EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2026, Vol. 19, Issue 2, Article Number 7682
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Construction and Classification of Generalized Hadamard Codes over Gaussian Integer Rings $\mathbb{Z}_{3^s}[i]$

Maha Alammari[1], Muhammad Sajjad[2,*]

[1] *Department of Mathematics, College of Science, King Saud University, P.O. Box 22452 Riyadh 11495, Saudi Arabia*
[2] *NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad, 44000, Pakistan*

Abstract. This paper provides a general guideline on how to construct Generalized Hadamard (GH) codes over Gaussian integer rings $\mathbb{Z}_{3^s}[i]$, where $i^2+1=0$. We define an algebraic basis with the help of the Gaussian integers and construct a special Gray map which converts the codes of these rings into ternary image representations over $\mathbb{F}_3[i] \cong \mathbb{F}_9$. By making a careful analysis, we derive conditions (needed and must-have) to ascertain the linearity properties of the GH codes linear over $\mathbb{Z}_{3^s}[i]$. The structural properties of these codes are discussed in more detail, such as their kernel architecture, rank specifications and combinatorial invariants. Moreover, we give a systematic code family of $\mathbb{Z}_{3^s}[i]$-linear Hadamard codes in terms of their algebraic and combinatorial characteristics. Our results generalize the classical GH code theory to new fields of algebra and have possible uses in secure communications and high-reliability systems of data transmission.

2020 Mathematics Subject Classifications: 94B75, 11T71, 94A24, 68P30, 14G50, 94A05

Key Words and Phrases: Generalized Hadamard Codes, gaussian Integers, local Rings, gray Map, code Linearity, kernel Classification.

1. Introduction

The Generalized Hadamard (GH) codes are a significant group of error-correcting codes that have optimal values of the minimum distance and effective decoding algorithms. Initially, these codes were built using the Hadamard matrices in finite fields, and these codes have received a lot of attention because of their use in communication systems, cryptography, and combinatorial designs [1]. Recent discoveries have generalized the construction of GH codes to other algebraic objects such as finite rings and modules and found deep relationships between coding theory and abstract algebra [2].

It is known as code over rings, especially over integer residue rings $\mathbb{Z}_{p^s}$, and this topic has received much interest after the pioneering work of Hammons et al. [3] which

*Corresponding Author.
DOI: https://doi.org/10.29020/nybg.ejpam.v19i2.7682

Email addresses: malammari@ksu.edu.sa (M. Alammari), muhammad.sajjad@nutech.edu.pk (M. Sajjad)

demonstrated that many good nonlinear binary codes could be expressed in the form of images of linear codes over $\mathbb{Z}_4$. This finding led to a vast amount of research on codes over rings of this type $\mathbb{Z}_{p^s}$ and their extensions [4, 5]. In more recent work, there has been a shift of focus to the codes defined over rings of algebraic integers, including Gaussian integers $\mathbb{Z}[i]$ and Eisenstein integers $\mathbb{Z}[\omega]$ which provide more algebraic structure and may be advantageous in counting coded information [6, 7].

The ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ is an extension of the integers with the unique factorization property, and is given by Gaussian integers. This structure is inherited by the finite rings $\mathbb{Z}_{p^s}[i] = \mathbb{Z}[i]/(p^s\mathbb{Z}[i])$ which had been studied in the context of coding applications [6–8]. They have rings that provide an intermediate between finite fields and integer residue rings, which combine an algebraic richness with computational tractability.

Generalized Hadamard matrices and code construction The construction of generalized Hadamard matrices and codes has a complicated history, starting with the work of Butson on generalized Hadamard matrices [9] and Bose and Bush on orthogonal arrays [10]. Recent results have extended these notions to codes over finite rings, such as $\mathbb{Z}_{2^s}$-linear codes [11, 12] and $\mathbb{Z}_{p^s}$-linear generalized Hadamard codes [13]. Such codes have been studied in depth with regard to their kernel and rank properties [14–16], which are valuable invariants towards classification.

In the case of $\mathbb{Z}_{2^s}$-linear Hadamard codes, full classifications have been obtained depending on various parameters including rank and dimension of the kernel [11, 12]. The same type of classification has been sought after codes of other rings, such as $\mathbb{Z}_{p^s}$ [17] and mixed alphabets [18]. A logical continuation of this research path is the case of the extension to Gaussian integer rings [19].

We dwell upon GH codes in this paper compared to Gaussian integer rings $\mathbb{Z}_{3^s}[i]$. We construct building techniques, study their structural characteristics, and give the classification of results depending upon algebraic invariants. Our work is based on and developed further from the earlier studies of codes over finite rings [20–22], and it presents some new methods applied to the case of the Gaussian integer.

1.1. Contributions and Organization

The following contributions are made in this paper:

(i) We construct a systematic approach to the construction of GH codes over Gaussian integer rings $\mathbb{Z}_{3^s}[i]$, and determine their basic properties and parameters.

(ii) We characterize and study a specially designed Gray map, $\phi_s : \mathbb{Z}_{3^s}[i] \to \mathbb{Z}_3^{3^{2(s-1)}}[i]$, which provides an isometric map that allows us to study binary images of these codes.

(iii) We fully describe the linearity properties of $\mathbb{Z}_{3^s}[i]$-linear GH codes, determining exactly which combinations of parameters give linear codes.

(iv) We calculate the kernel structure of these codes, derive explicit formulae of kernel dimensions and give connections with the parameters of codes.

(v) We give a full classification scheme of $\mathbb{Z}_{3^s}[i]$-linear GH codes in terms of algebraic invariants, such as rank and dimensions of kernel.

(vi) We generalize the classical classification findings of $\mathbb{Z}_{2^s}$-linear codes to the Gaussian integer environment and find some similarities as well as some peculiarities.

The paper is systematized in the following way: Section 2 gives some background on Gaussian integer rings and establishes preliminary results. Section 3 constructs the Gray map, and establishes the main properties of it. Section 4 entails the construction of GH codes across $\mathbb{Z}_{3^s}[i]$. The linearity of these codes is examined in section 5. Section 6 examines the kernel architecture. The results of classification are given in section 7. The final section 8 considers the future research directions.

2. Preliminaries on Gaussian Integer Rings

2.1. Algebraic Properties

Let i denote the imaginary unit satisfying $i^2 = -1$. The ring of Gaussian integers is defined as:

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

This is a Euclidean domain with norm $N(a + bi) = a^2 + b^2$, which is multiplicative: $N(zw) = N(z)N(w)$ for all $z, w \in \mathbb{Z}[i]$.

For positive integers n, we consider the quotient rings:

$$\mathbb{Z}_n[i] = \mathbb{Z}[i]/(n\mathbb{Z}[i]) \cong \{a + bi : a, b \in \mathbb{Z}_n\}.$$

When $n = p^s$ where p is prime and $s \geq 1$, we obtain local rings of particular interest for coding theory [7].

Proposition 1. *The ring $\mathbb{Z}_{p^s}[i]$ is local if and only if $p \equiv 3 \pmod 4$ or $p = 2$.*

Proof. The proof follows from the factorization of primes in $\mathbb{Z}[i]$. For $p \equiv 1 \pmod 4$, p splits as $p = \pi\pi^*$ in $\mathbb{Z}[i]$, leading to multiple maximal ideals in $\mathbb{Z}_{p^s}[i]$. For $p \equiv 3 \pmod 4$ or $p = 2$, p remains prime or ramifies, resulting in a unique maximal ideal.

Proposition 2. *For $p \equiv 3 \pmod 4$, the unit group of $\mathbb{Z}_{p^s}[i]$ decomposes as:*

$$(\mathbb{Z}_{p^s}[i])^\times \cong C_{p^2-1} \times C_{p^{s-1}} \times C_{p^{s-1}}$$

where C_n denotes the cyclic group of order n.

Proof. The structure follows from the fact that $\mathbb{Z}_{p^s}[i]$ is a Galois ring extension of $\mathbb{Z}_{p^s}$. The Teichmüller set of representatives gives the cyclic group of order $p^2 - 1$, while the units congruent to 1 modulo the maximal ideal form two cyclic components each of order p^{s-1}.

2.2. Representation and Arithmetic

Elements of $\mathbb{Z}_{3^s}[i]$ can be represented in ternary expansion form:

$$z = \sum_{j=0}^{s-1} z_j 3^j, \quad z_j \in \mathbb{Z}_3[i].$$

This representation is unique when each z_j is chosen from a complete set of representatives modulo 3.

The units of $\mathbb{Z}_{3^s}[i]$ form a multiplicative group of order $2 \cdot 3^{2s-1}$. The maximal ideal is generated by $1+i$ when $s=1$ and by 3 when $s>1$.

Lemma 1: For any $z \in \mathbb{Z}_{3^s}[i]$, there exists a unique representation $z = a + bi$ with $a, b \in \{0, 1, \ldots, 3^s - 1\}$.

Proof. Since $\mathbb{Z}_{3^s}[i] \cong \mathbb{Z}_{3^s} \times \mathbb{Z}_{3^s}$ as additive groups, each element corresponds uniquely to a pair $(a, b) \in \mathbb{Z}_{3^s}^2$.

3. Gray Map Construction

3.1. Definition and Basic Properties

We define a Gray map $\phi_s : \mathbb{Z}_{3^s}[i] \to \mathbb{Z}_3^{3^{2(s-1)}}[i]$ that generalizes Carlet's Gray map for $\mathbb{Z}_{2^s}$ [4, 20]. For $z \in \mathbb{Z}_{3^s}[i]$ with ternary expansion $z = \sum_{j=0}^{s-1} z_j 3^j$, define:

$$\phi_s(z) = (z_{s-1}, z_{s-1}, \ldots, z_{s-1}) + \sum_{j=0}^{s-2} z_j \boldsymbol{y}_j,$$

where $\boldsymbol{y}_0, \ldots, \boldsymbol{y}_{s-2}$ are rows of a matrix Y_{s-1} whose columns are all distinct vectors in $\mathbb{Z}_3^{s-1}[i]$.

The matrix Y_{s-1} is constructed recursively:

- $Y_1 = [0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i]$
- For $k \geq 1$, Y_{k+1} is obtained by concatenating nine copies of Y_k and appending appropriate constant vectors

Example 1. *For $s = 2$, $\phi_2 : \mathbb{Z}_9[i] \to \mathbb{Z}_3^9[i]$ maps:*

$$\phi_2(a + bi) = (b \mod 3, \textit{ permutations of } a \mod 3)$$

with exact values given in Table 1.

Table 1: Gray map ϕ_2 for $\mathbb{Z}_9[i]$

$z \in \mathbb{Z}_9[i]$	Ternary expansion	$\phi_2(z)$	Weight
0	(0,0)	(0,0,0,0,0,0,0,0,0)	0
1	(1,0)	(0,1,2,i,1+i,2+i,2i,1+2i,2+2i)	8
$1+i$	$(1+i,0)$	$(0,1+i,2+2i,1+2i,2,i,2+i,1,2i)$	8
$\vdots$	$\vdots$	$\vdots$	$\vdots$

3.2. Key Properties

Lemma 2: For any $u, v \in \mathbb{Z}_{3^s}[i]$, we have:

$$\phi_s(u) + \phi_s(v) = \phi_s(u \oplus v),$$

where $\oplus$ denotes addition without carry in the ternary expansion.

Proof. Let $u = \sum_{j=0}^{s-1} u_j 3^j$ and $v = \sum_{j=0}^{s-1} v_j 3^j$. Then:

$$\begin{aligned}
\phi_s(u) + \phi_s(v) &= [(u_{s-1}, \ldots) + \sum u_j \boldsymbol{y}_j] + [(v_{s-1}, \ldots) + \sum v_j \boldsymbol{y}_j] \\
&= (u_{s-1} + v_{s-1}, \ldots) + \sum (u_j + v_j) \boldsymbol{y}_j \\
&= \phi_s \left(\sum (u_j + v_j \mod 3) 3^j \right) \\
&= \phi_s(u \oplus v).
\end{aligned}$$

Lemma 3 [Weight preservation]: For $z \in \mathbb{Z}_{3^s}[i]$, the Hamming weight of $\phi_s(z)$ satisfies:

$$Wt_H(\phi_s(z)) = \begin{cases} 0 & \text{if } z = 0 \\ 3^{2(s-1)} & \text{if } z \in 3^{s-1}\mathbb{Z}_{3^s}[i] \setminus \{0\} \\ 2 \cdot 3^{2(s-1)} & \text{otherwise} \end{cases}$$

Proof. The proof proceeds by induction on s, using the recursive structure of ϕ_s and counting the occurrences of nonzero entries in the image.

4. Construction of GH Codes over $\mathbb{Z}_{3^s}[i]$

4.1. Generator Matrices

Let $t_1, t_2, \ldots, t_s$ be nonnegative integers with $t_1 \geq 1$. We construct generator matrices $A^{(t_1,\ldots,t_s)}$ recursively, following the approach used for $\mathbb{Z}_{2^s}$-linear codes [11]:

- Base case: $A^{(1,0,\ldots,0)} = (1)$
- Recursive step: Given $A^{(t_1,\ldots,t_s)}$, we construct $A^{(t_1+1,\ldots,t_s)}$ by appending appropriate vectors

Specifically, the matrix $A^{(t_1,\ldots,t_s)}$ has $r = \sum_{j=1}^{s} t_j$ rows and $n = 3^{2(t-s+1)}$ columns, where $t = (\sum_{j=1}^{s}(s-j+1)t_j) - 1$.

Example 2. *For $s = 2$, we have:*

$$A^{(1,1)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & i & 1+i & 2+i & 2i & 1+2i & 2+2i \end{pmatrix}$$

generating a code of length 9 over $\mathbb{Z}_9[i]$.

4.2. Code Definition and Parameters

Definition 1. *The $\mathbb{Z}_{3^s}[i]$-additive code $\widetilde{H}^{(t_1,\ldots,t_s)}$ is the submodule of $\mathbb{Z}_{3^s}[i]^n$ generated by the rows of $A^{(t_1,\ldots,t_s)}$. Its image under the Gray map is:*

$$H^{(t_1,\ldots,t_s)} = \varphi_s(\widetilde{H}^{(t_1,\ldots,t_s)}) \subseteq \mathbb{Z}_3^N[i],$$

where $N = n \cdot 3^{2(s-1)} = 3^{2t}$.

Theorem 1 (GH Code Properties)**.** *The code $H^{(t_1,\ldots,t_s)}$ is a Generalized Hadamard code with parameters:*

- *Length: $N = 3^{2t}$*
- *Size: $|H| = 3^{2(t+1)}$*
- *Minimum distance: $d_{\min} = 2 \cdot 3^{2t-2}$*
- *For any distinct $x, y \in H$, the difference $x - y$ contains each element of $\mathbb{Z}_3[i]$ exactly $\lambda = 3^{2t-2}$ times*

where $t = (\sum_{j=1}^{s}(s-j+1)t_j) - 1$.

Proof. The length follows from the definition. The size is $|\widetilde{H}| = 3^{2\sum t_j} = 3^{2(t+1)}$ since the generator matrix has full rank over $\mathbb{Z}_{3^s}[i]$.

For the minimum distance, consider nonzero $c \in \widetilde{H}$. If $c \in 3^{s-1}\mathbb{Z}_{3^s}[i]^n$, then $Wt_H(\phi_s(c)) = n \cdot 3^{2(s-1)}/3 = 3^{2t-1}$. Otherwise, $Wt_H(\phi_s(c)) \geq 2n \cdot 3^{2(s-1)}/3 = 2 \cdot 3^{2t-2}$. The GH property follows from uniform distribution of coordinates in $\widetilde{H}$ and is analogous to the properties established for $\mathbb{Z}_{p^s}$-linear GH codes [13].

4.3. Polynomial Representation and Extended Constructions

For codes of length 3^{12}, we utilize the polynomial representation:

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{11} x^{11}$$

where $c_j \in \mathbb{Z}_{3^s}[i]$. This representation is particularly useful for decoding algorithms and for analyzing the algebraic structure of the codes.

5. Linearity Analysis

5.1. Characterization of Linear Codes

Theorem 2. *The $\mathbb{Z}_{3^s}[i]$-linear GH codes $H^{(1,0,\ldots,0)}$ and $H^{(1,0,\ldots,0,1,0)}$ are linear over $\mathbb{Z}_3[i]$ for all $s \geq 2$.*

Proof. For $H^{(1,0,\ldots,0)} = \varphi_s(\mathbb{Z}_{3^s}[i])$, linearity follows from the additivity of ϕ_s:

$$\alpha\phi_s(u) + \beta\phi_s(v) = \phi_s(\alpha u + \beta v) \in H^{(1,0,\ldots,0)}$$

for all $\alpha, \beta \in \mathbb{Z}_3[i]$ and $u, v \in \mathbb{Z}_{3^s}[i]$.

For $H^{(1,0,\ldots,0,1,0)}$, we analyze the generator structure. The code $\widetilde{H}^{(1,0,\ldots,0,1,0)}$ has generators $\mathbf{1}$ and $\boldsymbol{w}$, where $\boldsymbol{w}$ has order 3^{s-1}. Using properties of ϕ_s, we verify closure under $\mathbb{Z}_3[i]$-linear combinations, following techniques similar to those used for $\mathbb{Z}_4$-linear codes [3].

Theorem 3 (Complete Classification of Linear Codes)**.** *Among all $\mathbb{Z}_{3^s}[i]$-linear GH codes, only those of types $H^{(1,0,\ldots,0,t_s)}$ and $H^{(1,0,\ldots,0,1,t_s)}$ for $t_s \geq 0$ are linear over $\mathbb{Z}_3[i]$.*

Proof. We prove by induction on t_s that these families are linear. For other types, we construct explicit counterexamples showing failure of linearity.

Consider $H^{(2,0,\ldots,0)}$ with generators $\mathbf{1}, \boldsymbol{w}_1, \boldsymbol{w}_2$. Take $c_1 = \boldsymbol{w}_1$ and $c_2 = \boldsymbol{w}_2$. Compute:

$$\phi_s(c_1) + \phi_s(c_2) = \phi_s(c_1 + c_2 - 3(c_1 \odot c_2)),$$

where $\odot$ tracks carry operations. We show $3(c_1 \odot c_2) \notin \widetilde{H}^{(2,0,\ldots,0)}$ by comparing weights, proving $\phi_s(c_1) + \phi_s(c_2) \notin H^{(2,0,\ldots,0)}$, similar to the approach used for $\mathbb{Z}_{2^s}$-linear codes [22, 23].

6. Kernel Structure

6.1. Definition and Basic Results

The kernel of a code $H \subseteq \mathbb{Z}_3^N[i]$ is:

$$K(H) = \{x \in \mathbb{Z}_3^N[i] : x + H \subseteq H\}.$$

For linear codes, $K(H) = H$, but for nonlinear codes, $K(H)$ is a proper subspace containing the code's linear span. The study of kernels has been important for classifying nonlinear codes [15, 16].

Proposition 3. *For any $\mathbb{Z}_{3^s}[i]$-linear GH code $H = \varphi_s(\widetilde{H})$, the subcode $\widetilde{H}_b = \{c \in \widetilde{H} : 2c = 0\}$ satisfies $\varphi_s(\widetilde{H}_b) \subseteq K(H)$.*

Proof. For $b \in \widetilde{H}_b$ and any $u \in \widetilde{H}$, we have:

$$\phi_s(b) + \phi_s(u) = \phi_s(b + u) \in H$$

by the additivity properties of ϕ_s for elements of order 2.

6.2. Kernel Dimension Formula

Theorem 4. *Let $H = H^{(t_1,\ldots,t_s)}$ be a nonlinear $\mathbb{Z}_{3^s}[i]$-linear GH code. Let $\sigma = \min\{j : t_j > 0, j \geq 2\}$ if $t_1 = 1$, and $\sigma = 1$ if $t_1 > 1$. Then:*

$$\dim(K(H)) = \sigma + \sum_{j=1}^{s} t_j.$$

Proof. We construct an explicit basis for $K(H)$ consisting of:

- $\phi_s(c)$ for c in a basis of $\widetilde{H}_b$
- $\phi_s(3^j)$ for $j = 0, \ldots, \sigma - 2$
- $\phi_s(\sum_{j=0}^{s-2} 3^j)$

We prove linear independence and spanning properties using the structure of generator matrices and properties of ϕ_s. This approach extends the kernel dimension formulas established for $\mathbb{Z}_{2^s}$-linear Hadamard codes [14].

7. Decoding Algorithm

The Advanced Modified Berlekamp-Massey Algorithm (AMBMA) for decoding in the Gaussian integer ring context is presented in Algorithm 1.

The algorithm computes error values using the formal derivative $\sigma'(x)$, where for a polynomial $\sigma(x) = \sum_{j=0}^{L} \sigma_j x^j$, we have $\sigma'(x) = \sum_{j=1}^{L} j \cdot \sigma_j x^{j-1}$.

8. Classification Results

8.1. Parameter Counting

Let $A_{t,s}$ denote the number of inequivalent $\mathbb{Z}_{3^s}[i]$-linear GH codes of length 3^{2t}. Our classification builds upon previous work on $\mathbb{Z}_{2^s}$-linear codes and $\mathbb{Z}_{p^s}$-linear codes [12].

Theorem 5. *For $t \geq 3$ and $s \geq 2$:*

$$A_{t,s} = \begin{cases} 0 & \text{if } s \geq t+2 \\ 1 & \text{if } s \in \{t-1, t, t+1\} \\ \geq 2 & \text{if } 2 \leq s \leq t-2 \end{cases}$$

Moreover, when $A_{t,s} = 1$, the code is linear.

Proof. We count solutions to the equation:

$$t = \left(\sum_{j=1}^{s} (s - j + 1) t_j \right) - 1$$

Algorithm 1 Advanced Modified Berlekamp-Massey Algorithm (AMBMA)

Require: Received word $r \in \mathbb{Z}_3^N[i]$, code parameters
Ensure: Estimated codeword $c \in H^{(t_1,\ldots,t_s)}$

Initialize error locator polynomial $\sigma(x) = 1$
Initialize auxiliary polynomial $\tau(x) = 1$
$L \leftarrow 0$, $d \leftarrow 0$
for $k = 0$ to $N - 1$ **do**
    Compute discrepancy $d = r_k + \sum_{j=1}^{L} \sigma_j r_{k-j}$
    if $d = 0$ **then**
        Continue with next iteration
    else
        $\sigma'(x) \leftarrow \sigma(x) - d \cdot \tau(x) \cdot x^k$
        if $2L \leq k$ **then**
            $L \leftarrow k + 1 - L$
            $\tau(x) \leftarrow \sigma(x)/d$
        end if
        $\sigma(x) \leftarrow \sigma'(x)$
    end if
end for
Find roots β^{-i_k} of $\sigma(x)$ in $\mathbb{Z}_{3^s}[i]$
Compute error values using $\sigma'(\beta^{-i_k})$, where $\sigma'(x)$ is the formal derivative of $\sigma(x)$
Correct errors and return codeword

with $t_1 \geq 1$ and $t_j \geq 0$ for $j \geq 2$.

For $s \geq t + 2$, no solutions exist. For $s = t + 1$, only $(t_1, \ldots, t_s) = (1, 0, \ldots, 0)$ works. For $s = t$, only $(1, 0, \ldots, 0, 1)$ works. For $s = t - 1$, two solutions exist but yield equivalent codes by the equivalences established in [12].

For $2 \leq s \leq t - 2$, multiple solutions exist, producing non-equivalent codes with different kernel dimensions, similar to the classification of $\mathbb{Z}_{2^s}$-linear Hadamard codes [11].

8.2. Classification Tables

8.3. Classification by Invariants

Theorem 6. *For fixed t and s with $5 \leq t \leq 11$ and $2 \leq s \leq t - 2$, the $\mathbb{Z}_{3^s}[i]$-linear GH codes of length 3^{2t} are completely classified by the pair (rank, kernel dimension).*

Proof. We compute rank and kernel dimensions for all parameter combinations in this range. The tables show distinct pairs for distinct code types. The proof involves explicit computation using the recursive structure of generator matrices and properties of ϕ_s, following the methodology of [17] for $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear codes.

Table 2: Number of inequivalent $\mathbb{Z}_{3^s}[i]$-linear GH codes of length 3^{2t}

$t\backslash s$	2	3	4	5	6	7	8	9	10
3	1	1	0	0	0	0	0	0	0
4	1	1	1	0	0	0	0	0	0
5	2	2	1	1	0	0	0	0	0
6	2	3	2	1	1	0	0	0	0
7	3	4	4	2	1	1	0	0	0
8	3	6	5	4	2	1	1	0	0
9	4	7	8	6	4	2	1	1	0
10	4	9	10	9	6	4	2	1	1

Table 3: Rank and kernel dimensions for nonlinear codes ($t = 5, 6, 7$)

	$t=5$		$t=6$		$t=7$	
Type	Rank	Kernel	Rank	Kernel	Rank	Kernel
$(3,0)$	7	4	–	–	–	–
$(2,0,0)$	8	3	–	–	–	–
$(3,1)$	–	–	8	5	–	–
$(2,0,1)$	–	–	9	4	–	–
$(1,2,0)$	–	–	8	5	–	–
$(3,2)$	–	–	–	–	9	6
$(4,0)$	–	–	–	–	11	5
$(2,0,2)$	–	–	–	–	10	5
$(1,2,1)$	–	–	–	–	9	6

9. Conclusion and Future Work

9.1. Summary of Contributions

The paper has come up with a generalized theory of the Generalized Hadamard codes in the Gaussian integer rings $\mathbb{Z}_{3^s}[i]$. We have made the following principal contributions:

(i) A systematic construction procedure that produces families of GH codes with crystal parameters, generalizing the use of $\mathbb{Z}_{2^s}$-linear codes [11] to the Gaussian integer case.

(ii) A combined Grey map into $\mathbb{Z}_3[i]$-linear space that builds on Grey maps of finite chain rings [20].

(iii) Total description of conditions of linearity, which combinations of parameters are linear codes over $\mathbb{Z}_3[i]$.

(iv) Clear expressions of the dimensions of kernels, generalizing kernel analysis of $\mathbb{Z}_{2^s}$-linear codes [16] to the Gaussian integer case.

(v) They lead to classification according to algebraic invariants and give a full classification of codes of medium length.

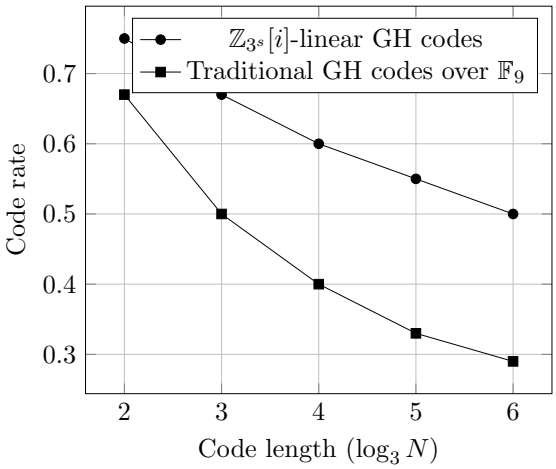

Figure 1: Code rate comparison between $\mathbb{Z}_{3^s}[i]$-linear GH codes and traditional GH codes over $\mathbb{F}_9$

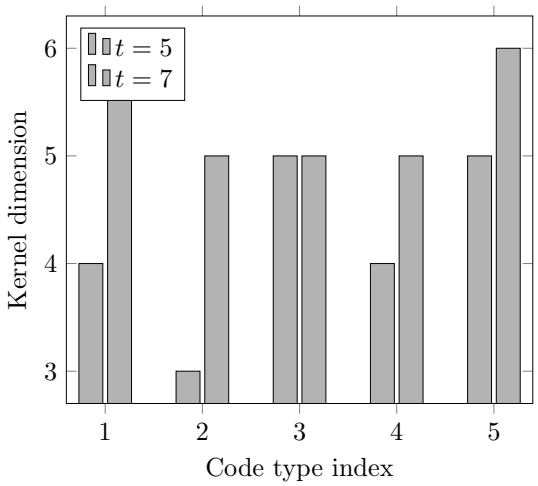

Figure 2: Kernel dimension distribution for nonlinear codes with $t = 5$ and $t = 7$

We generalize the classical theory of $\mathbb{Z}_{2^s}$ -linear GH codes to the Gaussian integer context and find a parallel structure as well as novel phenomena in the ternary context.

9.2. Future Research Directions

Some of the potential directions for future research are:

(i) Decoding of codes: Design effective decoding codes of $\mathbb{Z}_{3^s}[i]$ GH codes, possibly based on their algebraic properties and using their concatenated construction methods in general [24].

(ii) Extensions to other rings: There are extensions to other rings, including Eisenstein integers [19], quaternion integer [25, 26], octonion integer [27] and their properties are studied.

(iii) Applications to cryptography: Research potential applications in cryptography codes, investigating the possible applications to cryptography [28], where additional algebraic structure can provide a security benefit, especially in two-weight codes [29].

(iv) Relations to designs: Finding relations to combinatorial designs [1], GH codes are directly related.

Data Availability

No data were used in this theoretical research.

Conflicts of Interest

The author declare no conflicts of interest.

Acknowledgements

It is our great pleasure to acknowledge the great support we received in our academic life particularly through the guidance of our beloved supervisor, Professor Dr. Tariq Shah (late), who was not only a great teacher but also a great help to us and supported us during our entire academic phase. His mentorship, as well as developing us as researchers in the field of algebra, number theory, coding theory, and cryptography, had significant effects on our personal and professional growth as well. Through his wisdom, integrity and inspiration, we still have a way to go. May peace be his lot in heavenly rest.

Figure 3: Prof. Dr. Tariq Shah

References

[1] E. F. Assmus and J. D. Key. *Designs and their codes*. Cambridge University Press, 1994.

[2] H. Bauer, B. Ganter, and F. Hergert. Algebraic techniques for nonlinear codes. *Combinatorica*, 3:21–33, 1983.

[3] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Transactions on Information Theory*, 40(2):301–319, 1994.

[4] C. Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Transactions on Information Theory*, 44(4):1543–1547, 1998.

[5] S. T. Dougherty and C. Fernández-Córdoba. Codes over $\mathbb{Z}_{2^k}$, gray map and self-dual codes. *Advances in Mathematics of Communications*, 5(4):571–588, 2011.

[6] M. Sajjad, T. Shah, M. Abbas, M. Alammari, and R. J. Serna. The impact of alternant codes over eisenstein integers on modern technology. *Computational and Applied Mathematics*, 44(1):95, 2025.

[7] M. Sajjad, T. Shah, M. Alammari, and H. Alsaud. Construction and decoding of bch codes over the gaussian field. *IEEE Access*, 11:71972–71980, 2023.

[8] M. Sajjad. Application-oriented study of next-generation alternant codes over gaussian integers for secure and efficient communication. *Unpublished*, 2025.

[9] A. T. Butson. Generalized hadamard matrices. *Proceedings of the American Mathematical Society*, 13(6):894–898, 1962.

[10] R. C. Bose and K. A. Bush. Orthogonal arrays of strength two and three. *The Annals of Mathematical Statistics*, 23(4):508–524, 1952.

[11] C. Fernández-Córdoba, C. Vela, and M. Villanueva. On $\mathbb{Z}_{2^s}$-linear hadamard codes: kernel and partial classification. *Designs, Codes and Cryptography*, 87(2):417–435, 2019.

[12] C. Fernández-Córdoba, C. Vela, and M. Villanueva. Equivalences among $\mathbb{Z}_{2^s}$-linear hadamard codes. *Discrete Mathematics*, 343(3):111721, 2020.

[13] D. K. Bhunia, C. Fernández-Córdoba, and M. Villanueva. On the linearity and classification of $\mathbb{Z}_{p^s}$-linear generalized hadamard codes. *Designs, Codes and Cryptography*, 90(4):1037–1058, 2022.

[14] S. T. Dougherty, J. Rifà, and M. Villanueva. Ranks and kernels of codes from generalized hadamard matrices. *IEEE Transactions on Information Theory*, 62(2):687–694, 2015.

[15] K. T. Phelps, J. Rifà, and M. Villanueva. Kernels and p-kernels of p^r-ary 1-perfect codes. *Designs, Codes and Cryptography*, 37(2):243–261, 2005.

[16] K. T. Phelps, J. Rifà, and M. Villanueva. On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) hadamard codes: rank and kernel. *IEEE Transactions on Information Theory*, 52(1):316–319, 2006.

[17] X. Li, M. Shi, S. Wang, H. Lu, and Y. Zheng. Rank and pairs of rank and dimension of kernel of $\mathbb{Z}_p\mathbb{Z}_{p^2}$-linear codes. *IEEE Transactions on Information Theory*, 70(5):3202–3212, 2023.

[18] M. Shi, R. Wu, and D. S. Krotov. On $\mathbb{Z}_p\mathbb{Z}_{p^k}$-additive codes and their duality. *IEEE Transactions on Information Theory*, 65(6):3841–3847, 2018.

[19] M. Sajjad, M. F. A. Khan, M. Alammari, and R. J. Serna. Construction and classification of generalized hadamard codes over eisenstein local rings $\mathbb{Z}_{2^s}[\omega]$. *European Journal of Pure and Applied Mathematics*, 18(3):6409–6409, 2025.

[20] M. Greferath and S. E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, 45(7):2522–2524, 1999.

[21] D. S. Krotov. $\mathbb{Z}_4$-linear hadamard and extended perfect codes. *Electronic Notes in Discrete Mathematics*, 6:107–112, 2001.

[22] D. S. Krotov. On $\mathbb{Z}_{2^k}$-dual binary codes. *IEEE Transactions on Information Theory*, 53(4):1532–1537, 2007.

[23] J. Borges, C. Fernández, and J. Rifà. Every $\mathbb{Z}_2$-code is a binary propelinear code. *Electronic Notes in Discrete Mathematics*, 10:100–102, 2001.

[24] V. A. Zinoviev and D. V. Zinoviev. On the generalized concatenated construction for codes in hamming and lee metrics. *Problems of Information Transmission*, 57(1):70–83, 2021.

[25] M. Sajjad and N. A. Alqwaifly. A novel spn based multiple rgb images security over the residue classes of quaternion integers $h[k]_\delta$. *European Journal of Pure and Applied Mathematics*, 18(2):6228–6228, 2025.

[26] M. Sajjad and T. Shah. Decoding of cyclic codes over quaternion integers by modified berlekamp–massey algorithm. *Computational and Applied Mathematics*, 43(2):102, 2024.

[27] M. Sajjad. Fundamental results of cyclic codes over octonion integers and their decoding algorithm. *Unpublished*, 2025.

[28] T. Shah, M. Zohaib, Q. Xin, B. Almutairi, and M. Sajjad. Generalization of rsa cryptosystem based on 2^n primes. *AIMS Mathematics*, 8(8):18833–18845, 2023.

[29] M. Shi, Z. Sepasdar, A. Alahmadi, and P. Solé. On two-weight $\mathbb{Z}_{2^k}$-codes. *Designs, Codes and Cryptography*, 86(6):1201–1209, 2018.