American Journal of Information Science and Technology (AJIST)
2026; 10(1): 15-24
http://www.sciencepublishinggroup.com/j/ajist
doi: 10.11648/j.ajist.20261001.13

A Novel Approach to Constructing Certain Classes of Quasi-Cyclic Codes

Akram Saleh*, Mohammad Reza Soleymani

Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

Email address:

akram.saleh@concordia.ca (Akram Saleh), reza.soleymani@concordia.ca (Mohammad Reza Soleymani)
*Corresponding author

To cite this article:

Akram Saleh, Mohammad Reza Soleymani. (2026). A Novel Approach to Constructing Certain Classes of Quasi-Cyclic Codes, *American Journal of Information Science and Technology, 10*(1), 15-24. https://doi.org/10.11648/j.ajist.20261001.13

Received: 15 December 2025; **Accepted:** 26 December 2025; **Published:** 20 January 2026

Abstract: This paper investigates a construction algorithm for two specific families of quasi-cyclic codes defined over a finite commutative chain ring. First, by employing the Generalized Discrete Fourier Transform, we develop an efficient and systematic algorithm for constructing the generator matrix of repeated-root quasi-cyclic codes under specific structural constraints on the code length and the underlying ring. The proposed method avoids the need for exhaustive enumeration of constituent subcodes and instead operates directly on their generator matrices, leading to improved computational performance. Building on this result, using the Discrete Fourier Transform, we further specialize the proposed framework to derive an algorithm for obtaining the generator matrix of a particular class of simple-root quasi-cyclic codes over a restricted and well-defined category of rings. This specialization demonstrates the performance of the proposed approach and highlights its applicability to different quasi-cyclic code structures in a unified algebraic setting. The proposed construction methods offer significant improvements in computational efficiency when compared to existing approaches that rely on code construction techniques based on constituent subcodes. To evaluate the practical benefits of the proposed algorithms, we present a detailed performance comparison in terms of encoding time per iteration and memory consumption. The comparative results, illustrated through histograms, clearly indicate that the proposed methods achieve faster encoding, lower memory usage, highlighting their superior performance compared to conventional construction techniques as the code length increases.

Keywords: Quasi-cyclic Codes, Repeated-root Codes, Simple-root Codes, Chain Rings, Discrete Fourier Transform

1. Introduction

Quasi-cyclic (QC) codes generalize cyclic codes and constitute an important and broad class of error-correcting codes that have been extensively studied in the literature [1–7]. Owing to their rich algebraic structure, QC codes are of significant interest both from a theoretical perspective and for practical applications.

The study of algebraic properties of linear codes over rings, particularly finite chain rings, has attracted considerable attention. This interest stems not only from their intrinsic theoretical significance but also from the fact that codes over rings provide valuable insights into the study of linear codes over finite fields. There are two main reasons for this connection. First, any finite field can be viewed as a special case of a finite chain ring. Second, several works have demonstrated that codes over rings can be mapped to optimal or near-optimal codes over finite fields via suitable Gray maps [8, 9].

Motivated by these observations, we investigate in this paper the structure of a certain class of QC codes over finite commutative chain rings, denoted by R. The ring R possesses a unique maximal ideal, generated by a fixed element γ. The residue field of R modulo its maximal ideal $\langle\gamma\rangle$ is denoted by $\mathbb{F}_q = R/\langle\gamma\rangle$ and q is defined as the characteristic of the ring R.

A linear code of length n over R is defined as an R-submodule of R^n. The notions of cyclic and QC codes over rings extend naturally from their counterparts over finite fields.

A code is said to be cyclic if it is invariant under cyclic shifts of its codewords. A code is called quasi-cyclic if it is invariant under cyclic shifts of blocks of equal length ℓ. Consequently, the length n of a QC code is a multiple of its index ℓ, and we define the co-index of the code as $m := n/\ell$ [10].

QC codes can be broadly classified into two main categories. When the co-index m is coprime to the characteristic of the underlying ring, the code belongs to the class of *simple-root* QC codes. In contrast, when the co-index is divisible by the characteristic of the ring, the code is referred to as a *repeated-root* QC code.

The algebraic structures of both simple-root and repeated-root QC codes have been extensively investigated by Ling *et al.*, with results reported in a sequence of influential works [10–12]. These seminal contributions laid the foundation for further research on QC codes and introduced broader families known as quasi-twisted (QT) codes. QT codes have been shown to be closely related to QC codes from an algebraic standpoint and, under certain conditions, provide a useful framework for simplifying the structure and analysis of repeated-root QC codes [5, 13, 14].

San Ling and Patrick Sole were among the first to study simple-root quasi-cyclic (QC) codes over finite fields by interpreting them as linear codes over an intermediate ring. Using the Discrete Fourier Transform (DFT), this ring can be decomposed into a direct product of coprime component rings, which enables the construction of QC codes from shorter-length constituent codes [10]. This framework was later extended to QC codes over finite chain rings and to repeated-root QC codes over finite fields [11]. A further generalization to repeated-root QC codes over rings was subsequently developed by employing the Generalized Discrete Fourier Transform (GDFT) [12].

The central idea underlying this series of works is the development of construction algorithms that generate QC codewords from the codewords of their constituent codes. However, as the length of a QC code increases, the computational complexity of such codeword-based construction algorithms grows rapidly. Motivated by this limitation, subsequent research sought to generalize and refine these approaches in order to reduce construction complexity, which also led to the discovery of several record-breaking codes in terms of minimum distance [6].

Building upon these prior studies, the present work advances the existing methodology by proposing algorithms that directly construct the generator matrices of QC codes from the generator matrices of their component codes. By avoiding explicit codeword generation, the proposed approach significantly improves computational efficiency and enables the construction process to be carried out entirely at the level of generator matrices.

This work investigates two types of QC codes over a finite chain ring R with characteristic q and proposes generator matrix construction algorithms for each. The two classes of codes are described as follows:

1. *Repeated-root QC codes:* These are QC codes whose generator polynomials have roots with multiplicity greater than one. We consider codes of length $n = \ell m$, where m is an even integer written as $m = 2m'$, and m' is an odd number. We assume that $q = 2^t$, and the condition $ord_{m'}(2^t) = m' - 1$ is held.
2. *Simple-root QC codes:* These are QC codes whose generator polynomials have only simple roots (i.e., multiplicity one). Their length is also $n = \ell m$, and we assume that $ord_m(q) = m - 1$.

The remainder of this paper is organized as follows. In Section 2, we introduce fundamental concepts and notations. Section 3 provides a detailed investigation into repeated-root QC codes and presents a generator matrix for a specific class of these codes. Section 4 focuses on simple-root QC codes and describes an algorithm for constructing their generator matrices. In Section 5, we evaluate the efficiency of our proposed algorithms in comparison with traditional approaches, analyzing encoding time per iteration and memory usage. Finally, Section 6 concludes the paper with a summary of our findings.

2. Preliminary Concepts

Throughout this paper, let R be a finite commutative chain ring with identity, where γ is a fixed generator of its maximal ideal. The residue field of R, denoted by $\mathbb{F}$, is given by $\mathbb{F} = R/\langle\gamma\rangle$, with $|\mathbb{F}| = q$, where q is a power of a prime number.

The natural ring homomorphism $^-$is defined as

$$^-\colon R \to \mathbb{F} = R/\langle\gamma\rangle, \quad a \mapsto a + \langle\gamma\rangle, \quad \forall a \in R,$$

which can be extended to a ring homomorphism from $R[x]$ to $\mathbb{F}[x]$ as follows:

$$\forall f = \sum a_k x^k \in R[x], \text{ where } a_k \in R, \quad \bar{f} = \sum \bar{a}_k x^k.$$

A monic polynomial $f \in R[x]$ is termed *monic basic irreducible* (primitive) over R if $\bar{f}$ is an irreducible (primitive) polynomial over $\mathbb{F}$.

If $f(x)$ is a monic basic irreducible polynomial of degree m over R, the quotient ring $\mathcal{R} := R[x]/\langle f(x)\rangle$ is known as the *m-th Galois extension ring* of R. The ring $\mathcal{R}$ is itself a finite chain ring with maximal ideal $\langle\gamma\rangle$. If ζ is a root of $f(x)$, then $\mathcal{R} = R[\zeta]$, and $\mathcal{R}$ forms a free module of rank m over R with the basis $\{1, \zeta, \ldots, \zeta^{m-1}\}$.

The following well-known result characterizes finite commutative chain rings [15].

Proposition 2.1. Let R be a finite commutative chain ring with maximal ideal $M = \langle\gamma\rangle$ and residue field $\mathbb{F} = R/\langle\gamma\rangle$. Then, for some prime p and positive integers k and t (where $k \geq t$), the orders of R and $\mathbb{F}$ are given by $|R| = p^k$ and $|\mathbb{F}| = p^t$, respectively. In other words, the characteristic of both R and $\mathbb{F}$ is a power of p.

A fundamental result in this context is Hensel's lemma, which ensures that the factorization of a polynomial over $\mathbb{F}$ can be lifted to R under suitable conditions.

Lemma 2.1 ([15]). Let f be a polynomial over R, and assume that its factorization modulo $\langle\gamma\rangle$ factors as $\bar{f} = g_1 g_2 \cdots g_r$, where $g_1, g_2, \ldots, g_r$ are pairwise coprime

polynomials over $\mathbb{F}$. Then, there exist pairwise coprime polynomials $f_1, f_2, \ldots, f_r$ over R such that

$$f = f_1 f_2 \cdots f_r, \quad \text{and} \quad \bar{f}_i = g_i, \quad \forall i = 1, 2, \ldots, r.$$

A linear code of length n over R is an R-submodule of R^n. A *generator matrix* G of C is a matrix whose rows form a minimal set of generators for C. Since C is not necessarily a free R-module, the rows of G may not be linearly independent over R.

A linear code C over R is called *cyclic* if, for every codeword $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the cyclic shift $(c_{n-1}, c_0, \ldots, c_{n-2})$ also belongs to C. Extending this idea leads to quasi-cyclic (QC) codes.

Definition 2.1. A linear code C of length $n = \ell m$ over R is called an ℓ-QC code if, for each codeword

$$\begin{aligned} c = (&c_{00}, c_{01}, \ldots, c_{0,\ell-1}, \\ &c_{10}, c_{11}, \ldots, c_{1,\ell-1}, \\ &\cdots, \\ &c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,\ell-1}) \in C, \end{aligned}$$

the vector

$$\begin{aligned} (&c_{m-1,0}, c_{m-1,1}, \ldots, c_{m-1,\ell-1}, \\ &c_{00}, c_{01}, \ldots, c_{0,\ell-1}, \\ &\cdots, \\ &c_{m-2,0}, c_{m-2,1}, \ldots, c_{m-2,\ell-1}) \end{aligned}$$

is also an element of C. Here, ℓ is referred to as the *index* of C, and m is its *co-index*.

In the study of San Ling and Patrick Sole, the authors established that a QC code of length $n = \ell m$ over a ring R can be regarded as an $\frac{R[x]}{\langle x^m-1\rangle}$-submodule of $\left(\frac{R[x]}{\langle x^m-1\rangle}\right)^{\ell}$ [10, 11]. This perspective is known as the *conventional row circulant* definition of QC codes.

3. Repeated-root Framework

In this section, we consider a special case in which the characteristic of the finite chain ring R shares a common factor with the co-index of the code. Specifically, we present a generator matrix construction for a repeated-root QC code of length $n = \ell m$ over a finite chain ring R with characteristic equal to a power of 2, namely 2^t. The co-index is assumed to be even and of the form $m = 2m'$, where m' is an odd integer. Moreover, we impose the condition $ord_{m'}(2^t) = m' - 1$.

The previous study established a trace formula for repeated-root QC codes over rings [12]. The authors utilize the Generalized Discrete Fourier Transform (GDFT) to express a QC code as a direct sum of its element codes.

Algorithm 1 outlines a procedure for constructing a repeated-root QC code of length $n = \ell m$ over a finite chain ring R with characteristic p^k, where $m = p^a m'$ where m' is coprime to p [12].

Algorithm 1 Construction of a repeated-root QC code [12]

procedure REPEATED-ROOTQCCODE(ℓ, m, R, p^a, m')
  Factorize $x^m - 1$ over R as follows
  $$x^m - 1 = x^{p^a m'} - 1 = f_1^{p^a} f_2^{p^a} \cdots f_r^{p^a},$$
  where f_i's are distinct basic irreducible polynomials over R;
  for $i = 1$ to r **do**
    $R_i \leftarrow R[x]/(f_i)^{p^a}$;
    Let C_i be a code of length ℓ over R_i;
    Let Z_i denote the cyclotomic coset of $\mathbb{Z}/m'\mathbb{Z}$ corresponding to f_i and fix $z_i \in Z_i$;
    for $x_i \in C_i$ **do**
      $x_i = x_{i,0} + ux_{i,1} + \cdots + u^{p^a-1} x_{i,p^a-1}$, where the vectors $x_{i,g}$'s are in $(R[x]/(f_i(x)))^{\ell}$;
    end for
  end for
  Let ζ be a primitive m'-th root of unity in some Galois extension of R;
  for $i = 0$ to $p^a - 1$ **do**
    for $j = 0$ to $m' - 1$ **do**

$$\begin{aligned} c_{i+jp^a} = &\frac{1}{m'} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \\ &\times \sum_{\omega=1}^{r} \mathrm{Tr}_{\omega}\left(x_{z_\omega, g}\, \zeta^{(g-i-p^a j) z_\omega} \right). \end{aligned} \tag{1}$$

      return c_{i+jp^a};
    end for
  end for
end procedure

In Eq. (1), the summations over w extend across representatives of cyclotomic cosets, and Tr signifies the trace operation from the respective rings R_i down to R. For a comprehensive discussion on the trace formula, interested readers may consult the related reference [12].

Theorem 3.1. [12] Consider the code

$$C = \{(c_0, \cdots, c_{m-1}) \mid \forall x_i \in C_i\},$$

which is generated using Algorithm 1. This code forms a QC code of length ℓm and index ℓ over R. Conversely, any QC code of length ℓm and index ℓ over R can be derived through this construction.

Algorithm 1 employs the trace representation to map codewords of the constituent codes to the corresponding codewords of the resulting QC code. However, as the number of constituent codes increases, particularly for codes with large length and dimension, the computational complexity of this approach grows rapidly.

To overcome this limitation, we extend Algorithm 1 by operating directly on the generator matrices of the component

codes rather than on individual codewords. This modification leads to a substantial reduction in computational complexity, especially when dealing with high-dimensional or long component codes. Such scenarios frequently arise in both theoretical and practical settings, where the construction of optimal QC codes with large minimum distance and long length n is of primary interest. Moreover, the proposed algorithm outputs the generator matrix of the resulting QC code instead of enumerating its codewords, yielding a more compact and computationally efficient representation.

The proposed algorithm constructs QC codes of length $n = \ell m$, where $m = 2m'$ and m' is an odd integer, over a finite chain ring R with characteristic 2^t. We further assume that $ord_{m'}(2^t) = m'-1$. Under these assumptions, the polynomial $x^m - 1$ decomposes into distinct irreducible factors over R as follows:

$$x^m - 1 = x^{2m'} - 1 = (x-1)^2 f(x)^2.$$

We then define $R_1 = R[x]/(x-1)^2$ and $R_2 = R[x]/(f(x))^2$.

It is established that when $g(x)$ is an irreducible polynomial, the residue ring $R[x]/(g(x))^{p^a}$ can be expressed as follows [12],

$$R[x]/(g(x))^{p^a} \cong R[x]/(g(x)) + uR[x]/(g(x)) + \cdots + u^{p^a-1}R[x]/(g(x)), \;\; u^{p^a} = 0.$$

From this, we obtain the following isomorphisms:

$$R_1 = R[x]/(x-1)^2 \cong R[x] + uR[x], \quad u^2 = 0,$$

$$R_2 = R[x]/(f(x))^2 \cong R[x]/(f(x)) + uR[x]/(f(x)) \cong \mathcal{R} + u\mathcal{R}, \quad u^2 = 0.$$

Let C_1 and C_2 be linear codes of length ℓ over R_1 and R_2 with generator matrices G_1 and G_2, correspondingly. Any codeword $x_1 \in C_1$ and $x_2 \in C_2$ can be written as:

$$x_1 = x_{10} + ux_{11},$$
$$x_2 = x_{20} + ux_{21},$$

where $x_{10}, x_{11} \in R^\ell$ and $x_{20}, x_{21} \in \mathcal{R}^\ell$. Since each $x_1 \in C_1$ is a linear combination of the rows of G_1, we have $x_1 = vG_1$, where v is a vector over R_1. Decomposing v as $v = v_1 + uv_2$, where v_1 and v_2 are vectors over R, leads to:

$$\begin{aligned} x_1 &= vG_1 \\ &= (v_1 + uv_2)G_1 \\ &= (v_1 \quad v_2)\begin{pmatrix} G_1 \\ uG_1 \end{pmatrix} \\ &:= (v_1 \quad v_2)G_1'. \end{aligned}$$

Since G_1' is a matrix over R_1, we can express it as:

$$G_1' = G_{10}' + uG_{11}', \tag{2}$$

where G_{10}' and G_{11}' are matrices over R.

Similarly, any codeword $x_2 \in C_2$ can be represented as:

$$\begin{aligned} x_2 &= \nu G_2 \\ &= (\nu_1 \quad \nu_2)\begin{pmatrix} G_2 \\ uG_2 \end{pmatrix} \\ &:= (\nu_1 \quad \nu_2)G_2' \\ &= (\nu_1 \quad \nu_2)(G_{20}' + uG_{21}'), \end{aligned}$$

where $\nu = \nu_1 + u\nu_2$ is a vector over R_2, with ν_1 and ν_2 being vectors over $\mathcal{R}$.

For a codeword c_i generated by the matrix $G_{2,i}'$ $(i = 0, 1)$, we have:

$$c_i = \omega G_{2,i}',$$

where ω is a vector over $\mathcal{R}$. Since $\mathcal{R}$ is a free module of rank $\deg(f)$ over R, any vector $\omega \in \mathcal{R}$ can be expressed as:

$$\omega = \omega_0 + \omega_1\zeta + \cdots + \omega_{m'-2}\zeta^{m'-2},$$

where ζ is a root of $f(x)$ in a suitable Galois extension of R, and ω_i's are vectors over R. Consequently, we obtain:

$$\begin{aligned} c_i &= (\omega_0 + \omega_1\zeta + \cdots + \omega_{m'-2}\zeta^{m'-2})G_{2,i}' \\ &= (\omega_0 \quad \omega_1 \quad \cdots \quad \omega_{m'-2})\begin{pmatrix} G_{2,i}' \\ \zeta G_{2,i}' \\ \vdots \\ \zeta^{m'-2}G_{2,i}' \end{pmatrix} \\ &:= (\omega_0 \quad \omega_1 \quad \cdots \quad \omega_{m'-2})G_{2,i}'', \end{aligned}$$

where $G_{2,i}''$ is a matrix over $\mathcal{R}$. For simplicity, we denote $G_{2,i}''$ as G_{2i}''. It follows that:

$$G_{2i}'' = G_{2i,0}'' + G_{2i,1}''\zeta + \cdots + G_{2i,m'-2}''\zeta^{m'-2}, \tag{3}$$

where each $G_{2i,j}''$ $(0 \le j \le m'-2)$ is a matrix over R.

By applying the trace formula as in Eq. 1 and expressing any codeword as the linear combination of the rows of its generator matrix, we present procedure 1, which outlines the step-by-step construction of the generator matrix G for a repeated-root QC code over a finite chain ring under the mentioned specified conditions [6].

Generator Matrix Construction Procedure 1

Step 1: Preprocessing of component generator matrices

Let G_1 and G_2 denote the generator matrices of the component codes. Using the decompositions given in Equations (2) and (3), we first determine the auxiliary matrices

$$G_{1i}', \quad i \in \{0, 1\},$$

and

$$G_{2i,j}'', \quad i \in \{0, 1\}, \quad 0 \le j \le m'-1.$$

These matrices correspond to the simple-root and repeated-root components that will be combined to form the generator matrix of the QC code.

Step 2: Definition of an aggregate matrix

To simplify subsequent expressions, we define the matrix

$$\mathfrak{G} = \sum_{i=0}^{1} \sum_{j=0}^{m'-2} G''_{2i,j}.$$

This matrix aggregates all repeated-root contributions except the boundary terms. For notational convenience and to avoid special index cases, we further define

$$G''_{21,-1} = 0 \quad \text{and} \quad G''_{20,m'-1} = 0.$$

Step 3: Construction of the first block row

The first block row of the generator matrix G depends only on the matrices G'_{10} and G'_{11}. For each $k = 0, 1, \ldots, m'-1$, we define

$$\mathcal{G}_{0,2k} = G'_{10} + G'_{11}, \qquad \mathcal{G}_{0,2k+1} = G'_{11}.$$

This alternating structure reflects the contribution of the simple-root component across the quasi-cyclic blocks.

Step 4: Construction of the second block row (even indices)

Next, we construct part of the second block row using even block indices. For $k = 0, 1, \ldots, (m'-1)/2$, we set

$$\mathcal{G}_{1,2k} = \mathfrak{G} - \left(G''_{20,2k} + G''_{21,2k-1}\right),$$

and

$$\mathcal{G}_{1,m'+2k} = \mathfrak{G} - G''_{21,2k-1}.$$

These expressions subtract the appropriate repeated-root contributions to preserve the QC structure.

Step 5: Construction of the second block row (odd indices)

Similarly, for odd block indices $k = 0, 1, \ldots, (m'-3)/2$, we define

$$\mathcal{G}_{1,2k+1} = \mathfrak{G} - G''_{21,2k},$$

and

$$\mathcal{G}_{1,m'+2k+1} = \mathfrak{G} - \left(G''_{20,2k+1} + G''_{21,2k}\right).$$

Together with Step 4, this completes the construction of the second block row.

Step 6: Assembly of the generator matrix

Finally, the generator matrix of the repeated-root QC code is obtained by assembling the block matrices as

$$G = \begin{pmatrix} \mathcal{G}_{00} & \mathcal{G}_{01} & \mathcal{G}_{02} & \cdots & \mathcal{G}_{0,m-1} \\ \mathcal{G}_{10} & \mathcal{G}_{11} & \mathcal{G}_{12} & \cdots & \mathcal{G}_{1,m-1} \end{pmatrix}.$$

Example 3.1 provides a numerical application of Procedure 1.

Example 3.1. Let $R = \mathbb{F}_2$. So that the factorization of $x^6 - 1 \in \mathbb{F}_2[x]$ into irreducible factors is

$$x^6 - 1 = (x-1)^2(x^2+x+1)^2.$$

According to Procedure 1, we set

$$R_1 = \mathbb{F}_2[x]/(x-1)^2 \cong \mathbb{F}_2 + u\mathbb{F}_2,\ u^2 = 0,$$

$$R_2 = \mathbb{F}_2[x]/(x^2+x+1)^2 \cong \mathbb{F}_4 + u\mathbb{F}_4,\ u^2 = 0.$$

Let ζ be a root of (x^2+x+1) in $\mathbb{F}_4$. We assume that C_1 and C_2 are linear codes of the same length 2 over $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$, with generator matrices $G_1 = \begin{pmatrix} 1 & 1+u \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & \zeta+u \end{pmatrix}$, respectively. According to Equations (2) and (3), we have

$$G'_1 = \begin{pmatrix} 1 & 1+u \\ u & u \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + u \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} := G'_{10} + uG'_{11}$$

$$G'_2 = \begin{pmatrix} 1 & \zeta+u \\ u & u\zeta \end{pmatrix} = \begin{pmatrix} 1 & \zeta \\ 0 & 0 \end{pmatrix} + u \begin{pmatrix} 0 & 1 \\ 1 & \zeta \end{pmatrix} := G'_{20} + uG'_{21}$$

$$G''_{20} = \begin{pmatrix} 1 & \zeta \\ 0 & 0 \\ \zeta & 1+\zeta \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} + \zeta \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix} := G''_{20,0} + \zeta G''_{20,1}$$

$$G''_{21} = \begin{pmatrix} 0 & 1 \\ 1 & \zeta \\ 0 & \zeta \\ \zeta & 1+\zeta \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix} + \zeta \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} := G''_{21,0} + \zeta G''_{21,1}$$

$$\mathfrak{G} = \sum_{i=0}^{1} \sum_{j=0}^{1} G''_{2i,j} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Regarding Procedure 1, the following matrix G is a generator matrix of a binary QC code of length 12 and index 2.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

4. Simple-root QC codes

Throughout this section, we assume that R is a finite chain ring with characteristic q. We explore quasi-cyclic (QC) codes of length $n = \ell m$ over R where the code co-index is coprime to q and $\mathrm{ord}_m(q) = m-1$.

We begin by revisiting Algorithm 2, which outlines a method for constructing simple-root QC codes over a finite chain ring [11].

Algorithm 2 Construction of a simple-root QC code [11]

procedure SIMPLE-ROOTQCCODE(ℓ, m, R)
  Write $x^m - 1 = f_1 f_2 \cdots f_r$, where f_i's, $1 \le i \le r$, are basic irreducible factors over R;
  for $i = 1$ to r **do**
    $R_i \leftarrow \frac{R[x]}{\langle f_i \rangle}$;
    Let U_i denote the cyclotomic coset of Z_m corresponding to R_i, and fix an element $u_i \in U_i$;
    Let C_i be a code of length ℓ over R_i;
  end for
  Let ζ be a primitive m-th root of unity in some Galois extension of R;
  Let $x_i \in C_i$;
  for $g = 0$ to $m - 1$ **do**

$$c_g := \sum_{i=1}^{r} Tr_{R_i/R}\left(x_i \zeta^{-g u_i}\right); \tag{4}$$

    return c_g;
  end for
end procedure

In Equation (4), let E be a Galois extension of the finite chain ring R, and let $x \in E$. The trace of x from E down to R, denoted by $\mathrm{Tr}_{E/R}(x)$, is defined as:

$$\mathrm{Tr}_{E/R}(x) := x + x^q + x^{q^2} + \cdots + x^{q^{e-1}},$$

where e is the extension degree of E over R.

If x is a vector over E, then its trace is computed component-wise; that is, the trace of the vector is the vector formed by applying the scalar trace function to each of its entries.

The following Theorem, derived from Algorithm 2, provides a structural characterization of quasi-cyclic codes with simple roots over finite chain rings.

Theorem 4.1. [11] Let C be the code defined as

$$C = \{(c_0, c_1, \ldots, c_{m-1}) \mid x_i \in C_i \text{ for all } 1 \le i \le r\},$$

where the C_i are the component codes specified in Algorithm 2. Then C forms an ℓ-quasi-cyclic (QC) code of length ℓm over the ring R.

Conversely, any ℓ-QC code of length $n = \ell m$ over R can be constructed via this procedure.

We now investigate a special instance of Theorem 4.1, where the order of q modulo m satisfies $\mathrm{ord}_m(q) = m - 1$. Under this condition, the polynomial $x^m - 1$ splits into distinct irreducible factors over the field $\mathbb{F}_q[x]$. Employing Hensel's lemma, this factorization can be lifted to the ring $R[x]$, yielding

$$\begin{aligned} x^m - 1 &= (x-1)(1 + x + x^2 + \cdots + x^{m-1}) \\ &= (x-1) f(x). \end{aligned} \tag{5}$$

Define $R_1 := R[x]/\langle x - 1\rangle \cong R$ and $R_2 := R[x]/\langle f(x)\rangle$. It is known that R_2 forms a free R-module of rank $\deg(f) = m - 1$, with a basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-2}\}$, where ζ is a root of $f(x)$ in an appropriate Galois extension ring of R. Consequently, any element $x \in R_2$ admits the expansion

$$x = x_0 + x_1\zeta + x_2\zeta^2 + \cdots + x_{m-2}\zeta^{m-2}, \tag{6}$$

with coefficients $x_i \in R$.

Let C_1 and C_2 be linear codes of length ℓ over R_1 and R_2 respectively, equipped with generator matrices G_1 and G_2. Any codeword $c \in C_2$ may be expressed as

$$c = uG_2,$$

where u is a row vector over R_2. Using the expansion in Equation (6), write

$$u = u_0 + u_1\zeta + u_2\zeta^2 + \cdots + u_{m-2}\zeta^{m-2},$$

with u_i vectors over R. This yields:

$$\begin{aligned} c &= uG_2 \\ &= (u_0 + u_1\zeta + \cdots + u_{m-2}\zeta^{m-2})G_2 \\ &= (u_0\ u_1\ \cdots\ u_{m-2}) \begin{bmatrix} G_2 \\ \zeta G_2 \\ \vdots \\ \zeta^{m-2} G_2 \end{bmatrix} = (u_0\ u_1\ \cdots\ u_{m-2}) G_2'. \end{aligned}$$

Each entry of G_2' can be expressed via the expansion (6), giving

$$G_2' = G_{20}' + G_{21}'\zeta + \cdots + G_{2,m-2}'\zeta^{m-2}, \tag{7}$$

where $G_{2,i}'$ are matrices over R. Hence,

$$c = (u_0\ u_1\ \cdots\ u_{m-2})\left(G_{20}' + G_{21}'\zeta + \cdots + G_{2,m-2}'\zeta^{m-2}\right).$$

Now, applying the trace-based construction from Equation (4), the g-th component of a codeword is given by

$$\begin{aligned} c_g &= \sum_{i=1}^{2} \mathrm{Tr}_{R_i/R}\left(x_i \zeta^{-g u_i}\right) \\ &= x_1 + (x_2\zeta^{-g}) + (x_2\zeta^{-g})^q + \cdots + (x_2\zeta^{-g})^{q^{m-2}}, \end{aligned} \tag{8}$$

where x_i ranges over codewords in C_i, for $i = 1, 2$.

According to Equation (6), a codeword $x_2 \in C_2$ can be expanded as

$$x_2 = x_{20} + x_{21}\zeta + \cdots + x_{2,m-2}\zeta^{m-2},$$

with $x_{2,i} \in R^\ell$. Substituting into Equation (8), we get:

$$\begin{aligned} c_0 &= x_1 + x_2 + x_2^q + \cdots + x_2^{q^{m-2}} \\ &= x_1 + \sum_{j=0}^{m-2} \left(\sum_{k=0}^{m-2} \zeta^{j q^k} \right) x_{2,j} \\ &= x_1 + (m-1)x_{20} - \sum_{j=1}^{m-2} x_{2,j}, \end{aligned}$$

using the fact that ζ is a root of $f(x)$, hence $1+\zeta+\cdots+\zeta^{q^{m-2}}=0$.

In general, for $0 \le g \le m-2$, one obtains:

$$c_g = x_1 - x_{20} - \cdots + (m-1)x_{2,g} - \cdots - x_{2,m-2}. \quad (9)$$

For $g = m-1$, we derive:

$$\begin{aligned} c_{m-1} &= x_1 + (x_2\zeta) + (x_2\zeta)^q + \cdots + (x_2\zeta)^{q^{m-2}} \\ &= x_1 - x_{20} - x_{21} - \cdots - x_{2,m-2}. \end{aligned} \quad (10)$$

We now seek a generator matrix G for the QC code constructed through this method. Based on Equations (9) and (10), we have:

$$c_g = vG_1 - \nu G'_{20} - \cdots + (m-1)\nu G'_{2,g} - \cdots - \nu G'_{2,m-2},$$

$$0 \le g \le m-2.$$

and

$$c_{m-1} = vG_1 - \nu G'_{20} - \nu G'_{21} - \cdots - \nu G'_{2,m-2},$$

where v, ν are vectors over R.

This leads to Procedure 2 for constructing a generator matrix G of a certain category of simpe-root QC codes.

Generator Matrix Construction Procedure 2

Step 1: Extension of the second component code

Let G_1 and G_2 be the generator matrices of the component codes. Using the extension defined in Equation (7), we first determine the matrices

$$G'_{2,i}, \qquad 0 \le i \le m-2.$$

These matrices capture the contribution of the second component code to each quasi-cyclic block.

Step 2: Construction of the first block row

The first block row of the generator matrix consists of identical blocks. Specifically, for all block indices $k = 0, 1, \ldots, m-1$, we define

$$\mathcal{G}_{0,k} = G_1.$$

This uniform structure reflects the repetition of the first component code across all cyclic positions.

Step 3: Construction of the second block row

The second block row is formed using linear combinations of the matrices $G'_{2,i}$. For $k = 0, 1, \ldots, m-2$, we define

$$\mathcal{G}_{1,k} = (m-1)G'_{2,k} - \sum_{\substack{j=0 \\ j\neq k}}^{m-2} G'_{2,j}.$$

The last block in the second row is defined separately as

$$\mathcal{G}_{1,m-1} = -\sum_{j=0}^{m-2} G'_{2,j}.$$

These expressions ensure that the resulting generator matrix satisfies the structural constraints of the simple-root QC code.

Step 4: Assembly of the generator matrix

Finally, the generator matrix of the simple-root QC code is obtained by assembling the block matrices as

$$G = \begin{bmatrix} \mathcal{G}_{00} & \mathcal{G}_{01} & \mathcal{G}_{02} & \cdots & \mathcal{G}_{0,m-1} \\ \mathcal{G}_{10} & \mathcal{G}_{11} & \mathcal{G}_{12} & \cdots & \mathcal{G}_{1,m-1} \end{bmatrix}.$$

As a consequence of the preceding analysis, we arrive at the following theorem.

We now illustrate apply Procedure 2 through Example 4.1 to construct a generator matrix for a quasi-cyclic (QC) code of length 10 and index 2 over the finite chain ring $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. This construction is based on the generator matrices of two linear codes of length 2 defined over R and over its Galois extension ring $\mathcal{R} = \mathbb{F}_{16} + u\mathbb{F}_{16}$, where $u^2 = 0$.

Example 4.1. Let $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. Then R is a finite chain ring with maximal ideal $\langle u \rangle$ and residue field $R/\langle u \rangle \cong \mathbb{F}_2$.

We consider QC codes of length 10 and index 2 over R. Since $x^5 - 1$ factors over R as

$$\begin{aligned} x^5 - 1 &= (x-1)\left(1 + x + x^2 + x^3 + x^4\right) \\ &= (x-1)f(x), \end{aligned}$$

we define two rings:

1. $R_1 = R[x]/\langle x-1 \rangle \cong R$
2. $R_2 = R[x]/\langle f(x) \rangle$

Let ζ be a root of $f(x)$ in some Galois extension of R. Let C_1 and C_2 be linear codes of length 2 over R_1 and R_2, respectively, with the following generator matrices:

$$G_1 = \begin{pmatrix} 1 & u \end{pmatrix}, \qquad G_2 = \begin{pmatrix} 1+u+u\zeta^3 & (1+u)\zeta^2 \end{pmatrix}.$$

Then, by Procedure 2, the following matrix G generates a QC code of length 10 and index 2 over R:

$$G = \begin{pmatrix} 1 & u & 1 & u & 1 & u & 1 & u & 1 & u \\ u & u & 1 & u & 1 & 0 & 1+u & u & 1 & u \\ u & 1+u & u & 1+u & u & 1+u & u & 0 & 0 & 1+u \\ u & 1+u & 0 & 1+u & u & 1+u & 0 & 1+u & 0 & 0 \\ 1 & 0 & 1+u & 1+u & 1 & 1+u & u & 1+u & 1 & 1+u \end{pmatrix}.$$

5. Numerical Comparisons

It is worth noting that codes over chain rings can offer valuable insights into the structure and performance of codes over finite fields. In particular, when $R = \mathbb{F}_q$, the setting naturally reduces to codes over fields. Consequently, Procedures 1 and 2 can be applied to repeated-root and simple-root binary QC codes, i.e., QC codes over $\mathbb{F}_2$.

In this section, we present numerical results that compare the performance of our proposed algorithms with existing methods. Specifically, we focus on repeated-root and simple-root binary QC codes and evaluate performance in terms of encoding time per iteration and memory consumption. The comparison is visualized using histograms to highlight the efficiency and improvements achieved by our proposed approaches in this paper.

We conduct two sets of comparisons to demonstrate the efficiency of the proposed algorithms for both repeated-root and simple-root classes of codes. First, as illustrated in Figure. 1, we compare the proposed algorithms with existing methods from the literature in terms of memory usage (MB) and encoding time (ms) as the code length increases. The results clearly indicate that the proposed algorithms exhibit superior performance, particularly for larger code lengths.

To further validate these findings, we present additional results showing that the proposed algorithms remain effective not only as the code length increases but also when variations in the code dimension are taken into account too. This analysis leads to the three-dimensional histograms shown in Figure. 2. For this scenario, we provide both bar plots and the corresponding surface plots. The surface plots are obtained by connecting discrete data points, thereby offering a continuous visualization of the performance trends of the proposed algorithms for both repeated-root and simple-root cases.

For each interval represented in the histograms, we computed the average encoding time and memory usage over a set of code co-indices m that satisfy the assumptions of our proposed algorithms. Specifically, for the code length range of 200 to 400, we selected values of m within the range 100 to 200 such that $\mathrm{ord}_m(2) = m - 1$, which guarantees the irreducibility of the polynomial $1+x+\cdots+x^{m-1}$ over $\mathbb{F}_2$. The selected values of m in this interval are: 101, 107, 131, 139, 149, 163, 173, 179, 181, and 197. For each of these values, the corresponding code dimension was determined using our algorithms, and both encoding time and memory usage were recorded. The histogram plots then display the average of these values over the selected set. A similar approach was applied to all other code length intervals shown in the histograms.

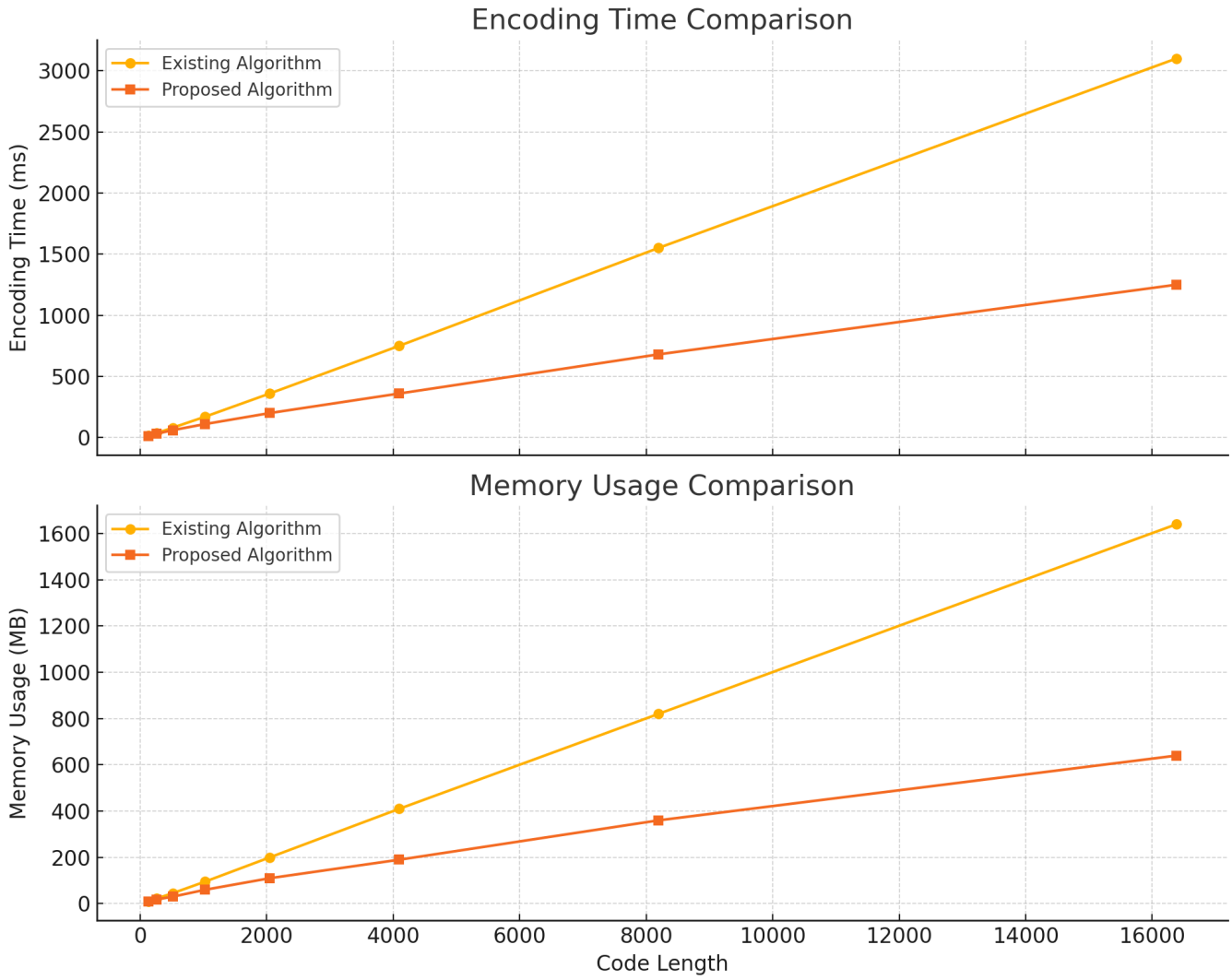

Figure 1. *Two-dimensional Comparison diagrams.*

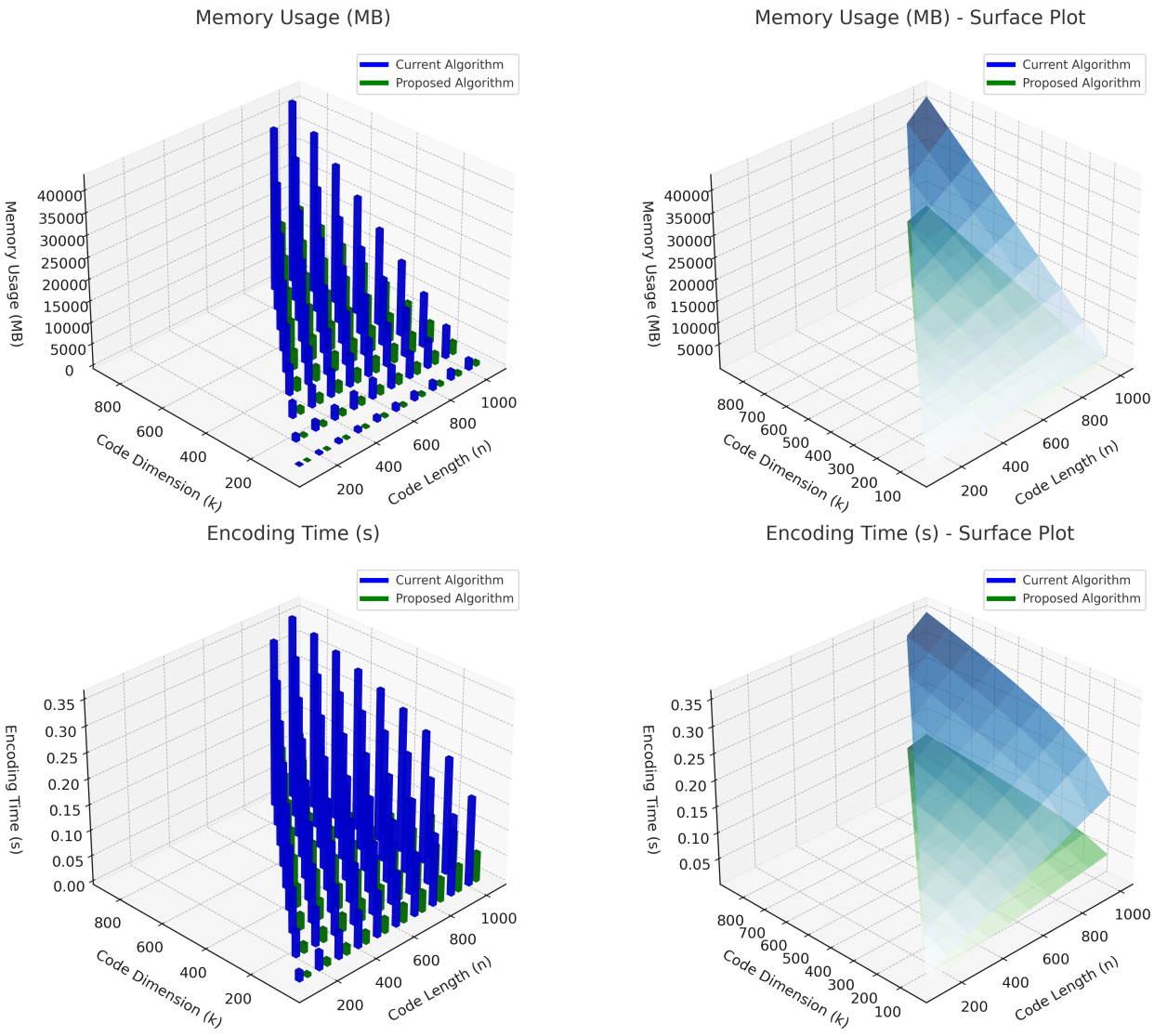

Figure 2. *Three-dimansional Comparison diagrams.*

6. Conclusion

In this paper, we investigated both repeated-root and simple-root quasi-cyclic (QC) codes. By exploiting the generalized discrete Fourier transform (GDFT), along with its special case, the discrete Fourier transform (DFT), we derived explicit generator matrix construction methods for specific classes of QC codes.

The main advantage of the proposed approach lies in its reduced computational complexity compared to conventional construction methods. Traditional techniques typically take the codewords of the component (constituent) codes as input and produce the codewords of the resulting QC code as output. As the code length, dimension, or the number of constituent codes increases, the computational complexity of these methods grows rapidly.

In contrast, our approach operates directly on the generator matrices of the constituent codes rather than on individual codewords. Moreover, instead of enumerating the codewords of the QC code, the proposed algorithms output its generator matrix. This matrix-based framework leads to a more compact representation and significantly improves computational efficiency, particularly for QC codes with large length and dimension.

To validate the effectiveness of the proposed methods, we presented numerical results comparing encoding time and memory usage for several classes of QC codes. The results clearly demonstrate the superior performance of the proposed algorithms over existing methods reported in the literature.

ORCID

0009-0004-3959-6929 (Akram Saleh)
0009-0005-6805-4341 (Mohammad Reza Soleymani)

Abbreviations

QC	Quasi-Cyclic
QT	Quasi-Twisted
DFT	Discrete Fourier Transform
GDFT	Generalized Discrete Fourier Transform

Author Contributions

Akram Saleh: Conceptualization analysis, Methodology, Data curation, Formal Analysis, Software, Validation, Writing – original draft

Mohammad Reza Soleymani: Conceptualization, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Visualization, Writing – review & editing

Conflicts of Interest

The authors declare that they have no conflict of interest.

References

[1] N. Aydin and I. Siap, "New quasi-cyclic codes over F_5," *Applied Mathematics Letters*, vol. 15, no. 7, pp. 833–836, Oct. 2002. https://doi.org/10.1016/S0893-9659(02)00050-2

[2] Z. Chen, "Six new binary quasi-cyclic codes," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1666–1667, 1994. https://doi.org/10.1109/18.333888

[3] E. Z. Chen, "New quasi-cyclic codes from simplex codes," *IEEE Transactions on Information Theory*, vol. 53, no. 3, pp. 1193–1196, 2007. https://doi.org/10.1109/TIT.2006.890727

[4] R. Daskalov, P. Hristov, and E. Metodieva, "New minimum distance bounds for linear codes over $GF(5)$," *Discrete Mathematics*, vol. 275, no. 1–3, pp. 97–110, 2004. https://doi.org/10.1016/S0012-365X(03)00126-2

[5] A. Saleh and M. R. Soleymani, "A novel framework for relating quasi-cyclic codes and quasi-twisted codes," in *2023 Biennial Symposium on Communications (BSC)*, pp. 38–41, IEEE, Jul. 2023. https://doi.org/10.1109/BSC57238.2023.10201835

[6] A. Saleh and M. Soleymani, "A novel construction technique for some classes of quasi-cyclic codes," in *2023 IEEE International Symposium on Information Theory (ISIT)*, pp. 591–595, IEEE, Jun. 2023. https://doi.org/10.1109/ISIT54713.2023.10206961

[7] M. N. Danish, S. A. Pasha, and A. J. Hashmi, "Quasi-cyclic LDPC codes for short block-lengths," in *2021 IEEE Aerospace Conference*, pp. 1–8, IEEE, 2021. https://doi.org/10.1109/AERO50100.2021.9438238

[8] M. I. Hidayat, Irwansyah, and I. G. A. W. Wardhana, "A construction of generalized quasi-cyclic codes over finite field using Gray map," *AIP Conference Proceedings*, vol. 2641, no. 1, 2022. https://doi.org/10.1063/5.0114988

[9] S. Benjwal, M. Bhaintwal, and R. Kumar, "On quantum codes derived from quasi-cyclic codes over a non-chain ring," *Quantum Information Processing*, vol. 23, no. 9, art. no. 309, 2024. https://doi.org/10.1007/S11128-024-04514-7

[10] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes. I: Finite fields," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2751–2760, 2001. https://doi.org/10.1109/18.959257

[11] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes II: Chain rings," *Designs, Codes and Cryptography*, vol. 30, pp. 113–130, 2003. https://doi.org/10.1023/A:1024715527805

[12] S. Ling, P. Solé, and H. Niederreiter, "On the algebraic structure of quasi-cyclic codes IV: Repeated roots," *Designs, Codes and Cryptography*, vol. 38, no. 3, pp. 337–361, 2006. https://doi.org/10.1007/S10623-005-1431-7

[13] A. Saleh and M. Esmaeili, "Some classes of quasi-twisted codes over finite chain rings," *Journal of Applied Mathematics and Computing*, vol. 57, no. 1, pp. 629–646, 2018. https://doi.org/10.1007/S12190-017-1125-0

[14] M. F. Ezerman, M. Grassl, S. Ling, F. Ozbudak, and B. Ozkaya, "Characterization of nearly self-orthogonal quasi-twisted codes and related quantum codes," *IEEE Transactions on Information Theory*, vol. 71, no. 1, pp. 499–517, 2024. https://doi.org/10.1109/TIT.2024.3503420

[15] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York, 1974.