EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6414
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

Structural Insights and Decoding Strategies for BCH Codes over Quasi-Galois Rings

Muhammad Sajjad[1,*], Muhammad Shoaib Abid[2], Maha Alammari[3], Robinson-Julian Serna[4]

[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] *Department of Mathematics, College of Science, King Saud University, P.O. Box 22452 Riyadh 11495, Saudi Arabia*
[4] *Escuela de Matemáticas y Estadística, Universidad Pedagógica y Tecnológica de Colombia, Tunja, Colombia*

Abstract. Robust data disclosure constitutes an essential problem for contemporary system communication, and the theory of coding becomes the key to maintaining data integrity. This paper discusses constructions and decoding of Bose–Chaudhuri–Hocquenghem (BCH) codes over Quasi-Galois Rings (QGRs) – generalization of classical Galois rings. The QGRs provide richer algebraic structures that lead to improved error correction capabilities, greater code rates, and more codewords than their Galois counterparts. We provide an all-round theory of construction for BCH codes over QGRs, describe them in their construction process, and walk through an efficient decoding technique. Our findings demonstrate the ability of BCH codes under QGR to provide high reliability and performance for the communication systems, which will make them a candidate for future use in data transmission and storage.

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

Key Words and Phrases: Quasi-Galois Rings, BCH Codes, Error Correction, Code Rate, Ring-Based Coding Theory, Cyclic Subgroups

1. Introduction

It relates to how information that is to be transmitted is put into another form that can easily be transmitted through a channel, which is usually a wire or broadcasting system. This entails the use of different codes to reduce errors that may be occasioned by the transmission medium, such as noise, interference or loss of signal strength. The

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6414

Email addresses: muhammad.sajjad@nutech.edu.pk (M. Sajjad), janjuashoaib814@gmail.com (M. S. Abid), malammari@ksu.edu.sa (M. Alammari), robinson.serna@uptc.edu.co (R. J. Serna)

principles of error-detecting and error-correcting codes are very essential to ensure high data reliability, and this involves the Hamming codes, Reed-Solomon codes, and BCH codes. These techniques enhance the dependability of the original data in that the receiver checks and rectifies errors without having to ask for retransmission. As inferred from the above observations, this paper aims at showing that the selection of a particular scheme to be used can greatly affect the dependability and efficiency of the communication system with respect to the RB/SSS trade-off. Hence, the coding theory is a very enabling tool for a plethora of utilization opportunities in the digital world, such as in digital communication, data storage, deep-space signals and even in the new fashion wireless networks [1].

This section is devoted to the discussion of major achievements and the state of the progress as well as the results of recent decades in the study of BCH codes over different algebraic structures. The first step was defined by Assmus and Mattson in [1] who gave an axiomatic approach to error-correcting codes and stated fundamental theorems of modern coding theory. Their work provided what is now acknowledged as the first formal mathematical definitions for making and deciphering codes that are still in use today. Augot, Betti, and Orsini [2] also elaborated on linear and cyclic codes and their importance in the real world, in fields like cryptography and data transmission. A thorough introduction is given to their basic algebraic properties and the encoding methods that are crucial in enhancing the code's performance. Blake [3] studied codes over certain rings, thus enriching and developing theoretical fundamentals of coding theory for various algebraic structures except for fields. His work laid the foundation for studying BCH codes over non-field rings such as the integer residue rings [4, 5] and modular rings [6, 7] which are vital in studying BCH codes over QGRs. Shah et al. [8] discussed constructions of codes by the semigroup rings, which discussed new way of code construction and encoding techniques. Their work helps to increase the area of algebraic applications of BCH codes and construct them over QGR, enhancing the usability and reliability of error-correcting codes.

For achieving efficient error correction in finite field applications, Kim, Lee and Yoo [9] introduced an infinite family of Griesmer quasi-cyclic self-orthogonal codes. Their work shows that BCH codes are far better compared to QGRs in improving the coding efficiency and resilience in actual applications. Zullo [10] also discussed multi-orbit cyclic subspace codes and linear sets, which give more of the algebraic properties and the structures of cyclic codes. It is necessary to state that this research advances the knowledge of the theoretical background and real-world applications of BCH codes over various algebraic structures. Andrade and Palazzo [3] studied the construction and decoding of BCH codes over finite commutative rings that constituted the first step towards constructing the BCH code over rings other than the Galois fields. Their study stresses the ability to apply BCH codes in various algebraic settings, including possible over QGRs. Shankar [11] surveyed BCH codes over an arbitrary integer ring, extending the theory of BCH codes to other algebraic structures. The contribution of this research is useful in improving the reliability and usability of BCH codes in various communication and storage systems. Interlando and Palazzo [12] have given a structural description of cyclic code over $\mathbb{Z}_m$, and the decoding process in detail. Their research provides significant information regarding the enhancement of the BCH codes applied to the modular rings and other non-field structures,

as well as the possible use in the QGRs. Sajjad et al.'s [13–17] recent works have involved decoding algorithms that are designed to work on certain algebraic structures, including Gaussian fields, Eisenstein fields, quaternion integers, and octonion integers. These studies have substantially contributed to the improvement of the error correction capability of BCH codes as applicable to today's communication systems.

Lee, Li, Wu and Zeng [18] continued with the investigation of the hulls of primitive binary and ternary BCH codes with respect to particular structures that can improve code performance indicators. Their paper offers useful information about the enhancement of BCH codes in terms of performance for error correction and information reliability in implementation. In a work devoted to the description of specific properties and decoding of specific binary BCH codes of length $n = 2^m + 1$, Liu Li Fu Lu and Rao [19], this research with the collection of BCH codes which can be used for different communication schemes and data-storing methods. Further, new studies by different authors [20, 21] have explored details of BCH codes with the parameters and families of negacyclic and constacyclic BCH codes besides using them in cryptography and communication. These works present the continued research on the improvements of the additive BCH codes in terms of redundancy and code length in various algebraic structures.

Several studies have contributed significantly to the advancement of BCH codes and their decoding strategies. Asif and Shah [22] explored a computational approach to BCH codes and demonstrated their effectiveness in image encryption applications, showcasing the practical utility of algebraic coding in data security. Shah and Andrade [23] proposed a decoding method aimed at enhancing both the code rate and error correction capabilities, thereby improving the overall performance of BCH codes. Further, Shah, Qamar, and de Andrade [24] investigated the construction and decoding of BCH codes over a chain of commutative rings, providing an algebraic foundation for extending classical code structures. Additionally, Shah, Khan, and Andrade [25] introduced a novel decoding technique by embedding an n-length binary BCH code within a $n(n+1)$ -length cyclic code, allowing for improved decoding accuracy. These foundational works underscore the importance of algebraic generalizations and decoding efficiency in enhancing the reliability of BCH codes for modern communication systems. Furthermore, cyclic codes were compared by Shah and De Andrade [26] with the help of $B[X]$, $B\left[X, \frac{1}{p^k}Z_0\right]$, and $B\left[X, \frac{1}{kp}Z_0\right]$ pointing to further developments in constructing methods as well as decoding rules. Their work offers understanding on how to implement BCH code for certain algebraic structures, focusing on enhanced error correction and speed. Zhu, Li, and Zhu [27] identified parameters of two classes of negacyclic BCH codes, their structure, and decoding. Thus, the results of this research can be used to improve the efficiency and practical use of BCH codes in the field of cryptography and in digital communication systems. Wang, Sun and Ding [28] proposed two families of negacyclic BCH codes that were proved to be more powerful in correcting more errors and more reliable in data transmission. Citing their discoveries, they emphasize that BCH codes are applicable in any algebraic structure, which makes them useful in today's communication networks. Moreover, the research of Pang, Zhu, Yang, Gao, Zhou, Kai, and others [29, 30] focuses on BCH codes with a larger hull dimen-

sionality and ternary LCD consta-cyclic BCH codes. These have included broadening of the theoretical as well as practical applications of the BCH codes and, in addition, the improvements of the performance characteristics of BCH codes in extended communication networks.

An ever-evolving communication technology means that there is a constant need for enhanced methods of error correction for the effective transfer of data. BCH (Bose-Chaudhuri-Hocquenghem) codes have always been acknowledged for their suitability for error correction because of the clear algebraic structure of the code and the availability of efficient decoding procedures. However, the desire to make coding more efficient has resulted in the consideration of what is called codes over other algebraic structures like the integer residue rings and finite commutative rings [1, 31]. Therefore, the theory of quasi-Galois rings (QGRs) is a natural and quite a powerful generalization of the theory of Galois rings that could be useful for improving the BCH codes [1]. Compared to the previous Galois rings, QGRs have additional algebraic characteristics that make it possible to build BCH codes with higher error-correcting capability and code rate. These properties include an increased number of code words, which makes the BCH codes over QGRs more suitable for modern communication systems, and an improved code rate. New studies have established that it is possible to construct and decode BCH codes over QGRs. For instance, while applying Andrade and Palazzo's work on BCH codes over finite commutative rings, there has been a marked enhancement in the error correction efficiency [1]. Likewise, Shankar's work further extending the BCH codes over arbitrary integer rings has added more feathers in the hat of these codes in numerous applications [31]. These works form a base upon which further research can be conducted in order to better understand the characteristics of QGRs and the use of these groups in constructing BCH codes.

This article has important contributions to the domain of coding theory in order to implement BCH codes over Quasi-Galois Rings (QGRs) for enhancing the actual communication systems. From this, a comprehensive theoretical background for BCH codes over QGRs is presented to explain possible higher code rates and a larger number of code words compared to the use of Galois rings. Thus, the article demonstrates the practical applicability of the QGR-based BCH codes as a result of presenting novel construction methods and efficient decoding strategies. The enhanced understanding of these codes' theoretical and practical characteristics underlines their capability to dramatically improve the effectiveness and stability of today's communication networks in various applications. Thus, this investigation is expected to bring the BCH code over QGRs into light as potent and effective candidates to be incorporated in the advanced communication systems as well as contribute to the continuous improvement of coding methods in the modern world.

2. Preliminaries

This section consists of basic results that are useful to understand the upcoming sections [12–14, 18, 19, 26].

2.1. Quasi-Galois Ring

Let a Quasi-Galois Ring (Q-GR) be a local, finite, commutative ring with cardinality p^{rs} and characteristic p (where p is a prime and n, s are any positive integers). Particularly from the perspective of applications in coding theory, Q-GRs are highly intriguing because they possess the desirable attribute of having prime characteristics. It is denoted by and defined as

$$A(p^s, n) = \frac{\mathbb{F}_{p^s}[x]}{\langle x^n \rangle} = \left\{ \sum_{i=0}^{n-1} a_i \theta^i : a_i \in \mathbb{F}_{p^s} \right\} \tag{1}$$

where θ is a formal non-trivial root of the polynomial $x^n \in \mathbb{F}_{p^s}[x]$, i.e., $\theta^n = 0$.

2.2. Units in Q-GR

If $a_0 \neq 0$ in the expression,

$$\sum_{i=0}^{n-1} a_i \theta^i, \quad a_i \in \mathbb{F}_{p^s},$$

then the element is a unit in $A(p^s, n)$.

2.3. Nilpotent Elements in Q-GR

If $a_0 = 0$ in,

$$A(p^s, n) = \frac{\mathbb{F}_{p^s}[x]}{\langle x^n \rangle} = \left\{ \sum_{i=0}^{n-1} a_i \theta^i : a_i \in \mathbb{F}_{p^s} \right\},$$

then the element is nilpotent. If $a_0 = 1$, then it corresponds to a principal unit element.

Proposition 2.1. Let $A(p^s, n)$ be a Q-GR. Then the group of units in $A(p^s, n)$ is isomorphic to the direct product of two groups,

$$U(A(p^s, n)) \cong G_1 \times G_2,$$

where G_1 is a cyclic group of order $p^s - 1$, and G_2 is an Abelian p-group of order $p^s(n-1)$.

Particularly, if $s = 1$ and $n = 2$, then G_2 is a cyclic group of order p. While for $p = 2, s = 1, n = 3$, we have $G_2 \cong C_4$.

2.4. Ideal Structure of Q-GR

Since Q-GR is a local ring, it contains a unique maximal ideal, and the ring is given by:

$$A(p^s, n) = \frac{\mathbb{F}_{p^s}[x]}{\langle x^n \rangle} = \left\{ \sum_{i=0}^{n-1} a_i \theta^i : a_i \in \mathbb{F}_{p^s} \right\}, \quad \theta^n = 0.$$

Every proper ideal in Q-GR is of the form:

$$J_k = \theta^k A(p^s, n), \quad 1 \leq k \leq n-1.$$

3. BCH Code Construction over QGR

Before designing BCH codes over Q-GRs, it is necessary to specify the Galois extension of Q-GRs in order to factorize $x^n - 1$ over the group of units of the applicable extension ring of the known local ring (QGR) and then construct the generator polynomial for the BCH code.

3.1. Galois Extension of Q-GR $A(p^s, n)$

Let $A(p^s, n)$ be a class of local finite rings with a unique maximal ideal $\mathfrak{m}(p^s, n)$, and let the residue field be:

$$K = A(p^s, n)/\mathfrak{m}(p^s, n) \cong \mathbb{F}_{p^s}.$$

Consider the natural projection map,

$$\pi : A(p^s, n)[x] \to K[x],$$

where $A(p^s, n)[x]$ denotes the ring of polynomials in the variable x with coefficients from $A(p^s, n)$, and is defined by:

$$\pi(a(x)) = \overline{a(x)}.$$

If $f(x)$ is a monic polynomial of degree m such that $\pi(f(x))$ is irreducible over the residue field K, then $f(x)$ is irreducible over $A(p^s, n)$.

The ring

$$R = \frac{A(p^s, n)[x]}{\langle f(x) \rangle}$$

is called the Galois extension of the Q-GR $A(p^s, n)$, and consists of the collection of residue class polynomials in the variable x over $A(p^s, n)$, modulo the polynomial $f(x)$. The elements of R are of the form:

$$R = \left\{ \sum_{i=0}^{m-1} c_i \alpha^i : c_i \in A(p^s, n) \right\},$$

where α is a root of $f(x)$, i.e., $f(\alpha) = 0$.

Let R^* be the multiplicative Abelian group of the units of R, which can be expressed as the direct product of subgroups. A cyclic subgroup of R^* is denoted by G_s. The unit elements of R can be described as:

$$R^* = \left\{ x = c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} \in R : \exists c_i \in U(A(p^s, n)) \text{ for } i = 0, 1, \ldots, m-1 \right\},$$

where $U(A(p^s, n))$ indicates the group of units of the Q-GR $A(p^s, n)$.

On the other hand, the nilradical of R, denoted by $\mathrm{Nil}(R)$, is defined as:

$$\mathrm{Nil}(R) = \left\{ c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} : c_i \in \mathrm{Nil}(A(p^s, n)) \right\}.$$

Similarly, the extension of the residue field K of $A(p^s, n)$ is:

$$K' = \frac{(A(p^s, n)/\mathfrak{m}(p^s, n))[x]}{\langle \pi(f(x)) \rangle} = \frac{K[x]}{\langle \pi(f(x)) \rangle},$$

which has cardinality p^{ms}. The multiplicative group of units in K' is denoted by K'^*.

3.2. Generator Polynomial of BCH Codes using Maximal Cyclic Subgroup of Group Units of Q-GR

The generator polynomial of a BCH code of length n is defined as

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

where $m_i(x)$ are the minimal polynomials corresponding to each ψ^i, for $i = 1, 2, \ldots, d-1$.

The parity-check matrix H of the BCH code with the generator polynomial $g(x)$ is given by:

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

Equivalently, the code C is the null space of the matrix H.

The following steps are used to construct the generator polynomial of an n-length BCH code over a Galois ring:

(i) Create the maximal cyclic subgroup of the group of units of order n.

(ii) Compute the minimal polynomials for each design distance.

(iii) Find the least common multiple of all the minimal polynomials.

The pseudocode for construction of BCH codes over the Quasi-Galois ring is given in Algorithm 1.

Example 3.1: BCH Codes over $A(2, 2)$

Let $A(2, 2)$ be a Quasi-Galois ring (QGRs), defined as:

$$A(2,2) = \frac{\mathbb{F}_2[y]}{\langle y^2 \rangle} = \left\{ \sum_{i=0}^{1} a_i \theta^i : a_i \in \mathbb{F}_2,\ \theta^2 = 0 \mod 2 \right\} = \{a_0 + a_1\theta : a_0, a_1 \in \mathbb{F}_2 = \{0, 1\}\} = \{0, 1, \theta, 1+\theta\}.$$

The group of units in $A(2, 2)$ is:

$$U(A(2, 2)) = \{1, 1 + \theta\}.$$

Basic Irreducible Polynomial in $A(2, 2)[x]$: The residue field of $A(2, 2)$ is $\mathbb{F}_2$, and the natural projection is:

$$\pi : A(2, 2)[x] \to \mathbb{F}_2[x].$$

Case 1: Let $f(x) \in A(2, 2)[x]$ be a monic polynomial of degree 2 of the form:

$$f(x) = a_0 + a_1 x + x^2, \quad \text{where } a_0, a_1 \in A(2, 2).$$

Algorithm 1 Construction of BCH Codes over Q-Galois Rings (QGRs)

Require: Prime p, integers s, n, design distance d, offset c
Ensure: Generator polynomial $g(x)$ and parity-check matrix H

Step 1: Define the QGR and its Residue Field
Construct the QGR $A(p^s, n)$
Determine its maximal ideal $\mathfrak{m}(p^s, n)$
Compute the residue field $K = A(p^s, n)/\mathfrak{m}(p^s, n) \cong \mathbb{F}_{p^s}$
Step 2: Construct the Galois Extension
Select a monic polynomial $f(x) \in A(p^s, n)[x]$ such that $\pi(f(x)) \in K[x]$ is irreducible
Define the Galois extension ring:

$$R = \frac{A(p^s, n)[x]}{\langle f(x) \rangle}$$

Let α be a root of $f(x)$, so that $f(\alpha) = 0$
Step 3: Construct Maximal Cyclic Subgroup
Determine the unit group $R^* \subset R$
Identify a maximal cyclic subgroup $G_s \subset R^*$ of order n
Let $\psi \in G_s$ be a generator of this cyclic group
Step 4: Compute Minimal Polynomials
for $i = c$ to $c + d - 2$ **do**
    Compute the minimal polynomial $m_i(x)$ of ψ^i over $A(p^s, n)$
end for
Step 5: Construct the Generator Polynomial
Compute the least common multiple:

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

Step 6: Construct Parity-Check Matrix
Form matrix $H \in A(p^s, n)^{(d-1)\times n}$ with entries:

$$H_{i,j} = \psi^{(j-1)(c+i-1)} \quad \text{for } 1 \le i \le d-1,\ 1 \le j \le n$$

Step 7: Output Code Parameters
Return generator polynomial $g(x)$ and parity-check matrix H

Choose $a_0 = 1$, $a_1 = 1 + \theta$, then:

$$f(x) = x^2 + (1 + \theta)x + 1.$$

Now we check if $f(x)$ is irreducible over $A(2, 2)$. Its image under projection is:

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

which is a monic irreducible polynomial over $\mathbb{F}_2$. We now evaluate $f(x)$ at all possible elements of $A(2, 2)$:

$$f(0) = 1 \neq 0,$$
$$f(1) = 1 + (1 + \theta) + 1 = 1 + \theta \neq 0,$$

$$f(\theta) = \theta^2 + (1+\theta)\theta + 1 = 0 + \theta + 1 + 1 = \theta \neq 0,$$
$$f(1+\theta) = (1+\theta)^2 + (1+\theta)^2 + 1 = 1 + \theta + 1 + \theta + 1 = 1 \neq 0.$$

Thus, $f(x)$ is irreducible over $A(2,2)$ and hence is a basic irreducible polynomial.

Extension of $A(2,2)$ with Respect to $f(x)$: The Galois extension of $A(2,2)$ by the basic irreducible polynomial $f(x)$ is defined as:

$$R = \frac{A(2,2)[x]}{\langle f(x)\rangle} = \left\{ \sum_{i=0}^{1} c_i \alpha^i : c_i \in A(2,2) \right\},$$

where $f(x) = x^2 + (1+\theta)x + 1$ and $f(\alpha) = 0$.

Maximal Cyclic Subgroup of R^*: Given that α satisfies:

$$\alpha^2 = (1+\theta)\alpha + 1,$$

we compute the successive powers:

$$\begin{aligned}
\alpha^3 &= (1+\theta)\alpha^2 + \alpha = (1+\theta)((1+\theta)\alpha + 1) + \alpha = (1+\theta)^2\alpha + (1+\theta) + \alpha \\
&= \alpha + 1 + \theta + \alpha = 1 + \theta, \\
\alpha^4 &= \alpha \cdot \alpha^3 = \alpha(1+\theta) = (1+\theta)\alpha, \\
\alpha^5 &= \alpha \cdot \alpha^4 = \alpha \cdot (1+\theta)\alpha = (1+\theta)\alpha^2 = (1+\theta)((1+\theta)\alpha + 1) = \alpha + 1, \\
\alpha^6 &= \alpha \cdot \alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (1+\theta)\alpha + 1 + \alpha = 1.
\end{aligned}$$

So, the order of α is 6. The maximal cyclic subgroup $G_3 \subset R^*$ generated by $\gamma = \alpha^2$ is:

$$G_3 = \{\gamma, \gamma^2, \gamma^3 = 1\} = \{1 + (1+\theta)\alpha, (1+\theta)\alpha, 1\}.$$

Generator Polynomial of BCH Code over $A(2,2)$: Since γ is a primitive cube root of unity in G_3, and taking design distance $d = 3$, we need the minimal polynomials of γ^i for $i = 1, 2$. Both γ and γ^2 share the same minimal polynomial:

$$m_1(x) = (x - \gamma)(x - \gamma^2) = x^2 + x + 1.$$

Hence, the generator polynomial is:

$$g(x) = \text{lcm}(m_1(x), m_2(x)) = m_1(x) = x^2 + x + 1.$$

For $r = 2$, $q = 2$, and $m = 2$, the length of the narrow-sense primitive BCH code is:

$$n = q^m - 1 = 2^2 - 1 = 3.$$

The cyclic code C generated by $g(x)$ over $G_3 \subset R^* \subset A(2,2)$ has dimension 1. Thus, the BCH code C is a:

$[3, 1, 3]$ primitive narrow-sense BCH code over the maximal cyclic subgroup of the group of units in $A(2,2)$.

Case 2: BCH Codes over $A(2,2)$ with Degree 3 Extension

Let $f(x) \in A(2,2)[x]$ be a monic polynomial of degree 3, of the form:

$$f(x) = a_0 + a_1 x + x^3, \quad \text{where } a_0, a_1 \in A(2,2).$$

Choose $a_0 = 1$, $a_1 = 1 + \theta$, then:

$$f(x) = x^3 + (1+\theta)x + 1.$$

Under the natural projection $\pi : A(2,2)[x] \to \mathbb{F}_2[x]$, we get:

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

which is a monic irreducible polynomial over $\mathbb{F}_2$. We now verify the irreducibility of $f(x)$ over $A(2,2)$ by evaluating:

$$\begin{aligned} f(0) &= 1 \neq 0, \\ f(1) &= 1 + (1+\theta) + 1 = 1 + \theta \neq 0, \\ f(\theta) &= \theta^3 + (1+\theta)\theta + 1 = 0 + \theta + 1 + 1 = \theta \neq 0, \\ f(1+\theta) &= (1+\theta)^3 + (1+\theta)^2 + 1 = 1 + \theta \neq 0. \end{aligned}$$

Hence, $f(x)$ is a basic irreducible polynomial in $A(2,2)[x]$.

Extension of $A(2,2)$ with Respect to $f(x)$: Define the extension ring as:

$$R = \frac{A(2,2)[x]}{\langle f(x) \rangle} = \left\{ \sum_{i=0}^{2} c_i \alpha^i : c_i \in A(2,2) \right\},$$

where α is a root of $f(x)$, i.e., $f(\alpha) = 0$, implying:

$$\alpha^3 = (1+\theta)\alpha + 1.$$

Maximal Cyclic Subgroup of R^*: Since $f(x) = x^3 + (1+\theta)x + 1$ is basic irreducible and α is its root, the multiplicative group R^* has a cyclic subgroup G_7 of order 7 generated by $\gamma = \alpha^2$. Then:

$$G_7 = \{\gamma, \gamma^2, \ldots, \gamma^7 = 1\} = \{\alpha^2, \alpha + (1+\theta)\alpha^2, \ldots, 1\}.$$

This is isomorphic to the residue field:

$$K = \frac{\mathbb{F}_2[x]}{\langle \pi(f(x)) \rangle} = \frac{\mathbb{F}_2[x]}{\langle x^3 + x + 1 \rangle}.$$

Table 1: Multiplicative Group of Order 14

Exp.	Polynomial	Exp.	Polynomial
1	α	8	$\alpha + u\alpha^2$
2	α^2	9	$\alpha^2 + u\alpha + u$
3	$(1+u)\alpha + 1$	10	$\alpha^2 u + \alpha + 1$
4	$\alpha + (1+u)\alpha^2$	11	$\alpha^2 + (1+u)\alpha + u$
5	$\alpha^2 + \alpha + (1+u)$	12	$1 + \alpha + (1+u)\alpha^2$
6	$\alpha^2 + 1$	13	$\alpha^2 + u + 1$
7	$\alpha u + 1$	14	1

Generator Polynomial of BCH Code over $A(2,2)$: Since $\gamma = \alpha^2$ is a primitive cube root of unity in G_7, and for design distance $d = 3$, we need the minimal polynomials of γ^i for $i = 1, 2$.

Let $m_1(x)$ be the minimal polynomial of γ. Then $\gamma, \gamma^2, \gamma^4$ have the same minimal polynomial:

$$m_1(x) = (x - \gamma)(x - \gamma^2)(x - \gamma^4) = x^3 + x + 1.$$

Hence, the generator polynomial is:

$$g(x) = \text{lcm}\{m_1(x), m_2(x)\} = m_1(x) = x^3 + x + 1.$$

Given $r = 3$, $q = 2$, $m = 3$, and $c = 1$ (narrow-sense BCH code), the code length is:

$$n = q^m - 1 = 2^3 - 1 = 7.$$

The cyclic code C generated by $g(x)$ over $G_7 \subset R^* \subset A(2,2)$ has dimension 4. Thus, C is a:

$[7, 4, 3]$ primitive narrow-sense BCH code over the maximal cyclic subgroup of units in $A(2,2)$.

Case 3: BCH Codes over $A(2,2)$ with Degree 4 Extension

Let $f(x) \in A(2,2)[x]$ be a monic polynomial of degree 4:

$$f(x) = a_0 + a_1 x + x^4, \quad \text{where } a_0, a_1 \in A(2,2).$$

Choose $a_0 = 1$, $a_1 = 1 + \theta$, then:

$$f(x) = x^4 + (1+\theta)x + 1.$$

The projection map $\pi : A(2,2)[x] \to \mathbb{F}_2[x]$ gives:

$$\pi(f(x)) = x^4 + x + 1,$$

which is a monic irreducible polynomial over $\mathbb{F}_2$. We now verify irreducibility over $A(2,2)$:

$$\begin{aligned} f(0) &= 1 \neq 0, \\ f(1) &= 1 + (1+\theta) + 1 = 1 + \theta \neq 0, \\ f(\theta) &= \theta^4 + (1+\theta)\theta + 1 = \theta + \theta + 1 = 1 \neq 0, \\ f(1+\theta) &= (1+\theta)^4 + (1+\theta)^2 + 1 = 1 + \theta \neq 0. \end{aligned}$$

Thus, $f(x)$ is a basic irreducible polynomial in $A(2,2)[x]$.

Extension of $A(2,2)$ with Respect to $f(x)$: We define the Galois extension ring:

$$R = \frac{A(2,2)[x]}{\langle f(x) \rangle} = \left\{ \sum_{i=0}^{3} c_i \alpha^i : c_i \in A(2,2) \right\},$$

where $f(x) = x^4 + (1+\theta)x + 1$ and $f(\alpha) = 0$, hence:

$$\alpha^4 = (1+\theta)\alpha + 1.$$

Maximal Cyclic Subgroup of R^*: The multiplicative group R^* has a cyclic subgroup G_{15} of order 15 generated by $\gamma = \alpha^2$. This subgroup is isomorphic to the residue field:

$$K = \frac{\mathbb{F}_2[x]}{\langle \pi(f(x)) \rangle} = \frac{\mathbb{F}_2[x]}{\langle x^4 + x + 1 \rangle}.$$

Table 2: Cyclic Group of Order 30

Exp.	Polynomial	Exp.	Polynomial
1	α	16	$(1+u)\alpha$
2	α^2	17	$(1+u)\alpha^2$
3	α^3	18	$(1+u)\alpha^3$
4	$1 + (1+u\alpha)$	19	$(1+u) + \alpha$
5	$\alpha + (1+u\alpha^2)$	20	$(1+u)\alpha + \alpha^2$
6	$\alpha^2 + (1+u)\alpha^3$	21	$(1+u)\alpha^2 + \alpha^3$
7	$\alpha^3 + \alpha + 1 + u$	22	$1 + (1+u)\alpha + (1+u)\alpha^3$
8	$\alpha^2 + 1$	23	$(1+u) + (1+u)\alpha^2$
9	$\alpha^3 + \alpha$	24	$(1+u)\alpha + (1+u)\alpha^3$
10	$\alpha^2 + (1+u)\alpha + 1$	25	$(1+u) + \alpha + (1+u)\alpha^2$
11	$\alpha^3 + (1+u)\alpha^2 + \alpha$	26	$(1+u)\alpha + \alpha^2 + (1+u)\alpha^3$
12	$(1+u)\alpha^3 + \alpha^2 + (1+u)\alpha + 1$	27	$(1+u) + \alpha + (1+u)\alpha^2 + \alpha^3$
13	$\alpha^3 + (1+u)\alpha^2 + (1+u)$	28	$1 + \alpha^2 + (1+u)\alpha^3$
14	$(1+u)\alpha^3 + 1$	29	$(1+u) + \alpha^3$
15	$1+u$	30	1

Generator Polynomial of BCH Code over $A(2,2)$: Since $\gamma = \alpha^2$ is a primitive cube root of unity in G_{15}, for design distance $d = 3$, we need the minimal polynomials of γ^i, $i = 1, 2$.

Let $m_1(x)$ be the minimal polynomial of γ. Then $\gamma, \gamma^2, \gamma^4, \gamma^8$ all share the same minimal polynomial:

$$m_1(x) = (x-\gamma)(x-\gamma^2)(x-\gamma^4)(x-\gamma^8) = x^4 + x + 1.$$

Therefore, the generator polynomial is:

$$g(x) = \text{lcm}\{m_1(x), m_2(x)\} = m_1(x) = x^4 + x + 1.$$

Given $r = 4$, $q = 2$, $m = 4$, and $c = 1$, the code length is:

$$n = q^m - 1 = 2^4 - 1 = 15.$$

The cyclic code C generated by $g(x)$ over $G_{15} \subset R^* \subset A(2,2)$ has dimension 11. Hence, C is a:

$[15, 11, 3]$ primitive narrow-sense BCH code over the maximal cyclic subgroup of units in $A(2,2)$.

4. Decoding of BCH Codes over QGRs and Their Significance [13, 14, 16]

4.1. Decoding of BCH Codes using Advanced Modified Berlekamp–Massey Algorithm

Let C be a BCH code with length n, designed distance d, and received vector r. Let S denote the syndrome vector, computed as the multiplication of the parity-check matrix H and the transpose of the received vector:

$$S = Hr^t.$$

Apply the Advanced Modified Berlekamp–Massey Algorithm (AMBMA) to find the error-locator polynomial $\delta^n(x)$ under the following initial conditions:

$$d_{-1} = 1, \quad \delta^{-1}(x) = 1, \quad l_{-1} = 0, \quad l_0 = 0, \quad \delta^0(x) = 1, \quad d_0 = \text{first non-zero syndrome.}$$

Let d_n represent the discrepancy at iteration n. If $d_n = 0$ or is a zero divisor, then:

$$\delta^n(x) = \delta^{n+1}(x), \quad l_n = l_{n+1}.$$

If d_n is a nonzero unit element, choose $m \leq n-1$ such that $n - l_m$ is the largest or equal to the last column index satisfying the update condition. From $d_n - yd_m = 0$, compute y, and update the error-locator polynomial as:

$$\delta^{n+1}(x) = \delta^n(x) - yx^{n-m}\delta^m(x).$$

The next discrepancy is given by:

$$d_{n+1} = S_{n+2} + \delta_1^{(n+1)} S_{n+1} + \delta_2^{(n+1)} S_n + \cdots + \delta_{l_{n+1}}^{(n+1)} S_{n+2-l_{n+1}}.$$

Next, compute the reciprocal polynomial $g(x)$ of $\delta^n(x)$, and find its roots in the form x_u. These roots correspond to the error locations. Choose elements z_u such that $(z_u - x_u)$ are either zero or zero divisors, where $1 \leq u \leq n-1$ and $x_u = \alpha^u$.

Now construct the error-locator polynomial using the elementary symmetric function:

$$(x - z_1)(x - z_2) \cdots (x - z_v) = \delta_0 x^v + \delta_1 x^{v-1} + \cdots + \delta_v,$$

where $z_1, z_2, \ldots, z_v$ represent the v error locations.

Using Forney's algorithm [13, 14, 16], compute the error magnitudes y_j as:

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

where the recurrence relation for $\delta_{j,u}$ is:

$$\delta_0 = \delta_{j,0} = 1, \quad \delta_{j,u} = \delta_u + x_j \cdot \delta_{j,u-1}, \quad u = 1, 2, \ldots, v-1, \quad j = 1, 2, \ldots, v.$$

The final error vector e is obtained, and the corrected codeword is:

$$c = r - e.$$

The pseudocode for the decoding of BCH codes over the Quasi-Galois ring using AMBMA is given in Algorithm 2.

Example 4.1

Let $(7, 4, 3)$ be a BCH code over the QGRs $A(2, 2)$ as described in Section 4, and let the received vector be

$$r = (0, 0, 0, \ldots, \alpha^2 u + \alpha + 1)_{1\times 7}.$$

Compute the syndrome vector S as:

$$S = Hr^T = \begin{pmatrix} 1 & \gamma & \gamma^2 & \cdots & \gamma^6 \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{12} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ \alpha^2 u + \alpha + 1 \end{pmatrix} = \begin{pmatrix} \gamma^{11} \\ \gamma^{12} \end{pmatrix} = \begin{pmatrix} \gamma^4 \\ \gamma^3 \end{pmatrix} = \begin{pmatrix} \alpha + u\alpha^2 \\ \alpha^2 + 1 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix}.$$

Apply the AMBMA to determine $\delta^n(x)$ using the iteration steps shown in Table 3.

Algorithm 2 Decoding BCH Codes over Quasi-Galois Rings (QGRs)

Require: Parity-check matrix H, received vector r, designed distance d
Ensure: Corrected codeword c

Compute the syndrome vector: $S \leftarrow H \cdot r^T$
Initialize:

- $\delta^{-1}(x) \leftarrow 1$, $\delta^0(x) \leftarrow 1$
- $d_{-1} \leftarrow 1$, $d_0 \leftarrow$ first non-zero entry in S
- $l_{-1} \leftarrow 0$, $l_0 \leftarrow 0$

for $n = 0$ to $2t - 1$ **do** ▷ $t = \lfloor \frac{d-1}{2} \rfloor$
  if $d_n = 0$ or d_n is a zero divisor **then**
    $\delta^{n+1}(x) \leftarrow \delta^n(x)$
    $l_{n+1} \leftarrow l_n$
  else
    Choose $m \leq n-1$ such that $(n - l_m)$ is maximal
    Compute $y \leftarrow d_n/d_m$
    Update $\delta^{n+1}(x) \leftarrow \delta^n(x) - yx^{n-m}\delta^m(x)$
    $l_{n+1} \leftarrow \max(l_n, l_m + n - m)$
  end if
  Compute next discrepancy:

$$d_{n+1} = S_{n+2} + \delta_1^{(n+1)} S_{n+1} + \cdots + \delta_{l_{n+1}}^{(n+1)} S_{n+2-l_{n+1}}$$

end for
Compute reciprocal polynomial $g(x)$ of $\delta^n(x)$
Find roots x_u of $g(x)$
Select z_u such that $(z_u - x_u)$ is zero or a zero divisor
Construct elementary symmetric polynomial:

$$(x - z_1)(x - z_2)\cdots(x - z_v) = \delta_0 x^v + \delta_1 x^{v-1} + \cdots + \delta_v$$

for $j = 1$ to v **do**
  $\delta_{j,0} \leftarrow 1$
  for $u = 1$ to $v - 1$ **do**
    $\delta_{j,u} \leftarrow \delta_u + x_j \cdot \delta_{j,u-1}$
  end for
  Compute error magnitude using Forney's formula:

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

end for
Initialize error vector $e \leftarrow \mathbf{0}$
for each error location z_j with magnitude y_j **do**
  $e[\text{position}(z_j)] \leftarrow y_j$
end for 2
Compute corrected codeword: $c \leftarrow r - e$
return c

Table 3: AMBMA for finding the linear polynomial

Iterations	$\boldsymbol{\delta^n(x)}$	$\boldsymbol{d_n}$	$\boldsymbol{l_n}$	$\boldsymbol{n - l_n}$
-1	1	1	0	-1
0	1	$\alpha + u\alpha^2$	0	0
1	$1 + \gamma^4 x$	1	1	0
2	$1 + \gamma^6 x$			

Thus, it follows that:

$$\delta^2(x) = 1 + \gamma^6 x,$$

and the reciprocal function is $g(x) = \gamma^6 + x$.

The root of $g(x)$ is γ^6, which indicates the error is located at position 7 in the received

vector r. The error-locator polynomial

$$\delta_0 x^v + \delta_1 = x - \gamma^6$$

is a symmetric function for $v = 1$.

Compute the error magnitude using Forney's formula,

$$y_1 = \frac{\delta_{1,0} S_1}{\delta_{1,0} x_1} = \frac{S_1}{z_1} = \frac{\gamma^4}{\gamma^6} = \gamma^5 = \alpha^2 u + \alpha + 1,$$

where $\delta_0 = 1$, $\delta_1 = -\alpha^2 u - \alpha - 1$, and $v = 1$.

Therefore, the error vector is:

$$e = (0, 0, 0, \ldots, \alpha^2 u + \alpha + 1),$$

and the corrected codeword is:

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

Example 4.2

Let $(15, 11, 3)$ be a BCH code over the QGRs $A(2, 2)$ as described in Section 4, and let the received vector be

$$r = (0, (1+u)\alpha, 0, 0, \ldots, 0)_{1\times 15}.$$

Compute the syndrome vector S as:

$$S = Hr^T = \begin{pmatrix} 1 & \gamma & \gamma^2 & \cdots & \gamma^{14} \\ 1 & \gamma^2 & \gamma^4 & \cdots & \gamma^{28} \end{pmatrix} \begin{pmatrix} 0 \\ (1+u)\alpha \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} (1+u)\alpha^3 \\ (1+u)\alpha + \alpha^2 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} \gamma^9 \\ \gamma^{10} \end{pmatrix}.$$

Apply the AMBMA to determine $\delta^n(x)$ using the iteration steps shown in Table 4.

Table 4: AMBMA for finding the polynomial

Iterations	$\boldsymbol{\delta^n(x)}$	$\boldsymbol{d_n}$	$\boldsymbol{l_n}$	$\boldsymbol{n - l_n}$
-1	1	1	0	-1
0	1	$(1+u)\alpha^3$	0	0
1	$1 + \gamma^9 x$	$(1+u)\alpha + (1+u)\alpha^3$	1	0
2	$1 + \gamma x$			

Hence, we find:

$$\delta^2(x) = 1 + \gamma x,$$

and the reciprocal function is $g(x) = \gamma + x$.

The root of $g(x)$ is γ, indicating that the error occurred at a position 2 in the received vector r. The symmetric form of the error-locator polynomial is:

$$\delta_0 x^v + \delta_1 = x - \gamma,$$

where $v = 1$.

Using Forney's formula, compute the error magnitude

$$y_1 = \frac{\delta_{1,0} S_1}{\delta_{1,0} x_1} = \frac{S_1}{z_1} = \frac{\gamma^9}{\gamma} = \gamma^8 = \alpha^{16} = (1+u)\alpha,$$

where $\delta_0 = 1$, $\delta_1 = -(1+u)\alpha$, and $v = 1$.

Therefore, the error vector is

$$e = (0, (1+u)\alpha, 0, 0, \ldots, 0),$$

and the corrected codeword is:

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

4.2. Significance of Quasi-Galois Ring-Based BCH Code Construction and Decoding in Modern Data Transmission

The use of Quasi-Galois Rings (QGRs) in the construction and decoding of BCH codes marks a significant advancement in the field of error-correcting codes, particularly for modern data transmission applications. QGRs extend the algebraic framework of classical Galois rings, enabling richer structural properties that lead to greater design flexibility. This allows for BCH codes with improved minimum distances, larger codeword sets, and higher code rates—key features for ensuring data integrity in bandwidth-intensive and noise-prone communication environments such as satellite systems, mobile networks, and high-density data storage devices. Moreover, the decoding strategies developed for BCH codes over QGRs enhance the reliability and speed of error correction. These methods exploit the algebraic depth of QGRs to support efficient syndrome computation and error location, making them suitable for real-time and low-latency systems. As data communication continues to evolve, especially with emerging technologies requiring robust and scalable coding schemes, QGR-based BCH codes offer a future-ready solution by balancing strong theoretical foundations with practical performance benefits.

5. Comparison and Discussion

This section provides a comparative analysis of BCH codes over Galois rings [3] and Quasi-Galois Rings (QGRs). Let the parameters be as follows: code length n, designed distance d, dimensions k_1 and k_2, code rates R_1 and R_2, and the number of codewords q^k for BCH codes defined over Galois rings $\mathrm{GR}(p^n, s)$ and Quasi-Galois rings $\mathcal{A}(p^s, n)$. Comparative results using the examples $\mathrm{GR}(2, 2)$ and $\mathcal{A}(2, 2)$ are summarized in Tables 5

Table 5: Code analysis of BCH codes over Galois rings GR$(2, 2)$

Characteristic	n	d	k	2^k	R_1
2	3	3	1	2^1	0.3333

Table 6: Code analysis of BCH codes over Quasi-Galois rings $\mathcal{A}(2, 2)$

Characteristic	n	d	k	2^k	R_2
2	15	3	11	2^{44}	0.7333
2	15	5	7	2^{28}	0.4647
2	15	7	5	2^{20}	0.3333
2	15	9	1	2^4	0.0667
2	15	11	1	2^4	0.0667
2	15	13	1	2^4	0.0667

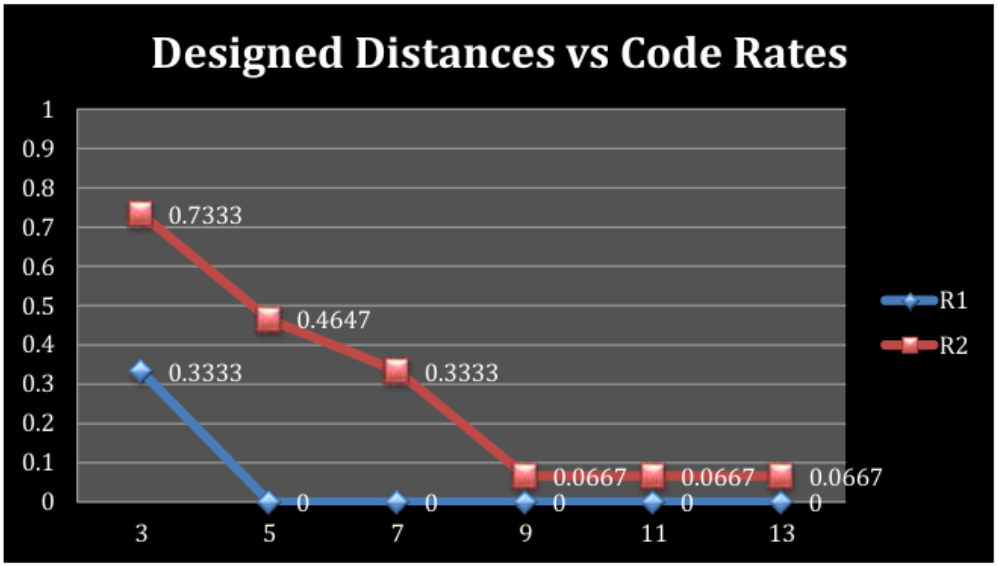

Figure 1: Designed distances vs. Code rates of BCH codes over GR$(2, 2)$ and $\mathcal{A}(2, 2)$

and 6. Furthermore, graphical comparisons of the designed distances, code rates, and dimensions are shown in Figures 1 and 2.
From the analysis above, we observe the following:

- In the case of the Galois ring GR$(2, 2)$, only one possibility exists for constructing BCH codes, whereas six distinct possibilities are available for $\mathcal{A}(2, 2)$.
- The maximum code length achievable over GR$(2, 2)$ is 3, while for $\mathcal{A}(2, 2)$ it is 15.
- Designed distance values for BCH codes over $\mathcal{A}(2, 2)$ range from 3 to 13, whereas for GR$(2, 2)$ it is only 3. This indicates that BCH codes over Quasi-Galois rings offer superior error-correction capabilities.

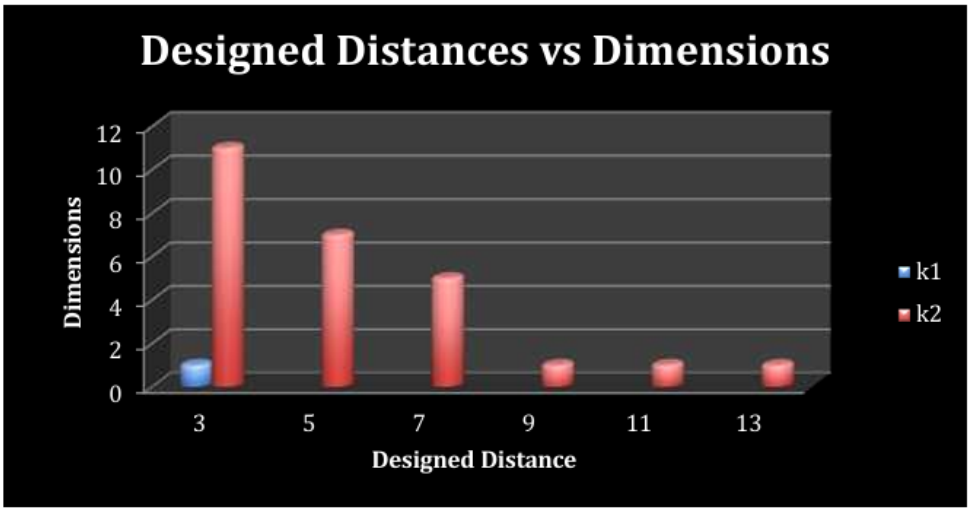

Figure 2: Designed distances vs. Dimensions of BCH codes over $\mathrm{GR}(2,2)$ and $\mathcal{A}(2,2)$

- Furthermore, the number of codewords over $\mathcal{A}(2,2)$ is significantly larger than that of BCH codes over $\mathrm{GR}(2,2)$, enhancing their usefulness in applications requiring higher data capacity and reliability.

6. Conclusions and Future Directions

The study of BCH codes over Quasi-Galois Rings (QGRs), as presented in this article, demonstrates their strong potential in enhancing modern communication systems. Through a comprehensive analysis of the underlying theoretical foundations, construction methodologies, and decoding algorithms, it is evident that the extended algebraic structure and intrinsic properties of QGRs contribute significantly to improving both code rates and the total number of codewords. These enhanced attributes translate into superior error correction capabilities, making QGR-based BCH codes promising candidates for contemporary and next-generation communication technologies. The ability to construct longer codes with greater flexibility and efficiency over QGRs, as compared to classical Galois rings, further substantiates their relevance.

Future research can be directed toward refining the construction and decoding processes of BCH codes over QGRs, with a focus on optimizing algorithmic complexity and implementation feasibility. Additionally, exploring the practical deployment of QGR-based codes in real-world communication systems could provide valuable insights into their performance under practical constraints. Another promising direction involves the integration of BCH codes over QGRs with higher layers of coding and modern cryptographic protocols. Such hybrid approaches may lead to more robust and secure communication architectures. Therefore, building upon the findings of this article, the continued development of BCH codes over Quasi-Galois Rings can significantly contribute to the advancement of reliable and efficient communication networks.

Acknowledgements

This research is supported by Universidad Pedagógica y Tecnológica de Colombia (SGI 3725) and Minciencias (Conv. 934).

Data availability

All the data is given in this study.

Tribute

We would like to express our heartfelt gratitude to our beloved supervisor, Professor Dr. Tariq Shah (late), whose exceptional guidance, profound expertise, and steadfast support were instrumental in shaping our academic journey. His mentorship not only nurtured our growth as researchers in algebra, number theory, coding theory, and cryptography but also profoundly influenced our personal and professional development. His legacy of wisdom, integrity, and inspiration continues to guide us. May his soul rest in eternal peace.

Figure 3: Prof. Dr. Tariq Shah

References

[1] E. F. Jr. Assmus and H. F. Mattson. Error-correcting codes: An axiomatic approach. *Information and Control*, 6(4):315–330, 1963.

[2] D. Augot, E. Betti, and E. Orsini. An introduction to linear and cyclic codes. In *Gröbner Bases, Coding, and Cryptography*, pages 47–68. Springer, 2009.
[3] A. A. De Andrade and R. Jr. Palazzo. Construction and decoding of bch codes over finite commutative rings. *Linear Algebra and Its Applications*, 286(1–3):69–85, 1999.
[4] I. F. Blake. Codes over certain rings. *Information and Control*, 20(4):396–404, 1972.
[5] I. F. Blake. Codes over integer residue rings. *Information and Control*, 29(4):295–300, 1975.
[6] E. Spiegel. Codes over zm. *Information and Control*, 35(1):48–51, 1977.
[7] E. Spiegel. Codes over zm, revisited. *Information and Control*, 37(1):100–104, 1978.
[8] T. Shah, A. Khan, and A. A. de Andrade. Constructions of codes through the semigroup ring b [x; 122z0] and encoding. *Computers & Mathematics with Applications*, 62(4):1645–1654, 2011.
[9] B. Kim, Y. Lee, and J. Yoo. An infinite family of griesmer quasi-cyclic self-orthogonal codes. *Finite Fields and Their Applications*, 76:101923, 2021.
[10] F. Zullo. Multi-orbit cyclic subspace codes and linear sets. *Finite Fields and Their Applications*, 87:102153, 2023.
[11] P. Shankar. On bch codes over arbitrary integer rings (corresp.). *IEEE Transactions on Information Theory*, 25(4):480–483, 1979.
[12] J. C. Interlando and R. Palazzo Jr. A note on cyclic codes over zm. *Latin Amer. Appl. Res*, 25:83–85, 1995.
[13] M. Sajjad, T. Shah, M. Alammari, and H. Alsaud. Construction and decoding of bch-codes over the gaussian field. *IEEE Access*, pages 1–8, 2023.
[14] M. Sajjad, T. Shah, Q. Xin, and B. Almutairi. Eisenstein field bch codes construction and decoding. *AIMS Mathematics*, 8(12):29453–29473, 2023.
[15] M. Sajjad, T. Shah, M. M. Hazzazi, A. R. Alharbi, and I. Hussain. Quaternion integers based higher length cyclic codes and their decoding algorithm. *Computers, Materials & Continua*, 73(1):1–17, 2022.
[16] 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.
[17] M. Sajjad, T. Shah, R. J. Serna, Z. E. Suárez Aguilar, and O. S. Delgado. Fundamental results of cyclic codes over octonion integers and their decoding algorithm. *Computation*, 10(12):219, 2022.
[18] Y. Lei, C. Li, Y. Wu, and P. Zeng. More results on hulls of some primitive binary and ternary bch codes. *Finite Fields and Their Applications*, 82:102066, 2022.
[19] Y. Liu, R. Li, Q. Fu, L. Lu, and Y. Rao. Some binary bch codes with length n= 2ˆm+ 1. *Finite Fields and Their Applications*, 55:109–133, 2019.
[20] S. R. Nagpaul. *Topics in Applied Abstract Algebra*, volume 15. American Mathematical Society, 2005.
[21] A. A. De Andrade and T. Shah. Goppa codes through polynomials of b [x;(1/2$\hat{2}$) z_0] and its decoding principle. *Journal of Advanced Research in Applied Mathematics*, pages 12–20, 2011.
[22] M. Asif and T. Shah. Bch codes with computational approach and its applications in

image encryption. *Journal of Intelligent & Fuzzy Systems*, 37(3):3925–3939, 2019.

[23] T. Shah and A. A. D. Andrade. A decoding procedure which improves code rate and error corrections. *JARAM*, 4(4):37–50, 2012.

[24] T. Shah, A. Qamar, and A. A. de Andrade. Construction and decoding of bch codes over chain of commutative rings. *Mathematical Sciences*, 6(1):51, 2012.

[25] T. Shah, M. Khan, and A. A. D. Andrade. A decoding method of an n length binary bch code through $(n+1)n$ length binary cyclic code. *Anais da Academia Brasileira de Ciências*, 85(3):863–872, 2013.

[26] T. Shah and A. A. De Andrade. Cyclic codes through $b[x]$, $b\left[x, \frac{1}{p^k}z_0\right]$, and $b\left[x, \frac{1}{kp}z_0\right]$, and: A comparison. *Journal of Algebra and its Applications*, 11(04):1250078, 2012.

[27] H. Zhu, J. Li, and S. Zhu. Parameters of two classes of negacyclic bch codes. *Journal of Applied Mathematics and Computing*, 69(6):4353–4380, 2023.

[28] X. Wang, Z. Sun, and C. Ding. Two families of negacyclic bch codes. *Designs, Codes and Cryptography*, 91(7):2395–2420, 2023.

[29] B. Pang, S. Zhu, T. Yang, and J. Gao. Bch codes with larger dimensional hull. *Designs, Codes and Cryptography*, 91(12):3933–3951, 2023.

[30] Y. Zhou, X. Kai, and S. Zhu. Two classes of ternary lcd constacyclic bch codes. *Cryptography and Communications*, 15(5):905–919, 2023.

[31] R. E. Blahut. *Algebraic Codes for Data Transmission*. Cambridge University Press, 2003.