

Research Paper

MULTI-TWISTED CODES AS FREE MODULES OVER PRINCIPAL IDEAL DOMAINS

RAMY TAKI ELDIN*

ABSTRACT. We begin by introducing the simple algebraic structure of cyclic, constacyclic, quasi-cyclic (QC), quasi-twisted (QT), generalized quasi-cyclic (GQC), and multi-twisted (MT) codes over finite fields. Then, we establish the correspondence between these codes and submodules of the free $\mathbb{F}_q[x]$ -module $(\mathbb{F}_q[x])^\ell$. We show that an MT code is a linear code over the principal ideal domain (PID) $\mathbb{F}_q[x]$. Hence, a basis of this code exists and is used to build a generator matrix with polynomial entries, called the generator polynomial matrix (GPM). The Hermite normal form of matrices over PIDs is exploited to achieve the reduced GPMs of MT codes. Some properties of the reduced GPM are introduced, for example, the identical equation. A formula for a GPM of the dual code of an MT code is established. At this point, special attention is paid to QC codes. We characterize GPMs for QC codes that combine reversibility and self-duality/self-orthogonality. We show the existence of binary self-orthogonal reversible QC codes that have the best known parameters as linear codes.

DOI: 10.22034/as.2025.19868.1629

MSC(2010): Primary: 11T71; Secondary: 13C10, 15A54.

Keywords: Dual code, Generator polynomial matrix, Hermite normal form, Multi-twisted code.

Received: 14 March 2023, Accepted: 19 January 2025.

*Corresponding author

1. INTRODUCTION

During data transmission, noise may undoubtedly cause data errors and distortion. Error correction techniques provide transmission robustness by detecting and correcting data distortion. A code is defined as the set of all possible transmitted codewords. By defining a metric, e.g., the Hamming distance, the code with the largest minimum distance between its codewords has the greatest error-correcting capability. For fixed code length and code size, the code with the largest minimum Hamming distance is called an optimal code. Researchers use computer search to find optimal codes over different alphabets [6, 16]. Linear codes with rich algebraic structure have found their superiority in engineering applications. For example, cyclic codes constitute a class of linear codes with a rich algebraic structure. This was followed by many generalizations for the algebraic structure of cyclic codes that led to other classes of linear codes with more complicated algebraic descriptions.

A cyclic code over a ring R is a linear code with the structure of an ideal in the ring of polynomials over R . The class of quasi-cyclic (QC) codes is obtained by not limiting the shift index of cyclic codes to unity. A QC code is a linear code invariant under the cyclic shift of a number of coordinates. QC codes have been addressed in several studies, e.g., [2, 3, 4]. Another class of linear codes is the class of constacyclic codes, which is obtained by generalizing the shift constant of cyclic codes. See [17] for a detailed description of constacyclic codes and their algebraic structure. Although the shift index of QC codes is not limited to unity, the block lengths are equal. Generalizing block lengths of QC codes, such that they are not necessarily equal, has led to a more general class of codes known in the literature as generalized quasi-cyclic (GQC) codes. In [18, 27], the algebraic structure of GQC codes is explained. However, generalizing the shift constant of QC codes, such that it does not necessarily equal unity, led to the class of quasi-twisted (QT) codes [19, 12]. In [1], QT and GQC codes are generalized to multi-twisted (MT) codes. MT codes are similar to GQC codes in that the block lengths are not necessarily equal, and they are similar to QT codes in that the shift constant is not necessarily equal to unity, moreover, the shift constants for different blocks are not necessarily the same. The algebraic structure of MT codes over finite fields is studied in [26, 5].

In this study, we start by defining cyclic and constacyclic codes over finite fields and presenting their algebraic structures as ideals in quotient rings. We unified the definition of QC, QT, GQC, and MT codes over finite fields as invariant linear codes under some linear transformations. Such invariance is the key behind defining an action on these codes which gives them the structure of modules over a principal ideal domain (PID); cf. [21, 24]. Specifically, we consider QC, QT, GQC, and MT codes as linear codes over PIDs. We show how generators of these codes can be deduced from their generator matrices. Hence, these generators are used to construct a generator polynomial matrix (GPM) for the code as a linear code over a

PID. For the broader class of MT codes, we aim to provide a minimal generating set and an algorithmic technique for finding this minimal set. Many known properties of vector spaces remain true for modules over PIDs. For instance, a submodule of a free module over a PID is free [25]. This makes MT codes free modules over PIDs, and we show how a basis of MT codes can be inferred. Although this basis is used to construct a GPM with entries from a PID, we aimed to find a unique reduced matrix form. This reduced form can be achieved by the Hermite normal form [20]. We show how to get the unique reduced GPM from any GPM. We prove the relationship between the code dimension and the diagonal entries of the reduced GPM. We present the identical equation satisfied by the GPM. The identical equation plays a major role in constructing the GPM of the dual code. We describe the dual code of any MT code, which has been shown to be MT as well. Using the identical equation, we explain how to construct a GPM for the dual of an MT code. Specifying to subclasses of MT codes, formulas for GPMs of the dual codes of QC, QT, and GQC codes are presented. Intuitively, this provides conditions for the self-duality and self-orthogonality of these codes. In fact, a code is self-dual if it is identical to its dual, while it is self-orthogonal if it is contained in its dual.

A code is called reversible if it is invariant under reversing the coordinates of its codewords. Massey [23] considered reversibility in the class of cyclic codes. He demonstrated that a cyclic code over a finite field is reversible if and only if its generator polynomial is self-reciprocal. Since QC codes generalize cyclic codes, it was natural to study reversibility in the class of QC codes. In [8, 10, 9], reversibility for some classes of QC codes has been considered. We show an explicit formula for a GPM of the reversed code of a QC code, where the reversed code is the code obtained by reversing the coordinates of all codewords. Using this formula, we summarize some of the results of [11] about the relations between reversibility, self-duality, and self-orthogonality of QC codes and their impact on the GPMs. We restrict ourselves to QC codes because this class contains many codes with the best known parameters [22], where a code has the best known parameters if its minimum distance meets the upper bound in [16]. Specifically, we present some QC codes that combine reversibility, self-orthogonality, and optimality. We conclude the study by listing some results obtained by computer search for binary optimal self-orthogonal reversible QC codes in Table 1.

2. FROM CYCLIC TO MULTI-TWISTED CODES

Let \mathbb{F}_q be the finite field of order q , where q is a prime power. If q is a prime number, then \mathbb{F}_q is isomorphic to the quotient ring $\mathbb{Z}/\langle q \rangle$, where $\langle q \rangle = \{0, \pm q, \pm 2q, \pm 3q, \dots\}$ is the ideal generated by q in the ring of integers \mathbb{Z} . In $\mathbb{Z}/\langle q \rangle$, additions and multiplications are carried modulo q . However, if $q = p^d$ for a prime p and an integer $d > 1$, then \mathbb{F}_q is isomorphic to

the quotient ring $\mathbb{F}_p[x]/\langle f(x) \rangle$, where $\mathbb{F}_p[x]$ is the ring of polynomials in the indeterminate x with coefficient from \mathbb{F}_p , $f(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d , and $\langle f(x) \rangle = \{a(x)f(x) | a(x) \in \mathbb{F}_p[x]\}$.

A code \mathcal{C} over the alphabet \mathbb{F}_q of length n is a subset of the vector space \mathbb{F}_q^n . The elements of \mathcal{C} are called codewords. The weight of a codeword of \mathcal{C} is the number of non-zero coordinates in the codeword. The minimum weight of \mathcal{C} is the smallest weight among all non-zero codewords. The Hamming distance between two codewords of \mathcal{C} is the number of coordinates at which the two codewords differ. The minimum Hamming distance of \mathcal{C} , denoted $d_{\min}(\mathcal{C})$ or d_{\min} , is the smallest Hamming distance between each pair of unequal codewords. If \mathcal{C} is a code over \mathbb{F}_q of length n and minimum distance d_{\min} , then the first $n - d_{\min} + 1$ coordinates of all the codewords are distinct. Hence, there are at most $q^{n-d_{\min}+1}$ codewords in \mathcal{C} . This gives the following fundamental bound on the minimum distance of a code, which is known as the Singleton bound.

Theorem 2.1 (Singleton Bound). *Let \mathcal{C} be a code of length n over an alphabet of size q . If \mathcal{C} has a minimum distance d_{\min} , then*

$$|\mathcal{C}| \leq q^{n-d_{\min}+1}.$$

A code \mathcal{C} is linear if it is a subspace of \mathbb{F}_q^n , that is, \mathcal{C} is closed under addition and scalar multiplication by elements of \mathbb{F}_q . The dimension k of a linear code is its dimension as a vector space over \mathbb{F}_q . Therefore, the size of a linear code of dimension k is $|\mathcal{C}| = q^k$. The minimum weight and the minimum Hamming distance are equal for any linear code, and the Singleton bound takes the form

$$(1) \quad d_{\min} \leq n - k + 1.$$

There are other minimum distance bounds, for example, sphere-packing bound [7] and Gilbert–Varshamov bound [14]. For fixed alphabet, code length, and dimension, a code with the largest minimum Hamming distance is best for practical communication systems. A code that achieves the upper bound of any of the bounds on the minimum distance is called optimal. In particular, a code that achieves the Singleton bound is called maximum distance separable (MDS), while a code that achieves the sphere-packing bound is called perfect. Researchers are interested in using computer searches to find optimal codes. Their results yield codes with the best known d_{\min} for fixed n and k . These records can be found in [16].

A linear code \mathcal{C} over \mathbb{F}_q of length n is cyclic if it is invariant under cyclic shifts of its coordinates. Namely,

$$(c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \dots, c_{n-3}, c_{n-2}) \in \mathcal{C}.$$

The main advantage of using cyclic codes over other codes in communication systems is that cyclic codes can be efficiently encoded using shift registers. Let \mathcal{R} be the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. Elements of \mathcal{R} are represented by polynomials in the indeterminate x over \mathbb{F}_q of degree at most $n - 1$ with addition and multiplication carried out modulo $x^n - 1$. In addition, \mathcal{R} can be viewed as a vector space over \mathbb{F}_q of dimension n , so \mathcal{R} is isomorphic to \mathbb{F}_q^n . It is usual to use this isomorphism to represent codewords by polynomials rather than vectors. Precisely, the word $(a_0, a_1, \dots, a_{n-2}, a_{n-1}) \in \mathbb{F}_q^n$ has a polynomial representation $a_0 + a_1x + \dots + a_{n-2}x^{n-2} + a_{n-1}x^{n-1}$ for its correspondence in \mathcal{R} . In its polynomial representation, a linear code is an \mathbb{F}_q -subspace of \mathcal{R} . Since multiplication is carried modulo $x^n - 1$, cyclic shift of a codeword corresponds to multiplying its polynomial representation by x . The ring \mathcal{R} can be thought of as an \mathcal{R} -module. Therefore, the property of a cyclic code being invariant under cyclic shifts makes this code acts as an \mathcal{R} -submodule of \mathcal{R} , i.e., an ideal in \mathcal{R} . There is a one-to-one correspondence between cyclic codes over \mathbb{F}_q of length n and ideals of \mathcal{R} . This property is generalized to a broader class, the class of constacyclic codes. For a non-zero $\lambda \in \mathbb{F}_q$, a linear code \mathcal{C} is λ -constacyclic if

$$(c_0, c_1, \dots, c_{n-2}, c_{n-1}) \in \mathcal{C} \Rightarrow (\lambda c_{n-1}, c_0, \dots, c_{n-3}, c_{n-2}) \in \mathcal{C}.$$

We call λ the shift constant. A 1-constacyclic code is simply a cyclic code. A (-1) -constacyclic code is called negacyclic; any negacyclic code over a ring of characteristic 2 is cyclic. The class of constacyclic codes includes cyclic and negacyclic codes. Analogous to cyclic codes, constacyclic codes have a polynomial representation. Consequently, a λ -constacyclic code over \mathbb{F}_q of length n is an ideal in the quotient ring $\mathcal{R}_\lambda = \mathbb{F}_q[x]/\langle x^n - \lambda \rangle$, and there is a one-to-one correspondence between λ -constacyclic codes and ideals of \mathcal{R}_λ .

A PID is an integral domain in which each ideal is principal. That is, an integral domain R is a PID if for every ideal I of R , there is an element $a \in I$ such that $I = Ra = \{ra | r \in R\}$. The element a is a generator of I and we write $I = \langle a \rangle$. Examples of PIDs are the ring of integers \mathbb{Z} , the quotient ring $\mathbb{Z}[x]/\langle x^2 + 1 \rangle$, and the ring of polynomials $\mathbb{F}_q[x]$. PIDs play an important role in the algebraic structure of some classes of codes. For instance, for constacyclic codes, we have the following:

Proposition 2.2. *Let \mathcal{C} be a λ -constacyclic code over \mathbb{F}_q of length n and dimension k . Then $\mathcal{C} = \langle g(x) \rangle$ for some $g(x) \in \mathbb{F}_q[x]$ such that $g(x) | (x^n - \lambda)$. Moreover, $k = n - \deg(g(x))$.*

Proof. We know that \mathcal{C} is an ideal in \mathcal{R}_λ . However, the projection map $\pi : \mathbb{F}_q[x] \rightarrow \mathcal{R}_\lambda$ defines a bijection between ideals of $\mathbb{F}_q[x]$ that contain $\langle x^n - \lambda \rangle$ and ideals of \mathcal{R}_λ . Then, \mathcal{C} can be shown as an ideal of $\mathbb{F}_q[x]$ containing $\langle x^n - \lambda \rangle$. Since $\mathbb{F}_q[x]$ is a PID, $\mathcal{C} = \langle g(x) \rangle \supseteq \langle x^n - \lambda \rangle$ for some $g(x) \in \mathbb{F}_q[x]$. But $\langle g(x) \rangle \supseteq \langle x^n - \lambda \rangle$ if and only if $g(x) | (x^n - \lambda)$, i.e., $a(x)g(x) = x^n - \lambda$ for some $a(x) \in \mathbb{F}_q[x]$. We call $a(x)$ the check polynomial of \mathcal{C} . The dimension of \mathcal{C} is the

dimension of $\langle g(x) \rangle / \langle x^n - \lambda \rangle$ as an \mathbb{F}_q -vector space. Therefore, $k = \deg(a(x)) = n - \deg(g(x))$.

□

The polynomial $g(x)$ is not uniquely specified; any $g(x)$ such that $\mathcal{C} = \langle g(x) \rangle$ is called a generator polynomial of \mathcal{C} . However, restricting $g(x)$ to be monic ensures its uniqueness. Thus, one can uniquely define $g(x)$ to be the least degree monic polynomial in \mathcal{C} as an ideal in $\mathbb{F}_q[x]$. So far we have shown that a λ -constacyclic code \mathcal{C} is completely determined by the monic polynomial $g(x) \in \mathcal{C}$ that divides $x^n - \lambda$ and generates \mathcal{C} as an ideal in the PID $\mathbb{F}_q[x]$. Consequently, all λ -constacyclic codes over \mathbb{F}_q of length n can be enumerated by decomposing $x^n - \lambda$ into irreducible factors in $\mathbb{F}_q[x]$. We aim to give the corresponding unique representation in the broader class of multi-twisted codes.

Example 2.3. Let $\mathbb{F}_9 = \{0, 1, 2, \theta, 2\theta, 1 + \theta, 1 + 2\theta, 2 + \theta, 2 + 2\theta\}$, where $\theta^2 + 2\theta + 2 = 0$. We construct a 2-constacyclic code \mathcal{C} over \mathbb{F}_9 of length 5. In \mathbb{F}_9 , $2 = -1$, then \mathcal{C} is negacyclic as well. Factorizing $x^5 - 2$ to irreducible factors yields $x^5 - 2 = (x + 1)(x^2 + 2\theta x + 1)(x^2 + (\theta + 2)x + 1)$. Different 2-constacyclic codes over \mathbb{F}_9 of length 5 are obtained through different choices of generator polynomials from the factorization of $x^5 - 2$ in $\mathbb{F}_9[x]$. Let $\mathcal{C} = \langle g(x) \rangle$, where $g(x) = x^2 + 2\theta x + 1$. The dimension of \mathcal{C} is $k = n - \deg(g(x)) = 3$. The check polynomial of \mathcal{C} is $a(x) = \frac{x^5 - 2}{g(x)} = (x + 1)(x^2 + (\theta + 2)x + 1)$. By listing all codewords of \mathcal{C} , one can observe that the codewords with the fewest number of monomials in their polynomial representation contain three monomials. Therefore, $d_{\min} = 3$. From (1), \mathcal{C} achieves the Singleton bound, and is therefore MDS.

Constacyclic codes generalize cyclic codes by generalizing the shift constant λ . A different generalization of cyclic codes is obtained by generalizing the shift index, and this leads to the class of QC codes.

Definition 2.4. A linear code \mathcal{C} over \mathbb{F}_q of length n is ℓ -QC if it is invariant under cyclic shift by ℓ coordinates. Namely,

$$(2) \quad (c_1, c_2, \dots, c_n) \in \mathcal{C} \Rightarrow (c_{n-\ell+1}, \dots, c_n, c_1, c_2, \dots, c_{n-\ell}) \in \mathcal{C}.$$

Define the index of a QC code to be the smallest positive integer ℓ satisfying (2). Hereinafter, the index is denoted by ℓ .

Proposition 2.5. *The index ℓ of a QC code divides the code length n .*

Proof. Let m be the unique positive integer defined such that $0 \leq m\ell - n < \ell$. Since \mathcal{C} is invariant under ℓ shifts of coordinates, it is invariant under $m\ell - n$ shifts. Then $m\ell - n = 0$ because $m\ell - n < \ell$ and ℓ is the smallest integer satisfying (2). Thus $n = m\ell$ and $\ell | n$. □

The integer $m = n/\ell$ in the proof of Proposition 2.5 is called the co-index of \mathcal{C} . A codeword of an ℓ -QC code \mathcal{C} of length n and co-index m can be partitioned as follows:

$$(3) \quad \mathbf{c} = (c_{0,1}, c_{0,2}, \dots, c_{0,\ell}, c_{1,1}, c_{1,2}, \dots, c_{1,\ell}, \dots, c_{m-1,1}, c_{m-1,2}, \dots, c_{m-1,\ell}).$$

A linear code \mathcal{C} is QC if and only if, for every $\mathbf{c} \in \mathcal{C}$ in the form of (3), \mathcal{C} contains the codeword

$$(c_{m-1,1}, c_{m-1,2}, \dots, c_{m-1,\ell}, c_{0,1}, c_{0,2}, \dots, c_{0,\ell}, \dots, c_{m-2,1}, c_{m-2,2}, \dots, c_{m-2,\ell}).$$

Let T_ℓ be the automorphism of \mathbb{F}_q^n that corresponds to shifting by ℓ coordinates. That is, $T_\ell : (a_1, a_2, \dots, a_n) \mapsto (a_{n-\ell+1}, \dots, a_n, a_1, a_2, \dots, a_{n-\ell})$ for every $(a_1, a_2, \dots, a_n) \in \mathbb{F}_q^n$. In the standard basis of \mathbb{F}_q^n , T_ℓ has the $n \times n$ matrix representation

$$\begin{pmatrix} \mathbf{0}_{\ell \times (n-\ell)} & \mathbf{I}_{\ell \times \ell} \\ \mathbf{I}_{(n-\ell) \times (n-\ell)} & \mathbf{0}_{(n-\ell) \times \ell} \end{pmatrix},$$

where $\mathbf{0}_{i \times j}$ and \mathbf{I}_i are the zero matrix of size $i \times j$ and the identity matrix of size $i \times i$, respectively. An alternative definition of an ℓ -QC code is a linear subspace of \mathbb{F}_q^n that is invariant under T_ℓ . This invariance is used to give QC codes the structure of module over PID. Although QC codes generalize cyclic codes because cyclic codes are QC with $\ell = 1$, QC codes do not generalize constacyclic codes. One can find a class containing QC and constacyclic codes as subclasses by generalizing the linear operator T_ℓ . For $0 \neq \lambda \in \mathbb{F}_q$, let $T_{(\ell, \lambda)}$ be the automorphism of \mathbb{F}_q^n such that $T_{(\ell, \lambda)} : (a_1, a_2, \dots, a_n) \mapsto (\lambda a_{n-\ell+1}, \dots, \lambda a_n, a_1, a_2, \dots, a_{n-\ell})$. In the standard basis of \mathbb{F}_q^n , $T_{(\ell, \lambda)}$ has the $n \times n$ matrix representation

$$(4) \quad \mathbf{M} = \begin{pmatrix} \mathbf{0}_{\ell \times (n-\ell)} & \lambda \mathbf{I}_\ell \\ \mathbf{I}_{(n-\ell)} & \mathbf{0}_{(n-\ell) \times \ell} \end{pmatrix}.$$

Obviously $T_\ell = T_{(\ell, 1)}$, and this generalizes QC codes to QT codes. From (4), we have $\mathbf{M}^m = \lambda \mathbf{I}_n$, hence $\frac{1}{\lambda} T_{(\ell, \lambda)}^m$ is the identity map on \mathbb{F}_q^n . Then $\mathbf{M}^{mt} = \mathbf{I}_n$ and $T_{(\ell, \lambda)}^{mt}$ is the identity map, where t is the multiplicative order of λ , i.e., t is the least positive integer such that $\lambda^t = 1$.

Definition 2.6. For a non-zero $\lambda \in \mathbb{F}_q$, a linear code \mathcal{C} is called (ℓ, λ) -QT if \mathcal{C} is invariant under $T_{(\ell, \lambda)}$. That is,

$$(5) \quad (c_1, c_2, \dots, c_n) \in \mathcal{C} \Rightarrow (\lambda c_{n-\ell+1}, \dots, \lambda c_n, c_1, c_2, \dots, c_{n-\ell}) \in \mathcal{C}.$$

The index of \mathcal{C} is the smallest positive integer ℓ that satisfies (5). We call λ the shift constant of \mathcal{C} .

Similar to QC codes, the index of a QT code divides its length. The co-index of \mathcal{C} is the integer $m = n/\ell$. By partitioning the codewords of a linear code \mathcal{C} of length $m\ell$ to m blocks of length ℓ each, then \mathcal{C} is (ℓ, λ) -QT if and only if

$$(\lambda c_{m-1,1}, \lambda c_{m-1,2}, \dots, \lambda c_{m-1,\ell}, c_{0,1}, c_{0,2}, \dots, c_{0,\ell}, \dots, c_{m-2,1}, c_{m-2,2}, \dots, c_{m-2,\ell}),$$

is a codeword in \mathcal{C} for every codeword in the form of (3). The class of QT codes generalizes QC and constacyclic codes because an ℓ -QC code is $(\ell, 1)$ -QT, a λ -constacyclic code is $(1, \lambda)$ -QT, and a cyclic code is $(1, 1)$ -QT.

Theorem 2.7. *Let \mathcal{C} be a linear code over \mathbb{F}_q of length n , dimension k , and a $k \times n$ generator matrix \mathbf{G} . Then, \mathcal{C} is (ℓ, λ) -QT if and only if the rank of the block matrix*

$$(6) \quad \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}^t \end{pmatrix},$$

is k , where t stands for matrix transpose and \mathbf{M} is given by (4).

Proof. Assume \mathbf{G} satisfies

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}^t \end{pmatrix} = k.$$

For any codeword $\mathbf{c} \in \mathcal{C}$, there exists $\mathbf{a} \in \mathbb{F}_q^k$ such that $\mathbf{c} = \mathbf{a}\mathbf{G}$. Since the dimension of \mathcal{C} is k , $\text{rank}(\mathbf{G}) = k$ and

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{c}\mathbf{M}^t \end{pmatrix} \geq k.$$

But

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{c}\mathbf{M}^t \end{pmatrix} = \text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{a}\mathbf{G}\mathbf{M}^t \end{pmatrix} = \text{rank} \left(\begin{pmatrix} \mathbf{I}_k & \mathbf{0}_{k \times k} \\ \mathbf{0}_{1 \times k} & \mathbf{a} \end{pmatrix} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}^t \end{pmatrix} \right) \leq \text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}^t \end{pmatrix} = k.$$

Then

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{c}\mathbf{M}^t \end{pmatrix} = k.$$

This shows that $\mathbf{c}\mathbf{M}^t \in \mathcal{C}$ and \mathcal{C} is (ℓ, λ) -QT because it is invariant under $T_{\ell, \lambda}$.

Conversely, if \mathcal{C} is (ℓ, λ) -QT, then rows of $\mathbf{G}\mathbf{M}^t$ are codewords and

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}^t \end{pmatrix} = k.$$

□

Example 2.8. Let \mathcal{C} be the linear code over \mathbb{F}_4 of length $n = 9$, dimension $k = 6$, and systematic generator matrix

$$(7) \quad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1+\theta & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1+\theta & \theta & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \theta \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & \theta & \theta \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \theta & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1+\theta & 1 & 1+\theta \end{pmatrix},$$

where $\theta^2 + \theta + 1 = 0$. By Theorem 2.7, \mathcal{C} is $(3, \theta)$ -QT code because

$$\text{rank} \begin{pmatrix} G \\ GM^t \end{pmatrix} = \text{rank} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1+\theta & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1+\theta & \theta & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \theta \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & \theta & \theta \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \theta & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1+\theta & 1 & 1+\theta \\ 0 & 1 & \theta & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1+\theta & \theta & 0 & 1 & 0 & 0 & 0 & 0 \\ \theta & 0 & 1+\theta & 0 & 0 & 1 & 0 & 0 & 0 \\ \theta & 1+\theta & 1+\theta & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1+\theta & \theta & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & \theta & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = 6.$$

In fact, \mathcal{C} is optimal because its minimum distance is $d_{\min} = 3$, which is the best known minimum distance for a linear code over \mathbb{F}_4 of length 9 and dimension 6, see [16].

The linear transformation $T_{\ell, \lambda}$ is an automorphism of the vector space $\mathbb{F}_q^{m\ell}$. Define an $\mathbb{F}_q[x]$ -module structure on $\mathbb{F}_q^{m\ell}$ such that the action of x on $\mathbb{F}_q^{m\ell}$ is the action of $T_{\ell, \lambda}$. Specifically, the action of $f(x) = \sum_h f_h x^h \in \mathbb{F}_q[x]$ on $\mathbf{a} \in \mathbb{F}_q^{m\ell}$ is defined by $f(x)\mathbf{a} = \sum_h f_h T_{\ell, \lambda}^h(\mathbf{a})$. Let \mathcal{C} be an (ℓ, λ) -QT code over \mathbb{F}_q of length $m\ell$. Since \mathcal{C} is a $T_{\ell, \lambda}$ -invariant \mathbb{F}_q -subspace of $\mathbb{F}_q^{m\ell}$, it is an $\mathbb{F}_q[x]$ -submodule of $\mathbb{F}_q^{m\ell}$. The opposite is also true; meaning that an $\mathbb{F}_q[x]$ -submodule of $\mathbb{F}_q^{m\ell}$ is an (ℓ, λ) -QT code over \mathbb{F}_q of length $m\ell$. In addition, the following result shows that an (ℓ, λ) -QT code corresponds to an $\mathbb{F}_q[x]$ -submodule of \mathcal{R}_λ^ℓ , where $\mathcal{R}_\lambda = \mathbb{F}_q[x]/\langle x^m - \lambda \rangle$. This correspondence leads to the definition of the polynomial representation of (ℓ, λ) -QT codes.

Theorem 2.9. *There is a one-to-one correspondence between (ℓ, λ) -QT codes over \mathbb{F}_q of length $m\ell$ and $\mathbb{F}_q[x]$ -submodules of \mathcal{R}_λ^ℓ , where $\mathcal{R}_\lambda = \mathbb{F}_q[x]/\langle x^m - \lambda \rangle$.*

Proof. Let $\phi : \mathbb{F}_q^{m\ell} \rightarrow \mathcal{R}_\lambda^\ell$ be the \mathbb{F}_q -vector space isomorphism such that

$$\begin{aligned} \phi : \mathbf{a} &= (a_{0,1}, a_{0,2}, \dots, a_{0,\ell}, a_{1,1}, a_{1,2}, \dots, a_{1,\ell}, \dots, a_{m-1,1}, a_{m-1,2}, \dots, a_{m-1,\ell}) \\ &\mapsto \mathbf{a}(x) = (a_1(x), a_2(x), \dots, a_\ell(x)), \end{aligned}$$

where $a_j(x) = a_{0,j} + a_{1,j}x + a_{2,j}x^2 + \dots + a_{m-1,j}x^{m-1} \in \mathcal{R}_\lambda$ for $1 \leq j \leq \ell$. Consider the following diagram of \mathbb{F}_q -vector space isomorphisms

$$(8) \quad \begin{array}{ccc} \mathbb{F}_q^{m\ell} & \xrightarrow{\phi} & \mathcal{R}_\lambda^\ell \\ T_{\ell,\lambda} \downarrow & & \downarrow \psi \\ \mathbb{F}_q^{m\ell} & \xrightarrow{\phi} & \mathcal{R}_\lambda^\ell \end{array}$$

where $\psi : (a_1(x), a_2(x), \dots, a_\ell(x)) \mapsto (xa_1(x), xa_2(x), \dots, xa_\ell(x))$. Diagram (8) is commutative because

$$\begin{aligned} \phi \circ T_{\ell,\lambda}(\mathbf{a}) &= \phi(\lambda a_{m-1,1}, \lambda a_{m-1,2}, \dots, \lambda a_{m-1,\ell}, a_{0,1}, a_{0,2}, \dots, a_{0,\ell}, \dots, a_{m-2,1}, a_{m-2,2}, \dots, a_{m-2,\ell}) \\ &= (\lambda a_{m-1,1} + a_{0,1}x + a_{1,1}x^2 + \dots + a_{m-2,1}x^{m-1}, \dots, \\ &\quad \lambda a_{m-1,\ell} + a_{0,\ell}x + a_{1,\ell}x^2 + \dots + a_{m-2,\ell}x^{m-1}) \\ &= (a_{m-1,1}x^m + a_{0,1}x + a_{1,1}x^2 + \dots + a_{m-2,1}x^{m-1}, \dots, \\ &\quad a_{m-1,\ell}x^m + a_{0,\ell}x + a_{1,\ell}x^2 + \dots + a_{m-2,\ell}x^{m-1}) \\ &= x(a_{0,1} + a_{1,1}x + \dots + a_{m-1,1}x^{m-1}, \dots, a_{0,\ell} + a_{1,\ell}x + \dots + a_{m-1,\ell}x^{m-1}) \\ &= x\phi(\mathbf{a}) = \psi \circ \phi(\mathbf{a}). \end{aligned}$$

For any $f(x) = \sum_h f_h x^h \in \mathbb{F}_q[x]$, we have

$$f(x)\phi(\mathbf{a}) = \sum_h f_h x^h \phi(\mathbf{a}) = \sum_h f_h \psi^h \circ \phi(\mathbf{a}) = \sum_h f_h \phi \circ T_{\ell,\lambda}^h(\mathbf{a}) = \phi(f(T_{\ell,\lambda})(\mathbf{a})).$$

Then ϕ is an $\mathbb{F}_q[x]$ -module isomorphism, where the module structure of $\mathbb{F}_q^{m\ell}$ is described in the paragraph before Theorem 2.9. This isomorphism determines the correspondence between submodules of \mathcal{R}_λ^ℓ and submodules of $\mathbb{F}_q^{m\ell}$, i.e., (ℓ, λ) -QT codes over \mathbb{F}_q of length $m\ell$. \square

Let \mathcal{C} be an (ℓ, λ) -QT code over \mathbb{F}_q of length $m\ell$. Then \mathcal{C} is an $\mathbb{F}_q[x]$ -submodule of $\mathbb{F}_q^{m\ell}$, and $f(x) \in \mathbb{F}_q[x]$ acts on a codeword $\mathbf{c} \in \mathcal{C}$ by $f(T_{\ell,\lambda})(\mathbf{c})$. Since QT codes generalize the constacyclic codes, we aim to provide a polynomial representation for (ℓ, λ) -QT codes similar to that of cyclic and constacyclic codes. The polynomial representation of an (ℓ, λ) -QT code $\mathcal{C} \subseteq \mathbb{F}_q^{m\ell}$ is $\phi(\mathcal{C})$, its image under the isomorphism defined in the proof of Theorem 2.9.

Specifically, the codeword \mathbf{c} given by (3) is represented by the polynomial vector

$$(9) \quad \begin{aligned} \mathbf{c}(x) = & (c_{0,1} + c_{1,1}x + c_{2,1}x^2 + \cdots + c_{m-1,1}x^{m-1}, \\ & c_{0,2} + c_{1,2}x + c_{2,2}x^2 + \cdots + c_{m-1,2}x^{m-1}, \dots, \\ & c_{0,\ell} + c_{1,\ell}x + c_{2,\ell}x^2 + \cdots + c_{m-1,\ell}x^{m-1}) \in \mathcal{R}_\lambda^\ell. \end{aligned}$$

We do not distinguish between the code and its polynomial representation. That is, an (ℓ, λ) -QT code \mathcal{C} over \mathbb{F}_q of length $m\ell$ is an $\mathbb{F}_q[x]$ -submodule of \mathcal{R}_λ^ℓ . Hence, \mathcal{C} is a torsion $\mathbb{F}_q[x]$ -module [25]. In fact, $(x^m - \lambda)$ annihilates all codewords $\mathbf{c}(x) \in \mathcal{C}$, i.e., $(x^m - \lambda)\mathbf{c}(x) = \mathbf{0}$. Then, the ideal $\langle x^m - \lambda \rangle \subset \mathbb{F}_q[x]$ is in the annihilator of \mathcal{C} . This allows \mathcal{C} to be seen as an \mathcal{R}_λ -module. However, our interest will be in the $\mathbb{F}_q[x]$ -module structure of \mathcal{C} . But more than that, we need to make \mathcal{C} into an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$; the following result leads to this.

Theorem 2.10. *There is a one-to-one correspondence between (ℓ, λ) -QT codes over \mathbb{F}_q of length $m\ell$ and $\mathbb{F}_q[x]$ -submodules of $(\mathbb{F}_q[x])^\ell$ that contain the submodule*

$$M = ((x^m - \lambda)\mathbb{F}_q[x])^\ell.$$

Proof. $(\mathbb{F}_q[x])^\ell$ is a free $\mathbb{F}_q[x]$ -module of rank ℓ and M is the submodule

$$\begin{aligned} M = & \{((x^m - \lambda)f_1(x), (x^m - \lambda)f_2(x), \dots, (x^m - \lambda)f_\ell(x)) \\ & \text{such that } f_j(x) \in \mathbb{F}_q[x] \text{ for } 1 \leq j \leq \ell\}. \end{aligned}$$

Let $\pi : (\mathbb{F}_q[x])^\ell \rightarrow (\mathbb{F}_q[x])^\ell / M$ be the projection homomorphism. Then, π defines a one-to-one correspondence between submodules of $(\mathbb{F}_q[x])^\ell$ that contain M and submodules of $(\mathbb{F}_q[x])^\ell / M$. In addition, let τ be the natural $\mathbb{F}_q[x]$ -module isomorphism between $(\mathbb{F}_q[x])^\ell / M$ and \mathcal{R}_λ^ℓ . Then, τ induces one-to-one correspondence between submodules of \mathcal{R}_λ^ℓ and the submodules of $(\mathbb{F}_q[x])^\ell$ that contain M . The result follows from Theorem 2.9. \square

Theorem 2.9 presents any (ℓ, λ) -QT code \mathcal{C} as an $\mathbb{F}_q[x]$ -submodule of \mathcal{R}_λ^ℓ . While Theorem 2.10 presents \mathcal{C} as an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$. The proof of Theorem 2.10 provides a way to get generators of \mathcal{C} as a submodule of $(\mathbb{F}_q[x])^\ell$ from those generating \mathcal{C} as a submodule of \mathcal{R}_λ^ℓ . Specifically, let \mathcal{C} be generated as a submodule of \mathcal{R}_λ^ℓ by the set

$$\{(g_{i,1}(x) + \langle x^m - \lambda \rangle, g_{i,2}(x) + \langle x^m - \lambda \rangle, \dots, g_{i,\ell}(x) + \langle x^m - \lambda \rangle) \mid 1 \leq i \leq r\},$$

where $g_{i,j}(x) \in \mathbb{F}_q[x]$ for $1 \leq i \leq r$ and $1 \leq j \leq \ell$. Then \mathcal{C} as a submodule of $(\mathbb{F}_q[x])^\ell$ is generated by

$$(10) \quad \begin{aligned} & \{(g_{i,1}(x), g_{i,2}(x), \dots, g_{i,\ell}(x)) \mid 1 \leq i \leq r\} \cup \\ & \{(x^m - \lambda, 0, \dots, 0), (0, x^m - \lambda, 0, \dots, 0), \dots, (0, \dots, 0, x^m - \lambda)\}. \end{aligned}$$

Example 2.11. We continue discussing the $(3, \theta)$ -QT code \mathcal{C} started in Example 2.8. Rows of the generator matrix given by (7) generate \mathcal{C} as an \mathbb{F}_4 -subspace of \mathbb{F}_4^9 . Hence, they generate \mathcal{C} as an $\mathbb{F}_4[x]$ -submodule of \mathbb{F}_4^9 , see the paragraph before Theorem 2.9. The polynomial representations of these rows are their image under the isomorphism ϕ given in the proof of Theorem 2.9; they construct the set

$$\begin{aligned} & \{(1, (1 + \theta)x^2, x^2), ((1 + \theta)x^2, 1 + \theta x^2, x^2), (x^2, 0, 1 + \theta x^2), \\ & (x + x^2, \theta x^2, \theta x^2), (0, x + \theta x^2, x^2), ((1 + \theta)x^2, x^2, x + (1 + \theta)x^2)\} \subset \mathcal{R}_\theta^3. \end{aligned}$$

Since ϕ is an $\mathbb{F}_4[x]$ -module isomorphism, the above set generates \mathcal{C} as an $\mathbb{F}_4[x]$ -submodule of \mathcal{R}_θ^3 . From (10), a generating set for \mathcal{C} as an $\mathbb{F}_4[x]$ -submodule of $(\mathbb{F}_4[x])^3$ is

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

This set is not necessarily a minimal generating set of \mathcal{C} , but we will show later how it can be reduced to a minimal one.

Again, we will not distinguish between an (ℓ, λ) -QT code \mathcal{C} as a $T_{\ell, \lambda}$ -invariant subspace of $\mathbb{F}_q^{m_\ell}$ and the corresponding $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$ that contains M . That is, \mathcal{C} is a linear code over $\mathbb{F}_q[x]$ of length ℓ , where a linear code over a ring R of length ℓ is an R -submodule of R^ℓ . On the other hand, a linear code over $\mathbb{F}_q[x]$ of length ℓ is an (ℓ, λ) -QT code if it contains M . However, we note that the minimum distance, code length, and rank of \mathcal{C} as a linear code over $\mathbb{F}_q[x]$ are different from those of \mathcal{C} as a linear code over \mathbb{F}_q . We aim to find a generator matrix for \mathcal{C} as a linear code over $\mathbb{F}_q[x]$. We call any such matrix a GPM of \mathcal{C} because its entries are polynomials over \mathbb{F}_q . A GPM can be constructed from the generating set given by (10). Since a GPM is a matrix over the PID $\mathbb{F}_q[x]$, one might ask for a unique reduced form GPM. Matrices over PIDs and their reduced form are discussed in Section 3.

We conclude this section by defining the class of MT codes that provides an additional generalization of QT codes. This generalization is based on generalizing the co-index into ℓ block lengths, which are not necessarily equal.

Definition 2.12. Let m_1, m_2, \dots, m_ℓ be positive integers and $\Lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$, where $0 \neq \lambda_j \in \mathbb{F}_q$ for $1 \leq j \leq \ell$. A Λ -MT code over \mathbb{F}_q of code length $n = m_1 + m_2 + \dots + m_\ell$ and block lengths $(m_1, m_2, \dots, m_\ell)$ is an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$ that contains the submodule

$$\begin{aligned} M_\Lambda &= \{(x^{m_1} - \lambda_1)f_1(x), (x^{m_2} - \lambda_2)f_2(x), \dots, (x^{m_\ell} - \lambda_\ell)f_\ell(x)\} \\ &\quad \text{such that } f_j(x) \in \mathbb{F}_q[x] \text{ for } 1 \leq j \leq \ell. \end{aligned}$$

From Theorem 2.10, an (ℓ, λ) -QT code is Λ -MT of equal block lengths and $\Lambda = (\lambda, \lambda, \dots, \lambda)$.

Theorem 2.13. *There is a one-to-one correspondence between $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT codes over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ and T_Λ -invariant \mathbb{F}_q -subspaces of \mathbb{F}_q^n , where $n = m_1 + m_2 + \dots + m_\ell$ and T_Λ is the automorphism of \mathbb{F}_q^n given by*

(11)

$$T_\Lambda : (a_{0,1}, \dots, a_{m_1-1,1}, a_{0,2}, \dots, a_{m_2-1,2}, \dots, a_{0,\ell}, \dots, a_{m_\ell-1,\ell}) \mapsto$$

$$(\lambda_1 a_{m_1-1,1}, a_{0,1}, \dots, a_{m_1-2,1}, \lambda_2 a_{m_2-1,2}, a_{0,2}, \dots, a_{m_2-2,2}, \dots, \lambda_\ell a_{m_\ell-1,\ell}, a_{0,\ell}, \dots, a_{m_\ell-2,\ell}).$$

Proof. For $1 \leq j \leq \ell$, let $\mathcal{R}_{m_j, \lambda_j} = \mathbb{F}_q[x] / \langle x^{m_j} - \lambda_j \rangle$ and $\pi_j : \mathbb{F}_q[x] \rightarrow \mathcal{R}_{m_j, \lambda_j}$ be the projection homomorphism. Then $\pi = \bigoplus_{j=1}^\ell \pi_j : (\mathbb{F}_q[x])^\ell \rightarrow \bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ is a surjective homomorphism with kernel M_Λ . Actually, π defines a one-to-one correspondence between $\mathbb{F}_q[x]$ -submodules of $\bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ and $\mathbb{F}_q[x]$ -submodules of $(\mathbb{F}_q[x])^\ell$ that contain M_Λ given in Definition 2.12. Hence, there is a one-to-one correspondence between $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT codes over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ and submodules of $\bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$.

The automorphism T_Λ makes \mathbb{F}_q^n into an $\mathbb{F}_q[x]$ -module, where the action of x on \mathbb{F}_q^n is the action of T_Λ . In this setting, $\mathbb{F}_q[x]$ -submodules of \mathbb{F}_q^n are precisely the T_Λ -invariant \mathbb{F}_q -subspaces of \mathbb{F}_q^n . We establish a one-to-one correspondence between submodules of $\bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ and T_Λ -invariant \mathbb{F}_q -subspaces of \mathbb{F}_q^n by obtaining an $\mathbb{F}_q[x]$ -module isomorphism between $\bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ and \mathbb{F}_q^n . There is an \mathbb{F}_q -vector space isomorphism $\phi : \mathbb{F}_q^n \rightarrow \bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ given by

$$(12) \quad (a_{0,1}, \dots, a_{m_1-1,1}, \dots, a_{0,\ell}, \dots, a_{m_\ell-1,\ell}) \mapsto (a_1(x), a_2(x), \dots, a_\ell(x)),$$

where $a_j(x) = a_{0,j} + a_{1,j}x + \dots + a_{m_j-1,j}x^{m_j-1}$ for $1 \leq j \leq \ell$. Consider the following diagram of \mathbb{F}_q -vector space isomorphisms

$$(13) \quad \begin{array}{ccc} \mathbb{F}_q^n & \xrightarrow{\phi} & \bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j} \\ T_\Lambda \downarrow & & \downarrow \psi \\ \mathbb{F}_q^n & \xrightarrow{\phi} & \bigoplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j} \end{array}$$

where $\psi : (a_1(x), a_2(x), \dots, a_\ell(x)) \mapsto (xa_1(x), xa_2(x), \dots, xa_\ell(x))$. From Equation (11), Diagram (13) is commutative. To see this, we have for any $\mathbf{a} \in \mathbb{F}_q^n$

$$\begin{aligned} \psi(\phi(\mathbf{a})) &= x\phi(\mathbf{a}) = x\phi(a_{0,1}, \dots, a_{m_1-1,1}, \dots, a_{0,\ell}, \dots, a_{m_\ell-1,\ell}) = x(a_1(x), a_2(x), \dots, a_\ell(x)) \\ &= (xa_1(x), xa_2(x), \dots, xa_\ell(x)) = \phi(T_\Lambda(\mathbf{a})). \end{aligned}$$

Therefore, ϕ is an $\mathbb{F}_q[x]$ -module isomorphism.

If \mathcal{C} is a $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$, then $\phi^{-1} \circ \pi(\mathcal{C})$ is a T_Λ -invariant \mathbb{F}_q -subspace of \mathbb{F}_q^n . Conversely, the image of any T_Λ -invariant \mathbb{F}_q -subspace of \mathbb{F}_q^n under the map $\pi^{-1} \circ \phi$ is an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$ that contains M_Λ . \square

In literature, an MT code may mean a T_Λ -invariant subspace of \mathbb{F}_q^n , a submodule of $\oplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$, or a submodule of $(\mathbb{F}_q[x])^\ell$ that contains M_Λ . We do not distinguish between the three representations, and the representation used is determined by context. However, the polynomial representation of an MT code is the corresponding submodule of $\oplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$.

Similar to what we did with QT codes, if a Λ -MT code \mathcal{C} is generated as a submodule of $\oplus_{j=1}^\ell \mathcal{R}_{m_j, \lambda_j}$ by the set

$$\{(g_{i,1}(x) + \langle x^{m_1} - \lambda_1 \rangle, g_{i,2}(x) + \langle x^{m_2} - \lambda_2 \rangle, \dots, g_{i,\ell}(x) + \langle x^{m_\ell} - \lambda_\ell \rangle) \mid 1 \leq i \leq r\},$$

where $g_{i,j}(x) \in \mathbb{F}_q[x]$ for $1 \leq i \leq r$ and $1 \leq j \leq \ell$, then \mathcal{C} is generated as a submodule of $(\mathbb{F}_q[x])^\ell$ by the set

$$\{(g_{i,1}(x), g_{i,2}(x), \dots, g_{i,\ell}(x)) \mid 1 \leq i \leq r\} \cup \{(x^{m_1} - \lambda_1, 0, \dots, 0), (0, x^{m_2} - \lambda_2, 0, \dots, 0), \dots, (0, \dots, 0, x^{m_\ell} - \lambda_\ell)\}.$$

Hence, \mathcal{C} is a linear code over $\mathbb{F}_q[x]$ of length ℓ with generator matrix

$$\mathbf{G} = \begin{pmatrix} g_{1,1}(x) & g_{1,2}(x) & g_{1,3}(x) & \cdots & g_{1,\ell}(x) \\ g_{2,1}(x) & g_{2,2}(x) & g_{2,3}(x) & \cdots & g_{2,\ell}(x) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{r,1}(x) & g_{r,2}(x) & g_{r,3}(x) & \cdots & g_{r,\ell}(x) \\ x^{m_1} - \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & x^{m_2} - \lambda_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & x^{m_\ell} - \lambda_\ell \end{pmatrix}.$$

Since the entries of \mathbf{G} are polynomials, so it is called GPM. Rows of \mathbf{G} are not necessary to form a minimal generating set for \mathcal{C} . However, a reduced form for \mathbf{G} can be obtained, see the next section.

In the standard basis of \mathbb{F}_q^n , the matrix representation of T_Λ is the block diagonal matrix

$$(14) \quad \mathbf{M}_\Lambda = \text{diag}[\mathbf{M}_{\lambda_1, m_1}, \mathbf{M}_{\lambda_2, m_2}, \dots, \mathbf{M}_{\lambda_\ell, m_\ell}],$$

where

$$\mathbf{M}_{\lambda_j, m_j} = \begin{pmatrix} \mathbf{0}_{1 \times (m_j-1)} & \lambda_j \\ \mathbf{I}_{(m_j-1)} & \mathbf{0}_{(m_j-1) \times 1} \end{pmatrix} \text{ for } 1 \leq j \leq \ell.$$

Although the following result can be proven in a similar way to the proof of Theorem 2.7, we will present another proof.

Theorem 2.14. Let \mathcal{C} be a linear code over \mathbb{F}_q of length n , dimension k , and a $k \times n$ generator matrix \mathbf{G} . Then, \mathcal{C} is $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT with block lengths $(m_1, m_2, \dots, m_\ell)$ if and only if

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}_\Lambda^t \end{pmatrix} = k.$$

Proof. Assume \mathcal{C} is $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT with block lengths $(m_1, m_2, \dots, m_\ell)$. Then the rows of $\mathbf{G}\mathbf{M}_\Lambda^t$ are codewords in \mathcal{C} , which means that $\mathbf{G}\mathbf{M}_\Lambda^t = \mathbf{N}\mathbf{G}$ for some $k \times k$ matrix \mathbf{N} . Thus

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}_\Lambda^t \end{pmatrix} = \text{rank}(\mathbf{G}) = k.$$

Conversely, if

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}_\Lambda^t \end{pmatrix} = k,$$

and since $\text{rank}(\mathbf{G}) = k$, there exists a $k \times k$ matrix \mathbf{N} such that $\mathbf{G}\mathbf{M}_\Lambda^t = \mathbf{N}\mathbf{G}$. Applying the linear transformation T_Λ to the codeword $\mathbf{a}\mathbf{G}$ yields $\mathbf{a}\mathbf{G}\mathbf{M}_\Lambda^t = \mathbf{a}\mathbf{N}\mathbf{G} = \mathbf{a}'\mathbf{G}$, which is again a codeword. Hence, \mathcal{C} is $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT. \square

Example 2.15. Let \mathcal{C} be the linear code over \mathbb{F}_3 of length 60, dimension 6, and generator matrix $\mathbf{G} = \begin{pmatrix} \mathbf{I}_6 & \mathbf{N} \end{pmatrix}$, where \mathbf{N} is given by

$$\begin{pmatrix} 1 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 0 & 2 & 1 & 2 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 1 & 2 & 2 & 0 & 2 & 2 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & 2 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 & 0 & 0 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 0 \\ 1 & 0 & 1 & 2 & 2 & 2 & 0 & 0 & 2 & 1 & 0 & 2 & 0 & 0 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 & 2 & 2 & 0 & 0 & 2 & 1 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 & 0 & 0 & 2 & 1 & 0 & 2 & 1 & 2 & 1 & 2 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 2 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 0 & 2 & 1 \\ 2 & 1 & 2 & 2 & 1 & 0 & 2 & 0 & 2 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 1 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 2 & 0 & 1 & 0 & 1 & 1 & 2 & 2 & 0 & 2 & 2 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 2 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}.$$

By brute-force, the minimum distance of \mathcal{C} is 36, hence \mathcal{C} is optimal according to [16]. Furthermore, Theorem 2.14 emphasizes that \mathcal{C} is $(2, 1)$ -MT with block lengths $m_1 = 20$ and $m_2 = 40$ because

$$\text{rank} \begin{pmatrix} \mathbf{G} \\ \mathbf{G}\mathbf{M}_\Lambda^t \end{pmatrix} = 6.$$

A generating set S for \mathcal{C} as an $\mathbb{F}_3[x]$ -submodule of $\mathcal{R}_{20,2} \oplus \mathcal{R}_{40,1}$ can be obtained from the polynomial representations of rows of \mathbf{G} . Namely,

$$\begin{aligned}
S = \Big\{ & (1 + x^6 + 2x^7 + x^8 + 2x^9 + 2x^{10} + x^{11} + 2x^{13} + 2x^{15} + x^{16} + 2x^{17} + x^{19}, \\
& 1 + x^2 + x^3 + 2x^5 + 2x^7 + 2x^{10} + 2x^{11} + 2x^{13} + x^{15} + x^{17} + x^{18} + 2x^{19} + 2x^{20} \\
& + 2x^{22} + 2x^{23} + x^{25} + x^{27} + x^{30} + x^{31} + x^{33} + 2x^{35} + 2x^{37} + 2x^{38} + x^{39}), \\
& (x + x^6 + x^{10} + x^{12} + 2x^{13} + 2x^{14} + 2x^{15} + 2x^{18} + x^{19}, \\
& 2 + x + x^2 + 2x^3 + x^4 + 2x^5 + 2x^6 + 2x^7 + 2x^8 + 2x^{10} + x^{11} + 2x^{12} + 2x^{13} \\
& + 2x^{14} + x^{15} + x^{16} + x^{17} + 2x^{18} + x^{20} + 2x^{21} + 2x^{22} + x^{23} + 2x^{24} + x^{25} + x^{26} \\
& + x^{27} + x^{28} + x^{30} + 2x^{31} + x^{32} + x^{33} + x^{34} + 2x^{35} + 2x^{36} + 2x^{37} + x^{38}), \\
& (x^2 + x^6 + x^8 + 2x^9 + 2x^{10} + 2x^{11} + 2x^{14} + x^{15} + 2x^{17}, \\
& 1 + 2x + 2x^2 + 2x^3 + 2x^4 + 2x^6 + x^7 + 2x^8 + 2x^9 + 2x^{10} + x^{11} + x^{12} + x^{13} \\
& + 2x^{14} + x^{16} + 2x^{17} + 2x^{18} + x^{19} + 2x^{20} + x^{21} + x^{22} + x^{23} + x^{24} + x^{26} + 2x^{27} \\
& + x^{28} + x^{29} + x^{30} + 2x^{31} + 2x^{32} + 2x^{33} + x^{34} + 2x^{36} + x^{37} + x^{38} + 2x^{39}), \\
& (x^3 + x^7 + x^9 + 2x^{10} + 2x^{11} + 2x^{12} + 2x^{15} + x^{16} + 2x^{18}, \\
& 2 + x + 2x^2 + 2x^3 + 2x^4 + 2x^5 + 2x^7 + x^8 + 2x^9 + 2x^{10} + 2x^{11} + x^{12} + x^{13} \\
& + x^{14} + 2x^{15} + x^{17} + 2x^{18} + 2x^{19} + x^{20} + 2x^{21} + x^{22} + x^{23} + x^{24} + x^{25} + x^{27} \\
& + 2x^{28} + x^{29} + x^{30} + x^{31} + 2x^{32} + 2x^{33} + 2x^{34} + x^{35} + 2x^{37} + x^{38} + x^{39}), \\
& (x^4 + x^8 + x^{10} + 2x^{11} + 2x^{12} + 2x^{13} + 2x^{16} + x^{17} + 2x^{19}, \\
& 1 + 2x + x^2 + 2x^3 + 2x^4 + 2x^5 + 2x^6 + 2x^8 + x^9 + 2x^{10} + 2x^{11} + 2x^{12} + x^{13} \\
& + x^{14} + x^{15} + 2x^{16} + x^{18} + 2x^{19} + 2x^{20} + x^{21} + 2x^{22} + x^{23} + x^{24} + x^{25} + x^{26} \\
& + x^{28} + 2x^{29} + x^{30} + x^{31} + x^{32} + 2x^{33} + 2x^{34} + 2x^{35} + x^{36} + 2x^{38} + x^{39}), \\
& (x^5 + 2x^6 + x^7 + 2x^8 + 2x^9 + x^{10} + 2x^{12} + 2x^{14} + x^{15} + 2x^{16} + x^{18} + 2x^{19}, \\
& x + x^2 + 2x^4 + 2x^6 + 2x^9 + 2x^{10} + 2x^{12} + x^{14} + x^{16} + x^{17} + 2x^{18} + 2x^{19} + 2x^{21} \\
& + 2x^{22} + x^{24} + x^{26} + x^{29} + x^{30} + x^{32} + 2x^{34} + 2x^{36} + 2x^{37} + x^{38} + x^{39}) \Big\}.
\end{aligned}$$

However, as an $\mathbb{F}_3[x]$ -submodule of $(\mathbb{F}_3[x])^2$, \mathcal{C} is generated by

$$(15) \quad S \cup \{(x^{20} + 1, 0), (0, x^{40} + 2)\}.$$

As a linear code over $\mathbb{F}_3[x]$, a GPM for \mathcal{C} can be constructed from the latter set. In Section 3, we will discuss how to reduce this generating set to a minimal set, see Example 3.9 below.

GQC codes form a subclass of MT codes; an ℓ -GQC code of block lengths $(m_1, m_2, \dots, m_\ell)$ is $(1, 1, \dots, 1)$ -MT. The following is a corollary of Theorem 2.13.

Corollary 2.16. *Any of the following can be used to represent an ℓ -GQC code of block lengths $(m_1, m_2, \dots, m_\ell)$ over \mathbb{F}_q :*

(a) *An $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$ that contains*

$$\{((x^{m_1} - 1)f_1(x), (x^{m_2} - 1)f_2(x), \dots, (x^{m_\ell} - 1)f_\ell(x)) \mid f_1(x), \dots, f_\ell(x) \in \mathbb{F}_q[x]\}.$$

Hence, an ℓ -GQC is a linear code over $\mathbb{F}_q[x]$ of length ℓ .

(b) *An $\mathbb{F}_q[x]$ -submodule of $\bigoplus_{j=1}^\ell \mathcal{R}_{m_j,1}$, where $\mathcal{R}_{m_j,1} = \mathbb{F}_q[x]/\langle x^{m_j} - 1 \rangle$.*

(c) *An invariant \mathbb{F}_q -subspace of \mathbb{F}_q^n , where $n = \sum_{j=1}^\ell m_j$, under the automorphism*

$$(a_{0,1}, \dots, a_{m_1-1,1}, a_{0,2}, \dots, a_{m_2-1,2}, \dots, a_{0,\ell}, \dots, a_{m_\ell-1,\ell}) \mapsto (a_{m_1-1,1}, a_{0,1}, \dots, a_{m_1-2,1}, \dots, a_{m_\ell-1,\ell}, a_{0,\ell}, \dots, a_{m_\ell-2,\ell}).$$

In the standard basis of \mathbb{F}_q^n and using (14) with $\lambda_j = 1$ for $1 \leq j \leq \ell$, the matrix representation of the automorphism given in Corollary 2.16 is

$$\mathbf{M}_1 = \text{diag}[\mathbf{M}_{1,m_1}, \mathbf{M}_{1,m_2}, \dots, \mathbf{M}_{1,m_\ell}].$$

For $1 \leq j \leq \ell$, \mathbf{M}_{1,m_j} is a permutation matrix of size m_j . In addition, \mathbf{M}_{1,m_j} has multiplicative order m_j , i.e., $\mathbf{M}_{1,m_j}^{m_j} = \mathbf{I}_{m_j}$. Consequently, \mathbf{M}_1 is a permutation matrix with multiplicative order $N = \text{lcm}(m_1, m_2, \dots, m_\ell)$, the least common multiple of m_1, m_2, \dots, m_ℓ . This can be generalized to the matrix \mathbf{M}_Λ given by (14); the multiplicative order of \mathbf{M}_Λ is $\text{lcm}(t_1 m_1, t_2 m_2, \dots, t_\ell m_\ell)$, where t_j is the multiplicative order of λ_j for $1 \leq j \leq \ell$. Equivalently, $T_\Lambda^{\text{lcm}(t_1 m_1, t_2 m_2, \dots, t_\ell m_\ell)}$ is the identity map.

3. GPMS AS MATRICES OVER PID

Let R be a commutative ring with identity and \mathcal{M} be a finitely generated R -module. The rank of \mathcal{M} is the size of the minimal generating set of \mathcal{M} . An R -module \mathcal{M} is free if there exists an R -linearly independent generating set $\{\nu_1, \nu_2, \dots, \nu_r\}$ for \mathcal{M} . The set $\{\nu_1, \nu_2, \dots, \nu_r\}$ forms a basis for \mathcal{M} . That is, for each $m \in \mathcal{M}$, there is a unique $(a_1, a_2, \dots, a_r) \in R^r$ such that $m = \sum_{i=1}^r a_i \nu_i$. The “invariant basis number” property for commutative rings asserts that any two bases of \mathcal{M} have the same cardinality, and that a basis forms a minimal generating set. Hence, if $\{\nu_1, \nu_2, \dots, \nu_r\}$ is a basis of an R -module \mathcal{M} , then \mathcal{M} is isomorphic to R^r and has rank r . The free R -module R^r of rank r has the standard basis $\{e_1, e_2, \dots, e_r\}$, where e_i is the vector that has 1 in the i^{th} coordinate and zeros in the remaining coordinates. Many

interesting properties of modules over PID can be found in [25]. In the following, we assume R PID. The reason for the interest in modules over PIDs is that many of the known results of vector spaces still apply to these modules. We summarize some of these properties without proof.

Theorem 3.1. [25] *Let \mathcal{M} be a finitely generated R -module, where R is PID.*

- (a) *If \mathcal{M} is free of rank r , then \mathcal{M} is torsion-free. That is, $am = 0$ for $a \in R$ and $m \in \mathcal{M}$ if and only if $a = 0$ or $m = 0$. This is easy to see since \mathcal{M} is isomorphic to R^r . Thus, if $am = 0$ for $a \neq 0$, then $a(a_1, a_2, \dots, a_r) = \mathbf{0}$, where $(a_1, a_2, \dots, a_r) \in R^r$ is the image of m under the isomorphism $\mathcal{M} \simeq R^r$. Since R is an integral domain, $aa_i = 0$ and $a_i = 0$ for every $1 \leq i \leq r$. Hence $(a_1, a_2, \dots, a_r) = \mathbf{0}$ and $m = 0$.*
- (b) *If \mathcal{M} is torsion-free, then \mathcal{M} is free.*
- (c) *If \mathcal{N} is a submodule of \mathcal{M} , then $\text{rank}(\mathcal{N}) \leq \text{rank}(\mathcal{M})$.*
- (d) *If \mathcal{M} is free and \mathcal{N} is a submodule, then \mathcal{N} is free.*
- (e) *Similar to vector spaces, if \mathcal{M} is free of rank r , then any generating set of size r forms a basis of \mathcal{M} . On the other hand, unlike vector spaces, if \mathcal{M} is free of rank r , then an R -linearly independent set of size r does not necessarily generate \mathcal{M} . For instance, let $R = \mathbb{Z}$, $\mathcal{M} = \mathbb{Z}^2$, and $S = \{e_1, 2e_2\}$. Although S is \mathbb{Z} -linearly independent of size 2, it does not generate $(0, 1)$, i.e., $\langle S \rangle \neq \mathcal{M}$.*
- (f) *Let \mathcal{M} be free of rank r and let \mathcal{N} be a submodule of rank t . There is a subset $\{\tau_1, \tau_2, \dots, \tau_t\}$ of some basis $\{\nu_1, \nu_2, \dots, \nu_r\}$ of \mathcal{M} and elements $s_1, s_2, \dots, s_t \in R$ such that*
 - (a) $s_1 | s_2 | s_3 | \dots | s_t$, and
 - (b) $\{s_1\tau_1, s_2\tau_2, \dots, s_t\tau_t\}$ is a basis of \mathcal{N} .

The elements s_1, s_2, \dots, s_t are called the invariant factors of \mathcal{N} and are independent of the choice of basis of \mathcal{M} .

Throughout this section, let \mathcal{C} refer to a Λ -MT code over \mathbb{F}_q with block lengths $(m_1, m_2, \dots, m_\ell)$, where $\Lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$. From Definition 2.12, \mathcal{C} is a submodule of a free module of rank ℓ over a PID. Hence, Theorem 3.1 asserts that \mathcal{C} is a free $\mathbb{F}_q[x]$ -module of rank at most ℓ . We aim to find a basis of \mathcal{C} in a reduced form. A generating set of \mathcal{C} as a submodule of $(\mathbb{F}_q[x])^\ell$ can be obtained from any generator matrix of \mathcal{C} as a linear code over \mathbb{F}_q , see Example 2.15. This generating set can be reduced to a basis of \mathcal{C} using the Hermite normal form of matrices over PIDs. More generally, suppose that R is a PID and that \mathcal{M} is an R -submodule of R^ℓ . From Theorem 3.1, \mathcal{M} is a finitely generated free module. Suppose that $S = \{\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_r\} \subseteq \mathcal{M}$ is a generating set of \mathcal{M} , where $\mathbf{g}_i = (g_{i,1}, g_{i,2}, \dots, g_{i,\ell}) \in R^\ell$

for $1 \leq i \leq r$. An $r \times \ell$ generator matrix for \mathcal{M} is constructed as follows:

$$(16) \quad \mathbf{G} = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,\ell} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,\ell} \\ \vdots & \vdots & \ddots & \vdots \\ g_{r,1} & g_{r,2} & \cdots & g_{r,\ell} \end{pmatrix}.$$

Let $\phi : R^r \rightarrow \mathcal{M}$ be the R -module homomorphism defined by $\phi(\mathbf{a}) = \mathbf{a}\mathbf{G}$ for every $\mathbf{a} \in R^r$. Since S generates \mathcal{M} , ϕ is surjective. Suppose that \mathcal{N} is a submodule of R^r that has a generator matrix \mathbf{G}' of size $t \times \ell$. On the one hand, \mathcal{N} is a submodule of \mathcal{M} if and only if $\mathbf{G}' = \mathbf{N}\mathbf{G}$ for some matrix \mathbf{N} over R of size $t \times r$. On the other hand, if $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for an invertible matrix \mathbf{U} , then $\mathcal{M} = \mathcal{N}$, because $\mathbf{G}' = \mathbf{U}\mathbf{G}$ implies $\mathcal{N} \subseteq \mathcal{M}$, while $\mathbf{G} = \mathbf{U}^{-1}\mathbf{G}'$ implies $\mathcal{M} \subseteq \mathcal{N}$.

Definition 3.2. Let \mathbf{G} and \mathbf{G}' be two matrices over R of the same size. We say that \mathbf{G} and \mathbf{G}' are left equivalent if $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for some invertible matrix \mathbf{U} . Thus, two left equivalent matrices over R generate the same R -module.

An Euclidean domain is an integral domain in which we can perform Euclidean division. Examples of Euclidean domains include \mathbb{Z} , $\mathbb{F}_q[x]$, and the ring of formal power series over any field. Every ideal in a Euclidean domain is generated by a single element, so Euclidean domains are automatically PIDs. A matrix over a Euclidean domain is invertible if and only if it is a product of elementary matrices, where an elementary matrix is the identity matrix after performing one elementary row operation. In addition, left and right multiplications by elementary matrices correspond to performing elementary row and column operations, respectively. Thus, for matrices over a Euclidean domain, a left equivalent matrix can be obtained by elementary row operations. Furthermore, for a module \mathcal{M} over a Euclidean domain with a generator matrix \mathbf{G} , applying some elementary row operations to \mathbf{G} results in a left equivalent matrix, the latter being a generator matrix for \mathcal{M} as well. We will be interested in the case where \mathcal{M} is an MT code over \mathbb{F}_q , hence $R = \mathbb{F}_q[x]$ and \mathbf{G} is a GPM.

Theorem 3.3. Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ that has an $\ell \times \ell$ GPM \mathbf{G} . As an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$, \mathcal{C} is free of rank ℓ . Moreover, rows of \mathbf{G} form a basis for \mathcal{C} .

Proof. We know that $(\mathbb{F}_q[x])^\ell$ is a free module of rank ℓ over a PID. From Theorem 3.1, \mathcal{C} is free of rank $\leq \ell$. The submodule M_Λ given in Definition 2.12 is free of rank ℓ ; M_Λ has the basis $\{(x^{m_j} - \lambda_j)\mathbf{e}_j\}_{j=1}^\ell$. Then $\text{rank}(\mathcal{C}) \geq \ell$ because $\mathcal{C} \supseteq M_\Lambda$. Thus, \mathcal{C} is free of rank ℓ . Rows of \mathbf{G} form a generating set for \mathcal{C} of size equal to the rank, and thus form a basis by Theorem 3.1. \square

Theorem 3.4. *Let \mathcal{C} and \mathcal{C}' be two Λ -MT codes of block lengths $(m_1, m_2, \dots, m_\ell)$ with $\ell \times \ell$ GPMs \mathbf{G} and \mathbf{G}' , respectively. Then, $\mathcal{C}' \subseteq \mathcal{C}$ if and only if $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for some matrix \mathbf{U} , where \mathbf{U} is invertible if and only if $\mathcal{C}' = \mathcal{C}$.*

Proof. We have $\mathcal{C}' \subseteq \mathcal{C}$ if and only if \mathbf{G} generates the rows of \mathbf{G}' if and only if $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for some matrix \mathbf{U} .

Assume $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for an invertible \mathbf{U} . Then $\mathcal{C}' \subseteq \mathcal{C}$, and $\mathcal{C} \subseteq \mathcal{C}'$ because $\mathbf{G} = \mathbf{U}^{-1}\mathbf{G}'$, hence $\mathcal{C}' = \mathcal{C}$. Conversely, assume that $\mathcal{C}' = \mathcal{C}$. From the first part of this theorem, there is a matrix \mathbf{V} such that $\mathbf{G} = \mathbf{V}\mathbf{G}'$. Now $\mathbf{G}' = \mathbf{U}\mathbf{G} = \mathbf{U}\mathbf{V}\mathbf{G}'$. That is, $(\mathbf{U}\mathbf{V} - \mathbf{I}_\ell)\mathbf{G}' = \mathbf{0}$. From Theorem 3.3, rows of \mathbf{G}' form a basis for \mathcal{C} , hence $\mathbf{U}\mathbf{V} - \mathbf{I}_\ell = \mathbf{0}$. Then \mathbf{U} is invertible. \square

Theorem 3.5. *Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ that has an $\ell \times \ell$ GPM \mathbf{G} . An $\ell \times \ell$ matrix \mathbf{G}' is a GPM of \mathcal{C} if and only if \mathbf{G} and \mathbf{G}' are left equivalent.*

Proof. Let \mathcal{C}' be the $\mathbb{F}_q[x]$ -module generated by \mathbf{G}' . From Theorem 3.4, $\mathcal{C}' = \mathcal{C}$ if and only if $\mathbf{G}' = \mathbf{U}\mathbf{G}$ for an invertible matrix \mathbf{U} if and only if \mathbf{G} and \mathbf{G}' are left equivalent. \square

From the discussion before Theorem 3.3 and the fact that $\mathbb{F}_q[x]$ is a PID, the following is proven.

Corollary 3.6. *Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ that has an $\ell \times \ell$ GPM \mathbf{G} . An $\ell \times \ell$ matrix \mathbf{G}' is a GPM of \mathcal{C} if and only if \mathbf{G}' can be obtained from \mathbf{G} by elementary row operations.*

In the representation of Λ -MT codes by $\mathbb{F}_q[x]$ -submodules of $(\mathbb{F}_q[x])^\ell$ containing M_Λ , the zero code is represented by M_Λ . However, M_Λ is a free module with basis $\{(x^{m_j} - \lambda_j)\mathbf{e}_j\}_{j=1}^\ell$. Hence, a GPM for M_Λ is the diagonal matrix

$$\mathbf{D} = \text{diag}[x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \dots, x^{m_\ell} - \lambda_\ell] = \begin{pmatrix} x^{m_1} - \lambda_1 & 0 & \dots & 0 \\ 0 & x^{m_2} - \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & x^{m_\ell} - \lambda_\ell \end{pmatrix}.$$

For any Λ -MT code \mathcal{C} with a GPM \mathbf{G} , the \mathbb{F}_q -linearity of \mathcal{C} indicates that it contains the zero code. Then from Theorem 3.4, there is a matrix \mathbf{A} such that

$$(17) \quad \mathbf{A}\mathbf{G} = \mathbf{D}.$$

Equation (17) is called the identical equation [24]. In particular, if \mathcal{C} is (ℓ, λ) -QT, then \mathbf{A} and \mathbf{G} commute.

Theorem 3.7. *Let \mathcal{C} be an (ℓ, λ) -QT code with a GPM \mathbf{G} that satisfies (17) by the matrix \mathbf{A} . Then $\mathbf{GA} = \mathbf{D}$.*

Proof. Assume $\mathbf{GA} = \mathbf{B}$. Then $\mathbf{BG} = \mathbf{GAG} = \mathbf{GD} = (x^m - \lambda)\mathbf{G} = \mathbf{DG}$. That is, $(\mathbf{B} - \mathbf{D})\mathbf{G} = \mathbf{0}$. Since rows of \mathbf{G} are $\mathbb{F}_q[x]$ -linearly independent, $(\mathbf{B} - \mathbf{D}) = \mathbf{0}$ and $\mathbf{B} = \mathbf{D}$. \square

The matrix \mathbf{A} plays a fundamental role in constructing a GPM for the dual code of an MT code. An $\ell \times \ell$ polynomial matrix over $\mathbb{F}_q[x]$ is GPM of a $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT code if and only if it satisfies the identical equation. Let us fix ℓ , Λ , and the block lengths $(m_1, m_2, \dots, m_\ell)$. Set

$$\mathcal{S} = \{\mathbf{G}_i \mid \exists \mathbf{A}_i \text{ such that } \mathbf{A}_i \mathbf{G}_i = \mathbf{D}\},$$

the set of all the $\ell \times \ell$ matrices that satisfy the identical equation. Then for any Λ -MT code with a GPM \mathbf{G} , we have $\mathbf{G} \in \mathcal{S}$. However, each $\mathbf{G} \in \mathcal{S}$ is a GPM for some Λ -MT code. We partition \mathcal{S} with an equivalence relation \sim defined by the left equivalence of matrices. That is, every pair $(\mathbf{G}_i, \mathbf{G}_j)$ of elements in \mathcal{S} is equivalent, written $\mathbf{G}_i \sim \mathbf{G}_j$, if and only if $\mathbf{G}_i = \mathbf{U}\mathbf{G}_j$ for an invertible \mathbf{U} . The quotient \mathcal{S}/\sim is the set of all equivalence classes of \mathcal{S} by \sim . Theorem 3.5 shows a one-to-one correspondence between the set of all Λ -MT codes and \mathcal{S}/\sim . Our next goal is to find a unique simple representative for each equivalence class that can be obtained in an algorithmic way. The representative of each equivalence class is called the reduced GPM of the corresponding Λ -MT code. GPMs are matrices over the Euclidean domain $\mathbb{F}_q[x]$, hence the Hermite normal form of left equivalent matrices over a PID is an intuitive representation to use. In addition, a matrix over a PID is left equivalent to a unique Hermite normal form [13].

Two elements r_1 and r_2 in a PID R are associate if there is a unit $u \in R$ such that $r_1 = ur_2$. A complete set of non-associates of R is a set \mathcal{P} such that for every $r \in R$, there exists a unique $a \in \mathcal{P}$ associate of r . Examples of a complete set of non-associates include

- (a) $\mathcal{P} = \{0, 1, 2, 3, \dots\}$ for $R = \mathbb{Z}$,
- (b) \mathcal{P} is the set of all monic polynomials over \mathbb{F}_q for $R = \mathbb{F}_q[x]$, and
- (c) $\mathcal{P} = \{x^i + x^{i+1}f(x) \mid f(x) \in R \text{ and } i \geq 0\}$ for $R = \mathbb{F}[[x]]$, the ring of formal power series in x over the field \mathbb{F} .

If R is a PID with a complete set of non-associates \mathcal{P} , then there is a one-to-one correspondence between the set of ideals of R and \mathcal{P} . Specifically, the ideal $\langle r \rangle \subseteq R$ corresponds to the unique associate element of r in \mathcal{P} . For every $a \in \mathcal{P}$, let $\mathcal{Q}(a) \subseteq R$ be a complete set of coset representatives of the quotient ring $R/\langle a \rangle$. That is, for each $b + \langle a \rangle \in R/\langle a \rangle$, there is a unique $c \in \mathcal{Q}(a)$ such that $c - b \in \langle a \rangle$. Continuing the above examples, we have

- (a) $\mathcal{Q}(a) = \{0, 1, 2, \dots, a-1\}$ for $R = \mathbb{Z}$,

- (b) $\mathcal{Q}(a)$ is the set of all polynomials over \mathbb{F}_q of degree less than that of a , and
- (c) $\mathcal{Q}(a) = \{a_0 + a_1x + \cdots + a_{i-1}x^{i-1} \mid a_0, a_1, \dots, a_{i-1} \in \mathbb{F}\}$ for $R = \mathbb{F}[[x]]$ and a is an element of \mathcal{P} in which the leading term is x^i .

Definition 3.8. Let R be a PID, let \mathcal{P} be a complete set of non-associates of R , and let $\mathcal{Q}(a)$ be a complete set of coset representatives for every $a \in \mathcal{P}$. A matrix $\mathbf{G} = [g_{i,j}]$ over R of size $h \times \ell$ and rank r is in Hermite normal form if the i^{th} row of \mathbf{G} is zero for $r < i \leq h$ and there is a sequence $1 \leq j_1 < j_2 < j_3 < \cdots < j_r \leq \ell$ such that for every $1 \leq i \leq r$

- (a) $0 \neq g_{i,j_i} \in \mathcal{P}$,
- (b) $g_{i,t} = 0$ for all $1 \leq t < j_i$, and
- (c) $g_{t,j_i} \in \mathcal{Q}(g_{i,j_i})$ for all $1 \leq t < i$.

As a typical example, for $R = \mathbb{Z}$, $\mathcal{P} = \{0, 1, 2, \dots\}$, and $\mathcal{Q}(a) = \{0, 1, 2, \dots, a-1\}$, the matrix

$$\begin{pmatrix} 0 & 3 & -5 & 4 & 10 & 0 & 0 \\ 0 & 0 & 0 & 7 & -1 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

is in Hermite normal form. The Hermite normal form of any matrix \mathbf{G} over a PID is the unique matrix that has the form described in Definition 3.8 and is left equivalent to \mathbf{G} . The Hermite normal form is unique as long as we fix a complete set of non-associates \mathcal{P} and a complete set of coset representatives for each element of \mathcal{P} . In literature, the Hermite normal form is the known reduced row echelon form when R is a field. When R is a Euclidean domain, the Hermite normal form can be obtained by applying elementary row operations.

Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q and let S be a generating set for \mathcal{C} as an $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$. From (16), S can be used to construct a GPM for \mathcal{C} of size $|S| \times \ell$. From now on, we shall use \mathbf{G} to refer to the Hermite normal form of any GPM of \mathcal{C} (see Theorem 3.5), and we call \mathbf{G} the reduced GPM of \mathcal{C} . From Theorem 3.3, \mathcal{C} and \mathbf{G} are of rank ℓ . Hence, \mathbf{G} is an $\ell \times \ell$ matrix of rank ℓ in Hermite normal form. Then Definition 3.8 shows that \mathbf{G} is an upper triangular matrix having diagonal entries as non-zero monic polynomials. Let $\mathbf{A} = [a_{i,j}]$ be the matrix that satisfies the identical equation (17) of \mathbf{G} . Actually, \mathbf{A} is upper triangular because R is an integral domain and \mathbf{G} and \mathbf{D} are upper triangular matrices. Now, the identical equation shows that $a_{i,i}g_{i,i} = x^{m_i} - \lambda_i$ for $1 \leq i \leq \ell$. That is, the i^{th} diagonal entry $g_{i,i}$ of \mathbf{G} divides $(x^{m_i} - \lambda_i)$ for $1 \leq i \leq \ell$.

Example 3.9. We continue with the $(2, 1)$ -MT code \mathcal{C} given in Example 2.15. We have shown that \mathcal{C} as an $\mathbb{F}_3[x]$ submodule of $(\mathbb{F}_3[x])^2$ is generated from the set given by (15). In (16), we showed how such a generating set could build a GPM \mathbf{M} for \mathcal{C} . Although the size of \mathbf{M} is

8×2 , Theorem 3.3 asserts that $\text{rank}(\mathbf{M}) = 2$. Since \mathbf{M} has entries in the Euclidean domain $\mathbb{F}_3[x]$, elementary row operations are applied to \mathbf{M} to get the reduced GPM \mathbf{G} of \mathcal{C} . Actually, \mathbf{G} is formed from the non-zero rows of the Hermite normal form of \mathbf{M} . Namely,

$$\mathbf{G} = \begin{pmatrix} g_{1,1} & g_{1,2} \\ 0 & x^{40} + 2 \end{pmatrix},$$

where $g_{1,1} = 2 + x + 2x^2 + x^3 + x^4 + 2x^5 + x^7 + x^9 + 2x^{10} + x^{11} + 2x^{13} + x^{14} + x^4 + x^5 + x^7 + 2x^9 + 2x^{11} + 2x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + 2x^{19} + 2x^{21} + 2x^{24} + 2x^{25} + 2x^{27} + x^{29} + x^{31} + x^{32} + 2x^{33} + 2x^{34} + 2x^{36} + 2x^{37} + x^{39}$. One can check that \mathbf{G} satisfies the identical equation for

$$\mathbf{A} = \begin{pmatrix} 2 + 2x + x^4 + x^5 + x^6 & 2x(1 + x)^4 \\ 0 & 1 \end{pmatrix}.$$

Theorem 3.10. *Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ and let $\mathbf{G} = [g_{i,j}]$ be the reduced GPM of \mathcal{C} . Then \mathcal{C} is an \mathbb{F}_q -vector space of dimension*

$$k = \sum_{j=1}^{\ell} (m_j - \deg(g_{j,j})).$$

Proof. Set $n = \sum_{j=1}^{\ell} m_j$. In this proof, we consider \mathbb{F}_q^n , $(\mathbb{F}_q[x])^\ell$, and $\oplus_{j=1}^{\ell} \mathcal{R}_{m_j, \lambda_j}$ as \mathbb{F}_q -vector spaces. To remove any ambiguity, we write \mathcal{C} , \mathcal{C}' , and \mathcal{C}'' to refer to the code as a subspace of \mathbb{F}_q^n , $(\mathbb{F}_q[x])^\ell$, and $\oplus_{j=1}^{\ell} \mathcal{R}_{m_j, \lambda_j}$, respectively.

Let $\tau : (\mathbb{F}_q[x])^\ell \rightarrow \mathcal{C}'$ be the map $\tau(\mathbf{a}) = \mathbf{a}\mathbf{G}$. Since the rows of \mathbf{G} form a basis of \mathcal{C}' , τ is a vector space isomorphism. Let $\pi : \mathcal{C}' \rightarrow \mathcal{C}''$ be the restriction of the projection homomorphism $(\mathbb{F}_q[x])^\ell \rightarrow \oplus_{j=1}^{\ell} \mathcal{R}_{m_j, \lambda_j}$, see the proof of Theorem 2.13. Then $\text{Ker}(\pi) = \mathcal{C}' \cap M_\Lambda = M_\Lambda$. Let $\mathbf{A} = [a_{i,j}]$ be the matrix that satisfies the identical equation of \mathbf{G} , and let \mathcal{A} be the $\mathbb{F}_q[x]$ -submodule of $(\mathbb{F}_q[x])^\ell$ generated by the rows of \mathbf{A} . We let \mathcal{A} be viewed as an \mathbb{F}_q -vector space.

We claim that $\text{Ker}(\pi \circ \tau) = \mathcal{A}$. To see this, we have $\mathcal{A} \subseteq \text{Ker}(\pi \circ \tau)$ because $\pi \circ \tau(\mathbf{b}\mathbf{A}) = \pi(\mathbf{b}\mathbf{A}\mathbf{G}) = \pi(\mathbf{b}\mathbf{D}) = \mathbf{0}$ for any $\mathbf{b} \in (\mathbb{F}_q[x])^\ell$. Conversely, if $\mathbf{a} \in \text{Ker}(\pi \circ \tau)$, then $\tau(\mathbf{a}) \in \text{Ker}(\pi) = M_\Lambda$, hence $\mathbf{a}\mathbf{G} = \mathbf{b}\mathbf{D} = \mathbf{b}\mathbf{A}\mathbf{G}$ for some $\mathbf{b} \in (\mathbb{F}_q[x])^\ell$. Then, $\mathbf{a} = \mathbf{b}\mathbf{A} \in \mathcal{A}$ because the rows of \mathbf{G} are $\mathbb{F}_q[x]$ -linearly independent.

The isomorphism ϕ given by (12) confirms that $\mathcal{C} \simeq \mathcal{C}''$. Now, the sequence of vector space homomorphisms

$$(\mathbb{F}_q[x])^\ell \xrightarrow{\tau} \mathcal{C}' \xrightarrow{\pi} \mathcal{C}'' \simeq \mathcal{C}.$$

shows that $\mathcal{C} \simeq (\mathbb{F}_q[x])^\ell / \mathcal{A}$. It remains only to determine the dimension of the vector space $(\mathbb{F}_q[x])^\ell / \mathcal{A}$.

Let $\mathbf{f} = (f_1(x), f_2(x), \dots, f_\ell(x)) \in (\mathbb{F}_q[x])^\ell$. Using the division algorithm iteratively, one can uniquely determine $q_j, r_j \in \mathbb{F}_q[x]$ for $1 \leq j \leq \ell$ such that

$$f_j(x) - \sum_{i=1}^{j-1} q_i a_{i,j} = q_j a_{j,j} + r_j,$$

where $\deg(r_j) < \deg(a_{j,j}) = m_j - \deg(g_{j,j})$. Then

$$\mathbf{f} = [q_1, q_2, \dots, q_\ell] \mathbf{A} + \mathbf{r},$$

where $\mathbf{r} = (r_1, r_2, \dots, r_\ell)$ and, hence, $\mathbf{f} - \mathbf{r} \in \mathcal{A}$. Therefore

$$(\mathbb{F}_q[x])^\ell / \mathcal{A} = \{(r_1, r_2, \dots, r_\ell) + \mathcal{A} \mid \deg(r_j) < m_j - \deg(g_{j,j}) \text{ for } 1 \leq j \leq \ell\}.$$

Thus $(\mathbb{F}_q[x])^\ell / \mathcal{A}$ as a vector space has a dimension of $\sum_{j=1}^{\ell} (m_j - \deg(g_{j,j}))$. \square

4. DUAL CODES OF MT CODES

The standard inner product on \mathbb{F}_q^n is defined by

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=0}^{n-1} a_i b_i,$$

where $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ and $\mathbf{b} = (b_0, b_1, \dots, b_{n-1})$. Let \mathcal{C} be a subset of \mathbb{F}_q^n , the dual of \mathcal{C} is defined to be

$$(18) \quad \mathcal{C}^\perp = \{\mathbf{a} \in \mathbb{F}_q^n \mid \langle \mathbf{a}, \mathbf{c} \rangle = 0 \ \forall \ \mathbf{c} \in \mathcal{C}\}.$$

The inner product is a symmetric bilinear form, hence \mathcal{C}^\perp is a linear code over \mathbb{F}_q even if \mathcal{C} is non-linear. Equation (18) shows that $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$, where equality holds if \mathcal{C} is linear.

Let \mathcal{C} be a linear code over \mathbb{F}_q of length n , dimension k , and a $k \times n$ generator matrix \mathbf{G} . Then \mathcal{C}^\perp is the null space of \mathbf{G} , or, equivalently, $\mathcal{C}^\perp = \{\mathbf{a} \in \mathbb{F}_q^n \mid \mathbf{G}\mathbf{a}^t = \mathbf{0}_{k \times 1}\}$. The rank plus nullity theorem [25] emphasizes that \mathcal{C}^\perp is a linear subspace of \mathbb{F}_q^n of dimension $n - k$. A code \mathcal{C} is self-orthogonal if $\mathcal{C}^\perp \supseteq \mathcal{C}$, and in this case $n - k \geq k$, hence $k \leq \frac{n}{2}$. However, \mathcal{C} is self-dual if $\mathcal{C}^\perp = \mathcal{C}$. In fact, the code length of any self-dual code must be even because self-duality implies $n - k = k$, hence $n = 2k$. Additionally, a self-dual code is precisely a self-orthogonal code whose dimension is equal to half the code length, i.e., $k = \frac{n}{2}$.

The MacWilliams identity is a fundamental result in coding theory that relates the weight enumerator of a linear code to the weight enumerator of its dual. Before we present MacWilliams identity in Theorem 4.2, we define the weight enumerator of a code.

Definition 4.1. Let \mathcal{C} be a code over \mathbb{F}_q of length n and let the weight of a codeword $\mathbf{c} \in \mathcal{C}$ be denoted by $\omega(\mathbf{c})$. The weight enumerator of \mathcal{C} is a polynomial $W_{\mathcal{C}}(x, y) \in \mathbb{Z}[x, y]$ defined by

$$W_{\mathcal{C}}(x, y) = \sum_{\mathbf{c} \in \mathcal{C}} x^{n-\omega(\mathbf{c})} y^{\omega(\mathbf{c})}.$$

The size of the code can be determined from its weight enumerator since $W_{\mathcal{C}}(1, 1) = |\mathcal{C}|$. Also, the polynomial $W_{\mathcal{C}}(1, y)$ describes the different weights of codewords in \mathcal{C} . For example, if $W_{\mathcal{C}}(1, y) = 1 + 100y^5 + 200y^6 + 300y^7$, then \mathcal{C} contains the zero codeword, 100 codewords of weight 5, 200 codewords of weight 6, and 300 codewords of weight 7. Hence, \mathcal{C} contains 601 codewords and has a minimum weight of 5. The MacWilliams identity relates $W_{\mathcal{C}}$ to $W_{\mathcal{C}^\perp}$. The identity is valid for linear codes over a wide class of rings called Frobenius rings [7]. We state MacWilliams identity in its general form, where codes over finite fields are a special case.

Theorem 4.2 (MacWilliams Identity). *Let \mathcal{C} be a linear code over a finite commutative Frobenius ring of size q . Then*

$$W_{\mathcal{C}^\perp}(x, y) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}(x + (q-1)y, x - y).$$

Example 4.3. We continue with the $(2, 1)$ -MT code \mathcal{C} discussed in Examples 2.15 and 3.9. A brute force calculation of the weight enumerator of \mathcal{C} shows that $W_{\mathcal{C}}(x, y) = x^{60} + 400x^{24}y^{36} + 328x^{15}y^{45}$. From Theorem 4.2, we find that the weight enumerator of the dual of \mathcal{C} is as follows:

$$\begin{aligned} W_{\mathcal{C}^\perp}(x, y) &= \frac{1}{729} W_{\mathcal{C}}(x + 2y, x - y) \\ &= x^{60} + 40x^{58}y^2 + 240x^{57}y^3 + 8760x^{56}y^4 + \cdots + \\ &\quad 47445329187307520xy^{59} + 1581510989447168y^{60}. \end{aligned}$$

Therefore, \mathcal{C}^\perp is a linear code over \mathbb{F}_3 of length 60, dimension 54, and $d_{\min}(\mathcal{C}^\perp) = 2$.

We now turn our attention to MT codes and focus on investigating their duals. The dual of an MT code is not only a linear code, it is MT as well, but with different shift constants.

Theorem 4.4. *Let \mathcal{C} be a Λ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$, where $\Lambda = (\lambda_1, \lambda_2, \dots, \lambda_\ell)$. Then \mathcal{C}^\perp is Δ -MT of block lengths $(m_1, m_2, \dots, m_\ell)$, where $\Delta = (\frac{1}{\lambda_1}, \frac{1}{\lambda_2}, \dots, \frac{1}{\lambda_\ell})$.*

Proof. From Theorem 2.13, \mathcal{C} is a T_Λ -invariant subspace of \mathbb{F}_q^n , where $n = \sum_{j=1}^\ell m_j$ and T_Λ is the automorphism given by (11). Let $N = \text{lcm}(t_1 m_1, t_2 m_2, \dots, t_\ell m_\ell)$, where t_j is the multiplicative order of λ_j for $1 \leq j \leq \ell$. According to the discussion after Corollary 2.16, T_Λ^N

is the identity map. We show that $T_\Delta(\mathbf{b}) \in \mathcal{C}^\perp$ for every $\mathbf{b} \in \mathcal{C}^\perp$. For any $\mathbf{b} \in \mathcal{C}^\perp$ and $\mathbf{c} \in \mathcal{C}$, we have

$$\langle \mathbf{c}, T_\Delta(\mathbf{b}) \rangle = \langle T_\Lambda^N(\mathbf{c}), T_\Delta(\mathbf{b}) \rangle = \langle T_\Lambda \circ T_\Lambda^{N-1}(\mathbf{c}), T_\Delta(\mathbf{b}) \rangle = \langle T_\Lambda^{N-1}(\mathbf{c}), \mathbf{b} \rangle = 0,$$

because $T_\Lambda^{N-1}(\mathbf{c}) \in \mathcal{C}$. Then, $T_\Delta(\mathbf{b}) \in \mathcal{C}^\perp$ and \mathcal{C}^\perp is Δ -MT. \square

Since the dual of a Λ -MT code is Δ -MT, it can be represented by a submodule of $(\mathbb{F}_q[x])^\ell$ containing M_Δ , see Definition 2.12. We aim to present a GPM for \mathcal{C}^\perp . The following definition provides such a GPM.

Definition 4.5. For $1 \leq i \leq \ell$, let $0 \neq \lambda_i \in \mathbb{F}_q$ and let m_i be a positive integer. For an MT code of index ℓ , let $\mathbf{G} = [g_{i,j}]$ be the reduced GPM, let $\mathbf{A} = [a_{i,j}]$ be the matrix that satisfies the identical equation of \mathbf{G} , and let $d_j = \deg(g_{j,j})$ for $1 \leq j \leq \ell$.

- (a) Let $\mathbf{A}(\frac{1}{x})$ be the matrix obtained from \mathbf{A} when x is replaced by $\frac{1}{x}$.
- (b) Let \mathbf{A}^* be the matrix obtained after multiplying the (i, j) -th entry of $\mathbf{A}(\frac{1}{x})$ by $x^{m_i - d_j}$.
- (c) (Eliminate the negative exponents in \mathbf{A}^*) Let \mathbf{A}^{**} be the matrix obtained from \mathbf{A}^* by reducing the (i, j) -th entry (for $i < j$) of \mathbf{A}^* modulo $(x^{m_i} - \frac{1}{\lambda_i})$. Specifically, $x^{-\mu}$ is replaced by $\lambda_i x^{m_i - \mu}$ for $\mu \geq 1$.
- (d) The matrix \mathbf{H} is defined to be the transpose of \mathbf{A}^{**} .

Theorem 4.6. Let \mathcal{C} be a $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$, let $\mathbf{G} = [g_{i,j}]$ be the reduced GPM of \mathcal{C} , and let $\mathbf{A} = [a_{i,j}]$ be the matrix that satisfies the identical equation of \mathbf{G} . The polynomial matrix \mathbf{H} given in Definition 4.5 is a GPM for \mathcal{C}^\perp .

Example 4.7. We continue with the $(2, 1)$ -MT code \mathcal{C} discussed in Examples 2.15, 3.9, and 4.3. From Theorem 4.4, \mathcal{C}^\perp is $(2, 1)$ -MT over \mathbb{F}_3 of length 60 and dimension 54. A GPM for \mathcal{C}^\perp can be obtained from Definition 4.5 and Theorem 4.6 as follows:

$$\mathbf{A} = \begin{pmatrix} 2 + 2x + x^4 + x^5 + x^6 & 2x(1 + x)^4 \\ 0 & 1 \end{pmatrix}.$$

$$\begin{aligned}
\mathbf{A} \left(\frac{1}{x} \right) &= \begin{pmatrix} x^{-6} + x^{-5} + x^{-4} + 2x^{-1} + 2 & 2x^{-1}(x^{-1} + 1)^4 \\ 0 & 1 \end{pmatrix}. \\
\mathbf{A}^* &= \begin{pmatrix} x^{20-14} (x^{-6} + x^{-5} + x^{-4} + 2x^{-1} + 2) & 2x^{20-40} x^{-1} (x^{-1} + 1)^4 \\ 0 & x^{40-40} \end{pmatrix} \\
&= \begin{pmatrix} 1 + x + x^2 + 2x^5 + 2x^6 & 2x^{-25} + 2x^{-24} + 2x^{-22} + 2x^{-21} \\ 0 & 1 \end{pmatrix}. \\
\mathbf{A}^{**} &= \begin{pmatrix} 1 + x + x^2 + 2x^5 + 2x^6 & x^{-5} + x^{-4} + x^{-2} + x^{-1} \\ 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 + x + x^2 + 2x^5 + 2x^6 & 2x^{15} + 2x^{16} + 2x^{18} + 2x^{19} \\ 0 & 1 \end{pmatrix}. \\
\mathbf{H} &= \begin{pmatrix} 1 + x + x^2 + 2x^5 + 2x^6 & 0 \\ 2x^{15} + 2x^{16} + 2x^{18} + 2x^{19} & 1 \end{pmatrix}.
\end{aligned}$$

The reduced GPM \mathbf{G}^\perp of \mathcal{C}^\perp is obtained by reducing \mathbf{H} to its Hermite normal form. Namely,

$$\mathbf{G}^\perp = \begin{pmatrix} 1 & 2x + 2x^2 + x^3 + x^4 + x^5 \\ 0 & 2 + 2x + 2x^2 + x^5 + x^6 \end{pmatrix}.$$

Corollary 4.8. *Let \mathcal{C} be an ℓ -QC code over \mathbb{F}_q of co-index m and the reduced GPM $\mathbf{G} = [g_{i,j}]$. If $\mathbf{A} = [a_{i,j}]$ is the matrix satisfying the identical equation of \mathbf{G} , then \mathcal{C}^\perp is ℓ -QC of co-index m and a GPM*

$$\mathbf{H} = \left(\mathbf{A} \left(\frac{1}{x} \right) \text{diag} [x^{m-d_1}, \dots, x^{m-d_\ell}] \pmod{x^m - 1} \right)^t,$$

where $d_j = \deg(g_{j,j})$ for $1 \leq j \leq \ell$. The reduction modulo $x^m - 1$ is applied to remove negative exponents of x by replacing $x^{-\mu}$ with $x^{m-\mu}$ for $\mu \geq 1$.

Corollary 4.9. *Let \mathcal{C} be an (ℓ, λ) -QT code over \mathbb{F}_q of co-index m and the reduced GPM $\mathbf{G} = [g_{i,j}]$. If $\mathbf{A} = [a_{i,j}]$ is the matrix satisfying the identical equation of \mathbf{G} , then \mathcal{C}^\perp is $(\ell, \frac{1}{\lambda})$ -QT of co-index m and a GPM*

$$\mathbf{H} = \left(\mathbf{A} \left(\frac{1}{x} \right) \text{diag} [x^{m-d_1}, \dots, x^{m-d_\ell}] \pmod{x^m - \frac{1}{\lambda}} \right)^t,$$

where $d_j = \deg(g_{j,j})$ for $1 \leq j \leq \ell$. The reduction modulo $x^m - \frac{1}{\lambda}$ is applied to remove negative exponents of x by replacing $x^{-\mu}$ with $\lambda x^{m-\mu}$ for $\mu \geq 1$.

Corollary 4.10. *Let \mathcal{C} be an ℓ -GQC code over \mathbb{F}_q of block lengths $(m_1, m_2, \dots, m_\ell)$ and the reduced GPM $\mathbf{G} = [g_{i,j}]$. If $\mathbf{A} = [a_{i,j}]$ is the matrix satisfying the identical equation of \mathbf{G} , then*

\mathcal{C}^\perp is ℓ -GQC of block lengths $(m_1, m_2, \dots, m_\ell)$ and a GPM \mathbf{H} , where

$$\text{Column}_j(\mathbf{H}) = \text{row}_j \left(\mathbf{A} \left(\frac{1}{x} \right) \text{diag} \left[x^{m_j-d_1}, \dots, x^{m_j-d_\ell} \right] \pmod{x^{m_j}-1} \right),$$

and $d_j = \deg(g_{j,j})$ for $1 \leq j \leq \ell$. The reduction modulo $x^{m_j}-1$ is applied to remove negative exponents of x by replacing $x^{-\mu}$ with $x^{m_j-\mu}$ for $\mu \geq 1$.

Corollary 4.11. *Let \mathcal{C} denote an ℓ -QC, (ℓ, λ) -QT, ℓ -GQC, or $(\lambda_1, \lambda_2, \dots, \lambda_\ell)$ -MT code over \mathbb{F}_q and let \mathbf{H} be an $\ell \times \ell$ GPM of \mathcal{C}^\perp , e.g., \mathbf{H} is the polynomial matrix defined in Corollary 4.8, Corollary 4.9, Corollary 4.10, or Definition 4.5 respectively. If \mathbf{G} is an $\ell \times \ell$ GPM of \mathcal{C} , then \mathcal{C} is self-orthogonal if and only if there is a polynomial matrix \mathbf{U} such that $\mathbf{G} = \mathbf{U}\mathbf{H}$. Additionally, \mathcal{C} is self-dual if and only if \mathbf{U} is invertible.*

Proof. Theorem 4.6 shows that \mathbf{H} is a GPM for \mathcal{C}^\perp . The result then follows from Theorem 3.4. \square

Example 4.12. We investigate in detail one of the QC codes given in Table 1. Let \mathcal{C} be the binary 5-QC code of length 25 that has the reduced GPM

$$\mathbf{G} = \begin{pmatrix} 1+x & 0 & 0 & x+x^4 & x+x^2+x^3+x^4 \\ 0 & 1+x & 0 & x+x^2+x^3+x^4 & x+x^4 \\ 0 & 0 & 1+x^5 & 0 & 0 \\ 0 & 0 & 0 & 1+x^5 & 0 \\ 0 & 0 & 0 & 0 & 1+x^5 \end{pmatrix}.$$

Using brute force method, the weight enumerator of \mathcal{C} is $W_{\mathcal{C}}(x, y) = x^{25} + 130x^{17}y^8 + 120x^{13}y^{12} + 5x^9y^{16}$ and, hence, $d_{\min}(\mathcal{C}) = 8$. By Theorem 3.10, the dimension of \mathcal{C} is 8. Hence \mathcal{C} is optimal [16]. The identical equation of \mathbf{G} is satisfied by the polynomial matrix

$$\mathbf{A} = \begin{pmatrix} 1+x+x^2+x^3+x^4 & 0 & 0 & x+x^2+x^3 & x+x^3 \\ 0 & 1+x+x^2+x^3+x^4 & 0 & x+x^3 & x+x^2+x^3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Corollary 4.8 provides a GPM for \mathcal{C}^\perp which is given by

$$\mathbf{H} = \begin{pmatrix} 1+x+x^2+x^3+x^4 & 0 & 0 & 0 & 0 \\ 0 & 1+x+x^2+x^3+x^4 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ x^2+x^3+x^4 & x^2+x^4 & 0 & 1 & 0 \\ x^2+x^4 & x^2+x^3+x^4 & 0 & 0 & 1 \end{pmatrix}.$$

Finding the Hermite normal form of \mathbf{H} yields the reduced GPM

$$\mathbf{G}^\perp = \begin{pmatrix} 1 & 0 & 0 & x+x^2+x^3 & x+x^3 \\ 0 & 1 & 0 & x+x^3 & x+x^2+x^3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1+x+x^2+x^3+x^4 & 0 \\ 0 & 0 & 0 & 0 & 1+x+x^2+x^3+x^4 \end{pmatrix}.$$

The dual code \mathcal{C}^\perp is 5-QC over \mathbb{F}_2 of length 25 and dimension 17. From the MacWilliams identity, the weight enumerator of \mathcal{C}^\perp is

$$\begin{aligned} W_{\mathcal{C}^\perp}(x, y) &= \frac{1}{256} W_{\mathcal{C}}(x+y, x-y) \\ &= x^{25} + 5x^{24}y + 10x^{23}y^2 + 10x^{22}y^3 + \cdots + 10x^2y^{23} + 5xy^{24} + y^{25}. \end{aligned}$$

From Corollary 4.11, \mathcal{C} is self-orthogonal because $\mathbf{G} = \mathbf{U}\mathbf{G}^\perp$, where

$$\mathbf{U} = \begin{pmatrix} 1+x & 0 & 0 & 0 & 0 \\ 0 & 1+x & 0 & 0 & 0 \\ 0 & 0 & 1+x^5 & 0 & 0 \\ 0 & 0 & 0 & 1+x & 0 \\ 0 & 0 & 0 & 0 & 1+x \end{pmatrix}.$$

5. COMBINING PROPERTIES OF QC CODES

Suppose that \mathcal{C} is a linear code over \mathbb{F}_q of length n . For any codeword $\mathbf{c} \in \mathcal{C}$, the reverse of \mathbf{c} is the vector $\mathbf{r} \in \mathbb{F}_q^n$ obtained by reversing the coordinates of \mathbf{c} . That is, $\mathbf{r} = (c_{n-1}, \dots, c_1, c_0)$ whenever $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$. The set of all reverses of the codewords of \mathcal{C} forms a linear code over \mathbb{F}_q of length n . In this section, \mathcal{C} is restricted to be ℓ -QC of co-index m and length $n = m\ell$. Hence, the reverse of the codeword given by (3) is

$$\mathbf{r} = (c_{m-1,\ell}, \dots, c_{m-1,2}, c_{m-1,1}, c_{m-2,\ell}, \dots, c_{m-2,2}, c_{m-2,1}, \dots, c_{0,\ell}, \dots, c_{0,2}, c_{0,1}).$$

Definition 5.1. Let \mathcal{C} be an ℓ -QC code over \mathbb{F}_q . The reversed code \mathcal{R} of \mathcal{C} is the set containing the reverse of each codeword of \mathcal{C} . That is,

$$\mathcal{R} = \{\text{The reverse of } \mathbf{c} \mid \mathbf{c} \in \mathcal{C}\}.$$

In addition, \mathcal{C} is called reversible if $\mathcal{C} = \mathcal{R}$, i.e., the reverse of each codeword is a codeword.

Theorem 5.2. Let \mathcal{C} and \mathcal{R} be as in Definition 5.1. Then \mathcal{R} is linear, QC, and has the same index, co-index, dimension, and minimum distance as \mathcal{C} .

Proof. In fact, \mathcal{C} and \mathcal{R} are permutation equivalent. Hence, \mathcal{R} is linear and has the same length, dimension and minimum distance as \mathcal{C} . Let ℓ and m be the index and co-index of \mathcal{C} , respectively. For any $\mathbf{r} \in \mathcal{R}$, there exists a codeword $\mathbf{c} \in \mathcal{C}$ such that \mathbf{r} is the reverse of \mathbf{c} . It can be seen that $T_\ell(\mathbf{r})$ is the reverse of $T_\ell^{-1}(\mathbf{c}) \in \mathcal{C}$, where T_ℓ is the automorphism of \mathbb{F}_q^n that corresponds to ℓ coordinates shift. Thus, $T_\ell(\mathbf{r}) \in \mathcal{R}$ and \mathcal{R} is ℓ -QC of co-index m . \square

The polynomial representation of the codewords of \mathcal{R} is related to that of the codewords of \mathcal{C} . Specifically, if we write the polynomial representation of a codeword of \mathcal{C} as $\mathbf{c} = (c_1(x), c_2(x), \dots, c_\ell(x))$, the polynomial representation of its reverse is

$$(19) \quad \mathbf{r} = x^{m-1} \left(c_\ell \left(\frac{1}{x} \right), c_{\ell-1} \left(\frac{1}{x} \right), \dots, c_2 \left(\frac{1}{x} \right), c_1 \left(\frac{1}{x} \right) \right).$$

The following result provides an explicit GPM formula for \mathcal{R} , and the proof can be found in [11].

Theorem 5.3. Let \mathcal{C} be an ℓ -QC code over \mathbb{F}_q of co-index m with a GPM $\mathbf{G} = [g_{i,j}]$. Let $\mathbf{J} = [\delta_{i,\ell+1-j}]$ be the $\ell \times \ell$ backward identity matrix. A GPM for the reversed code \mathcal{R} of \mathcal{C} is given by

$$(20) \quad \mathbf{F} = \left(\text{diag} \left[x^{m+d_1}, \dots, x^{m+d_\ell} \right] \mathbf{G} \left(\frac{1}{x} \right) + (1 - x^m) \text{diag} [g_{1,1}^*, \dots, g_{\ell,\ell}^*] \right) \mathbf{J},$$

where $d_i = \deg(g_{i,i})$ and $g_{i,i}^* = x^{d_i} g_{i,i} \left(\frac{1}{x} \right)$ for $1 \leq i \leq \ell$.

From Theorems 3.4 and 5.3, a QC code with a GPM \mathbf{G} is reversible if and only if there is an invertible polynomial matrix \mathbf{U} such that $\mathbf{F} = \mathbf{U}\mathbf{G}$, where \mathbf{F} is given by (20). By the uniqueness of the Hermite normal form, an equivalent condition for the reversibility of a QC code is that writing \mathbf{F} in its Hermite normal form yields the reduced GPM of \mathcal{C} .

Example 5.4. We continue with the binary 5-QC code \mathcal{C} given in Example 4.12. From Theorem 5.3, a GPM for the reversed code \mathcal{R} of \mathcal{C} is

$$\mathbf{F} = \begin{pmatrix} x^2 + x^3 + x^4 + x^5 & x^2 + x^5 & 0 & 0 & 1 + x \\ x^2 + x^5 & x^2 + x^3 + x^4 + x^5 & 0 & 1 + x & 0 \\ 0 & 0 & 1 + x^5 & 0 & 0 \\ 0 & 1 + x^5 & 0 & 0 & 0 \\ 1 + x^5 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

One can show that \mathcal{C} is reversible because $\mathbf{F} = \mathbf{U}\mathbf{G}$ for the invertible polynomial matrix

$$\mathbf{U} = \begin{pmatrix} x^2 + x^4 & x^2 + x^3 + x^4 & 0 & 0 & 1 + x \\ x^2 + x^3 + x^4 & x^2 + x^4 & 0 & 1 + x & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 + x + x^2 + x^3 + x^4 & 0 & x + x^3 & x + x^2 + x^3 \\ 1 + x + x^2 + x^3 + x^4 & 0 & 0 & x + x^2 + x^3 & x + x^3 \end{pmatrix}.$$

Equivalently, \mathcal{C} is reversible because the Hermite normal form of \mathbf{F} is \mathbf{G} . Therefore, we have shown that \mathcal{C} is binary optimal self-orthogonal reversible QC code.

In [11], computer search is used to present some binary optimal self-orthogonal reversible QC codes with different index values. The minimum distances of these codes are calculated using brute force or the method mentioned in [15]. We present these computer search results in Table 1. The reader can check the properties of these codes in the same way we used in Examples 4.12 and 5.4, see also Example 5.6 below. Table 1 records the non-zero entries $g_{i,j}$ of the reduced GPMs $\mathbf{G} = [g_{i,j}]$ of these codes. In this table, $\{0, 6, 7, 8, 10, 11\}$ is used to abbreviate the polynomial $1 + x^6 + x^7 + x^8 + x^{10} + x^{11} \in \mathbb{F}_2[x]$. We conclude this paper by summarizing some sufficient and necessary conditions that represent the different states between QC code, its dual code, and its reversed code. We omit the proof of the following result which can be found in [11].

Theorem 5.5. *Let \mathcal{C} be an ℓ -QC code over \mathbb{F}_q of co-index m . Let \mathbf{G} be the reduced GPM of \mathcal{C} and let \mathbf{A} be the matrix that satisfies the identical equation of \mathbf{G} . Let \mathcal{C}^\perp and \mathcal{R} be the dual and reversed code of \mathcal{C} , respectively. Then,*

- (a) $\mathcal{C}^\perp \supseteq \mathcal{R}$ if and only if $\mathbf{G}\mathbf{J}\mathbf{G}^t \equiv \mathbf{0}_{\ell \times \ell} \pmod{x^m - 1}$. Therefore, if \mathcal{C} is reversible, then \mathcal{C} is self-orthogonal if and only if $\mathbf{G}\mathbf{J}\mathbf{G}^t \equiv \mathbf{0}_{\ell \times \ell} \pmod{x^m - 1}$.
- (b) $\mathcal{C}^\perp \subseteq \mathcal{R}$ if and only if $\mathbf{A}^t\mathbf{J}\mathbf{A} \equiv \mathbf{0}_{\ell \times \ell} \pmod{x^m - 1}$. Therefore, if \mathcal{C} is reversible, then $\mathcal{C}^\perp \subseteq \mathcal{C}$ if and only if $\mathbf{A}^t\mathbf{J}\mathbf{A} \equiv \mathbf{0}_{\ell \times \ell} \pmod{x^m - 1}$.

TABLE 1. Binary optimal self-orthogonal reversible QC codes

ℓ	n	k	d_{\min}	$G = (g_{i,j})$
2	64	32	12	$g_{1,1} = \{0\}, g_{2,2} = \{0, 32\},$ $g_{1,2} = \{2, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 19, 20, 22, 24, 25, 28, 29, 30, 31\}$
3	36	6	16	$g_{1,1} = \{0, 1, 2, 4, 5, 6\}, g_{1,2} = \{1, 5, 7, 11\},$ $g_{1,3} = \{0, 6, 7, 8, 10, 11\}, g_{2,2} = g_{3,3} = \{0, 12\}$
4	68	34	12	$g_{1,1} = g_{1,2} = \{0\}, g_{1,3} = \{0, 3, 4, 7, 10, 11, 14\},$ $g_{1,4} = \{1, 2, 6, 7, 10, 12, 14\}, g_{2,2} = \{0, 1\},$ $g_{2,3} = \{1, 4, 5, 9, 10, 15\}, g_{2,4} = \{0, 3, 4, 7, 8, 9, 12, 14\}, g_{4,4} = \{0, 17\},$ $g_{3,3} = g_{3,4} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
5	25	8	8	$g_{1,1} = g_{2,2} = \{0, 1\}, g_{1,4} = g_{2,5} = \{1, 4\},$ $g_{1,5} = g_{2,4} = \{1, 2, 3, 4\}, g_{3,3} = g_{4,4} = g_{5,5} = \{0, 5\}$
6	36	18	8	$g_{1,1} = g_{1,3} = g_{2,2} = g_{2,5} = \{0\}, g_{1,4} = \{2, 4\},$ $g_{1,5} = g_{4,4} = g_{4,6} = \{0, 1, 2, 3, 4, 5\}, g_{1,6} = \{0, 1, 3, 5\},$ $g_{2,4} = \{3\}, g_{2,6} = \{0, 1, 2, 4, 5\}, g_{3,3} = \{0, 1\}, g_{3,4} = \{0, 3, 4\},$ $g_{3,5} = \{3, 4\}, g_{3,6} = \{0, 2, 5\}, g_{5,5} = g_{6,6} = \{0, 6\}$
7	42	14	12	$g_{1,1} = \{0\}, g_{1,3} = \{0, 1, 2, 3\}, g_{1,4} = \{0, 3\}, g_{1,5} = \{5\}, g_{1,6} = \{2, 3, 4, 5\},$ $g_{2,2} = \{0, 1\}, g_{2,3} = \{2\}, g_{2,4} = \{1, 4\}, g_{2,5} = \{0, 1, 4, 5\},$ $g_{2,6} = g_{3,6} = g_{4,4} = g_{4,6} = \{0, 1, 2, 3, 4, 5\}, g_{2,7} = \{1\},$ $g_{3,3} = \{0, 2, 4\}, g_{3,7} = \{1, 3, 5\}, g_{5,5} = g_{6,6} = g_{7,7} = \{0, 6\}$
8	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = \{0\}, g_{1,5} = g_{4,8} = \{0, 2, 4\},$ $g_{1,6} = g_{2,5} = g_{3,8} = g_{4,7} = \{0, 1, 4\}, g_{1,7} = g_{2,8} = \{0, 2\}, g_{1,8} = \{1, 2, 4\},$ $g_{2,6} = g_{3,7} = \{3\}, g_{2,7} = \{2\}, g_{3,5} = g_{4,6} = \{1\}, g_{3,6} = \{1, 4\},$ $g_{4,5} = \{1, 2, 3, 4\}, g_{5,5} = g_{6,6} = g_{7,7} = g_{8,8} = \{0, 5\}$
9	54	24	12	$g_{1,1} = g_{1,2} = g_{3,3} = g_{3,4} = \{0\}, g_{1,6} = \{1\}, g_{1,7} = \{1, 3, 5\},$ $g_{1,8} = \{0, 2\}, g_{1,9} = g_{2,5} = g_{3,5} = g_{4,5} = \{1, 2, 4, 5\}, g_{2,2} = g_{4,4} = \{0, 1\},$ $g_{2,6} = g_{4,8} = \{0, 1, 4\}, g_{2,7} = \{0, 1, 2, 3, 4\}, g_{2,8} = \{1, 4\}, g_{2,9} = \{0, 2, 3, 4\},$ $g_{3,6} = \{3, 4\}, g_{3,7} = \{0, 1, 3, 5\}, g_{3,8} = \{2\}, g_{3,9} = \{2, 3, 5\},$ $g_{4,6} = \{0, 1, 2, 3\}, g_{4,7} = \{0, 1, 2, 5\}, g_{4,9} = \{0, 2, 4\},$ $g_{5,5} = g_{7,7} = g_{9,9} = \{0, 6\}, g_{6,6} = g_{6,7} = g_{8,8} = g_{8,9} = \{0, 1, 2, 3, 4, 5\}$
10	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = g_{5,5} = g_{3,6} = g_{5,8} = \{0\},$ $g_{1,6} = g_{3,8} = g_{5,10} = \{0, 1\}, g_{1,7} = g_{1,9} = g_{2,10} = g_{4,10} = g_{5,6} = \{2, 3\},$ $g_{1,8} = g_{2,7} = g_{3,10} = g_{4,9} = \{1, 2\}, g_{1,10} = g_{4,6} = g_{5,7} = \{3\},$ $g_{2,6} = g_{5,9} = \{0, 1, 2\}, g_{2,8} = g_{3,9} = \{1\}, g_{2,9} = g_{4,7} = \{2\},$ $g_{3,7} = g_{4,8} = \{0, 2, 3\}, g_{6,6} = g_{7,7} = g_{8,8} = g_{9,9} = g_{10,10} = \{0, 4\}$

- (c) If \mathcal{C} is reversible, then \mathcal{C} is self-dual if and only if $\mathbf{GJG}^t \equiv \mathbf{A}^t \mathbf{J} \mathbf{A} \equiv \mathbf{0}_{\ell \times \ell} \pmod{x^m - 1}$ if and only if $\mathbf{A} = \mathbf{JG}^t \mathbf{J}$.
- (d) If $\mathbf{A} = \mathbf{JG}^t \mathbf{J}$, then \mathcal{C} is self-dual if and only if \mathcal{C} is reversible,
- (e) If \mathcal{C} is self-dual, then \mathcal{C} is reversible if and only if $\mathbf{A} = \mathbf{JG}^t \mathbf{J}$.

Example 5.6. We continue with the binary optimal self-orthogonal reversible QC code discussed in Example 5.4. Since \mathcal{C} is reversible, Theorem 5.5 can be used to check the self-orthogonality of \mathcal{C} , see Example 4.12. Specifically, \mathcal{C} is self-orthogonal if and only if $\mathbf{GJG}^t \equiv \mathbf{0}_{\ell \times \ell} \pmod{1 + x^5}$. In fact, we have

$$\mathbf{GJG}^t = (1 + x^5) \begin{pmatrix} 0 & 0 & 0 & 0 & 1 + x \\ 0 & 0 & 0 & 1 + x & 0 \\ 0 & 0 & 1 + x^5 & 0 & 0 \\ 0 & 1 + x & 0 & 0 & 0 \\ 1 + x & 0 & 0 & 0 & 0 \end{pmatrix}.$$

6. CONCLUSION

We introduced cyclic, constacyclic, QC, QT, GQC, and MT codes as submodules of the free $\mathbb{F}_q[x]$ -module $(\mathbb{F}_q[x])^\ell$. We demonstrated how a GPM for any MT code may be established. As a result, we proved several interesting properties and identities for GPMs. Because the dual of an MP code is also MP, we presented a GPM formula for the dual of any MT code using the identical equation of the reduced GPM of the original code. Hence, we established the necessary and sufficient conditions for the self-orthogonality and self-duality of MT codes. We next turned our attention to QC codes, investigating conditions to combine self-orthogonality, reversibility, and optimality for QC codes. Finally, we presented various binary QC codes that combined these properties.

7. ACKNOWLEDGMENTS

The authors wish to sincerely thank the referees for several useful comments.

REFERENCES

- [1] N. Aydin and A. Halilović, *A generalization of quasi-twisted codes: Multi-twisted codes*, Finite Fields Their Appl., **45** (2017) 96-106.
- [2] M. Barbier, C. Chabot, and G. Quintin, *On quasi-cyclic codes as a generalization of cyclic codes*, Finite Fields Their Appl., **18** No. 5 (2012) 904-919.
- [3] Y. Cao, *Structural properties and enumeration of 1-generator generalized quasi-cyclic codes*, Des. Codes Cryptogr., **60** No. 1 (2010) 67-79.

- [4] P. L. Cayrel, C. Chabot, and A. Necer, *Quasi-cyclic codes as codes over rings of matrices*, Finite Fields Their Appl., **16** No. 2 (2010) 100-115.
- [5] V. Chauhan, *Multi-twisted Codes Over Finite Fields and Their Generalizations*, Ph.D. thesis, Indraprastha Institute of Information Technology, 2021.
- [6] E. Chen and N. Aydin, *A database of linear codes over \mathbb{F}_{13} with minimum distance bounds and new quasi-twisted codes from a heuristic search algorithm*, J. Algebra Comb. Discrete Struct. Appl., **2** (2015).
- [7] S. T. Dougherty, *Algebraic coding theory over finite commutative rings*, 1st ed., Springer International Publishing, Switzerland, 2017.
- [8] R. Taki Eldin and H. Matsui, *Quasi-cyclic codes via unfolded cyclic codes and their reversibility*, IEEE Access, **7** (2019) 184500-184508.
- [9] R. Taki Eldin and H. Matsui, *Good reversible quasi-cyclic codes via unfolding cyclic codes*, IEICE Commun. Express, **9** No. 12 (2020) 668-673.
- [10] R. Taki Eldin and H. Matsui, *On reversibility and self-duality for some classes of quasi-cyclic codes*, IEEE Access, **8** (2020) 143285-143293.
- [11] R. Taki Eldin and H. Matsui, *Linking reversed and dual codes of quasi-cyclic codes*, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., **105** No. 3 (2021) 381-388.
- [12] J. Gao and F. W. Fu, *Note on quasi-twisted codes and an application*, J. Appl. Math. Comput., **47** No. 1-2 (2014) 487-506.
- [13] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 3rd ed., Cambridge University Press, 2013.
- [14] E. N. Gilbert, *A comparison of signalling alphabets*, Bell Syst. Tech. J., **31** No. 3 (1952) 504-522.
- [15] M. Grassl, *Searching for linear codes with large minimum distance*, In Discovering Mathematics with Magma, pp. 287-313, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.
- [16] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at <http://www.codetables.de> (2007).
- [17] G. G. L. Guardia, *On optimal constacyclic codes*, Linear Algebra Appl., **496** (2016) 594-610.
- [18] C. Güneri, F. Özbudak, B. Özkaya, E. Saçıkara, Z. Sepasdar, and P. Solé, *Structure and performance of generalized quasi-cyclic codes*, Finite Fields Their Appl., **47** (2017) 183-202.
- [19] Y. Jia, *On quasi-twisted codes over finite fields*, Finite Fields Their Appl., **18** No. 2 (2012) 237-257.
- [20] R. Kipp Martin, *Large Scale Linear and Integer Optimization: A Unified Approach*, Springer, New York, 2012.
- [21] K. Lally and P. Fitzpatrick, *Algebraic structure of quasicyclic codes*, Discrete Appl. Math., **111** No. 1-2 (2001) 157-175.
- [22] C. Martinez-Perez and W. Willems, *Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good*, IEEE Trans. Inf. Theory, **53** No. 11 (2007) 4302-4308.
- [23] J. L. Massey, *Reversible codes*, Inf. Control, **7** No. 3 (1964) 369-380.
- [24] H. Matsui, *On generator and parity-check polynomial matrices of generalized quasi-cyclic codes*, Finite Fields Their Appl., **34** (2015) 280-304.
- [25] S. Roman, *Advanced Linear Algebra*, Graduate Texts in Mathematics, Springer, New York, 2008.
- [26] A. Sharma, V. Chauhan, and H. Singh, *Multi-twisted codes over finite fields and their dual codes*, Finite Fields Their Appl., **51** (2018) 270-297.

- [27] I. Siap and N. Kulhan, *The structure of generalized quasi-cyclic codes*, Appl. Math. E-Notes, **5** (2005) 24-30.

Ramy Taki Eldin

Faculty of Engineering,

Ain Shams University,

Cairo, Egypt.

`ramy.farouk@eng.asu.edu.eg`