contexts, for example, BCH codes. Cyclotomic linear codes of order three were studied by Ding and Niederreiter, and cyclic codes with certain specified weight distributions were investigated by Ding et al. [10, 11], because such codes have been deemed useful in application, particularly in efficient error correction. Shah et al. introduced codes and decoding using generalized polynomials and sequences in [12, 13]. Linear codes from 2-designs have also been designed by Ding, who offered a new way to define codes with performance characteristics that would be suitable for various practical uses [14]. An important part of the development of coding theory demands the consideration of shortened and punctured codes. Goldwasser studied the relation between code shortening and MacWilliams identities by giving significant information about the structure of these codes [15]. Yardi and Pellikaan also investigated

the behaviour of shortened cyclic codes in more detail regarding that being useful for solving error correction for a constraint [16]. Gaussian fields are extended to Eisenstein fields, which have attracted attention as a sound algebraic structure for implementing richer error-correcting codes. Huber extended codes over Eisenstein-Jacobi integers, which laid down the groundwork for approaching these fields in coding theory [17]. Later on, Sajjad et al. did more advanced work on Eisenstein and Gaussian fields using cryptology and error correction codes, showing more efficiency in noisy channel communication systems [18, 19].

The Berlekamp-Massey Algorithm (BMA) has played an important role in decoding schemes of linear and cyclic codes, BCH codes. Appropriate overviews of the overall algorithm and explanations of its uses were given by Lin and Huffman and Pless for decoding finite geometry and cyclic codes [20, 21]. Nonetheless, the computational complexity of the classical BMA remains fairly high, and innovative modified algorithms have been adapted to solve concrete algebraic structures. The adoption of such modifications, mainly for Eisenstein fields, is a useful step forward in terms of simplification of decoding and increasing the convergence rate [19]. Other important works have brought to the knowledge of issues on the algebraic structures for the coding theory. The combinatorial characteristics of linear codes were examined using t-designs by Assmus and Mattson, while t-covers of the finite projective spaces were studied by Beutelspacher, which also focused on the geometry [20, 22]. These concepts have been further generalized to mixed binary/ternary codes by Brower et al. [16] and to codes obtained from Boolean functions by Tang et al. [23], thus proving the versatility of algebraic methods in terms of reliable code construction.

This paper extends the literature presented above by developing abbreviated BCH codes over Eisenstein fields and presenting an adapted BMA appropriate to the arithmetic of the shortened BCH codes. This work fills the gap of existing Eisenstein field theoretical developments and applies them to error correction and amplification of several features, promoting the reliability and performance of communication systems. Thus, this thesis supplements prior research and helps further develop the theory of coding for the next generations by utilizing the algebraic characteristics of Eisenstein fields and enhancing the decoding approach [7, 9, 17–19, 24].

Shortened Bose-Chaudhuri-Hocquenghem (BCH) codes have been found to be very useful in correcting errors, thereby facilitating smooth data communication in noisy media. Their flexibility and speed are ideal for the current data transmission networks where the probability of error and computational time are critical concerns [9, 24]. While the classical BCH codes over finite fields are highly efficient, they seem to have drawbacks that cropped up in some high-reliability applications, such as the trade-off between the code length and error-correcting capability [7, 8]. The proposed concept of Eisenstein fields as an algebraic structure is prospective to open a new direction toward research on the construction of higher coding schemes. Eisenstein fields are a natural generalization of Gaussian fields and offer a higher level of structural complexity, which can contribute to the improvement of the error-correcting code. A number of previous works, including Huber and Sajjad et al., have shown that Eisenstein and Gaussian fields could be applied in cryptographic

applications and coding theory; hence, more investigation needs to be made on the use of Eisenstein and Gaussian fields in the construction of BCH code [17, 18]. Moreover, current improvements in decoding techniques like the Berlekamp-Massey Algorithm (BMA) offer potentialities to make moderate decoding procedures and lessen the computational intricacy required to defend contemporary communication systems [19, 20]. This research is motivated by developing error-correcting codes with enhanced performance measures and channel decoding techniques using Eisenstein field advantages. The proposed modification of BMA and integration with these three fields is designed to contribute to the further development of coding theory and real communication applications.

Despite significant advancements in coding theory, several research gaps persist in the development of shortened BCH codes and their decoding techniques. Although the fields of Eisenstein have been discussed in the sphere of cryptography and the theory of codes, the application of such fields to construct shortened BCH codes has not been thoroughly investigated. In finite and Gaussian fields, most of the previous studies have been performed on them [17–19]. The classical BMA has been studied in detail in literature, but its complexity is high and thus becomes a problem when one needs to use it in the real-time application. Extensions of the above-described BMA, especially those that take into account arithmetic properties of Eisenstein fields, are few and far between in the literature [19, 21, 25]. Previous research works that analyze the shortened BCH codes mostly focus on either the length reduction aspect or the error-correcting capability dimension without providing a balance between the two factors. Such balance is envisaged for applications that demand both high reliability and low latency [7–9]. Closing these gaps, this research is aimed at developing shortened BCH codes over the Eisenstein fields, deriving the generator polynomials for them, and presenting the modified BMA for decoding. Therefore, this study seeks to solve the problem of developing an understanding of the trade-offs and performance measures to close the gap that exists between theoretical enhancements and application in coding theory.

This work presents new approaches toward the construction and decoding of error-correcting codes using shortened BCH codes over the Eisenstein fields. The study constructs these codes from a fresh perspective with reference to the properties of Eisenstein fields as an augmentation of Gaussian fields to attain optimal generator polynomials and algebraic architecture. The obtained codes strike a perfect balance between possible code length and the code's ability to correct errors, making it perfect for applications where reliability is paramount and latency is low. An original approach proposed in this work is the modified Berlekamp-Massey Algorithm (BMA) suitable for the Eisenstein fields. The approach outlined in this modification is capable of utilizing more complex methods to deal with wider residue classes in order to offer better convergence and lower computational demands than needed for the classical BMA. In the analysis of performance, the work reveals that the proposed codes exhibit higher error correction and better computational complexity compared to conventional BCH over finite fields. In addition, this research expands on the cyclic subgroups of fields of Eisenstein for coding theory, as it now incorporates settings outside of cryptographic applications, thereby finding its usefulness in next-generation communication systems. These contributions are firm to fill the existing

gaps in coding theory and also plan a strong base for many more inventions in the field.

2. Eisenstein Field

From [26], assume ω being the cubic root of unity correspondingly $1+\omega+\omega^2=0$. Assume that $\mathbb{Z}[\omega]=\{a+b\omega : a,b\in\mathbb{Z}\}$ be the Euclidean domain of the Eisenstein integers. Consequently, it $\mathbb{Z}_p[\omega]=\{a+b\omega : a,b\in\mathbb{Z}_p\}$ is a commutative ring with identity and $\mathbb{Z}_p[\omega]$ is an Eisenstein field (EF) if $p\equiv 2 \pmod 3$.

Illustration 2.1: From [24, 26], let $\mathbb{Z}_2[\omega]=\{0,1,\omega,1+\omega\}$ be the EF, as every nonzero element of $\mathbb{Z}_2[\omega]$ is a unit element and the cardinality of $\mathbb{Z}_2[\omega]$ is $2^2=4$.

Remark 2.1 [26]: $\mathbb{Z}_p[\omega]$ has p^2 elements if $p\equiv 2 \pmod 3$.

2.1. Eisenstein Field Extension

From [26], assume $\mathbb{Z}_p[\omega]$ with $p\equiv 2 \pmod 3$ is an EF, then $\mathbb{Z}_p[\omega][x]$ is a Euclidean domain. For the extension of EF, $\mathbb{Z}_p[\omega]^m$, we have:

$$\mathbb{Z}_p[\omega]^m=\frac{\mathbb{Z}_p[\omega][x]}{\langle H(x)\rangle}\cong \mathrm{GF}(p^{2m}),$$

where $\langle H(x)\rangle$ is the maximal ideal generated by an irreducible polynomial $H(x)$ of degree k in $\mathbb{Z}_p[\omega][x]$. Let β be the coset $x+\langle H(x)\rangle$, so that $H(\beta)=0$. Moreover,

$$\mathbb{Z}_p[\omega]^m=\left\{a_0+a_1\beta+a_2\beta^2+\cdots+a_{m-1}\beta^{m-1} : \forall a_0,a_1,\ldots,a_{m-1}\in\mathbb{Z}_p[\omega]\right\}.$$

$\mathbb{Z}_p[\omega]^m$ is an m-degree extension field of $\mathbb{Z}_p[\omega]$. The multiplicative group $\mathbb{Z}_p[\omega]^{*m}=\mathbb{Z}_p[\omega]^m\setminus\{0\}$ is a cyclic group (CG) of order $p^{2m}-1$.

Remark 2.2 [26, Remark 3]: The cardinality of $\mathbb{Z}_p[\omega]^m$ is p^{2m}.

Illustration 2.2: Assume that the quotient ring

$$\frac{\mathbb{Z}_2[\omega][x]}{\langle x^2+\omega x+\omega\rangle}=\{a_0+a_1x : \forall a_0,a_1\in\mathbb{Z}_2[\omega]\}=\mathbb{Z}_2[\omega]^2,$$

is generated by the primitive irreducible polynomial $H(x)=x^2+\omega x+\omega$ over $\mathbb{Z}_2[\omega]$. Let α be a root of $H(x)$ in the extension field $\mathbb{Z}_2[\omega][x]$, then $H(\alpha)=0$ as $\alpha^2+\omega\alpha+\omega=0$, and $\mathbb{Z}_2[\omega]^{*2}=\mathbb{Z}_2[\omega]^2\setminus\{0\}$ is a cyclic group (CG) of order $2^{2\cdot 2}-1=15$ as shown in Table 1.

Now, for finding the total number of possible polynomials, the possible irreducible polynomials, and the number of primitive irreducible polynomials over the Eisenstein Field (EF)

$$\frac{\mathbb{Z}_2[\omega][x]}{\langle f(x)\rangle}$$

for $f(x)$ being a polynomial of degree 2, consider Table 2.

Table 1: Cyclic Group over Eisenstein Integers of Order 15

S. No.	**Power of α's**	**S. No.**	**Power of α's**
1	α	9	$\omega+1+\alpha\omega$
2	$\alpha\omega+\omega$	10	$1+\omega$
3	$\alpha+\omega+1$	11	$\alpha+\alpha\omega$
4	$\alpha+\omega$	12	$1+\alpha$
5	ω	13	$\omega+\alpha(1+\omega)$
6	$\alpha\omega$	14	$1+\alpha+\alpha\omega$
7	$\alpha(1+\omega)+1+\omega$	15	1
8	$\alpha\omega+1$		

Illustration 2.3: Let the quotient ring

$$\frac{\mathbb{Z}_2[\omega][x]}{\langle x^3+x^2+x+1+\omega\rangle}=\left\{a_0+a_1x+a_2x^2 \mid a_0,a_1,a_2\in\mathbb{Z}_2[\omega]\right\}=\mathbb{Z}_2[\omega][x]^3,$$

be generated by the irreducible primitive polynomial $H(x)=x^3+x^2+x+1+\omega$ over $\mathbb{Z}_2[\omega]$, and let α be the root of $H(x)$ in the extension field $\mathbb{Z}_2[\omega][x]$. Then $H(\alpha)=0$ implies

$$\alpha^3+\alpha^2+\alpha+1+\omega=0 \quad \Rightarrow \quad \alpha^3=\alpha^2+\alpha+1+\omega.$$

Therefore, $\mathbb{Z}_2[\omega]_3^*=\mathbb{Z}_2[\omega]^3\setminus\{0\}$ is a cyclic group of order $2^{2\cdot3}-1=64-1=63$, as illustrated in Table 3.

Remark 2.4: The order of a subgroup of Eisenstein integers must divide the order of the corresponding group of Eisenstein integers.

Illustration 2.4: If we require a subgroup of five elements over the extension field $Z_2[\omega][x]$, then we know that we cannot directly obtain it from any polynomial $f(x)$ of degree 2 over

$$\frac{Z_2[\omega][x]}{\langle f(x)\rangle}.$$

We obtain a cyclic group of order

$$n=\left((2)^2\right)^2-1=16-1=15.$$

The desired subgroup is obtained by dividing n by 5, i.e.,

$$\frac{15}{5}=3.$$

If α is the root of the extension field $Z_2[\omega][x]$, then α^3 is the generator of the required subgroup of $Z_2[\omega][x]^2$ for $n=5$. Similarly, we can find a subgroup for $n=3$.

Illustration 2.5: If we want a subgroup of twenty-one elements over $Z_2[\omega][x]$, we cannot directly obtain it from any polynomial $f(x)$ of degree 3 over

$$\frac{Z_2[\omega][x]}{\langle f(x)\rangle}.$$

Table 2: Details of Irreducible and Primitive Irreducible Polynomials

Polynomials of degree two over $\mathbb{Z}_2[\omega]$	**Irreducible**	**Primitive Irreducible**
x^2	×	×
x^2+1	×	×
$x^2+\omega$	✓	×
$x^2+1+\omega$	✓	×
x^2+x	×	×
$x^2+\omega x$	×	×
$x^2+(1+\omega)x$	×	×
x^2+x+1	×	×
$x^2+x+\omega$	✓	✓
$x^2+x+1+\omega$	✓	✓
$x^2+\omega x+1$	✓	×
$x^2+\omega x+\omega$	✓	✓
$x^2+\omega x+1+\omega$	×	×
$x^2+(1+\omega)x+1$	×	×
$x^2+(1+\omega)x+\omega$	×	×
$x^2+(1+\omega)x+1+\omega$	✓	×

Instead, we obtain a cyclic group of order

$$n = \left((2)^2\right)^3 - 1 = 64 - 1 = 63.$$

The desired subgroup is obtained by dividing n by 21, i.e.,

$$\frac{63}{21} = 3.$$

If α is the root of the extension field $Z_2[\omega][x]$, then α^3 is the generator of the required subgroup of $Z_2[\omega][x]$ for $n = 21$. Similarly, subgroups of orders 3, 7, and 9 can be found with generators α^{21}, α^9, and α^7 respectively.

3. Shortened BCH Codes over the Eisenstein Field

Shortened BCH codes over the Eisenstein fields involve taking a longer BCH code, perhaps over a bigger Eisenstein field, and shortening it to achieve specific design goals, such as minimizing complexity or meeting certain constraints. It involves nearly the same steps as shortened BCH codes over Eisenstein fields [13, 17, 26].

3.1. Encoding of Shortened BCH Code over the Eisenstein Field

First of all, obtain the shortened BCH code from the full length BCH code over the extension field $Z_p[\omega]$, where $p \equiv 2 \pmod 3$. Assume that the integers $c, n, k, d > 0$, such

Table 3: Cyclic Group over Eisenstein Integers of Order 63

S. No.	**Power of α's**	**S. No.**	**Power of α's**
1	α	33	$(\alpha+1+\omega\alpha)^2$
2	α^2	34	$(\alpha(1+\omega)+1+(1+\omega)\alpha)^2$
3	$\alpha^2+\alpha+1+\omega$	35	$\omega+\omega\alpha$
4	$1+\omega+\omega\alpha$	36	$(\omega\alpha+\omega\alpha)^2$
5	$\alpha+\omega\alpha+\alpha^2\omega$	37	$\omega\alpha+1$
6	$\alpha^2+\omega\alpha+1$	38	$\alpha+\omega\alpha^2$
7	$\alpha^2(1+\omega)+1+\omega$	39	$(1+\omega)\alpha^2+1+\omega\alpha$
8	$\alpha^2(1+\omega)+\omega$	40	$\alpha^2+\omega+\omega\alpha$
9	$\alpha+\alpha^2(1+\omega)+\omega$	41	$1+\omega+(1+\omega)\alpha^2+(1+\omega)\alpha$
10	$\alpha+\omega+\omega\alpha^2$	42	ω
11	$\alpha^2(1+\omega)+1$	43	$\omega\alpha$
12	$(1+\omega)\alpha^2+\omega+\omega\alpha$	44	$\omega\alpha^2$
13	$\alpha+\omega+\alpha^2$	45	$\omega\alpha^2+1+\omega\alpha$
14	$1+\omega+(1+\omega)\alpha$	46	$(1+\omega)\alpha+1$
15	$(1+\omega)\alpha^2+\omega\alpha$	47	$\alpha+(1+\omega)\alpha^2$
16	$\omega+(1+\omega)\alpha$	48	$\omega\alpha^2+\omega+(1+\omega)\alpha$
17	$(1+\omega)\alpha^2+\omega\alpha$	49	α^2+1
18	$\alpha^2+\omega+(1+\omega)\alpha$	50	$\alpha^2+1+\omega$
19	$\omega\alpha^2+1+\omega+(1+\omega)\alpha$	51	$1+\omega+\alpha^2+\omega\alpha$
20	$\alpha+\alpha^2+1$	52	$1+\omega+(1+\omega)\alpha^2+\omega\alpha$
21	$1+\omega$	53	$\alpha^2+\omega$
22	$(1+\omega)\alpha$	54	$\alpha^2+1+\omega+(1+\omega)\alpha$
23	$(1+\omega)\alpha^2$	55	$1+\omega+\omega\alpha^2+\omega\alpha$
24	$(1+\omega)\alpha^2+\omega+(1+\omega)\alpha$	56	$\alpha+1$
25	$\alpha+\omega$	57	$\alpha+\alpha^2$
26	$\alpha^2+\omega\alpha$	58	$\alpha+1+\omega$
27	$\alpha+1+\omega+(1+\omega)\alpha^2$	59	$\alpha^2+(1+\omega)\alpha$
28	$\omega\alpha^2+\omega$	60	$\alpha+\omega+1+\omega\alpha^2$
29	$\omega\alpha^2+1$	61	$\alpha+(1+\omega)\alpha^2+1$
30	$\omega\alpha^2+(1+\omega)\alpha+1$	62	$\omega+\omega\alpha+\omega\alpha^2$
31	$\alpha^2+(1+\omega)\alpha+1$	63	1
32	$\omega\alpha^2+1+\omega$		

that k is a prime power, $2 \leq d \leq n-1$, and $\gcd(n,k)=1$. Assume that there is a smallest positive integer b such that

$$p^{2b} \equiv 1 \pmod{n}.$$

Then, by Euler's theorem, if

$$p^{2\varphi(n)} \equiv 1 \pmod{n},$$

then b divides $\varphi(n)$, where φ is the Euler phi function. Thus,

$$n \mid (p^{2b}-1).$$

Let β be an element of the extension field $Z_p[\omega]^b$. Consider the minimal polynomials $b_i(x) \in Z_p[\omega][x]$ of β^i. The least common multiple (lcm) of all distinct polynomials $b_i(x)$, for $i = c, c+1, c+2, \ldots, c+d-2$, is known as the generator polynomial $g(x)$, i.e.,

$$g(x) = \operatorname{lcm}\{b_i(x) \mid i = c, c+1, c+2, \ldots, c+d-2\}.$$

Since all minimal polynomials divide x^n-1, the generator polynomial $g(x)$ also divides x^n-1. Let C be the cyclic code generated by $g(x)$ in the ring $Z_p[\omega][x]^m$, then C is called a BCH code of length n over the extension field $Z_p[\omega]$ with designed distance d.

Now, if the code length is shorter than the full length BCH code, then it is known as a shortened BCH code. If the code is a narrow-sense shortened BCH code, then $c = 1$.

Pseudocode of the encoding algorithm is given in Algorithm 3.1.

Algorithm 1 Encode Shortened BCH Codes over EF

Input: Prime p such that $p \equiv 2 \pmod 3$
  Code parameters: n (length), k (dimension), d (designed distance), c (starting exponent)
  Message vector $m(x)$ of length k over $Z_p[\omega]$
Output: Codeword $c(x)$ of length n over $Z_p[\omega]$
1. Verify Preconditions:
  a. Ensure $\gcd(n, k) = 1$
  b. Ensure $2 \leq d \leq n-1$
  c. Ensure k is a prime power
2. Compute Extension Degree b**:**
  a. Find smallest positive integer b such that $p^{2b} \equiv 1 \pmod n$
  b. Ensure b divides $\varphi(n)$, where φ is Euler's totient function
3. Construct Extension Field:
  a. Define extension field $E = Z_p[\omega]^b$
  b. Select a primitive element $\beta \in E$
4. Determine Generator Polynomial $g(x)$**:**
for each $i = c$ to $c + d - 2$ **do**
  a. Compute minimal polynomial $b_i(x)$ of β^i over $Z_p[\omega]$
end for
b. Compute generator polynomial:

$$g(x) = \text{lcm}\{b_i(x) \mid i = c, c+1, \ldots, c+d-2\}$$

5. Construct BCH Code:
  a. Define BCH code C as cyclic code generated by $g(x)$ over ring $Z_p[\omega][x]/(x^n - 1)$
6. Apply Shortening:
  i. Let $n' < n$ be the shortened length
  ii. Restrict codeword positions to a subset of size n'
  iii. Set the unused message bits to zero
  iv. Resulting code is a shortened BCH code of length n'
7. Encode Message:
  a. Multiply message polynomial $m(x)$ by $g(x)$:

$$c(x) = m(x) \cdot g(x) \mod (x^n - 1)$$

8. Return codeword $c(x)$

Theorem 3.1 [26] : Assume α is an element of the extension field $Z_p[\omega]^m$ where $p \equiv 2 \pmod 3$. Then, the elements

$$\alpha^{p^0}, \quad \alpha^{p^2}, \quad \alpha^{p^4}, \quad \alpha^{p^6}, \quad \ldots$$

have minimal polynomials over the Eisenstein field $Z_p[\omega]$.

Illustration 3.1: Construct a Shortened BCH code for a degree-two polynomial by taking $n = 3$ over the Eisenstein field $Z_2[\omega]^2$.

Let us take a degree-two polynomial

$$f(x) = x^2 + \omega x + \omega,$$

which is primitive and irreducible over $Z_2[\omega]$. As proved in Section 2, the cardinality of the cyclic group generated by $f(x)$ is 15, and since $15/3 = 5$, our required cyclic subgroup is generated by $\langle \beta = \alpha^5 \rangle$, where β is the root of $f(x)$.

The required cyclic subgroup is

$$G^* = \{\alpha^5, \alpha^{10}, \alpha^{15} = 1\} = \{\omega, 1 + \omega, 1\}.$$

Thus, there is only one case for the construction of Shortened BCH codes over $Z_2[\omega]^2$ with parameters $n = 3$ and $d = 3$.

- For $i = 1$, let $\beta \in Z_2[\omega]^2$. Then, by Theorem 3.1, β has a minimal polynomial

$$\varphi_1(x) = (x - \beta) = x + \omega.$$

- For $i = 2$, let $\beta^2 \in Z_2[\omega]^2$. Then, by Theorem 3.1, β^2 has a minimal polynomial by itself:

$$\varphi_2(x) = (x - \beta^2) = x + (1 + \omega).$$

Now, the generator polynomial is

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) = (x + \omega)(x + (1 + \omega)) = x^2 + x + 1.$$

Since $k = 3 - 2 = 1$, the parameters of the Shortened BCH code are $(n, k, d) = (3, 1, 3)$.

Illustration 3.2: Construct a Shortened BCH code for a degree-two polynomial by taking $n = 5$ over the Eisenstein field $Z_2[\omega]^2$.

Let us take a degree-two polynomial

$$f(x) = x^2 + \omega x + \omega,$$

which is primitive and irreducible over $Z_2[\omega]$. As proved in Section 2, the cardinality of the cyclic group generated by $f(x)$ is 15 and $15/5 = 3$. So, our required cyclic subgroup is generated by $\langle \beta = \alpha^3 \rangle$, where β is the root of $f(x)$.

The required cyclic subgroup is

$$G^* = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15} = 1\} = \{1 + \omega + \alpha, \alpha\omega, 1 + \omega + \alpha\omega, \alpha + 1, 1\}.$$

Thus, there are two cases for the construction of Shortened BCH codes over $Z_2[\omega]^2$.

Case 1: For $n = 5$ and $d = 3$, $i = 1, 2$.

- For $i = 1$, let $\beta \in Z_2[\omega]^2$. By Theorem 3.1, β and β^4 have the same minimal polynomial:

$$\varphi_1(x) = (x - \beta)(x - \beta^4) = x^2 - (\beta + \beta^4)x + \beta^5 = x^2 + \omega x + 1.$$

- For $i = 2$, let $\beta^2 \in Z_2[\omega]^2$. By Theorem 3.1, β^2 and β^3 have the same minimal polynomial:

$$\varphi_2(x) = (x - \beta^2)(x - \beta^3) = x^2 - (\beta^2 + \beta^3)x + \beta^5 = x^2 + (1 + \omega)x + 1.$$

The generator polynomial is

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) = (x^2 + \omega x + 1)(x^2 + (1 + \omega)x + 1) = x^4 + x^3 + x^2 + x + 1.$$

Since $k = 5-4 = 1$, the parameters of the Shortened BCH code are $(n, k, d) = (5, 1, 3)$.

Case 2: For $n = 5$ and $d = 5$, $i = 1, 2, 3, 4$.

- For $i = 1$, as before,

$$\varphi_1(x) = x^2 + \omega x + 1.$$

- For $i = 2$,

$$\varphi_2(x) = x^2 + (1 + \omega)x + 1.$$

- For $i = 3$, by Theorem 3.1, β^3 and β^2 have the same minimal polynomial, so

$$\varphi_3(x) = \varphi_2(x) = x^2 + (1 + \omega)x + 1.$$

- For $i = 4$,

$$\varphi_4(x) = \varphi_1(x) = x^2 + \omega x + 1.$$

The generator polynomial is again

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) = (x^2 + \omega x + 1)(x^2 + (1 + \omega)x + 1) = x^4 + x^3 + x^2 + x + 1.$$

Since $k = 5-4 = 1$, the parameters of this Shortened BCH code are $(n, k, d) = (5, 1, 5)$.

Illustration 3.3: Construct a Shortened BCH code for a degree-three polynomial by taking $n = 3$ over the Eisenstein field $Z_2[\omega]^3$.

Let us take a degree-three polynomial

$$f(x) = x^3 + x^2 + x + 1 + \omega,$$

which is primitive and irreducible over $Z_2[\omega]$. As proved in Section 2, the cardinality of the cyclic group generated by $f(x)$ is 63, and

$$\frac{63}{3} = 21.$$

So, our required cyclic subgroup is generated by $\langle\beta = \alpha^{21}\rangle$, where β is the root of $f(x)$.

The required cyclic subgroup is

$$G^* = \{\alpha^{21}, \alpha^{42}, \alpha^{63} = 1\} = \{1 + \omega, \omega, 1\}.$$

Hence, there is only one case for the construction of Shortened BCH codes over the Eisenstein field $Z_2[\omega]^3$.

For $n = 3$ and $d = 3$, $i = 1, 2$:

- For $i = 1$, let $\beta \in Z_2[\omega]^3$. By Theorem 3.1, β has minimal polynomial itself:

$$\varphi_1(x) = (x - \beta) = x + (1 + \omega).$$

- For $i = 2$, let $\beta^2 \in Z_2[\omega]^3$. By Theorem 3.1, β^2 has minimal polynomial itself:

$$\varphi_2(x) = (x - \beta^2) = x + \omega.$$

The generator polynomial is

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) = (x + \omega)(x + (1 + \omega)) = x^2 + x + 1.$$

Since $k = 3-2 = 1$, the parameters of this Shortened BCH code are $(n, k, d) = (3, 1, 3)$.

Illustration 3.4: Construct a Shortened BCH code for three-degree polynomial by taking $n = 9$ over the EF $\mathbb{Z}_2[\omega]^3$.

Let us take $f(x) = x^3 + x^2 + x + 1 + \omega$, which is primitive and irreducible over $\mathbb{Z}_2[\omega]$. As we proved in Section 2, the cardinality of the cyclic group of $f(x)$ is 63 and $\frac{63}{9} = 7$. So, our required cyclic subgroup is generated by $\langle\beta = \alpha^7\rangle$ by taking β to be the root of $f(x)$. Then cyclic subgroup is

$$G^8 = \{\beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6, \beta^7, \beta^8, \beta^9 = 1\} = \{\alpha^7, \alpha^{14}, \alpha^{21}, \alpha^{28}, \alpha^{35}, \alpha^{42}, \alpha^{49}, \alpha^{56}, \alpha^{63} = 1\}$$

$$= \{\alpha^2(1 + \omega) + 1 + \omega, 1 + \omega + (1 + \omega)\alpha, 1 + \omega, \omega\alpha^2 + \omega, \omega + \omega\alpha, \omega, \alpha^2 + 1, \alpha + 1, 1\}.$$

So, there are four cases for the construction of Shortened BCH codes over the EF $\mathbb{Z}_2[\omega]^3$.

Case 1: For $n = 9$ and $d = 3$, $i = 1, 2$.

- For $i = 1$, let $\beta \in \mathbb{Z}_2[\omega]^3$. By Theorem 3.1, β, β^4, β^7 have the minimal polynomial

$$\varphi_1(x) = (x - \beta)(x - \beta^4)(x - \beta^7) = (x^2 + (\beta + \beta^4)x + \beta^5)(x - \beta^7)$$

$$= (x^2 + (\beta + \beta^4)x + \beta^5)(x + \beta^7) = x^3 + (\beta + \beta^4 + \beta^7)x^2 + (\beta^2 + \beta^5 + \beta^8)x + \beta^3$$

$$= x^3 + 0 \cdot x^2 + 0 \cdot x + \beta^3 = x^3 + 1 + \omega.$$

- For $i = 2$, let $\beta^2 \in \mathbb{Z}_2[\omega]^3$. By Theorem 3.1, $\beta^2, \beta^5, \beta^8$ have the minimal polynomial

$$\varphi_2(x) = (x - \beta^2)(x - \beta^5)(x - \beta^8) = (x^2 + (\beta^2 + \beta^5)x + \beta^7)(x + \beta^8)$$

$$= x^3 + (\beta^2 + \beta^5 + \beta^8)x^2 + (\beta + \beta^4 + \beta^7)x + \beta^6 = x^3 + 0 \cdot x^2 + 0 \cdot x + \beta^6 = x^3 + \omega.$$

Now the generator polynomial is

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) = (x^3 + \omega)(x^3 + 1 + \omega) = x^6 + \omega x^3 + (1 + \omega)x^3 + 1 = x^6 + x^3 + 1.$$

Hence, $k = 9 - 6 = 3$. So the shortened BCH code parameters are $(n, k, d) = (9, 3, 3)$.
Case 2: For $n = 9$ and $d = 5$, $i = 1, 2, 3, 4$.

- For $i = 1$, $\varphi_1(x) = x^3 + 1 + \omega$ (as in Case 1).
- For $i = 2$, $\varphi_2(x) = x^3 + \omega$ (as in Case 1).
- For $i = 3$, let $\beta^3 \in \mathbb{Z}_2[\omega]^3$ then by Theorem 3.1,

$$\varphi_3(x) = (x - \beta^3) = (x + 1 + \omega).$$

- For $i = 4$, $\varphi_4(x) = \varphi_1(x) = x^3 + 1 + \omega$.

The generator polynomial is

$$\begin{aligned} G(x) = \operatorname{lcm}(\varphi_1(x), \varphi_2(x), \varphi_3(x), \varphi_4(x)) &= (x^3 + \omega)(x^3 + 1 + \omega)(x + 1 + \omega) \\ &= (x^6 + \omega x^3 + (1 + \omega)x^3 + 1)(x + 1 + \omega) \\ &= x^7 + x^6(\omega + 1) + x^4 + x^3(1 + \omega) + x + 1 + \omega. \end{aligned}$$

Hence, $k = 9 - 7 = 2$. So the shortened BCH code parameters are $(9, 2, 5)$.
Case 3: For $n = 9$ and $d = 7$, $i = 1, 2, 3, 4, 5, 6$.

- For $i = 1$, $\varphi_1(x) = x^3 + 1 + \omega$.
- For $i = 2$, $\varphi_2(x) = x^3 + \omega$.
- For $i = 3$, $\varphi_3(x) = x + 1 + \omega$.
- For $i = 4$, $\varphi_4(x) = \varphi_1(x)$.
- For $i = 5$, $\varphi_5(x) = \varphi_2(x)$.
- For $i = 6$, let $\beta^6 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1,

$$\varphi_6(x) = (x - \beta^6) = (x + \omega).$$

The generator polynomial is

$$\begin{aligned} G(x) = \operatorname{lcm}(\varphi_1(x), \varphi_2(x), \varphi_3(x), \varphi_4(x), \varphi_5(x), \varphi_6(x)) &= (x^3+\omega)(x^3+1+\omega)(x+1+\omega)(x+\omega) \\ = (x^6 + \omega x^3 + (1 + \omega)x^3 + 1)(x + 1 + \omega)(x + \omega) &= (x^6 + x^3 + 1)(x + 1 + \omega)(x + \omega) \\ = (x^7 + x^6(\omega + 1) + x^4 + x^3(1 + \omega) + x + 1 + \omega)(x + \omega) & \\ = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1. & \end{aligned}$$

Hence, $k = 9 - 8 = 1$. So the shortened BCH code parameters are $(9, 1, 7)$.

Illustration 3.5: *Construct a Shortened BCH code for a three-degree polynomial by taking* $n = 21$ *over the Eisenstein field* $\mathbb{Z}_2[\omega]^3$.

Let us take

$$f(x) = (x^3 + x)^2 + x + 1 + \omega$$

which is primitive and irreducible over $\mathbb{Z}_2[\omega]$. As shown in Section 2, the cardinality of the cyclic group generated by $f(x)$ is 63. Since $\frac{63}{21} = 3$, the required cyclic subgroup is generated by

$$\langle \beta = \alpha^3 \rangle,$$

where β is a root of $f(x)$. Then the cyclic subgroup is

$$G^* = \{\beta, \beta^2, \ldots, \beta^{21} = 1\} = \{\alpha^3, \alpha^6, \alpha^9, \ldots, \alpha^{63}\}.$$

Thus, explicitly:

$$G^* = \{\alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15}, \alpha^{18}, \alpha^{21}, \alpha^{24}, \alpha^{27}, \alpha^{30}, \alpha^{33}, \alpha^{36}, \alpha^{39}, \alpha^{42}, \alpha^{45}, \alpha^{48}, \alpha^{51}, \alpha^{54}, \alpha^{57}, \alpha^{60}, \alpha^{63} = 1\}.$$

So, there are ten cases for the construction of Shortened BCH codes over the EF $\mathbb{Z}_2[\omega]^3$.

Case 1: For $n = 21$, $d = 3$, $i = 1, 2$.
For $i = 1$, let $\beta \in \mathbb{Z}_2[\omega]^3$. By Theorem 3.1, the minimal polynomial of $\beta, \beta^4, \beta^{16}$ is

$$\varphi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

For $i = 2$, the minimal polynomial of $\beta^2, \beta^8, \beta^{11}$ is

$$\varphi_2(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+(\beta^2+\beta^8+\beta^{11})x^2+(\beta^{10}+\beta^{13}+\beta^{19})x+\beta^{21} = x^3+\omega x^2+1.$$

Generator polynomial:

$$G(x) = \varphi_1(x)\varphi_2(x) = (x^3 + (1 + \omega)x^2 + 1)(x^3 + \omega x^2 + 1) = x^6 + x^5 + x^4 + x^2 + x + 1.$$

Therefore, $k = 21 - 6 = 15$, and the BCH code is $(n, k, d) = (21, 15, 3)$.

Case 2: For $n = 21$, $d = 5$, $i = 1, 2, 3, 4$.
The minimal polynomials are:

$$\begin{aligned}
\varphi_1(x) &= x^3 + (1 + \omega)x^2 + 1,\\
\varphi_2(x) &= x^3 + \omega x^2 + 1,\\
\varphi_3(x) &= (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1,\\
\varphi_4(x) &= \varphi_2(x).
\end{aligned}$$

Generator polynomial:

$$G(x) = \varphi_1(x)\varphi_2(x)\varphi_3(x) = (x^6 + x^5 + x^4 + x^2 + x + 1)(x^3 + x + 1) = x^9 + x^8 + x^5 + 1.$$

Therefore, $k = 21 - 9 = 12$, and the BCH code is $(n, k, d) = (21, 12, 5)$.

Case 3: For $n = 21$, $d = 7$, $i = 1, 2, 3, 4, 5, 6$.
The minimal polynomials are:

$$\begin{aligned}
&\varphi_1(x) = x^3 + (1+\omega)x^2 + 1,\\
&\varphi_2(x) = x^3 + \omega x^2 + 1,\\
&\varphi_3(x) = x^3 + x + 1,\\
&\varphi_4(x) = \varphi_2(x),\\
&\varphi_5(x) = (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) = x^3 + (1+\omega)x + 1,\\
&\varphi_6(x) = \varphi_3(x).
\end{aligned}$$

Generator polynomial:

$$G(x) = \varphi_1(x)\varphi_2(x)\varphi_3(x)\varphi_5(x).$$

[Polynomial multiplication can be performed explicitly if required.]
Therefore, $k = 21 - (\deg G(x))$, and the BCH code is $(n, k, d) = (21, 9, 7)$.

Case 4: For $n = 21$ and $d = 9$, $i = 1, 2, 3, 4, 5, 6, 7, 8$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, $\beta, \beta^4, \beta^{16}$ has the minimal polynomial

  $$\varphi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_2(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+(\beta^2+\beta^8+\beta^{11})x^2+(\beta^{10}+\beta^{13}+\beta^{19})x+\beta^{21} = x^3+\omega x^2+1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_3(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+(\beta^3+\beta^6+\beta^{12})x^2+(\beta^9+\beta^{18}+\beta^{15})x+\beta^{21} = x^3+x+1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_4(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+\omega x^2+1 = \varphi_2(x).$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_5(x) = (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) = x^3+(\beta^5+\beta^{17}+\beta^{20})x^2+(\beta+\beta^4+\beta^{16})x+\beta^{21} = x^3+(1+\omega)x+1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$, then

$$\varphi_6(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1 = \varphi_3(x).$$

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$, then

$$\varphi_7(x) = (x - \beta^7) = x + 1 + \omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$, then

$$\varphi_8(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1 = \varphi_2(x).$$

Now Generator polynomial is

$$G(x) = \varphi_1(x)\varphi_2(x)\varphi_3(x)\varphi_5(x)\varphi_7(x)$$

$$= (x^{12} + x^{11} + (1 + \omega)x^{10} + \omega x^9 + (1 + \omega)x^6 + x^5 + x^3 + (1 + \omega)x + 1)(x + 1 + \omega)$$

$$= x^{13}+\omega x^{12}+x^9+(1+\omega)x^7+(1+\omega)x^6+(1+\omega)x^5+x^4+(1+\omega)x^3+(1+\omega)x^2+(1+\omega)x+1+\omega.$$

Now $k = 21 - 13 = 8$. So $(n, k, d) = (21, 8, 9)$ is a shortened BCH code.
Case 5: For $n = 21$ and $d = 11$, $i = 1, 2, 3, \ldots, 10$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β, β^4 and β^{16} have the minimal polynomial

$$\phi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

$$\phi_2(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+(\beta^2+\beta^8+\beta^{11})x^2+(\beta^{10}+\beta^{13}+\beta^{19})x+\beta^{21} = x^3+\omega x^2+1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

$$\phi_3(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+(\beta^3+\beta^6+\beta^{12})x^2+(\beta^9+\beta^{18}+\beta^{15})x+\beta^{21} = x^3+x+1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

$$\phi_4(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1 = \phi_2(x).$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1 β^5, β^{17}, and β^{20} have the minimal polynomial

  $$\phi_5(x) = (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) = x^3+(\beta^5+\beta^{17}+\beta^{20})x^2+(\beta+\beta^4+\beta^{16})x+\beta^{21} = x^3+(1+\omega)x+1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

  $$\phi_6(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+x+1 = \phi_3(x).$$

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^7 has the minimal polynomial

  $$\phi_7(x) = (x-\beta^7) = x+1+\omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\phi_8(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+\omega x^2+1 = \phi_2(x).$$

- For $i = 9$,
  Let $\beta^9 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^9, β^{18}, and β^{15} have the minimal polynomial

  $$\phi_9(x) = (x-\beta^9)(x-\beta^{18})(x-\beta^{15}) = x^3+(\beta^9+\beta^{15}+\beta^{18})x^2+(\beta^3+\beta^6+\beta^{12})x+\beta^{21} = x^3+x^2+1.$$

- For $i = 10$,
  Let $\beta^{10} \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^{10}, β^{13}, and β^{19} have the minimal polynomial

  $$\phi_{10}(x) = (x-\beta^{10})(x-\beta^{13})(x-\beta^{19}) = x^3+(\beta^{10}+\beta^{13}+\beta^{19})x^2+(\beta^2+\beta^8+\beta^{11})x+\beta^{21} = x^3+\omega x+1.$$

Now the generator polynomial is

$$G(x) = \phi_1(x)\phi_2(x)\phi_3(x)\phi_5(x)\phi_7(x)\phi_9(x)\phi_{10}(x)$$

$$= x^{19}+(1+\omega)x^{18}+x^{16}+(1+\omega)x^{15}+(1+\omega)x^{14}+(1+\omega)x^{13}+x^8+\omega x^7+(1+\omega)x^6+x^5+(1+\omega)x^4+x^2+\omega x+1+\omega.$$

Now $k = 21-19 = 2$. So the parameters are:

$$(n, k, d) = (21, 2, 11) \quad \text{Shortened BCH code.}$$

Case 6: For $n = 21$ and $d = 13$, $i = 1, 2, \ldots, 12$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β, β^4, and β^{16} have the minimal polynomial

  $$\varphi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\varphi_2(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+(\beta^2+\beta^8+\beta^{11})x^2+(\beta^{10}+\beta^{13}+\beta^{19})x+\beta^{21} = x^3+\omega x^2+1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

  $$\varphi_3(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+(\beta^3+\beta^6+\beta^{12})x^2+(\beta^9+\beta^{18}+\beta^{15})x+\beta^{21} = x^3+x+1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\varphi_4(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+\omega x^2+1 = \varphi_2(x).$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^5, β^{17}, and β^{20} have the minimal polynomial

  $$\varphi_5(x) = (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) = x^3+(\beta^5+\beta^{17}+\beta^{20})x^2+(\beta+\beta^4+\beta^{16})x+\beta^{21} = x^3+(1+\omega)x+1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

  $$\varphi_6(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+x+1 = \varphi_3(x).$$

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^7 has the minimal polynomial

  $$\varphi_7(x) = (x-\beta^7) = x+1+\omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\varphi_8(x) = x^3+\omega x^2+1 = \varphi_2(x).$$

- For $i = 9$,
  Let $\beta^9 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^9, β^{18}, and β^{15} have the minimal polynomial

  $$\varphi_9(x) = x^3+x^2+1.$$

- For $i = 10$,
  Let $\beta^{10} \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^{10}, β^{13}, and β^{19} have the minimal polynomial

  $$\varphi_{10}(x) = x^3+\omega x+1.$$

- For $i = 11$,
  Let $\beta^{11} \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

$$\varphi_{11}(x) = x^3 + \omega x^2 + 1 = \varphi_2(x).$$

- For $i = 12$,
  Let $\beta^{12} \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

$$\varphi_{12}(x) = x^3 + x + 1 = \varphi_3(x).$$

Now, the generator polynomial is

$$G(x) = \varphi_1(x)\varphi_2(x)\varphi_2(x)\varphi_5(x)\varphi_7(x)\varphi_9(x)\varphi_{10}(x)$$

$$= x^{19}+(1+\omega)x^{18}+x^{16}+(1+\omega)x^{15}+(1+\omega)x^{14}+(1+\omega)x^{13}+x^8+\omega x^7+(1+\omega)x^6+x^5+(1+\omega)x^4+x^2+\omega x+1+\omega.$$

Hence, $k = 21 - 19 = 2$. So the parameters of the shortened BCH code are:

$$(n, k, d) = (21, 2, 13).$$

Case 7: For $n = 21$ and $d = 15$, $i = 1, 2, 3, \ldots, 14$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β, β^4 and β^{16} have the minimal polynomial

$$\varphi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial

$$\varphi_2(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial

$$\varphi_3(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial

$$\varphi_4(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1 = \varphi_2(x).$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^5, β^{17} and β^{20} have the minimal polynomial
  $$\varphi_5(x) = (x - \beta^5)(x - \beta^{17})(x - \beta^{20}) = x^3 + (1 + \omega)x + 1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial
  $$\varphi_6(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1 = \varphi_3(x).$$

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^7 has the minimal polynomial
  $$\varphi_7(x) = (x - \beta^7) = x + 1 + \omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial
  $$\varphi_8(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1 = \varphi_2(x).$$

- For $i = 9$,
  Let $\beta^9 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^9, β^{18} and β^{15} have the minimal polynomial
  $$\varphi_9(x) = (x - \beta^9)(x - \beta^{18})(x - \beta^{15}) = x^3 + x^2 + 1.$$

- For $i = 10$,
  Let $\beta^{10} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{10}, β^{13} and β^{19} have the minimal polynomial
  $$\varphi_{10}(x) = (x - \beta^{10})(x - \beta^{13})(x - \beta^{19}) = x^3 + \omega x + 1.$$

- For $i = 11$,
  Let $\beta^{11} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial
  $$\varphi_{11}(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = \varphi_2(x).$$

- For $i = 12$,
  Let $\beta^{12} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial
  $$\varphi_{12}(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1 = \varphi_3(x).$$

- For $i = 13$,
  Let $\beta^{13} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{10}, β^{13} and β^{19} have the minimal polynomial
  $$\varphi_{13}(x) = (x - \beta^{10})(x - \beta^{13})(x - \beta^{19}) = x^3 + \omega x + 1 = \varphi_{10}(x).$$

- For $i = 14$,

  Let $\beta^{14} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{14} has the minimal polynomial

$$\varphi_{14}(x) = (x - \beta^{14}) = x + \omega.$$

  Now the generator polynomial is

$$G(x) = \varphi_1(x) \cdot \varphi_2(x) \cdot \varphi_3(x) \cdot \varphi_5(x) \cdot \varphi_7(x) \cdot \varphi_9(x) \cdot \varphi_{10}(x) \cdot \varphi_{14}(x).$$

  Expanding,

$$G(x) = x^{20} + x^{18} + x^{17} + x^{16} + \omega x^{15} + \omega x^{14} + x^{13} + x^9 + x^5 + x^4 + x^3 + 1.$$

Since $k = 21 - 20 = 1$, the code parameters are $(n, k, d) = (21, 1, 15)$, which is a shortened BCH code.

Case 8: For $n = 21$ and $d = 17, i = 1, 2, 3, \ldots, 16$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β, β^4 and β^{16} have the minimal polynomial

$$\varphi_1(x) = (x - \beta)(x - \beta^4)(x - \beta^{16}) = x^3 + (1 + \omega)x^2 + 1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial

$$\varphi_2(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = x^3 + \omega x^2 + 1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial

$$\varphi_3(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial

$$\varphi_4(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = \varphi_2(x).$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^5, β^{17} and β^{20} have the minimal polynomial

$$\varphi_5(x) = (x - \beta^5)(x - \beta^{17})(x - \beta^{20}) = x^3 + (1 + \omega)x + 1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial

$$\varphi_6(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = \varphi_3(x).$$

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^7 has the minimal polynomial
  $$\varphi_7(x) = (x - \beta^7) = x + 1 + \omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial
  $$\varphi_8(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = \varphi_2(x).$$

- For $i = 9$,
  Let $\beta^9 \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^9, β^{18} and β^{15} have the minimal polynomial
  $$\varphi_9(x) = (x - \beta^9)(x - \beta^{18})(x - \beta^{15}) = x^3 + x^2 + 1.$$

- For $i = 10$,
  Let $\beta^{10} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{10}, β^{13} and β^{19} have the minimal polynomial
  $$\varphi_{10}(x) = (x - \beta^{10})(x - \beta^{13})(x - \beta^{19}) = x^3 + \omega x + 1.$$

- For $i = 11$,
  Let $\beta^{11} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^2, β^8 and β^{11} have the minimal polynomial
  $$\varphi_{11}(x) = (x - \beta^2)(x - \beta^8)(x - \beta^{11}) = \varphi_2(x).$$

- For $i = 12$,
  Let $\beta^{12} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^3, β^6 and β^{12} have the minimal polynomial
  $$\varphi_{12}(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12}) = x^3 + x + 1 = \varphi_3(x).$$

- For $i = 13$,
  Let $\beta^{13} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{10}, β^{13} and β^{19} have the minimal polynomial
  $$\varphi_{13}(x) = (x - \beta^{10})(x - \beta^{13})(x - \beta^{19}) == x^3 + \omega x + 1 = \varphi_{10}(x).$$

- For $i = 14$,
  Let $\beta^{14} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^{14} has the minimal polynomial
  $$\varphi_{14}(x) = (x - \beta^{14}) = x + \omega.$$

- For $i = 15$,
  Let $\beta^{15} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β^9, β^{18} and β^{15} have the minimal polynomial
  $$\varphi_{15}(x) = (x - \beta^9)(x - \beta^{18})(x - \beta^{15}) = \varphi_9(x).$$

- For $i = 16$,
  Let $\beta^{16} \in \mathbb{Z}_2[\omega]^3$. Then by Theorem 3.1, β, β^4 and β^{16} have the minimal polynomial

$$\varphi_{16}(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3 + (1+\omega)x^2 + 1 = \varphi_1(x).$$

Now the generator polynomial is

$$\begin{aligned} G(x) &= \varphi_1(x) \cdot \varphi_2(x) \cdot \varphi_3(x) \cdot \varphi_5(x) \cdot \varphi_7(x) \cdot \varphi_9(x) \cdot \varphi_{10}(x) \cdot \varphi_{14}(x) \\ &= \big(x^{19} + (1+\omega)x^{18} + x^{16} + (1+\omega)x^{15} + (1+\omega)x^{14} + (1+\omega)x^{13} + x^8 + \omega x^7 + (1+\omega)x^6 \\ &\quad + x^5 + (1+\omega)x^4 + x^2 + \omega x + 1 + \omega\big)(\omega + x) \\ &= x^{20} + x^{18} + x^{17} + x^{16} + \omega x^{15} + \omega x^{14} + x^{13} + x^9 + x^5 + x^4 + x^3 + 1. \end{aligned}$$

Now, $k = 21 - 20 = 1$. So the parameters of the shortened BCH code are $(n, k, d) = (21, 1, 17)$.

Case 9: For $n = 21$ and $d = 19$, $i = 1, 2, 3, \ldots, 18$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β, β^4 and β^{16} have the minimal polynomial

$$\begin{aligned} \phi_1(x) &= (x-\beta)(x-\beta^4)(x-\beta^{16}) \\ &= x^3 + (\beta + \beta^4 + \beta^{16})x^2 + (\beta^5 + \beta^{17} + \beta^{20})x + \beta^{21} \\ &= x^3 + (1+\omega)x^2 + 1. \end{aligned}$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$, then $\beta^2, \beta^8, \beta^{11}$ have

$$\begin{aligned} \phi_2(x) &= (x-\beta^2)(x-\beta^8)(x-\beta^{11}) \\ &= x^3 + (\beta^2 + \beta^8 + \beta^{11})x^2 + (\beta^{10} + \beta^{13} + \beta^{19})x + \beta^{21} \\ &= x^3 + \omega x^2 + 1. \end{aligned}$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$, then $\beta^3, \beta^6, \beta^{12}$ have

$$\begin{aligned} \phi_3(x) &= (x-\beta^3)(x-\beta^6)(x-\beta^{12}) \\ &= x^3 + (\beta^3 + \beta^6 + \beta^{12})x^2 + (\beta^9 + \beta^{18} + \beta^{15})x + \beta^{21} \\ &= x^3 + x + 1. \end{aligned}$$

- For $i = 4$, $\phi_4(x) = \phi_2(x) = x^3 + \omega x^2 + 1$.
- For $i = 5$,

$$\begin{aligned} \phi_5(x) &= (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) \\ &= x^3 + (\beta^5 + \beta^{17} + \beta^{20})x^2 + (\beta + \beta^4 + \beta^{16})x + \beta^{21} \\ &= x^3 + (1+\omega)x + 1. \end{aligned}$$

- For $i = 6$, $\phi_6(x) = \phi_3(x) = x^3 + x + 1$.
- For $i = 7$, $\phi_7(x) = (x - \beta^7) = x + 1 + \omega$.
- For $i = 8$, $\phi_8(x) = \phi_2(x) = x^3 + \omega x^2 + 1$.
- For $i = 9$,

$$\begin{aligned}\phi_9(x) &= (x - \beta^9)(x - \beta^{18})(x - \beta^{15}) \\ &= x^3 + (\beta^9 + \beta^{15} + \beta^{18})x^2 + (\beta^3 + \beta^6 + \beta^{12})x + \beta^{21} \\ &= x^3 + x^2 + 1.\end{aligned}$$

- For $i = 10$,

$$\begin{aligned}\phi_{10}(x) &= (x - \beta^{10})(x - \beta^{13})(x - \beta^{19}) \\ &= x^3 + (\beta^{10} + \beta^{13} + \beta^{19})x^2 + (\beta^2 + \beta^8 + \beta^{11})x + \beta^{21} \\ &= x^3 + \omega x + 1.\end{aligned}$$

- For $i = 11$, $\phi_{11}(x) = \phi_2(x) = x^3 + \omega x^2 + 1$.
- For $i = 12$, $\phi_{12}(x) = \phi_3(x) = x^3 + x + 1$.
- For $i = 13$, $\phi_{13}(x) = \phi_{10}(x) = x^3 + \omega x + 1$.
- For $i = 14$, $\phi_{14}(x) = (x - \beta^{14}) = x + \omega$.
- For $i = 15$, $\phi_{15}(x) = \phi_9(x) = x^3 + x^2 + 1$.
- For $i = 16$, $\phi_{16}(x) = \phi_1(x) = x^3 + (1 + \omega)x^2 + 1$.
- For $i = 17$, $\phi_{17}(x) = \phi_5(x) = x^3 + (1 + \omega)x + 1$.
- For $i = 18$, $\phi_{18}(x) = \phi_9(x) = x^3 + x^2 + 1$.

Now the generator polynomial is

$$\begin{aligned}G(x) &= \phi_1(x) \cdot \phi_2(x) \cdot \phi_3(x) \cdot \phi_5(x) \cdot \phi_7(x) \cdot \phi_9(x) \cdot \phi_{10}(x) \cdot \phi_{14}(x) \\ &= (x^{19} + (1 + \omega)x^{18} + x^{16} + (1 + \omega)x^{15} + (1 + \omega)x^{14} + (1 + \omega)x^{13} + x^8 \\ &\quad + \omega x^7 + (1 + \omega)x^6 + x^5 + (1 + \omega)x^4 + x^2 + \omega x + 1 + \omega)(\omega + x) \\ &= x^{20} + x^{18} + x^{17} + x^{16} + \omega x^{15} + \omega x^{14} + x^{13} + x^9 + x^5 + x^4 + x^3 + 1.\end{aligned}$$

Thus, the dimension of the code is

$$k = 21 - 20 = 1.$$

Case 10: For $n = 21$ and $d = 21$, $i = 1, 2, 3, \ldots, 20$.

- For $i = 1$,
  Let $\beta \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β, β^4, and β^{16} have the minimal polynomial

  $$\varphi_1(x) = (x-\beta)(x-\beta^4)(x-\beta^{16}) = x^3+(\beta+\beta^4+\beta^{16})x^2+(\beta^5+\beta^{17}+\beta^{20})x+\beta^{21} = x^3+(1+\omega)x^2+1.$$

- For $i = 2$,
  Let $\beta^2 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\varphi_2(x) = (x-\beta^2)(x-\beta^8)(x-\beta^{11}) = x^3+\omega x^2+1.$$

- For $i = 3$,
  Let $\beta^3 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^3, β^6, and β^{12} have the minimal polynomial

  $$\varphi_3(x) = (x-\beta^3)(x-\beta^6)(x-\beta^{12}) = x^3+x+1.$$

- For $i = 4$,
  Let $\beta^4 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^2, β^8, and β^{11} have the minimal polynomial

  $$\varphi_4(x) = \varphi_2(x) = x^3+\omega x^2+1.$$

- For $i = 5$,
  Let $\beta^5 \in \mathbb{Z}_2[\omega]^3$, then by Theorem 3.1, β^5, β^{17}, and β^{20} have the minimal polynomial

  $$\varphi_5(x) = (x-\beta^5)(x-\beta^{17})(x-\beta^{20}) = x^3+(1+\omega)x+1.$$

- For $i = 6$,
  Let $\beta^6 \in \mathbb{Z}_2[\omega]^3$, then $\varphi_6(x) = \varphi_3(x) = x^3+x+1$.

- For $i = 7$,
  Let $\beta^7 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_7(x) = x+1+\omega.$$

- For $i = 8$,
  Let $\beta^8 \in \mathbb{Z}_2[\omega]^3$, then $\varphi_8(x) = \varphi_2(x) = x^3+\omega x^2+1$.

- For $i = 9$,
  Let $\beta^9 \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_9(x) = x^3+x^2+1.$$

- For $i = 10$,
  Let $\beta^{10} \in \mathbb{Z}_2[\omega]^3$, then

  $$\varphi_{10}(x) = x^3+\omega x+1.$$

- For $i = 11$,
  Let $\beta^{11} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{11}(x) = \varphi_2(x) = x^3+\omega x^2+1$.

- For $i = 12$,
  Let $\beta^{12} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{12}(x) = \varphi_3(x) = x^3 + x + 1$.
- For $i = 13$,
  Let $\beta^{13} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{13}(x) = \varphi_{10}(x) = x^3 + \omega x + 1$.
- For $i = 14$,
  Let $\beta^{14} \in \mathbb{Z}_2[\omega]^3$, then
  $$\varphi_{14}(x) = x + \omega.$$
- For $i = 15$,
  Let $\beta^{15} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{15}(x) = \varphi_9(x) = x^3 + x^2 + 1$.
- For $i = 16$,
  Let $\beta^{16} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{16}(x) = \varphi_1(x) = x^3 + (1 + \omega)x^2 + 1$.
- For $i = 17$,
  Let $\beta^{17} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{17}(x) = \varphi_5(x) = x^3 + (1 + \omega)x + 1$.
- For $i = 18$,
  Let $\beta^{18} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{18}(x) = \varphi_9(x) = x^3 + x^2 + 1$.
- For $i = 19$,
  Let $\beta^{19} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{19}(x) = \varphi_{10}(x) = x^3 + \omega x + 1$.
- For $i = 20$,
  Let $\beta^{20} \in \mathbb{Z}_2[\omega]^3$, then $\varphi_{20}(x) = \varphi_5(x) = x^3 + (1 + \omega)x + 1$.

Now the generator polynomial is

$$G(x) = \phi_1(x) \cdot \phi_2(x) \cdot \phi_3(x) \cdot \phi_5(x) \cdot \phi_7(x) \cdot \phi_9(x) \cdot \phi_{10}(x) \cdot \phi_{14}(x)$$

$$= x^{20} + x^{18} + x^{17} + x^{16} + \omega x^{15} + \omega x^{14} + x^{13} + x^9 + x^5 + x^4 + x^3 + 1.$$

Now, $k = 21 - 20 = 1$. So the parameters of the shortened BCH code are $(n, k, d) = (21, 1, 21)$.

4. 4. Decoding Algorithm for Shortened BCH Codes over the Eisenstein Fields

This section is based on the procedure of decoding Shortened BCH codes over Eisenstein fields of length n, using a modified Berlekamp–Massey Algorithm (BMA). The procedure follows the same principles as decoding conventional BCH codes.

Theorem 4.1 [6, Theorem 4.2]: Let C be a BCH or Shortened BCH code of length n, defined over the Eisenstein field $\mathbb{Z}_p[\omega]$, with designed distance d. Then, the code C is the null space of the matrix N, where

$$N = \begin{bmatrix} 1 & \beta^{c} & \beta^{2c} & \dots & \beta^{(n-1)c} \\ 1 & \beta^{c+1} & \beta^{2(c+1)} & \dots & \beta^{(n-1)(c+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta^{c+d-2} & \beta^{2(c+d-2)} & \dots & \beta^{(n-1)(c+d-2)} \end{bmatrix}.$$

Here, β is a primitive element in the extension field containing $\mathbb{Z}_p[\omega]$, and the matrix N consists of $d-1$ rows and n columns. The codewords of C are those vectors $v \in \mathbb{Z}_p[\omega]^n$ such that $Nv^T = 0$.

4.1. Algorithm for Decoding of Shortened BCH Codes over the Eisenstein Fields

Assume that $\mathbf{c}$ is a codeword from a narrow-sense Shortened BCH code (n, k, d) over an Eisenstein field, and the received word is $\mathbf{r}$. The designed distance is d. The following steps outline the decoding process using the modified Berlekamp–Massey algorithm (BMA).

Step 1: Syndrome Calculation

Let S_i for $i = c, c+1, \dots, c+d-2$ denote the syndromes computed from the received word $\mathbf{r}$ and the matrix N:

$$S_i = \mathbf{r}N^T \mod p = (S_c, S_{c+1}, \dots, S_{c+d-2}).$$

Alternatively, each syndrome can be computed using:

$$S_i = \mathbf{r}\beta^i = b_0 + b_1\beta^i + \cdots + b_{n-1}\beta^{(n-1)i}, \quad \text{for } i = c, c+1, \dots, c+d-2.$$

If all $S_i = 0$, then $\mathbf{c} = \mathbf{r}$, indicating no error. Otherwise, proceed to the next step.

Step 2: Compute the Error Locator Polynomial $\Delta^n(y)$

Apply the modified BMA to find $\Delta^n(y)$, the error locator polynomial. Let ϑ_n be the discrepancy, and $u_n = \deg(\Delta^n(y))$. The maximum number of correctable errors is t. Table 4 shows the initialization values.

Table 4: Error Correcting Polynomials by Modified BMA

Iterations n	$\Delta^n(y)$	ϑ_n	u_n	$n - u_n$
-1	1	1	0	-1
0	1	First non-zero syndrome	0	0
1				
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$2t$				

Case 1: If $\vartheta_n = 0$, then:

$$\Delta^{n+1}(y) = \Delta^n(y), \quad u_{n+1} = u_n.$$

Case 2: If $\vartheta_n \neq 0$, choose $m \leq n-1$ such that $n - u_m$ is maximal or equal to $n - u_n$. Then, using $\vartheta_n - z\vartheta_m = 0$, solve for z and compute:

$$\Delta^{n+1}(y) = \Delta^n(y) - zy^{n-m}\Delta^m(y),$$

and update the discrepancy as:

$$\vartheta_{n+1} = S_{n+2} + \Delta_1^{(n+1)}(y)S_{n+1} + \Delta_2^{(n+1)}(y)S_n + \cdots + \Delta_{u_{n+1}}^{(n+1)}(y)S_{n+2-u_{n+1}}.$$

Step 3: Find the Reciprocal Function

From $\Delta^n(y)$, compute its reciprocal $g(y)$. Let y_j be the roots of $g(y)$, and suppose $x_j = p^j$ are error positions if $x_j - y_j = 0$, for $1 \leq j \leq n-1$.

Step 4: Symmetric Function

Determine the elementary symmetric function of the error locations:

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

where v is the total number of error locations.

Step 5: Error Magnitudes by Forney's Formula [27]

The magnitude z_i of the error at location y_i is given by:

$$z_i = \frac{\sum_{l=0}^{v-1} \Delta_{(i,l)} S_{v-l}}{\sum_{l=0}^{v-1} \Delta_{(i,l)} y_i^{v-l}},$$

with initialization $\Delta_0 = \Delta_{(i,0)} = 1$, and recurrence:

$$\Delta_{(i,j)} = \Delta_j + x_i \Delta_{(i,j-1)}, \quad j = 1, 2, \ldots, v-1, \ i = 1, 2, \ldots, v.$$

Step 6: Recover the Codeword

Finally, compute the corrected codeword:

$$\mathbf{c} = \mathbf{r} - \mathbf{e},$$

where $\mathbf{e}$ is the error vector.

The pseudocode of this decoding process is given in Algorithm 4.1.

Illustration 4.1: Assume that $[3, 1, 3]$ narrow-sense shortened BCH code over the Eisenstein field $\mathbb{Z}_2[\omega]^2$ and the received vector $r = (1, 1, \omega)$. Determine the corrected codeword (if possible).

Algorithm 2 Decode Shortened BCH Codes over EF

Require: Received word r of length n over $\mathbb{Z}_p[\omega]$, code parameters (n, k, d) with $c = 1$, prime $p \equiv 2 \pmod 3$, field element $\beta \in \mathbb{Z}_p[\omega]^b$
Ensure: Corrected codeword c, Error vector e

Step 1: Compute Syndromes
for $i = c$ to $c + d - 2$ **do**
  $S_i = \sum_{j=0}^{n-1} r_j(\beta^i)^j \bmod p$
end for
if all $S_i = 0$ **then return** $c = r$
elsecontinue
end if
Step 2: Modified Berlekamp–Massey Algorithm
$\Delta^{(-1)}(y) = \Delta^{(0)}(y) = 1$, $u_{-1} = u_0 = 0$, $\vartheta_0 =$ first non-zero S_i
for $n = 1$ to $2t$ **do**
  if $\vartheta_n = 0$ **then**
    $\Delta^{(n+1)} = \Delta^{(n)}$, $u_{n+1} = u_n$
  else
    Find $m \leq n - 1$ maximizing $n - u_m$, solve z from $\vartheta_n - z\vartheta_m = 0$
    $\Delta^{(n+1)} = \Delta^{(n)} - zy^{n-m}\Delta^{(m)}$
    $u_{n+1} = \max(u_n, n - u_m + 1)$
    $\vartheta_{n+1} = S_{n+2} + \sum_{j=1}^{u_{n+1}} \Delta_j^{(n+1)} S_{n+2-j}$
  end if
end for
Step 3: Error Locations
Solve $g(y) = \Delta^{(n)}(y) = 0$ for roots y_j, set $x_j = p^j$ if $x_j - y_j = 0$
Step 4: Symmetric Polynomial
$\Lambda(y) = \prod_{i=1}^{v}(y - x_i) = \sum_{j=0}^{v} \Delta_j y^{v-j}$
Step 5: Forney's Algorithm
$\Delta_0 = \Delta_{i,0} = 1$
for $i = 1$ to v **do**
  for $j = 1$ to $v - 1$ **do**
    $\Delta_{i,j} = \Delta_j + x_i\Delta_{i,j-1}$
  end for
end for
for each y_i **do**
  $z_i = \dfrac{\sum_{l=0}^{v-1} \Delta_{l,j} S_{v-l}}{\sum_{l=0}^{v-1} \Delta_{l,j} y_i^{v-l}}$
end for
Step 6: Correct Errors
Form e using locations x_j and magnitudes z_j, set $c = r - e$
return c, e

As $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$, the number of iterations will be $2t = 2$. Let

$$S = rH^T = (1, 1, \omega) \begin{pmatrix} 1 & 1 \\ \beta & \beta^2 \\ \beta^2 & \beta^4 \end{pmatrix}^T = \begin{pmatrix} 1 \\ \omega \end{pmatrix},$$

where $S_1 = \beta^3$ and $S_2 = \beta$ are the syndromes.

Next, we find $\Delta^2(y)$ using the modified Berlekamp–Massey Algorithm (BMA), summarized in Table 5.

Iteration 1: The initial non-zero syndrome is 1. Applying Case 2 of Step 2 from the modified BMA, since $\vartheta_0 \neq 0$, $-1 \leq -1$, and $0 - u_{-1} = 0$ is the maximum value of the last column, we get

$$\vartheta_0 - z\vartheta_{-1} = 0 \Rightarrow z = \frac{\vartheta_0}{\vartheta_{-1}} = \frac{1}{1} = 1.$$

Table 5: Single Error Locating Polynomials

n	$\Delta^n(y)$	ϑ_n	u_n	$n-u_n$
-1	1	1	0	-1
0	1	1	0	0
1	$1+y$	$1+\omega$	1	0
2	$1+\omega y$			

Thus,

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

Now compute

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

Iteration 2: Since $\vartheta_1 \neq 0$, and $1-u_0 = 1-0 = 1$ is the highest value of the last column, we have:

$$\vartheta_1 - z\vartheta_0 = 0 \Rightarrow z = \frac{\vartheta_1}{\vartheta_0} = \frac{1+\omega}{1} = 1+\omega.$$

Hence,

$$\Delta^2(y) = \Delta^1(y) - (1+\omega)y^{1-0}\Delta^0(y) = 1+\omega y.$$

The reciprocal polynomial is $g(y) = y+\omega$. The root of $g(y)$ is ω, i.e., $y_1 = \omega = \beta^2$, indicating that the error occurred at the second position of r.

The elementary symmetric function (ESF) is given by:

$$\Delta_0 y^v + \Delta_1 = y - \beta^2.$$

Error Magnitude:

$$z_1 = \frac{\Delta_{1,0} S_1}{\Delta_{1,0} y_1} = \frac{\beta^3}{\beta^2} = \beta = 1+\omega.$$

where $\Delta_0 = 1$, $\Delta_1 = \beta^2$, and $v = 1$.

Corrected Codeword:

$$c = r - e = (1,1,\omega) - (0,1+\omega,0) = (1,1,1).$$

Thus, the corrected codeword is $c = (1,1,1)$, which is a valid codeword of the $(3,1,3)$ BCH code.

Illustration 4.2: Assume that $[9,3,3]$ narrow sense shortened BCH code over the Eisenstein field $\mathbb{Z}_2[\omega]^2$ and the received vector $r = (1,0,\omega,1,0,0,1,0,0)$, determine the corrected code word (if possible).

As $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$. So, the number of iterations will also be $2t = 2$. Let

$$S = rH^T = (1,0,\omega,1,0,0,1,0,0) \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^8 \\ 1 & \beta^2 & \beta^4 & \cdots & \beta^{16} \end{pmatrix}^T = \begin{pmatrix} \beta^8 \\ \beta \end{pmatrix},$$

Table 6: Error Locating Polynomials

n	$\Delta^n(y)$	ϑ_n	u_n	$n-u_n$
-1	1	1	0	-1
0	1	β^8	0	0
1	$1+\beta^8 y$	β^4	1	0
2	$1+\omega y$			

where $S_1 = \beta^8$ and $S_2 = \beta$ are the syndromes. Next, we will find $\Delta^2(y)$ (see Table 2) by applying the modified BMA shown in Table 6.

Iteration 1: The initial non-zero syndrome is β^8. We apply Case 2 of Step 2 from the modified BMA as $\vartheta_0 \neq 0$, $-1 \leq -1$, and $0 - u_{-1} = 0$ is the extreme value of the end column. Then,

$$\vartheta_0 - z\vartheta_{-1} = 0 \Rightarrow z = \frac{\vartheta_0}{\vartheta_{-1}} = \frac{\beta^8}{1} = \beta^8.$$

So, the polynomial:

$$\Delta^1(y) = \Delta^0(y) - \beta^8 y^{0+1}\Delta^{-1}(y) = 1 + \beta^8 y.$$

$$\vartheta_1 = S_2 + \Delta_1^1(y)S_1 = \beta + \beta^8 \cdot \beta^8 = \beta + \beta^7 = \beta^4.$$

Iteration 2: Let $\vartheta_1 \neq 0$ in iteration one, $0 = 1 - 1$, and $1 - u_0 = 1 - 0 = 1$ is the highest value of the last column. Thus,

$$\vartheta_1 - z\vartheta_0 = 0 \Rightarrow z = \frac{\vartheta_1}{\vartheta_0} = \frac{\beta^4}{\beta^8} = \beta^5.$$

So, the polynomial:

$$\Delta^2(y) = \Delta^1(y) - \beta^5 y^{1-0}\Delta^0(y) = 1 + (\beta^5 + \beta^8)y = 1 + \beta^2 y.$$

Now, the reciprocal function of $\Delta^2(y) = 1 + \beta^2 y$ is $g(y) = y + \beta^2$. So β^2 is the only root of $g(y)$. Hence $y_1 = \beta^2$, and the error takes place in the third position of r.

$\Delta_0 y^v + \Delta_1 = y - \beta^2$ is an error-locator polynomial (ESF). The error magnitude is:

$$z_1 = \frac{\Delta_{1,0}S_1}{\Delta_{1,0}y_1} = \frac{\beta^8}{\beta^2} = \beta^6 = \omega,$$

where $\Delta_0 = 1$, $\Delta_1 = \beta^2$, and $v = 1$.

The revised code word is:

$$c = r - e = (1, 0, \omega, 1, 0, 0, 1, 0, 0) - (0, 0, \omega, 0, 0, 0, 0, 0, 0) = (1, 0, 0, 1, 0, 0, 1, 0, 0).$$

Thus, c is the corrected narrow sense shortened $(9, 3, 3)$ BCH code.

5. The Importance of Shortened Codes over EF in Modern-Day Transmission

Being able to code and decode shortened BCH codes within the Eisenstein field $\mathbb{Z}_p[\omega]$, where $p \equiv 2 \pmod 3$, is highly beneficial in modern data transmission systems. Defining codes over $\mathbb{Z}_p[\omega]$ provides the codes with symmetry and enables shorter distances due to the identity $\omega^3 = 1$. When $p \equiv 2 \pmod 3$ is selected, the corresponding polynomial becomes irreducible in $\mathbb{Z}_p[\omega]$, thereby preserving the field extension and making the construction of codes using Eisenstein arithmetic more convenient. Depending on the required block length and level of error correction, shortened BCH codes can be designed in this setting. These codes are particularly suitable for applications such as Internet of Things (IoT) devices, satellite communication, and mobile networks where strict power and bandwidth limitations exist. The anti-noise efficiency of these codes is enhanced owing to dense encoding schemes and improved distances measured via both Euclidean and Eisenstein weights. In this context, coding algorithms, especially those based on syndrome decoding and the Berlekamp–Massey algorithm, exploit the algebraic structure of the field to efficiently correct errors. Overall, utilizing BCH codes over $\mathbb{Z}_p[\omega]$ presents a promising approach to enhancing the robustness and reliability of modern digital communication infrastructures.

6. Comparative Analysis

In this section, we compare the performance of narrow-sense shortened BCH codes over the finite field $\mathrm{GF}(p^m)$ and the Eisenstein field $\mathbb{Z}_p[\omega]^{m/2}$, where $p \equiv 2 \pmod 3$. The comparison is made by identifying key parameters, including the code length (n), minimum distance (d), code dimension (k), number of codewords ($|C|$), and code rate (R). The analysis draws on prior research findings, particularly [6] and Sections 3 and 4 of this article. We provide a comparison based on the finite field $\mathrm{GF}(2^6)$ and the Eisenstein field $\mathbb{Z}_2[\omega]^3$, as represented in Tables 7 and 8.

From Tables 7 and 8, both $\mathrm{GF}(2^6)$ and $\mathbb{Z}_2[\omega]^3$ yield shortened BCH codes with comparable lengths and distances. The comparative outcomes are summarized below:

Dimension: The dimensions of codes over $\mathbb{Z}_2[\omega]^3$ often match or surpass their $\mathrm{GF}(2^6)$ counterparts. For instance, for $n = 21$, both fields provide $k = 15$ at $d = 3$, indicating equivalent capacity. However, $\mathbb{Z}_2[\omega]^3$ offers greater dimensions at higher distances, indicating better payload accommodation.

Number of Codewords: Due to the quadratic growth in the symbol set, codes over $\mathbb{Z}_2[\omega]^3$ provide significantly more codewords for the same dimension k. For example, at $n = 21$ and $d = 3$, we obtain $|C| = 1073741824$ for $\mathbb{Z}_2[\omega]^3$, compared to only $|C| = 32768$ in $\mathrm{GF}(2^6)$. This suggests an advantage in applications requiring high codeword dispersion.

Code Rate: The code rate is equivalent in some cases. For $n = 21$ and $d = 3$, both fields yield $R = 0.7143$. Yet, for other configurations, $\mathbb{Z}_2[\omega]^3$ offers better performance,

Table 7: Analysis of Shortened BCH Codes over the Galois Field $\mathrm{GF}(2^6)$

n	d	k	$\lvert C\rvert = 2^k$	$R = k/n$
3	3	1	2	0.3333
7	3	4	16	0.5714
	5	1	2	0.1429
	7	1	2	0.1429
9	3	3	8	0.3333
	5	1	2	0.1111
	7	1	2	0.1111
	9	1	2	0.1111
21	3	15	32768	0.7143
	5	12	4096	0.5714
	7	6	64	0.2857
	9	4	16	0.1905
	11	1	2	0.0476
	13	NA	NA	NA
	15	NA	NA	NA
	17	NA	NA	NA
	19	NA	NA	NA
	21	NA	NA	NA

such as $R = 0.3900$ at $n = 21$, $d = 9$, compared to $R = 0.2857$ in $\mathrm{GF}(2^6)$.

In summary, the higher codeword diversity and greater dimensions offered by $\mathbb{Z}_p[\omega]^{m/2}$, where $p \equiv 2 \pmod 3$, make it particularly suitable for applications demanding robust error correction. These benefits come at the cost of potentially lower data rates. Furthermore, the demonstrated higher-order minimum distances in the Eisenstein field indicate enhanced error resilience, positioning such codes well for next-generation communication systems and storage solutions requiring high reliability and minimal redundancy.

7. Conclusion and Future Directions

This article proposed a new approach in shortened BCH codes over the Eisenstein fields and established its improved error correction performance through modified BMA. Due to the natural extension of Gaussian fields, the algebraic characteristics of Eisenstein fields turn out to be suitable for the development of efficient codes where high reliability and low latency are desired in noisy channels. Many of the changes that have been proposed for the BMA strongly contribute to the growth of the decoding efficiency by taking into account the computational concerns of using Eisenstein field arithmetic. Therefore, this study adds value to the development of the coding theory by bringing conceptuality in theory and idea in application in order to accommodate future issues with respect to reliable data transmission. Efficient implementations of the proposed codes and decoding algorithms in communication structures are possible if the suggested structures are used. The extension

Table 8: Analysis of Shortened BCH Codes over the Eisenstein Field $\mathbb{Z}_2[\omega]^3$

n	d	k	$\lvert C\rvert = 2^{2k}$	$R = k/n$
3	3	1	4	0.3333
7	3	1	4	0.1429
	5	2	16	0.2857
	7	1	4	0.1429
9	3	1	4	0.1111
	5	2	16	0.2222
	7	1	4	0.1111
	9	1	4	0.1111
21	3	15	1073741824	0.7143
	5	12	16777216	0.5714
	7	9	262144	0.4286
	9	8	65536	0.3900
	11	2	16	0.0952
	13	1	2	0.0476
	15	1	2	0.0476
	17	1	2	0.0476
	19	1	2	0.0476
	21	1	2	0.0476

of these methods into multidimensional and spatially coupled codes holds great potential to be useful in new fields such as storage systems and sensor networks. Likely expanding the areas of application in QEC and in the further advancement of next-generation wireless networks, such as 6G, the techniques based on the Eisenstein field-based codes can bring added value to the transformative technologies.

Acknowledgements

This research is supported by the Ongoing Research Funding program - Research Chairs (ORF-RC-2025-5300), King Saud University, Riyadh, Saudi Arabia.

Tribute

We wish to express our heartfelt gratitude to our beloved supervisor, Professor Dr. Tariq Shah (late), whose exceptional guidance, profound knowledge, and unwavering support profoundly shaped our journey as researchers in algebra, number theory, coding theory, and cryptography. His mentorship was a cornerstone of our academic and personal growth, and his presence continues to inspire our scholarly endeavours. May his soul rest in eternal peace.

Data availability

All the data given in this article.

References

[1] Gilberto Bini and Fabio Flamini. *Finite commutative rings and their applications*, volume 680. Springer Science & Business Media, 2012.

[2] Robert Gilmer. *Commutative semigroup rings*. University of Chicago Press, 1984.

[3] Anthony W Knapp. *Basic real analysis*. Springer Science & Business Media, 2007.

[4] Sanjay R Nagpaul. *Topics in applied abstract algebra*, volume 15. American Mathematical Society, 2005.

[5] Tariq Shah, Sobia Farwa, and Rana S Badar. A generalization of integral dependence. *Advances in Algebra*, 3(1):43–55, 2010.

[6] Claude E Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948.

[7] Hsien T Hsu. A class of binary shortened cyclic codes for a compound channel. *Information and Control*, 18(2):126–139, 1971.

[8] Tadao Kasami. Optimum shortened cyclic codes for burst-error correction. *IEEE Transactions on Information Theory*, 9(2):105–109, 1963.

[9] H Helgert and R Stinaff. Shortened bch codes (corresp.). *IEEE Transactions on Information Theory*, 19(6):818–820, 1973.

[10] Cunsheng Ding, Jinyuan Luo, and Harald Niederreiter. Two-weight codes punctured from irreducible cyclic codes. In *Coding and Cryptology*, pages 119–124, 2008.

[11] Cunsheng Ding and Harald Niederreiter. Cyclotomic linear codes of order 3. *IEEE Transactions on Information Theory*, 53(6):2274–2277, 2007.

[12] Tariq Shah, Asif Khan, and Aline A Andrade. Encoding through generalized polynomial codes. *Computational & Applied Mathematics*, 30:349–366, 2011.

[13] Tariq Shah, Awais Qamar, and Aline A De Andrade. Constructions and decoding of a sequence of bch codes, 2012. Unpublished manuscript.

[14] Cunsheng Ding. Linear codes from some 2-designs. *IEEE Transactions on Information Theory*, 61(6):3265–3275, 2015.

[15] Jay L Goldwasser. Shortened and punctured codes and the macwilliams identities. *Linear Algebra and its Applications*, 253(1-3):1–13, 1997.

[16] Arpita Yardi and Ruud Pellikaan. On shortened and punctured cyclic codes. *arXiv preprint arXiv:1705.09859*, 2017.

[17] Klaus Huber. Codes over eisenstein-jacobi integers. *Contemporary Mathematics*, 168:165–165, 1994.

[18] Mohammed M Hazzazi, Muhammad Sajjad, Ziad Bassfar, Tariq Shah, and Abdullah Albakri. Nonlinear components of a block cipher over eisenstein integers. *CMC-Computers Materials & Continua*, 77(3):3659–3675, 2023.

[19] Muhammad Sajjad, Tariq Shah, Mohammed Alammari, and Hatem Alsaud. Construction and decoding of bch-codes over the gaussian field. *IEEE Access*, 2023.

[20] Cunsheng Ding. Designs from linear codes, 2022. Manuscript.
[21] Shu Lin. Shortened finite geometry codes (corresp.). *IEEE Transactions on Information Theory*, 18(5):692–696, 1972.
[22] Cunsheng Ding and Chengju Li. Infinite families of 2-designs and 3-designs from linear codes. *Discrete Mathematics*, 340(10):2415–2431, 2017.
[23] Florence Jessie MacWilliams. *The theory of error-correcting codes*, volume 2. Elsevier, 1977.
[24] Muhammad Sajjad, Tariq Shah, Muhammad Abbas, Mohammed Alammari, and Julian Serna. The impact of alternant codes over eisenstein integers on modern technology. *Computational and Applied Mathematics*, 44(1):95, 2025.
[25] W Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.
[26] Muhammad Sajjad, Tariq Shah, Qiong Xin, and Bader Almutairi. Eisenstein field bch codes construction and decoding. *AIMS Mathematics*, 8(12):29453–29473, 2023.
[27] G David Forney. On decoding bch codes. *IEEE Transactions on Information Theory*, 11(4):549–557, 1965.