AIMS Mathematics, 11(1): 353–365.
DOI: 10.3934/math.2026015
Received: 08 August 2025
Revised: 22 November 2025
Accepted: 12 December 2025
Published: 05 January 2026

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

Research article

Noncyclic BCH and Srivastava codes over Eisenstein integers toward next-generation error-correcting codes

Muhammad Sajjad[1,*] **and Nawaf A. Alqwaifly**[2,*]

[1] NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad, 44000, Pakistan

[2] Department of Electrical Engineering, College of Engineering, Qassim University, Buraydah, Saudi Arabia

* **Correspondence:** Email: nkoiefly@qu.edu.sa, muhammad.sajjad@nutech.edu.pk; Tel: +923067759056.

Abstract: This article investigates noncyclic BCH and Srivastava codes over Eisenstein integer fields $\mathbb{Z}_p[\omega]$, where $p \equiv 2 \pmod 3$. By leveraging the algebraic structure of Eisenstein fields, we construct parity-check matrices with an alternant structure such that all maximal-order determinants satisfy the required algebraic conditions. These constructions provide explicit lower bounds on the minimum distance and enhance the error-correcting performance of the codes. The study further generalizes noncyclic forms of BCH and Srivastava codes, enabling higher code rates and larger minimum distances than their cyclic counterparts. Numerical examples illustrate the feasibility and effectiveness of the proposed constructions for reliable data transmission.

Keywords: Eisenstein integer codes; alternant codes; noncyclic BCH codes; Srivastava codes; minimum distance; signal processing; cryptography; wireless communications
Mathematics Subject Classification: 11T71, 68P30, 94A24, 97G70

1. Introduction

Error-correcting codes are fundamental in modern communication and data storage systems, enabling reliable data transmission in the presence of noise. Among widely studied codes, BCH codes, introduced by Bose and Ray-Chaudhuri [1], are notable for their algebraic structure and efficient error-correcting capabilities. Despite their widespread use, cyclic BCH codes face limitations in certain applications, motivating the study of noncyclic generalizations such as those proposed by Helgert [2].

Noncyclic codes provide greater flexibility in code design and can be adapted to various algebraic structures. In this work, we extend noncyclic BCH and Srivastava codes to Eisenstein integer fields

$\mathbb{Z}_p[\omega]$ with $p \equiv 2 \pmod 3$. These fields possess specific algebraic and geometric properties that enable the construction of parity-check matrices with alternant structures. By ensuring the non-singularity of coefficient matrices, we establish lower bounds for the minimum distance and characterize the error-correcting capability of the resulting codes.

Previous studies have investigated error-correcting codes over alternative algebraic structures. Spiegel [3, 4] examined codes over $\mathbb{Z}_m$, Berlekamp [5] provided efficient decoding methods for BCH codes, and Muir and Metzler [6] explored determinant-based approaches in coding theory. More recent work includes Sajjad et al. [7–9], who examined codes over quaternion, Gaussian, and Eisenstein integers, and investigated extensions to noncyclic constructions.

Several contemporary studies focus on code properties and applications, including hulls of BCH codes [10, 11], negacyclic codes [12], and multi-orbit cyclic subspace codes [13]. These developments demonstrate the relevance of exploring noncyclic and generalized code structures for practical applications in high-reliability systems, quantum communication, IoT networks, and cloud storage.

The present study systematically constructs noncyclic BCH and Srivastava codes over Eisenstein fields. By employing alternant parity-check matrices, we derive explicit lower bounds on the minimum distance and illustrate how noncyclic extensions can enhance code parameters, including code rate and error-correcting capability. Numerical examples validate the theoretical constructions and highlight the potential of these codes in modern communication and data-storage systems.

2. Eisenstein fields and their extensions

Let p be a prime such that $p \equiv 2 \pmod 3$. Throughout this paper, the symbol ω denotes the primitive cubic root of unity satisfying

$$\omega^2 + \omega + 1 = 0, \qquad \omega \neq 1.$$

In this setting, the Eisenstein ring over the finite field $\mathbb{Z}_p$ is defined as

$$\mathbb{Z}_p[\omega] = \{\, a + b\omega : a, b \in \mathbb{Z}_p \,\}.$$

Since the polynomial $x^2 + x + 1$ is irreducible over $\mathbb{Z}_p$ whenever $p \equiv 2 \pmod 3$, the ring $\mathbb{Z}_p[\omega]$ becomes a finite field of order p^2. This field serves as the fundamental algebraic structure for constructing noncyclic BCH codes and Srivastava codes over Eisenstein integers.

To obtain higher-order extensions, let $h(x)$ be a monic irreducible polynomial of degree m over $\mathbb{Z}_p[\omega][x]$. Then the quotient ring

$$\mathbb{Z}_p[\omega]^m = \mathbb{Z}_p[\omega][x]/\langle h(x)\rangle$$

defines a field extension of degree m over $\mathbb{Z}_p[\omega]$, and consequently a field of size p^{2m}.

Let

$$\gamma = x + \langle h(x)\rangle$$

denote the residue class of x in the quotient field. By construction, γ satisfies

$$h(\gamma) = 0.$$

Every element of the extension field $\mathbb{Z}_p[\omega]^m$ admits a unique representation of the form

$$a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{m-1}\gamma^{m-1}, \qquad a_i \in \mathbb{Z}_p[\omega].$$

Thus, $\mathbb{Z}_p[\omega]^m$ forms a well-defined Eisenstein field extension, with γ serving as the algebraic root of the defining polynomial $h(x)$. These fields will be used in constructing and analyzing next-generation noncyclic BCH and Srivastava codes.

Example 2.1. *Following [9, 14], consider the smallest Eisenstein field*

$$\mathbb{Z}_2[\omega] = \{0, 1, \omega, 1 + \omega\},$$

where ω *satisfies* $\omega^2 + \omega + 1 = 0$ *in characteristic* 2.

Let

$$h(x) = x^2 + \omega x + \omega$$

which is irreducible over $\mathbb{Z}_2[\omega]$. *The degree-2 Eisenstein extension is*

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

If $\rho \in \mathbb{Z}_2[\omega]^2$ *denotes the coset of x, then* ρ *satisfies*

$$\rho^2 + \omega\rho + \omega = 0.$$

Using this relation, all powers of ρ *generate a cyclic multiplicative group of order* 15. *Table 1 lists the cyclic structure.*

Table 1. Cyclic group of Eisenstein integers of order 15.

Serial No.	ρ^k	Serial No.	ρ^k
1	ρ	9	$\omega + 1 + \rho\omega$
2	$\rho\omega + \omega$	10	$1 + \omega$
3	$\rho + \omega + 1$	11	$\rho + \rho\omega$
4	$\rho + \omega$	12	$1 + \rho$
5	ω	13	$\omega + \rho(1 + \omega)$
6	$\rho\omega$	14	$1 + \rho + \rho\omega$
7	$\rho(1 + \omega) + 1 + \omega$	15	1
8	$\rho\omega + 1$		

3. Alternants and Cauchy-type determinants over Eisenstein field extensions

In this section, we review classical results concerning alternants and Cauchy-type determinants over the Eisenstein field extension $\mathbb{Z}_p[\omega]^m$, where $p \equiv 2 \pmod 3$ and $m \geq 1$. These results illustrate standard determinant properties in the context of Eisenstein fields, without introducing new structural features of the field itself.

3.1. Alternant determinants

An alternant of order s is defined as the determinant

$$\Delta_s = \begin{vmatrix} f_0(x_0) & f_0(x_1) & \cdots & f_0(x_{s-1}) \\ f_1(x_0) & f_1(x_1) & \cdots & f_1(x_{s-1}) \\ \vdots & \vdots & \ddots & \vdots \\ f_{s-1}(x_0) & f_{s-1}(x_1) & \cdots & f_{s-1}(x_{s-1}) \end{vmatrix},$$

where $x_0, x_1, \ldots, x_{s-1} \in \mathbb{Z}_p[\omega]^m$ and $f_k(x)$ are polynomials over $\mathbb{Z}_p[\omega]$.

A key property of alternants is that $\Delta_s = 0$ whenever $x_i = x_j$ for some $i \neq j$. Consequently, Δ_s contains as a factor the product of pairwise differences

$$\phi(x_0, x_1, \ldots, x_{s-1}) = \prod_{0 \le i < j \le s-1} (x_i - x_j),$$

and the quotient Δ_s/ϕ is a symmetric function of the variables.

If the polynomials are chosen as

$$f_j(x) = a_{0,j} + a_{1,j}x + \cdots + a_{s-1,j}x^{s-1}, \quad a_{l,j} \in \mathbb{Z}_p[\omega],$$

then

$$\Delta_s = \phi(x_0, \ldots, x_{s-1}) \det(A),$$

where $A = (a_{i,j})_{0 \le i,j \le s-1}$ is the coefficient matrix. In particular, if A is the identity, Δ_s reduces to the classical Vandermonde determinant.

3.2. Double alternants and Cauchy determinants

A double alternant is a determinant formed from two-variable functions and is divisible by the product of differences in each variable set. For the Eisenstein extension $\mathbb{Z}_p[\omega]^m$, let

$$\Delta_D = \begin{vmatrix} \frac{1}{\prod_{k=1}^{r}(x_1 - y_{1k})} & \cdots & \frac{1}{\prod_{k=1}^{r}(x_l - y_{1k})} \\ \vdots & \ddots & \vdots \\ \frac{1}{\prod_{k=1}^{r}(x_1 - y_{sk})} & \cdots & \frac{1}{\prod_{k=1}^{r}(x_l - y_{sk})} \end{vmatrix}, \quad l = sr,$$

where $y_{ij} \neq y_{ik}$ for $j \neq k$ and all entries belong to $\mathbb{Z}_p[\omega]^m$.

By performing elementary row operations, Δ_D can be transformed into the classical Cauchy determinant

$$\Delta_C = \begin{vmatrix} \frac{1}{x_1 - y_{11}} & \cdots & \frac{1}{x_l - y_{11}} \\ \vdots & \ddots & \vdots \\ \frac{1}{x_1 - y_{sr}} & \cdots & \frac{1}{x_l - y_{sr}} \end{vmatrix},$$

whose closed-form expression is

$$\Delta_C = \frac{(-1)^{\binom{l}{2}} \phi(x_1, \ldots, x_l) \prod_{i=1}^{s} \phi(y_{i1}, \ldots, y_{ir})}{\prod_{j=1}^{l} u(x_j)},$$

where $u(x_j) = \prod_{i=1}^{s} \prod_{k=1}^{r} (x_j - y_{ik})$.

It follows that $\Delta_D \neq 0$ whenever all x_j are distinct from all y_{ik} and all y_{ik} in a fixed row are mutually distinct. This recovers the classical property of Cauchy determinants, now expressed over the Eisenstein field extension.

4. Noncyclic BCH and Srivastava codes over Eisenstein fields

We can now look at a matrix with this structure:

$$H = \begin{pmatrix} y_0h_0(x_0) & y_1h_0(x_1) & \cdots & y_{n-1}h_0(x_{n-1}) \\ y_0h_1(x_0) & y_1h_1(x_1) & \cdots & y_{n-1}h_1(x_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ y_0h_{s-1}(x_0) & y_1h_{s-1}(x_1) & \cdots & y_{n-1}h_{s-1}(x_{n-1}) \end{pmatrix}, \tag{4.1}$$

when $n \geq s$, the y's can be any nonzero elements (which may coincide) belonging to the set $\mathbb{Z}_p[\omega]^m$. The x's need to be different components of $\mathbb{Z}_p[\omega]^m$. The degree of the polynomial

$$h_{i'}(x) = c_{0,i'} + c_{1,i'}x + c_{2,i'}x^2 + \cdots + c_{s-1,i'}x^{s-1} \leq s-1,$$

and its coefficients are from $\mathbb{Z}_p[\omega]$. This holds for $i' = 0, 1, 2, \ldots, s-1$.

When extending H in $\mathbb{Z}_p[\omega]^m$, each row is replaced with m elements belonging to $\mathbb{Z}_p[\omega]^m$. Consequently, H has ms rows and n columns over this field.

Let $n-k$ be the number of linearly independent rows in $\mathbb{Z}_p[\omega]$. If $n > n-k$, then H is the parity-check matrix of a linear (n,k) code. The subsequent theorem provides a lower bound on the minimum distance of this code.

Theorem 4.1. *If the rank of matrix H in the Eisenstein field $\mathbb{Z}_p[\omega]$, over all the row complexity vectors, is less than the number of columns, then the matrix H in Eq (4.1) defines a linear code of minimum distance d that is at least greater than twice the number of these columns if and only if the coefficient matrix C is invertible, where*

$$C = \begin{pmatrix} c_{0,0} & c_{1,0} & \cdots & c_{s-1,0} \\ c_{0,1} & c_{1,1} & \cdots & c_{s-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{0,s-1} & c_{1,s-1} & \cdots & c_{s-1,s-1} \end{pmatrix}.$$

Proof. Select any $2s$-order determinant from H and subtract the y-term from each of the columns. The outcome is a single alternate which, as the authors mentioned in the preceding section, is non-zero only if C is invertible. In the second case, the columns of H contain $2s$ linearly independent vectors, and the code must then have Hamming distance at least twice the number of such columns. □

Example 4.1. *Let $n = 14$ and $s = 2$. We select the polynomials*

$$h_0(x) = (1+\omega) + \omega x \quad \textit{and} \quad h_1(x) = \omega + \omega x,$$

with coefficients from $\mathbb{Z}_2[\omega]$.

If we define $y_{i'} = \omega$ and $x_{i'} = \rho^{1+i'}$, where ρ is a primitive element of $\mathbb{Z}_2[\omega]^2$ and a root of the irreducible polynomial $f(x) = x^2 + \omega x + \omega$, then the matrix H can be expressed by using Table 1 in the form

$$H = \begin{pmatrix} \omega h_0(\rho) & \omega h_0(\rho^2) & \omega h_0(\rho^3) & \omega h_0(\rho^4) & \cdots & \omega h_0(\rho^{14}) \\ \omega h_1(\rho) & \omega h_1(\rho^2) & \omega h_1(\rho^3) & \omega h_1(\rho^4) & \cdots & \omega h_1(\rho^{14}) \end{pmatrix}$$

$$= \begin{pmatrix} 1+(\omega+1)\rho & \rho & 1+(\omega+1)\rho^3 & (\omega+1)\rho^4 & \cdots & \omega+\omega\rho^{14} \\ (1+\omega)+(\omega+1)\rho & \omega+\rho & 1+(\omega+1)\rho^3 & \omega+(\omega+1)\rho^4 & \cdots & \omega\rho^{14} \end{pmatrix}.$$

Converting the above into $\mathbb{Z}_2[\omega]$, we get:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & \cdots & \omega \\ 1+\omega & 1 & 1+\omega & 1+\omega & \cdots & \omega \\ 1+\omega & \omega & 1 & \omega & \cdots & 0 \\ 1+\omega & 1 & 1+\omega & 1+\omega & \cdots & \omega \end{pmatrix}.$$

It is confirmed that the second and fourth rows are linearly dependent. Therefore, the difference between n and k is 3, and H is the check matrix of the linear code $(14, 11)$.

The coefficient matrix C is:

$$C = \begin{pmatrix} 1 & 0 & 1 \\ 1+\omega & 1 & 1+\omega \\ 1+\omega & \omega & 1 \end{pmatrix}.$$

We know that the determinant of C is $\det(C) = \omega \neq 0$. Therefore, C is invertible.

The proof of the required minimum distance d of the code being at least 3 has already been established in Theorem 4.1. In addition, a simple computation confirms that $d = 3$. Moreover, Theorem 4.1 presents this as the minimal possible value for the error.

The codes defined by Eq (4.1) are of the BCH type over the extension of Eisenstein fields $\mathbb{Z}_p[\omega]$, where the prime $p \equiv 2 \pmod 3$. The set of such codes is determined using a parity-check matrix of the form:

$$H = \begin{pmatrix} 1 & (\rho^c)^1 & (\rho^c)^2 & \cdots & (\rho^c)^{n-1} \\ 1 & (\rho^{c+a})^1 & (\rho^{c+a})^2 & \cdots & (\rho^{c+a})^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (\rho^{c+(s-1)a})^1 & (\rho^{c+(s-1)a})^2 & \cdots & (\rho^{c+(s-1)a})^{n-1} \end{pmatrix}.$$

Here, $\rho \in \mathbb{Z}_p[\omega]$ is a non-zero element of multiplicative order n, and $s, c \in \mathbb{Z}$ are integers such that $\gcd(s, n) = 1$.

As defined earlier, we have:

$$y_{i'} = (\rho^c)^{i'}, \quad x_{i'} = (\rho^a)^{i'}, \quad \text{for } i' = 0, 1, 2, \ldots, n-1,$$

and the set of functions:

$$f_j(x) = x^j, \quad \text{for } j = 0, 1, 2, \ldots, s-1.$$

Clearly, all $y_{i'}$ and $x_{i'}$ values are distinct and non-zero. Therefore, the condition in Theorem 4.1 is satisfied, implying that the resulting code has a minimum distance $d \geq 2s$.

Since the $x_{i'}$ values (used in the parity-check matrix H) must all be distinct, the maximum code length n is bounded by p^{2m}. However, under specific conditions, it is possible to increase the code length to $p^{2m} + 1$ without violating the minimum distance constraint.

This can be achieved by adding an appropriate column to H. For instance, suppose the last column of the coefficient matrix C contains just one non-zero entry $a_{s-1,i}$, and the determinant of the submatrix formed using this value is non-zero. Then, adding a new column to matrix H, with only a non-zero entry in the i-th position, results in a new code that still maintains a minimum distance of at least $2s$.

To validate this statement, one can examine the determinant of a $2s \times 2s$ matrix including this additional column. If the determinant is non-zero, the minimum distance remains $\geq 2s$.

The number of parity-check symbols (i.e., check symbols) in accordance with Eq (4.1) is equal to the number of linearly independent rows of H over $\mathbb{Z}_p[\omega]$, and this number does not exceed $2ms$. However, by selecting specific forms of the functions $f_j(x)$, it may be feasible to increase this upper bound significantly.

Proposition 4.1. *For the Eisenstein field extension $\mathbb{Z}_p[\omega]^m$, where $p \equiv 2 \pmod 3$, any element in a row of the parity-check matrix H can be expressed as the q-th power of an element from another row of H. This implies a potential linear dependency between the elements of this row and other rows of matrix H over $\mathbb{Z}_p[\omega]$.*

Proof. Let $x \in \mathbb{Z}_p[\omega]^m$ be an arbitrary element with $p \equiv 2 \pmod 3$, and let $\rho \in \mathbb{Z}_p[\omega]^m$ be a generating element. Then x can be expressed as:

$$x = u_0 + u_1\rho + u_2\rho^2 + \cdots + u_{m-1}\rho^{m-1}, \quad \text{where } u_i \in \mathbb{Z}_p[\omega].$$

Then, raising x to the $2p$-th power yields:

$$x^{2p} = (u_0 + u_1\rho + u_2\rho^2 + \cdots + u_{m-1}\rho^{m-1})^{2p} = c_0 + c_1\rho + c_2\rho^2 + \cdots + c_{m-1}\rho^{m-1}, \quad c_i \in \mathbb{Z}_p[\omega].$$

Define the following expansion:

$$\rho^{i'p} = A_{i',0} + A_{i',1}\rho + A_{i',2}\rho^2 + \cdots + A_{i',m-1}\rho^{m-1}, \quad \text{for } i' = 0, 1, \ldots, m-1, \quad A_{i',j} \in \mathbb{Z}_p[\omega].$$

Then, the coefficients can be written in matrix form as:

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} A_{0,0} & A_{1,0} & \cdots & A_{m-1,0} \\ A_{0,1} & A_{1,1} & \cdots & A_{m-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{0,m-1} & A_{1,m-1} & \cdots & A_{m-1,m-1} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{m-1} \end{pmatrix}.$$

Therefore, from the coefficients of x, we obtain a linear transformation to the coefficients of x^{2p}, which establishes the lemma. □

Now let us consider the following matrix over $\mathbb{Z}_p[\omega]^m$:

$$H = \begin{pmatrix} x_0h_0(x_0) & x_1h_0(x_1) & \cdots & x_{n-1}h_0(x_{n-1}) \\ x_0h_1(x_0) & x_1h_1(x_1) & \cdots & x_{n-1}h_1(x_{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ x_0h_{2pt-1}(x_0) & x_1h_{2pt-1}(x_1) & \cdots & x_{n-1}h_{2pt-1}(x_{n-1}) \end{pmatrix}, \tag{4.2}$$

where $0 < t \leq \frac{n}{2p}$, and x_i for $i = 1, 2, ..., n-1$ are distinct nonzero elements of $\mathbb{Z}_p[\omega]^m$, and $h_j(x)$ is a polynomial of degree j in x.

We define:

$$h_{lq-1}(x_i) = x_i^{2p-1} \cdot h_{l-1}^{2p}(x_i), \quad \text{for } l = 1, 2, \ldots, t.$$

From Proposition 4.1, we can infer that the $2lp$-th row of H is equal to the $(2p)$-th power of the $(l-1)$-th row, for $l = 1, 2, \ldots, t$.

Furthermore, when factoring out the common powers of x's from a determinant of order $2pt$, we are left with only a single alternant (if any), and the resulting polynomials are of degree at most $2pt - 1$. Additionally, the coefficient matrix C is triangular, with all diagonal entries non-zero. Therefore, the alternant is non-zero.

Hence, if H is the parity-check matrix of a code, it guarantees a minimum distance of at least $2pt+1$. The number of check symbols does not exceed $mt(2p-1)$.

Since all x_i's in Eq (4.2) are distinct and non-zero, the maximum code length n is bounded above by $p^{2(m/2)} - 1$.

Theorem 4.2. *Let $t \geq 1$ be a positive integer, and suppose $n > mt(2p-1)$. Then the matrix H defined in Eq (4.2) serves as the parity-check matrix for a code. For such codes, the minimum distance is at least $2pt + 1$, and the maximum distance is at most $mt(2p-1)$.*

Theorem 4.3. *Let $j = 1, 2, \ldots, s$, $i' = 1, 2, \ldots, n$, and $k = 1, 2, \ldots, r$, and suppose that the elements $z_{i'}, x_{i'}, y_{i'k} \in \mathbb{Z}_p[\omega]^m$, where $p \equiv 2 \pmod 3$. Assume that all $z_{i'} \neq 0$, all $x_{i'}$ are distinct from all y_{jk}, and that $y_{ij} \neq y_{lk}$ for $i' \neq l$ and for all j, k.*

Define the matrix H over $\mathbb{Z}_p[\omega]$ by

$$H = \begin{pmatrix} \frac{z_1}{x_1-y_{11}} & \frac{z_2}{x_2-y_{11}} & \cdots & \frac{z_n}{x_n-y_{11}} \\ \frac{z_1}{(x_1-y_{11})(x_1-y_{12})} & \frac{z_2}{(x_2-y_{11})(x_2-y_{12})} & \cdots & \frac{z_n}{(x_n-y_{11})(x_n-y_{12})} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{z_1}{(x_1-y_{11})(x_1-y_{12})\cdots(x_1-y_{1r})} & \frac{z_2}{(x_2-y_{11})(x_2-y_{12})\cdots(x_2-y_{1r})} & \cdots & \frac{z_n}{(x_n-y_{11})(x_n-y_{12})\cdots(x_n-y_{1r})} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{z_1}{(x_1-y_{s1})(x_1-y_{s2})\cdots(x_1-y_{sr})} & \frac{z_2}{(x_2-y_{s1})(x_2-y_{s2})\cdots(x_2-y_{sr})} & \cdots & \frac{z_n}{(x_n-y_{s1})(x_n-y_{s2})\cdots(x_n-y_{sr})} \end{pmatrix}, \tag{4.3}$$

If $rs < n$, then H serves as the parity-check matrix of a code with a minimum distance of at least $rs+1$.

Several important special cases arise:

(1) **Generalized BCH codes ($s = 1$).** Setting $y_{1i'} = 0$, $z_{i'} = \rho^{c-a_{i'}-1}$, and $x_{i'} = \rho^{-a_{i'}-1}$, the matrix H reduces to the familiar generalized BCH form:

$$H_{\text{BCH}} = \begin{pmatrix} 1 & \rho^{c} & \rho^{2c} & \cdots & \rho^{(n-1)c} \\ 1 & \rho^{c+a} & \rho^{2(c+a)} & \cdots & \rho^{(n-1)(c+a)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \rho^{c+(r-1)a} & \rho^{2(c+(r-1)a)} & \cdots & \rho^{(n-1)(c+(r-1)a)} \end{pmatrix}.$$

Example 4.2. *Let $n = 7$, $r = 3$, $c = 1$, $a = 1$, and ρ a primitive element of $\mathbb{Z}_2[\omega]$. Then,*

$$H_{BCH} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \rho & \rho^2 & \rho^3 & \rho^4 & \rho^5 & \rho^6 \\ 1 & \rho^2 & \rho^4 & \rho^6 & \rho & \rho^3 & \rho^5 \end{pmatrix}.$$

(2) **Srivastava-like codes ($r = 1$).** Equation (4.3) simplifies to:

$$H = \begin{pmatrix} \frac{z_1}{x_1 - y_{11}} & \frac{z_2}{x_2 - y_{11}} & \cdots & \frac{z_n}{x_n - y_{11}} \\ \frac{z_1}{x_1 - y_{21}} & \frac{z_2}{x_2 - y_{21}} & \cdots & \frac{z_n}{x_n - y_{21}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{z_1}{x_1 - y_{s1}} & \frac{z_2}{x_2 - y_{s1}} & \cdots & \frac{z_n}{x_n - y_{s1}} \end{pmatrix}.$$

Example 4.3. *Let $n = 5$, $s = 2$, $z_i = 1$, $x_i = \rho^i$, $y_{11} = 0$, $y_{21} = 1$. Then*

$$H = \begin{pmatrix} 1/\rho & 1/\rho^2 & 1/\rho^3 & 1/\rho^4 & 1/\rho^5 \\ 1/(\rho - 1) & 1/(\rho^2 - 1) & 1/(\rho^3 - 1) & 1/(\rho^4 - 1) & 1/(\rho^5 - 1) \end{pmatrix}.$$

(3) **Specialized Srivastava-like codes ($r = 2tp$).** Each block in H consists of $2tp$ rows, and can be reduced using Proposition 4.1:

$$H = \begin{pmatrix} \frac{1}{x_1 - y_{11}} & \cdots & \frac{1}{x_n - y_{11}} \\ \vdots & \ddots & \vdots \\ \frac{1}{x_1 - y_{2tp,1}} & \cdots & \frac{1}{x_n - y_{2tp,1}} \end{pmatrix}.$$

Example 4.4. *Let $r = 1, s = 2, n = 13$, $t = 1, p = 2$, $z_i = 1$, and ρ a generator of $\mathbb{Z}_2[\omega]^2$. Let*

$$y_{11} = 0, \quad y_{21} = 1.$$

Then, the parity check matrix H is:

$$H = \begin{bmatrix} 1/\rho & 1/\rho^2 & \cdots & 1/\rho^{13} \\ 1/(\rho - 1) & 1/(\rho^2 - 1) & \cdots & 1/(\rho^{13} - 1) \\ 1/(\rho^2 - 1) & 1/(\rho^3 - 1) & \cdots & 1/(\rho - 1) \\ 1/(\rho^3 - 1) & 1/(\rho^4 - 1) & \cdots & 1/(\rho^2 - 1) \end{bmatrix}.$$

The resulting code has parameters $(13, 5)$ *with minimum distance* 9*, and its dual has parameters* $(13, 8)$ *with minimum distance* 3*.*

5. Comparison and discussion

This section compares noncyclic BCH and Srivastava codes over Galois fields and Eisenstein fields in terms of code length n, designed minimal distance d, code dimension k, redundancy $n - k$, degree of the generator polynomial $r = \deg(g(x))$, cardinality $|C|$, and code rate $R = k/n$. Tables 2 and 3 summarize the reported results.

Table 2. Comparison of noncyclic BCH and Srivastava codes over GF(2^m) and $\mathbb{Z}_p[\omega]^{m/2}$.

Parameters	BCH over GF	BCH over EF	Srivastava over GF	Srivastava over EF
n	$\leq p^m - s$	$\leq p^{2(m/2)} - 2s$	$\leq p^m - s$	$\leq p^{2(m/2)} - 2s$
$\deg(g(x))$	m	$m/2$	m	$m/2$
k	$\leq p^m - s - r$	$\leq p^m - s - r$	$\leq p^m - s - r$	$\leq p^m - 2s - r$
d	$s + 1$	$2s + 1$	$2s + 1$	$4s + 1$
$\lvert C\rvert$	p^k	p^{2k}	p^k	p^{2k}
$n - k$	$\leq p^m - s - k$	$\leq p^m - s - k$	$\leq p^m - s - k$	$\leq p^m - 2s - k$
$R = k/n$	$\frac{p^m - s - r}{p^m - s}$	$\frac{p^m - s - r}{p^m - s}$	$\frac{p^m - s - r}{p^m - s}$	$\frac{p^m - 2s - r}{p^m - 2s}$

Table 3. Reported results of noncyclic BCH and Srivastava codes over GF(2^4) and $\mathbb{Z}_2[\omega]^2$ (original data, not fully verified).

Parameters	BCH over GF(2^4)	BCH over $\mathbb{Z}_2[\omega]^2$	Srivastava over GF(2^4)	Srivastava over $\mathbb{Z}_2[\omega]^2$
n	14	13	14	13
$\deg(g(x))$	4	2	4	2
k	9	10	6	6
d	3	5	5	9
$\lvert C\rvert$	512	1048576	32	4096
$n - k$	5	3	8	7
$R = k/n$	0.6429	0.7692	0.4286	0.4286

Figures 1 and 2 illustrate the comparisons of the number of codewords and code dimensions, respectively. Despite some numerical inconsistencies, the results indicate that Eisenstein-field constructions tend to produce shorter codes with larger minimum distances and higher code rates compared to their Galois field counterparts. This suggests potential advantages in terms of error correction and transmission efficiency, although a fully verified analysis is required before drawing rigorous conclusions.

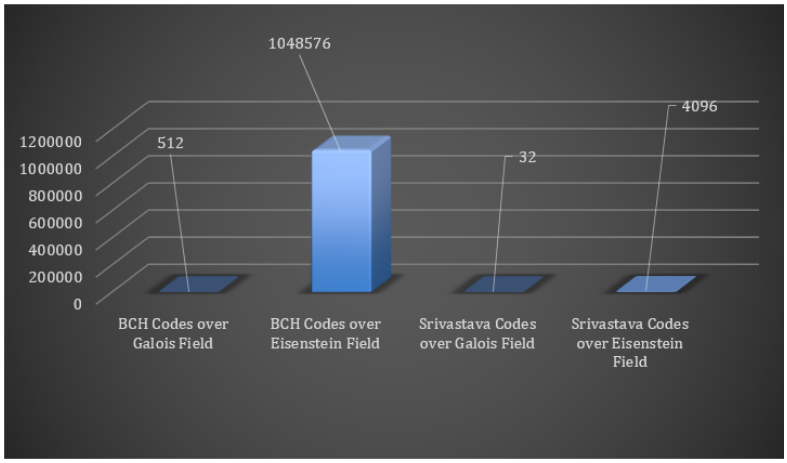

Figure 1. Comparison of the number of codewords of the BCH and Srivastava codes.

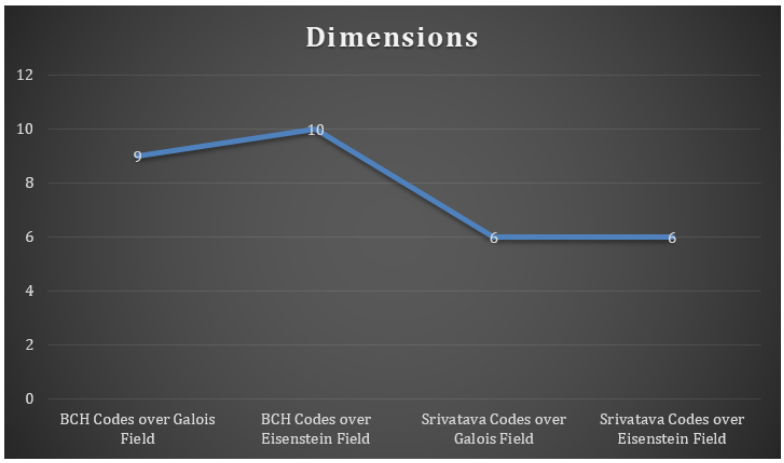

Figure 2. Comparison of dimensions of BCH and Srivastava codes.

6. Conclusions and future directions

This work presents a new approach for developing and evaluating noncyclic BCH and Srivastava codes over Eisenstein fields $\mathbb{Z}_p[\omega]$, where $p \equiv 2 \pmod 3$. By leveraging the algebraic structure of Eisenstein fields, we constructed extended parity-check matrices using an Alternant-type framework that maximizes determinant values. This enables the derivation of exact lower bounds on the minimum distance, thereby enhancing the error-correction capability. A comparison with classical cyclic codes shows that the proposed noncyclic generalization achieves higher code rates and larger minimum distances. The study also highlights the potential relevance of these codes to modern technological domains, including quantum communication, secure data storage, and high-performance computing. The observed performance patterns differ from traditional coding schemes, offering new insights for developing stable and efficient code families.

This framework lays the groundwork for further investigation of noncyclic codes over Eisenstein fields, contributing meaningfully to coding theory and information security. Future work will focus on extending these constructions, developing more advanced decoding algorithms, and exploring practical applications in cryptography, such as image encryption, audio encryption, AES S-box design, and RSA-based security. Additionally, the structural properties of these codes may be examined for use in DNA decoding frameworks, which could support genomic data analysis and contribute to emerging applications such as mutation detection and cancer treatment.

Author contributions

Muhammad Sajjad and Nawaf A. Alqwaifly: Conceptualization, methodology, software implementation, analysis, editing, and critical revisions. All authors of this article have contributed equally. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

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

Acknowledgments

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2025).

Dedication

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 legacy continues to inspire our scholarly endeavours. May his soul rest in eternal peace.

Conflict of interest

The authors declare no conflicts of interest.

References

1. R. C. Bose, D. K. Ray-Chaudhuri, On a class of error correcting binary group codes, *Inf. Control*, **3** (1960), 68–79. https://doi.org/10.1016/S0019-9958(60)90287-4
2. H. J. Helgert, Noncyclic generalizations of BCH and Srivastava codes, *Inf. Control*, **21** (1972), 280–290. https://doi.org/10.1016/S0019-9958(72)80007-X
3. E. Spiegel, Codes over $\mathbb{Z}_m$, *Inf. Control*, **35** (1977), 48–51. https://doi.org/10.1016/S0019-9958(77)90526-5
4. E. Spiegel, Codes over $\mathbb{Z}_m$, revisited, *Inf. Control*, **37** (1978), 100–104. https://doi.org/10.1016/S0019-9958(78)90461-8
5. E. R. Berlekamp, *Algebraic coding theory*, World Scientific Publishing Co., Inc., 2015.
6. T. Muir, W. H. Metzler, *A treatise on the theory of determinants*, New York: Dover Publications, 1960.
7. M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi, I. Hussain, Quaternion integers based higher length cyclic codes and their decoding algorithm, *CMC Comput. Mater. Continua*, **73** (2022), 1177–1194. https://doi.org/10.32604/cmc.2022.025245
8. 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
9. M. Sajjad, T. Shah, Q. Xin, B. Almutairi, Eisenstein field BCH codes construction and decoding, *AIMS Mathematics*, **8** (2023), 29453–29473. https://doi.org/10.3934/math.20231508
10. 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

11. G. Xu, G. Luo, X. Cao, H. Xu, Hulls of linear codes from simplex codes, *Des. Codes Cryptogr.*, **92** (2024), 1095–1112. https://doi.org/10.1007/s10623-023-01331-4

12. Z. Sun, X. Liu, S. Zhu, Y. Tang, Negacyclic BCH codes of length $\frac{q^{2m-1}}{q+1}$ and their duals, *Des. Codes Cryptogr.*, **92** (2024), 2085–2101. https://doi.org/10.1007/s10623-024-01380-3

13. 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

14. M. Sajjad, T. Shah, M. Abbas, M. Alammari, R. J. Serna, The impact of alternant codes over Eisenstein integers on modern technology, *Comp. Appl. Math.*, **44** (2025), 95. https://doi.org/10.1007/s40314-024-03057-y

AIMS Press