



m -adic residue codes from minimal idempotents over $\mathbb{F}_q S$

Eda Tekin^a

^aDepartment of Business, Karabük University, Karabük, Turkey

Abstract. We study m -adic residue codes of prime length p over the mixed-alphabet semisimple ring $\mathbb{F}_q S$ with $S = \mathbb{F}_q + v\mathbb{F}_q$ and $v^2 = v$. Via the Chinese Remainder Theorem we identify $(\mathbb{F}_q S)[x]/\langle x^p - 1 \rangle \cong (\mathbb{F}_q[x]/\langle x^p - 1 \rangle)^3$, and use minimal idempotents to construct two complementary families of m -adic residue codes (Type A/B) over $\mathbb{F}_q S$. We derive explicit orthogonal idempotents that generate these codes and describe their componentwise structure.

We show that when $q = 2^k$ and $t = (p - 1)/m$ is even, the generator polynomials of all components (over $\mathbb{F}_q$ and over S) are palindromic. This algebraic symmetry enables applications to DNA coding. Fixing a standard bijection $\theta : \mathbb{F}_{16} \rightarrow \{A, T, C, G\}^2$, we extend it to Ψ and Θ on codewords and define an involutive reversal operator $\mathcal{A}$ on $\mathbb{F}_{16} S$ that models basewise reversal under Θ . Using a tailored Ω -set construction, a palindromic generator $g(x)$ with $k = n - \deg g$ even leads to a code whose DNA image $\Theta(C)$ is closed under reversal.

We then extend the framework to satisfy the reverse-complement (RC) constraint. A table-induced complement-based permutation η on $\mathbb{F}_{16}$ defines a coefficient operator $\mathcal{B}$ that algebraically models RC; an Ω_{RC} construction produces RC-closed DNA codes without requiring η to be a ring automorphism. In the special Frobenius case $\eta(\gamma) = \gamma^{2^s}$, an lcm-based cyclic closure guarantees $\mathcal{B}$ -invariance.

Examples are included to illustrate the construction. The approach is constructive, compatible with computer algebra, and extends to other polyadic families and non-chain rings.

1. Introduction

Error-correcting codes play a fundamental role in modern digital communication and data storage systems by ensuring the reliable transmission of information across noisy channels. Cyclic codes, an important class of linear codes, have been extensively studied due to their rich algebraic structure, which allows for efficient encoding and decoding implementations [9]. Among the most celebrated families of cyclic codes are the quadratic residue (QR) codes and their generalizations, the m -adic residue codes. These codes are known for their large minimum distances and for containing many examples of optimal or near-optimal codes [6, 9]. Their generalization, the m -adic residue codes, was introduced in [7].

The study of codes over finite rings, rather than exclusively over finite fields, has led to significant theoretical advancements and practical applications, including the famous discovery of non-linear binary

2020 *Mathematics Subject Classification.* Primary 94B15; Secondary 11T71, 13M05.

Keywords. m -adic residue codes; idempotents; Chinese remainder theorem; palindromic generators; DNA codes; reverse-complement constraint.

Received: 10 August 2025; Revised: 28 January 2026; Accepted: 09 February 2026

Communicated by Paola Bonacini

Email address: tedatekin@gmail.com (Eda Tekin)

ORCID iD: <https://orcid.org/0000-0001-9271-7487> (Eda Tekin)

codes with better parameters than previously known linear codes [5]. Research has since expanded to a wide variety of ring structures, with a particular interest in non-chain rings, which offer a richer algebraic framework. In this context, we focus on the commutative non-chain ring $S = \mathbb{F}_q + v\mathbb{F}_q$ with $v^2 = v$, and the mixed-alphabet ring $\mathbb{F}_q S = \mathbb{F}_q \times S$. By the Chinese Remainder Theorem (CRT), this ring is isomorphic to the direct product $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$. This decomposition allows us to analyze codes over $\mathbb{F}_q S$ via their constituent component codes over the base field $\mathbb{F}_q$; related cyclic variants over mixed-alphabet rings (including skew-cyclic structures) have also been investigated in settings close to $\mathbb{F}_q S$ [12].

From an algebraic viewpoint, cyclic codes of length p over a commutative ring can be identified with ideals of the quotient ring $R[x]/\langle x^p - 1 \rangle$, and in semisimple settings these ideals admit idempotent descriptions. In particular, working with explicit idempotents is convenient for tracking constituent decompositions under CRT and for certifying symmetry constraints through coefficient-wise operators. This perspective will be used throughout the paper: we first construct m -adic residue families via idempotents over $\mathbb{F}_q S$, and then translate palindromicity/symmetry into reversal and reverse-complement closure at the DNA level.

In parallel with these algebraic developments, DNA computing has emerged as a promising technology for high-density data storage and massively parallel computation [1]. The design of reliable DNA codebooks, however, requires adherence to strict combinatorial and thermodynamic constraints to prevent unintended hybridizations and ensure stability. One important constraint is the reverse constraint, which requires that the reverse of any DNA sequence in the codebook must also be a sequence within the codebook [2]. Constructing large codebooks that satisfy this property remains an active topic in the field. In algebraic code design, such closure constraints are often enforced by structural symmetries (e.g., reciprocity/palindromicity of generators) rather than by enumerating codewords. Cyclic-code based approaches to DNA code design over ring alphabets have also been considered in the literature, providing complementary algebraic routes to enforce biological constraints [11].

This paper connects these themes by studying m -adic residue codes of prime length over the mixed-alphabet semisimple ring $\mathbb{F}_q S$ and by using the resulting palindromic structure to obtain DNA codebooks closed under reversal and reverse-complement operations. Our main contribution is the introduction and detailed analysis of m -adic residue codes of length p over the ring $\mathbb{F}_q S$. The key aspects of our work are as follows:

- We define m -adic residue code families over $\mathbb{F}_q S$ and derive their idempotent descriptions via a CRT triplet view.
- We identify explicit conditions ensuring that the relevant generator polynomials are palindromic, which is the key symmetry used later.
- Specializing to $q = 16$, we give a concrete ring-to-DNA framework and use coefficient-wise operators to guarantee closure under reversal and reverse-complement constraints.

The remainder of the paper is organized as follows. In Section 2 we review the algebraic setting, including the CRT decomposition of $\mathbb{F}_q S$, the Lee weight used in the sequel, and the classical definition of m -adic residue codes over $\mathbb{F}_q$. Section 3 introduces Type A/Type B m -adic residue code families over $\mathbb{F}_q S$ via minimal idempotents and describes their constituent structure under the CRT triplet view. In Section 4 we establish palindromic (reciprocal) properties of the relevant generator polynomials and set up the ring-to-DNA mapping framework. Section 5 develops the reversal automorphism and the Ω -set construction yielding reversible DNA codebooks. Section 6 extends the method to reverse-complement closure via a coefficient-wise operator and an Ω_{RC} construction, including an optional Frobenius/lcm cyclic closure variant. Finally, Section 7 concludes the paper with limitations and directions for future work.

1.1. Literature positioning and contributions

The items below place polyadic/ m -adic results over fields and rings in context and indicate where reversal/RC constraints have (not) been addressed.

Theme	Setting	Result snapshot	Reversal/RC
Polyadic/ m -adic codes over fields	$\mathbb{F}_q$, prime length p	Coset/character theory, minimal idempotents, complementary even/odd-like families; classical structure and parameters [3, 7].	Not explicit
m -adic over idempotent ring $\mathbb{F}_q[v]/(v^2-v)$	Non-chain ring	Definition and basic properties; DNA-oriented constructions over this ring reported [8].	Partial (reversal), RC not systematic
Codes over $\mathbb{F}_q + v\mathbb{F}_q$ (and variants)	Non-chain skew/cyclic rings,	Structural/decomposition results and cyclic/skew-cyclic families over $\mathbb{F}_q + v\mathbb{F}_q$ [4].	Not targeted
DNA mappings from finite fields/rings	$\mathbb{F}_{16}, \mathbb{F}_4 + v\mathbb{F}_4$	Field-to-DNA bijections θ ; code constructions with reversal heuristics, omega-set style ideas [2, 10].	Reversal treated; RC ad hoc
This paper	$\mathbb{F}_q S$ with $S = \mathbb{F}_q + v\mathbb{F}_q$	Minimal idempotent-based m -adic families over mixed alphabet; palindromic generators under explicit conditions; reversal and RC via coefficient operators aligned with θ .	Reversal and RC, systematic

Scope and contributions. Within the setting of prime length p , $\gcd(p, q) = 1$, $m \mid (p-1)$ and $q \pmod{p} \in Q_0$, we:

- develop Type A/B m -adic residue codes over $\mathbb{F}_q S$ from minimal idempotents using a CRT triplet view;
- show that, for $q = 2^k$ and $t = (p-1)/m$ even, the resulting generators are palindromic (with a degree-matching condition over S);
- introduce an Ω -set method ensuring reversal when $k = n - \deg g$ is even; and
- extend to reverse-complement closure via a table-induced coefficient operator $\mathcal{B}$, without requiring a ring-automorphism hypothesis.

In the Frobenius case $\eta(\gamma) = \gamma^{2^s}$ we additionally provide a cyclic lcm-closure. Examples for $(5, 2, 16)$ and $(17, 4, 16)$ illustrate generator choices and distances. We do not claim optimality of parameters; the emphasis is on a transparent algebraic pathway from idempotents to reversal/RC properties.

2. Preliminaries

In this section, we introduce the fundamental algebraic structures and definitions that will be used throughout the paper. We first describe the structure of the ring $\mathbb{F}_q S$, then define linear codes and a suitable distance-preserving metric over this ring, and finally, we review the classical theory of m -adic residue codes over finite fields.

2.1. The Ring Structure of $\mathbb{F}_q S$

Let $\mathbb{F}_q$ be a finite field, where q is a prime power. We consider the commutative ring $S = \mathbb{F}_q + v\mathbb{F}_q = \{\xi + v\mu \mid \xi, \mu \in \mathbb{F}_q\}$, where the multiplication is defined by the relation $v^2 = v$. The element v is a non-trivial idempotent, which implies that $1-v$ is also an idempotent. These two idempotents are orthogonal, i.e., $v(1-v) = v-v^2 = 0$, and they form a complete set, as $v + (1-v) = 1$.

The existence of these idempotents allows for a decomposition of the ring S into a direct product of simpler rings via the Chinese Remainder Theorem (CRT). Specifically, S is isomorphic to the direct product of its component ideals:

$$S \cong S(1-v) \oplus Sv.$$

Since $S / \langle v \rangle \cong \mathbb{F}_q$ and $S / \langle 1-v \rangle \cong \mathbb{F}_q$, this leads to the ring isomorphism $S \cong \mathbb{F}_q \times \mathbb{F}_q$. An element $\xi + v\mu \in S$ can be uniquely expressed as $\xi(1-v) + (\xi + \mu)v$, which corresponds to the pair $(\xi, \xi + \mu)$ under this isomorphism.

The primary alphabet for our codes is the ring $\mathbb{F}_q S$, defined as the direct product of the field $\mathbb{F}_q$ and the ring S :

$$\mathbb{F}_q S := \mathbb{F}_q \times S = \{(\partial, \xi + v\mu) \mid \partial, \xi, \mu \in \mathbb{F}_q\}.$$

Consequently, $\mathbb{F}_q S$ is a semi-local ring. As a direct product of fields, $\mathbb{F}_q S \cong \mathbb{F}_q^3$ is a commutative semi-simple ring. In such a ring, every ideal is generated by a single idempotent element, and therefore $\mathbb{F}_q S$ is a principal ideal ring (PIR). Applying the CRT again, we obtain the key isomorphism for our work:

$$\mathbb{F}_q S \cong \mathbb{F}_q \times S \cong \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q.$$

We define the explicit ring isomorphism $\Phi : \mathbb{F}_q S \rightarrow \mathbb{F}_q^3$ as:

$$\Phi(\partial, \xi + v\mu) = (\partial, \xi, \xi + \mu).$$

This map is fundamental as it allows us to study codes over the abstract ring $\mathbb{F}_q S$ by analyzing their simpler constituent components over the field $\mathbb{F}_q$.

2.2. Linear Codes over $\mathbb{F}_q S$ and the Lee Weight

A **linear code** C of length n over $\mathbb{F}_q S$ is an $\mathbb{F}_q S$ -submodule of the free module $(\mathbb{F}_q S)^n$. A code C is called **cyclic** if for any codeword $(c_0, c_1, \dots, c_{n-1}) \in C$, its cyclic shift $(c_{n-1}, c_0, \dots, c_{n-2})$ is also in C .

By the CRT decomposition established above, any linear code C over $\mathbb{F}_q S$ corresponds to a triplet of linear codes (C_1, C_2, C_3) over $\mathbb{F}_q$, where $C = \Phi^{-1}(C_1 \times C_2 \times C_3)$. The code C is cyclic if and only if each of its component codes C_1, C_2, C_3 is cyclic over $\mathbb{F}_q$.

To measure the distance between codewords, we define a Lee weight on $\mathbb{F}_q S$ that is compatible with the CRT decomposition. This is a natural extension of the Hamming weight on $\mathbb{F}_q$.

Definition 2.1. The **Lee weight** w_L of an element $a = (\partial, \xi + v\mu) \in \mathbb{F}_q S$ is defined as the sum of the Hamming weights of its components under the isomorphism Φ :

$$w_L(a) = w_H(\Phi(a)) = w_H(\partial) + w_H(\xi) + w_H(\xi + \mu),$$

where $w_H(x)$ is the standard Hamming weight for $x \in \mathbb{F}_q$ ($w_H(x) = 1$ if $x \neq 0$ and $w_H(0) = 0$). The Lee weight of a codeword $c = (c_0, \dots, c_{n-1}) \in (\mathbb{F}_q S)^n$ is $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$. The **Lee distance** $d_L(x, y)$ between two codewords x, y is defined as $w_L(x - y)$. For a linear code, the minimum Lee distance is equal to the minimum non-zero Lee weight of any codeword.

2.3. m -adic Residue Codes over $\mathbb{F}_q$

We conclude our preliminaries by reviewing the classical construction of m -adic residue codes over a finite field $\mathbb{F}_q$, which will serve as the building blocks for our codes.

Let p be an odd prime and q be a prime power such that $\gcd(p, q) = 1$. Let $m \geq 2$ be an integer such that $m \mid (p - 1)$. Let b be a primitive root modulo p . The set of m -adic residues modulo p is the subgroup $Q_0 = \{a^m \pmod{p} \mid a \in \mathbb{Z}_p^*\}$ of $\mathbb{Z}_p^*$. The cosets of Q_0 in $\mathbb{Z}_p^*$ are given by $Q_i = b^i Q_0$ for $i = 0, 1, \dots, m - 1$.

For the theory of cyclic codes, it is required that the code alphabet $\mathbb{F}_q$ has a specific relationship with the cosets. We assume that q is an m -adic residue modulo p , i.e., $q \pmod{p} \in Q_0$. This condition ensures that the permutation $\mu_q : j \mapsto qj \pmod{p}$ fixes each coset Q_i , which in turn guarantees that the ideals generated by the polynomials defined below are ideals of the ring $\mathbb{F}_q[x]/(x^p - 1)$.

Let λ be a primitive p -th root of unity in some extension field of $\mathbb{F}_q$.

Definition 2.2. Let p be an odd prime, q a prime power with $\gcd(p, q) = 1$, and $m \mid (p - 1)$ such that $q \pmod{p} \in Q_0$. Let $t = (p - 1)/m$. Let λ be a primitive p -th root of unity in an extension field of $\mathbb{F}_q$. The two families of m -adic residue codes are defined as follows:

- (1) The family of **even-like class m -adic residue codes** of length p over $\mathbb{F}_q$ are the cyclic codes C_i generated by the polynomials:

$$g_i(x) = \frac{x^p - 1}{\prod_{j \in Q_{-i}} (x - \lambda^j)} = (x - 1) \prod_{j \in \mathbb{Z}_p^* \setminus Q_{-i}} (x - \lambda^j)$$

for $i = 0, 1, \dots, m - 1$. The degree of the generator $g_i(x)$ is $p - t - 1 + 1 = p - t$, and the dimension of the code C_i is t .

- (2) The family of **odd-like class m -adic residue codes** of length p over $\mathbb{F}_q$ are the cyclic codes $\widehat{C}_i$ generated by the polynomials:

$$\widehat{g}_i(x) = \prod_{j \in Q_{-i}} (x - \lambda^j)$$

for $i = 0, 1, \dots, m - 1$. The degree of the generator $\widehat{g}_i(x)$ is t , and the dimension of the code $\widehat{C}_i$ is $p - t$.

Remark 2.3. Note that the codes C_i and $\widehat{C}_i$ are complementary, meaning their corresponding idempotents sum to $\mathbf{1}$. In much of the literature, the larger dimension codes ($\widehat{C}_i$) are referred to as odd-like codes.

Remark 2.4. The naming conventions and generator definitions for m -adic codes can vary in the literature. The definitions provided here are standard and suitable for our constructions. The key property is that the set of zeros for each code is a union of these m -adic cosets.

3. m -adic Residue Codes over $\mathbb{F}_q S$

In this section, we construct the main objects of our study: m -adic residue codes over the ring $\mathbb{F}_q S$. Our strategy is to leverage the structure of classical m -adic codes over the base field $\mathbb{F}_q$. We will use their idempotent generators as building blocks to define new families of codes in the larger ring. Throughout this section, we denote the ring $(\mathbb{F}_q S)[x]/(x^p - 1)$ by $\mathcal{R}_p$. From the isomorphism $\Phi : \mathbb{F}_q S \rightarrow \mathbb{F}_q^3$ defined in Section 2.1, we have the corresponding ring isomorphism:

$$\mathcal{R}_p = (\mathbb{F}_q S)[x]/(x^p - 1) \cong (\mathbb{F}_q[x]/(x^p - 1))^3.$$

Any element $A \in \mathcal{R}_p$ can therefore be represented as a triplet $A = (A_1, A_2, A_3)$, where each $A_i \in \mathbb{F}_q[x]/(x^p - 1)$. Specifically, an element of the form $(\partial, \xi + v\mu) \in \mathbb{F}_q S$ corresponds to the triplet $(\partial, \xi, \xi + \mu)$. This decomposition is fundamental to our construction.

3.1. Idempotent Generators

Let p be a prime and q be a prime power such that $\gcd(p, q) = 1$ and q is an m -adic residue modulo p . The ring $\mathbb{F}_q[x]/(x^p - 1)$ can be decomposed into a direct sum of minimal ideals, which are generated by a set of primitive idempotents. In the polyadic (m -adic) setting, the idempotents used below are generally orthogonal and may be sums of primitive idempotents. For m -adic residue codes, the relevant idempotents are linear combinations of the basis elements $l_i(x) = \sum_{j \in Q_i} x^j$.

Let $\{e_0, e_1, \dots, e_{m-1}\}$ be a set of mutually orthogonal (polyadic) idempotents associated with the m -adic cosets $Q_0, Q_1, \dots, Q_{m-1}$ respectively. Let ι_0 be the principal idempotent corresponding to the factor $x - 1$, given by $\iota_0 = p^{-1} \sum_{j=0}^{p-1} x^j$. These idempotents satisfy the following fundamental properties in the ring $\mathbb{F}_q[x]/(x^p - 1)$:

- (i) $e_k e_l = \delta_{kl} e_k$ for $k, l \in \{0, \dots, m - 1\}$, where δ_{kl} is the Kronecker delta.
- (ii) $\sum_{k=0}^{m-1} e_k = \mathbf{1} - \iota_0$, where $\mathbf{1}$ is the multiplicative identity.
- (iii) There exists an element $a \in Q_1$ such that the permutation $\mu_a : f(x) \mapsto f(x^a)$ cyclically permutes the set of idempotents, i.e., $\mu_a(e_k) = e_{k+1 \pmod{m}}$.

We first establish a lemma for constructing idempotents in the larger ring $\mathcal{R}_p$.

Proposition 3.1. *Let f_1, f_2, f_3 be any three idempotents in $\mathbb{F}_q[x]/(x^p - 1)$. Then the element $F = (f_1, f_2, f_3)$ is an idempotent in $\mathcal{R}_p \cong (\mathbb{F}_q[x]/(x^p - 1))^3$.*

Proof. We compute the square of F component-wise:

$$F^2 = (f_1, f_2, f_3) \cdot (f_1, f_2, f_3) = (f_1^2, f_2^2, f_3^2).$$

Since f_1, f_2 , and f_3 are idempotents in $\mathbb{F}_q[x]/(x^p - 1)$, we have $f_i^2 = f_i$ for $i = 1, 2, 3$. Thus, $F^2 = (f_1, f_2, f_3) = F$, proving that F is an idempotent in $\mathcal{R}_p$. $\square$

We now use this result to construct families of orthogonal idempotents over $\mathbb{F}_q S$.

Proposition 3.2. *Let $\{e_0, \dots, e_{m-1}\}$ be the set of orthogonal idempotents for the m -adic codes over $\mathbb{F}_q$. Choose initial indices $i_0, j_0, k_0 \in \{0, \dots, m-1\}$ and define an initial idempotent $E_0 = (e_{i_0}, e_{k_0}, e_{j_0}) \in \mathcal{R}_p$. The use of distinct initial indices (i_0, k_0, j_0) allows for the construction of codes with varied constituent codes, providing a richer structure that is crucial for the asymmetric nature of the reversal automorphism defined in Section 5. Let the permutation μ_a act component-wise, and define a family of m idempotents by setting $E_r = \mu_a^r(E_0)$ for $r = 0, 1, \dots, m-1$. Then this family $\{E_0, \dots, E_{m-1}\}$ has the following properties:*

- (1) Each E_r is an idempotent in $\mathcal{R}_p$.
- (2) The idempotents are mutually orthogonal: $E_r E_s = (0, 0, 0)$ for $r \neq s$.
- (3) Their sum is $\sum_{r=0}^{m-1} E_r = (\mathbf{1} - \iota_0, \mathbf{1} - \iota_0, \mathbf{1} - \iota_0)$.

Proof. (1) By construction, $E_r = \mu_a^r(E_0) = (\mu_a^r(e_{i_0}), \mu_a^r(e_{k_0}), \mu_a^r(e_{j_0})) = (e_{i_0+r}, e_{k_0+r}, e_{j_0+r})$. Since μ_a maps idempotents to idempotents, each component is an idempotent. By Proposition 3.1, E_r must be an idempotent.

(2) Let $r, s \in \{0, \dots, m-1\}$ with $r \neq s$. The product $E_r E_s$ is:

$$\begin{aligned} E_r E_s &= (e_{i_0+r}, e_{k_0+r}, e_{j_0+r}) \cdot (e_{i_0+s}, e_{k_0+s}, e_{j_0+s}) \\ &= (e_{i_0+r} e_{i_0+s}, e_{k_0+r} e_{k_0+s}, e_{j_0+r} e_{j_0+s}). \end{aligned}$$

Since $r \neq s$, the indices in each component are distinct (mod m). As the base idempotents $\{e_k\}$ are mutually orthogonal, we have $e_u e_v = 0$ for $u \neq v$. Therefore, each component of the product is zero. Thus, $E_r E_s = (0, 0, 0)$.

(3) We compute the sum:

$$\sum_{r=0}^{m-1} E_r = \left(\sum_{r=0}^{m-1} e_{i_0+r}, \sum_{r=0}^{m-1} e_{k_0+r}, \sum_{r=0}^{m-1} e_{j_0+r} \right).$$

As r ranges from 0 to $m-1$, each set of indices covers all values from 0 to $m-1$ exactly once. Thus, the sum of idempotents in each component is $\sum_{k=0}^{m-1} e_k = \mathbf{1} - \iota_0$. Substituting this into the expression gives:

$$\sum_{r=0}^{m-1} E_r = (\mathbf{1} - \iota_0, \mathbf{1} - \iota_0, \mathbf{1} - \iota_0).$$

This completes the proof. $\square$

3.2. Code Classes from Minimal Idempotents over $\mathbb{F}_q S$

The families of orthogonal idempotents constructed in Proposition 3.2 serve as the generators for our new codes. We define two complementary classes of codes based on these fundamental building blocks.

Definition 3.3. A code $C_r^{(A)} = \langle E_r \rangle$, generated by an idempotent E_r from the family defined in Proposition 3.2, is called a member of the **Type A class of m -adic residue codes** of length p over $\mathbb{F}_q S$.

The codes that are algebraically complementary to the Type A class are generated by the idempotents $1 - E_r$.

Definition 3.4. A code $C_r^{(B)} = \langle 1 - E_r \rangle$, generated by a complementary idempotent $1 - E_r$, is called a member of the **Type B class of m -adic residue codes** of length p over $\mathbb{F}_q S$.

The idempotents generating the Type B codes, which we can denote by $E'_r = 1 - E_r$, form a cyclically permuted family with the following interesting properties.

Proposition 3.5. Let $\{E_0, \dots, E_{m-1}\}$ be the family of orthogonal idempotents from Proposition 3.2 and let $E'_r = (1, 1, 1) - E_r$. The following hold:

- (1) $\mu_a(E'_r) = E'_{r+1 \pmod{m}}$.
- (2) $E'_r + E'_s - E'_r E'_s = (1, 1, 1)$ for all $r \neq s$.
- (3) $\prod_{r=0}^{m-1} E'_r = (\iota_0, \iota_0, \iota_0)$.

Proof. (1) Since μ_a is a ring automorphism and $\mu_a(1) = 1$, we have $\mu_a(E'_r) = \mu_a((1, 1, 1) - E_r) = (1, 1, 1) - \mu_a(E_r) = (1, 1, 1) - E_{r+1 \pmod{m}} = E'_{r+1 \pmod{m}}$.

(2) For $r \neq s$, we use the fact that $E_r E_s = (0, 0, 0)$.

$$\begin{aligned} E'_r + E'_s - E'_r E'_s &= ((1, 1, 1) - E_r) + ((1, 1, 1) - E_s) - ((1, 1, 1) - E_r)((1, 1, 1) - E_s) \\ &= 2(1, 1, 1) - E_r - E_s - ((1, 1, 1) - E_r - E_s + E_r E_s) \\ &= 2(1, 1, 1) - E_r - E_s - (1, 1, 1) + E_r + E_s - (0, 0, 0) = (1, 1, 1). \end{aligned}$$

(3) Since $E_r E_s = (0, 0, 0)$ for $r \neq s$, the product of the complementary idempotents expands to:

$$\prod_{r=0}^{m-1} E'_r = \prod_{r=0}^{m-1} ((1, 1, 1) - E_r) = (1, 1, 1) - \sum_{r=0}^{m-1} E_r.$$

Using the result from Proposition 3.2(3), this becomes:

$$(1, 1, 1) - (1 - \iota_0, 1 - \iota_0, 1 - \iota_0) = (\iota_0, \iota_0, \iota_0).$$

□

Example 3.6 (Concrete generator for $(p, m, q) = (5, 2, 16)$). Fix $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]/\langle \alpha^4 + \alpha + 1 \rangle$ and let $\lambda := \alpha^3$ (so $\text{ord}(\lambda) = 5$). The quadratic-residue classes modulo 5 are $Q_0 = \{1, 4\}$ and $Q_1 = \{2, 3\}$.

Even-like, $i = 0$. The degree-3 generator over $\mathbb{F}_{16}$ is

$$g_0(x) = (x - 1) \prod_{j \in \mathbb{Z}_5^* \setminus Q_0} (x - \lambda^j) = (x - 1)(x - \lambda^2)(x - \lambda^3).$$

Using $\alpha^4 = \alpha + 1$, $\lambda^2 = \alpha^6 = \alpha^3 + \alpha^2$, $\lambda^3 = \alpha^9 = \alpha^3 + \alpha$, one obtains

$$g_0(x) = x^3 + (\alpha^2 + \alpha + 1)x^2 + (\alpha^2 + \alpha + 1)x + 1,$$

which is palindromic and generates a $[5, 2, 4]$ code over $\mathbb{F}_{16}$.

Odd-like (reference). For $i = 0$,

$$\widehat{g}_0(x) = (x - \lambda)(x - \lambda^4) = x^2 + (\lambda + \lambda^4)x + 1 = x^2 + (\alpha^2 + \alpha + 1)x + 1.$$

Even-like, $i = 1$. Here

$$g_1(x) = (x - 1)(x - \lambda)(x - \lambda^4) = x^3 + (\alpha^2 + \alpha)x^2 + (\alpha^2 + \alpha)x + 1,$$

also palindromic.

Generator over $S = \mathbb{F}_{16} + v\mathbb{F}_{16}$, $v^2 = v$. With the choice $E_0 = (e_0, e_0, e_1)$, the S -component generator is

$$g_S(x) = (1 - v)g_0(x) + v g_1(x) = x^3 + c x^2 + c x + 1, \quad c := (1 - v)(\alpha^2 + \alpha + 1) + v(\alpha^2 + \alpha),$$

hence $g_S(x)$ is palindromic. The resulting code over $\mathbb{F}_{16}S$ has three $[5, 2, 4]$ constituents and minimum Lee distance $d_L = 4$ (via the CRT components).

Remark 3.7. For $p = 5$ and $q = 16$, the even-like constituents have $\deg g = 3$ so $k = n - \deg g = 2$ is even. Thus the Type A class (generated by the idempotents E_r) fits the Ω/Ω_{RC} construction and yields three $[5, 2, 4]$ constituents and $d_L = 4$ over $\mathbb{F}_{16}S$.

4. Palindromic Properties and Application to DNA Codes

In this section, we investigate a crucial structural property of the m -adic residue codes over $\mathbb{F}_qS$: the palindromicity of their generator polynomials. A polynomial is called palindromic (or reciprocal) if its sequence of coefficients reads the same forwards and backwards. This symmetry is not merely mathematical; it is the key algebraic property that enables the construction of codes satisfying the important *reversal constraint* required in applications such as DNA-based data storage.

4.1. Palindromic Generator Polynomials

We begin by establishing two fundamental properties of the m -adic cosets Q_j , which are standard results in this field.

Lemma 4.1. Let p be an odd prime, and let $m \geq 2$ be an integer dividing $p - 1$. Let Q_j for $j \in \{0, 1, \dots, m - 1\}$ be the m -adic cosets modulo p . Let $t = |Q_0| = (p - 1)/m$.

- (i) If t is an even integer, then for any $i \in Q_j$, its additive inverse $-i \pmod{p}$ is also in Q_j .
- (ii) If $t > 1$, then the sum of the elements in any coset is zero modulo p : $\sum_{i \in Q_j} i \equiv 0 \pmod{p}$.

Proof. (i) If $t = (p - 1)/m$ is even, then $(p - 1)/2 = m(t/2)$. For a primitive root $b \pmod{p}$, we have $-1 \equiv b^{(p-1)/2} \pmod{p}$. Thus, $-1 \equiv b^{m(t/2)} = (b^{t/2})^m$, which shows that -1 is an m -th power. Therefore, $-1 \in Q_0$. Since $Q_j = b^j Q_0$, if $i \in Q_j$, then $i = b^j k$ for some $k \in Q_0$. It follows that $-i = (-1)i = (-1)b^j k$. As Q_0 is a group, $(-1)k \in Q_0$, which implies $-i \in b^j Q_0 = Q_j$.

(ii) Let $S_j = \sum_{i \in Q_j} i$. Since $t > 1$, there exists an element $c \in Q_0$ such that $c \not\equiv 1 \pmod{p}$. Multiplication by c permutes the elements of Q_0 , so $cS_0 = \sum_{k \in Q_0} ck \equiv \sum_{k' \in Q_0} k' = S_0 \pmod{p}$. This implies $(c - 1)S_0 \equiv 0 \pmod{p}$. Since $c \not\equiv 1 \pmod{p}$, we must have $S_0 \equiv 0 \pmod{p}$. For any j , $S_j = \sum_{k \in Q_0} b^j k = b^j S_0 \equiv 0 \pmod{p}$. $\square$

With these properties, we can establish the palindromic nature of the generator polynomials for the constituent codes over $\mathbb{F}_q$ when q is a power of 2.

Proposition 4.2. Let $q = 2^k$ for some $k \geq 1$, and let p be a prime satisfying the conditions of Lemma 4.1. Assume $t = (p - 1)/m$ is even. Let $f(x)$ be the generator polynomial of any m -adic residue code over $\mathbb{F}_q$ (either even-like or odd-like class), whose roots are determined by a union of cosets $U = \bigcup_{i \in I} Q_i$. Then $f(x)$ is a palindromic polynomial.

Proof. Let λ be a primitive p -th root of unity in an extension field of $\mathbb{F}_q$. Since the characteristic is 2, the generator polynomial is $f(x) = \prod_{j \in U} (x + \lambda^j)$, which is monic by definition. Let $d = \deg(f) = |U|$. The reciprocal polynomial is $f^*(x) = x^d f(x^{-1})$. The roots of $f^*(x)$ are the inverses of the roots of $f(x)$, which are $\{\lambda^{-j} \mid j \in U\}$.

By Lemma 4.1(i), since t is even, the set of indices U is closed under negation modulo p . This means that the set of roots $\{\lambda^j \mid j \in U\}$ is the same as the set of their inverses $\{\lambda^{-j} \mid j \in U\}$. Therefore, $f(x)$ and $f^*(x)$ share the same set of roots.

To show they are identical, we must also show $f^*(x)$ is monic. The constant term of $f(x)$ is $f(0) = \prod_{j \in U} \lambda^j = \lambda^{\sum_{j \in U} j}$. By Lemma 4.1(ii), the sum of elements in any coset Q_i (for $t > 1$) is 0 (mod p). Since U is a union of such cosets, the total sum of indices is also 0 (mod p). Therefore, $f(0) = \lambda^0 = 1$. The leading coefficient of $f^*(x)$ is the constant term of $f(x)$, which is 1.

Since $f(x)$ and $f^*(x)$ are both monic and share the same set of roots, they must be identical. Thus, $f(x) = f^*(x)$ and is palindromic. $\square$

We now extend this property to the generator polynomials of codes over the ring $\mathbb{F}_q S$.

Theorem 4.3. *Let $q = 2^k$ for $k \geq 1$, and assume $(p-1)/m$ is even. Let C be an m -adic residue code of length p over $\mathbb{F}_q S$ (either Type A or Type B class). The generator polynomials of its component codes over $\mathbb{F}_q$ and S are palindromic.*

Proof. An m -adic residue code C of Type A or B is generated by an idempotent $E \in \mathcal{R}_p$. In Section 3, we represented these idempotents in their triplet form, e.g., $E = (e_i, e_k, e_j)$, corresponding to the isomorphism $\mathcal{R}_p \cong (\mathbb{F}_q[x]/(x^p - 1))^3$.

To analyze the generator polynomial over the ring S , it is useful to express E in its mixed form over $\mathbb{F}_q \times S$. The two representations are linked by the isomorphism Φ from Section 2.1, which relies on the map from S to $\mathbb{F}_q \times \mathbb{F}_q$ defined by $\xi + v\mu \mapsto (\xi, \xi + \mu)$. We now show the explicit correspondence for our idempotents. To obtain the pair (e_k, e_j) in the last two components of the triplet form, we can set $\xi = e_k$ and $\mu = e_j - e_k$. The corresponding element in the S -form is:

$$\xi + v\mu = e_k + v(e_j - e_k) = e_k + ve_j - ve_k = (1 - v)e_k + ve_j.$$

Therefore, the idempotent $E = (e_i, e_k, e_j)$ in triplet form is equivalent to the mixed form $(e_i, (1 - v)e_k + ve_j)$. From this, it is clear that the code C decomposes into three constituent codes over $\mathbb{F}_q$ generated by the idempotents e_i, e_k , and e_j .

Let the generator polynomials for these three base codes be $g_i(x), g_k(x)$, and $g_j(x)$, respectively. The generator polynomial for the first component of C (over $\mathbb{F}_q$) is simply $g_i(x)$. Since the conditions of Proposition 4.2 are met, $g_i(x)$ is palindromic. The generator for the code over S can be written as $g_S(x) = vg_j(x) + (1 - v)g_k(x)$. By Proposition 4.2, both $g_j(x)$ and $g_k(x)$ are palindromic.

For the resulting polynomial $g_S(x)$ to be palindromic, it is necessary that its constituent polynomials have the same degree. In the construction, $g_j(x)$ and $g_k(x)$ are generator polynomials for codes belonging to the same class over $\mathbb{F}_q$ (i.e., both are generators for what become components of a Type A code, or both for a Type B code). Therefore, their degrees are always equal. Let this common degree be d .

Let the coefficients of $g_j(x)$ and $g_k(x)$ be a_l and b_l , respectively, which satisfy the palindromic property $a_l = a_{d-l}$ and $b_l = b_{d-l}$. The l -th coefficient of $g_S(x)$ is $c_l = va_l + (1 - v)b_l$. We check the $(d - l)$ -th coefficient:

$$c_{d-l} = va_{d-l} + (1 - v)b_{d-l} = va_l + (1 - v)b_l = c_l.$$

This shows that $g_S(x)$ is also a palindromic polynomial. Thus, all generator polynomials associated with the code C are palindromic. $\square$

4.2. Framework for DNA Code Construction

To apply our algebraic results, we now establish a concrete framework for constructing DNA codes. For this purpose, we specialize our alphabet to the finite field $\mathbb{F}_{16}$, which provides a natural way to represent pairs of DNA bases. Let $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]/\langle \alpha^4 + \alpha + 1 \rangle$.

Definition 4.4 (Base DNA Map θ). Let the map $\theta : \mathbb{F}_{16} \rightarrow \{A, T, C, G\}^2$ assign a unique DNA base pair to each element of $\mathbb{F}_{16}$. We adopt the specific mapping from [10], as detailed in Table 1.

Table 1: The mapping $\theta : \mathbb{F}_{16} \rightarrow \{A, T, C, G\}^2$ [10].

Element	Poly.	DNA Pair	Element	Poly.	DNA Pair
0	0	AA	α^8	$1 + \alpha^2$	CG
1	1	TT	α^9	$\alpha + \alpha^3$	CA
α	α	AT	α^{10}	$1 + \alpha + \alpha^2$	GG
α^2	α^2	GC	α^{11}	$\alpha + \alpha^2 + \alpha^3$	CT
α^3	α^3	AG	α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	GA
α^4	$1 + \alpha$	TA	α^{13}	$1 + \alpha^2 + \alpha^3$	TG
α^5	$\alpha + \alpha^2$	CC	α^{14}	$1 + \alpha^3$	TC
α^6	$\alpha^2 + \alpha^3$	AC	α^7	$1 + \alpha + \alpha^3$	GT

Using the CRT isomorphism Φ from Section 2, we define a map from our algebraic ring to a short DNA sequence.

Definition 4.5 (Ring-to-DNA Map Ψ). The map $\Psi : \mathbb{F}_{16}S \rightarrow \{A, T, C, G\}^6$ is defined by applying θ to each of the three components obtained from the Φ isomorphism:

$$\Psi(\beta) = (\theta(\beta_1), \theta(\beta_2), \theta(\beta_3)),$$

where $\Phi(\beta) = (\beta_1, \beta_2, \beta_3)$, and the result is the concatenation of the three DNA base pairs.

This mapping is then extended from a single ring element to an entire codeword.

Definition 4.6 (Codeword-to-DNA Map Θ). Let $C \subseteq (\mathbb{F}_{16}S)^n$ be a code of length n . The map $\Theta : C \rightarrow (\{A, T, C, G\}^6)^n$ transforms a codeword $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$ into a DNA sequence of length $6n$ by component-wise application of Ψ :

$$\Theta(\mathbf{c}) = (\Psi(c_0), \Psi(c_1), \dots, \Psi(c_{n-1})).$$

This framework translates palindromic generator structure into reversal and reverse-complement closure properties for DNA strands, developed in the next section.

5. Construction of Reversible DNA Codes

In the previous section, we established the conditions under which the generators of our m -adic codes are palindromic and developed a framework to map algebraic codewords to DNA sequences. In this section, we bring these threads together to present a systematic method for constructing DNA codebooks that satisfy the reversal constraint.

5.1. The Reversal Automorphism and Code Reversibility

A DNA codebook $\mathcal{D}$ is called **reversible** if for every sequence $X \in \mathcal{D}$, its reverse sequence X^r is also in $\mathcal{D}$. Our goal is to construct algebraic codes over $\mathbb{F}_{16}S$ whose images under the map Θ satisfy this property. To do this, we first define an algebraic operation that models the physical reversal of a DNA sequence.

Recall from Section 4 that a DNA sequence is generated as $\Psi(\beta) = (\theta(\beta_1), \theta(\beta_2), \theta(\beta_3))$. The reversal of this 6-base sequence is:

$$\text{Reverse}(\Psi(\beta)) = (\text{Reverse}(\theta(\beta_3)), \text{Reverse}(\theta(\beta_2)), \text{Reverse}(\theta(\beta_1))).$$

A key property of the mapping θ from Table 1 is its relationship with the Frobenius automorphism $\gamma \mapsto \gamma^4$ of $\mathbb{F}_{16}$ over its subfield $\mathbb{F}_4$. For any $\gamma \in \mathbb{F}_{16}$, this relationship is given by [10]:

$$\text{Reverse}(\theta(\gamma)) = \theta(\gamma^4).$$

This identity is a design feature of the specific map θ in [10], and we exploit it to align algebraic operations with DNA reversal. The map is constructed such that the Frobenius automorphism $\gamma \mapsto \gamma^4$ over $\mathbb{F}_{16}$ (which fixes the subfield $\mathbb{F}_4$) corresponds precisely to the reversal of the DNA pair.

To illustrate, let us test this identity with an element from Table 1. Consider $\gamma = \alpha$.

- From the table, $\theta(\alpha) = AT$. The physical reversal is $\text{Reverse}(AT) = TA$.
- The algebraic operation gives α^4 , which corresponds to the element $1 + \alpha$ in the polynomial representation.
- Looking up this result in the table, we find $\theta(1 + \alpha) = TA$.

Thus, we see that $\text{Reverse}(\theta(\alpha)) = \theta(\alpha^4)$. A formal proof of this property for all elements can be found in the cited literature. Using this property, the reversed DNA sequence corresponds to the algebraic triplet $(\theta(\beta_3^4), \theta(\beta_2^4), \theta(\beta_1^4))$. This motivates the definition of an automorphism on $\mathbb{F}_{16}S$ that permutes and transforms the components in precisely this manner.

Definition 5.1 (Reversal Automorphism $\mathcal{A}$). Let $\mathcal{A}^* : \mathbb{F}_{16}^3 \rightarrow \mathbb{F}_{16}^3$ be the map defined by $\mathcal{A}^*(\beta_1, \beta_2, \beta_3) = (\beta_3^4, \beta_2^4, \beta_1^4)$. This map is a ring automorphism of $\mathbb{F}_{16}^3$. The **reversal automorphism** $\mathcal{A} : \mathbb{F}_{16}S \rightarrow \mathbb{F}_{16}S$ is defined via the isomorphism Φ as:

$$\mathcal{A} = \Phi^{-1} \circ \mathcal{A}^* \circ \Phi.$$

By construction, for any $\beta \in \mathbb{F}_{16}S$, the automorphism $\mathcal{A}$ satisfies $\Psi(\mathcal{A}(\beta)) = \text{Reverse}(\Psi(\beta))$.

Remark 5.2. Note that the reversal automorphism $\mathcal{A}$ is an involution, i.e., $\mathcal{A}^2 = \text{Id}$. This can be seen by applying the component-wise map $\mathcal{A}^*$ twice:

$$\mathcal{A}^*(\mathcal{A}^*(\beta_1, \beta_2, \beta_3)) = \mathcal{A}^*(\beta_3^4, \beta_2^4, \beta_1^4) = ((\beta_1^4)^4, (\beta_2^4)^4, (\beta_3^4)^4) = (\beta_1^{16}, \beta_2^{16}, \beta_3^{16}).$$

Since for any element $x \in \mathbb{F}_{16}$, we have $x^{16} = x$, this simplifies to $(\beta_1, \beta_2, \beta_3)$. Thus, applying $\mathcal{A}$ twice returns the original element. This property is crucial for the proof of our reversal identity.

A code $C \subseteq (\mathbb{F}_{16}S)^n$ will produce a set of DNA sequences closed under reversal if the code C itself is closed under the extended automorphism $\mathcal{A}$ applied component-wise. For cyclic codes, this closure property is directly related to their generator polynomials.

5.2. The Ω -Set Construction

While a palindromic generator ensures a cyclic code is reversible in the classical sense, achieving closure under the specific automorphism $\mathcal{A}$ requires a more tailored construction. We use the Ω -set method, a technique designed to build codes with such symmetries [2].

Let $g(x) \in (\mathbb{F}_{16}S)[x]$ be a palindromic generator polynomial of degree d for an m -adic code of length $n = p$. Let $k = n - d$ be the dimension parameter. We define the polynomial $\mathcal{A}(g(x))$ by applying the reversal automorphism $\mathcal{A}$ to each coefficient of $g(x)$:

$$\mathcal{A}(g(x)) = \sum_{j=0}^d \mathcal{A}(g_j)x^j, \quad \text{where } g(x) = \sum_{j=0}^d g_jx^j.$$

Since $g(x)$ is palindromic and $\mathcal{A}$ is an automorphism, $\mathcal{A}(g(x))$ is also a palindromic polynomial.

Definition 5.3 (The Ω -Set). Let $g(x)$ be a palindromic generator polynomial of degree d over $\mathbb{F}_{16}S$ for a code of length n . The Ω -set associated with $g(x)$, denoted by Λ_g , is the set of $k = n - d$ polynomials in the ring $R_n = (\mathbb{F}_{16}S)[x]/\langle x^n - 1 \rangle$:

$$\Lambda_g = \{\Lambda_0, \Lambda_1, \dots, \Lambda_{k-1}\},$$

where the polynomials Λ_i are defined for $i \in \{0, 1, \dots, k-1\}$ as follows:

$$\Lambda_i = \begin{cases} x^i g(x) \pmod{x^n - 1} & \text{if } i \text{ is even} \\ x^i \mathcal{A}(g(x)) \pmod{x^n - 1} & \text{if } i \text{ is odd} \end{cases}$$

The final code, which we will demonstrate to be reversible, is the linear span of this Ω -set.

$$C = \text{span}_{\mathbb{F}_{16}S}(\Lambda_g) = \left\{ \sum_{i=0}^{k-1} \beta_i \Lambda_i \mid \beta_i \in \mathbb{F}_{16}S \right\}.$$

To prove our main theorem, we first establish the central identity that connects the algebraic structure of our code with the physical reversal of the corresponding DNA sequence. This identity is the cornerstone of the Ω -set construction.

Lemma 5.4. Let $g(x)$ be a palindromic generator polynomial of degree d and let $k = n - d$ be an even integer. Let $C = \text{span}_{\mathbb{F}_{16}S}(\Lambda_g)$ be the code generated by the Ω -set Λ_g . For any codeword $c(x) = \sum_{i=0}^{k-1} \beta_i \Lambda_i \in C$, the following identity holds:

$$\left(\Theta \left(\sum_{i=0}^{k-1} \beta_i \Lambda_i \right) \right)^R = \Theta \left(\sum_{i=0}^{k-1} \mathcal{A}(\beta_i) \Lambda_{k-1-i} \right).$$

Proof. [Short Proof of the Reversal Identity] Let $c(x) = \sum_{i=0}^{k-1} \beta_i \Lambda_i(x)$. The physical reversal on the LHS corresponds to applying Θ to an algebraically reversed polynomial, which we denote by $(c(x))^R = \mathcal{A}(x^{n-1}c(x^{-1}))$. The polynomial on the RHS is $c''(x) = \sum_{i=0}^{k-1} \mathcal{A}(\beta_i) \Lambda_{k-1-i}(x)$. To prove the identity, it suffices to show that $(c(x))^R = c''(x)$.

By linearity, this is equivalent to showing that the identity holds for each basis element, i.e., $(\Lambda_i(x))^R = \Lambda_{k-1-i}(x)$ for all $i \in \{0, \dots, k-1\}$. We check this by cases.

Case 1: i is even. $(\Lambda_i(x) = x^i g(x))$ Using the palindromic property $g(x^{-1}) = x^{-d}g(x)$ and $n - d = k$:

$$\begin{aligned} (\Lambda_i(x))^R &= \mathcal{A}(x^{n-1} \cdot (x^{-i} g(x^{-1}))) = \mathcal{A}(x^{n-1-i} \cdot x^{-d} g(x)) \\ &= \mathcal{A}(x^{k-1-i} g(x)) = x^{k-1-i} \mathcal{A}(g(x)). \end{aligned}$$

Since k is even and i is even, the index $k-1-i$ is odd. By the definition of the Ω -set, this resulting polynomial is precisely $\Lambda_{k-1-i}(x)$.

Case 2: i is odd. $(\Lambda_i(x) = x^i \mathcal{A}(g(x)))$ Using the fact that $\mathcal{A}(g(x))$ is also palindromic and $\mathcal{A}$ is an involution ($\mathcal{A}^2 = Id$):

$$\begin{aligned} (\Lambda_i(x))^R &= \mathcal{A}(x^{n-1} \cdot (x^{-i} \mathcal{A}(g(x^{-1})))) = \mathcal{A}(x^{n-1-i} \cdot x^{-d} \mathcal{A}(g(x))) \\ &= \mathcal{A}(x^{k-1-i} \mathcal{A}(g(x))) = x^{k-1-i} \mathcal{A}(\mathcal{A}(g(x))) = x^{k-1-i} g(x). \end{aligned}$$

Since k is even and i is odd, the index $k-1-i$ is even. By definition, this resulting polynomial is precisely $\Lambda_{k-1-i}(x)$.

Since $(\Lambda_i)^R = \Lambda_{k-1-i}$ holds for all basis elements, linearity implies:

$$(c(x))^R = \left(\sum_{i=0}^{k-1} \beta_i \Lambda_i \right)^R = \sum_{i=0}^{k-1} \mathcal{A}(\beta_i) (\Lambda_i)^R = \sum_{i=0}^{k-1} \mathcal{A}(\beta_i) \Lambda_{k-1-i} = c''(x).$$

This completes the proof of the identity. $\square$

Theorem 5.5 (Reversibility Theorem). Let $g(x)$ be a generator polynomial of an m -adic residue code over $\mathbb{F}_{16}S$ of length $n = p$. Assume that $g(x)$ is palindromic and that its dimension parameter $k = n - d$ is an even integer. Let $C = \text{span}_{\mathbb{F}_{16}S}(\Lambda_g)$ be the linear code generated by the Ω -set Λ_g . Then the set of DNA sequences $\Theta(C)$ is a reversible DNA code.

Proof. Let $c(x) = \sum_{i=0}^{k-1} \beta_i \Lambda_i$ be an arbitrary codeword in C . Let $X = \Theta(c(x))$ be its corresponding DNA sequence. We must show that its reverse, X^r , is also in the DNA codebook $\Theta(C)$.

By Lemma 5.4, the reverse sequence is given by:

$$X^r = \Theta \left(\sum_{i=0}^{k-1} \mathcal{A}(\beta_i) \Lambda_{k-1-i} \right).$$

Let $c'(x) = \sum_{i=0}^{k-1} \mathcal{A}(\beta_i) \Lambda_{k-1-i}$. To complete the proof, we only need to show that $c'(x)$ is a valid codeword in C .

Let $j = k - 1 - i$. As i ranges from 0 to $k - 1$, j also ranges over the same set. The sum can be re-indexed in terms of j :

$$c'(x) = \sum_{j=0}^{k-1} \mathcal{A}(\beta_{k-1-j}) \Lambda_j.$$

Since $\mathcal{A}$ is an automorphism of $\mathbb{F}_{16}S$, each coefficient $\mathcal{A}(\beta_{k-1-j})$ is a valid scalar in the ring. Therefore, $c'(x)$ is an $\mathbb{F}_{16}S$ -linear combination of the basis elements of Λ_g , which means $c'(x)$ belongs to the span of Λ_g . By definition, $c'(x) \in C$.

Since $X^r = \Theta(c'(x))$ and we have shown that $c'(x) \in C$, the reverse of any DNA sequence is also in the codebook. Thus, $\Theta(C)$ is a reversible DNA code. $\square$

Example 5.6. We present the construction for the parameters $p = 17$ and $m = 4$ over $\mathbb{F}_{16}$.

- We choose these parameters because $m = 4$ divides $p - 1 = 16$, and $q = 16$ is a 4-adic residue modulo 17.
- The size of the cosets is $t = (17 - 1)/4 = 4$, which is an even integer. By Theorem 4.3, this ensures the generator polynomials of our m -adic codes over $\mathbb{F}_{16}S$ are palindromic.

Our goal is to use the Ω -set construction from Definition 5.4. A critical condition of Theorem 5.5 is that the dimension parameter for the construction, $k = n - d$, must be an even integer. We next determine which family of m -adic codes satisfies this condition for our parameters ($n = 17, t = 4$).

1. For the **Type B class** ($C_r^{(B)}$), the constituent codes are generated by complementary idempotents $1 - e_k$. The dimension of each constituent is $p - t$, and the generator polynomial has degree $t = 4$. This yields a construction parameter $k = n - d = 17 - 4 = 13$. Since 13 is odd, this code family **cannot** be used for this method.
2. For the **Type A class** ($C_r^{(A)}$), the constituent codes are cyclic ideals generated by e_k . The dimension of each constituent is t , and the generator polynomial has degree $p - t = 13$. This yields a construction parameter $k = n - d = 17 - 13 = 4$. Since 4 is even, this code family **satisfies** the theorem's condition.

Therefore, we must choose a generator polynomial $g(x)$ corresponding to a code from the **Type A class** of 4-adic codes of length 17. The dimension parameter for the Ω -set construction is $k = 4$. The Ω -set Λ_g is a set of 4 polynomials:

$$\Lambda_g = \{g(x), \quad x\mathcal{A}(g(x)), \quad x^2g(x), \quad x^3\mathcal{A}(g(x))\}.$$

The code $C = \text{span}_{\mathbb{F}_{16}S}(\Lambda_g)$ generated by this set is, by Theorem 5.5, guaranteed to produce a reversible DNA codebook $\Theta(C)$. The resulting DNA strands will have length $6n = 6 \times 17 = 102$. This framework provides a systematic method for generating large, algebraically-structured, reversible DNA codebooks.

6. Construction of Reverse-Complement DNA Codes

In this section, we strengthen our framework to satisfy the *reverse-complement* (RC) constraint, which is often required in DNA data storage. A DNA codebook $\mathcal{D}$ is **RC-closed** if for every sequence $X \in \mathcal{D}$, its reverse-complement X^{rc} is also in $\mathcal{D}$. The RC of a string is obtained by first reversing, then applying the Watson-Crick complement $A \leftrightarrow T$ and $C \leftrightarrow G$ symbolwise.

We follow the reversal construction of Theorem 5.5 and add a base-level complement operator *compatible* with the field-to-DNA map θ in Table 1. The key point is that we do *not* need this complement to be a ring automorphism in general; it suffices to define it as the *unique* permutation induced by θ and the Watson-Crick complement on pairs. When the complement happens to coincide with a Frobenius automorphism, we also give a stronger, purely algebraic closure via an lcm construction.

6.1. An algebraic model of Watson-Crick complement on $\mathbb{F}_{16}$

Definition 6.1 (Complement map induced by θ). Let $\theta : \mathbb{F}_{16} \rightarrow \{A, T, C, G\}^2$ be the fixed bijection in Table 1. Define the map

$$\eta : \mathbb{F}_{16} \longrightarrow \mathbb{F}_{16}$$

uniquely by the requirement

$$\theta(\eta(\gamma)) = \text{Comp}(\theta(\gamma)) \quad (\forall \gamma \in \mathbb{F}_{16}),$$

where Comp applies the Watson-Crick complement to each base in the DNA pair.

Remark 6.2. Since Comp is an involution on $\{A, T, C, G\}^2$ and θ is a bijection, η is automatically a permutation of $\mathbb{F}_{16}$ and an involution, i.e. $\eta^2 = \text{id}_{\mathbb{F}_{16}}$. No additional assumption on η is needed for our RC construction below.

Remark 6.3 (Optional semi-linear normal form). In some instances (including alternative θ 's used in the literature), the complement map admits a semi-linear form

$$\eta(\gamma) = u \gamma^{2^s}, \quad u \in \mathbb{F}_{16}^\times, \quad s \in \{0, 1, 2, 3\}.$$

If one wishes η to be an involution, then necessarily $2s \equiv 0 \pmod{4}$ and $u \cdot u^{2^s} = 1$. If, moreover, one wants η to be a field automorphism (hence a ring automorphism), then necessarily $u = 1$ and $\eta(\gamma) = \gamma^{2^s}$ (Frobenius). Our main Ω_{RC} construction does not require η to be a ring automorphism; the optional lcm construction below does.

6.2. The reverse-complement operator on coefficients

Recall the reversal operator $\mathcal{A}^* : \mathbb{F}_{16}^3 \rightarrow \mathbb{F}_{16}^3$ from Theorem 5.5, defined by

$$\mathcal{A}^*(\beta_1, \beta_2, \beta_3) = (\beta_3^4, \beta_2^4, \beta_1^4),$$

and $\mathcal{A} = \Phi^{-1} \circ \mathcal{A}^* \circ \Phi$ on $\mathbb{F}_{16}\mathbb{S}$. Using the complement map η of Definition 6.1 we set:

Definition 6.4 (Coefficient-wise RC operator). Define $\mathcal{B}^* : \mathbb{F}_{16}^3 \rightarrow \mathbb{F}_{16}^3$ by

$$\mathcal{B}^*(\beta_1, \beta_2, \beta_3) := (\eta(\beta_3^4), \eta(\beta_2^4), \eta(\beta_1^4)).$$

Then define $\mathcal{B} : \mathbb{F}_{16}\mathbb{S} \rightarrow \mathbb{F}_{16}\mathbb{S}$ by

$$\mathcal{B} = \Phi^{-1} \circ \mathcal{B}^* \circ \Phi.$$

For a polynomial $h(x) = \sum_{j=0}^d h_j x^j \in (\mathbb{F}_{16}\mathbb{S})[x]$, we write

$$\mathcal{B}(h(x)) := \sum_{j=0}^d \mathcal{B}(h_j) x^j.$$

Lemma 6.5 (RC corresponds to $\mathcal{B}$ under Θ). For any $\beta \in \mathbb{F}_{16}S$ we have

$$\Psi(\mathcal{B}(\beta)) = \text{RC}(\Psi(\beta)),$$

and for any codeword $\mathbf{c} = (c_0, \dots, c_{n-1})$,

$$\Theta(\mathcal{B}(\mathbf{c})) = (\Theta(\mathbf{c}))^{rc},$$

where $\mathcal{B}$ acts componentwise on $\mathbf{c}$.

Proof. By definition of $\mathcal{A}$ and η we have, for each component in $\Phi(\beta) = (\beta_1, \beta_2, \beta_3)$,

$$\text{Reverse}(\theta(\beta_i)) = \theta(\beta_i^4) \quad [2, 10], \quad \text{Comp}(\theta(\gamma)) = \theta(\eta(\gamma)).$$

Therefore

$$\text{RC}(\Psi(\beta)) = (\text{Comp}(\text{Reverse}(\theta(\beta_3))), \text{Comp}(\text{Reverse}(\theta(\beta_2))), \text{Comp}(\text{Reverse}(\theta(\beta_1)))) = (\theta(\eta(\beta_3^4)), \theta(\eta(\beta_2^4)), \theta(\eta(\beta_1^4))),$$

which equals $\Psi(\mathcal{B}(\beta))$ by Definition 6.4. Extending componentwise along the coordinates of $\mathbf{c}$ yields the statement for Θ . $\square$

Remark 6.6. In general η is only a permutation (Remark 6.2). Hence $\mathcal{B}$ is a well-defined bijection of the coefficient ring as a set, not necessarily a ring automorphism. This suffices for the Ω_{RC} construction below. In the special case when η is Frobenius (Remark 6.3 with $u = 1$), $\mathcal{B}$ becomes a ring automorphism; then we also present an lcm-based cyclic closure.

6.3. Reverse–complement constructions: default and Frobenius variant

Route A (default; used in this paper). When η is the table-induced complement on $\mathbb{F}_{16}$ (a permutation compatible with θ), define the coefficient operator $\mathcal{B}$ as in Definition 6.4 and build the Ω_{RC} -set (Definition 6.7). This route does not require η (hence $\mathcal{B}$) to be a ring automorphism and is the one we use in all examples.

Route B (Frobenius special case; optional). If, in addition, $\eta(\gamma) = \gamma^{2^s}$ for some s (so that $\mathcal{B}$ is a ring automorphism), one may still apply Route A; alternatively, a purely cyclic closure is available. Let $C = \langle g(x) \rangle$ be a cyclic code in $(\mathbb{F}_{16}S)[x]/\langle x^n - 1 \rangle$. Then:

- the smallest $\mathcal{B}$ -invariant cyclic code containing C is

$$\widetilde{C}_{\text{up}} = \langle \gcd(g(x), \mathcal{B}(g(x))) \rangle;$$

- the largest $\mathcal{B}$ -invariant cyclic subcode of C is

$$\widetilde{C}_{\text{down}} = \langle \text{lcm}(g(x), \mathcal{B}(g(x))) \rangle.$$

The gcd/lcm relations are the standard lattice rules for cyclic ideals. We include Route B for completeness; our numerical instances do not rely on the Frobenius assumption.

6.4. An Ω -set construction for RC-closed DNA codes

Let $n = p$ and let $g(x) \in (\mathbb{F}_{16}S)[x]$ be a palindromic generator of degree d for an m -adic residue code as in Theorem 5.5. Set $k := n - d$.

Definition 6.7 ($\Omega_{\text{RC}}\text{-set}$). Assume k is even. Define

$$\Lambda_i^{\text{RC}} := \begin{cases} x^i g(x) \pmod{x^n - 1}, & i \text{ even}, \\ x^i \mathcal{B}(g(x)) \pmod{x^n - 1}, & i \text{ odd}, \end{cases} \quad i = 0, 1, \dots, k-1.$$

Then set

$$C_{\text{RC}} := \text{span}_{\mathbb{F}_{16}\mathbb{S}} \{ \Lambda_0^{\text{RC}}, \dots, \Lambda_{k-1}^{\text{RC}} \} \subseteq (\mathbb{F}_{16}\mathbb{S})[x] / \langle x^n - 1 \rangle.$$

Lemma 6.8 (RC reversal identity). Let $c(x) = \sum_{i=0}^{k-1} \beta_i \Lambda_i^{\text{RC}}(x)$. Then

$$\left(\Theta(c(x)) \right)^{rc} = \Theta \left(\sum_{i=0}^{k-1} \mathcal{B}(\beta_i) \Lambda_{k-1-i}^{\text{RC}}(x) \right).$$

Proof. [Proof sketch] Define the algebraic RC-reversal operator on R_n by

$$R_{\text{RC}}(h) := \mathcal{B}(x^{n-1}h(x^{-1})).$$

Let $g(x)$ be palindromic of degree d , so $g(x^{-1}) = x^{-d}g(x)$ and $k = n - d$. For even i we have

$$R_{\text{RC}}(x^i g(x)) = \mathcal{B}(x^{n-1-i} g(x^{-1})) = \mathcal{B}(x^{k-1-i} g(x)) = x^{k-1-i} \mathcal{B}(g(x)).$$

For odd i we use that $\mathcal{B}$ acts coefficientwise and is an involution, hence

$$R_{\text{RC}}(x^i \mathcal{B}(g(x))) = \mathcal{B}(x^{n-1-i} \mathcal{B}(g(x^{-1}))) = x^{n-1-i} \mathcal{B}^2(g(x^{-1})) = x^{k-1-i} g(x).$$

Since k is even, $k-1-i$ has opposite parity to i , so $R_{\text{RC}}(\Lambda_i^{\text{RC}}) = \Lambda_{k-1-i}^{\text{RC}}$. Linearity gives the claimed identity. $\square$

Theorem 6.9 (RC-closed DNA code via Ω_{RC}). Let $g(x)$ be palindromic of degree d , $k = n - d$ even, and let C_{RC} be as in Definition 6.7. Then $\Theta(C_{\text{RC}})$ is RC-closed:

$$X \in \Theta(C_{\text{RC}}) \implies X^{rc} \in \Theta(C_{\text{RC}}).$$

Remark 6.10 (Distance and parameters). The Lee-distance of C_{RC} equals that of the underlying even/odd-like components, namely

$$d_L(C_{\text{RC}}) = \min \{ d_H(C^{(1)}), d_H(C^{(2)}), d_H(C^{(3)}) \},$$

since Θ only permutes/acts coordinatewise on symbols via Ψ and does not change supports. Thus the parameter analysis in the reversible case carries over under the same Lee-weight definition / CRT decomposition.

6.5. Cyclic RC-closure via lcm (when η is Frobenius)

The following purely algebraic construction is available in the special case when η is a field automorphism, i.e. $\eta(\gamma) = \gamma^{2^s}$.

Proposition 6.11 (lcm RC-closure). Assume $\eta(\gamma) = \gamma^{2^s}$ so that $\mathcal{B}$ is a ring automorphism. For any cyclic code $C = \langle g(x) \rangle \subseteq (\mathbb{F}_{16}\mathbb{S})[x] / \langle x^n - 1 \rangle$ set

$$\widetilde{C} := \langle \text{lcm}(g(x), \mathcal{B}(g(x))) \rangle.$$

Then $\Theta(\widetilde{C})$ is RC-closed. Moreover, $\widetilde{C}$ is the largest $\mathcal{B}$ -invariant cyclic subcode of C .

Proof. Since $\mathcal{B}$ is a ring automorphism, $\langle g \rangle$ and $\langle \mathcal{B}(g) \rangle$ are cyclic ideals and their intersection is generated by the lcm. $\mathcal{B}$ fixes $\text{lcm}(g, \mathcal{B}(g))$ up to units, hence $\widetilde{C}$ is $\mathcal{B}$ -invariant. The statement on Θ follows from Lemma 6.5. $\square$

Example 6.12 ($p = 5, m = 2, q = 16$). We keep $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]/\langle \alpha^4 + \alpha + 1 \rangle$ and reuse the concrete even-like generator from Example 3.6:

$$g_S(x) = x^3 + c x^2 + c x + 1, \quad c := (1 - v)(\alpha^2 + \alpha + 1) + v(\alpha^2 + \alpha),$$

which is palindromic with $\deg g = 3$, hence $k = n - \deg g = 5 - 3 = 2$.

The Ω_{RC} basis and the RC-closed code. With $k = 2$ the Ω_{RC} -set is

$$\Lambda_0^{\text{RC}} = g_S(x), \quad \Lambda_1^{\text{RC}} = x \mathcal{B}(g_S(x)) \pmod{x^5 - 1},$$

where $\mathcal{B}$ is applied coefficientwise as in Definition 6.4. Define

$$C_{\text{RC}} = \text{span}_{\mathbb{F}_{16}S} \{ \Lambda_0^{\text{RC}}, \Lambda_1^{\text{RC}} \} \subset (\mathbb{F}_{16}S)[x]/\langle x^5 - 1 \rangle.$$

By Theorem 6.9, $\Theta(C_{\text{RC}})$ is reverse-complement closed. Its Lee distance equals $d_L(C_{\text{RC}}) = 4$ (Remark 6.10), since the three CRT components are the even-like $[5, 2, 4]$ codes over $\mathbb{F}_{16}$.

Remark 6.13. The operator $\mathcal{B}$ is a symbolwise permutation induced by the DNA complement (it is not a ring automorphism); thus it need not preserve units (e.g. $\mathcal{B}(1) = 0$ under the table in Table 1). The Ω_{RC} construction and Theorem 6.9 only require $\mathcal{B}$ to be an involutive permutation compatible with θ , not monicity or degree preservation of $\mathcal{B}(g)$.

7. Conclusion

We studied m -adic residue codes over the mixed alphabet $\mathbb{F}_qS = \mathbb{F}_q \times (\mathbb{F}_q + v\mathbb{F}_q)$ through a CRT-based, idempotent framework. Under the standing assumptions p prime, $\gcd(p, q) = 1$, $m \mid (p-1)$ and $q \bmod p \in Q_0$, we described Type A/B families from minimal idempotents and an explicit triplet representation. For $q = 2^k$ and $t = (p-1)/m$ even, we obtained palindromic generators componentwise; over S a simple degree-matching condition preserves palindromicity.

Motivated by DNA storage, we modeled reversal via a coefficient operator $\mathcal{A}$ compatible with a standard map $\theta : \mathbb{F}_{16} \rightarrow \{A, T, C, G\}^2$, and gave an Ω -set construction that ensures reversal when $k = n - \deg g$ is even. We further introduced a table-induced complement η on $\mathbb{F}_{16}$ and the associated operator $\mathcal{B}$ to obtain an Ω_{RC} construction for reverse-complement closure without requiring η to be a ring automorphism; in the Frobenius special case $\eta(\gamma) = \gamma^{2^s}$ we also recorded a cyclic gcd/lcm closure. Small-length instances for $(p, m, q) = (5, 2, 16)$ and $(17, 4, 16)$ illustrate the method with explicit generators and distances (e.g., three $[5, 2, 4]$ constituents and Lee distance 4 over $\mathbb{F}_{16}S$).

Limitations. Our analysis focuses on prime length, the residue condition $q \bmod p \in Q_0$, and table-driven η tied to the chosen θ ; we did not pursue parameter optimality or decoding/complexity aspects.

Outlook.

- Construct generators $g(x)$ that are fixed points of $\mathcal{B}$, leading to simpler RC-closed cyclic codes.
- Extend the framework to duadic/polyadic/constacyclic families over $\mathbb{F}_qS$ and related non-chain rings; compare parameters systematically.
- Incorporate biophysical filters (GC-content, homopolymer limits, melting temperature) into the algebraic design and quantify trade-offs.
- Develop decoding algorithms and complexity analyses aligned with the CRT decomposition.
- Investigate Frobenius cases in depth and structural criteria for minimal $\mathcal{B}$ -invariant closures.

References

- [1] L. M. Adleman, *Molecular computation of solutions to combinatorial problems*, Science **266** (5187) (1994), 1021–1024.
- [2] A. Bayram, E. S. Oztas, I. Siap, *Codes over $\mathbb{F}_4 + v\mathbb{F}_4$ and some DNA applications*, Designs, Codes and Cryptography **80** (2016), 379–393.
- [3] R. A. Brualdi, V. S. Pless, *Polyadic codes*, Discrete Applied Mathematics. **25** (1-2) (1989), 3–17.
- [4] F. Gursoy, I. Siap, B. Yildiz, *Construction of skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q$* , Advances in Mathematics of Communications **8** (3) (2014), 313–322.
- [5] A. R. Hammons Jr., 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** (2) (1994), 301–319.
- [6] W. C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
- [7] V. R. Job, *M-adic residue codes*, IEEE Transactions on Information Theory **38** (2) (1992), 496–501.
- [8] F. Kuruz, E. S. Oztas, I. Siap, *m-adic residue codes over $\mathbb{F}_q[v]/(v^2 - v)$ and DNA codes*, Bull. Korean Math. Soc. **55** (2018), 921–935.
- [9] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, **16** Elsevier, 1977.
- [10] E. S. Oztas, I. Siap, *Lifted polynomials over $\mathbb{F}_{16}$ and their applications to DNA codes*, Filomat **27** (3) (2013), 459–466.
- [11] T. Yildirim, *Construction of cyclic DNA codes over $\mathbb{Z}_4R$* , Indian Journal of Pure and Applied Mathematics **55** (4) (2024), 1465–1476.
- [12] T. Yildirim, *Linear Skew Cyclic Codes over $\mathbb{F}_qS$* , An. Șt. Univ. Ovidius Constanța **32** (3) (2024), 173–192, doi:10.2478/auom-2024-0035.