AIMS Mathematics, 11(3): 7497–7528.
DOI: 10.3934/math.2026307
Received: 12 January 2026
Revised: 08 March 2026
Accepted: 17 March 2026
Published: 23 March 2026

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

Research article

Quantum and DNA codes from cyclic codes over the ring $\mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha\rangle$

Sami H. Saif* **and Shayea Aldossari**

Mathematics Department, College of Science, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia; shaaldossari@ksu.edu.sa

* **Correspondence:** Email: ssiaf1@ksu.edu.sa.

Abstract: This paper studies cyclic, quantum, and DNA codes over the mixed-characteristic ring $\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha\rangle$, where p is an odd prime and $\alpha \in \mathbb{F}_p^*$. When α is a quadratic residue modulo p, the polynomial $u^2 - \alpha$ splits over $\mathbb{Z}_{p^2}$ and $\mathcal{R}_{p,\alpha}$ is a semi-local ring isomorphic to $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$. In this decomposable case, every $\mathcal{R}_{p,\alpha}$-linear cyclic code admits a canonical idempotent decomposition into two cyclic codes over $\mathbb{Z}_{p^2}$, leading to explicit descriptions of generator polynomials, dual codes, and Lee distances. Both the coprime-length case $\gcd(n, p) = 1$ and the repeated-root case $n = p^s$ are analyzed, reflecting their distinct ideal-theoretic behavior. An $\mathbb{F}_p$-linear Gray map is constructed that induces a Lee-to-Hamming isometry from $\mathcal{R}_{p,\alpha}^n$ to $\mathbb{F}_p^{4n}$. Using a compatible bilinear form, we show that the Gray image of a Euclidean self-orthogonal cyclic code remains symplectic self-orthogonal over $\mathbb{F}_p$, which enables the construction of p-ary quantum stabilizer codes via the Calderbank–Shor–Steane method. Explicit computations for small parameters illustrate the resulting quantum code parameters and show that several examples meet or improve known bounds. For $p = 5$, the Gray map also admits an interpretation suitable for DNA coding. By mapping Gray images to the IUPAC nucleotide alphabet and exploiting the ring involution $u \mapsto -u$, we obtain reversible DNA codes through blockwise reversal symmetry. Using coterm polynomials, families of reversible DNA codes with prescribed minimum distance and controlled GC-content are constructed. These results demonstrate how cyclic codes over the mixed-characteristic ring $\mathcal{R}_{p,\alpha}$ can be used to derive quantum and DNA codes through the Gray map and related algebraic structures.

Keywords: cyclic codes; Gray map; quantum codes; DNA codes
Mathematics SubjectClassification: 11T71, 94B15, 94B05

1. Introduction

Finite commutative rings that are not chain rings play an increasingly important role in algebraic coding theory. Their richer ideal structures and module decompositions enable the construction of

linear and cyclic codes that have no direct analogues over finite fields or classical chain rings such as $\mathbb{Z}_{p^n}$ or $\mathbb{F}_q + u\mathbb{F}_q$ [1–3]. A major turning point was the discovery that several prominent nonlinear binary codes admit elegant $\mathbb{Z}_4$-linear representations [4], revealing deep algebraic connections between finite-ring modules and highly structured nonlinear codes. Since then, ring–based coding theory has developed into a substantial research area, supported by foundational treatments such as [5–7] and extensive studies of cyclic and constacyclic codes over non-chain rings [8–10]. In this paper, we investigate the coding-theoretic properties of the quadratic extension

$$\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha\rangle, \qquad p \text{ odd}, \ \ \alpha \in \mathbb{F}_p, \tag{1.1}$$

where α is embedded into $\mathbb{Z}_{p^2}$ via the canonical inclusion $\mathbb{F}_p \hookrightarrow \mathbb{Z}_{p^2}$. The algebraic structure of $\mathcal{R}_{p,\alpha}$ depends critically on the quadratic character of α modulo p, leading to two fundamentally different settings for cyclic codes. The binary case $p = 2$ has been studied separately in [11, 12].

(1) Decomposable case. If α is a quadratic residue modulo p, then $u^2 - \alpha$ splits over $\mathbb{Z}_{p^2}$, and therefore

$$\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}.$$

This decomposition yields two primitive orthogonal idempotents and endows $\mathcal{R}_{p,\alpha}$ with a semi-local, non-chain structure. Such decomposability is particularly effective for simplifying the structure of cyclic and constacyclic codes over related rings [1, 13]. In this setting, every $\mathcal{R}_{p,\alpha}$-linear cyclic code of length n decomposes canonically as a direct sum of two cyclic codes over $\mathbb{Z}_{p^2}$. This reduction allows generator polynomials, dual codes, and Lee distances to be described explicitly in terms of their $\mathbb{Z}_{p^2}$ counterparts. We consider both the coprime-length case $\gcd(n, p) = 1$ and the repeated-root case $n = p^s$, reflecting their distinct ideal-theoretic behaviors.

(2) Local ring cases. We also distinguish two essentially different local situations.

(i) Local Galois case. Assume that $\alpha \in \mathbb{Z}_{p^2}^{\times}$ and that its reduction modulo p is a non-quadratic residue in $\mathbb{F}_p$. Then, $u^2 - \alpha$ is irreducible over $\mathbb{F}_p$, and remains irreducible over $\mathbb{Z}_{p^2}$. Consequently,

$$\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha\rangle \cong \mathrm{GR}(p^2, 2),$$

which is a finite local (chain) ring. In this case, u is a unit, the unique maximal ideal is $\langle p\rangle$, and the residue field is $\mathbb{F}_{p^2}$.

(ii) Local non-reduced case. When $\alpha = 0$, one has

$$\mathcal{R}_{p,0} \cong \mathbb{Z}_{p^2}[u]/\langle u^2\rangle = \mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2},$$

which is again a local ring but no longer reduced. Here, u is nilpotent, the unique maximal ideal is $\langle p, u\rangle$, and the residue field is $\mathbb{F}_p$.

In both local cases, $\mathcal{R}_{p,\alpha}$ admits no nontrivial idempotent decomposition. Accordingly, cyclic codes are studied directly as ideals of $\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle$. Despite being algebraically more rigid than in the decomposable case, these local settings still admit a structural description of cyclic codes, particularly when $\gcd(n, p) = 1$; see [14, 15].

To connect the ring-theoretic and classical coding perspectives, we define a Gray map

$$\Psi : \mathcal{R}_{p,\alpha} \longrightarrow \mathbb{F}_p^4,$$

generalizing the Gray isometry for $\mathbb{Z}_4$-linear codes [4] and its subsequent extensions to finite rings [1, 16, 17]. Defined via the $\mathbb{Z}_{p^2}$-coordinate representation of elements of $\mathcal{R}_{p,\alpha}$, this map preserves both Lee and Hamming distances. Extended coordinate-wise, it yields an isometric embedding

$$\Psi : \mathcal{R}_{p,\alpha}^n \hookrightarrow \mathbb{F}_p^{4n},$$

allowing cyclic codes over $\mathcal{R}_{p,\alpha}$ to be studied through their Gray images as linear codes over $\mathbb{F}_p$.

Using an $\mathbb{F}_p$-valued bilinear form compatible with the Gray map, we show that the Gray image of any self-orthogonal cyclic code over $\mathcal{R}_{p,\alpha}$ remains self-orthogonal in $\mathbb{F}_p^{4n}$. This property enables the construction of p-ary quantum stabilizer codes via the Calderbank–Shor–Steane (CSS) framework [18–20]. While the CSS method and ring-based constructions of quantum codes are well established [21–23], our contribution is to apply these techniques to cyclic codes over $\mathcal{R}_{p,\alpha}$ and to analyze the resulting new families of quantum codes obtained through the Gray map. Explicit computations for small parameters illustrate the resulting code parameters and show that several examples meet or exceed known bounds [24, 25].

When $p = 5$, the Gray map also admits an interpretation suitable for DNA coding applications. By mapping the coordinates of $\Psi(r)$ to nucleotides via the IUPAC alphabet [26, 27], we obtain DNA codes of length $4n$ over $\mathcal{R}_{5,\alpha}$. Motivated by constraints from molecular computation and DNA word design [28–30], we use the ring automorphism $u \mapsto -u$ to induce a blockwise reversal symmetry on Gray images. Using coterm polynomials, we construct reversible DNA codes with prescribed minimum distance and controlled GC-content, extending earlier ring-based DNA code constructions [11, 31, 32] to this ring setting.

In summary, this paper studies cyclic, quantum, and DNA codes over the ring $\mathcal{R}_{p,\alpha}$. Our main results concern the decomposable case $\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$, where cyclic codes admit a componentwise description in terms of cyclic codes over $\mathbb{Z}_{p^2}$. The local cases are also discussed to illustrate the structural differences that arise when $\mathcal{R}_{p,\alpha}$ becomes a local ring. Combining these structural properties with an isometric Gray map, we derive cyclic codes whose Gray images yield p-ary quantum stabilizer codes and reversible DNA codes.

The remainder of the paper is organized as follows. Section 2 introduces notation and defines the Gray map. Section 3 analyzes the algebraic structure of $\mathcal{R}_{p,\alpha}$, classifies cyclic codes, and studies their duals and Lee distances. Section 4 applies these results to quantum stabilizer codes, while Section 5 develops reversible DNA codes. Finally, Section 6 presents illustrative examples supporting the theoretical results.

2. Preliminaries and notations

Throughout the paper, let p be an odd prime and let $\alpha \in \mathbb{F}_p$. We view α as an element of $\mathbb{Z}_{p^2}$ via the canonical embedding $\mathbb{F}_p \hookrightarrow \mathbb{Z}_{p^2}$. We study the mixed-characteristic quadratic extension

$$\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha \rangle. \tag{2.1}$$

Then, $\mathcal{R}_{p,\alpha}$ is a free $\mathbb{Z}_{p^2}$-module of rank 2 with basis $\{1, u\}$. Since each element of $\mathbb{Z}_{p^2}$ admits a unique p-adic expansion $a + pb$ with $a, b \in \mathbb{F}_p$, every element of $\mathcal{R}_{p,\alpha}$ can be written uniquely as

$$r = a + pb + uc + upd, \qquad a, b, c, d \in \mathbb{F}_p, \tag{2.2}$$

and hence $|\mathcal{R}_{p,\alpha}| = p^4$. Multiplication is determined by $u^2 = \alpha$; for $r_1, r_2, r_1', r_2' \in \mathbb{Z}_{p^2}$, one has

$$(r_1 + r_2u)(r_1' + r_2'u) = (r_1r_1' + \alpha r_2r_2') + (r_1r_2' + r_1'r_2)u. \tag{2.3}$$

2.1. Algebraic structure according to α

The algebraic nature of $\mathcal{R}_{p,\alpha}$ depends on whether α is a square in $\mathbb{F}_p$. Since $\alpha \in \mathbb{F}_p$, only the square, non-square, and zero cases arise.

(I) Square case (decomposable ring). Assume that α is a quadratic residue in $\mathbb{F}_p$, and fix $\beta \in \mathbb{F}_p$ with $\beta^2 = \alpha$. Since p is odd, $2\beta \neq 0$ in $\mathbb{F}_p$. By Hensel's lemma, there exists a lift $\beta' \in \mathbb{Z}_{p^2}$ such that

$$\beta' \equiv \beta \pmod{p}, \qquad (\beta')^2 = \alpha.$$

Thus, $u^2 - \alpha = (u - \beta')(u + \beta')$ in $\mathbb{Z}_{p^2}[u]$, and by the Chinese remainder theorem,

$$\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2}[u]/\langle u - \beta' \rangle \oplus \mathbb{Z}_{p^2}[u]/\langle u + \beta' \rangle \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}.$$

Define the orthogonal idempotents

$$e_1 = \frac{u + \beta'}{2\beta'}, \qquad e_2 = \frac{\beta' - u}{2\beta'}, \tag{2.4}$$

so that $e_1^2 = e_1$, $e_2^2 = e_2$, $e_1e_2 = 0$, and $e_1 + e_2 = 1$. Every element $r \in \mathcal{R}_{p,\alpha}$ then decomposes uniquely as

$$r = e_1r_1 + e_2r_2, \qquad r_1, r_2 \in \mathbb{Z}_{p^2}. \tag{2.5}$$

(II) Non-square and zero cases (local rings). If $\alpha = 0$, we obtain $\mathcal{R}_{p,0} = \mathbb{Z}_{p^2}[u]/\langle u^2 \rangle$, a local non-chain ring studied in [14]. If $\alpha \neq 0$ is a quadratic nonresidue, then $x^2 - \alpha$ is irreducible modulo p, and hence also irreducible over $\mathbb{Z}_{p^2}$. Thus, $\mathcal{R}_{p,\alpha}$ is the Galois ring $\mathrm{GR}(p^2, 2)$. In both cases, $\mathcal{R}_{p,\alpha}$ is local with maximal ideal $\langle p \rangle$ (or $\langle p, u \rangle$ if $\alpha = 0$), and residue field $\mathbb{F}_{p^2}$ (or $\mathbb{F}_p$ if $\alpha = 0$). Moreover, if $\alpha \neq 0$, then u is a unit with $u^{-1} = u/\alpha$.

Therefore, the algebraic type of $\mathcal{R}_{p,\alpha}$ is determined entirely by α. Table 1 summarizes the resulting possibilities.

Table 1. Structure of $\mathcal{R}_{p,\alpha}$ for $\alpha \in \mathbb{F}_p$.

Condition on α	Ring type	Maximal ideal	Residue
α square	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$	$\langle p, u + \beta' \rangle$, $\langle p, u - \beta' \rangle$	$\mathbb{F}_p \times \mathbb{F}_p$
$\alpha = 0$	local ring $\mathbb{Z}_{p^2}[u]/\langle u^2 \rangle$	$\langle p, u \rangle$	$\mathbb{F}_p$
α non-square	Galois ring $\mathrm{GR}(p^2, 2)$	$\langle p \rangle$	$\mathbb{F}_{p^2}$

2.2. Linear and cyclic codes over $\mathcal{R}_{p,\alpha}$

Let $n \geq 1$. A *linear code* of length n over $\mathcal{R}_{p,\alpha}$ is an $\mathcal{R}_{p,\alpha}$-submodule $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$. We endow $\mathcal{R}_{p,\alpha}^n$ with the Euclidean inner product

$$\langle \mathbf{x}, \mathbf{y} \rangle_{\mathrm{e}} = \sum_{i=1}^{n} x_iy_i, \qquad \mathbf{x}, \mathbf{y} \in \mathcal{R}_{p,\alpha}^n. \tag{2.6}$$

The Euclidean dual is

$$\mathscr{C}^{\perp} = \left\{ \mathbf{y} \in \mathcal{R}_{p,\alpha}^{n} \;\middle|\; \langle \mathbf{x}, \mathbf{y} \rangle_{\mathrm{e}} = 0 \text{ for all } \mathbf{x} \in \mathscr{C} \right\}.$$

A code is *self-orthogonal* if $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ and *self-dual* if $\mathscr{C} = \mathscr{C}^{\perp}$. A code $\mathscr{C}$ is *cyclic* if it is invariant under the cyclic shift

$$(c_0, c_1, \ldots, c_{n-1}) \longmapsto (c_{n-1}, c_0, \ldots, c_{n-2}).$$

Under the standard identification

$$(c_0, \ldots, c_{n-1}) \;\longleftrightarrow\; c_0 + c_1 x + \cdots + c_{n-1} x^{n-1},$$

cyclic codes correspond to ideals of the quotient ring $\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1 \rangle$.

For a polynomial $f(x) = f_0 + f_1 x + \cdots + f_t x^t \in \mathcal{R}_{p,\alpha}[x]$ with $f_t \neq 0$, the *reciprocal polynomial* is

$$f^*(x) = x^t f(1/x) = f_t + f_{t-1} x + \cdots + f_0 x^t, \tag{2.7}$$

used in describing dual and self-orthogonal cyclic codes.

A vector $\mathbf{c} = (c_0, \ldots, c_{n-1})$ is *reversible* if its reversal $\mathbf{c}^r = (c_{n-1}, \ldots, c_0)$ also lies in the code. Reversibility will play a central role in the DNA-code constructions below.

Remark 1. *Throughout this paper, we primarily consider the case where $\alpha \in \mathbb{F}_p^{\times}$ is a quadratic residue. In this situation,*

$$\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2},$$

and hence admits a nontrivial idempotent decomposition. As a consequence, cyclic codes over $\mathcal{R}_{p,\alpha}$ decompose canonically into pairs of cyclic codes over $\mathbb{Z}_{p^2}$, yielding explicit generator descriptions, duality conditions, and manageable Lee-distance formulas. These features are essential for the quantum and DNA code constructions developed in later sections.

The case $\alpha = 0$ is excluded, since $\mathbb{Z}_{p^2}[u]/\langle u^2 \rangle$ is non-reduced and does not admit a compatible idempotent or distance-preserving Gray-map framework. When α is a non-quadratic residue modulo p, the ring $\mathcal{R}_{p,\alpha}$ becomes the local Galois ring $\mathrm{GR}(p^2, 2)$; although cyclic codes exist in this setting, the lack of orthogonal idempotents prevents the componentwise analysis central to this work.

2.3. Gray maps for $\mathcal{R}_{p,\alpha}$

Define the $\mathbb{F}_p$-linear bijection

$$\Psi_0 : \mathbb{Z}_{p^2} \longrightarrow \mathbb{F}_p^2, \qquad a + pb \longmapsto (a, b), \quad a, b \in \mathbb{F}_p.$$

We define the Lee weight on $\mathbb{Z}_{p^2}$ by

$$w_L(z) = w_H(\Psi_0(z)),$$

and extend it coordinatewise to $\mathbb{Z}_{p^2}^n$.

Assume α is a square and use the idempotents e_1, e_2 from (2.4). Writing $r = e_1 r_1 + e_2 r_2$ with $r_1, r_2 \in \mathbb{Z}_{p^2}$, define the *product Gray map*

$$\Psi_{\mathrm{sq}}(r) = (\Psi_0(r_1), \Psi_0(r_2)) \in \mathbb{F}_p^4. \tag{2.8}$$

Equivalently, using the unique coordinate expansion (2.2), define the *coordinate Gray map*

$$\Psi_s(a + pb + uc + upd) = (a, c, b, d) \in \mathbb{F}_p^4. \tag{2.9}$$

The two maps differ by an invertible $\mathbb{F}_p$-linear transformation. More precisely, if $r_i = a_i + pb_i$ with $a_i, b_i \in \mathbb{F}_p$, then

$$\begin{pmatrix} a \\ c \\ b \\ d \end{pmatrix} = M \begin{pmatrix} a_1 \\ b_1 \\ a_2 \\ b_2 \end{pmatrix}, \qquad M = \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ \beta^{-1} & 0 & -\beta^{-1} & 0 \\ 0 & 1 & 0 & 1 \\ 0 & \beta^{-1} & 0 & -\beta^{-1} \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_p), \tag{2.10}$$

where β^{-1} denotes the inverse of β in $\mathbb{F}_p$. (In particular, only the reduction of β' modulo p is relevant.)

Let

$$S = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

Then, $M^T S M = \lambda S$ with $\lambda = \beta^{-2} = \alpha^{-1}$ in $\mathbb{F}_p$, so M is a symplectic similitude.

For the remainder of the paper, we fix one such Gray map and denote it simply by $\Psi : \mathcal{R}_{p,\alpha} \to \mathbb{F}_p^4$. We define the Lee weight on $\mathcal{R}_{p,\alpha}$ by

$$w_L(r) = w_H(\Psi(r)),$$

and the Lee distance on $\mathcal{R}_{p,\alpha}^n$ by

$$d_L(\mathbf{r}, \mathbf{s}) = w_L(\mathbf{r} - \mathbf{s}).$$

Lemma 1. *The Gray map $\Psi : \mathcal{R}_{p,\alpha}^n \to \mathbb{F}_p^{4n}$ is an $\mathbb{F}_p$-linear bijection and an isometry from $(\mathcal{R}_{p,\alpha}^n, d_L)$ onto $(\mathbb{F}_p^{4n}, d_H)$.*

Proof. $\mathbb{F}_p$-linearity is immediate from the coordinate description. By the definition of d_L via Ψ, for any $\mathbf{r}, \mathbf{s}$, we have

$$d_L(\mathbf{r}, \mathbf{s}) = w_H(\Psi(\mathbf{r} - \mathbf{s})) = w_H(\Psi(\mathbf{r}) - \Psi(\mathbf{s})) = d_H(\Psi(\mathbf{r}), \Psi(\mathbf{s}))\,.$$

Bijectivity follows from the uniqueness of the expansion (2.2). □

For an $\mathcal{R}_{p,\alpha}$-linear code $\mathscr{C}$, we obtain

$$\dim_{\mathbb{F}_p} \Psi(\mathscr{C}) = \log_p |\mathscr{C}|.$$

In particular, if $\mathscr{C}^{(i)} = \langle g_i(x) \rangle \subseteq \mathbb{Z}_{p^2}^n$ is a cyclic code with $\deg(g_i) = d_i$ in the coprime case, then $|\mathscr{C}^{(i)}| = p^{2(n-d_i)}$, and hence $\dim_{\mathbb{F}_p} \Psi_0(\mathscr{C}^{(i)}) = 2(n - d_i)$.

3. The ring $\mathcal{R}_{p,\alpha}$ and cyclic codes

Let p be an odd prime. Throughout this section, we assume that $\alpha \in \mathbb{F}_p^\times$ is a quadratic residue. By the structural results of Section 2, the ring

$$\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha \rangle$$

is decomposable and admits orthogonal idempotents e_1, e_2 in (2.4) satisfying

$$\mathcal{R}_{p,\alpha} = e_1\mathcal{R}_{p,\alpha} \oplus e_2\mathcal{R}_{p,\alpha}, \qquad e_1\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2}, \quad e_2\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2}.$$

Accordingly, every element $r \in \mathcal{R}_{p,\alpha}$ decomposes uniquely as in (2.5).

Let $n \geq 1$. A cyclic code $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$ is identified with an ideal of $\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle$. Coefficientwise lifting of e_1, e_2 gives the ambient decomposition

$$\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle \;\cong\; \Big(\mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle\Big) \;\oplus\; \Big(\mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle\Big), \tag{3.1}$$

via

$$f(x) = e_1 f_1(x) + e_2 f_2(x) \mapsto (f_1(x), f_2(x)).$$

Hence, the structure of cyclic codes over $\mathcal{R}_{p,\alpha}$ follows from the standard description of ideals in direct product rings.

Proposition 1. *Let $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$ be a cyclic code. Then, there exist unique cyclic codes $\mathscr{C}^{(1)}, \mathscr{C}^{(2)} \subseteq \mathbb{Z}_{p^2}^n$ such that*

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \;\oplus\; e_2\mathscr{C}^{(2)}. \tag{3.2}$$

Under the isomorphism (3.1)*, the ideal corresponding to $\mathscr{C}$ is $\mathscr{C}^{(1)} \oplus \mathscr{C}^{(2)}$.*

Proof. Let I be the ideal corresponding to $\mathscr{C}$ in $\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle$, and let Φ denote the isomorphism in (3.1). Since ideals of a direct product ring are precisely direct products of ideals, we have $\Phi(I) = I_1 \oplus I_2$ for some ideals $I_i \subseteq \mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle$. Let $\mathscr{C}^{(i)}$ be the cyclic code corresponding to I_i. Applying Φ^{-1} yields $I = e_1 I_1 \oplus e_2 I_2$, hence $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$. Uniqueness follows from the relations $e_1 e_2 = 0$ and $e_1 + e_2 = 1$. □

Euclidean duality also decomposes componentwise for every n; no coprimality assumption is needed.

Theorem 1. *Let $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ be a cyclic code of length n over $\mathcal{R}_{p,\alpha}$. Then,*

$$\mathscr{C}^{\perp} = e_1(\mathscr{C}^{(1)})^{\perp} \;\oplus\; e_2(\mathscr{C}^{(2)})^{\perp},$$

where the duals on the right are Euclidean duals in $\mathbb{Z}_{p^2}^n$.

Proof. Write $\mathbf{c} = e_1\mathbf{c}_1 + e_2\mathbf{c}_2$ and $\mathbf{d} = e_1\mathbf{d}_1 + e_2\mathbf{d}_2$ with $\mathbf{c}_i \in \mathscr{C}^{(i)}$ and $\mathbf{d}_i \in \mathbb{Z}_{p^2}^n$. Using $e_i^2 = e_i$ and $e_1 e_2 = 0$,

$$\langle \mathbf{c}, \mathbf{d}\rangle = e_1\langle \mathbf{c}_1, \mathbf{d}_1\rangle_{\mathbb{Z}_{p^2}} + e_2\langle \mathbf{c}_2, \mathbf{d}_2\rangle_{\mathbb{Z}_{p^2}}.$$

Since e_1, e_2 are orthogonal and sum to 1, this vanishes in $\mathcal{R}_{p,\alpha}$ if and only if both inner products vanish in $\mathbb{Z}_{p^2}$, which gives the claim. □

Corollary 1. *A cyclic code $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ is self-orthogonal if and only if $\mathscr{C}^{(i)} \subseteq (\mathscr{C}^{(i)})^{\perp}$ for $i = 1, 2$.*

Proof. This is immediate from Theorem 1 by multiplying the inclusion $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ by e_1 and e_2. □

Remark 2. *If α is a non-quadratic residue modulo p, then $u^2 - \alpha$ is irreducible modulo p and $\mathcal{R}_{p,\alpha} \cong \mathrm{GR}(p^2, 2)$ is a chain ring with no nontrivial idempotents. The componentwise analysis used here does not apply in that setting.*

3.1. The coprime case $\gcd(n, p) = 1$

Assume $\gcd(n, p) = 1$. Then, $\mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle$ is a principal ideal ring, so every cyclic $\mathbb{Z}_{p^2}$-code has a monic generator polynomial dividing $x^n - 1$.

Theorem 2. *Assume* $\gcd(n, p) = 1$ *and write* $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$. *If* $\mathscr{C}^{(i)} = \langle g_i(x)\rangle$ *in* $\mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle$ *with monic* $g_i(x) \mid x^n - 1$, *then*

$$\mathscr{C} = \langle e_1 g_1(x) + e_2 g_2(x)\rangle$$

as an ideal of $\mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle$.

Proof. Under Φ in (3.1), the ideal of $\mathscr{C}$ corresponds to $\langle g_1(x)\rangle \oplus \langle g_2(x)\rangle$. Let $g(x) = e_1 g_1(x) + e_2 g_2(x)$; then, $\Phi(g(x)) = (g_1(x), g_2(x))$. Hence, $\Phi(\langle g(x)\rangle) = \langle g_1(x)\rangle \oplus \langle g_2(x)\rangle$, so $\langle g(x)\rangle$ equals the ideal of $\mathscr{C}$. □

Corollary 2. *Assume* $\gcd(n, p) = 1$ *and let* $\mathscr{C} = e_1\langle g_1(x)\rangle \oplus e_2\langle g_2(x)\rangle$. *Then,* $\mathscr{C}$ *is self-orthogonal if and only if*

$$x^n - 1 \mid g_1(x)g_1^*(x) \qquad \text{and} \qquad x^n - 1 \mid g_2(x)g_2^*(x).$$

Proof. By Corollary 1, $\mathscr{C}$ is self-orthogonal if and only if each component $\langle g_i(x)\rangle$ is self-orthogonal over $\mathbb{Z}_{p^2}$. For $\gcd(n, p) = 1$, if $x^n - 1 = g_i(x)h_i(x)$, then $\langle g_i(x)\rangle^\perp = \langle h_i^*(x)\rangle$, hence $\langle g_i\rangle \subseteq \langle g_i\rangle^\perp$ if and only if $h_i^*(x) \mid g_i(x)$, equivalently $x^n - 1 \mid g_i(x)g_i^*(x)$. □

3.2. The repeated-root case $n = p^s$

We now treat the repeated-root case $n = p^s$ with $s \geq 1$. Throughout, p is an odd prime and $\alpha \in \mathbb{F}_p^\times$ is a quadratic residue, so that $\mathcal{R}_{p,\alpha}$ splits as $\mathcal{R}_{p,\alpha} = e_1\mathbb{Z}_{p^2} \oplus e_2\mathbb{Z}_{p^2}$ with orthogonal idempotents e_1, e_2 as in (2.4). We write $n = p^s$ and introduce the ambient rings

$$A = \mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle, \qquad B = \mathcal{R}_{p,\alpha}[x]/\langle x^n - 1\rangle.$$

Cyclic codes of length n over $\mathbb{Z}_{p^2}$ (resp. $\mathcal{R}_{p,\alpha}$) correspond to ideals of A (resp. B).

Next, we show the $(x - 1)$-nilpotency in A. The key point is that $x^n - 1$ has the repeated root $x = 1$ modulo p. This forces $(x - 1)$ to be nilpotent in A. Note that $p \mid \binom{n}{k}$ for all $1 \leq k \leq n - 1$.

Lemma 2. *In* $A = \mathbb{Z}_{p^2}[x]/\langle x^n - 1\rangle$, *one has*

$$(x - 1)^n = p\, f(x) \text{ for some } f(x) \in A, \text{ and hence } (x - 1)^{2n} = 0.$$

Proof. Expand

$$(x - 1)^n = \sum_{k=0}^{n} \binom{n}{k} x^k (-1)^{n-k} = x^n - 1 + \sum_{k=1}^{n-1} \binom{n}{k} x^k (-1)^{n-k}.$$

Then, each intermediate coefficient is divisible by p, so

$$(x - 1)^n = x^n - 1 + p\, g(x)$$

for some $g(x) \in \mathbb{Z}_{p^2}[x]$. Modulo $\langle x^n - 1\rangle$ we get $(x - 1)^n \equiv p\, g(x)$, i.e., $(x - 1)^n = p\, f(x)$ in A, where $f(x)$ is the class of $g(x)$. Multiplying again by $(x - 1)^n$ gives

$$(x - 1)^{2n} = p^2 f(x)^2 = 0$$

because $p^2 = 0$ in $\mathbb{Z}_{p^2}$. □

Lemma 3. *Every element $a \in A$ admits a unique $(x-1)$-adic expansion*

$$a = \sum_{j=0}^{n-1} a_j (x-1)^j, \qquad a_j \in \mathbb{Z}_{p^2}. \tag{3.3}$$

Equivalently, $\{1, (x-1), \ldots, (x-1)^{n-1}\}$ is a $\mathbb{Z}_{p^2}$-basis of A.

Proof. Every element of A is represented by a polynomial in x of degree at most $n-1$, since $x^n = 1$ in A. Thus, it suffices to rewrite each power x^i $(0 \le i \le n-1)$ in terms of powers of $(x-1)$. By the binomial theorem,

$$x^i = ((x-1)+1)^i = \sum_{j=0}^{i} \binom{i}{j} (x-1)^j.$$

Hence, every polynomial in x of degree at most $n-1$ is a $\mathbb{Z}_{p^2}$-linear combination of

$$1,\ (x-1),\ \ldots,\ (x-1)^{n-1}.$$

Therefore, every element $a \in A$ admits an expansion

$$a = \sum_{j=0}^{n-1} a_j (x-1)^j, \qquad a_j \in \mathbb{Z}_{p^2}.$$

To prove uniqueness, suppose

$$\sum_{j=0}^{n-1} a_j (x-1)^j = 0 \quad \text{in } A.$$

Then, the polynomial $\sum_{j=0}^{n-1} a_j (x-1)^j$ represents an element of the ideal $\langle x^n - 1 \rangle$ in $\mathbb{Z}_{p^2}[x]$. Since this polynomial has degree strictly less than n while $x^n - 1$ has degree n, the only possibility is that all coefficients vanish, i.e., $a_j = 0$ for all j.

Hence, the representation is unique, and therefore $\{1, (x-1), \ldots, (x-1)^{n-1}\}$ is a $\mathbb{Z}_{p^2}$-basis of A. □

Let $\pi : A \to \overline{A} = A/pA$ be the natural projection. As noted above,

$$\overline{A} \cong \mathbb{F}_p[x]/\langle (x-1)^n \rangle,$$

whose ideals are exactly $\langle (x-1)^t \rangle$ for $0 \le t \le n$.

Lemma 4. *Every ideal $\overline{I} \subseteq \overline{A}$ is uniquely of the form $\overline{I} = \langle (x-1)^{\iota_0} \rangle$ for some $0 \le \iota_0 \le n$.*

Proof. This is immediate because $\overline{A} \cong \mathbb{F}_p[y]/\langle y^n \rangle$ is a principal ideal ring generated by the nilpotent element y. □

Now, let I be an ideal of A. Define the first invariant ι_0 by

$$\pi(I) = \overline{I} = \langle (x-1)^{\iota_0} \rangle \subseteq \overline{A}, \tag{3.4}$$

so ι_0 is uniquely determined by Lemma 4. Equivalently, ι_0 is the smallest integer such that I contains an element whose reduction modulo p has $(x-1)$-adic order ι_0.

Next, define the p-torsion of A:

$$\mathrm{Tor}_p(A) = \{a \in A : \ pa = 0\}.$$

Since $p^2 = 0$ in $\mathbb{Z}_{p^2}$, one has $pA \subseteq \mathrm{Tor}_p(A)$. Conversely, if $pa = 0$ and $a = \sum_{j=0}^{n-1} a_j(x-1)^j$ as in Lemma 3, then $pa_j = 0$ in $\mathbb{Z}_{p^2}$, so each a_j is divisible by p, hence $a \in pA$. Thus,

$$\mathrm{Tor}_p(A) = pA. \tag{3.5}$$

Define the second invariant ι_1 by

$$\iota_1 = \min\{t \in \{0, 1, \ldots, n\} : \ p(x-1)^t \in I\}. \tag{3.6}$$

This minimum exists because $p(x-1)^n = p \cdot pf(x) = 0$ by Lemma 2, so the set is nonempty.

Lemma 5. *For every ideal $I \subseteq A$, one has*

$$0 \le \iota_1 \le \iota_0 \le n.$$

Moreover,

$$I \cap pA = \langle p(x-1)^{\iota_1} \rangle. \tag{3.7}$$

Proof. Clearly, $0 \le \iota_0 \le n$ by Lemma 4, and $0 \le \iota_1 \le n$ by definition. To show $\iota_1 \le \iota_0$, note that by (3.4) the ideal I contains some $a \in I$ with $\pi(a) = (x-1)^{\iota_0}$ in $\overline{A}$. Write $a = (x-1)^{\iota_0} + pq(x)$. Then, $p(x-1)^{\iota_0} = pa \in I$, so by minimality of ι_1 we get $\iota_1 \le \iota_0$.

For (3.7), first observe that by definition, $p(x-1)^{\iota_1} \in I \cap pA$, so $\langle p(x-1)^{\iota_1} \rangle \subseteq I \cap pA$. Conversely, let $z \in I \cap pA$. Then, $z = pw$ for some $w \in A$. Write $w = \sum_{j=0}^{n-1} w_j(x-1)^j$. Let t be the smallest index with $w_t \not\equiv 0 \pmod p$ (if none exists then $w \in pA$ and $z = pw = 0$ is already in $\langle p(x-1)^{\iota_1} \rangle$). Then, $w = (x-1)^t u(x) + p(\cdots)$ with $u(1) \not\equiv 0 \pmod p$, hence $u(x)$ is a unit in A (a polynomial in $(x-1)$ with constant term a unit in $\mathbb{Z}_{p^2}$ is a unit). Thus, $pw = p(x-1)^t u(x) \in I$. Since $u(x)$ is a unit and I is an ideal, this implies $p(x-1)^t \in I$. By minimality of ι_1 we have $t \ge \iota_1$, hence $p(x-1)^t \in \langle p(x-1)^{\iota_1} \rangle$, and therefore $z \in \langle p(x-1)^{\iota_1} \rangle$. This proves $I \cap pA \subseteq \langle p(x-1)^{\iota_1} \rangle$. □

Now we construct a normalized generator and the two-generator form. Let $I \subseteq A$ be an ideal with invariants ι_0, ι_1. By (3.4) there exists $a \in I$ with $\pi(a) = (x-1)^{\iota_0}$. Write

$$a = (x-1)^{\iota_0} + pq(x) \qquad \text{with } q(x) \in A.$$

Expand $q(x)$ $(x-1)$-adically as $q(x) = \sum_{j=0}^{n-1} q_j(x-1)^j$. If $q(x) = 0$, we set $e = \iota_1$ and $b(x) = 0$ below. Otherwise, let

$$e = \min\{j : \ q_j \not\equiv 0 \pmod p\},$$

and write $q(x) = (x-1)^e b(x)$ where $b(x)$ has unit constant term (hence is a unit in A). Replacing $b(x)$ by its truncation modulo $(x-1)^{\iota_1 - e}$ (which is legitimate because $p(x-1)^{\iota_1} \in I$) gives the normalization

$$\deg_{x-1} b < \iota_1 - e. \tag{3.8}$$

Lemma 6. *With the above choice, one has $0 \le e < \iota_1$.*

Proof. If $q = 0$, we may set $e = 0$, and the claim is trivial. Assume $q \neq 0$ and $q = (x-1)^e b$ with b a unit. If $e \geq \iota_1$, then $pq = p(x-1)^e b \in \langle p(x-1)^{\iota_1} \rangle \subseteq I$. Hence,

$$(x-1)^{\iota_0} = a - pq \in I.$$

Then, $p(x-1)^{\iota_0} \in I$, forcing $\iota_1 \leq \iota_0$ (already true). More importantly, we can improve a by subtracting a suitable multiple of $p(x-1)^{\iota_1}$ to reduce the p-part to start before ι_1; explicitly, since $pq \in \langle p(x-1)^{\iota_1} \rangle$, there exists $t(x)$ with $pq = p(x-1)^{\iota_1} t(x)$, and hence

$$a - (x-1)^{\iota_0} = (pq) \in p(x-1)^{\iota_1} A.$$

Thus, replacing a by $a - p(x-1)^{\iota_1} t(x)$ gives an element in I with the same reduction modulo p but whose p-part begins in degree $< \iota_1$. Therefore, a normalized choice always exists with $e < \iota_1$. □

Define the normalized element

$$f(x) = (x-1)^{\iota_0} + p(x-1)^e b(x) \ \in I, \tag{3.9}$$

with $0 \leq e < \iota_1$ and $b(x)$ either 0 or a unit satisfying (3.8).

Theorem 3. *Let $I \subseteq A$ be an ideal and let ι_0, ι_1 be defined by* (3.4) *and* (3.6)*. Then, I is generated by two elements:*

$$I = \langle f(x),\ p(x-1)^{\iota_1} \rangle, \tag{3.10}$$

where $f(x)$ is the normalized element in (3.9) *with $0 \leq e < \iota_1$ and $b(x)$ either* 0 *or a unit satisfying* (3.8)*. Moreover, the pair (ι_0, ι_1) is uniquely determined by I.*

Proof. Let $J = \langle f(x),\ p(x-1)^{\iota_1} \rangle$. Since $f \in I$ and $p(x-1)^{\iota_1} \in I$, we have $J \subseteq I$.

To prove $I \subseteq J$, take any $h(x) \in I$. Reduce modulo p. Since $\pi(I) = \langle (x-1)^{\iota_0} \rangle$ in $\overline{A}$, we may write in $\overline{A}$:

$$\pi(h(x)) = (x-1)^{\iota_0} \cdot \overline{t(x)}$$

for some $\overline{t(x)} \in \overline{A}$. Choose a lift $t(x) \in A$ of $\overline{t(x)}$. Then,

$$\pi\big(h(x) - f(x)t(x)\big) = \pi(h(x)) - \pi(f(x))\pi(t(x)) = (x-1)^{\iota_0}\overline{t(x)} - (x-1)^{\iota_0}\overline{t(x)} = 0,$$

hence

$$h(x) - f(x)t(x) \in pA. \tag{3.11}$$

Because $h \in I$ and $f \in I$, we have $h - ft \in I$, so (3.11) gives $h - ft \in I \cap pA$. By Lemma 5, $I \cap pA = \langle p(x-1)^{\iota_1} \rangle$. Thus, there exists $u(x) \in A$ such that

$$h(x) - f(x)t(x) = p(x-1)^{\iota_1} u(x) \in J,$$

and therefore $h(x) \in J$. This shows $I \subseteq J$, hence $I = J$.

Finally, uniqueness of (ι_0, ι_1) follows because ι_0 is determined uniquely by $\pi(I)$ in (3.4), and ι_1 is the minimal t with $p(x-1)^t \in I$ by (3.6). □

We find the exact size of an ideal in terms of (ι_0, ι_1).

Theorem 4. *Let $I \subseteq A$ be an ideal with invariants (ι_0, ι_1). Then,*

$$|I| = p^{2n-(\iota_0+\iota_1)}. \tag{3.12}$$

Equivalently, I has $\mathbb{F}_p$-dimension $2n - (\iota_0 + \iota_1)$.

Proof. Consider the exact sequence of additive groups

$$0 \longrightarrow I \cap pA \longrightarrow I \xrightarrow{\pi} \pi(I) \longrightarrow 0,$$

where surjectivity holds by definition of $\pi(I)$. Thus,

$$|I| = |I \cap pA| \cdot |\pi(I)|.$$

First, compute $|\pi(I)|$. Since $\pi(I) = \langle (x-1)^{\iota_0} \rangle$ in $\overline{A} \cong \mathbb{F}_p[y]/\langle y^n \rangle$, the quotient $\overline{A}/\pi(I) \cong \mathbb{F}_p[y]/\langle y^{\iota_0} \rangle$ has size p^{ι_0}, hence

$$|\pi(I)| = \frac{|\overline{A}|}{|\overline{A}/\pi(I)|} = \frac{p^n}{p^{\iota_0}} = p^{n-\iota_0}.$$

Next, compute $|I \cap pA|$. By Lemma 5, $I \cap pA = \langle p(x-1)^{\iota_1} \rangle$. Using the $(x-1)$-adic basis (3.3), the ideal pA consists of all $\sum_{j=0}^{n-1} pc_j(x-1)^j$ with $c_j \in \mathbb{F}_p$, hence $|pA| = p^n$. Similarly, $\langle p(x-1)^{\iota_1} \rangle$ consists of all $\sum_{j=\iota_1}^{n-1} pc_j(x-1)^j$, so it has size $p^{n-\iota_1}$. Therefore,

$$|I| = p^{n-\iota_1} \cdot p^{n-\iota_0} = p^{2n-(\iota_0+\iota_1)},$$

which is (3.12). □

We now transfer these results from A to $\mathcal{R}_{p,\alpha}$ via the orthogonal idempotents e_1, e_2. Because $\mathcal{R}_{p,\alpha} = e_1\mathbb{Z}_{p^2} \oplus e_2\mathbb{Z}_{p^2}$, we have

$$B = \mathcal{R}_{p,\alpha}[x]/\langle x^n - 1 \rangle \cong A \oplus A$$

and ideals in B correspond to ordered pairs of ideals in A.

Theorem 5. *Let $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$ be a cyclic code with $n = p^s$. Then, there exist unique cyclic codes $\mathscr{C}^{(1)}, \mathscr{C}^{(2)} \subseteq \mathbb{Z}_{p^2}^n$ such that*

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}.$$

Moreover, for each $i \in \{1, 2\}$, there exist integers $\iota_0^{(i)}, \iota_1^{(i)}$ and $e^{(i)}, b^{(i)}(x)$ such that

$$\mathscr{C}^{(i)} = \left\langle (x-1)^{\iota_0^{(i)}} + p(x-1)^{e^{(i)}} b^{(i)}(x), \;\; p(x-1)^{\iota_1^{(i)}} \right\rangle \tag{3.13}$$

in $\mathbb{Z}_{p^2}[x]/\langle x^n - 1 \rangle$, with

$$0 \le \iota_0^{(i)} < n, \quad 0 \le \iota_1^{(i)} \le \min\{p^{s-1}, \iota_0^{(i)}\}, \qquad 0 \le e^{(i)} < \iota_1^{(i)}, \qquad \deg_{x-1} b^{(i)} < \iota_1^{(i)} - e^{(i)}$$

when $b^{(i)} \neq 0$ (and $b^{(i)} = 0$ allowed).

Proof. The decomposition $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ follows exactly as in Proposition 1 by identifying $B \cong A \oplus A$. Each component $\mathscr{C}^{(i)}$ corresponds to an ideal $I_i \subseteq A$, and Theorem 3 gives the explicit form (3.13) with the displayed constraints. Uniqueness of the decomposition follows from the orthogonality of e_1, e_2. □

To find the cardinalities and Gray-image dimensions, we let $|\mathscr{C}^{(i)}| = p^{\kappa_i}$. Since the decomposition is direct,

$$|\mathscr{C}| = |\mathscr{C}^{(1)}||\mathscr{C}^{(2)}| = p^{\kappa_1+\kappa_2}.$$

By Theorem 4 applied to each component,

$$\kappa_i = 2n - (\iota_0^{(i)} + \iota_1^{(i)}). \tag{3.14}$$

Hence,

$$\kappa_1 + \kappa_2 = 4n - \left(\iota_0^{(1)} + \iota_1^{(1)} + \iota_0^{(2)} + \iota_1^{(2)}\right). \tag{3.15}$$

In particular, for the Gray map Ψ used later (assumed $\mathbb{F}_p$-linear),

$$\dim_{\mathbb{F}_p} \Psi(\mathscr{C}) = \kappa_1 + \kappa_2 = 4n - \left(\iota_0^{(1)} + \iota_1^{(1)} + \iota_0^{(2)} + \iota_1^{(2)}\right).$$

Moreover, if Ψ is an isometry from Lee to Hamming distance and respects the idempotent splitting into disjoint coordinate blocks, then

$$d_H(\Psi(\mathscr{C})) = \min\{d_L(\mathscr{C}^{(1)}),\, d_L(\mathscr{C}^{(2)})\}. \tag{3.16}$$

The componentwise dual decomposition does not use principality, only orthogonal idempotents and bilinearity of the Euclidean inner product.

Theorem 6. *Let $n = p^s$, and let $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ be a cyclic code over $\mathcal{R}_{p,\alpha}$. Then,*

$$\mathscr{C}^{\perp} = e_1(\mathscr{C}^{(1)})^{\perp} \;\oplus\; e_2(\mathscr{C}^{(2)})^{\perp},$$

where the duals on the right are Euclidean duals in $\mathbb{Z}_{p^2}^n$.

Proof. Write $\mathbf{c} = e_1\mathbf{c}_1 + e_2\mathbf{c}_2$ with $\mathbf{c}_i \in \mathscr{C}^{(i)}$, and similarly $\mathbf{d} = e_1\mathbf{d}_1 + e_2\mathbf{d}_2$ with $\mathbf{d}_i \in \mathbb{Z}_{p^2}^n$. Using $e_i^2 = e_i$ and $e_1e_2 = 0$,

$$\langle \mathbf{c}, \mathbf{d}\rangle = e_1\langle \mathbf{c}_1, \mathbf{d}_1\rangle_{\mathbb{Z}_{p^2}} + e_2\langle \mathbf{c}_2, \mathbf{d}_2\rangle_{\mathbb{Z}_{p^2}}.$$

Since e_1, e_2 are orthogonal idempotents with $e_1 + e_2 = 1$, this equals 0 in $\mathcal{R}_{p,\alpha}$ if and only if both inner products vanish in $\mathbb{Z}_{p^2}$. This gives the stated description of $\mathscr{C}^{\perp}$. □

Corollary 3. *Let $n = p^s$. Then,*

$$\mathscr{C} \subseteq \mathscr{C}^{\perp} \quad\Longleftrightarrow\quad \mathscr{C}^{(i)} \subseteq (\mathscr{C}^{(i)})^{\perp} \text{ for } i = 1, 2.$$

Proof. This is immediate from Theorem 6 by multiplying the inclusion by e_1 and e_2. □

Corollary 4. *Let $n = p^s$ and $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$. If $\mathscr{C}^{(i)}$ has invariants $(\iota_0^{(i)}, \iota_1^{(i)})$, then*

$$|\mathscr{C}| = |\mathscr{C}^{(1)}||\mathscr{C}^{(2)}| = p^{\,4n-\left(\iota_0^{(1)}+\iota_1^{(1)}+\iota_0^{(2)}+\iota_1^{(2)}\right)}.$$

Proof. By Theorem 4, $|\mathscr{C}^{(i)}| = p^{2n-(\iota_0^{(i)}+\iota_1^{(i)})}$, and the decomposition is direct, so $|\mathscr{C}| = |\mathscr{C}^{(1)}||\mathscr{C}^{(2)}|$. □

Finally, the repeated-root dual generator formula over $\mathbb{Z}_{p^2}$ is as follows.

For a polynomial

$$b(x) = p^k(x-1)^e \sum_{i=0}^{\iota_k - 1} b_i (x-1)^i$$

in A, we define its dual polynomial by

$$b^{\perp}(x) = \sum_{i=0}^{\iota_i - 1} \left(\sum_{j=0}^{i} (-1)^{\iota_0 + e + j + 1} \binom{\iota_0 + \iota_1 - e - j}{i - j} b_j \right) (x-1)^i. \tag{3.17}$$

Theorem 7. *Let $\mathscr{D} = \langle (x-1)^{\iota_0} + p(x-1)^e b(x),\ p(x-1)^{\iota_1} \rangle$ be a cyclic code over $\mathbb{Z}_{p^2}$, where*

$$0 \le \iota_0 < p^s, \qquad 0 \le \iota_1 \le \min\{p^{s-1}, \iota_0\}, \qquad e + \deg b < \iota_1,$$

and

$$b(x) = \sum_{k=0}^{\iota_1 - e - 1} b_k (x-1)^k.$$

Then, the Euclidean dual $\mathscr{D}^{\perp}$ is cyclic and generated by

$$\mathscr{D}^{\perp} = \left\langle (x-1)^{p^s - \iota_1} + p(x-1)^{p^s - \iota_0 - \iota_1 + e} b^{\perp}(x) + p\epsilon (x-1)^{p^{s-1} - \iota_1},\ p(x-1)^{p^s - \iota_0} \right\rangle, \tag{3.18}$$

where $b^{\perp}(x)$ is given by (3.17) *and*

$$\epsilon = \begin{cases} (-1)^{p^{s-1} - \iota_1}, & \text{if } 0 < p^{s-1} - \iota_1 < \iota_1, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let

$$g_1(x) = (x-1)^{\iota_0} + p(x-1)^e b(x), \qquad g_2(x) = p(x-1)^{\iota_1}.$$

Using the relation

$$x^{p^s} - 1 = (x-1)^{p^s} + p(x-1)^{p^{s-1}} \vartheta_{p,s},$$

where $\vartheta_{p,s}$ is a unit in $\mathbb{Z}_{p^2}[x]/\langle x^{p^s} - 1 \rangle$. One checks that

$$g_1(x)h(x) = 0, \qquad g_2(x)h(x) = 0,$$

where

$$h(x) = (x-1)^{p^s - \iota_1} + p(x-1)^{p^{s-1} - \iota_1} \vartheta_{p,s} - p(x-1)^{p^s - \iota_0 - \iota_1 + e} b(x).$$

Hence,

$$D = \langle h(x),\ p(x-1)^{p^s - \iota_0} \rangle \subseteq \operatorname{Ann}(\mathscr{D}).$$

Since $\mathscr{D}$ has residual degree ι_0 and torsion degree ι_1,

$$|\mathscr{D}| = p^{2p^s - \iota_0 - \iota_1}.$$

Because the ambient ring $A = \mathbb{Z}_{p^2}[x]/\langle x^{p^s} - 1 \rangle$ is Frobenius,

$$|\mathscr{D}|\,|\operatorname{Ann}(\mathscr{D})| = |A| = p^{2p^s}.$$

Thus, $|\operatorname{Ann}(\mathscr{D})| = p^{\iota_0+\iota_1}$. Moreover, the two generators of D have residual and torsion degrees $p^s - \iota_1$ and $p^s - \iota_0$, respectively, so $|D| = p^{\iota_0+\iota_1}$. Hence, $D = \operatorname{Ann}(\mathscr{D})$. Taking reciprocals of the generators of $\operatorname{Ann}(\mathscr{D})$ yields the generators of the dual code. Since $x^n = 1$ in A, we have $x^{-1} = x^{n-1}$. Writing $x = (x-1) + 1$ and expanding the reciprocal of the first generator in the $(x-1)$–adic basis, while reducing higher powers using

$$(x-1)^{p^s} = -p(x-1)^{p^{s-1}}\vartheta_{p,s},$$

we obtain

$$(x-1)^{p^s-\iota_1} + p(x-1)^{p^s-\iota_0-\iota_1+e}b^{\perp}(x) + p\epsilon(x-1)^{p^{s-1}-\iota_1}.$$

Similarly, the reciprocal of $p(x-1)^{p^s-\iota_0}$ has leading $(x-1)$–degree $p^s - \iota_0$, and therefore reduces to $p(x-1)^{p^s-\iota_0}$ in the $(x-1)$–adic representation. Consequently,

$$\mathscr{D}^{\perp} = \left\langle (x-1)^{p^s-\iota_1} + p(x-1)^{p^s-\iota_0-\iota_1+e}b^{\perp}(x) + p\epsilon(x-1)^{p^{s-1}-\iota_1},\ p(x-1)^{p^s-\iota_0} \right\rangle.$$

□

Example 1. *Let $p = 3$ and $s = 1$, so that $n = p^s = 3$. Consider the cyclic code*

$$\mathscr{D} = \left\langle (x-1)^2 + 3,\ 3(x-1) \right\rangle = \langle (x-1)^{\iota_0} + 3(x-1)^e b(x),\ 3(x-1)^{\iota_1} \rangle$$

with $\iota_0 = 2$, $\iota_1 = 1$, $e = 0$ and $b(x) = 1$. Since $p^{s-1} = 1$, we have $p^{s-1} - \iota_1 = 0$, and therefore $\epsilon = 0$. Using (3.17)*, we obtain*

$$b^{\perp}(x) = 2.$$

Hence, by Theorem 7,

$$\mathscr{D}^{\perp} = \left\langle (x-1)^2 + 6,\ 3(x-1) \right\rangle.$$

Equivalently, since $(x-1)^2 = x^2 - 2x + 1 \equiv x^2 + 7x + 1 \pmod 9$, one may write

$$\mathscr{D}^{\perp} = \langle x^2 + 7x + 7,\ 3(x-1) \rangle \subseteq \mathbb{Z}_9[x]/\langle x^3 - 1 \rangle.$$

4. Quantum codes from cyclic codes over $\mathcal{R}_{p,\alpha}$

In this section, we construct p-ary quantum stabilizer codes from cyclic codes over $\mathcal{R}_{p,\alpha}$ using the Gray map developed earlier. Throughout, p is an odd prime and $\alpha \in \mathbb{F}_p^{\times}$ is a quadratic residue, so that

$$\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}, \qquad r = e_1 r_1 + e_2 r_2,$$

with orthogonal idempotents e_1, e_2 as in (2.4).

For the purposes of quantum-code constructions, we use the symplectic ordering of Gray coordinates

$$\Psi_s : \mathcal{R}_{p,\alpha} \longrightarrow \mathbb{F}_p^4, \qquad \Psi_s(a + pb + uc + upd) = (a, c, b, d), \tag{4.1}$$

extended coordinatewise to $\Psi_s : \mathcal{R}_{p,\alpha}^n \to \mathbb{F}_p^{4n}$. This map is $\mathbb{F}_p$-linear and isometric from Lee distance to Hamming distance, since it differs from the Gray map of Section 2 only by an invertible $\mathbb{F}_p$-linear change of coordinates.

We identify $\mathbb{F}_p^{4n}$ with $\mathbb{F}_p^{2N}$, where $N = 2n$, by grouping coordinates into pairs:

$$(x_1, \ldots, x_{2N}) = (x \mid z), \qquad x, z \in \mathbb{F}_p^N.$$

The standard symplectic inner product on $\mathbb{F}_p^{2N}$ is

$$\langle (x \mid z), (x' \mid z') \rangle_s = x \cdot z' - z \cdot x',$$

and for a linear code $D \subseteq \mathbb{F}_p^{2N}$ its symplectic dual is

$$D^{\perp_s} = \{\, v \in \mathbb{F}_p^{2N} \mid \langle v, w \rangle_s = 0 \text{ for all } w \in D \,\}.$$

Theorem 8 ([2])**.** *Let $D \subseteq \mathbb{F}_p^{2N}$ be an $\mathbb{F}_p$-linear code satisfying $D \subseteq D^{\perp_s}$. Then, there exists a p-ary quantum stabilizer code with parameters*

$$[[\, N,\ N - \dim_{\mathbb{F}_p} D,\ d_q \,]]_p, \qquad d_q = \min\{\, w_H(v) \mid v \in D^{\perp_s} \setminus D \,\}.$$

The relationship between Euclidean orthogonality in $\mathcal{R}_{p,\alpha}^n$ and symplectic orthogonality in $\mathbb{F}_p^{4n}$ is governed by the linear transformation relating the Gray coordinate orderings. Let

$$S = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix}.$$

If $M \in \mathrm{GL}_4(\mathbb{F}_p)$ denotes the change-of-coordinates matrix appearing earlier (cf. (2.10)), then

$$M^T S M = \lambda S, \qquad \lambda \in \mathbb{F}_p^{\times}. \tag{4.2}$$

Thus, M is a symplectic similitude: symplectic orthogonality is preserved (up to a nonzero scalar), and therefore preserved as a vanishing condition.

Lemma 7. *Let $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$. If $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ with respect to the Euclidean inner product over $\mathcal{R}_{p,\alpha}$, then*

$$\Psi_s(\mathscr{C}) \subseteq \Psi_s(\mathscr{C})^{\perp_s} \quad \text{in} \quad \mathbb{F}_p^{4n} \cong \mathbb{F}_p^{2N},\ N = 2n.$$

Proof. Write $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ with $\mathscr{C}^{(i)} \subseteq \mathbb{Z}_{p^2}^n$ cyclic, as in (3.2). For $\mathbf{c} = e_1\mathbf{c}_1 + e_2\mathbf{c}_2$ and $\mathbf{d} = e_1\mathbf{d}_1 + e_2\mathbf{d}_2$, one has

$$\langle \mathbf{c}, \mathbf{d} \rangle = e_1 \langle \mathbf{c}_1, \mathbf{d}_1 \rangle_{\mathbb{Z}_{p^2}} + e_2 \langle \mathbf{c}_2, \mathbf{d}_2 \rangle_{\mathbb{Z}_{p^2}}$$

using $e_i^2 = e_i$ and $e_1 e_2 = 0$. Hence, $\mathscr{C} \subseteq \mathscr{C}^{\perp}$ implies $\mathscr{C}^{(i)} \subseteq (\mathscr{C}^{(i)})^{\perp}$ for $i = 1, 2$.

Under the Gray map on $\mathbb{Z}_{p^2}^n$, Euclidean orthogonality is carried to symplectic orthogonality of the Gray image. Passing from that coordinate ordering to Ψ_s is achieved by a block-diagonal matrix with n copies of M; by (4.2), symplectic orthogonality is preserved. Therefore, $\Psi_s(\mathscr{C}) \subseteq \Psi_s(\mathscr{C})^{\perp_s}$. □

Theorem 9. *Let $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$ be a cyclic code such that $\mathscr{C} \subseteq \mathscr{C}^{\perp}$. Set $N = 2n$ and $D = \Psi_s(\mathscr{C}) \subseteq \mathbb{F}_p^{2N}$. Then, there exists a p-ary quantum stabilizer code with parameters*

$$[[\, 2n,\ 2n - \dim_{\mathbb{F}_p} D,\ d_q \,]]_p, \qquad d_q = \min\{\, w_H(v) \mid v \in D^{\perp_s} \setminus D \,\}.$$

Moreover, since Ψ_s is an isometry,

$$d_H(D) = d_L(\mathscr{C}).$$

Proof. By Lemma 7, $D \subseteq D^{\perp_s}$. Applying Theorem 8 yields a stabilizer code with parameters $[[N, N - \dim_{\mathbb{F}_p} D, d_q]]_p$ where $N = 2n$. Finally, Ψ_s preserves Lee and Hamming distances, so $d_H(D) = d_L(\mathscr{C})$. □

The quantum distance d_q is controlled by vectors in $D^{\perp_s} \setminus D$. In general, one always has

$$d_q \ \geq \ d_H(D^{\perp_s}), \tag{4.3}$$

since $D^{\perp_s} \setminus D \subseteq D^{\perp_s} \setminus \{0\}$. However, the stronger bound $d_q \geq d_H(D) = d_L(\mathscr{C})$ requires a *purity* condition.

Definition 1. *A symplectic self-orthogonal code $D \subseteq \mathbb{F}_p^{2N}$ is called* pure *if D contains no nonzero vector of symplectic dual weight below d_q; equivalently,*

$$\min\{w_H(v) \mid v \in D^{\perp_s} \setminus \{0\}\} = \min\{w_H(v) \mid v \in D^{\perp_s} \setminus D\}.$$

Proposition 2. *Let $D \subseteq \mathbb{F}_p^{2N}$ satisfy $D \subseteq D^{\perp_s}$. If*

$$d_H(D^{\perp_s}) \ \geq \ d_H(D), \tag{4.4}$$

then the associated stabilizer code is pure and

$$d_q \geq d_H(D).$$

Consequently, for $D = \Psi_s(\mathscr{C})$, one obtains

$$d_q \geq d_H(D) = d_L(\mathscr{C}).$$

Proof. Assume (4.4). Then, every nonzero vector in $D^{\perp_s}$ has Hamming weight at least $d_H(D^{\perp_s}) \geq d_H(D)$. In particular, every $v \in D^{\perp_s} \setminus D$ has weight at least $d_H(D)$, hence

$$d_q = \min\{w_H(v) \mid v \in D^{\perp_s} \setminus D\} \geq d_H(D).$$

The last assertion follows from $d_H(D) = d_L(\mathscr{C})$. □

Condition (4.4) is not automatic, but it becomes clean and checkable in several natural families arising from cyclic constructions.

Family A: designed dual distance via BCH-type bounds. Suppose the Gray image $D = \Psi_s(\mathscr{C})$ (or an equivalent monomially-permuted version of it) is a cyclic code over $\mathbb{F}_p$. Then, $D^{\perp_s}$ is again cyclic, and one may lower the bound $d_H(D^{\perp_s})$ by a BCH bound, using the defining set of $D^{\perp_s}$. In particular, if one can guarantee a designed distance δ for $D^{\perp_s}$, i.e.,

$$d_H(D^{\perp_s}) \geq \delta,$$

and if simultaneously $d_H(D) \leq \delta$, then (4.4) holds and hence

$$d_q \geq d_H(D) = d_L(\mathscr{C}).$$

This is especially useful in the coprime case $\gcd(n, p) = 1$, where the cyclic structure is most rigid and BCH estimates are clean.

Family B: componentwise dual-distance domination. Write $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$ with $\mathscr{C}^{(i)} \subseteq \mathbb{Z}_{p^2}^n$ cyclic. If in addition the Gray image splits into disjoint coordinate blocks as in (4.5), then one can ensure (4.4) by imposing the stronger pair of conditions

$$d_H(\Psi_0((\mathscr{C}^{(i)})^\perp)) \;\geq\; d_H(\Psi_0(\mathscr{C}^{(i)})) \qquad (i = 1, 2),$$

because then

$$d_H(D^{\perp_s}) \geq \min_{i=1,2} d_H(\Psi_0((\mathscr{C}^{(i)})^\perp)) \geq \min_{i=1,2} d_H(\Psi_0(\mathscr{C}^{(i)})) = d_H(D).$$

In practice, one enforces this by choosing component codes whose *dual* has a known BCH (or other) designed distance not smaller than that of the code itself.

Family C: enforced purity by excluding low-weight dual vectors. If a construction guarantees that *every* vector in $D^{\perp_s}$ of weight $< d_H(D)$ actually lies in D, then automatically $d_q \geq d_H(D)$. Equivalently,

$$D^{\perp_s} \cap \{v :\; 1 \leq w_H(v) < d_H(D)\} \subseteq D.$$

This is often verified computationally for short lengths (and then used as a design constraint in searches), and it is exactly the classical notion of purity for stabilizer codes.

To express $\dim_{\mathbb{F}_p} D$ and $d_L(\mathscr{C})$ in terms of cyclic components, write

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)},$$

with $\mathscr{C}^{(i)} \subseteq \mathbb{Z}_{p^2}^n$ cyclic. Since Ψ_s is $\mathbb{F}_p$-linear and acts componentwise with respect to the idempotent decomposition, write

$$\dim_{\mathbb{F}_p} \Psi_s(\mathscr{C}) = \dim_{\mathbb{F}_p} \Psi_0(\mathscr{C}^{(1)}) + \dim_{\mathbb{F}_p} \Psi_0(\mathscr{C}^{(2)}). \tag{4.5}$$

Because the Gray map acts on the two idempotent components in disjoint coordinate blocks, one has

$$d_L(\mathscr{C}) = \min\{d_L(\mathscr{C}^{(1)}),\, d_L(\mathscr{C}^{(2)})\}. \tag{4.6}$$

Theorem 10. *Let $\mathscr{C} \subseteq \mathcal{R}_{p,\alpha}^n$ be cyclic and self-orthogonal, and write $\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}$. Set*

$$k_i = \dim_{\mathbb{F}_p} \Psi_0(\mathscr{C}^{(i)}), \qquad d_i = d_L(\mathscr{C}^{(i)}).$$

Assume that

$$k_1 + k_2 \leq 2n.$$

Then, $\Psi_s(\mathscr{C})$ yields a p-ary quantum stabilizer code with parameters

$$[[\, 2n,\; 2n - (k_1 + k_2),\; d_q \,]]_p,$$

where

$$d_q = \min\{\, w_H(v) \mid v \in D^{\perp_s} \setminus D \,\}, \qquad D = \Psi_s(\mathscr{C}).$$

If, in addition, $d_H(D^{\perp_s}) \geq d_H(D)$ (e.g. by Proposition 2), then the code is pure and satisfies

$$d_q \geq d_H(D) = \min\{d_1, d_2\}.$$

Proof. The dimension condition ensures $\dim_{\mathbb{F}_p} D \le N = 2n$. Lemma 7 gives $D \subseteq D^{\perp_s}$, so Theorem 8 applies and yields the stated parameters. Finally, $d_H(D) = \min\{d_1, d_2\}$ follows from (4.6) and the isometry of Ψ_s. The purity refinement is exactly Proposition 2. □

Remark 3. *A nontrivial quantum dimension requires $k_1 + k_2 \le 2n$. When searching for good quantum codes, one typically enforces simultaneously: (i) self-orthogonality $\mathscr{C} \subseteq \mathscr{C}^{\perp}$, (ii) the dimension constraint $k_1 + k_2 \le 2n$, and (iii) a purity constraint such as $d_H(D^{\perp_s}) \ge d_H(D)$, which guarantees $d_q \ge d_L(\mathscr{C})$.*

5. DNA codes over $\mathcal{R}_{5,\alpha}$

In this section, we use $\mathcal{R}_{5,\alpha}$-linear codes to construct reversible DNA codes. We fix $p = 5$ and assume that $\alpha \in \mathbb{F}_5^{\times}$ is a quadratic residue. Then, $\mathcal{R}_{5,\alpha} \cong \mathbb{Z}_{25} \oplus \mathbb{Z}_{25}$ via the orthogonal idempotents e_1, e_2 from Section 3, and every $r \in \mathcal{R}_{5,\alpha}$ decomposes uniquely as

$$r = e_1 r_1 + e_2 r_2, \qquad r_1, r_2 \in \mathbb{Z}_{25}.$$

We use the IUPAC alphabet with wildcard

$$\Sigma = \{\mathtt{A}, \mathtt{T}, \mathtt{G}, \mathtt{C}, \mathtt{N}\},$$

together with the bijection $\vartheta : \mathbb{F}_5 \to \Sigma$ defined by

$$\vartheta(0) = \mathtt{N}, \quad \vartheta(1) = \mathtt{A}, \quad \vartheta(2) = \mathtt{G}, \quad \vartheta(3) = \mathtt{T}, \quad \vartheta(4) = \mathtt{C}. \tag{5.1}$$

For $v = (v_1, \ldots, v_m) \in \mathbb{F}_5^m$, we write

$$\vartheta(v) = \vartheta(v_1)\vartheta(v_2)\cdots\vartheta(v_m),$$

viewed as a DNA string of length m.

We encode ring symbols using the product Gray map adapted to the idempotent splitting. Let $\Psi_0 : \mathbb{Z}_{25} \to \mathbb{F}_5^2$ be the standard Gray map

$$\Psi_0(a + 5b) = (a, b), \qquad a, b \in \mathbb{F}_5.$$

Define

$$\Psi : \mathcal{R}_{5,\alpha} \longrightarrow \mathbb{F}_5^4, \qquad \Psi(e_1 r_1 + e_2 r_2) = \big(\Psi_0(r_1), \Psi_0(r_2)\big), \tag{5.2}$$

and extend Ψ coordinatewise to $\Psi : \mathcal{R}_{5,\alpha}^n \to \mathbb{F}_5^{4n}$. This Gray map is $\mathbb{F}_5$-linear and preserves Lee and Hamming distances (as established earlier). This choice is convenient here because each ring coordinate gives rise to a natural Gray block of length 4.

Definition 2. *For $r \in \mathcal{R}_{5,\alpha}$, define the DNA block of length* 4 *by*

$$\eta(r) = \vartheta(\Psi(r)).$$

For a code $\mathscr{C} \subseteq \mathcal{R}_{5,\alpha}^n$, define its DNA image by

$$\eta(\mathscr{C}) = \Big\{\eta(c_1)\eta(c_2)\cdots\eta(c_n) \;\Big|\; (c_1, \ldots, c_n) \in \mathscr{C}\Big\},$$

which is a set of DNA strings of length $4n$.

Reversibility of DNA strings corresponds to invariance under reversal of coordinates. Let $\mathrm{rev}_n : \mathcal{R}_{5,\alpha}^n \to \mathcal{R}_{5,\alpha}^n$ be the coordinate reversal

$$\mathrm{rev}_n(c_1, \ldots, c_n) = (c_n, \ldots, c_1),$$

and let rev_{4n} denote the reversal on $\mathbb{F}_5^{4n}$ that reverses the order of the n length-4 Gray blocks (equivalently, reverses the DNA sequence of length $4n$). Since Ψ is applied coordinatewise, it commutes with reversal at the block level.

Lemma 8. *For every $c \in \mathcal{R}_{5,\alpha}^n$, one has*

$$\Psi(\mathrm{rev}_n(c)) = \mathrm{rev}_{4n}(\Psi(c)).$$

Consequently, if $\mathscr{C} \subseteq \mathcal{R}_{5,\alpha}^n$ satisfies $\mathrm{rev}_n(\mathscr{C}) = \mathscr{C}$, then $\Psi(\mathscr{C}) \subseteq \mathbb{F}_5^{4n}$ and $\eta(\mathscr{C})$ are reversible under rev_{4n}.

Proof. The first identity follows immediately from the coordinatewise definition of Ψ, because reversing the n coordinates of c reverses the order of the corresponding n Gray blocks. If $\mathrm{rev}_n(\mathscr{C}) = \mathscr{C}$ and $y = \Psi(c) \in \Psi(\mathscr{C})$, then $\mathrm{rev}_{4n}(y) = \Psi(\mathrm{rev}_n(c)) \in \Psi(\mathscr{C})$, so the Gray image is reversible. Since ϑ is applied coordinatewise, it commutes with reversal, hence $\eta(\mathscr{C})$ is reversible. □

The ring automorphism $u \mapsto -u$ plays a structural role because it interchanges the two idempotent components. Define $\varphi : \mathcal{R}_{5,\alpha} \to \mathcal{R}_{5,\alpha}$ by $\varphi(u) = -u$ and $\varphi(a) = a$ for $a \in \mathbb{Z}_{25}$, extended $\mathbb{Z}_{25}$-linearly. Since $(-u)^2 = u^2 = \alpha$, φ is a ring automorphism. On Gray coordinates, φ induces a swap of the two $\mathbb{F}_5^2$-halves within each length-4 block.

Lemma 9. *One has $\varphi(e_1) = e_2$ and $\varphi(e_2) = e_1$. Hence, for $r = e_1 r_1 + e_2 r_2$,*

$$\varphi(r) = e_1 r_2 + e_2 r_1.$$

Moreover,

$$\Psi(\varphi(r)) = \mathrm{sw}(\Psi(r)), \qquad \mathrm{sw}(x_1, x_2, x_3, x_4) = (x_3, x_4, x_1, x_2),$$

and the same identity holds coordinatewise on $\mathcal{R}_{5,\alpha}^n$ and $\mathbb{F}_5^{4n}$ by applying sw *inside each length-*4 *block.*

Proof. Using the explicit idempotents $e_1 = (u + \beta')/(2\beta')$ and $e_2 = (\beta' - u)/(2\beta')$ from (2.4), the substitution $u \mapsto -u$ interchanges them, so $\varphi(e_1) = e_2$ and $\varphi(e_2) = e_1$. Therefore, $\varphi(e_1 r_1 + e_2 r_2) = e_2 r_1 + e_1 r_2 = e_1 r_2 + e_2 r_1$. Applying (5.2) gives the stated swap on $\mathbb{F}_5^4$, and extending coordinatewise gives the length-4 blockwise swap on $\mathbb{F}_5^{4n}$. □

We now give a convenient algebraic condition ensuring reversibility for a cyclically generated family. Let

$$g(x) = \beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1} \in \mathcal{R}_{5,\alpha}[x], \qquad \mathbf{g} = (\beta_0, \beta_1, \ldots, \beta_{n-1}) \in \mathcal{R}_{5,\alpha}^n,$$

and write $\mathbf{g}^j$ for the jth cyclic shift of $\mathbf{g}$ (indices modulo n).

Definition 3. *The polynomial $g(x)$ is called* coterm *if $\beta_i = \beta_{n-i}$ for all $1 \le i \le \lfloor n/2 \rfloor$.*

The coterm condition is exactly the statement that the coefficient vector is palindromic: $\mathrm{rev}_n(\mathbf{g}) = \mathbf{g}$, and more generally $\mathrm{rev}_n(\mathbf{g}^j) = \mathbf{g}^{-j}$ for all j (with indices taken modulo n). Fix an integer t with $0 \le t \le \lfloor (n-1)/2 \rfloor$ and define a matrix with rows

$$G_t = \begin{bmatrix} \varphi(\mathbf{g}^{-(t+1)}) \\ \vdots \\ \varphi(\mathbf{g}^{-1}) \\ \mathbf{g}^0 \\ \mathbf{g}^1 \\ \vdots \\ \mathbf{g}^t \end{bmatrix}, \qquad \mathscr{C} = \langle G_t \rangle \subseteq \mathcal{R}_{5,\alpha}^n. \tag{5.3}$$

Theorem 11. *Let $g(x)$ be coterm and let $\mathscr{C}$ be the $\mathcal{R}_{5,\alpha}$-linear code generated by* (5.3)*. Then,* $\mathrm{rev}_n(\mathscr{C}) = \mathscr{C}$*. Consequently, $\Psi(\mathscr{C}) \subseteq \mathbb{F}_5^{4n}$ is reversible under* rev_{4n}*, and the DNA code $\eta(\mathscr{C})$ is reversible.*

Proof. Because g is coterm, $\mathrm{rev}_n(\mathbf{g}^j) = \mathbf{g}^{-j}$ for all j. Since φ is a ring automorphism, it commutes with taking $\mathcal{R}_{5,\alpha}$-linear spans and satisfies

$$\mathrm{rev}_n(\varphi(\mathbf{g}^{-j})) = \varphi(\mathrm{rev}_n(\mathbf{g}^{-j})) = \varphi(\mathbf{g}^j).$$

Indeed, for each $j = 0, \ldots, t$, one has $\mathrm{rev}_n(\mathbf{g}^j) = \mathbf{g}^{-j}$, while for $j = 1, \ldots, t+1$,

$$\mathrm{rev}_n(\varphi(\mathbf{g}^{-j})) = \varphi(\mathbf{g}^j),$$

and these vectors lie in the $\mathcal{R}_{5,\alpha}$-span generated by the rows of G_t. Therefore, the row span $\mathscr{C} = \langle G_t \rangle$ is stable under rev_n, i.e., $\mathrm{rev}_n(\mathscr{C}) = \mathscr{C}$. The remaining conclusions follow from Lemma 8 and the coordinatewise nature of ϑ. □

The Gray map allows us to read distance and GC-content directly from the $\mathbb{F}_5$-image. Since Ψ is a Gray isometry,

$$d_H(\Psi(\mathscr{C})) = d_L(\mathscr{C}),$$

and the natural DNA distance induced via ϑ agrees with Hamming distance on $\Psi(\mathscr{C})$. Thus, the metric properties of $\eta(\mathscr{C})$ are controlled by the Lee distance of $\mathscr{C}$ (equivalently, the Hamming distance of $\Psi(\mathscr{C})$). Under the fixed bijection (5.1), the GC-content of a DNA word is the number of symbols in $\{\mathtt{G}, \mathtt{C}\}$, hence it is determined by the frequency of field symbols 2 and 4 in the Gray vector. Because each ring coordinate contributes a length-4 Gray block, the distribution of 2 and 4 can be influenced through the choice of the coterm polynomial $g(x)$ and the parameter t in (5.3), which together control the set of Gray words that occur.

Finally, we record a simple closure property for the wildcard deletion operation, which is often used when one wishes to remove unspecified bases from a code over Σ.

Proposition 3. *Let $\mathcal{D}$ be a reversible DNA code over $\Sigma = \{\mathtt{A}, \mathtt{T}, \mathtt{G}, \mathtt{C}, \mathtt{N}\}$. For $s \in \mathcal{D}$, let $\widetilde{s}$ be the string obtained by deleting all occurrences of* N*, and set*

$$\widetilde{\mathcal{D}} = \{\widetilde{s} \mid s \in \mathcal{D}\}.$$

Then, $\widetilde{\mathcal{D}}$ is reversible.

Proof. Let $d(\cdot)$ denote deletion of all N-symbols, and let rev denote reversal of a DNA string. Since deletion is performed symbolwise and reversal only permutes positions, one has

$$d(\mathrm{rev}(s)) = \mathrm{rev}(d(s))$$

for every DNA string s. If $s \in \mathcal{D}$, then $\mathrm{rev}(s) \in \mathcal{D}$ by reversibility. Hence, if $\widetilde{s} = d(s) \in \widetilde{\mathcal{D}}$, then

$$\mathrm{rev}(\widetilde{s}) = \mathrm{rev}(d(s)) = d(\mathrm{rev}(s)) \in \widetilde{\mathcal{D}}.$$

Therefore, $\widetilde{\mathcal{D}}$ is reversible. □

6. Numerical examples and code constructions

This section illustrates the theoretical results of Sections 4 and 5 through explicit computations and concrete code constructions. We also compare the parameters of the resulting codes with the best-known values reported in the literature. Throughout this section, all computations were performed using the computer algebra system Magma [33]. Unless stated otherwise, distances reported for Gray images are Hamming distances over the field $\mathbb{F}_3$.

We begin with the ternary settings $p = 3, \alpha = 1$, for which the ring

$$\mathcal{R}_{3,1} = \mathbb{Z}_9[u]/\langle u^2 - 1\rangle \cong \mathbb{Z}_9 \oplus \mathbb{Z}_9$$

is decomposable. This decomposition plays a central role in the construction of cyclic codes over $\mathcal{R}_{3,1}$ and in the analysis of their Gray images.

Since $\alpha = 1$ is a square in $\mathbb{F}_3$, we take $\beta' = 1 \in \mathbb{Z}_9$ as a Hensel lift of $\beta = 1 \in \mathbb{F}_3$. The idempotents in (2.4) specialize to

$$e_1 = \frac{u+1}{2}, \qquad e_2 = \frac{1-u}{2},$$

where $1/2 = 2$ in both $\mathbb{Z}_9$ and $\mathbb{F}_3$. Every element $r \in \mathcal{R}_{3,1}$ can therefore be written uniquely as

$$r = e_1 r_1 + e_2 r_2, \qquad r_i = a_i + 3b_i \in \mathbb{Z}_9, \;\; a_i, b_i \in \mathbb{F}_3.$$

The product Gray map used in the classical and DNA-code discussions is

$$\Psi(r) = (\Psi_0(r_1), \Psi_0(r_2)) = (a_1, b_1, a_2, b_2) \in \mathbb{F}_3^4, \qquad \Psi_0(a + 3b) = (a, b).$$

For the construction of quantum stabilizer codes we use the symplectic ordering. Writing $r = a + 3b + uc + 3ud$ with $a, b, c, d \in \mathbb{F}_3$, we set

$$\Psi_s(r) = (a, c, b, d) \in \mathbb{F}_3^4.$$

These two Gray descriptions are related by the linear change-of-coordinates matrix in (2.10). For $\beta' = 1$, this matrix becomes

$$M = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_3),$$

hence, using $1/2 = 2$ and $-1 = 2$ in $\mathbb{F}_3$,

$$M = \begin{pmatrix} 2 & 0 & 2 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & 0 & 1 \end{pmatrix}, \qquad M^{-1} = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix}.$$

In particular, Ψ and Ψ_s are linearly equivalent and hence induce the same Lee/Hamming isometry.

We first consider the case of coprime lengths. Let n be a positive integer with $\gcd(n, 3) = 1$. By Proposition 1, every cyclic code $\mathscr{C} \subseteq \mathcal{R}_{3,1}^n$ decomposes as

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}, \qquad \mathscr{C}^{(i)} = \langle g_i(x) \rangle \subseteq \mathbb{Z}_9[x]/\langle x^n - 1 \rangle,$$

where $g_i(x)$ are monic divisors of $x^n - 1$ in $\mathbb{Z}_9[x]$.

The Gray image $\Psi(\mathscr{C})$ is then a ternary linear code of length $N = 4n$ and dimension

$$k = \dim_{\mathbb{F}_3} \Psi(\mathscr{C}) = 2[(n - \deg g_1) + (n - \deg g_2)] = 4n - 2(\deg g_1 + \deg g_2). \tag{6.1}$$

Example 2. *For the values of n listed in Table 2, we fixed Hensel lifts in $\mathbb{Z}_9[x]$ of factorizations of $x^n - 1$ over $\mathbb{F}_3[x]$ (unique up to the standard* Magma *normalization). The auxiliary factors used are*

$$\begin{aligned}
&n = 7: && x^7 - 1 = (x - 1)h_1h_2, \;\; h_1 = x^3 + x + 1, \;\; h_2 = x^3 + 2x + 1, \\
&n = 11: && x^{11} - 1 = (x - 1)q_1q_2, \;\; q_1 = x^5 + x^3 + x^2 + 2, \;\; q_2 = x^5 + 2x^3 + 2x^2 + 2, \\
&n = 13: && x^{13} - 1 = (x - 1)h_1h_2h_3h_4, \;\; h_3 = x^3 + x^2 + 2, \;\; h_4 = x^3 + 2x^2 + 2, \\
&n = 17: && x^{17} - 1 = (x - 1)f_{16}(x), \\
&n = 19: && x^{19} - 1 = (x - 1)f_{18}(x),
\end{aligned}$$

where, for reproducibility,

$$\begin{aligned}
f_{16}(x) &= x^{16} + x^{15} + x^{14} + 2x^{13} + 2x^{12} + x^{11} + 2x^{10} + 2x^9 + x^8 + 2x^7 + 2x^6 + x^5 \\
&\quad + 2x^4 + 2x^3 + x^2 + x + 1, \\
f_{18}(x) &= x^{18} + x^{17} + 2x^{16} + x^{15} + 2x^{14} + 2x^{13} + 2x^{12} + x^{11} + 2x^{10} + 2x^9 + x^8 + 2x^7 \\
&\quad + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 1.
\end{aligned}$$

Table 2. Parameters of Gray images of cyclic codes over $\mathcal{R}_{3,1}$ for $\gcd(n, 3) = 1$.

n	Generator pair (g_1, g_2)	$\deg g_1$	$\deg g_2$	$[N, k, d]_3$	Status
7	$(h_1h_2,\ x - 1)$	6	1	$[28, 14, 8]_3$	optimal
11	$(q_1,\ x - 1)$	5	1	$[44, 32, 10]_3$	optimal
13	$(h_1h_2,\ h_3)$	6	3	$[52, 34, 12]_3$	optimal
13	$(h_1h_2h_3,\ x - 1)$	9	1	$[52, 32, 14]_3$	best known
13	$(h_1h_2h_3h_4,\ x - 1)$	12	1	$[52, 20, 3]_3$	optimal
17	$(f_{16},\ x - 1)$	16	1	$[68, 34, 20]_3$	optimal
19	$(f_{18},\ x - 1)$	18	1	$[76, 38, 22]_3$	optimal

In Table 2, the dimension k follows from (6.1), while the minimum distance d was computed in Magma by applying minimum-distance routines to the ternary Gray generator matrices. The status of each code was determined by comparison with the database of best-known linear codes maintained by Grassl [24]. In Table 2, the label *optimal* indicates that the code attains the best possible minimum distance for the given length and dimension, while *best known* indicates that it matches the largest currently recorded distance in [24].

These examples demonstrate that the decomposable structure $\mathcal{R}_{3,1} \cong \mathbb{Z}_9 \oplus \mathbb{Z}_9$ can produce strong ternary linear codes through the Gray map. A recurring effective strategy is to choose one component generator of relatively large degree to increase the minimum distance while keeping the other component close to $x - 1$ in order to maintain dimension. Notably, the code $[52, 32, 14]_3$ improves the previously listed minimum distance for the same parameters in [24].

Remark 4. *In our search for $p = 3$ and prime lengths $n \in \{5, 7, 11, 13, 17, 19\}$, we found no nontrivial Euclidean self-orthogonal cyclic codes over $\mathcal{R}_{3,1}$ arising from the componentwise criterion*

$$\mathscr{C} \subseteq \mathscr{C}^{\perp} \quad \Longleftrightarrow \quad \mathscr{C}^{(i)} \subseteq (\mathscr{C}^{(i)})^{\perp}, \qquad i = 1, 2,$$

together with the reciprocal-divisibility condition over $\mathbb{Z}_9$. This reflects the rigidity of defining sets at these prime lengths; the negation-closure obstruction makes it difficult to select large defining sets avoiding $-T$ simultaneously. For such prime lengths, quantum constructions are therefore more naturally pursued via asymmetric CSS pairs $(\mathscr{C}^{(2)})^{\perp} \subseteq \mathscr{C}^{(1)}$, or via repeated-root lengths $n = 3^s$ where dual-containing conditions can be enforced through the vanishing-order parameters (ι_0, ι_1).

Next, we illustrate the construction of optimal quantum codes obtained from cyclic codes over the ring $\mathbb{Z}_{p^2}$ using the structure theory of Section 3.2 and the quantum construction in Theorem 10. In contrast with the classical finite-field setting, the ring framework provides additional algebraic flexibility through its repeated-root structure. The following examples show how this extra structure leads to quantum stabilizer codes with optimal parameters, and therefore highlight one of the main contributions of this work.

Example 3. *Let $p = 7$ and $n = 6$. Then, $N = 2n = 12$, and the symplectic Gray image lives in*

$$\mathbb{F}_7^{4n} \cong \mathbb{F}_7^{2N} = \mathbb{F}_7^{24}.$$

First, consider the cyclic code $C_0 \subseteq \mathbb{F}_7^6$ generated by

$$g(x) = x^3 + 3x^2 + x + 6.$$

A Magma *computation shows that $g(x) \mid (x^6 - 1)$ and that C_0 has parameters*

$$[6, 3, 4]_7.$$

Viewing C_0 as an $\mathbb{F}_7$-subspace of $\mathbb{Z}_{49}^6$ via the natural embedding $\mathbb{F}_7 \hookrightarrow \mathbb{Z}_{49}$, set

$$\mathscr{C}^{(1)} = 7C_0, \qquad \mathscr{C}^{(2)} = 7C_0.$$

Let

$$\mathcal{R}_{7,1} = \mathbb{Z}_{49}[u]/\langle u^2 - 1\rangle \cong \mathbb{Z}_{49} \oplus \mathbb{Z}_{49}$$

with orthogonal idempotents e_1, e_2, and define

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)} \subseteq \mathcal{R}_{7,1}^6.$$

Let $D = \Psi_s(\mathscr{C}) \subseteq \mathbb{F}_7^{24}$. The associated Gray-image component codes satisfy

$$k_1 = k_2 = 3, \qquad d_1 = d_2 = 4.$$

Hence,

$$k = 12 - k_1 - k_2 = 12 - 3 - 3 = 6, \qquad d_q = \min\{d_1, d_2\} = 4,$$

and this construction yields a 7-ary stabilizer code with parameters

$$[[12, 6, 4]]_7.$$

Since the quantum Singleton bound gives

$$d_q \leq \frac{12 - 6}{2} + 1 = 4,$$

this code is quantum MDS and therefore optimal. It also matches the optimal parameters listed in the database of [24] for length 12 *and dimension* 6 *over* $\mathbb{F}_7$.

Next, consider the cyclic code $C_0 \subseteq \mathbb{F}_7^6$ generated by

$$g(x) = x^4 + x^2 + 1.$$

Again, $g(x) \mid (x^6 - 1)$, and C_0 has parameters

$$[6, 2, 3]_7.$$

Viewing C_0 as a $\mathbb{Z}_{49}$-submodule of $\mathbb{Z}_{49}^6$, set

$$\mathscr{C}^{(1)} = 7C_0, \qquad \mathscr{C}^{(2)} = 7C_0,$$

and define

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)} \subseteq \mathcal{R}_{7,1}^6.$$

Let $D = \Psi_s(\mathscr{C}) \subseteq \mathbb{F}_7^{24}$. In this case

$$k_1 = k_2 = 2, \qquad d_1 = d_2 = 3.$$

Therefore,

$$k = 12 - k_1 - k_2 = 12 - 2 - 2 = 8, \qquad d_q = \min\{d_1, d_2\} = 3,$$

and we obtain a stabilizer code with parameters

$$[[12, 8, 3]]_7.$$

Since the quantum Singleton bound gives

$$d_q \leq \frac{12 - 8}{2} + 1 = 3,$$

this code is also quantum MDS and therefore optimal.

These examples demonstrate that the ring-based construction can produce optimal stabilizer codes of different quantum dimensions for the same ambient length.

The next example gives a coprime-length example whose parameters meet the quantum Singleton bound and improve upon the previously recorded minimum distance.

Example 4. *Let $p = 5$, $\alpha = 1$, and $n = 12$. Then, $N = 2n = 24$, and the symplectic Gray image lives in*

$$\mathbb{F}_5^{4n} \cong \mathbb{F}_5^{2N} = \mathbb{F}_5^{48}.$$

Let $\mathscr{C}_0 \subseteq \mathbb{F}_5^{12}$ be the cyclic code generated by

$$g(x) = x^7 + 4x^6 + x^5 + 2x^4 + 2x^2 + 4 \in \mathbb{F}_5[x].$$

A Magma *verification shows that $g(x) \mid (x^{12} - 1)$, and that $\mathscr{C}_0$ has parameters*

$$[12, 5, 6]_5.$$

View $\mathscr{C}_0$ as a $\mathbb{Z}_{25}$-submodule of $\mathbb{Z}_{25}^{12}$ by lifting the coefficients

$$\{0, 1, 2, 3, 4\} \subset \mathbb{Z}_{25},$$

and set

$$\mathscr{C}^{(1)} = 5C_0 \subseteq \mathbb{Z}_{25}^{12}, \qquad \mathscr{C}^{(2)} = 5C_0 \subseteq \mathbb{Z}_{25}^{12}.$$

Let

$$\mathcal{R}_{5,1} = \mathbb{Z}_{25}[u]/\langle u^2 - 1\rangle \cong \mathbb{Z}_{25} \oplus \mathbb{Z}_{25}$$

with orthogonal idempotents e_1, e_2, and define the cyclic code

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)} \subseteq \mathcal{R}_{5,1}^{12}.$$

Let

$$D = \Psi_s(\mathscr{C}) \subseteq \mathbb{F}_5^{48}.$$

A Magma *computation confirms that D is an $\mathbb{F}_5$-linear code with*

$$\dim_{\mathbb{F}_5}(D) = 10, \qquad d_H(D) = 6, \qquad D \subseteq D^{\perp_s}.$$

Hence, by Theorem 8, D yields a 5-ary stabilizer code with parameters

$$[[\, N,\ N - \dim_{\mathbb{F}_5}(D),\ d_q \,]]_5 = [[\, 24,\ 14,\ d_q \,]]_5, \qquad d_q = \min\{d_1, d_2\} = 6.$$

Computing d_q directly from the definition in Magma *gives $d_q = 6$. Since the quantum Singleton bound implies*

$$d_q \leq \frac{24 - 14}{2} + 1 = 6,$$

the resulting code has parameters

$$[[24, 14, 6]]_5,$$

and is therefore quantum MDS.

For comparison, the database of [24] lists the entry $[[24, 14, 5]]_5$ for length 24 and dimension 14 over $\mathbb{F}_5$. Thus, the present construction improves the previously recorded minimum distance, and at the same time, meets the quantum Singleton bound.

The preceding examples follow a common construction pattern, which we summarize below.

$$[[2n, k_q, d_q]]_p$$

from cyclic codes $\mathscr{C}$ over $\mathcal{R}_{p,\alpha}$. Let $N = 2n$. The construction proceeds as follows:
Step 1. Construct two cyclic codes

$$\mathscr{C}^{(1)}, \mathscr{C}^{(2)} \subseteq \mathbb{Z}_{p^2}^n.$$

Step 2. Form the combined code

$$\mathscr{C} = e_1\mathscr{C}^{(1)} \oplus e_2\mathscr{C}^{(2)}.$$

Step 3. Apply the symplectic Gray map to obtain

$$D = \Psi_s(\mathscr{C}) \subseteq \mathbb{F}_p^{2N}.$$

Step 4. Verify the symplectic self-orthogonality condition

$$D \subseteq D^{\perp_s}.$$

Step 5. Compute the Hamming distances of the component Gray images

$$d_i = d_H(\Psi_0(\mathscr{C}^{(i)})), \qquad i = 1, 2,$$

and set

$$d_q = \min\{d_1, d_2\}.$$

Step 6. Report the parameters of the resulting quantum code as

$$[[N, K, d_q]]_p,$$

where

$$K = N - \dim_{\mathbb{F}_p} D.$$

We close with reversible DNA constructions over $\mathcal{R}_{5,1}$ obtained via the coterm method of Theorem 11. By selecting coterm polynomials $g(x) \in \mathcal{R}_{5,1}[x]$ together with a parameter t, one obtains families of reversible DNA codes whose algebraic, metric, and biochemical properties can be tuned explicitly.

Example 5. *Throughout this subsection, we fix $\alpha = 1$, so that*

$$\mathcal{R}_{5,1} \cong \mathbb{Z}_{25} \oplus \mathbb{Z}_{25},$$

and we use the nucleotide correspondence ϑ from (5.1)*. Reversibility is enforced algebraically through the coterm condition together with the involution $u \mapsto -u$, while the Hamming distance and GC-content can be controlled through the coefficient structure of the coterm polynomial $g(x)$.*

Table 3 lists representative reversible DNA codes obtained from coterm constructions over $\mathcal{R}_{5,1}$. In each case, the resulting DNA code has length $4n$, is reversible by construction, and exhibits controlled GC-content. In particular, several examples achieve exact 50% GC-content, while longer coterm polynomials allow nontrivial deviations when desired.

Table 3. Reversible DNA codes from coterm constructions over $\mathcal{R}_{5,1}$.

n	Coterm $g(x)$	t	DNA length $4n$	d_H	GC-content
3	$e_1(x^2+4x+1)+e_2(x+4)$	0	12	3	50%
4	$e_1(x^3+4x^2+4x+1)+e_2(x^2+1)$	0	16	4	50%
6	$e_1(x+1)^2(x+4)+e_2(x+4)$	1	24	3	50%
7	$e_1(x^6+x^5+x^4+x^3+x^2+x+1)+e_2(x^6+x^5+x^4+x^3+x^2+x+1)$	0	28	28	42.9%
8	$e_1(x^5+1)(x^2+3x+3)+e_2(x+4)$	1	32	4	50%

Example 6. *Let $n = 3$ and consider the coterm polynomial*

$$g(x) = e_1(x^2+4x+1)+e_2(x+4) \in \mathcal{R}_{5,1}[x].$$

With $t = 0$, the generator matrix G_0 in (5.3) *defines an $\mathcal{R}_{5,1}$-linear code $\mathscr{C} \subseteq \mathcal{R}_{5,1}^3$. Its Gray image*

$$C = \Psi(\mathscr{C}) \subseteq \mathbb{F}_5^{12}$$

is a reversible linear code with minimum Hamming distance $d_H(C) = 3$.

Applying the DNA map $\eta = \vartheta \circ \Psi$ produces a reversible DNA code $\eta(\mathscr{C})$ of length 12*. Representative DNA strings generated by this coterm polynomial are listed in Table 4. Each string appears together with its reverse, and all listed codewords contain exactly six symbols from* {G, C}*, yielding GC-content equal to* 50%*.*

Table 4. DNA strings from the coterm polynomial $g(x) = e_1(x^2+4x+1)+e_2(x+4)$.

DNA string	Reverse	GC-content
CGGTTAGCGTCA	ACTGCGATTGGC	6/12
GCTGCGATATGT	TGTATAGCGTCG	6/12
ATGCGCTTACGA	AGCATTCGCGTA	6/12
GCGATATGCTGC	CGTCGTATAGCG	6/12

Taken together, Tables 3 and 4 show that the decomposable structure of $\mathcal{R}_{5,1}$ provides an effective algebraic setting for DNA code design. Reversibility is guaranteed at the ring level, Gray isometries preserve distance, and biochemical constraints such as GC-content can be incorporated directly through algebraic choices of coterm polynomials, without the need for postprocessing at the DNA-symbol level.

Example 7. *We continue with the coterm construction of Example 6 and describe explicitly the associated Gray blocks and DNA symbols, see Table 5. Let $n = 3$ and*

$$g(x) = e_1(x^2+4x+1)+e_2(x+4) \in \mathcal{R}_{5,1}[x].$$

Then, $\mathbf{g} = (\beta_0, \beta_1, \beta_2)$ with

$$\beta_0 = e_1(1)+e_2(4), \qquad \beta_1 = e_1(4)+e_2(1), \qquad \beta_2 = e_1(1)+e_2(0).$$

Under the product Gray map,

$$\Psi(\beta_0) = (1, 0, 4, 0), \qquad \Psi(\beta_1) = (4, 0, 1, 0), \qquad \Psi(\beta_2) = (1, 0, 0, 0).$$

Using the nucleotide correspondence $\vartheta(0) = \mathtt{N}$, $\vartheta(1) = \mathtt{A}$, $\vartheta(4) = \mathtt{C}$, *we obtain*

$$\eta(\beta_0) = \mathtt{ANCN}, \qquad \eta(\beta_1) = \mathtt{CNAN}, \qquad \eta(\beta_2) = \mathtt{ANNN}.$$

Hence, the DNA word associated with $\mathbf{g}$ *is*

$$\eta(\mathbf{g}) = \mathtt{ANCNCNANANNN},$$

which has length $4n = 12$.

Table 5. Exact alignment of Gray coordinates with DNA symbols (product Gray map).

$r = e_1(a_1 + 5b_1) + e_2(a_2 + 5b_2)$	$\Psi(r) = (a_1, b_1, a_2, b_2)$	$\eta(r) = \vartheta(a_1)\vartheta(b_1)\vartheta(a_2)\vartheta(b_2)$
$e_1(1) + e_2(4)$	$(1, 0, 4, 0)$	ANCN
$e_1(4) + e_2(1)$	$(4, 0, 1, 0)$	CNAN
$e_1(1) + e_2(0)$	$(1, 0, 0, 0)$	ANNN

7. Conclusions

This work studies cyclic, quantum, and DNA codes over the mixed-characteristic ring $\mathcal{R}_{p,\alpha} = \mathbb{Z}_{p^2}[u]/\langle u^2 - \alpha\rangle, \alpha \in \mathbb{F}_p^*$, with particular emphasis on the decomposable case where α is a quadratic residue. In this situation, the ring splits as $\mathcal{R}_{p,\alpha} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$, which yields canonical descriptions of cyclic codes through two cyclic $\mathbb{Z}_{p^2}$ components, together with explicit generators, duals, and self-orthogonality criteria. An $\mathbb{F}_p$-linear Gray isometry $\mathcal{R}_{p,\alpha}^n \to \mathbb{F}_p^{4n}$ transfers Lee distance to Hamming distance and produces classical p-ary codes with optimal or best-known parameters. Using a symplectic ordering, the same Gray map supports CSS quantum stabilizer constructions. In particular, repeated-root lengths $n = p^s$ are well suited for producing dual-containing families, while coprime lengths exhibit inherent self-orthogonality restrictions. For $p = 5$, the product Gray map combined with a nucleotide bijection yields DNA codes of length $4n$. Reversibility is enforced algebraically through the involution $u \mapsto -u$ and coterm polynomials, enabling direct control of distance and GC-content through ring-linear design.

Future work includes constacyclic and skew-cyclic analogues over $\mathcal{R}_{p,\alpha}$, extensions to $\mathbb{Z}_{p^k}[u]/\langle u^2 - \alpha\rangle$, and investigating whether Gray images of cyclic families exhibit LDPC-type sparsity properties. On the DNA side, incorporating reverse-complement constraints and establishing bounds for reversible codes with prescribed GC-content remain promising directions.

Author contributions

Sami H. Saif: Conceptualization, Methodology, Formal analysis, Investigation, Writing-review and editing, Writing-original draft; Shayea Aldossari: Data curation, Software, Visualization, Writing – review & editing, Funding acquisition. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

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

Acknowledgments

The authors would like to extend their sincere appreciation to the Ongoing Research Funding program, (ORF-2026-839), King Saud University, Riyadh, Saudi Arabia.

Conflict of interest

The authors declare no conflicts of interest.

References

1. S. Zhu, Y. Wang, M. Shi, Some results on cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory*, **56** (2010), 1680–1684. https://doi.org/10.1109/TIT.2010.2040896
2. M. Ashraf, N. Khan, G. Mohammad, New quantum and LCD codes over finite fields of odd characteristic, *Int. J. Theor. Phys.*, **60** (2021), 2322–2332. https://doi.org/10.1007/s10773-021-04849-2
3. X. Zeng, Y. Zhang, J. Gao, Linear codes from defining sets over $\mathbb{F}_p + u\mathbb{F}_p$ and their applications, *Comput. Appl. Math.*, **43** (2024), 13. https://doi.org/10.1007/s40314-023-02527-z
4. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, **40** (1994), 301–319. https://doi.org/10.1109/18.312154
5. M. Ashraf, G. Mohammad, Quantum codes from cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, *Quantum Inf. Process.*, **15** (2016), 4089–4098. https://doi.org/10.1007/s11128-016-1379-8
6. B. Yildiz, I. Siap, Cyclic codes over $\mathbb{F}_2[u]/(u^4 - 1)$ and applications to DNA codes, *Comput. Math. Appl.*, **63** (2012), 1169–1176. https://doi.org/10.1016/j.camwa.2011.12.029
7. J. Qian, W. Ma, W. Gou, Quantum codes from cyclic codes over finite rings, *Int. J. Quantum Inf.*, **50** (2009), 1277–1283.
8. X. Kai, S. Zhu, Quaternary construction of quantum codes from cyclic codes over $\mathbb{F}_4 + u\mathbb{F}_4$, *Int. J. Quant. Inf.*, **9** (2011), 689–700. https://doi.org/10.1142/s0219749911007757
9. J. Gao, Quantum codes from cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q + v^3\mathbb{F}_q$, *Int. J. Quant. Inf.*, **13** (2015), 1550063. https://doi.org/10.1142/S021974991550063X
10. S. H. Saif, Constructions and enumerations of self-dual and LCD double circulant codes over a local ring, *Mathematics*, **13** (2025), 3527. https://doi.org/10.3390/math13213527
11. H. Q. Dinh, A. K. Singh, S. Pattanayak, S. Sriboonchitta, Construction of cyclic DNA codes over the ring $\mathbb{Z}_4[u]/\langle u^2 - 1\rangle$ based on the deletion distance, *Theor. Comput. Sci.*, **773** (2019), 27–42. https://doi.org/10.1016/j.tcs.2018.06.002

12. H. Q. Dinh, A. K. Singh, S. Pattanayak, S. Sriboonchitta, Cyclic DNA codes over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2 + v^2\mathbb{F}_2 + uv^2\mathbb{F}_2$, *Des. Codes Cryptogr.*, **86** (2018), 1451–1467. https://doi.org/10.1007/s10623-017-0405-x

13. E. S. Oztas, B. Yildiz, I. Siap, A novel approach for constructing reversible codes and applications to DNA codes over the ring $\mathbb{F}_2[u]/(u^{2k} - 1)$, *Finite Fields Appl.*, **46** (2017), 217–234. https://doi.org/10.1016/j.ffa.2017.04.001

14. S. H. Saif, Structures, ranks and minimal distances of cyclic codes over $\mathbb{Z}_{p^2} + u\mathbb{Z}_{p^2}$, *Mathematics*, **13** (2025), 3354. https://doi.org/10.3390/math13203354

15. S. Alabiad, A. A. Alhomaidhi, Various structures of cyclic codes and LCD codes over $\mathrm{GR}(p^3, m)[v]/\langle v^2 - p^2\alpha, pv\rangle$, *AIMS Math.*, **10** (2025), 27535–27559. https://doi.org/10.3934/math.20251211

16. S. Ali, S. A. Alali, E. S. Oztas, P. Sharma, Construction of quantum codes over the class of commutative rings and their applications to DNA codes, *Mathematics*, **11** (2023), 1430. https://doi.org/10.3390/math11061430

17. H. Q. Dinh, S. Pathak, A. K. Upadhyay, W. Yamaka, New DNA codes from cyclic codes over mixed alphabets, *Mathematics*, **8** (2020) 1977. https://doi.org/10.3390/math8111977

18. P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A*, **52** (1995), 2493–2496. https://doi.org/10.1103/PhysRevA.52.R2493

19. A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error-correction via codes over GF(4), *IEEE Trans. Inform. Theory*, **44** (1998), 1369–1387. https://doi.org/10.1109/18.681315

20. H. Islam, O. Prakash, New quantum and LCD codes over finite fields of even characteristic, *Def. Sci. J.*, **71** (2020), 656–661. https://doi.org/10.14429/dsj.71.16641

21. M. Özen, N. T. Özzaim, H. Ince, Quantum codes from cyclic codes over $\mathbb{F}_3 + u\mathbb{F}_3 + v\mathbb{F}_3 + uv\mathbb{F}_3$, *J. Phys.: Conf. Ser.*, **766** (2016), 012020. https://doi.org/10.1088/1742-6596/766/1/012020

22. M. Ashraf, G. Mohammad, Quantum codes over $\mathbb{F}_p$ from cyclic codes over $\mathbb{F}_p[u, v]/\langle u^2 - 1, v^3 - v, uv - vu\rangle$, *Cryptogr. Commun.*, **11** (2019), 325–335. https://doi.org/10.1007/s12095-018-0299-0

23. H. Islam, O. Prakash, Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring, *Cryptogr. Commun.*, **14** (2022), 59–73. https://doi.org/10.1007/s12095-021-00516-9

24. M. Grassl, Code tables: bounds on the parameters of various types of codes. Available from: `http://www.codetables.de/`.

25. M. Grassl, T. Beth, M. Rötteler, On optimal quantum codes, *Int. J. Quant. Inf.*, **2** (2004), 55–64. https://doi.org/10.1142/s0219749904000079

26. A. Marathe, A. E. Condon, R. M. Corn, On combinatorial DNA word design, *J. Comput. Biol.*, **8** (2001), 201–220.

27. A. D. Johnson, An extended IUPAC nomenclature code for polymorphic nucleic acids, *Bioinformatics*, **26** (2010), 1386–1389. https://doi.org/10.1093/bioinformatics/btq098

28. O. D. King, Bounds for DNA codes with constant GC-content, *Electron. J. Comb.*, **10** (2003), R33.

29. M. Li, H. J. Lee, A. E. Condon, R. M. Corn, DNA word design strategy for creating sets of non-interacting oligonucleotides for DNA microarrays, *Langmuir*, **18** (2002), 805–812. https://doi.org/10.1021/la0112209

30. T. Abualrub, A. Ghrayeb, X. Zeng, Construction of cyclic codes over GF(4) for DNA computing, *J. Franklin Inst.*, **343** (2006), 448–457. https://doi.org/10.1016/j.jfranklin.2006.02.009

31. I. Siap, T. Abualrub, A. Ghrayeb, Cyclic DNA codes over the ring $\mathbb{F}_2[u]/(u^2 - 1)$ based on the deletion distance, *J. Franklin Inst.*, **346** (2009), 731–740. https://doi.org/10.1016/j.jfranklin.2009.07.002

32. K. Gowdhaman, S. Gupta, C. Mohan, K. Guenda, D. Chinnapillai, Cyclic DNA codes over the ring $\mathbb{Z}_4 + u\mathbb{Z}_4 + u^2\mathbb{Z}_4$, *J. Algebra Comb. Discrete Appl.*, **8** (2021), 219–231. https://doi.org/10.13069/jacodesmath.1000959

33. W. Bosma, J. Cannon, *Handbook of Magma functions*, University of Sydney, 1995.