Multi-twisted Codes Over Finite Fields And Their Generalizations

by

VARSHA CHAUHAN

Under the Supervision of Dr. Anuradha Sharma

Indraprastha Institute of Information Technology Delhi

January 2021

Multi-twisted Codes Over Finite Fields And Their Generalizations

by

VARSHA CHAUHAN

Department of Mathematics

Submitted

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

to the

Indraprastha Institute of Information Technology Delhi

January 2021

Dedicated to

my parents

my parents-in-law

and

my beloved husband Nishant Rana

Certificate

This is to certify that the thesis entitled **"Multi-twisted Codes Over Finite Fields And Their Generalizations"** being submitted by **"Ms. Varsha Chauhan"** to the **Indraprastha Institute of Information Technology Delhi**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by her under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

New Delhi
January 2021

Dr. Anuradha Sharma
Professor
Department of Mathematics
IIIT-Delhi

Acknowledgements

It is a great pleasure for me to express my respect and deep sense of gratitude to my Ph.D. supervisor Dr. Anuradha Sharma for her wisdom, vision, expertise, co-operation, enthusiastic involvement and persistent encouragement during the planning and development of this research work. I am indebted to her for being available whenever there was a need to discuss my doubts and for her invaluable advice and regular guidance. I also gratefully acknowledge her painstaking efforts in thoroughly going through and improving the manuscripts.

I wish to acknowledge all the faculty members of Department of Mathematics, IIIT-Delhi for their support and co-operation. My special thanks are extended to my doctoral committee members Dr. Pravesh Biyani and Dr. Samrith Ram for their valuable time and insightful comments. Also, I am extremely thankful to Dr. Shanta Laisharam (Indian Statistical Institue, New Delhi, India) who was the external examiner on the occasion of my comprehensive exam and fellowship enhancement seminar.

I convey my heartfelt thank to all my friends and research fellows at IIIT-Delhi as well for the discussion and sharing their valuable ideas which helped me to understand the concepts well. I would also like to thank all the supporting staff who directly or indirectly have helped me to complete my work smoothly at IIIT-Delhi.

I am extremely grateful to my thesis evaluation committee members Prof. Simon Litsyn (Tel Aviv University, Israel), Prof. Edgar Martínez-Moro (University Of Valladolid, Spain) and Prof. Patrick Solé (Aix-Marseille University, France) for their valuable time and consideration. I would also like to thank University Grants Commission (UGC) for providing financial support.

I am very thankful to my parents Mr. Jitendra Chauhan and Mrs. Vinesh Chauhan, and parents-in-laws Mr. Brahampal Rana and Mrs. Saroj Bala for being supportive, understanding and helping me in every possible way, which kept me going throughout my tough journey. I am especially thankful to my husband Nishant Rana for his patience, love, encouragement and care during this journey.

To you all, I dedicate this work. Thank you for being a part of my success story.

Above all I am indebted and grateful to the Almighty for helping me in this endeavor.

New Delhi *Varsha Chauhan*

January 2021

Abstract

Nowadays error-correcting codes are widely used in communication systems, returning pictures from deep space, designing registration numbers, and storage of data in memory systems. An important family of error-correcting codes is that of linear codes, which contain many well-known codes such as Hamming codes, Hadamard codes, cyclic codes and quasi-cyclic codes. Recently, Aydin and Halilović [5] introduced and studied multi-twisted (MT) codes over the finite field $\mathbb{F}_q$, whose block lengths are coprime to q. These codes are generalizations of well-known classes of linear codes, such as constacyclic codes and generalized quasi-cyclic codes, having rich algebraic structures and containing record-breaker codes. In the same work, they obtained subcodes of MT codes with best-known parameters $[33, 12, 12]$ over $\mathbb{F}_3$, $[53, 18, 21]$ over $\mathbb{F}_5$, $[23, 7, 13]$ over $\mathbb{F}_7$ and optimal parameters $[54, 4, 44]$ over $\mathbb{F}_7$. Apart from this, they proved that the code parameters $[53, 18, 21]$ over $\mathbb{F}_5$ and $[33, 12, 12]$ over $\mathbb{F}_3$ can not be attained by constacyclic and quasi-cyclic codes, which suggests that this larger class of MT codes is more promising to find codes with better parameters than the current best known linear codes.

In this thesis, we first investigate algebraic structures of MT codes over $\mathbb{F}_q$, whose block lengths are coprime to q. We also study their dual codes with respect to Euclidean and Hermitian inner products, and derive necessary and sufficient conditions for a MT code to be (i) self-dual, (iii) self-orthogonal and (iii) linear

with complementary-dual (LCD). Applying these results, we provide enumeration formulae for all Euclidean and Hermitian self-dual, self-orthogonal and LCD MT codes over $\mathbb{F}_q$. We also derive some sufficient conditions under which a MT code is either Euclidean LCD or Hermitian LCD. We further develop generator theory for these codes and determine their parity-check polynomials. We also obtain a BCH type bound on their minimum Hamming distances, and express generating sets of Euclidean and Hermitian dual codes of some MT codes in terms of their generating sets. Besides this, we provide a trace description for all MT codes by viewing these codes as direct sums of certain concatenated codes, which leads to a method to construct these codes. We also obtain a lower bound on their minimum Hamming distances using their multilevel concatenated structure. Besides this, we explicitly determine all non-zero Hamming weights of codewords of several classes of MT codes over $\mathbb{F}_q$. Using these results, we explicitly determine Hamming weight distributions of several classes of MT codes with a few weights. Among these classes of MT codes with a few weights, we identify two classes of optimal equidistant MT codes that attain the Griesmer as well as Plotkin bounds, and several other classes of MT codes that are useful in constructing secret sharing schemes with nice access structures.

We further extend the family of MT codes and study algebraic structures of MT codes over $\mathbb{F}_q$, whose block lengths are arbitrary positive integers, not necessarily coprime to q. We study their dual codes with respect to the Galois inner product and derive necessary and sufficient conditions under which a MT code is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD. We also provide a trace description for all MT codes over finite fields by using the generalized discrete Fourier transform (GDFT), which gives rise to a method to construct these codes. We further provide necessary and sufficient conditions under which a Euclidean self-dual MT code over a finite field of even characteristic is a Type II code. We also show that each MT code has a unique normalized generating set. With the help

of a normalized generating set, we explicitly determine the dimension and the corresponding generating set of the Galois dual code of each MT code. Besides this, we identify several classes of MT codes over finite fields with a few weights and explicitly determine their Hamming weight distributions.

We next study skew analogues of MT codes over finite fields, *viz.* skew multi-twisted (MT) codes, which are linear codes and are generalizations of MT codes. We thoroughly investigate algebraic structures of skew MT codes over finite fields and their Galois duals. Besides this, we view skew MT codes as direct sums of certain concatenated codes and provide a method to construct these codes. We also develop generator theory for these codes, and obtain two lower bounds on their minimum Hamming distances.

Finally, we apply our results to obtain many linear codes with best known and optimal parameters from MT and skew MT codes over finite fields.

Contents

List of Symbols

Symbol	**Meaning**
$\|A\|$	*Cardinality* of the set A
$\max\{a, b\}$	*Maximum* of a and b
$\min\{a, b\}$	*Minimum* of a and b
$\dim_F V$	The *dimension* of a finite-dimensional vector space V over the field F
$\gcd(a, b)$	The *greatest common divisor* of a and b
$\mathrm{lcm}[a, b]$	The *least common multiple* of a and b
$a \equiv b \pmod{n}$	The integers a and b are congruent modulo a positive integer n
$O(a)$	The *multiplicative order* of the group element a
$\langle a \rangle$	The *cyclic group* generated by the element a
$\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_q$	The *q-binomial coefficient*
$\mathbb{F}_q$	The *finite field* of order q
$Tr_{\mathbb{F}_{q^t}/\mathbb{F}_q}$	The *trace map* from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$
$[\cdot, \cdot] \restriction_{U \times U}$	The *restriction* of the map $[\cdot, \cdot]$ to $U \times U$

$\lceil \vdots \rceil$	The *Ceiling* function
$\lfloor \vdots \rfloor$	The *Floor* function
$d_{\min}(\mathcal{C})$	The minimum *Hamming distance* of the code $\mathcal{C}$.

Research Publications

Published Articles:

1. Sharma, A., **Chauhan, V.** and Singh, H. : Multi-twisted codes over finite fields and their dual codes, *Finite Fields Appl.* 51, pp. 270-297, 2018.

2. Sharma, A. and **Chauhan, V.**: Skew multi-twisted codes over finite fields and their Galois duals, *Finite Fields Appl.* 59, pp. 297-334, 2019.

Communicated Articles:

1. **Chauhan, V.** and Sharma, A.: Hamming weights in multi-twisted codes over finite fields, communicated for publication.

2. **Chauhan, V.** and Sharma, A.: A generalization of multi-twisted codes over finite fields, their Galois duals and Type II codes, communicated for publication.

3. **Chauhan, V.** and Sharma, A.: Hamming weight distributions of multi-twisted codes over finite fields, communicated for publication.

1

Introduction

The object of this thesis is

- to investigate algebraic structures of multi-twisted codes over finite fields and their dual codes.
- to develop generator theory and to provide a construction method for multi-twisted codes over finite fields.
- to determine Hamming weight distributions of several classes of multi-twisted codes over finite fields.
- to study skew analogues of multi-twisted codes over finite fields and their Galois duals, and to develop generator theory for these codes.

Now we proceed to describe the problems that we have explored in this thesis.

1.1 Multi-twisted codes over finite fields and their dual codes

Prange [66] introduced and studied cyclic codes over finite fields, which form the most-studied class of linear codes containing many important codes such as BCH codes, Reed-Solomon codes and quadratic residue codes. These codes can be effectively encoded and decoded using linear feedback shift registers and can be viewed as ideals of a certain quotient ring of polynomial rings. Later, Townsend and Weldon [77] introduced and studied quasi-cyclic (QC) codes over finite fields, which are generalizations of cyclic codes. Kasami [49] and Weldon [79] further showed that these codes are asymptotically good due to their abundant population. Solomon and Tilborg [75] established a link between these codes and convolutional codes. Using this, they deduced many interesting properties of linear codes, which have applications in coding theory and modulation. Ling and Solé [53] viewed QC codes over finite fields as linear codes over a certain auxiliary ring and studied their dual codes with respect to the Euclidean inner product. They also explored the existence of some Euclidean self-dual QC codes and provided enumeration formulae for this class of codes in certain special cases. Later, Ling et al. [52] studied QC codes over rings of characteristic not coprime with the co-index. In the same work, they provided a trace description for these codes using the generalized discrete Fourier transform (GDFT) and studied their dual codes with respect to the Euclidean inner product. They also derived a characterization of Type II QC codes of singly even co-index over finite fields of even characteristic. Siap and Kulhan [73] further generalized these codes to generalized quasi-cyclic (GQC) codes over finite fields. They studied algebraic properties of 1-generator GQC codes and obtained a BCH type bound on their minimum Hamming distances. By applying the Chinese Remainder

Theorem and the results derived in Ling and Solé [55], Esmaeili and Yari [34] decomposed GQC codes into linear codes, and provided an improved lower bound on their minimum Hamming distances. Güneri et al. [41] decomposed GQC codes as direct sums of concatenated codes, which leads to a trace formula and a minimum distance bound for GQC codes. Jia [47] further generalized QC codes to quasi-twisted (QT) codes, and decomposed these codes into direct sums of linear codes over rings. She also studied their dual codes with respect to the Euclidean inner product and provided a method to construct QT codes using the inverse generalized discrete Fourier transform. Later, Saleh and Esmaeili [68] provided some sufficient conditions under which a QT code is linear with complementary dual (LCD) with respect to the Euclidean inner product. A large number of record-breaking QC and QT codes have been obtained [6, 7, 25–27] by using the search algorithm proposed in [8].

In a recent work, Aydin and Halilović [5] introduced multi-twisted (MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length $n = m_1 + m_2 + \cdots + m_\ell$ over $\mathbb{F}_q$, where $m_1, m_2, \cdots, m_\ell$ are positive integers coprime to q. These codes form an important class of linear codes and are generalizations of constacyclic and generalized quasi-cyclic (GQC) codes. They studied some basic properties of 1-generator MT codes. They also presented several methods to construct 1-generator MT codes and obtained several bounds on their minimum Hamming distances. In the same work, they obtained linear codes with best known parameters $[33, 12, 12]$ over $\mathbb{F}_3$, $[53, 18, 21]$ over $\mathbb{F}_5$, $[23, 7, 13]$ over $\mathbb{F}_7$ and optimal parameters $[54, 4, 44]$ over $\mathbb{F}_7$ from subcodes of MT codes. Apart from this, they proved that the code parameters $[53, 18, 21]$ over $\mathbb{F}_5$ and $[33, 12, 12]$ over $\mathbb{F}_3$ can not be attained by constacyclic or QC codes, which suggests that this larger class of MT codes is more promising to find codes with better parameters than the current best linear codes.

From now on, throughout this thesis, let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where p is a prime and r is a positive integer. Let ℓ be a positive integer, and let

$n = m_1 + m_2 + \cdots + m_\ell$, where $m_1, m_2, \cdots, m_\ell$ are positive integers. Let $\mathbb{F}_q^n$ denote the vector space consisting of all n-tuples over $\mathbb{F}_q$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$.

In Chapter 2, we state some preliminaries that are needed to derive our main results.

In Chapter 3, we study the algebraic structure of Λ-multi-twisted (Λ-MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and their dual codes with respect to the Euclidean and Hermitian inner products on $\mathbb{F}_q^n$, where $m_1, m_2, \cdots, m_\ell$ are positive integers satisfying $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. We also provide necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) Euclidean self-dual, (ii) Euclidean self-orthogonal, (iii) Euclidean LCD, (iv) Hermitian self-dual, (v) Hermitian self-orthogonal and (vi) Hermitian LCD. We also derive some sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is either Euclidean LCD or Hermitian LCD. We determine the parity-check polynomial of all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and obtain a BCH type bound on their minimum Hamming distances. We also express generating sets of Euclidean and Hermitian dual codes of some Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ in terms of their generating sets. Besides this, we provide a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by viewing these codes as direct sums of certain concatenated codes, which leads to a method to construct these codes. We also obtain a lower bound on their minimum Hamming distances using their multilevel concatenated structure.

In Chapter 4, we provide enumeration formulae for all Euclidean and Hermitian self-dual and self-orthogonal Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, where $m_1, m_2, \cdots, m_\ell$ are positive integers satisfying $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. We also enumerate all Euclidean and Hermitian LCD Λ-MT codes

of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ when $\lambda_i \in \{1, -1\}$ and $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$.

The Hamming distance of a code is a measure of its error-detecting and error-correcting capabilities, and hence is an important parameter of the code. The greater is the Hamming distance of a code, higher are its error-detecting and error-correcting capabilities. A linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. The Hamming distance of the code $\mathcal{C}$ is defined as the smallest of the Hamming weights of its non-zero codewords. Given a linear code $\mathcal{C}$ of length n, dimension k and Hamming distance d over $\mathbb{F}_q$, the Griesmer bound is a lower bound on the length n of the code $\mathcal{C}$ in terms of q, d and k, while the Plotkin bound is an upper bound on the size q^k of the code $\mathcal{C}$ in terms of q, n and d, provided $qd > n(q-1)$. Linear codes attaining either the Griesmer bound or the Plotkin bound are optimal codes, and have attracted the attention of many coding theorists [44, 48, 50, 64]. Besides the length n, dimension k and Hamming distance d, another important parameter of the code $\mathcal{C}$ is its Hamming weight distribution, which is defined as the list $A_0 = 1, A_1, A_2, \cdots, A_n$, where A_j denotes the number of codewords in $\mathcal{C}$ having the Hamming weight j for $0 \leq j \leq n$. The Hamming weight distribution of a code is useful in studying its error-performance with respect to various communication channels [14, 24, 62]. Thus the problem of determination of the Hamming weight distribution of a code is of great interest [28, 30, 33, 48, 50, 56, 58, 64]. Despite all the efforts, this is considered as a very difficult problem in coding theory and is still an open problem for most of the linear codes [28, 33, 58]. Furthermore, if t denotes the number of integers j satisfying $1 \leq j \leq n$ and $A_j \neq 0$, then the code $\mathcal{C}$ is called a t-weight code. In general, the code with a smaller value of τ is called a few weight code. Nowadays, a lot of progress has been made by many coding theorists to construct various classes of linear codes with a few weights [42, 48, 56], as few weight codes have recently found applications in constructing authentication codes [29] and in designing secret sharing schemes with nice access

structures [23, 54, 60, 80]. In particular, codes with $t = 1$ are called equidistant or constant weight codes, which are useful in constructing combinatorial designs [35, 76] and generating goodsets of frequency hopping lists in radio networks [74]. Bonisoli [15] showed that each equidistant linear code of a given length over a finite field can be obtained by replicating a simplex code, possibly by appending zero coordinates and by applying a monomial linear transformation.

The support of a vector $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_q^n$, denoted by $\mathrm{supp}(v)$, is defined as the set $\mathrm{supp}(v) = \{i : 0 \leq i \leq n-1, v_i \neq 0\}$. Further, a vector $u \in \mathbb{F}_q^n$ is said to cover another vector $v \in \mathbb{F}_q^n$ if $\mathrm{supp}(v) \subseteq \mathrm{supp}(u)$. A codeword $c \in \mathcal{C}$ is said to be minimal if c covers only the codewords $ac \in \mathcal{C}$ for all $a \in \mathbb{F}_q$, and c does not cover any other codeword of the code $\mathcal{C}$. The linear code $\mathcal{C}$ is said to be minimal if every codeword of $\mathcal{C}$ is minimal. Minimal linear codes have recently found interesting applications in designing secret sharing schemes with nice access structures [19, 59, 80] and in secure two-party computation [2, 22], and these codes can be effectively decoded with a minimum distance decoding algorithm [1]. Thus the problem of finding minimal linear codes has been an interesting research direction in Coding Theory and Cryptography, and has recently attracted the attention of several researchers [1, 2, 22, 43, 58–60].

In Chapter 5, we explicitly determine all non-zero Hamming weights of codewords of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, where $m_1, m_2, \cdots, m_\ell$ are positive integers satisfying $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. We also explicitly determine Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights. Among these classes of few weight Λ-MT codes, we identify two classes of optimal equidistant Λ-MT codes meeting both Griesmer and Plotkin bounds, which have nice connections with combinatorial designs and projective geometry and are also useful in designing distributed storage systems. Besides this, we identify three other classes of few weight Λ-MT codes, which are useful in constructing secret

sharing schemes with nice access structures.

In Chapter 6, we extend the family of MT codes and study all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, where the block lengths $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers not necessarily coprime to q. More precisely, we investigate algebraic structures of Λ-MT codes of block lengths $(m_1, m_2, \cdots \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and their Galois duals (i.e., orthogonal complements with respect to the Galois inner product on $\mathbb{F}_q^n$). We derive necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD. We further provide a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by using the generalized discrete Fourier transform (GDFT), which gives rise to a method to construct these codes. We also provide necessary and sufficient conditions under which a Euclidean self-dual Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_{2^r}$ is a Type II code when $\lambda_i = 1$ and $m_i = n_i 2^a$ for $1 \leq i \leq \ell$, where $a \geq 0$ is an integer and $n_1, n_2, \cdots, n_\ell$ are odd positive integers satisfying $n_1 \equiv n_2 \equiv \cdots \equiv n_\ell \pmod 4$. Moreover, we develop generator theory for Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and show that each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ has a unique normalized generating set. With the help of a normalized generating set, we explicitly determine the dimension and a generating set of the Galois dual of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$. Besides this, we obtain several linear codes with best-known and optimal parameters from 1-generator Λ-MT codes over $\mathbb{F}_q$, where $2 \leq q \leq 7$. It is worth mentioning that these code parameters can not be attained by any of their subclasses (such as constacyclic and quasi-twisted codes) containing record breaker codes. This shows that this generalized family of MT codes over finite fields is more promising to find codes with better parameters than the current best-known codes.

In Chapter 7, we explicitly determine Hamming weights of all non-zero codewords

of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, where $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers not necessarily coprime to q. Using these results, we explicitly determine Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights. Among these classes of few weight Λ-MT codes, we identify two classes of optimal equidistant Λ-MT codes that attain the Griesmer as well as Plotkin bounds, and several other classes of Λ-MT codes that are useful in constructing secret sharing schemes with nice access structures.

1.2 Skew multi-twisted codes over finite fields and their Galois duals

Ore [63] generalized polynomial rings to skew-polynomial rings, which are non-commutative rings and have recently found applications in coding theory and cryptography [3, 16, 18, 81]. Algebraic codes that are defined as ideals (resp. modules) in a certain quotient ring (resp. quotient module) of skew polynomial rings are called skew constacyclic codes (resp. module skew codes). Since a skew polynomial ring is not a unique factorization domain, there are many more skew codes as compared to the corresponding commutative cases. This motivated many coding theorists to study various classes of skew codes [3, 13, 17, 18, 31, 48]. Towards this, Boucher et al. [17] introduced and studied skew cyclic codes over finite fields, which are generalizations of cyclic codes. Within this class, they obtained many linear codes with better parameters as compared to the previously best known linear codes. Abualrub et al. [3] studied skew quasi-cyclic (QC) codes and showed that parity-check polynomials for skew QC codes are unique up to similarity. In the same work, they obtained new codes with Hamming distances exceeding Hamming distances of the previously best known linear codes with comparable parameters. Later, Gao et al. [38] studied skew generalized quasi-cyclic (GQC) codes and derived an analogue of the Chinese

Remainder Theorem for skew polynomial rings using the factorization theory of ideals, which leads to a canonical decomposition of skew GQC codes. They also defined the parity-check polynomial, determined the dimension and obtained a lower bound on minimum Hamming distances of 1-generator skew GQC codes. Abualrub et al. [4] further studied skew GQC codes and derived some good classical and quantum codes from these codes.

In Chapter 8, we study skew analogues of MT codes over finite fields. More precisely, we introduce a new class of linear codes over finite fields, *viz.* skew MT codes over finite fields. We thoroughly investigate algebraic structures of skew MT codes and their Galois duals. We further view skew MT codes as direct sums of certain concatenated codes, and provide a method to construct these codes. We also determine a lower bound on their minimum Hamming distances using their multilevel concatenated structure. Moreover, we derive necessary and sufficient conditions under which a skew MT code is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD. We also develop generator theory for skew MT codes over finite fields, and obtain two lower bounds on their minimum Hamming distances. Besides this, we obtain many linear codes with best known and optimal parameters from 1-generator skew MT codes over $\mathbb{F}_8$ and $\mathbb{F}_9$.

1.3 Conclusion and future work

In Chapter 9, we mention a brief conclusion and discuss some interesting open problems in this direction.

2

Some Preliminaries

In this chapter, we shall state some basic definitions and results that are needed to derive our main results.

To begin with, in the following section, we will present some basic results from groups and geometry, which are useful in the enumeration of all Euclidean and Hermitian self-dual, self-orthogonal and linear with complementary dual (LCD) multi-twisted (MT) codes over finite fields. For this, we assume, throughout this chapter, that $\mathbb{F}_q$ is the finite field of order $q = p^r$, where p is a prime number and r is a positive integer.

2.1 Some basic results from groups and geometry

Let V be a finite-dimensional vector space over the finite field F. Let B be a σ-sesquilinear form on V, where σ is an automorphism of F. Then the pair (V, B) is called a formed space. From now on, throughout this section, we suppose that B is a reflexive and non-degenerate σ-sesquilinear form on V. The formed space (V, B) is called (i) a symplectic space if B is an alternating form on V, (ii) a unitary space if B is a Hermitian form on V, and (iii) an orthogonal space (or a finite geometry) if B is a symmetric form on V. Further, a subspace of the formed space (V, B) is defined as a pair (U, B_U), where U is a subspace of V and $B_U = B \restriction_{U \times U}$. For a subspace U of the formed space (V, B), let us define $U^\perp = \{v \in V : B(u, v) = 0 \text{ for all } u \in U\}$.

Theorem 2.1.1. *[40, 78] If (V, B) is a finite-dimensional reflexive and non-degenerate space over the field F and U is a subspace of V, then $U^\perp$ is a subspace of V and $dim_F U^\perp = dim_F V - dim_F U$.*

A subspace U of V is said to be (i) self-dual if it satisfies $U = U^\perp$, (ii) self-orthogonal (or totally isotropic) if it satisfies $U \subseteq U^\perp$, (iii) linear with complementary dual (or LCD or non-degenerate) if it satisfies $U \cap U^\perp = \{0\}$, and (iv) dual-containing if it satisfies $U^\perp \subseteq U$. The Witt index of V is defined as the dimension of a maximal self-orthogonal subspace of V.

Next let $\mathbb{F}_q^\mu$ be the μ-dimensional vector space consisting of all μ-tuples over the finite field $\mathbb{F}_q$. Then with respect to the standard inner product on $\mathbb{F}_q^\mu$, the following hold.

Theorem 2.1.2. *(a) [44, Th. 9.1.3] There exists a self-dual subspace (or equivalently, a linear code) of even length μ over $\mathbb{F}_q$ if and only if $(-1)^{\mu/2}$ is a square in $\mathbb{F}_q$. Furthermore, if μ is an even integer and $(-1)^{\mu/2}$ is not a square in $\mathbb{F}_q$, then the dimension of a maximal self-orthogonal subspace of length μ over $\mathbb{F}_q$ is $(\mu - 2)/2$. If μ is an odd integer, then the dimension of a maximal self-orthogonal subspace of length μ over $\mathbb{F}_q$ is $(\mu - 1)/2$.*

(b) *[65, p. 217] Let $\mu \geq 2$ be an even integer, and let $(-1)^{\mu/2}$ be a square in $\mathbb{F}_q$. Then the number of distinct self-dual subspaces of even length μ over $\mathbb{F}_q$ is given by*

- $\prod_{a=1}^{\frac{\mu}{2}-1}(q^a+1)$ *when q is even.*
- $\prod_{a=0}^{\frac{\mu}{2}-1}(q^a+1)$ *when q is odd.*

In the following theorem, we state some basic properties of finite-dimensional symplectic spaces over finite fields.

Theorem 2.1.3. *[78] Let (V, B) be a μ-dimensional symplectic space over $\mathbb{F}_q$. Then the dimension μ of V is even and the following hold.*

(a) *The Witt index of V is $\frac{\mu}{2}$.*

(b) *For $0 \leq k \leq \frac{\mu}{2}$, the number of distinct k-dimensional self-orthogonal subspaces of V is given by*

$$\prod_{a=0}^{k-1}\frac{(q^{\mu-2a}-1)}{(q^{a+1}-1)} = \begin{bmatrix}\mu/2\\ k\end{bmatrix}_q \prod_{a=0}^{k-1}(q^{\frac{\mu}{2}-a}+1),$$

where $\begin{bmatrix}\mu/2\\ k\end{bmatrix}_q = \prod_{d=0}^{k-1}\frac{(q^{\mu/2}-q^d)}{(q^k-q^d)}$ is the q-binomial coefficient.

In the following theorem, we state some basic properties of finite-dimensional unitary spaces over finite fields.

Theorem 2.1.4. *[78] Let (V, B) be a μ-dimensional unitary space over $\mathbb{F}_{q^2}$. Let ν be the Witt index of (V, B). Then we have the following:*

(a) *The Witt index ν of V is given by* $\nu = \begin{cases} \frac{\mu}{2} & \text{if } \mu \text{ is even;} \\ \frac{\mu-1}{2} & \text{if } \mu \text{ is odd.} \end{cases}$

(b) For $0 \leq k \leq \nu$, the number of distinct k-dimensional self-orthogonal subspaces of V is given by

$$\frac{\prod_{a=\mu+1-2k}^{\mu}(q^a-(-1)^a)}{\prod_{j=1}^{k}(q^{2j}-1)}.$$

To study orthogonal spaces, let q be an odd prime power, and let V be a finite-dimensional vector space over $\mathbb{F}_q$. Then the map $\varphi : V \to \mathbb{F}_q$ is called a quadratic map on V if it satisfies

(i) $\varphi(av_1) = a^2\varphi(v_1)$ for all $a \in \mathbb{F}_q$ and $v_1 \in V$, and

(ii) the map $B_\varphi : V \times V \to \mathbb{F}_q$, defined by $B_\varphi(v_1, v_2) = \varphi(v_1 + v_2) - \varphi(v_1) - \varphi(v_2)$ for all $v_1, v_2 \in V$, is a symmetric bilinear form on V.

The pair (V, φ) is called a quadratic space over $\mathbb{F}_q$. The quadratic space (V, φ) over $\mathbb{F}_q$ is called non-degenerate if it satisfies $\varphi^{-1}(0) \cap V^\perp = \{0\}$, where $V^\perp = \{v \in V : B_\varphi(v, u) = 0 \text{ for all } u \in V\}$. If the quadratic space (V, φ) is non-degenerate, then the associated orthogonal space (V, B_φ) is called a finite geometry over $\mathbb{F}_q$. On the other hand, with every symmetric bilinear form B on a vector space V over $\mathbb{F}_q$, one can associate the following quadratic map:

$$Q_B(v) = \frac{1}{2}B(v, v) \quad \text{for each} \quad v \in V.$$

In the following theorem, we state some basic properties of non-degenerate quadratic spaces over a finite field of odd characteristic.

Theorem 2.1.5. *[65, 78] Let (V, φ) be a μ-dimensional non-degenerate quadratic space over the finite field $\mathbb{F}_q$ having an odd characteristic. Let ν be the Witt index of (V, φ). Then we have the following:*

(a) The Witt index ν of V is given by

$$\nu = \begin{cases} \frac{\mu-1}{2} & \text{if } \mu \text{ is odd;} \\ \frac{\mu}{2} & \text{if } \mu \text{ is even and } q \equiv 1 \pmod 4 \text{ or } \mu \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ \frac{\mu-2}{2} & \text{if } \mu \equiv 2 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

(b) For $0 \leq k \leq \nu$, the number of distinct k-dimensional self-orthogonal (or totally singular) subspaces of V is given by

$$\begin{bmatrix} \nu \\ k \end{bmatrix}_q \prod_{a=0}^{k-1} (q^{\nu-\varsigma-a} + 1),$$

where $\begin{bmatrix} \nu \\ k \end{bmatrix}_q = \prod_{d=0}^{k-1} (q^\nu - q^d)/(q^k - q^d)$ is the q-binomial coefficient and $\varsigma = 2\nu - \mu + 1$. (Note that $\varsigma = 1$ if $\nu = \frac{\mu}{2}$, $\varsigma = -1$ if $\nu = \frac{\mu-2}{2}$ and $\varsigma = 0$ if $\nu = \frac{\mu-1}{2}$.)

Next we recall the following well-known result:

Lemma 2.1.6. *If n, k are integers satisfying $0 \leq k \leq n$ and q is a prime power, then the number of distinct k-dimensional subspaces of an n-dimensional vector space over $\mathbb{F}_q$ is given by the q-binomial coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \left(\frac{q^n - q^i}{q^k - q^i} \right).$$

In the next section, we will state some basic results on character sums over finite fields, which are useful in the determination of Hamming weights of non-zero codewords of multi-twisted (MT) codes over finite fields.

2.2 Some basic results on character sums over finite fields

An additive character of $\mathbb{F}_q$ is defined as a group homomorphism from the additive group of the finite field $\mathbb{F}_q$ into the multiplicative group $\mathbb{C}^*$ of the field of complex numbers. The canonical additive character χ of $\mathbb{F}_q$ is defined as

$$\chi(y) = e^{\frac{2\pi\iota Tr_{\mathbb{F}_q/\mathbb{F}_p}(y)}{p}} \quad \text{for all } y \in \mathbb{F}_q.$$

Note that $\chi(0) = 1$. It is well-known that

$$\sum_{y\in\mathbb{F}_q} \chi(ay) = \begin{cases} q & \text{if } a = 0; \\ 0 & \text{if } a \neq 0. \end{cases} \tag{2.1}$$

Let E be a finite field extension of $\mathbb{F}_q$, and let μ be the canonical additive character of E, defined as

$$\mu(z) = e^{\frac{2\pi\iota Tr_{E/\mathbb{F}_p}(z)}{p}} \quad \text{for all } z \in E.$$

One can easily observe that

$$\mu(z) = \chi(Tr_{E/\mathbb{F}_q}(z)) \quad \text{for all } z \in E. \tag{2.2}$$

A multiplicative character of $\mathbb{F}_q$ is defined as a group homomorphism from the multiplicative group $\mathbb{F}_q^*$ of the finite field $\mathbb{F}_q$ into $\mathbb{C}^*$. The trivial multiplicative character ψ_0 of $\mathbb{F}_q$ is defined as $\psi_0(y) = 1$ for all $y \in \mathbb{F}_q^*$. It is well-known [51, p. 192] that

$$\sum_{y\in\mathbb{F}_q^*} \psi(y) = \begin{cases} q-1 & \text{if } \psi = \psi_0; \\ 0 & \text{otherwise.} \end{cases} \tag{2.3}$$

Further, if ψ_1 and ψ_2 are multiplicative characters of $\mathbb{F}_q$, then the mapping $\psi_1\psi_2 : \mathbb{F}_q^* \to \mathbb{C}^*$, defined as

$$(\psi_1\psi_2)(y) = \psi_1(y)\psi_2(y) \quad \text{for all} \quad y \in \mathbb{F}_q^*,$$

is also a multiplicative character of $\mathbb{F}_q$. If ψ is a multiplicative character of $\mathbb{F}_q$, then the conjugate character $\overline{\psi}$ of ψ is defined as $\overline{\psi}(y) = \overline{\psi(y)}$ for $y \in \mathbb{F}_q^*$, where $\overline{\ }$ denotes the complex conjugation. Further, it is easy to see that $\overline{\psi} = \psi^{-1}$. If β is a primitive element of $\mathbb{F}_q$, then the map $\phi : \mathbb{F}_q^* \to \mathbb{C}^*$, defined as

$$\phi(\beta^j) = e^{\frac{2\pi\iota j}{q-1}} \qquad \text{for} \quad 0 \le j \le q-2,$$

is a multiplicative character of $\mathbb{F}_q$. It is well-known [51, p. 191] that the set $\widehat{\mathbb{F}_q^*}$ of multiplicative characters of $\mathbb{F}_q$ is a cyclic group of order $q-1$, generated by ϕ.

For an additive character χ and a multiplicative character ψ of $\mathbb{F}_q$, the Gauss sum over the finite field $\mathbb{F}_q$ is defined as

$$G(\psi, \chi) = \sum_{y \in \mathbb{F}_q^*} \psi(y)\chi(y).$$

It is easy to see that

$$G(\overline{\psi}, \chi) = \psi(-1)\overline{G(\psi, \chi)} \ \text{ and } \ G(\psi_0, \chi) = -1. \tag{2.4}$$

Further, it is well-known that

$$\chi(y) = \frac{1}{q-1} \sum_{\psi \in \widehat{\mathbb{F}_q^*}} G(\overline{\psi}, \chi)\psi(y) \text{ for each } y \in \mathbb{F}_q^*, \tag{2.5}$$

which may be interpreted as the Fourier expansion of the restriction of χ to $\mathbb{F}_q^*$

in terms of the multiplicative characters of $\mathbb{F}_q$ with Gauss sums as Fourier coefficients. Now the following theorem determines the Gauss sum $G(\psi, \chi)$ when ψ is the quadratic character of $\mathbb{F}_q$.

Theorem 2.2.1. *[11] Let $q = p^r$, where p is a prime and r is a positive integer. If ψ is the quadratic character of $\mathbb{F}_q$ and χ is the canonical additive character of $\mathbb{F}_q$, then we have*

$$G(\psi, \chi) = (-1)^{r-1} \iota^{\frac{r(p-1)^2}{4}} \sqrt{q} = \begin{cases} (-1)^{r-1}\sqrt{q} & \text{if } p \equiv 1 \ (mod\ 4); \\ (-1)^{r-1}\iota^r\sqrt{q} & \text{if } p \equiv 3 \ (mod\ 4). \end{cases}$$

The following theorem determines the Gauss sum $G(\psi, \chi)$ in the semi-primitive case, i.e., when there exists a positive integer t satisfying $p^t \equiv -1 \pmod{M}$, where M is the multiplicative order of ψ.

Theorem 2.2.2. *[11] Let $q = p^r$, where p is a prime and r is a positive integer. Let χ be the canonical additive character of $\mathbb{F}_q$, and let ψ be a multiplicative character of $\mathbb{F}_q$ having order $M > 2$. Suppose that there exists a least positive integer t satisfying $p^t \equiv -1 \ (mod\ M)$. Then we have $r = 2t\gamma$ for some positive integer γ. Furthermore, for $1 \leq i \leq M-1$, we have*

$$G(\psi^i, \chi) = \begin{cases} (-1)^i\sqrt{q} & \text{if } M \text{ is even and } \frac{p\gamma(p^t+1)}{M} \text{ is odd}; \\ (-1)^{\gamma-1}\sqrt{q} & \text{otherwise.} \end{cases} \tag{2.6}$$

3

Multi-twisted codes over finite fields and their dual codes

3.1 Introduction

Let $\mathbb{F}_q$ denote the finite field of order q, and let $m_1, m_2, \cdots, m_\ell$ be positive integers satisfying $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. Let $n = m_1 + m_2 + \cdots + m_\ell$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. In this chapter, we shall thoroughly investigate algebraic structures of Λ-multi-twisted codes (Λ-MT) of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by writing a canonical form decomposition for these codes. We shall also study their dual codes and

derive necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) self-dual, (ii) self-orthogonal and (iii) linear with complementary dual (LCD) by placing Euclidean and Hermitian inner products on $\mathbb{F}_q^n$. We shall also develop generator theory for these codes and explicitly determine generating sets of Euclidean and Hermitian dual codes of some Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ from their generating sets. We shall also provide a trace description for these codes, which gives rise to a construction method for these codes. We shall also obtain two lower bounds on their minimum Hamming distances.

This chapter is structured as follows: In Section 3.2, we study algebraic structures of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$. In Section 3.3, we study their dual codes with respect to Euclidean and Hermitian inner products on $\mathbb{F}_q^n$, and derive necessary and sufficient conditions for a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ to be Euclidean or Hermitian (i) self-dual, (ii) self-orthogonal and (iii) linear with complementary dual (LCD) (Theorems 3.3.3 and 3.3.4). In Section 3.4, we determine the parity-check polynomial of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, and obtain a BCH type bound on their minimum Hamming distances (Theorems 3.4.1 and 3.4.3). We express generating sets of Euclidean and Hermitian dual codes of some Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ in terms of their generating sets (Theorem 3.4.2). We also obtain a lower bound on the dimension of a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, which is also invariant under the Ω-MT shift operator on $\mathbb{F}_q^n$, where $\Lambda \neq \Omega$ (Theorem 3.4.4). We also derive some sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is either Euclidean or Hermitian LCD (Theorems 3.4.5 and 3.4.6). In Section 3.5, we provide a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by viewing these codes as direct sums of certain concatenated codes, which leads to a method to construct these

codes (Theorem 3.5.2). We also obtain a lower bound on their minimum Hamming distances using their multilevel concatenated structure (Theorem 3.5.3).

3.2 Algebraic structures of MT codes over finite fields

In this section, we shall thoroughly investigate algebraic structures of MT codes over $\mathbb{F}_q$, whose block lengths are positive integers coprime to q. For this, we assume, throughout this chapter, that $\mathbb{F}_q$ is the finite field of order $q = p^r$, where p is a prime number and r is a positive integer. Let $m_1, m_2, \cdots, m_\ell$ be positive integers coprime to q, and let $n = m_1 + m_2 + \cdots + m_\ell$. Let $\mathbb{F}_q^n$ denote the vector space consisting of all n-tuples over $\mathbb{F}_q$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Then a Λ-multi-twisted (MT) module V is an $\mathbb{F}_q[x]$-module of the form

$$V = \prod_{i=1}^{\ell} V_i,$$

where $V_i = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \lambda_i \rangle}$ for $1 \leq i \leq \ell$. We further note that there exists an $\mathbb{F}_q$-linear vector space isomorphism from $\mathbb{F}_q^n$ onto V. From this point on, we shall represent each element $a \in \mathbb{F}_q^n$ as $a = (a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \cdots, a_{2,m_2-1}; \cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1})$ and the corresponding element $a(x) \in V$ as $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x))$, where $a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j} x^j \in V_i$ for $1 \leq i \leq \ell$.

Definition 3.2.1. *[5] A Λ-multi-twisted (MT) code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is defined as an $\mathbb{F}_q[x]$-submodule of the Λ-MT module V. Equivalently, a linear code $\mathcal{C}$ of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is called a Λ-MT code if $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots\cdots, c_{\ell,m_\ell-1}) \in \mathcal{C}$, then its Λ-MT shift $T_\Lambda(c) = (\lambda_1 c_{1,m_1-1}, c_{1,0}, \cdots, c_{1,m_1-2}; \lambda_2 c_{2,m_2-1}, c_{2,0}, \cdots, c_{2,m_2-2}; \cdots; \lambda_\ell c_{\ell,m_\ell-1}, c_{\ell,0}, \cdots, c_{\ell,m_\ell-2})$ is also a codeword of $\mathcal{C}$.*

In particular, when $m_1 = m_2 = \cdots = m_\ell$ and $\lambda_1 = \lambda_2 = \cdots = \lambda_\ell$, Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are permutation-equivalent to quasi-twisted (QT) codes of length $m_1\ell$ over $\mathbb{F}_q$. When $\lambda_i = 1$ for $1 \leq i \leq \ell$, Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ coincide with generalized quasi-cyclic (GQC) codes, which are first defined and studied by Siap and Kulhan [73]. Furthermore, when $m_1 = m_2 = \cdots = m_\ell$ and $\lambda_i = 1$ for $1 \leq i \leq \ell$, Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are permutation-equivalent to quasi-cyclic (QC) codes of length $m_1\ell$ and index ℓ over $\mathbb{F}_q$. Besides this, when $\ell = 1$, Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are λ_1-constacyclic codes of length m_1 over $\mathbb{F}_q$.

Now we shall express Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ as direct sums of certain linear codes of length ℓ over finite field extensions of $\mathbb{F}_q$. To do this, let $g_1(x), g_2(x), \cdots, g_\rho(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ over $\mathbb{F}_q$. For $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$, let us define

$$\epsilon_{w,i} = \begin{cases} 1 & \text{if } g_w(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise.} \end{cases}$$

Then for $1 \leq i \leq \ell$, we note that $x^{m_i} - \lambda_i = \prod_{w=1}^{\rho} g_w(x)^{\epsilon_{w,i}}$ is the irreducible factorization of $x^{m_i} - \lambda_i$ over $\mathbb{F}_q$. Now for each i, by applying the Chinese Remainder Theorem, we get

$$V_i \simeq \bigoplus_{w=1}^{\rho} \epsilon_{w,i} F_w$$

with $F_w = \frac{\mathbb{F}_q[x]}{\langle g_w(x) \rangle}$ for $1 \leq w \leq \rho$; the corresponding ring isomorphism from V_i onto $\bigoplus_{w=1}^{\rho} \epsilon_{w,i} F_w$ is given by $a_i(x) \mapsto \sum_{w=1}^{\rho} \Big(\epsilon_{w,i}(a_i(x) + \langle g_w(x) \rangle) \Big)$ for each $a_i(x) \in V_i$. This

further implies that

$$V \simeq \bigoplus_{w=1}^{\rho} \Big(\underbrace{\epsilon_{w,1}F_w, \epsilon_{w,2}F_w, \cdots, \epsilon_{w,\ell}F_w}_{\mathcal{G}_w} \Big),$$

where the ring isomorphism from V onto $\bigoplus_{w=1}^{\rho} \mathcal{G}_w$ is given by

$$a(x) \mapsto \sum_{w=1}^{\rho} \Big(\epsilon_{w,1}(a_1(x) + \langle g_w(x) \rangle), \epsilon_{w,2}(a_2(x) + \langle g_w(x) \rangle), \cdots, \epsilon_{w,\ell}(a_\ell(x) + \langle g_w(x) \rangle) \Big)$$

for each $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V$. If $d_w = \deg\, g_w(x)$, then we see that $F_w \simeq \mathbb{F}_{q^{d_w}}$ for $1 \leq w \leq \rho$. Next let $\epsilon_w = \sum_{i=1}^{\ell} \epsilon_{w,i}$ for each w. It is easy to see that for $1 \leq w \leq \rho$, the set $\mathcal{G}_w = \Big(\epsilon_{w,1}F_w, \epsilon_{w,2}F_w, \cdots, \epsilon_{w,\ell}F_w \Big)$ is an ϵ_w-dimensional vector space over F_w. From the above discussion, we deduce the following:

Theorem 3.2.2. *Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$, which is finitely-generated as an $\mathbb{F}_q[x]$-submodule of V by $\{(a_{d,1}(x), a_{d,2}(x), \cdots, a_{d,\ell}(x)) : 1 \leq d \leq \mu\} \subseteq \mathcal{C}$. Then the code $\mathcal{C}$ can be uniquely expressed as $\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w$, where for $1 \leq w \leq \rho$, the code $\mathcal{C}_w$ is an F_w-subspace of $\mathcal{G}_w$, given by*

$$\mathcal{C}_w = Span_{F_w}\{(\epsilon_{w,1}a_{d,1}(\delta_w), \epsilon_{w,2}a_{d,2}(\delta_w), \cdots, \epsilon_{w,\ell}a_{d,\ell}(\delta_w)) : 1 \leq d \leq \mu\}$$

with δ_w as a zero of $g_w(x)$ in F_w, (the codes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ are called the constituents of $\mathcal{C}$). Furthermore, we have

$$dim_{\mathbb{F}_q}\mathcal{C} = \sum_{w=1}^{\rho} dim_{F_w}\mathcal{C}_w deg\ g_w(x).$$

Conversely, if $\mathcal{D}_w$ is an F_w-subspace of $\mathcal{G}_w$ for $1 \leq w \leq \rho$, then $\mathcal{D} = \bigoplus_{w=1}^{\rho} \mathcal{D}_w$ is a Λ-MT code of length n over $\mathbb{F}_q$.

We shall illustrate the above theorem in the following example:

Example 3.2.1. *Let* $q = 7$, $\ell = 3$, $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $\Lambda = (2, 6, 4)$ *and* $\mathbb{F}_7 = \mathbb{Z}_7$. *Here we have* $V = V_1 \times V_2 \times V_3 = \frac{\mathbb{F}_7[x]}{\langle x^2-2\rangle} \times \frac{\mathbb{F}_7[x]}{\langle x^3-6\rangle} \times \frac{\mathbb{F}_7[x]}{\langle x^4-4\rangle}$. *Further, we see that the irreducible factorizations of the polynomials* $x^2 - 2$, $x^3 - 6$ *and* $x^4 - 4$ *over* $\mathbb{F}_7$ *are given by* $x^2 - 2 = (x + 3)(x + 4)$, $x^3 - 6 = (x + 1)(x + 2)(x + 4)$ *and* $x^4 - 4 = (x + 3)(x + 4)(x^2 + 2)$, *respectively. Now let* $g_1(x) = x + 1, g_2(x) = x + 2, g_3(x) = x + 3, g_4(x) = x + 4$ *and* $g_5(x) = x^2 + 2$. *Then we have* $F_1 \simeq F_2 \simeq F_3 \simeq F_4 \simeq \mathbb{F}_7$ *and* $F_5 \simeq \mathbb{F}_{49}$. *From this and by applying the Chinese remainder theorem, we get* $V_1 \simeq \{0\} \oplus \{0\} \oplus F_3 \oplus F_4 \oplus \{0\}$, $V_2 \simeq F_1 \oplus F_2 \oplus \{0\} \oplus F_4 \oplus \{0\}$, $V_3 \simeq \{0\} \oplus \{0\} \oplus F_3 \oplus F_4 \oplus F_5$, *which implies that* $V \simeq (\{0\}, F_1, \{0\}) \oplus (\{0\}, F_2, \{0\}) \oplus (F_3, \{0\}, F_3) \oplus (F_4, F_4, F_4) \oplus (\{0\}, \{0\}, F_5)$. *Now if* $\mathcal{C} \subseteq V$ *is a* Λ*-MT code of length* 9 *over* $\mathbb{F}_7$ *generated by* $\big\{(a_{d,1}(x), a_{d,2}(x), a_{d,3}(x)) : 1 \leq d \leq \mu\big\} \subseteq V$, *then we have*

$$\mathcal{C} = \bigoplus_{w=1}^{5} \mathcal{C}_w,$$

where the constituents $\mathcal{C}_w$*'s of* $\mathcal{C}$ *are given by*

$$\mathcal{C}_1 = Span_{F_1}\{(0, a_{d,2}(6), 0) : 1 \leq d \leq \mu\},$$

$$\mathcal{C}_2 = Span_{F_2}\{(0, a_{d,2}(5), 0) : 1 \leq d \leq \mu\},$$

$$\mathcal{C}_3 = Span_{F_3}\{(a_{d,1}(4), 0, a_{d,3}(4)) : 1 \leq d \leq \mu\},$$

$$\mathcal{C}_4 = Span_{F_4}\{(a_{d,1}(3), a_{d,2}(3), a_{d,3}(3)) : 1 \leq d \leq \mu\}$$

and

$$\mathcal{C}_5 = Span_{F_5}\{(0, 0, a_{d,3}(\delta_5)) : 1 \leq d \leq \mu\}$$

with δ_5 *as a zero of the polynomial* $g_5(x) = x^2 + 2$ *in* $F_5 \simeq \mathbb{F}_{49}$.

Next in the following theorem, we enumerate all Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 3.2.3. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Then the total number of distinct Λ-MT codes of length n over $\mathbb{F}_q$ is given by*

$$N_\Lambda = \prod_{w=1}^{\rho} \left(1 + \sum_{b=1}^{\epsilon_w} \begin{bmatrix} \epsilon_w \\ b \end{bmatrix}_{q^{d_w}} \right),$$

where $d_w = deg\ g_w(x)$ for each w.

Proof. By Theorem 3.2.2, we see that all the distinct Λ-MT codes of length n over $\mathbb{F}_q$ are given by $\bigoplus_{w=1}^{\rho} \mathcal{C}_w$, where $\mathcal{C}_w$ runs over F_w-subspaces of $\mathcal{G}_w$ for $1 \leq w \leq \rho$. Now by using the fact that $F_w \simeq \mathbb{F}_{q^{d_w}}$ and by applying Lemma 2.1.6, the desired result follows immediately. □

Remark 3.2.4. *It is easy to see that some Λ-MT codes can also be viewed as Ω-MT codes, where $\Omega \neq \Lambda$. For example, when $q = 7$, $m_1 = 2$ and $m_2 = 1$, the linear code $\mathcal{C}$ with the basis set $\{(1, 0; 0), (0, 1; 0)\}$ is a $(2, 1)$-MT as well as $(4, 1)$-MT code of length 3 over $\mathbb{F}_7$. Thus the total number of distinct MT codes of length n over $\mathbb{F}_q$ is not equal to $(q-1)^\ell N_\Lambda$.*

3.3 Euclidean and Hermitian dual codes of MT codes

In this section, we shall study Euclidean and Hermitian dual codes of Λ-MT codes of length n over $\mathbb{F}_q$. To do this, we first recall the definitions of Euclidean and Hermitian inner products on $\mathbb{F}_q^n$ as follows:

The Euclidean inner product on $\mathbb{F}_q^n$ is a mapping $\langle \cdot, \cdot \rangle_0 : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, defined as

$$\langle a, b \rangle_0 = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i - 1} a_{i,j} b_{i,j} \text{ for all } a, b \in \mathbb{F}_q^n.$$

Note that the Euclidean inner product $\langle \cdot, \cdot \rangle_0$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_q^n$. If $\mathcal{C}$ is a Λ-MT code of length n over $\mathbb{F}_q$, then its Euclidean dual code

$\mathcal{C}^{\perp_0}$ is defined as $\mathcal{C}^{\perp_0} = \{a \in \mathbb{F}_q^n : \langle a, c\rangle_0 = 0 \text{ for all } c \in \mathcal{C}\}$. One can easily observe that $\mathcal{C}^{\perp_0}$ is a Λ^{-1}-MT code of length n over $\mathbb{F}_q$, where $\Lambda^{-1} = (\lambda_1^{-1}, \lambda_2^{-1}, \cdots, \lambda_\ell^{-1})$.

The Hermitian inner product on $\mathbb{F}_q^n$ is defined only when r is an even integer and is a mapping $\langle \cdot, \cdot \rangle_{\frac{r}{2}} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, defined as

$$\langle a, b\rangle_{\frac{r}{2}} = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} a_{i,j} b_{i,j}^{p^{\frac{r}{2}}} \text{ for all } a, b \in \mathbb{F}_q^n.$$

Note that the Hermitian inner product $\langle \cdot, \cdot \rangle_{\frac{r}{2}}$ is a non-degenerate and reflexive $\sigma_{\frac{r}{2}}$-sesquilinear form on $\mathbb{F}_q^n$, where $\sigma_{\frac{r}{2}}$ is an automorphism of $\mathbb{F}_q$, defined as $\sigma(b) = b^{p^{\frac{r}{2}}}$ for each $b \in \mathbb{F}_q$. If $\mathcal{C}$ is a Λ-MT code of length n over $\mathbb{F}_q$, then its Hermitian dual code $\mathcal{C}^{\perp_{\frac{r}{2}}}$ is defined as $\mathcal{C}^{\perp_{\frac{r}{2}}} = \{a \in \mathbb{F}_q^n : \langle a, c\rangle_{\frac{r}{2}} = 0 \text{ for all } c \in \mathcal{C}\}$. One can easily observe that $\mathcal{C}^{\perp_{\frac{r}{2}}}$ is a $\Lambda^{-p^{\frac{r}{2}}}$-MT code of length n over $\mathbb{F}_q$, where $\Lambda^{-p^{\frac{r}{2}}} = (\lambda_1^{-p^{\frac{r}{2}}}, \lambda_2^{-p^{\frac{r}{2}}}, \cdots, \lambda_\ell^{-p^{\frac{r}{2}}})$.

From this point on, throughout this chapter, let k be an integer satisfying either $k = 0$ or $k = \frac{r}{2}$ when r is even, and let us define $\Lambda^{-p^k} = (\lambda_1^{-p^k}, \lambda_2^{-p^k}, \cdots, \lambda_\ell^{-p^k})$.

Next to study Euclidean and Hermitian dual codes of MT codes in more detail, let m be the order of the polynomial $\text{lcm}[x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell]$ in $\mathbb{F}_q[x]$, i.e., m is the smallest positive integer such that the polynomial $\text{lcm}[x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell]$ divides $x^m - 1$ in $\mathbb{F}_q[x]$. It is easy to observe that $m = \text{lcm}[m_1 O(\lambda_1), m_2 O(\lambda_2), \cdots, m_\ell O(\lambda_\ell)]$ and that $T_\Lambda^m = T_{\Lambda^{-p^k}}^m = I$, where I is the identity operator on $\mathbb{F}_q^n$ and $O(\lambda_i)$ denotes the multiplicative order of λ_i for each i.

Recall that the dual code $\mathcal{C}^{\perp_k}$ is a Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$, i.e., $\mathcal{C}^{\perp_k}$ is a linear code of length n over $\mathbb{F}_q$ satisfying the following: if $d = (d_{1,0}, d_{1,1}, \cdots, d_{1,m_1-1}; d_{2,0}, d_{2,1}, \cdots, d_{2,m_2-1}; \cdots; d_{\ell,0}, d_{\ell,1}, \cdots, d_{\ell,m_\ell-1}) \in \mathcal{C}^{\perp_k}$, then its Λ^{-p^k}-MT shift $T_{\Lambda^{-p^k}}(d)$ $= (\lambda_1^{-p^k} d_{1,m_1-1}, d_{1,0}, \cdots, d_{1,m_1-2}; \lambda_2^{-p^k} d_{2,m_2-1}, d_{2,0}, \cdots\cdots, d_{2,m_2-2}; \cdots; \lambda_\ell^{-p^k} d_{\ell,m_\ell-1}, d_{\ell,0}, \cdots, d_{\ell,m_\ell-2}) \in \mathcal{C}^{\perp_k}$. Equivalently, $\mathcal{C}^{\perp_k}$ is an $\mathbb{F}_q[x]$-submodule of the Λ^{-p^k}-MT module $V' = \prod_{i=1}^{\ell} V_i'$, where $V_i' = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \lambda_i^{-p^k} \rangle}$ for $1 \leq i \leq \ell$. Next let us define a

conjugation map $\mathcal{T}_k : \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle} \to \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$ as

$$\mathcal{T}_k(d(x)) = \sum_{j=0}^{m-1} d_j^{p^k} x^{-j} \text{ for each } d(x) = \sum_{j=0}^{m-1} d_j x^j \in \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}.$$

(Here we have $x^{-1} = x^{m-1} \in \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$). Further, for $1 \le i \le \ell$, define a conjugation map $\mathcal{T}_k^{(i)} : V_i' \to V_i$ as

$$\mathcal{T}_k^{(i)}(b_i(x)) = \sum_{j=1}^{m_i-1} b_{i,j}^{p^k} x^{-j}$$

for each $b_i(x) = \sum_{j=1}^{m_i-1} b_{i,j}x^j \in V_i'$, where $x^{-1} = \lambda_i^{-1} x^{m_i-1} \in V_i$.

Next we define a mapping $(\cdot,\cdot)_k : V \times V' \longrightarrow \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$ as

$$(a(x), b(x))_k := \sum_{i=1}^{\ell} \lambda_i a_i(x) \mathcal{T}_k^{(i)}(b_i(x)) \Big(\frac{x^m-1}{x^{m_i}-\lambda_i} \Big)$$

for $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V$ and $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in V'$, where V and V' are viewed as $\frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$-modules. Now the following lemma relates the map $(a(x), b(x))_k$ with Euclidean and Hermitian inner products on $\mathbb{F}_q^n$.

Lemma 3.3.1. *(a) For $a(x) \in V$ and $b(x) \in V'$, we have*

$$\begin{aligned}(a(x), b(x))_k &= \langle a, b\rangle_k + \big\langle a, T_{\Lambda^{-p^k}}(b)\big\rangle_k x + \cdots + \big\langle a, T^{m-1}_{\Lambda^{-p^k}}(b)\big\rangle_k x^{m-1} \\ &= \langle a, b\rangle_k + \big\langle T^{m-1}_{\Lambda}(a), b\big\rangle_k x + \cdots + \big\langle T_{\Lambda}(a), b\big\rangle_k x^{m-1} \text{ in } \tfrac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}.\end{aligned}$$

(b) The mapping $(\cdot,\cdot)_k$ is a non-degenerate and Hermitian $\mathcal{T}_k$-sesquilinear form on $V \times V'$.

Proof. (a) To prove this, we first write $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x))$ and $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x))$, where $a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j}x^j \in V_i$ and $b_i(x) = \sum_{j=0}^{m_i-1} b_{i,j}x^j \in V_i'$ for each i. For $1 \le i \le \ell$, we observe that $\frac{\lambda_i(x^m-1)}{x^{m_i}-\lambda_i} = 1 + \lambda_i^{-1}x^{m_i} + \lambda_i^{-2}x^{2m_i} + \cdots + \lambda_i^{-(\frac{m}{m_i}-2)} x^{(\frac{m}{m_i}-2)m_i} + \lambda_i x^{(\frac{m}{m_i}-1)m_i}$. Using this, we get $(a(x), b(x))_k = \langle a, b\rangle_k +$

$\left\langle a, T_{\Lambda^{-p^k}}(b)\right\rangle_k x + \cdots + \left\langle a, T^{m-1}_{\Lambda^{-p^k}}(b)\right\rangle_k x^{m-1}$. As $\left\langle a, T^j_{\Lambda^{-p^k}}(b)\right\rangle_k = \left\langle T^{m-j}_{\Lambda}(a), b\right\rangle_k$ for $0 \leq j \leq m-1$, we get $(a(x), b(x))_k = \langle a, b\rangle_k + \left\langle T^{m-1}_{\Lambda}(a), b\right\rangle_k x + \cdots + \langle T_\Lambda(a), b\rangle_k x^{m-1}$.

(b) It is easy to observe that $(\cdot,\cdot)_k$ is a Hermitian $\mathcal{T}_k$-sesquilinear form on $V \times V'$. To prove the non-degeneracy of $(\cdot,\cdot)_k$, suppose that $(a(x), b(x))_k = 0$ for all $b(x) \in V'$. Here we need to show that $a(x) = 0$. For this, by part (a), we see that $(a(x), b(x))_k = \langle a, b\rangle_k + \left\langle a, T_{\Lambda^{-p^k}}(b)\right\rangle_k x + \cdots + \left\langle a, T^{m-1}_{\Lambda^{-p^k}}(b)\right\rangle_k x^{m-1} = 0$ for all $b \in \mathbb{F}_q^n$. This implies that $\langle a, b\rangle_k = \left\langle a, T_{\Lambda^{-p^k}}(b)\right\rangle_k = \cdots = \left\langle a, T^{m-1}_{\Lambda^{-p^k}}(b)\right\rangle_k = 0$ for all $b \in \mathbb{F}_q^n$. As $\langle\cdot,\cdot\rangle_k$ is a non-degenerate bilinear form on $\mathbb{F}_q^n$, we get $a = 0$, which gives $a(x) = 0$. This proves (b).

□

From the above lemma, we deduce the following:

Proposition 3.3.2. *If $\mathcal{C} \subseteq V$ is a Λ-MT code of length n over $\mathbb{F}_q$, then the dual code $\mathcal{C}^{\perp_k} \subseteq V'$ is a Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$ and is given by*

$$\mathcal{C}^{\perp_k} = \{b(x) \in V' : (a(x), b(x))_k = 0 \text{ for all } a(x) \in \mathcal{C}\}.$$

Further, a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is said to be

(i) Euclidean (resp. Hermitian) self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp_0}$ (resp. $\mathcal{C} = \mathcal{C}^{\perp_{\frac{r}{2}}}$).

(ii) Euclidean (resp. Hermitian) self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_0}$ (resp. $\mathcal{C} \subseteq \mathcal{C}^{\perp_{\frac{r}{2}}}$).

(iii) Euclidean (resp. Hermitian) linear with complementary dual (LCD) code if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_0} = \{0\}$ (resp. $\mathcal{C} \cap \mathcal{C}^{\perp_{\frac{r}{2}}} = \{0\}$).

These classes of Λ-MT codes have nice algebraic structures and are useful in constructing modular forms. Now we proceed to study algebraic structures of Euclidean and Hermitian self-dual, self-orthogonal and LCD Λ-MT codes of length

n over $\mathbb{F}_q$. To do this, if $f(x) = a_0 + a_1x + \cdots + a_tx^t$ is a non-zero polynomial over $\mathbb{F}_q$, then its $\mathscr{T}_k$-conjugate polynomial is defined as $\mathscr{T}_k(f(x)) = a_0^{p^k}x^t + a_1^{p^k}x^{t-1} + \cdots + a_{t-1}^{p^k}x + a_t^{p^k}$. Further, the polynomial $f(x)(\neq 0) \in \mathbb{F}_q[x]$ is said to be $\mathscr{T}_k$-self-conjugate if it satisfies $\langle f(x)\rangle = \langle \mathscr{T}_k(f(x))\rangle$ in $\mathbb{F}_q[x]$. Two non-zero polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ are said to form a $\mathscr{T}_k$-conjugate pair if they satisfy $\langle g(x)\rangle = \langle \mathscr{T}_k(f(x))\rangle$ in $\mathbb{F}_q[x]$. Now we recall that $g_1(x), g_2(x), \cdots, g_\rho(x)$ are all the distinct irreducible factors of $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ with $\deg g_w(x) = d_w$ for $1 \leq w \leq \rho$. As $g_w(x)$ is irreducible over $\mathbb{F}_q$, we see that $\deg \mathscr{T}_k(g_w(x)) = \deg g_w(x) = d_w$ for each w. Further, suppose (by relabelling $g_w(x)$'s if required) that $g_1(x), g_2(x), \cdots, g_{e_1}(x)$ are all the distinct $\mathscr{T}_k$-self-conjugate polynomials, $g_{e_1+1}(x), \mathscr{T}_k(g_{e_1+1}(x)), \cdots, g_{e_2}(x), \mathscr{T}_k(g_{e_2}(x))$ are all the polynomials forming $\mathscr{T}_k$-conjugate pairs, and that $g_{e_2+1}(x), g_{e_2+2}(x), \cdots, g_{e_3}(x)$ are the remaining polynomials (that are neither $\mathscr{T}_k$-self-conjugate nor do they form $\mathscr{T}_k$-conjugate pairs), which appear in the irreducible factorizations of $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ over $\mathbb{F}_q$. Here $\rho = e_3 + e_2 - e_1$. Next for $1 \leq t \leq e_1$, $e_1 + 1 \leq \mu \leq e_2$ and $e_2 + 1 \leq u \leq e_3$, we note that $F_t = \frac{\mathbb{F}_q[x]}{\langle g_t(x)\rangle} \simeq \mathbb{F}_{q^{d_t}}$, $F_\mu = \frac{\mathbb{F}_q[x]}{\langle g_\mu(x)\rangle} \simeq \mathbb{F}_{q^{d_\mu}}$, $F'_\mu = \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k(g_\mu(x))\rangle} \simeq \mathbb{F}_{q^{d_\mu}}$, $F_u = \frac{\mathbb{F}_q[x]}{\langle g_u(x)\rangle} \simeq \mathbb{F}_{q^{d_u}}$ and $F'_u = \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k(g_u(x))\rangle} \simeq \mathbb{F}_{q^{d_u}}$. Therefore by applying the Chinese Remainder Theorem, we get

$$\begin{aligned} V \simeq & \left(\bigoplus_{t=1}^{e_1} \big(\underbrace{\epsilon_{t,1}F_t, \epsilon_{t,2}F_t, \cdots, \epsilon_{t,\ell}F_t}_{\mathcal{G}_t} \big) \right) \oplus \left(\bigoplus_{\mu=e_1+1}^{e_2} \Big\{ \big(\underbrace{\epsilon_{\mu,1}F_\mu, \epsilon_{\mu,2}F_\mu, \cdots, \epsilon_{\mu,\ell}F_\mu}_{\mathcal{G}_\mu} \big) \oplus \right. \\ & \left. \big(\underbrace{\epsilon'_{\mu,1}F'_\mu, \epsilon'_{\mu,2}F'_\mu, \cdots, \epsilon'_{\mu,\ell}F'_\mu}_{\mathcal{G}'_\mu} \big) \Big\} \right) \oplus \left(\bigoplus_{u=e_2+1}^{e_3} \big(\underbrace{\epsilon_{u,1}F_u, \epsilon_{u,2}F_u, \cdots, \epsilon_{u,\ell}F_u}_{\mathcal{G}_u} \big) \right) \quad (3.1) \end{aligned}$$

and

$$\begin{aligned} V' \simeq & \left(\bigoplus_{t=1}^{e_1} \big(\underbrace{\epsilon_{t,1}F_t, \epsilon_{t,2}F_t, \cdots, \epsilon_{t,\ell}F_t}_{\mathcal{G}_t} \big) \right) \oplus \left(\bigoplus_{\mu=e_1+1}^{e_2} \Big\{ \big(\underbrace{\epsilon'_{\mu,1}F_\mu, \epsilon'_{\mu,2}F_\mu, \cdots, \epsilon'_{\mu,\ell}F_\mu}_{\mathcal{H}_\mu} \big) \oplus \right. \end{aligned}$$

$$\Big(\underbrace{\epsilon_{\mu,1}F'_\mu, \epsilon_{\mu,2}F'_\mu, \cdots, \epsilon_{\mu,\ell}F'_\mu}_{\mathcal{H}'_\mu}\Big)\Big\}\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \Big(\underbrace{\epsilon_{u,1}F'_u, \epsilon_{u,2}F'_u, \cdots, \epsilon_{u,\ell}F'_u}_{\mathcal{G}'_u}\Big)\Big), \quad (3.2)$$

where for $1 \leq \alpha \leq e_3$, $e_1 + 1 \leq \mu \leq e_2$ and $1 \leq i \leq \ell$,

$$\epsilon_{\alpha,i} = \begin{cases} 1 & \text{if } g_\alpha(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise} \end{cases}$$

and

$$\epsilon'_{\mu,i} = \begin{cases} 1 & \text{if } \mathscr{T}_k(g_\mu(x)) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\dim_{F'_\mu}\mathcal{H}'_\mu = \epsilon_\mu$ for each μ. Further, if $\epsilon'_\mu = \sum_{i=1}^{\ell} \epsilon'_{\mu,i}$, then $\dim_{F'_\mu}\mathcal{G}'_\mu = \dim_{F_\mu}\mathcal{H}_\mu = \epsilon'_\mu$ for each μ. We also recall that $\dim_{F_\alpha}\mathcal{G}_\alpha = \epsilon_\alpha = \sum_{i=1}^{\ell} \epsilon_{\alpha,i}$ for $1 \leq \alpha \leq e_3$. In view of this, from now on, we will identify each element $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V$ as

$$A = (A_1, A_2, \cdots, A_{e_1}, A_{e_1+1}, A'_{e_1+1}, \cdots, A_{e_2}, A'_{e_2}, A_{e_2+1}, \cdots, A_{e_3}),$$

where $A_t = (A_{t,1}, A_{t,2}, \cdots, A_{t,\ell}) \in \mathcal{G}_t$, $A_\mu = (A_{\mu,1}, A_{\mu,2}, \cdots, A_{\mu,\ell}) \in \mathcal{G}_\mu$, $A'_\mu = (A'_{\mu,1}, A'_{\mu,2}, \cdots, A'_{\mu,\ell}) \in \mathcal{G}'_\mu$ and $A_u = (A_{u,1}, A_{u,2}, \cdots, A_{u,\ell}) \in \mathcal{G}_u$ with $A_{t,i} := \epsilon_{t,i}(a_i(x) + \langle g_t(x)\rangle)$, $A_{\mu,i} := \epsilon_{\mu,i}(a_i(x) + \langle g_\mu(x)\rangle)$, $A'_{\mu,i} := \epsilon'_{\mu,i}(a_i(x) + \langle \mathscr{T}_k(g_\mu(x))\rangle)$ and $A_{u,i} = \epsilon_{u,i}(a_i(x) + \langle g_u(x)\rangle)$ for $1 \leq i \leq \ell$, $1 \leq t \leq e_1$, $e_1 + 1 \leq \mu \leq e_2$ and $e_2 + 1 \leq u \leq e_3$. Analogously, we will identify each element $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in V'$ as

$$B = (B_1, B_2, \cdots, B_{e_1}, B_{e_1+1}, B'_{e_1+1}, \cdots, B_{e_2}, B'_{e_2}, B_{e_2+1}, \cdots, B_{e_3}),$$

where $B_t = (B_{t,1}, B_{t,2}, \cdots, B_{t,\ell}) \in \mathcal{G}_t$, $B_\mu = (B_{\mu,1}, B_{\mu,2}, \cdots, B_{\mu,\ell}) \in \mathcal{H}_\mu$, $B'_\mu = (B'_{\mu,1}, B'_{\mu,2}, \cdots, B'_{\mu,\ell}) \in \mathcal{H}'_\mu$ and $B_u = (B_{u,1}, B_{u,2}, \cdots, B_{u,\ell}) \in \mathcal{G}'_u$ with $B_{t,i} := \epsilon_{t,i}(b_i(x) + \langle g_t(x)\rangle)$, $B_{\mu,i} := \epsilon'_{\mu,i}(b_i(x) + \langle g_\mu(x)\rangle)$, $B'_{\mu,i} := \epsilon_{\mu,i}(b_i(x) + \langle \mathscr{T}_k(g_\mu(x))\rangle)$

and $B_{u,i} = \epsilon_{u,i}(b_i(x) + \langle \mathscr{T}_k(g_u(x))\rangle)$ for each i, t, μ and u.

For $1 \leq t \leq e_1$, let $\mathcal{T}_k : \epsilon_{t,i}F_t \to \epsilon_{t,i}F_t$ be the conjugation map, defined as

$$\mathcal{T}_k(h_t(x)) = \begin{cases} \sum_{b=0}^{d_t-1} h_{tb}^{p^k} x^{-b} & \text{if } \epsilon_{t,i} = 1; \\ 0 & \text{if } \epsilon_{t,i} = 0 \end{cases}$$

for all $h_t(x) = \sum_{b=0}^{d_t-1} h_{tb}x^b \in \epsilon_{t,i}F_t$. For $e_1 + 1 \leq \mu \leq e_2$, the conjugation map $\mathcal{T}_k : \epsilon'_{\mu,i}F_\mu \to \epsilon'_{\mu,i}F'_\mu$ is defined as

$$\mathcal{T}_k(h_\mu(x)) = \begin{cases} \sum_{b=0}^{d_\mu-1} h_{\mu b}^{p^k} x^{-b} & \text{if } \epsilon'_{\mu,i} = 1; \\ 0 & \text{if } \epsilon'_{\mu,i} = 0 \end{cases}$$

for all $h_\mu(x) = \sum_{b=0}^{d_\mu-1} h_{\mu b}x^b \in \epsilon'_{\mu,i}F_\mu$, while the conjugation map $\mathcal{T}_k : \epsilon_{\mu,i}F'_\mu \to \epsilon_{\mu,i}F_\mu$ is defined as

$$\mathcal{T}_k(\hat{h}_\mu(x)) = \begin{cases} \sum_{b=0}^{d_\mu-1} \hat{h}_{\mu b}^{p^k} x^{-b} & \text{if } \epsilon_{\mu,i} = 1; \\ 0 & \text{if } \epsilon_{\mu,i} = 0 \end{cases}$$

for all $\hat{h}_\mu(x) = \sum_{b=0}^{d_\mu-1} \hat{h}_{\mu b}x^b \in \epsilon_{\mu,i}F'_\mu$. For $e_2 + 1 \leq u \leq e_3$, the conjugation map $\mathcal{T}_k : \epsilon_{u,i}F'_u \to \epsilon_{u,i}F_u$ is defined as

$$\mathcal{T}_k(h_u(x)) = \begin{cases} \sum_{b=0}^{d_u-1} h_{ub}^{p^k} x^{-b} & \text{if } \epsilon_{u,i} = 1; \\ 0 & \text{if } \epsilon_{u,i} = 0 \end{cases}$$

for all $h_u(x) = \sum_{b=0}^{d_u-1} h_{ub}x^b \in \epsilon_{u,i}F'_u$. For $1 \leq i \leq \ell$ and $1 \leq t \leq e_1$ satisfying $\epsilon_{t,i} = 1$, we observe that the conjugation map $\mathcal{T}_k$ is the identity map when $k = 0$ and $d_t = 1$, while it is an automorphism of F_t when either $d_t = 1$ and $k = \frac{r}{2}$ with r even or $d_t > 1$. From this, we see that for each $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in V'$, the

element $\mathcal{T}_k(b(x)) \in V$ is given by

$$(\mathcal{T}_k(B_1), \mathcal{T}_k(B_2), \cdots, \mathcal{T}_k(B_{e_1}), \mathcal{T}_k(B'_{e_1+1}), \mathcal{T}_k(B_{e_1+1}), \cdots, \mathcal{T}_k(B'_{e_2}), \mathcal{T}_k(B_{e_2}),$$
$$\mathcal{T}_k(B_{e_2+1}), \cdots, \mathcal{T}_k(B_{e_3})),$$

where

$$\begin{aligned}
\mathcal{T}_k(B_t) &= (\mathcal{T}_k(B_{t,1}), \mathcal{T}_k(B_{t,2}), \cdots, \mathcal{T}_k(B_{t,\ell})) \in \mathcal{G}_t, \\
\mathcal{T}_k(B_\mu) &= (\mathcal{T}_k(B_{\mu,1}), \mathcal{T}_k(B_{\mu,2}), \cdots, \mathcal{T}_k(B_{\mu,\ell})) \in \mathcal{G}'_\mu, \\
\mathcal{T}_k(B'_\mu) &= (\mathcal{T}_k(B'_{\mu,1}), \mathcal{T}_k(B'_{\mu,2}), \cdots, \mathcal{T}_k(B'_{\mu,\ell})) \in \mathcal{G}_\mu \\
\mathcal{T}_k(B_u) &= (\mathcal{T}_k(B_{u,1}), \mathcal{T}_k(B_{u,2}), \cdots, \mathcal{T}_k(B_{u,\ell})) \in \mathcal{G}_u
\end{aligned}$$

with $\mathcal{T}_k(B_{t,i}) = \epsilon_{t,i}(\mathcal{T}_k(b_i(x)) + \langle g_t(x)\rangle)$, $\mathcal{T}_k(B_{\mu,i}) = \epsilon'_{\mu,i}(\mathcal{T}_k(b_i(x)) + \langle \mathscr{T}_k(g_\mu(x))\rangle)$, $\mathcal{T}_k(B'_{\mu,i}) = \epsilon_{\mu,i}(\mathcal{T}_k(b_i(x)) + \langle g_\mu(x)\rangle)$ and $\mathcal{T}_k(B_{u,i}) = \epsilon_{u,i}(\mathcal{T}_k(b_i(x)) + \langle g_u(x)\rangle)$ for each i, t, μ and u.

In view of this, a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as

$$\mathcal{C} = \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (\mathcal{C}_\mu \oplus \mathcal{C}'_\mu)\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{C}_u\Big), \tag{3.3}$$

where $\mathcal{C}_t$ (resp. $\mathcal{C}_\mu$, $\mathcal{C}'_\mu$ and $\mathcal{C}_u$) is a subspace of $\mathcal{G}_t$ (resp. $\mathcal{G}_\mu$, $\mathcal{G}'_\mu$ and $\mathcal{G}_u$) over the field F_t (resp. F_μ, F'_μ and F_u) for each t (resp. μ and u). To study their dual codes, we see that if for some α and i, $\epsilon_{\alpha,i} = 1$, then $x^{m_i} = \lambda_i$ in F_α, which implies that $\lambda_i(x^m - 1)/(x^{m_i} - \lambda_i) = m/m_i$ in F_α. In view of the above, the sesquilinear form corresponding to $(\cdot,\cdot)_k$ is a map $[\cdot,\cdot]_k$ from $\Big\{\Big(\bigoplus_{t=1}^{e_1} \mathcal{G}_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (\mathcal{G}_\mu \oplus \mathcal{G}'_\mu)\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{G}_u\Big)\Big\} \times$ $\Big\{\Big(\bigoplus_{t=1}^{e_1} \mathcal{G}_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (\mathcal{H}_\mu \oplus \mathcal{H}'_\mu)\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{G}'_u\Big)\Big\}$ into $\Big(\bigoplus_{t=1}^{e_1} F_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (F_\mu \oplus F'_\mu)\Big) \oplus$

$\Big(\bigoplus_{u=e_2+1}^{e_3} F_u \Big)$, which is defined as

$$\begin{aligned}[A,B]_k = \Big(& \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{1,i} A_{1,i} \mathcal{T}_k(B_{1,i}), \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{2,i} A_{2,i} \mathcal{T}_k(B_{2,i}), \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_1,i} A_{e_1,i} \mathcal{T}_k(B_{e_1,i}), \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_1+1,i} A_{e_1+1,i} \mathcal{T}_k(B'_{e_1+1,i}), \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon'_{e_1+1,i} A'_{e_1+1,i} \mathcal{T}_k(B_{e_1+1,i}), \cdots\cdots, \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2,i} A_{e_2,i} \mathcal{T}_k(B'_{e_2,i}), \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon'_{e_2,i} A'_{e_2,i} \mathcal{T}_k(B_{e_2,i}), \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2+1,i} A_{e_2+1,i} \mathcal{T}_k(B_{e_2+1,i}), \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2+2,i} A_{e_2+2,i} \mathcal{T}_k(B_{e_2+2,i}), \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_3,i} A_{e_3,i} \mathcal{T}_k(B_{e_3,i}) \Big) \end{aligned} \tag{3.4}$$

for each $A \in V$ and $B \in V'$. Furthermore, with respect to the sesquilinear form defined by (3.4), it is easy to see that the dual code $\mathcal{C}^{\perp_k}$ of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_k} = \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t^{\perp_k} \Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} ({\mathcal{C}'_\mu}^{\perp_k} \oplus \mathcal{C}_\mu^{\perp_k}) \Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{C}_u^{\perp_k} \Big), \tag{3.5}$$

where $\mathcal{C}_t^{\perp_k} (\subseteq \mathcal{G}_t)$ is the orthogonal complement of $\mathcal{C}_t$ with respect to $[\cdot,\cdot]_k \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$ for $1 \leq t \leq e_1$; $\mathcal{C}_\mu^{\perp_k} (\subseteq \mathcal{H}'_\mu)$ is the orthogonal complement of $\mathcal{C}_\mu$ with respect to $[\cdot,\cdot]_k \restriction_{\mathcal{G}_\mu \times \mathcal{H}'_\mu}$, $\mathcal{C}'^{\perp_k}_\mu (\subseteq \mathcal{H}_\mu)$ is the orthogonal complement of $\mathcal{C}'_\mu$ with respect to $[\cdot,\cdot]_k \restriction_{\mathcal{G}'_\mu \times \mathcal{H}_\mu}$ for $e_1+1 \leq \mu \leq e_2$; and $\mathcal{C}_u^{\perp_k} (\subseteq \mathcal{G}'_u)$ is the orthogonal complement of $\mathcal{C}_u$ with respect to $[\cdot,\cdot]_k \restriction_{\mathcal{G}_u \times \mathcal{G}'_u}$ for $e_2+1 \leq u \leq e_3$. Here $[\cdot,\cdot]_k \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$ (resp. $[\cdot,\cdot]_k \restriction_{\mathcal{G}_\mu \times \mathcal{H}'_\mu}$, $[\cdot,\cdot]_k \restriction_{\mathcal{G}'_\mu \times \mathcal{H}_\mu}$ and $[\cdot,\cdot]_k \restriction_{\mathcal{G}_u \times \mathcal{G}'_u}$) is the restriction of the sesquilinear form $[\cdot,\cdot]_k$ (defined by (3.4)) to $\mathcal{G}_t \times \mathcal{G}_t$ (resp. $\mathcal{G}_\mu \times \mathcal{H}'_\mu$, $\mathcal{G}'_\mu \times \mathcal{H}_\mu$ and $\mathcal{G}_u \times \mathcal{G}'_u$) for each t (resp. μ and u).

To study all Euclidean and Hermitian self-dual, self-orthogonal and LCD Λ-MT codes, let $\mathcal{K}_\mu = \mathcal{G}_\mu \cap \mathcal{H}_\mu$, $\mathcal{K}'_\mu = \mathcal{G}'_\mu \cap \mathcal{H}'_\mu$, and let τ_μ denote the number of integers i satisfying $1 \leq i \leq \ell$ and $\epsilon_{\mu,i} = \epsilon'_{\mu,i} = 1$ for $e_1+1 \leq \mu \leq e_2$. Note that $\tau_\mu = \sum_{i=1}^{\ell} \epsilon_{\mu,i} \epsilon'_{\mu,i}$ for each μ. One can easily observe that $\dim_{F_\mu} \mathcal{K}_\mu = \dim_{F'_\mu} \mathcal{K}'_\mu = \tau_\mu$ for each μ. In the following theorem, we characterize all Euclidean self-dual, self-orthogonal and LCD

Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 3.3.3. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed. Let $\mathcal{C} = \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (\mathcal{C}_\mu \oplus \mathcal{C}'_\mu)\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{C}_u\Big)$ be a Λ-MT code of length n over $\mathbb{F}_q$, where $\mathcal{C}_t$ (resp. $\mathcal{C}_\mu$, $\mathcal{C}'_\mu$ and $\mathcal{C}_u$) is a subspace of $\mathcal{G}_t$ (resp. $\mathcal{G}_\mu$, $\mathcal{G}'_\mu$ and $\mathcal{G}_u$) over F_t (resp. F_μ, F'_μ and F_u) for each t (μ and u). Then the following hold.*

(a) The code $\mathcal{C}$ is Euclidean self-dual if and only if all the irreducible factors of the polynomials $x^{m_1}-\lambda_1$, $x^{m_2}-\lambda_2, \cdots x^{m_\ell}-\lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_0$-self-conjugate or form $\mathscr{T}_0$-conjugate pairs (i.e., $e_3 \leq e_2$), $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ for $1 \leq t \leq e_1$ and $e_1+1 \leq \mu \leq e_2$. As a consequence, when all the irreducible factors of the polynomials $x^{m_1}-\lambda_1$, $x^{m_2}-\lambda_2, \cdots x^{m_\ell}-\lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_0$-self-conjugate or form $\mathscr{T}_0$-conjugate pairs (i.e., $e_3 \leq e_2$), the total number of distinct Euclidean self-dual Λ-MT codes of length n over $\mathbb{F}_q$ is given by $\mathfrak{N}_0 = \prod_{t=1}^{e_1} \mathfrak{D}_t \prod_{\mu=e_1+1}^{e_2} \mathfrak{D}_\mu$, where $\mathfrak{D}_t$ equals the number of distinct F_t-subspaces $\mathcal{C}_t$ of $\mathcal{G}_t$ satisfying $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$ for $1 \leq t \leq e_1$ and $\mathfrak{D}_\mu$ equals the number of distinct F_μ-subspaces of $\mathcal{K}_\mu$ for $e_1+1 \leq \mu \leq e_2$.

(b) The code $\mathcal{C}$ is Euclidean self-orthogonal if and only if $\mathcal{C}_t \subseteq \mathcal{C}_t^{\perp_0}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ and $\mathcal{C}_u = \{0\}$ for $1 \leq t \leq e_1$, $e_1+1 \leq \mu \leq e_2$ and $e_2+1 \leq u \leq e_3$. As a consequence, the total number of distinct Euclidean self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$ is given by $\mathfrak{N}_1 = \prod_{t=1}^{e_1} \mathfrak{E}_t \prod_{\mu=e_1+1}^{e_2} \mathfrak{E}_\mu$, where $\mathfrak{E}_t$ equals the number of distinct Euclidean self-orthogonal F_t-subspaces of $\mathcal{G}_t$ for $1 \leq t \leq e_1$ and $\mathfrak{E}_\mu$ equals the number of pairs $(\mathcal{C}_\mu, \mathcal{C}'_\mu)$ with $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) as a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) over F_μ (resp. F'_μ) satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ for $e_1+1 \leq \mu \leq e_2$.

(c) The code $\mathcal{C}$ is Euclidean LCD if and only if $\mathcal{C}_t \cap \mathcal{C}_t^{\perp_0} = \{0\}$, $\mathcal{C}_\mu \cap \mathcal{C}_\mu'^{\perp_0} = \mathcal{C}'_\mu \cap \mathcal{C}_\mu^{\perp_0} = \{0\}$ for $1 \leq t \leq e_1$ and $e_1+1 \leq \mu \leq e_2$. As a consequence, the total number of distinct Euclidean LCD Λ-MT codes of length n over $\mathbb{F}_q$ is

given by $\mathfrak{N}_2 = \prod_{t=1}^{e_1} \mathfrak{F}_t \prod_{\mu=e_1+1}^{e_2} \mathfrak{F}_\mu \prod_{u=e_2+1}^{e_3} \mathfrak{F}_u$, *where* $\mathfrak{F}_t$ *equals the number of distinct* F_t*-subspaces of* $\mathcal{G}_t$ *satisfying* $\mathcal{C}_t \cap \mathcal{C}_t^{\perp_0} = \{0\}$ *for* $1 \leq t \leq e_1$, $\mathfrak{F}_\mu$ *equals the number of distinct pairs* $(\mathcal{C}_\mu, \mathcal{C}'_\mu)$ *with* $\mathcal{C}_\mu$ *(resp.* $\mathcal{C}'_\mu$*) as a subspace of* $\mathcal{G}_\mu$ *(resp.* $\mathcal{G}'_\mu$*) over* F_μ *(resp.* F'_μ*) satisfying* $\mathcal{C}_\mu \cap \mathcal{C}'^{\perp_0}_\mu = \{0\}$ *and* $\mathcal{C}'_\mu \cap \mathcal{C}_\mu^{\perp_0} = \{0\}$ *for* $e_1 + 1 \leq \mu \leq e_2$, *and* $\mathfrak{F}_u$ *equals the number of distinct subspaces of* $\mathcal{G}_u$ *over* F_u *for* $e_2 + 1 \leq u \leq e_3$.

Proof. (a) In view of (3.3) and (3.5), we see that the code $\mathcal{C}$ is Euclidean self-dual if and only if the set $\{g_{e_2+1}(x), g_{e_2+2}(x), \cdots, g_{e_3}(x)\}$ is empty, $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$, $\mathcal{C}_\mu$ is a subspace of $\mathcal{K}_\mu$ and $\mathcal{C}'_\mu$ is a subspace of $\mathcal{K}'_\mu$ satisfying $\mathcal{C}_\mu = \mathcal{C}'^{\perp_0}_\mu \cap \mathcal{K}_\mu$ and $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ for each t and μ. Further, for $e_1 + 1 \leq \mu \leq e_2$, $\mathcal{C}_\mu$ is a subspace of $\mathcal{K}_\mu$ and $\mathcal{C}'_\mu$ is a subspace of $\mathcal{K}'_\mu$, then we observe that $\mathcal{C}_\mu = \mathcal{C}'^{\perp_0}_\mu \cap \mathcal{K}_\mu$ and $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ hold if and only if $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ holds. From this, part (a) follows immediately.

(b) By (3.3) and (3.5), we see that the code $\mathcal{C}$ is Euclidean self-orthogonal if and only if $\mathcal{C}_t \subseteq \mathcal{C}_t^{\perp_0}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ and $\mathcal{C}_\mu \subseteq \mathcal{C}'^{\perp_0}_\mu \cap \mathcal{K}_\mu$, and $\mathcal{C}_u \subseteq \{0\}$, $\{0\} \subseteq \mathcal{C}_u^{\perp_0}$ for each t, μ and u. Further, for $e_1 + 1 \leq \mu \leq e_2$, we see that if $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$), then $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ and $\mathcal{C}_\mu \subseteq \mathcal{C}'^{\perp_0}_\mu \cap \mathcal{K}_\mu$ hold if and only if $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ holds. From this, part (b) follows.

(c) By (3.3) and (3.5), we see that the code $\mathcal{C}$ is Euclidean LCD if and only if $\mathcal{C}_t \cap \mathcal{C}_t^{\perp_0} = \{0\}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{G}_\mu$ (resp. $\mathcal{G}'_\mu$) satisfying $\mathcal{C}_\mu \cap \mathcal{C}'^{\perp_0}_\mu = \{0\}$ and $\mathcal{C}'_\mu \cap \mathcal{C}_\mu^{\perp_0} = \{0\}$, and $\mathcal{C}_u \cap \{0\} = \{0\}$ and $\{0\} \cap \mathcal{C}_u^{\perp_0} = \{0\}$ for each t, μ and u. From this, part (c) follows.

□

In the following theorem, we characterize all Hermitian self-dual, self-orthogonal and LCD Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 3.3.4. *Let r be even and $k = \frac{r}{2}$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed. Let $\mathcal{C} = \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} (\mathcal{C}_\mu \oplus \mathcal{C}'_\mu)\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \mathcal{C}_u\Big)$ be a Λ-MT code of length n over $\mathbb{F}_q$, where $\mathcal{C}_t$ (resp. $\mathcal{C}_\mu$, $\mathcal{C}'_\mu$ and $\mathcal{C}_u$) is a subspace of $\mathcal{G}_t$ (resp. $\mathcal{G}_\mu$, $\mathcal{G}'_\mu$ and $\mathcal{G}_u$) over F_t (resp. F_μ, F'_μ and F_u) for each t (μ and u). Then the following hold.*

(a) The code is $\mathcal{C}$ is Hermitian self-dual if and only if all the irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_{\frac{r}{2}}$-self-conjugate or form $\mathscr{T}_{\frac{r}{2}}$-conjugate pairs (i.e., $e_3 \leq e_2$), $\mathcal{C}_t = \mathcal{C}_t^{\perp_{\frac{r}{2}}}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$ for $1 \leq t \leq e_1$ and $e_1 + 1 \leq \mu \leq e_2$. As a consequence, when all the irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_{\frac{r}{2}}$-self-conjugate or form $\mathscr{T}_{\frac{r}{2}}$-conjugate pairs (i.e., $e_3 \leq e_2$), the total number of distinct Hermitian self-dual Λ-MT codes of length n over $\mathbb{F}_q$ is given by $\mathfrak{M}_0 = \prod_{t=1}^{e_1} \mathcal{N}_t \prod_{\mu=e_1+1}^{e_2} \mathcal{N}_\mu$, where $\mathcal{N}_t$ equals the number of distinct F_t-subspaces $\mathcal{C}_t$ of $\mathcal{G}_t$ satisfying $\mathcal{C}_t = \mathcal{C}_t^{\perp_{\frac{r}{2}}}$ for $1 \leq t \leq e_1$ and $\mathcal{N}_\mu$ equals the number of distinct F_μ-subspaces of $\mathcal{K}_\mu$ for $e_1 + 1 \leq \mu \leq e_2$.

(b) The code $\mathcal{C}$ is Hermitian self-orthogonal if and only if $\mathcal{C}_t \subseteq \mathcal{C}_t^{\perp_{\frac{r}{2}}}$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$ and $\mathcal{C}_u = \{0\}$ for $1 \leq t \leq e_1$, $e_1 + 1 \leq \mu \leq e_2$ and $e_2 + 1 \leq u \leq e_3$. As a consequence, the total number of distinct Hermitian self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$ is given by $\mathfrak{M}_1 = \prod_{t=1}^{e_1} \mathcal{M}_t \prod_{\mu=e_1+1}^{e_2} \mathcal{M}_\mu$, where $\mathcal{M}_t$ equals the number of distinct Hermitian self-orthogonal F_t-subspaces of $\mathcal{G}_t$ for $1 \leq t \leq e_1$ and $\mathcal{M}_\mu$ equals the number of pairs $(\mathcal{C}_\mu, \mathcal{C}'_\mu)$ with $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) as a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) over F_μ (resp. F'_μ) satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$ for $e_1 + 1 \leq \mu \leq e_2$.

(c) The code $\mathcal{C}$ is Hermitian LCD if and only if $\mathcal{C}_t \cap \mathcal{C}_t^{\perp_{\frac{r}{2}}} = \{0\}$, $\mathcal{C}_\mu \cap \mathcal{C}_\mu'^{\perp_{\frac{r}{2}}} = \mathcal{C}'_\mu \cap \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} = \{0\}$ for $1 \leq t \leq e_1$ and $e_1 + 1 \leq \mu \leq e_2$. As a consequence, the total number of distinct Hermitian LCD Λ-MT codes of length n over $\mathbb{F}_q$

is given by $\mathfrak{M}_2 = \prod_{t=1}^{e_1} \mathcal{D}_t \prod_{\mu=e_1+1}^{e_2} \mathcal{D}_\mu \prod_{u=e_2+1}^{e_3} \mathcal{D}_u$, *where* $\mathcal{D}_t$ *equals the number of distinct* F_t*-subspaces of* $\mathcal{G}_t$ *satisfying* $\mathcal{C}_t \cap \mathcal{C}_t^{\perp_{\frac{r}{2}}} = \{0\}$ *for* $1 \leq t \leq e_1$, $\mathcal{D}_\mu$ *equals the number of distinct pairs* $(\mathcal{C}_\mu, \mathcal{C}'_\mu)$ *with* $\mathcal{C}_\mu$ *(resp.* $\mathcal{C}'_\mu$*) as a subspace of* $\mathcal{G}_\mu$ *(resp.* $\mathcal{G}'_\mu$*) over* F_μ *(resp.* F'_μ*) satisfying* $\mathcal{C}_\mu \cap \mathcal{C}_\mu^{\prime\perp_{\frac{r}{2}}} = \{0\}$ *and* $\mathcal{C}'_\mu \cap \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} = \{0\}$ *for* $e_1+1 \leq \mu \leq e_2$, *and* $\mathcal{D}_u$ *equals the number of distinct subspaces of* $\mathcal{G}_u$ *over* F_u *for* $e_2 + 1 \leq u \leq e_3$.

Proof. Working in a similar manner as in Theorem 3.3.3, the desired result follows immediately by (3.3) and (3.5). □

3.4 Generator theory for MT codes

In this section, we shall develop generator theory for Λ-MT codes of length n over $\mathbb{F}_q$. For this, we proceed as follows:

A Λ-MT $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called a ϱ-generator code if ϱ is the smallest positive integer with the property that there exist ϱ number of codewords $a_1(x), a_2(x), \cdots, a_\varrho(x) \in \mathcal{C}$ such that every $c(x) \in \mathcal{C}$ can be expressed as $c(x) = f_1(x)a_1(x) + f_2(x)a_2(x) + \cdots + f_\varrho(x)a_\varrho(x)$ for some $f_1(x), f_2(x), \cdots, f_\varrho(x) \in \mathbb{F}_q[x]$, and we denote $\mathcal{C} = \langle a_1(x), a_2(x), \cdots, a_\varrho(x) \rangle$. Now we shall study some basic properties of ϱ-generator Λ-MT codes over finite fields.

Let $\mathcal{C} = \langle a_1(x), a_2(x), \cdots, a_\varrho(x) \rangle$ be a ϱ-generator Λ-MT code of length n over $\mathbb{F}_q$, where $a_\varsigma(x) = (a_{\varsigma,1}(x), a_{\varsigma,2}(x), \cdots, a_{\varsigma,\ell}(x))$ for $1 \leq \varsigma \leq \varrho$. For $1 \leq i \leq \ell$, if π_i is the projection of V onto $V_i = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \lambda_i \rangle}$, then it is easy to observe that $\pi_i(\mathcal{C})$ is a λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ with the generator polynomial $\gcd(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x), x^{m_i} - \lambda_i)$. Further, the annihilator of $\mathcal{C}$ is defined as

$$\mathrm{Ann}(\mathcal{C}) = \{f(x) \in \mathbb{F}_q[x] : f(x)a_\varsigma(x) = 0 \text{ in } V \text{ for } 1 \leq \varsigma \leq \varrho\}.$$

It is easy to see that $\mathrm{Ann}(\mathcal{C})$ is an ideal of the principal ideal ring $\mathbb{F}_q[x]$. Note

that $\prod_{i=1}^{\ell}(x^{m_i}-\lambda_i) \in \mathrm{Ann}(\mathcal{C})$. Therefore there exists a unique smallest degree monic polynomial $h(x) \in \mathbb{F}_q[x]$, which generates $\mathrm{Ann}(\mathcal{C})$; the polynomial $h(x)$ is called the parity-check polynomial of $\mathcal{C}$. In the following theorem, we determine the parity-check polynomial of a ϱ-generator Λ-MT code of length n over $\mathbb{F}_q$.

Theorem 3.4.1. *Let $\mathcal{C} = \langle a_1(x), a_2(x), \cdots, a_\varrho(x)\rangle$ be a ϱ-generator Λ-MT code of length n over $\mathbb{F}_q$, where $a_\varsigma(x) = (a_{\varsigma,1}(x), a_{\varsigma,2}(x), \cdots, a_{\varsigma,\ell}(x))$ for $1 \le \varsigma \le \varrho$. Let $w_i(x) = \gcd(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x), x^{m_i}-\lambda_i)$ for $1 \le i \le \ell$. Then the following hold.*

(a) The parity-check polynomial $h(x)$ of $\mathcal{C}$ is given by $h(x) = \operatorname{lcm}_{1\le i\le \ell}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$.

(b) When $\varrho = 1$, we have $dim_{\mathbb{F}_q}\mathcal{C} = deg\ h(x)$.

Proof. To prove the first part, for $1 \le i \le \ell$, let π_i be the projection of V onto the ring V_i. Then for each i, we see that $\pi_i(\mathcal{C})$ is a λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ having the generator polynomial $w_i(x)$. From this, we observe that $\operatorname{lcm}_{1\le i\le \ell}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$ is an annihilating polynomial of the code $\mathcal{C}$, so $h(x)$ divides $\operatorname{lcm}_{1\le i\le \ell}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$. On the other hand, since $h(x)$ is the parity-check polynomial of $\mathcal{C}$, we must have $a_{\varsigma,i}(x)h(x) = 0$ in the ring V_i for $1 \le \varsigma \le \varrho$ and $1 \le i \le \ell$. This implies that $x^{m_i}-\lambda_i$ divides $h(x)\gcd(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x))$ in $\mathbb{F}_q[x]$, which further implies that $\frac{x^{m_i}-\lambda_i}{w_i(x)}$ divides $h(x)$ for each i. This shows that $\operatorname{lcm}_{1\le i\le \ell}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$ divides $h(x)$ in $\mathbb{F}_q[x]$. From this, we get $h(x) = \operatorname{lcm}_{1\le i\le \ell}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$.

To prove the second part, let $\varrho = 1$ so that $\mathcal{C} = \langle a_1(x)\rangle$. Now define a map $\Xi : \mathbb{F}_q[x] \to V$ as $\Xi(\alpha(x)) = \alpha(x)a_1(x)$ for each $\alpha(x) \in \mathbb{F}_q[x]$. We see that Ξ is an $\mathbb{F}_q[x]$-module homomorphism with kernal $\langle h(x)\rangle$ and image $\mathcal{C}$. From this, we get $\frac{\mathbb{F}_q[x]}{\langle h(x)\rangle} \simeq \mathcal{C}$, which implies that $\dim_{\mathbb{F}_q}\mathcal{C} = \deg\ h(x)$. □

In the following example, we show that Theorem 3.4.1(b) does not hold for a ϱ-generator Λ-MT code with $\varrho \ge 2$.

Example 3.4.1. *Let $q = 2$, $\ell = 3$, $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ and $\lambda_1 = \lambda_2 = \lambda_3 = 1$, so that $\Lambda = (1, 1, 1)$. Let $\mathcal{C}$ be a 2-generator Λ-MT code length 15 over $\mathbb{F}_2$, whose generating set is $\{(x^2+1, x^3+x, x^3+x+1), (x^2+x, x^4+x^3+x^2+x+1, x^3+x^2+1)\}$. Here $V = V_1 \times V_2 \times V_3$, where $V_1 = \frac{\mathbb{F}_2[x]}{\langle x^3-1\rangle}$, $V_2 = \frac{\mathbb{F}_2[x]}{\langle x^5-1\rangle}$ and $V_3 = \frac{\mathbb{F}_2[x]}{\langle x^7-1\rangle}$. In order to write down the decomposition of V, we see that $x^3 - 1 = (x + 1)(x^2 + x + 1)$, $x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$ and $x^7 - 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1)$ are irreducible factorizations of $x^3 - 1$, $x^5 - 1$ and $x^7 - 1$ over $\mathbb{F}_2$. Let us take $g_1(x) = x - 1$, $g_2(x) = x^2 + x + 1$, $g_3(x) = x^4 + x^3 + x^2 + x + 1$, $g_4(x) = x^3 + x^2 + 1$ and $g_5(x) = x^3 + x + 1$, so that $F_w = \mathbb{F}_2[x]/\langle g_w(x)\rangle$ for $1 \leq w \leq 5$. Note that $F_1 \simeq \mathbb{F}_2$, $F_2 \simeq \mathbb{F}_4$, $F_3 \simeq \mathbb{F}_{16}$ and $F_4 \simeq F_5 \simeq \mathbb{F}_8$. By applying Chinese remainder Theorem, we get $V \simeq \big(F_1, F_1, F_1\big) \oplus (F_2, 0, 0) \oplus \big(0, F_3, 0\big) \oplus \big(0, 0, F_4\big) \oplus \big(0, 0, F_5\big)$. From this and applying Theorem 3.2.2, we see that the constituents of $\mathcal{C}$ are given by $\mathcal{C}_1 = \langle (0, 0, 1), (0, 1, 1)\rangle$, $\mathcal{C}_2 = \langle (\delta_2, 0, 0), (1, 0, 0)\rangle$ with $\delta_2^2 + \delta_2 + 1 = 0$, $\mathcal{C}_3 = \langle (0, \delta_3^3 + \delta_3, 0), (0, 0, 0)\rangle$ with $\delta_3^4 + \delta_3^3 + \delta_3^2 + \delta_3 + 1 = 0$, $\mathcal{C}_4 = \langle (0, 0, \delta_4 + \delta_4^2), (0, 0, 0)\rangle$ with $\delta_4^3 + \delta_4^2 + 1 = 0$ and $\mathcal{C}_5 = \langle (0, 0, 0), (0, 0, \delta_5 + \delta_5^2)\rangle$ with $\delta_5^3 + \delta_5 + 1 = 0$. We observe that $dim_{F_1}\mathcal{C}_1 = 2$ and $dim_{F_2}\mathcal{C}_2 = dim_{F_3}\mathcal{C}_3 = dim_{F_4}\mathcal{C}_4 = dim_{F_5}\mathcal{C}_5 = 1$. Using this and by applying Theorem 3.2.2 again, we get $dim_{\mathbb{F}_2}\mathcal{C} = \sum_{w=1}^{5} dim_{F_w}\mathcal{C}_w \deg g_w(x) = 14$. On the other hand, by applying Theorem 3.4.1(a), we get $h(x) = (x + 1)(x^4 + x^3 + x^2 + x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)(x^2 + x + 1)$, which implies that $\deg h(x) = 13$. This shows that $dim_{\mathbb{F}_2}\mathcal{C} \neq \deg h(x)$ in this case.*

In the following theorem, we determine generating sets of Euclidean and Hermitian dual codes of some ϱ-generator MT codes of length n over $\mathbb{F}_q$.

Theorem 3.4.2. *Let $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ be pairwise coprime polynomials in $\mathbb{F}_q[x]$. Let $\mathcal{C} = \big\langle a_1(x), a_2(x), \cdots, a_\varrho(x)\big\rangle$ be a ϱ-generator Λ-MT code of length n over $\mathbb{F}_q$, where $a_\varsigma(x) = (a_{\varsigma,1}(x), a_{\varsigma,2}(x), \cdots, a_{\varsigma,\ell}(x))$ for $1 \leq \varsigma \leq \varrho$. Let $w_i(x) = \gcd(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x), x^{m_i} - \lambda_i)$ for $1 \leq i \leq \ell$. When k is either 0 or $\frac{r}{2}$*

(provided r is even), we have

$$\mathcal{C}^{\perp_k} = \langle H_1(x), H_2(x), \cdots, H_\ell(x) \rangle,$$

where $H_i(x) = (0, \cdots, 0, \underbrace{\mathcal{T}_k^{(i)}\Big(\frac{x^{m_i}-\lambda_i}{w_i(x)}\Big)}_{i^{th}}, 0, \cdots, 0)$ *for* $1 \leq i \leq \ell$.

Proof. In order to prove the result, we see, for $1 \leq \varsigma \leq \varrho$ and $1 \leq i \leq \ell$, that

$$\begin{aligned}(a_\varsigma(x), H_i(x))_k &= a_{\varsigma,i}(x)\mathcal{T}_k^{(i)}\Big(\mathcal{T}_k^{(i)}\Big(\frac{x^{m_i}-\lambda_i}{w_i(x)}\Big)\Big)\lambda_i\Big(\frac{x^m-1}{x^{m_i}-\lambda_i}\Big) \\ &= \frac{a_{\varsigma,i}(x)\lambda_i(x^m-1)}{w_i(x)} = 0 \text{ in } \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}.\end{aligned}$$

This implies that $H_i(x) \in \mathcal{C}^{\perp_k}$ for each i. Now let $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in \mathcal{C}^{\perp_k}$. Then we have $(a_\varsigma(x), b(x))_k = 0$ in $\frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$ for $1 \leq \varsigma \leq \varrho$. From this, we see that x^m-1 divides $\sum_{i=1}^{\ell} a_{\varsigma,i}(x)\mathcal{T}_k^{(i)}(b_i(x))\lambda_i\Big(\frac{x^m-1}{x^{m_i}-\lambda_i}\Big)$, which implies that $x^{m_j}-\lambda_j$ divides $\sum_{i=1}^{\ell} a_{\varsigma,i}(x)\mathcal{T}_k^{(i)}(b_i(x))\lambda_i\Big(\frac{x^m-1}{x^{m_i}-\lambda_i}\Big)$ for $1 \leq \varsigma \leq \varrho$ and $1 \leq j \leq \ell$. As $(x^{m_i}-\lambda_i, x^{m_j}-\lambda_j) = 1$ for all $j \neq i$, $x^{m_j}-\lambda_j$ divides $a_{\varsigma,j}(x)\mathcal{T}_k^{(j)}(b_j(x))$ for each ς. This implies that $\mathcal{T}_k^{(j)}\Big(\frac{x^{m_j}-\lambda_j}{w_j(x)}\Big)$ divides $b_j(x)$ for each j. This gives $b(x) \in \langle H_1(x), H_2(x), \cdots, H_\ell(x)\rangle$, from which the desired result follows. □

In the following theorem, we obtain a BCH type lower bound on minimum Hamming distances of ϱ-generator Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 3.4.3. *Let* $\mathcal{C} = \big\langle a_1(x), a_2(x), \cdots, a_\varrho(x)\big\rangle$ *be a* ϱ*-generator* Λ*-MT code of length* n *over* $\mathbb{F}_q$*, where* $a_\varsigma(x) = (a_{\varsigma,1}(x), a_{\varsigma,2}(x), \cdots, a_{\varsigma,\ell}(x))$ *for* $1 \leq \varsigma \leq \varrho$*. Then the minimum Hamming distance* $d_{\min}(\mathcal{C})$ *of the code* $\mathcal{C}$ *satisfies*

$$d_{\min}(\mathcal{C}) \geq \min_{1\leq i\leq \ell}(b_i+1),$$

where for each i*,* b_i *is the maximum number of consecutive exponents of zeros of*

gcd$(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x), x^{m_i}-\lambda_i)$ *over* $\mathbb{F}_q$. *(Here* $d_{\min}(\mathcal{C})$ *denotes the minimum Hamming distance of the code* $\mathcal{C}$*.)*

Proof. To prove the result, let $B_i(x) = (0, \cdots, 0, \underbrace{w_i(x)}_{i^{th}}, 0, \cdots, 0) \in V$, where $w_i(x) = \gcd(a_{1,i}(x), a_{2,i}(x), \cdots, a_{\varrho,i}(x), x^{m_i}-\lambda_i)$ for $1 \leq i \leq \ell$. Now let $\mathcal{C}' = \langle B_1(x), B_2(x), \cdots, B_\ell(x)\rangle$ be a Λ-MT code of length n over $\mathbb{F}_q$. Here for $1 \leq \varsigma \leq \varrho$, we observe that $a_\varsigma(x) = \sum_{i=1}^{\ell} \frac{a_{\varsigma,i}(x)}{w_i(x)} B_i(x)$, which implies that $\mathcal{C} \subseteq \mathcal{C}'$. From this, we obtain $d_{\min}(\mathcal{C}) \geq d_{\min}(\mathcal{C}')$. Next for $1 \leq i \leq \ell$, if π_i is the projection of V onto $\frac{\mathbb{F}_q[x]}{\langle x^{m_i}-\lambda_i\rangle}$, then $\pi_i(\mathcal{C}')$ is a λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ having the generator polynomial $w_i(x)$. Now if b_i is the maximum number of consecutive exponents of zeros of $w_i(x)$, then working in a similar manner as in Theorem 8 of [57, Ch. 7], we see that $d_{\min}(\pi_i(\mathcal{C}')) \geq b_i+1$. Further, we observe that if the ith block $c_i \in \mathbb{F}_q^{m_i}$ of a codeword $c = (c_1, c_2, \cdots, c_\ell) \in \mathcal{C}'$ is non-zero, then the Hamming weight $w_H(c_i)$ of c_i satisfies $w_H(c_i) \geq b_i + 1$. This implies that $w_H(c) \geq \min_{1\leq i\leq \ell}(b_i + 1)$ for each $c(\neq 0) \in \mathcal{C}'$. From this, we obtain the desired result. □

Next for $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, $\Omega = (\omega_1, \omega_2, \cdots, \omega_\ell) \in \mathbb{F}_q^\ell$, let us define $\mathcal{I}_{\Lambda,\Omega} = \{i : 1 \leq i \leq \ell, \lambda_i \neq \omega_i\}$ and $\Lambda - \Omega = (\lambda_1 - \omega_1, \lambda_2 - \omega_2, \cdots, \lambda_\ell - \omega_\ell)$. For $1 \leq i \leq \ell$, let π_i be the projection of V onto V_i. If $\mathcal{C}$ is a Λ-MT code of length n over $\mathbb{F}_q$, then one can easily observe that $\pi_i(\mathcal{C})$ is a λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ for $1 \leq i \leq \ell$. In the following theorem, we obtain a lower bound on the dimension of some $[\Lambda, \Omega]$-MT codes of length n over $\mathbb{F}_q$, where $\Lambda \neq \Omega$.

Theorem 3.4.4. *Let* $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ *and* $\Omega = (\omega_1, \omega_2, \cdots, \omega_\ell)$*, where* λ_i, ω_i*'s are non-zero elements of* $\mathbb{F}_q$*. Let* $\mathcal{C}$ *be a* Λ*-MT and an* Ω*-MT code of length* n *over* $\mathbb{F}_q$*. Let* $\mathcal{J}_\mathcal{C} = \{i : 1 \leq i \leq \ell, \pi_i(\mathcal{C}) \neq \{0\}\}$*. If* $\mathcal{I}_{\Lambda,\Omega} \cap \mathcal{J}_\mathcal{C}$ *is a non-empty set, then we have* $dim_{\mathbb{F}_q}\mathcal{C} \geq \max_{i\in\mathcal{I}_{\Lambda,\Omega}\cap\mathcal{J}_\mathcal{C}}\{m_i\}$.

As a consequence, if $\lambda_i \neq \omega_i$ *and* $\pi_i(\mathcal{C}) \neq \{0\}$ *for* $1 \leq i \leq \ell$*, then we have*

$$dim_{\mathbb{F}_q}\mathcal{C} \geq \max\{m_1, m_2, \cdots, m_\ell\}.$$

Proof. For each $i \in \mathcal{I}_{\Lambda,\Omega} \cap \mathcal{J}_{\mathcal{C}}$, as $\pi_i(\mathcal{C}) \neq \{0\}$, there exists a codeword $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots, c_{\ell,m_\ell-1}) \in \mathcal{C}$ such that $c_{i,m_i-1} \neq 0$. As $\mathcal{C}$ is a both Λ-MT and Ω-MT code, we note that $T_\Lambda(c), T_\Omega(c) \in \mathcal{C}$, which implies that $T_{\Lambda-\Omega}(c) = T_\Lambda(c) - T_\Omega(c) = ((\lambda_1 - \omega_1)c_{1,m_1-1}, 0, \cdots, 0; (\lambda_2 - \omega_2)c_{2,m_2-1}, 0, \cdots, 0; \cdots; (\lambda_\ell - \omega_\ell)c_{\ell,m_\ell-1}, 0, \cdots, 0) \in \mathcal{C}$. Further, for each $i \in \mathcal{I}_{\Lambda,\Omega} \cap \mathcal{J}_{\mathcal{C}}$, we see that $(\lambda_i - \omega_i)c_{i,m_i-1}$ is non-zero, which implies that $T_{\Lambda-\Omega}(c), T^2_{\Lambda-\Omega}(c), \cdots\cdots, T^{m_i}_{\Lambda-\Omega}(c) \in \mathcal{C}$ are linearly independent over $\mathbb{F}_q$, and hence $\dim_{\mathbb{F}_q}\mathcal{C} \geq m_i$. From this, it follows that $\dim_{\mathbb{F}_q}\mathcal{C} \geq \max\limits_{i \in \mathcal{I}_{\Lambda,\Omega} \cap \mathcal{J}_{\mathcal{C}}} \{m_i\}$. □

In the next two theorems, we derive sufficient conditions under which a Λ-MT code is Euclidean (or Hermitian) LCD. However, these conditions are not necessary for a Λ-MT code to be Euclidean (or Hermitian) LCD, which we will illustrate in Examples 3.4.3 and 3.4.4.

Theorem 3.4.5. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$ satisfying $\lambda_i \neq \lambda_i^{-p^k}$ for $1 \leq i \leq \ell$. Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$. Then according as k is either 0 or $\frac{r}{2}$ with r even, the following hold.*

(a) If either $\dim_{\mathbb{F}_q}\mathcal{C} < \min\limits_{1 \leq i \leq \ell}\{m_i\}$ or $\dim_{\mathbb{F}_q}\mathcal{C}^{\perp_k} < \min\limits_{1 \leq i \leq \ell}\{m_i\}$, then $\mathcal{C}$ is a Euclidean (or Hermitian) LCD code.

(b) If $\dim_{\mathbb{F}_q}\mathcal{C} = \min\limits_{1 \leq i \leq \ell}\{m_i\}$, then $\mathcal{C}$ is either a Euclidean (or Hermitian) LCD or a Euclidean (or Hermitian) self-orthogonal code.

(c) If $\dim_{\mathbb{F}_q}\mathcal{C}^{\perp_k} = \min\limits_{1 \leq i \leq \ell}\{m_i\}$, then $\mathcal{C}$ is either a Euclidean (or Hermitian) LCD or a Euclidean (or Hermitian) dual-containing code (i.e., $\mathcal{C}^{\perp_k} \subseteq \mathcal{C}$).

(d) If $\dim_{\mathbb{F}_q}\mathcal{C} = \dim_{\mathbb{F}_q}\mathcal{C}^{\perp_k} = \min\limits_{1 \leq i \leq \ell}\{m_i\}$, then $\mathcal{C}$ is either a Euclidean (or Hermitian) LCD or a Euclidean (or Hermitian) self-dual code.

Proof. (a) Note that $\mathcal{C} \cap \mathcal{C}^{\perp_k}$ is both a Λ-MT and a Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$. We assert that $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$. Then by Theorem 3.4.4, we get

$\dim_{\mathbb{F}_q}(\mathcal{C} \cap \mathcal{C}^{\perp_k}) \geq \min\limits_{1\leq i\leq \ell}\{m_i\}$. Since $\mathcal{C} \cap \mathcal{C}^{\perp_k}$ is a subspace of both $\mathcal{C}$ and $\mathcal{C}^{\perp_k}$, we get $\dim_{\mathbb{F}_q}\mathcal{C} \geq \min\limits_{1\leq i\leq \ell}\{m_i\}$ and $\dim_{\mathbb{F}_q}\mathcal{C}^{\perp_k} \geq \min\limits_{1\leq i\leq \ell}\{m_i\}$, which contradicts our hypothesis. So we must have $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$.

(b) If $\mathcal{C} \cap \mathcal{C}^{\perp_k} \neq \{0\}$, then working as in part (a), we see that $\dim_{\mathbb{F}_q}(\mathcal{C} \cap \mathcal{C}^{\perp_k}) \geq \min\limits_{1\leq i\leq \ell}\{m_i\}$. Now as $\dim_{\mathbb{F}_q}\mathcal{C} = \min\limits_{1\leq i\leq \ell}\{m_i\}$, we get $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \mathcal{C}$, which implies that $\mathcal{C} \subseteq \mathcal{C}^{\perp_k}$. This proves (b).

(c) Its proof is similar to that of part (b).

(d) It follows immediately from parts (b) and (c).

□

Theorem 3.4.6. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$ satisfying $\lambda_i \neq \lambda_i^{-p^k}$ for $1 \leq i \leq \ell$. Let $\mathcal{C}$ be a ϱ-generator Λ-MT code of length n over $\mathbb{F}_q$ such that either $\pi_i(\mathcal{C}) \neq <1>$ or $\pi_i(\mathcal{C}^{\perp_k}) \neq <1>$ for $1 \leq i \leq \ell$. Then $\mathcal{C}$ is either a Euclidean or a Hermitian LCD code, according as k is either 0 or $\frac{r}{2}$ with r even.*

Proof. For $1 \leq i \leq \ell$, we see that the linear code $\pi_i(\mathcal{C}) \cap \pi_i(\mathcal{C}^{\perp_k})$ is both λ_i-constacyclic and $\lambda_i^{-p^k}$-constacyclic code of length m_i over $\mathbb{F}_q$. Further, for each i, as $\lambda_i \neq \lambda_i^{-p^k}$, by Corollary 2.7 of Dinh [32], we see that either $\pi_i(\mathcal{C}) \cap \pi(\mathcal{C}^{\perp_k}) = \{0\}$ or $\pi_i(\mathcal{C}) \cap \pi(\mathcal{C}^{\perp_k}) = \langle 1\rangle$. Now since either $\pi_i(\mathcal{C}) \neq \langle 1\rangle$ or $\pi_i(\mathcal{C}^{\perp_k}) \neq \langle 1\rangle$, we get $\pi_i(\mathcal{C}) \cap \pi(\mathcal{C}^{\perp_k}) = \{0\}$ for each i. As $\pi_i(\mathcal{C} \cap \mathcal{C}^{\perp_k})$ is a subspace of $\pi_i(\mathcal{C}) \cap \pi_i(\mathcal{C}^{\perp_k})$, we get $\pi_i(\mathcal{C} \cap \mathcal{C}^{\perp_k}) = 0$ for $1 \leq i \leq \ell$. This implies that $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$ i.e., $\mathcal{C}$ is a Euclidean (resp. Hermitian) LCD code when $k = 0$ (resp. $k = \frac{r}{2}$ with r even). □

From Theorems 3.4.2 and 3.4.6, we deduce the following:

Corollary 3.4.7. *Let k be either 0 or $\frac{r}{2}$ with r even. Let $\lambda_1, \lambda_2, \cdots, \lambda_\ell \in \mathbb{F}_q \setminus \{0\}$ be such that $\lambda_i \neq \lambda_i^{-p^k}$ for $1 \leq i \leq \ell$ and the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ are pairwise coprime in $\mathbb{F}_q[x]$. Then any Λ-MT code of length n over $\mathbb{F}_q$ is either a Euclidean or a Hermitian LCD code, according as k is either 0 or $\frac{r}{2}$ with r even.*

In the following example, we illustrate Theorems 3.4.5(a) and 3.4.6.

Example 3.4.2. *Let $q = 5$, $\ell = 2$, $m_1 = m_2 = 3$, $\Lambda = (3, 2)$ and $\mathbb{F}_5 = \mathbb{Z}_5$. Here we have $V = V_1 \times V_2 = \frac{\mathbb{F}_5[x]}{\langle x^3-3\rangle} \times \frac{\mathbb{F}_5[x]}{\langle x^3-2\rangle}$. Now we see that the irreducible factorizations of the polynomials $x^3 - 3$ and $x^3 - 2$ over $\mathbb{F}_5$ are given by $x^3 - 3 = (x + 3)(x^2 + 2x + 4)$ and $x^3 - 2 = (x + 2)(x^2 + 3x + 4)$, respectively. Let $\mathcal{C}$ be a 1-generator Λ-MT code of length 6 over $\mathbb{F}_5$ with the generating set $\{(x + 3, x + 2)\}$. It is easy to observe that $\pi_1(\mathcal{C}) = \big\langle \gcd(x + 3, x^3 - 3)\big\rangle = \big\langle x + 3\big\rangle \neq \big\langle 1\big\rangle$ and $\pi_2(\mathcal{C}) = \big\langle \gcd(x + 2, x^3 - 2)\big\rangle = \big\langle x+2\big\rangle \neq \big\langle 1\big\rangle$. So by Theorem 3.4.6, we see that $\mathcal{C}$ is a Euclidean LCD code. On the other hand, we note that $V' = V_1' \times V_2' = \frac{\mathbb{F}_5[x]}{\langle x^3-2\rangle} \times \frac{\mathbb{F}_5[x]}{\langle x^3-3\rangle}$. By Theorem 3.4.2, we obtain $\mathcal{C}^{\perp_0} = \big\langle (x^2 + 3x + 4, 0), (0, x^2 + 2x + 4)\big\rangle$. It is easy to see that $\mathcal{C}_1^{\perp_0} = Span_{F_1}\{(2, 0)\}$, $\mathcal{C}_2^{\perp_0} = Span_{F_2}\{(0, 2)\}$ and $\mathcal{C}_3^{\perp_0} = \mathcal{C}_4^{\perp_0} = \{0\}$, where $F_1 \simeq F_2 \simeq \mathbb{F}_5$. Using Theorem 3.2.2, we get $dim_{\mathbb{F}_5}\mathcal{C}^{\perp_0} = 2$. By applying Theorem 3.4.5(a) also, we see that $\mathcal{C}$ is a Euclidean LCD code.*

In the following example, we show that the sufficient conditions derived in Theorems 3.4.5(a) are not necessary for a Λ-MT code to be Euclidean (or Hermitian) LCD.

Example 3.4.3. *Let $q = 7$, $\ell = 2$, $m_1 = m_2 = 2$, $\Lambda = (2, 5)$ and $\mathbb{F}_7 = \mathbb{Z}_7$. Here we have $r = 1$, $V = V_1 \times V_2 = \frac{\mathbb{F}_7[x]}{\langle x^2-2\rangle} \times \frac{\mathbb{F}_7[x]}{\langle x^2-5\rangle}$ and $V' = V_1' \times V_2' = \frac{\mathbb{F}_7[x]}{\langle x^2-4\rangle} \times \frac{\mathbb{F}_7[x]}{\langle x^2-3\rangle}$. It is easy to see that the polynomials x^2-3 and x^2-5 are irreducible over $\mathbb{F}_7$, and that the irreducible factorizations of the polynomials $x^2 - 3$ and $x^2 - 5$ over $\mathbb{F}_7$ are given by $x^2-2 = (x+3)(x+4)$ and $x^2-4 = (x+2)(x+5)$, respectively. Let $\mathcal{C}$ be a 1-generator Λ-MT code of length 4 over $\mathbb{F}_7$ with the generating set $\{(x+1, 0)\}$. It is easy to observe that $\pi_1(\mathcal{C}) = \big\langle \gcd(x+1, x^2-2)\big\rangle = \big\langle 1\big\rangle$ and $\pi_2(\mathcal{C}) = \big\langle \gcd(0, x^2-5)\big\rangle = \{0\}$. Further, as the polynomials x^2-2 and x^2-5 are coprime over $\mathbb{F}_7$, by applying Theorem 3.4.2, we obtain $\mathcal{C}^{\perp_0} = \big\langle (0, 0), (0, 1)\big\rangle$. From this, we get $\pi_1(\mathcal{C}^{\perp_0}) = \big\langle \gcd(0, 0, x^2-4)\big\rangle = \{0\}$ and $\pi_2(\mathcal{C}^{\perp_0}) = \big\langle \gcd(0, 1, x^2 - 3)\big\rangle = \big\langle 1\big\rangle$. Therefore by Theorem 3.4.6, we see that $\mathcal{C}$ is a Euclidean LCD code. On the other hand, by applying Theorem 3.4.1(a), we*

get $h(x) = x^2 - 2$. *Using Theorem 3.4.1(b), we get* $dim_{\mathbb{F}_7}\mathcal{C} = 2$. *Further, it is easy to see that* $\mathcal{C}_1^{\perp_0} = \mathcal{C}_2^{\perp_0} = \{0\}$ *and* $\mathcal{C}_3^{\perp_0} = Span_{F_3}\{(0,1)\}$, *where* $F_3 = \frac{\mathbb{F}_7[x]}{\langle x^2-3\rangle} \simeq \mathbb{F}_{49}$. *By Theorem 3.2.2, we get* $dim_{\mathbb{F}_7}\mathcal{C}^{\perp_0} = 2$. *This shows that the code* $\mathcal{C}$ *does not satisfy hypotheses of Theorem 3.4.5(a).*

In the following example, we show that the sufficient conditions derived in Theorems 3.4.6 are not necessary for a Λ-MT code to be Euclidean (or Hermitian) LCD.

Example 3.4.4. *Let* $q = 5$, $\ell = 2$, $m_1 = m_2 = 3$, $\Lambda = (3,3)$ *and* $\mathbb{F}_5 = \mathbb{Z}_5$. *Here we have* $r = 1$, $V = V_1 \times V_2 = \frac{\mathbb{F}_5[x]}{\langle x^3-3\rangle} \times \frac{\mathbb{F}_5[x]}{\langle x^3-3\rangle}$ *and* $V' = V_1' \times V_2' = \frac{\mathbb{F}_5[x]}{\langle x^3-2\rangle} \times \frac{\mathbb{F}_5[x]}{\langle x^3-2\rangle}$. *It is easy to see that the irreducible factorizations of the polynomials* x^3-3 *and* x^3-2 *over* $\mathbb{F}_5$ *are given by* $x^3-3 = (x-2)(x^2+2x+4)$ *and* $x^3-2 = (x-3)(x^2+3x+4)$, *respectively. Now let* $g_1(x) = x-2, g_2(x) = x^2+2x+4, h_1(x) = x-3$ *and* $h_2(x) = x^2+3x+4$. *Here we can easily observe that* $\mathscr{T}_0(g_1(x)) = h_1(x)$ *and* $\mathscr{T}_0(g_2(x)) = h_2(x)$. *Let* $\mathcal{C}$ *be a 1-generator* Λ*-MT code of length 6 over* $\mathbb{F}_5$ *with the generating set* $\{(1, x+1)\}$. *By applying Chinese Remainder Theorem, we get* $V = \big(F_1, F_1\big) \oplus (F_2, F_2\big)$ *and* $V' = \big(H_1, H_1\big) \oplus (H_2, H_2\big)$, *where* $F_w = \frac{\mathbb{F}_5[x]}{\langle g_w(x)\rangle}$ *and* $H_w = \frac{\mathbb{F}_5[x]}{\langle h_w(x)\rangle}$ *for* $1 \leq w \leq 2$. *From this and applying Theorem 3.2.2, we see that the constituents of* $\mathcal{C}$ *are given by* $\mathcal{C}_1 = \langle(1,3)\rangle$ *and* $\mathcal{C}_2 = \langle(1, x+1)\rangle$. *Further, in view of* (3.4), *we obtain* $\mathcal{C}_1^{\perp_0} = \langle(-3,1)\rangle$ *and* $\mathcal{C}_2^{\perp_0} = \langle(1, 2x+3)\rangle$. *Now by applying Chinese Remainder Theorem, we get* $\mathcal{C}^{\perp_0}$ *is generated by* $(-2x^2 - x + 3, x^2 + 2)$. *Moreover, it is easy to see that* $\pi_1(\mathcal{C}) = \big\langle \gcd(1, x^3-3)\big\rangle = \big\langle 1\big\rangle$, $\pi_2(\mathcal{C}) = \big\langle \gcd(x+1, x^3-3)\big\rangle = \big\langle 1\big\rangle$, $\pi_1(\mathcal{C}^{\perp_0}) = \big\langle \gcd(-2x^2 - x + 3, x^3 - 2)\big\rangle = \big\langle 1\big\rangle$ *and* $\pi_2(\mathcal{C}^{\perp_0}) = \big\langle \gcd(x^2+2, x^3-2)\big\rangle = \big\langle 1\big\rangle$, *which shows that the code* $\mathcal{C}$ *does not satisfy the hypotheses of Theorem 3.4.6. On the other hand, by Theorem 3.2.2, we have* $dim_{\mathbb{F}_5}\mathcal{C} = 3$ *and* $dim_{\mathbb{F}_5}\mathcal{C}^{\perp_0} = 3$. *It is easy to observe that* $\mathcal{C} \neq \mathcal{C}^{\perp_0}$. *Therefore by Theorem 3.4.5(d), we see that* $\mathcal{C}$ *is a Euclidean LCD code.*

3.5 Trace description of MT codes

In this section, we shall provide a trace description for Λ-MT codes of length n over $\mathbb{F}_q$ by extending the work of Güneri et al. [41] to Λ-MT codes. Towards this, for $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$, we recall that if $\epsilon_{w,i} = 1$, then $g_w(x)$ divides $x^{m_i} - \lambda_i$ in $\mathbb{F}_q[x]$, and the ideal $\left\langle \frac{x^{m_i}-\lambda_i}{g_w(x)} \right\rangle$ is a minimal λ_i-constacyclic code of length m_i over $\mathbb{F}_q$, whose generating idempotent is denoted by $\Theta_{w,i}$. If $\epsilon_{w,i} = 0$ for some w and i, then we shall denote the zero codeword of length m_i by $\Theta_{w,i}$. Now by Theorem 3.1 of Sharma and Rani [72], we see that there exist ring isomorphisms $\phi_{w,i} : \langle \Theta_{w,i} \rangle \to \epsilon_{w,i} F_w$ and $\psi_{w,i} : \epsilon_{w,i} F_w \to \langle \Theta_{w,i} \rangle$, defined as

$$\phi_{w,i}(a(x)) = \epsilon_{w,i} a(\delta_w) \text{ for all } a(x) \in \langle \Theta_{w,i} \rangle$$

and

$$\psi_{w,i}(\gamma) = \frac{1}{m_i}\big(Tr_{F_w/\mathbb{F}_q}(\gamma), Tr_{F_w/\mathbb{F}_q}(\gamma\delta_w^{-1}), \cdots, Tr_{F_w/\mathbb{F}_q}(\gamma\delta_w^{-(m_i-1)})\big) \text{ for all } \gamma \in \epsilon_{w,i} F_w, \tag{3.6}$$

where $Tr_{F_w/\mathbb{F}_q}$ is the trace map from F_w onto $\mathbb{F}_q$ and δ_w is a zero of $g_w(x)$ in F_w. Further, note that the ring isomorphisms $\phi_{w,i}$ and $\psi_{w,i}$ are inverses of each other, and that $\psi_{w,i}(\epsilon_{w,i} 1_w) = \Theta_{w,i}$, where 1_w is the multiplicative identity of F_w. We shall view $V = \prod_{i=1}^{\ell} V_i$ and $\mathcal{G}_w = \big(\epsilon_{w,1} F_w, \epsilon_{w,2} F_w, \cdots, \epsilon_{w,\ell} F_w\big)$ as rings with respect to the coordinate-wise addition $+$ and coordinate-wise multiplication $\odot$ for each w. In view of this, $1_V := (1, 1, \cdots, 1)$ and $1_{\mathcal{G}_w} := (\epsilon_{w,1} 1_w, \cdots, \epsilon_{w,\ell} 1_w)$ respectively are the multiplicative identities of V and $\mathcal{G}_w$ for each w. Now for $1 \leq w \leq \rho$, let us define the maps $\Phi_w : V \to \mathcal{G}_w$ and $\Psi_w : \mathcal{G}_w \to V$ as

$$\Phi_w(a_1(x), a_2(x), \cdots, a_\ell(x)) = (\epsilon_{w,1} a_1(\delta_w), \epsilon_{w,2} a_2(\delta_w), \cdots, \epsilon_{w,\ell} a_\ell(\delta_w))$$

for each $(a_1(x), a_2(x), \cdots, a_\ell(x)) \in V$ and

$$\Psi_w(\gamma_1, \gamma_2, \cdots, \gamma_\ell) = (\psi_{w,1}(\gamma_1), \psi_{w,2}(\gamma_2), \cdots, \psi_{w,\ell}(\gamma_\ell)) \text{ for each } (\gamma_1, \gamma_2, \cdots, \gamma_\ell) \in \mathcal{G}_w.$$

Note that both Φ_w and Ψ_w are $\mathbb{F}_q$-linear maps and are ring homomorphisms. Moreover, for each w, the restriction map $\Phi_w \restriction_{(\langle\Theta_{w,1}\rangle, \langle\Theta_{w,2}\rangle, \cdots, \langle\Theta_{w,\ell}\rangle)}$ and the map Ψ_w are inverses of each other. For $1 \leq w \leq \rho$, let us define $\Theta_w = (\Theta_{w,1}, \Theta_{w,2}, \cdots, \Theta_{w,\ell})$. It is easy to see that $V = \bigoplus_{w=1}^{\rho} \langle\Theta_w\rangle$, $\sum_{w=1}^{\rho} \Theta_w = 1_V$, $\langle\Theta_w\rangle = (\langle\Theta_{w,1}\rangle, \langle\Theta_{w,2}\rangle, \cdots, \langle\Theta_{w,\ell}\rangle)$, $\Theta_w \odot \Theta_w = \Theta_w$, $\Theta_{w'} \odot \Theta_w = 0$ for each $w \neq w'$.

Next the concatenation of $\langle\Theta_w\rangle = (\langle\Theta_{w,1}\rangle, \langle\Theta_{w,2}\rangle, \cdots, \langle\Theta_{w,\ell}\rangle)$ and a linear code $\mathcal{D}$ of length ℓ over $F_w \simeq \mathbb{F}_{q^{d_w}}$ is defined as

$$\langle\Theta_w\rangle \square \mathcal{D} = \big\{(\psi_{w,1}(x_{w,1}), \psi_{w,2}(x_{w,2}), \cdots, \psi_{w,\ell}(x_{w,\ell})) : x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{D}\big\}.$$

In the following theorem, we shall view Λ-MT codes as direct sums of certain concatenated codes.

Theorem 3.5.1. *(a) Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$. If $\tilde{\mathcal{C}_w} := \mathcal{C} \odot \Theta_w$ for $1 \leq w \leq \rho$, then we have $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle\Theta_w\rangle \square \Phi_w(\tilde{\mathcal{C}_w})$. Moreover, $\mathcal{C}_w = \Phi_w(\tilde{\mathcal{C}_w})$ holds for $1 \leq w \leq \rho$. As a consequence, we have $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle\Theta_w\rangle \square \mathcal{C}_w$.*

(b) Conversely, let $\mathfrak{C}_w (\subseteq \mathcal{G}_w)$ be a linear code of length ℓ over F_w for $1 \leq w \leq \rho$. Then $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle\Theta_w\rangle \square \mathfrak{C}_w$ is a Λ-MT code of length n over $\mathbb{F}_q$.

Proof. (a) To prove the result, we note that

$$\mathcal{C} = \mathcal{C} \odot 1_V = \mathcal{C} \odot \Big(\sum_{w=1}^{\rho} \Theta_w\Big) = \bigoplus_{w=1}^{\rho} \mathcal{C} \odot \Theta_w = \bigoplus_{w=1}^{\rho} \tilde{\mathcal{C}_w}.$$

For $1 \leq w \leq \rho$, we see that

$$\tilde{\mathcal{C}_w} = \big\{ \big(c_1(x)\Theta_{w,1}, c_2(x)\Theta_{w,2}, \cdots, c_\ell(x)\Theta_{w,\ell}\big) : \big(c_1(x), c_2(x), \cdots, c_\ell(x)\big) \in \mathcal{C} \big\},$$

which implies that

$$\begin{aligned}
\Phi_w(\tilde{\mathcal{C}_w}) &= \big\{ \big(\phi_{w,1}(c_1(x)\Theta_{w,1}), \phi_{w,2}(c_2(x)\Theta_{w,2}), \cdots, \phi_{w,\ell}(c_\ell(x)\Theta_{w,\ell})\big) \\
&\qquad : (c_1(x), c_2(x), \cdots, c_\ell(x)) \in \mathcal{C} \big\} \\
&= \big\{ \big(\epsilon_{w,1}c_1(\delta_w), \epsilon_{w,2}c_2(\delta_w), \cdots, \epsilon_{w,\ell}c_\ell(\delta_w)\big) : \big(c_1(x), c_2(x), \cdots, c_\ell(x)\big) \in \mathcal{C} \big\} \\
&= \mathcal{C}_w,
\end{aligned}$$

as $\phi_{w,i}(\Theta_{w,i}) = \epsilon_{w,i}1_w$ for each i and w. Further, since the restriction map $\Phi_w \restriction_{\langle\Theta_w\rangle}$ and the map Ψ_w are inverses of each other, we see that $\langle\Theta_w\rangle \square \Phi_w(\tilde{\mathcal{C}_w}) = \tilde{\mathcal{C}_w}$ for each w. From this, part (a) follows.

(b) To prove this, it is enough to prove that $\langle\Theta_w\rangle \square \mathfrak{C}_w$ is a Λ-MT code of length n over $\mathbb{F}_q$ for $1 \leq w \leq \rho$. For this, we observe that $\langle\Theta_w\rangle \square \mathfrak{C}_w = \{\Psi_w\big(x_w\big) : x_w \in \mathfrak{C}_w\}$. It is easy to see that $\Psi_w\big(x_w\big) + \Psi_w\big(y_w\big) = \Psi_w\big(x_w + y_w\big) \in \langle\Theta_w\rangle \square \mathfrak{C}_w$ for each $x_w, y_w \in \mathfrak{C}_w$. Further, for each $f(x) \in \mathbb{F}_q[x]$, we note that $f(\delta_w) \in F_w$ and that $f(\delta_w)x_w \in \mathfrak{C}_w$ for each $x_w = \big(x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}\big) \in \mathfrak{C}_w$. This implies that

$$\begin{aligned}
&\Psi_w\big(f(\delta_w)x_w\big) \\
&= \big(\psi_{w,1}(f(\delta_w))\psi_{w,1}(x_{w,1}), \psi_{w,2}(f(\delta_w))\psi_{w,2}(x_{w,2}), \cdots, \psi_{w,\ell}(f(\delta_w))\psi_{w,\ell}(x_{w,\ell})\big) \\
&= \big(f(x)\Theta_{w,1}\psi_{w,1}(x_{w,1}), f(x)\Theta_{w,2}\psi_{w,2}(x_{w,2}), \cdots, f(x)\Theta_{w,\ell}\psi_{w,\ell}(x_{w,\ell})\big) \\
&= \big(f(x)\psi_{w,1}(x_{w,1}), f(x)\psi_{w,2}(x_{w,2}), \cdots, f(x)\psi_{w,\ell}(x_{w,\ell})\big) \\
&= f(x)\Psi_w(x_w),
\end{aligned}$$

as $\psi_{w,i}(x_{w,i}) \in \langle\Theta_{w,i}\rangle$ and $\Theta_{w,i}$ is the unity of $\langle\Theta_{w,i}\rangle$ for $1 \leq i \leq \ell$. This shows

that $f(x)\Psi_w(x_w) \in \langle\Theta_w\rangle \,\square\, \mathfrak{C}_w$ for each $f(x) \in \mathbb{F}_q[x]$ and $x_w \in \mathfrak{C}_w$. From this, it follows that $\langle\Theta_w\rangle \,\square\, \mathfrak{C}_w$ is an $\mathbb{F}_q[x]$-submodule of V for each w, which proves (b).

□

In the following theorem, we provide a trace description for Λ-MT codes of length n over $\mathbb{F}_q$ using their concatenated structure.

Theorem 3.5.2. *Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$. For $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w$ with $1 \le w \le \rho$, let us define*

$$c_i(x_1, x_2, \cdots, x_\rho) = \frac{1}{m_i}\Big(\sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}), \sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}\delta_w^{-1}), \cdots, \sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}\delta_w^{-(m_i-1)})\Big)$$

for $1 \le i \le \ell$. Then we have

$$\mathcal{C} = \big\{\big(c_1(x_1, x_2, \cdots, x_\rho), c_2(x_1, x_2, \cdots, x_\rho), \cdots, c_\ell(x_1, x_2, \cdots, x_\rho)\big) : x_w \in \mathcal{C}_w \text{ for } 1 \le w \le \rho\big\}.$$

Proof. By Theorem 3.5.1, we see that the code $\mathcal{C}$ has the concatenated structure $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle\Theta_w\rangle \square \mathcal{C}_w$, where $\langle\Theta_w\rangle \square \mathcal{C}_w = \big\{(\psi_{w,1}(x_{w,1}), \psi_{w,2}(x_{w,2}), \cdots, \psi_{w,\ell}(x_{w,\ell})) : x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w\big\}$. From this, we get

$$\mathcal{C} = \Big\{(\sum_{w=1}^{\rho} \psi_{w,1}(x_{w,1}), \sum_{w=1}^{\rho} \psi_{w,2}(x_{w,2}), \cdots, \sum_{w=1}^{\rho} \psi_{w,\ell}(x_{w,\ell})) : x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w\Big\}.$$

Further, for $1 \le i \le \ell$, we see, by (3.6), that

$$\sum_{w=1}^{\rho} \psi_{w,i}(x_{w,i}) = \frac{1}{m_i}\Big(\sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}), \sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}\delta_w^{-1}), \cdots,$$

$$\sum_{w=1}^{\rho} Tr_{F_w/\mathbb{F}_q}(x_{w,i}\delta_w^{-(m_i-1)})\Big).$$

From this, the desired result follows immediately. □

We shall illustrate the above theorem in the following example:

Example 3.5.1. *Let $q = 7$, $\ell = 2$, $m_1 = 2$, $m_2 = 4$, $\Lambda = (2, 4)$ and $\mathbb{F}_7 = \mathbb{Z}_7$. Here we have $V = V_1 \times V_2$, where $V_1 = \frac{\mathbb{F}_7[x]}{\langle x^2-2\rangle}$ and $V_2 = \frac{\mathbb{F}_7[x]}{\langle x^4-4\rangle}$. Further, we see that the irreducible factorizations of the polynomials $x^2 - 2$ and $x^4 - 4$ over $\mathbb{F}_7$ are given by $x^2 - 2 = (x + 3)(x + 4), x^4 - 4 = (x + 3)(x + 4)(x^2 + 2)$. If we take $g_1(x) = x + 3, g_2(x) = x + 4$ and $g_3(x) = x^2 + 2$, then we have $F_1 \simeq F_2 \simeq \mathbb{F}_7$ and $F_3 \simeq \mathbb{F}_{49}$. From this and by applying Chinese Remainder Theorem, we get $V \simeq (F_1, F_1) \oplus (F_2, F_2) \oplus (\{0\}, F_3)$. Now if $\mathcal{C}$ is a $(2, 4)$-MT code of length 6 over $\mathbb{F}_7$ with the constituents $\mathcal{C}_1$, $\mathcal{C}_2$ and $\mathcal{C}_3$, then by Theorem 3.5.2, the code $\mathcal{C}$ is given by*

$$\Big\{\big(c_{1,0}, c_{1,1}; c_{2,0}, c_{2,1}, c_{2,2}, c_{2,3}\big) : (a, b) \in \mathcal{C}_1, (c, d) \in \mathcal{C}_2, (0, e + \delta_3 f) \in \mathcal{C}_3\Big\},$$

where $c_{1,0} = \frac{a+c}{2}, c_{1,1} = \frac{2a+5c}{2}, c_{2,0} = \frac{b+d+2e}{4}, c_{2,1} = \frac{2b+5d+2f}{4}, c_{2,2} = \frac{4b+4d+2e\delta_3^{-2}}{4}, c_{2,3} = \frac{b-d+2f\delta_3^{-2}}{4}$ and δ_3 is a root of the polynomial $g_3(x)$ in F_3.

In the following theorem, we obtain a minimum distance bound for Λ-MT codes of length n over $\mathbb{F}_q$ using their multilevel concatenated structure.

Theorem 3.5.3. *Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the non-zero constituents $\mathcal{C}_{w_1}, \mathcal{C}_{w_2}, \cdots, \mathcal{C}_{w_t}$, where $1 \leq w_1, w_2, \cdots, w_t \leq \rho$. Let $\mathfrak{d}_j$ be the minimum Hamming distance of the code $\mathcal{C}_{w_j}$ for $1 \leq j \leq t$. Let us assume that $\mathfrak{d}_1 \leq \mathfrak{d}_2 \leq \cdots \leq \mathfrak{d}_t$. Let us define $\mathfrak{K}_v = \min\limits_{\substack{I\subseteq\{1,2,\cdots,\ell\}\\ |I|=\mathfrak{d}_v}} \Big\{ \sum\limits_{g\in I} d_{\min}(\langle\Theta_{w_1,g}\rangle \oplus \langle\Theta_{w_2,g}\rangle \oplus \cdots \oplus \langle\Theta_{w_t,g}\rangle)\Big\}$ for $v \in \{1, 2, \cdots, t\}$. Then the minimum Hamming distance $d_{\min}(\mathcal{C})$ of the code $\mathcal{C}$ satisfies*

$$d_{\min}(\mathcal{C}) \geq min\{\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_t\}.$$

Proof. Working in a similar manner as in Theorem 4.2 of Güneri et al. [41], the desired result follows. □

4

Enumeration of Euclidean and Hermitian self-dual, self-orthogonal and LCD multi-twisted codes

4.1 Introduction

In this chapter, we shall enumerate all Euclidean and Hermitian self-dual, self-orthogonal and LCD multi-twisted (MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$

and length n over $\mathbb{F}_q$, where $m_1, m_2, \cdots, m_\ell$ are positive integers coprime to q, and $n = m_1 + m_2 + \cdots + m_\ell$. For this, we assume that $q = p^r$, where p is a prime number and r is a positive integer. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$.

This chapter is organized as follows: In Section 4.2, we enumerate all Euclidean self-dual and self-orthogonal Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ (Theorems 4.2.2 and 4.2.4). We also count all Euclidean linear with complementary dual (LCD) Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ when $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$ (Theorem 4.2.5). In Section 4.3, we enumerate all Hermitian self-dual and self-orthogonal Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ (Theorems 4.3.2 and 4.3.3). We also obtain the enumeration formula for all Hermitian LCD Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ when $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$ (Theorem 4.3.4).

From now on, throughout this chapter, we shall follow the same notations as in Chapters 2 and 3. We also assume, throughout this chapter, that k is an integer satisfying either $k = 0$ or $k = \frac{r}{2}$ when r is even.

4.2 Determination of the number of Euclidean self-dual, self-orthogonal and LCD MT codes

In this section, we will study and count all Euclidean self-dual, self-orthogonal and LCD Λ-MT codes of length n over $\mathbb{F}_q$ by applying the Witt decomposition Theory. For this, let us define $\mathcal{I}_1 = \{t : 1 \leq t \leq e_1, d_t = 1\}$ and $\mathcal{I}_2 = \{t : 1 \leq t \leq e_1, d_t > 1\}$. Note that the integer d_t is even for each $t \in \mathcal{I}_2$. Then we observe the following:

Lemma 4.2.1. *(a) For $1 \leq t \leq e_1$, $[\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$ is a non-degenerate and reflexive form on $\mathcal{G}_t$. Furthermore, $[\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$ is symmetric when $t \in \mathcal{I}_1$ and is*

Hermitian when $t \in \mathcal{I}_2$.

(b) When $t \in \mathcal{I}_1$ *and* q *is odd,* $(\mathcal{G}_t, Q_t)$ *is a non-degenerate quadratic space having dimension* ϵ_t *over* F_t*, where the quadratic map* $Q_t : \mathcal{G}_t \to F_t$ *is defined as* $Q_t(A_t) = \frac{1}{2}[A_t, A_t]_0$ *for all* $A_t \in \mathcal{G}_t$.

Proof. Proof is trivial. □

In the following theorem, we derive necessary and sufficient conditions for the existence of a Euclidean self-dual Λ-MT code of length n over $\mathbb{F}_q$. We also count all Euclidean self-dual Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 4.2.2. *Let* $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ *be fixed. For* $e_1 + 1 \leq \mu \leq e_2$*, let* τ_μ *denote the number of integers* i *satisfying* $1 \leq i \leq \ell$ *and* $\epsilon_{\mu,i} = \epsilon'_{\mu,i} = 1$.

(a) There exists a Euclidean self-dual Λ*-MT code of length* n *over* $\mathbb{F}_q$ *if and only if all the irreducible factors of the polynomials* $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots x^{m_\ell} - \lambda_\ell$ *in* $\mathbb{F}_q[x]$ *are either* $\mathscr{T}_0$*-self-conjugate or they form* $\mathscr{T}_0$*-conjugate pairs (i.e.,* $e_3 \leq e_2$*),* ϵ_t *is even for* $1 \leq t \leq e_1$ *and* $(-1)^{\epsilon_t/2}$ *is a square in* $\mathbb{F}_q$ *for all* $t \in \mathcal{I}_1$.

(b) When all the irreducible factors of the polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots x^{m_\ell} - \lambda_\ell$ *in* $\mathbb{F}_q[x]$ *are either* $\mathscr{T}_0$*-self-conjugate or they form* $\mathscr{T}_0$*-conjugate pairs (i.e.,* $e_3 \leq e_2$*),* ϵ_t *is even for* $1 \leq t \leq e_1$ *and* $(-1)^{\epsilon_t/2}$ *is a square in* $\mathbb{F}_q$ *for all* $t \in \mathcal{I}_1$*, the number* $\mathfrak{N}_0$ *of distinct Euclidean self-dual* Λ*-MT codes of length* n *over* $\mathbb{F}_q$ *is given by*

$$\mathfrak{N}_0 = \prod_{t=1}^{e_1} \mathfrak{D}_t \prod_{\mu=e_1+1}^{e_2} \left(\sum_{b=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ b \end{bmatrix}_{q^{d_\mu}} \right),$$

where for $1 \leq t \leq e_1$,

$$\mathfrak{D}_t = \begin{cases} \prod_{a=0}^{\epsilon_t/2-1} \left(q^a + 1\right) & \text{if } t \in \mathcal{I}_1 \text{ \& } q \text{ is odd;} \\ \prod_{a=1}^{\epsilon_t/2-1} \left(q^a + 1\right) & \text{if } t \in \mathcal{I}_1 \text{ \& } q \text{ is even;} \\ \prod_{a=0}^{\epsilon_t/2-1} \left(q^{(2a+1)d_t/2} + 1\right) & \text{if } t \in \mathcal{I}_2. \end{cases}$$

In order to prove this theorem, we need to prove the following lemma:

Lemma 4.2.3. *Let $1 \leq t \leq e_1$ be fixed. There exists an F_t-subspace $\mathcal{C}_t$ of $\mathcal{G}_t$ satisfying $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$ if and only if the following two conditions are satisfied: (i) ϵ_t is an even integer, and (ii) $(-1)^{\epsilon_t/2}$ is a square in $\mathbb{F}_q$ for all $t \in \mathcal{I}_1$. (Here $\mathcal{C}_t^{\perp_0} (\subseteq \mathcal{G}_t)$ is the orthogonal complement of $\mathcal{C}_t$ with respect to $[\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$.)*

Proof. To prove the result, we see, by Lemma 4.2.1(a), that $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is an orthogonal space having dimension ϵ_t over F_t when $t \in \mathcal{I}_1$ and that $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is a unitary space having dimension ϵ_t over F_t when $t \in \mathcal{I}_2$. Now if $\mathcal{C}_t$ is an F_t-subspace of $\mathcal{G}_t$, then by Theorem 2.1.1, we see that $\dim_{F_t} \mathcal{C}_t^{\perp_0} = \epsilon_t - \dim_{F_t} \mathcal{C}_t$. Further, if $\mathcal{C}_t$ satisfies $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$, then we get $\epsilon_t = 2 \dim_{F_t} \mathcal{C}_t$, which implies that ϵ_t is an even integer.

On the other hand, when $t \in \mathcal{I}_2$ and ϵ_t is even, by Theorem 2.1.4(a), we see that the Witt index of $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is $\epsilon_t/2$, so there exists an F_t-subspace $\mathcal{C}_t$ of $\mathcal{G}_t$ satisfying $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$. When $t \in \mathcal{I}_1$ and ϵ_t is even, by Theorem 2.1.2(a), we see that the Witt index of $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is $\epsilon_t/2$ if and only if $(-1)^{\epsilon_t/2}$ is a square in $\mathbb{F}_q$. That is, when $t \in \mathcal{I}_1$ and ϵ_t is even, there exists an F_t-subspace $\mathcal{C}_t$ of $\mathcal{G}_t$ satisfying $\mathcal{C}_t = \mathcal{C}_t^{\perp_0}$ if and only if $(-1)^{\epsilon_t/2}$ is a square in $\mathbb{F}_q$. This proves the lemma. □

Proof of Theorem 4.2.2. Part (a) follows immediately by Theorem 3.3.3(a) and Lemma 4.2.3. To prove (b), we see, by Theorem 3.3.3(a) again, that it is enough to determine the numbers $\mathfrak{D}_t$ for all $t \in \mathcal{I}_1 \cup \mathcal{I}_2$ and $\mathfrak{D}_\mu$ for $e_1 + 1 \leq \mu \leq e_2$.

To do this, we see, by Lemma 2.1.6, that for each μ $(e_1+1 \leq \mu \leq e_2)$, the number $\mathfrak{D}_\mu$ of distinct F_μ-subspaces of $\mathcal{K}_\mu$ equals $\mathfrak{D}_\mu = \sum_{b=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ b \end{bmatrix}_{q^{d_\mu}}$. Moreover, for $t \in \mathcal{I}_1$, by Lemma 4.2.1(a) and Theorem 2.1.2(b), we see that the number $\mathfrak{D}_t$ of distinct $\epsilon_t/2$-dimensional self-orthogonal subspaces of $\mathcal{G}_t$ over F_t is given by $\mathfrak{D}_t = \prod_{a=0}^{\epsilon_t/2-1} \left(q^a + 1\right)$ when q is odd, while the number $\mathfrak{D}_t$ of such subspaces is given by $\mathfrak{D}_t = \prod_{a=1}^{\epsilon_t/2-1} \left(q^a + 1\right)$ when q is even. For $t \in \mathcal{I}_2$, by Lemma 4.2.1(a) and Theorem 2.1.4(b), we see that the number $\mathfrak{D}_t$ of distinct $\epsilon_t/2$-dimensional self-orthogonal subspaces of $\mathcal{G}_t$ over F_t

is given by $\mathfrak{D}_t = \prod_{a=0}^{\epsilon_t/2-1} \left(q^{(2a+1)d_t/2}+1\right)$. From this and using Theorem 3.3.3(a) again, part (b) follows immediately. □

In the following theorem, we enumerate all Euclidean self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 4.2.4. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed. For $e_1 + 1 \leq \mu \leq e_2$, let τ_μ denote the number of integers i satisfying $1 \leq i \leq \ell$ and $\epsilon_{\mu,i} = \epsilon'_{\mu,i} = 1$. The number $\mathfrak{N}_1$ of distinct Euclidean self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$ is given by*

$$\mathfrak{N}_1 = \prod_{t=1}^{e_1} \mathfrak{E}_t \prod_{\mu=e_1+1}^{e_2} \left(\sum_{k_1=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ k_1 \end{bmatrix}_{q^{d_\mu}} \Big(\sum_{k_2=0}^{\tau_\mu - k_1} \begin{bmatrix} \tau_\mu - k_1 \\ k_2 \end{bmatrix}_{q^{d_\mu}} \Big) \right),$$

where for $1 \leq t \leq e_1$, $\mathfrak{E}_t$ equals

- $\sum_{b=0}^{\epsilon_t/2} \left(\begin{bmatrix} \epsilon_t/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\epsilon_t/2-a-1}+1\right) \right)$ *when $t \in \mathcal{I}_1$ and either $q \equiv 1 \pmod 4$, ϵ_t is even or $\epsilon_t \equiv 0 \pmod 4, q \equiv 3 \pmod 4$;*
- $\sum_{b=0}^{(\epsilon_t-2)/2} \left(\begin{bmatrix} (\epsilon_t-2)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\epsilon_t/2-a}+1\right) \right)$ *when $t \in \mathcal{I}_1$, $q \equiv 3 \pmod 4$ and $\epsilon_t \equiv 2 \pmod 4$;*
- $\sum_{b=0}^{(\epsilon_t-1)/2} \left(\begin{bmatrix} (\epsilon_t-1)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{(\epsilon_t-1)/2-a}+1\right) \right)$ *if $t \in \mathcal{I}_1$ & both q, ϵ_t are odd;*
- $\sum_{b=0}^{(\epsilon_t-1)/2} \left(\begin{bmatrix} (\epsilon_t-1)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{(\epsilon_t-2a-1)/2}+1\right) \right)$ *if $t \in \mathcal{I}_1$, q is even & ϵ_t is odd;*
- $\sum_{b=0}^{(\epsilon_t-2)/2} \begin{bmatrix} (\epsilon_t-2)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{(\epsilon_t-2a-2)/2}+1\right) + \sum_{k'=1}^{\epsilon_t/2} q^{\epsilon_t-2k'} \begin{bmatrix} (\epsilon_t-2)/2 \\ k'-1 \end{bmatrix}_q \prod_{a'=0}^{k'-2} \left(q^{(\epsilon_t-2a'-2)/2}+1\right)$ *if $t \in \mathcal{I}_1$ & both q, ϵ_t are even;*
- $\sum_{b=0}^{\epsilon_t/2} \Big(\prod_{a=\epsilon_t+1-2b}^{b} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) / \Big(\prod_{j=1}^{b} (q^{jd_t}-1) \Big)$ *if $t \in \mathcal{I}_2$ & ϵ_t is even;*
- $\sum_{b=0}^{(\epsilon_t-1)/2} \Big(\prod_{a=\epsilon_t+1-2b}^{b} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) / \Big(\prod_{j=1}^{b} (q^{jd_t}-1) \Big)$ *if $t \in \mathcal{I}_2$ & ϵ_t is odd.*

Proof. By Theorem 3.3.3(b), we see that to determine the number $\mathfrak{N}_1$, it is enough to determine the numbers $\mathfrak{E}_t$ for all $t \in \mathcal{I}_1 \cup \mathcal{I}_2$ and $\mathfrak{E}_\mu$ for $e_1 + 1 \leq \mu \leq e_2$.

I. First let $t \in \mathcal{I}_1$. Here we see, by Lemma 4.2.1(a), that for $t \in \mathcal{I}_1$, $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is an ϵ_t-dimensional orthogonal space over $F_t \simeq \mathbb{F}_q$. Now we shall distinguish the following two cases: (i) q is odd and (ii) q is even.

(i) When q is odd, one can view $\mathcal{G}_t$ as a non-degenerate quadratic space over F_t with respect to the quadratic map $Q_t : \mathcal{G}_t \to F_t$, defined as $Q_t(a(x)) = \frac{1}{2}[a(x), a(x)]_0$ for all $a(x) \in \mathcal{G}_t$. In view of this, we see, by Theorem 2.1.5(a), that the Witt index of $\mathcal{G}_t$ is given by

$$w_t = \begin{cases} \frac{\epsilon_t}{2} & \text{if either } \epsilon_t \text{ is even and } q \equiv 1 \pmod 4 \text{ or } \epsilon_t \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ \frac{\epsilon_t - 2}{2} & \text{if } \epsilon_t \equiv 2 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ \frac{\epsilon_t - 1}{2} & \text{if } \epsilon_t \text{ is odd.} \end{cases} \tag{4.1}$$

Further, by Theorem 2.1.5(b), we see that the number $\mathfrak{E}_t$ of distinct self-orthogonal subspaces of $\mathcal{G}_t$ over F_t is given by $\mathfrak{E}_t = \sum_{b=0}^{w_t} \left(\begin{bmatrix} w_t \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{w_t - \varsigma - a} + 1 \right) \right)$, where w_t (the Witt index of $\mathcal{G}_t$) is given by (4.1) and

$$\varsigma = \begin{cases} 1 & \text{if } w_t = \frac{\epsilon_t}{2}; \\ -1 & \text{if } w_t = \frac{\epsilon_t - 2}{2}; \\ 0 & \text{if } w_t = \frac{\epsilon_t - 1}{2}. \end{cases}$$

(ii) Next let q be even. Let us define $\mathcal{V}_t = \{(\epsilon_{t,1}c_{t,1}, \epsilon_{t,2}c_{t,2}, \cdots, \epsilon_{t,\ell}c_{t,\ell}) \in \mathcal{G}_t : \sum_{i=1}^{\ell} \epsilon_{t,i}c_{t,i} = 0\}$. Note that $\mathcal{V}_t$ is an F_t-subspace of $\mathcal{G}_t$ and $\dim_{F_t} \mathcal{V}_t = \epsilon_t - 1$. Let $\theta_t = (\epsilon_{t,1}, \epsilon_{t,2}, \cdots, \epsilon_{t,\ell}) \in \mathcal{G}_t$. Since $\sum_{i=1}^{\ell} \epsilon_{t,i} = \epsilon_t$, we see that $\theta_t \in \mathcal{V}_t$ if and only if ϵ_t is even.

When ϵ_t is odd, we see that $\theta_t \notin \mathcal{V}_t$, which implies that $\mathcal{G}_t = \mathcal{V}_t \oplus \langle \theta_t \rangle$. Next it is easy to observe that any self-orthogonal F_t-subspace of $\mathcal{G}_t$ is contained in $\mathcal{V}_t$ and that $[c, \theta_t]_0 = 0$ for each $c \in \mathcal{V}_t$. Further, we note that as q is even, all m_i's are odd.

This implies that m is odd, which further implies that $\frac{m}{m_i} = 1$ in F_t. Moreover, as $t \in \mathcal{I}_1$, the conjugation $\mathcal{T}_0$ is the identity map on F_t. This implies that for each $c_t = (\epsilon_{t,1}c_{t,1}, \epsilon_{t,2}c_{t,2}, \cdots, \epsilon_{t,\ell}c_{t,\ell}) \in \mathcal{V}_t$, we have $[c_t, c_t]_0 = \sum_{i=1}^{\ell} \epsilon_{t,i} c_{t,i}^2 \frac{m}{m_i} = (\sum_{i=1}^{\ell} \epsilon_{t,i} c_{t,i})^2 = 0$. From this, it follows that $[\cdot,\cdot]_0 \restriction_{\mathcal{V}_t \times \mathcal{V}_t}$ is a non-degenerate, reflexive and alternating bilinear form on $\mathcal{V}_t$, i.e., $(\mathcal{V}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{V}_t \times \mathcal{V}_t})$ is a symplectic space over F_t having the dimension $\epsilon_t - 1$ and the Witt index $\frac{\epsilon_t - 1}{2}$. Now by Theorem 2.1.3(b), we see that for $0 \leq b \leq \frac{\epsilon_b - 1}{2}$, the number of distinct b-dimensional self-orthogonal subspaces of $\mathcal{V}_t$ (and hence of $\mathcal{G}_t$) is given by $\begin{bmatrix} (\epsilon_t - 1)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\frac{\epsilon_t - 2a - 1}{2}} + 1\right)$. This implies that the number $\mathfrak{E}_t$ of distinct self-orthogonal subspaces of $\mathcal{G}_t$ over F_t is given by

$$\mathfrak{E}_t = \sum_{b=0}^{\frac{\epsilon_t - 1}{2}} \left(\begin{bmatrix} (\epsilon_t - 1)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\frac{\epsilon_t - 2a - 1}{2}} + 1\right) \right).$$

On the other hand, when ϵ_t is even, we see that $\theta_t \in \mathcal{V}_t$. Let $\widehat{\mathcal{V}}_t$ be an $(\epsilon_t - 2)$-dimensional F_t-subspace of $\mathcal{V}_t$ such that $\theta_t \notin \widehat{\mathcal{V}}_t$. Then we have $\mathcal{V}_t = \widehat{\mathcal{V}}_t \oplus \langle \theta_t \rangle$. Next we observe that there exists $z_t \in \widehat{\mathcal{V}}_t^{\perp_0} \setminus \mathcal{V}_t$. From this, it follows that $\mathcal{G}_t = \widehat{\mathcal{V}}_t \oplus \langle z_t \rangle \oplus \langle \theta_t \rangle$. It is easy to see that any self-orthogonal F_t-subspace of $\mathcal{G}_t$ is contained in $\mathcal{V}_t = \widehat{\mathcal{V}}_t \oplus \langle \theta_t \rangle$, which implies that any self-orthogonal subspace of $\mathcal{G}_t$ is either (i) contained in $\widehat{\mathcal{V}}_t$, or (ii) contained in $\widehat{\mathcal{V}}_t \oplus \langle \theta_t \rangle$ but not in $\widehat{\mathcal{V}}_t$. Further, we observe that $(\widehat{\mathcal{V}}_t, [\cdot,\cdot]_0 \restriction_{\widehat{\mathcal{V}}_t \times \widehat{\mathcal{V}}_t})$ is a symplectic space over F_t having the dimension $\epsilon_t - 2$ and the Witt index $(\epsilon_t - 2)/2$. Now by Theorem 2.1.3(b), we see that for $0 \leq b \leq \frac{\epsilon_t - 2}{2}$, the number $\mathfrak{E}_t$ of distinct b-dimensional totally isotropic subspaces of $\mathcal{G}_t$ is given by $\mathfrak{E}_t = \begin{bmatrix} (\epsilon_t - 2)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\frac{\epsilon_t - 2a - 2}{2}} + 1\right)$. Next we proceed to count all b-dimensional F_t-subspaces that are contained in $\widehat{\mathcal{V}}_t \oplus \langle \theta_t \rangle$ but not in $\widehat{\mathcal{V}}_t$. To do this, we observe that for $1 \leq b \leq \epsilon_t/2$, any such b-dimensional F_t-subspace of $\mathcal{G}_t$ is of the type $\langle y_1, y_2, \cdots, y_{b-1}, \theta_t + y_b \rangle$, where $y_h \in \widehat{\mathcal{V}}_t \setminus \{0\}$ for $1 \leq h \leq b-1$ and $y_b \in \widehat{\mathcal{V}}_t$. We further observe that the b-dimensional F_t-subspace $\langle y_1, y_2, \cdots, y_{b-1}, \theta_t + y_b \rangle$ of $\mathcal{G}_t$ is self-orthogonal if and only if $\langle y_1, y_2, \cdots, y_{b-1} \rangle$ is a self-orthogonal F_t-subspace of $\widehat{\mathcal{V}}_t$ and $y_b \in \langle y_1, y_2, \cdots, y_{b-1} \rangle^{\perp_0}$. Now by Theorem

2.1.3(b), for $1 \leq b \leq \epsilon_t/2$, we see that the number of distinct $(b-1)$-dimensional self-orthogonal F_t-subspaces of $\widehat{\mathcal{V}}_t$ is given by $\begin{bmatrix} (\epsilon_t-2)/2 \\ b-1 \end{bmatrix}_q \prod_{a=0}^{b-2} \left(q^{\frac{\epsilon_t-2a-2}{2}}+1\right)$. Next we observe that for $y_b, y_b' \in \langle y_1, y_2, \cdots, y_{b-1}\rangle^{\perp_0} \setminus \langle y_1, y_2, \cdots, y_{b-1}\rangle, \langle y_1, y_2 \cdots, y_{b-1}, \theta_t + y_b\rangle = \langle y_1, y_2 \cdots, y_{b-1}, \theta_t + y_b'\rangle$ if and only if $y_b - y_b' \in \langle y_1, y_2 \cdots, y_{b-1}\rangle$, i.e., all y_b's lying in different cosets of $\langle y_1, y_2 \cdots, y_{b-1}\rangle^{\perp_0} / \langle y_1, y_2, \cdots, y_{b-1}\rangle$ give rise to distinct self-orthogonal spaces of the type $\langle y_1, y_2, \cdots, y_{b-1}, \theta_t + y_b\rangle$. We also observe that the F_t-dimension of $\langle y_1, y_2, \cdots, y_{b-1}\rangle^{\perp_0}$ is $\epsilon_t - 2 - (b-1)$, which implies that y_b has q^{ϵ_t-2b} relevant choices. Therefore for $1 \leq b \leq \epsilon_t/2$, the number of distinct b-dimensional F_t-subspaces of $\mathcal{G}_t$ that are contained in $\widehat{\mathcal{V}}_t \oplus \langle \theta_t \rangle$ but not in $\widehat{\mathcal{V}}_t$, is given by $q^{\epsilon_t-2b}\begin{bmatrix} (\epsilon_t-2)/2 \\ b-1 \end{bmatrix}_q \prod_{a=0}^{b-2} \left(q^{\frac{\epsilon_t-2a-2}{2}}+1\right)$. On combining both the cases, we see that the number $\mathfrak{E}_t$ of distinct self-orthogonal F_t-subspaces of $\mathcal{G}_t$ is given by $\mathfrak{E}_t = \sum_{b=0}^{\frac{\epsilon_t-2}{2}} \begin{bmatrix} (\epsilon_t-2)/2 \\ b \end{bmatrix}_q \prod_{a=0}^{b-1} \left(q^{\frac{\epsilon_t-2a-2}{2}}+1\right) + \sum_{k'=1}^{\epsilon_t/2} q^{\epsilon_t-2k'} \begin{bmatrix} (\epsilon_t-2)/2 \\ k'-1 \end{bmatrix}_q \prod_{a'=0}^{k'-2} \left(q^{\frac{\epsilon_t-2a'-2}{2}}+1\right)$ when ϵ_t is even.

II. Next let $t \in \mathcal{I}_2$. Here we observe, from Lemma 4.2.1 (a), that $(\mathcal{G}_t, [\cdot,\cdot]_0 \restriction_{\mathcal{G}_t \times \mathcal{G}_t})$ is a unitary space over F_t having dimension ϵ_t. Further, by Theorem 2.1.4(a), the Witt index w_t of $\mathcal{G}_t$ is given by

$$w_t = \begin{cases} \epsilon_t/2 & \text{if } \epsilon_t \text{ is even;} \\ (\epsilon_t-1)/2 & \text{if } \epsilon_t \text{ is odd.} \end{cases}$$

Now by Theorem 2.1.4(b), we see that the number $\mathfrak{E}_t$ of distinct self-orthogonal F_t-subspaces of $\mathcal{G}_t$ is given by $\mathfrak{E}_t = \sum_{b=0}^{w_t} \Big(\prod_{a=\epsilon_t+1-2b}^{b} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) / \Big(\prod_{j=1}^{b} (q^{jd_t}-1) \Big)$.

III. Finally, for $e_1+1 \leq \mu \leq e_2$, we shall count the number of pairs $(\mathcal{C}_\mu, \mathcal{C}_\mu')$ with $\mathcal{C}_\mu$ as an F_μ-subspace of $\mathcal{K}_\mu$ and $\mathcal{C}_\mu'$ as an F_μ'-subspace of $\mathcal{K}_\mu'$ satisfying $\mathcal{C}_\mu' \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}_\mu'$. In order to do this, we note that $(\mathcal{K}_\mu \times \mathcal{K}_\mu', [\cdot,\cdot]_0 \restriction_{\mathcal{K}_\mu \times \mathcal{K}_\mu'})$ is non-degenerate. So if the dimension of $\mathcal{C}_\mu$ is k_1, then one can observe that the dimension of $\mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}_\mu'$ is $\tau_\mu - k_1$, where $0 \leq k_1 \leq \tau_\mu$. As $\mathcal{C}_\mu'$ has to be a subspace of $\mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}_\mu'$, by Lemma 2.1.6, $\mathcal{C}_\mu'$ has $\sum_{k_2=0}^{\tau_\mu-k_1} \begin{bmatrix} \tau_\mu-k_1 \\ k_2 \end{bmatrix}_{q^{d_\mu}}$ choices if $\dim_{F_\mu} \mathcal{C}_\mu = k_1$. Further, we see that the number of distinct

k_1-dimensional F_μ-subspaces of $\mathcal{G}_\mu$ is given by $\begin{bmatrix}\tau_\mu\\ k_1\end{bmatrix}_{q^{d_\mu}}$. From this, it follows the number $\mathfrak{E}_\mu$ of pairs $(\mathcal{C}_\mu, \mathcal{C}'_\mu)$ with $\mathcal{C}_\mu$ as an F_μ-subspace of $\mathcal{K}_\mu$ and $\mathcal{C}'_\mu$ as an F'_μ-subspace of $\mathcal{K}'_\mu$ satisfying $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_0} \cap \mathcal{K}'_\mu$ is given by $\mathfrak{E}_\mu = \sum_{k_1=0}^{\tau_\mu} \begin{bmatrix}\tau_\mu\\ k_1\end{bmatrix}_{q^{d_\mu}} \Big(\sum_{k_2=0}^{\tau_\mu - k_1} \begin{bmatrix}\tau_\mu - k_1\\ k_2\end{bmatrix}_{q^{d_\mu}}\Big)$. Now using Theorem 3.3.3(b) again, the desired result follows immediately. □

Now in the following theorem, we enumerate all Euclidean LCD Λ-MT codes of length n over $\mathbb{F}_q$ when $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$.

Theorem 4.2.5. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$. For $e_1 + 1 \leq \mu \leq e_2$, let τ_μ denote the number of integers i satisfying $1 \leq i \leq \ell$ and $\epsilon_{\mu,i} = \epsilon'_{\mu,i} = 1$. The total number of distinct Euclidean LCD Λ-MT codes of length n over $\mathbb{F}_q$ is given by*

$$\mathfrak{N}_2 = \prod_{t=1}^{e_1} \mathfrak{F}_t \prod_{\mu=e_1+1}^{e_2} \left(2 + \sum_{\iota=1}^{\tau_\mu - 1} q^{\iota(\tau_\mu - \iota)d_\mu} \begin{bmatrix}\tau_u\\ \iota\end{bmatrix}_{q^{d_\mu}}\right) \prod_{u=e_2+1}^{e_3} \left(\sum_{b=0}^{\epsilon_u} \begin{bmatrix}\epsilon_u\\ b\end{bmatrix}_{q^{d_u}}\right),$$

where for $1 \leq t \leq e_1$, $\mathfrak{F}_t$ equals

- $2 + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 0 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{\vartheta(\epsilon_t - \vartheta + 1)}{2}} \begin{bmatrix}(\epsilon_t-1)/2\\ \vartheta/2\end{bmatrix}_{q^2} + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 1 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{(\epsilon_t - \vartheta)(\vartheta+1)}{2}} \begin{bmatrix}(\epsilon_t-1)/2\\ (\vartheta-1)/2\end{bmatrix}_{q^2}$ *when $t \in \mathcal{I}_1$ and ϵ_t is odd;*
- $2 + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 0 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{\vartheta(\epsilon_t - \vartheta)}{2}} \begin{bmatrix}\epsilon_t/2\\ \vartheta/2\end{bmatrix}_{q^2} + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 1 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{(\epsilon_t \vartheta - \vartheta^2 - 1)}{2}} (q^{\frac{\epsilon_t}{2}} + 1) \begin{bmatrix}(\epsilon_t-2)/2\\ (\vartheta-1)/2\end{bmatrix}_{q^2}$ *when $t \in \mathcal{I}_1, \epsilon_t \equiv 2\ (mod\ 4)$ and $q \equiv 3\ (mod\ 4)$;*
- $2 + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 0 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{\vartheta(\epsilon_t - \vartheta)}{2}} \begin{bmatrix}\epsilon_t/2\\ \vartheta/2\end{bmatrix}_{q^2} + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 1 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{(\epsilon_t \vartheta - \vartheta^2 - 1)}{2}} (q^{\frac{\epsilon_t}{2}} - 1) \begin{bmatrix}(\epsilon_t-2)/2\\ (\vartheta-1)/2\end{bmatrix}_{q^2}$ *when $t \in \mathcal{I}_1$, either ϵ_t is even and $q \equiv 1\ (mod\ 4)$ or $\epsilon_t \equiv 0\ (mod\ 4)$ and $q \equiv 3\ (mod\ 4)$;*
- $2 + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 0 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{\epsilon_t \vartheta - \vartheta^2 - 2}{2}} \Big\{ (q^\vartheta + q - 1) \begin{bmatrix}(\epsilon_t-2)/2\\ (\vartheta)/2\end{bmatrix}_{q^2} + (q^{\epsilon_t - \vartheta + 1} - q^{\epsilon_t - \vartheta} + 1) \begin{bmatrix}(\epsilon_t-2)/2\\ (\vartheta-2)/2\end{bmatrix}_{q^2} \Big\} + \sum\limits_{\substack{\vartheta=1\\ \vartheta \equiv 1 (mod\ 2)}}^{\epsilon_t - 1} q^{\frac{\epsilon_t \vartheta - \vartheta^2 + \epsilon_t - 1}{2}} \begin{bmatrix}(\epsilon_t-2)/2\\ (\vartheta-1)/2\end{bmatrix}_{q^2}$ *when $t \in \mathcal{I}_1$ and both ϵ_t, q are even;*

- $2+\sum_{\vartheta=1}^{\epsilon_t-1} q^{\frac{\vartheta(\epsilon_t-\vartheta)d_t}{2}} \prod_{\tau=0}^{\vartheta-1}\left(\frac{q^{\frac{(\epsilon_t-\tau)d_t}{2}}-(-1)^{\epsilon_t-\tau}}{q^{\frac{(\vartheta-\tau)d_t}{2}}-(-1)^{\vartheta-\tau}}\right)$ *when* $t \in \mathcal{I}_2$.

Proof. By Theorem 3.3.3(c), we see that to determine the number $\mathfrak{N}_2$, it is enough to determine the numbers $\mathfrak{F}_t$ for all $t \in \mathcal{I}_1 \cup \mathcal{I}_2$, $\mathfrak{F}_\mu$ for $e_1+1 \leq \mu \leq e_2$ and $\mathfrak{F}_u$ for $e_2+1 \leq \mu \leq e_3$.

To do this, when $t \in \mathcal{I}_2$, working in a similar manner as in Proposition 3.5 of Sharma and Kaur [71], we get

$$\mathfrak{F}_t = 2+\sum_{\vartheta=1}^{\epsilon_t-1} q^{\frac{\vartheta(\epsilon_t-\vartheta)d_t}{2}} \prod_{\tau=0}^{\vartheta-1}\left(\frac{q^{\frac{(\epsilon_t-\tau)d_t}{2}}-(-1)^{\epsilon_t-\tau}}{q^{\frac{(\vartheta-\tau)d_t}{2}}-(-1)^{\vartheta-\tau}}\right).$$

When $t \in \mathcal{I}_1$, working in a similar manner as in Propositions 3.6 and 3.7 of Sharma and Kaur [71], we obtain the number $\mathfrak{F}_t$. Further, for $e_1+1 \leq \mu \leq e_2$, working in a similar manner as in Proposition 3.8 of Sharma and Kaur [71], we obtain $\mathfrak{F}_\mu = 2+\sum_{\iota=1}^{\tau_\mu-1} q^{\iota(\tau_\mu-\iota)d_\mu}\begin{bmatrix}\tau_\mu\\ \iota\end{bmatrix}_{q^{d_\mu}}$.

Moreover, by applying Lemma 2.1.6, we see that $\mathfrak{F}_u = \sum_{b=0}^{\epsilon_u}\begin{bmatrix}\epsilon_u\\ b\end{bmatrix}_{q^{d_u}}$ for $e_2+1 \leq u \leq e_3$. Now using Theorem 3.3.3(c) again, the desired result follows immediately. □

4.3 Determination of the number of Hermitian self-dual, self-orthogonal and LCD MT codes

In this section, we will study and count all Hermitian self-dual, Hermitian self-orthogonal and Hermitian LCD Λ-MT codes of length n over $\mathbb{F}_q$ by applying the Witt's decomposition Theory. Now we make the following observation:

Lemma 4.3.1. *(a) For* $1 \leq t \leq e_1$, $[\cdot,\cdot]_{\frac{r}{2}} \restriction_{\mathcal{G}_t \times \mathcal{G}_t}$ *is a non-degenerate, reflexive and Hermitian form on* $\mathcal{G}_t$. *That is, the formed space* $\left(\mathcal{G}_t, [\cdot,\cdot]_{\frac{r}{2}} \restriction_{\mathcal{G}_t \times \mathcal{G}_t}\right)$ *is a unitary space of dimension* ϵ_t *over* F_t.

(b) For $e_1+1 \leq \mu \leq e_2$, $[\cdot,\cdot]_{\frac{r}{2}} \restriction_{\mathcal{K}_\mu \times \mathcal{K}'_\mu}$ *is a non-degenerate form on* $\mathcal{K}_\mu \times \mathcal{K}'_\mu$.

Proof. Proof is trivial. □

In the following theorem, we derive necessary and sufficient conditions for the existence of a Hermitian self-dual Λ-MT code of length n over $\mathbb{F}_q$. We also provide the enumeration formula for all Hermitian self-dual Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 4.3.2. *Let r be even and $k = \frac{r}{2}$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$.*

(a) There exists a Hermitian self-dual Λ-MT code of length n over $\mathbb{F}_q$ if and only if irreducible factors of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_{\frac{r}{2}}$-self-conjugate or they form $\mathscr{T}_{\frac{r}{2}}$-conjugate pairs, and ϵ_t is even for $1 \leq t \leq e_1$.

(b) Suppose that irreducible factors of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_{\frac{r}{2}}$-self-conjugate or they form $\mathscr{T}_{\frac{r}{2}}$-conjugate pairs, and ϵ_t is even for $1 \leq t \leq e_1$. Then the total number of distinct Hermitian self-dual Λ-MT codes of length n over $\mathbb{F}_q$ is given by

$$\mathfrak{M}_0 = \prod_{t=1}^{e_1} \left(\prod_{a=0}^{\epsilon_t/2-1} (q^{(2a+1)d_t/2} + 1) \right) \prod_{\mu=e_1+1}^{e_2} \left(\sum_{b=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ b \end{bmatrix}_{q^{d_\mu}} \right).$$

Proof. (a) To prove the result, by Theorem 3.3.4(a), we see that the code $\mathcal{C}$ is Hermitian self-dual if and only if the following three conditions are satisfied:

- All the irreducible factors of the polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots x^{m_\ell} - \lambda_\ell$ in $\mathbb{F}_q[x]$ are either $\mathscr{T}_{\frac{r}{2}}$-self-conjugate or form $\mathscr{T}_{\frac{r}{2}}$-conjugate pairs (i.e., $e_3 \leq e_2$).
- For $1 \leq t \leq e_1$, $\mathcal{C}_t = \mathcal{C}_t^{\perp_{\frac{r}{2}}} \subseteq \mathcal{G}_t$, which, by Theorem 2.1.1, holds if and only if ϵ_t is even and $\mathcal{C}_t$ is an $\epsilon_t/2$-dimensional self-orthogonal F_t-subspace of $\mathcal{G}_t$.

- For $e_1+1 \leq \mu \leq e_2$, $\mathcal{C}_\mu$ (resp. $\mathcal{C}'_\mu$) is a subspace of $\mathcal{K}_\mu$ (resp. $\mathcal{K}'_\mu$) satisfying $\mathcal{C}'_\mu = \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$.

From this and by applying Lemma 4.3.1(a) and Theorem 2.1.4(a), part (a) follows immediately.

(b) By Theorem 3.3.4(a), we see that to determine the number $\mathfrak{M}_0$, it is enough to determine the numbers $\mathcal{N}_t$ for $1 \leq t \leq e_1$ and $\mathcal{N}_\mu$ for $e_1+1 \leq \mu \leq e_2$.

To do this, for $1 \leq t \leq e_1$, by Lemma 4.3.1(a) and Theorem 2.1.4(b), we obtain $\mathcal{N}_t = \prod_{a=0}^{\epsilon_t/2-1} \left(q^{(2a+1)d_t/2}+1\right)$. Further, by Lemma 2.1.6, we get $\mathcal{N}_\mu = \sum_{b=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ b \end{bmatrix}_{q^{d_\mu}}$ for $e_1+1 \leq \mu \leq e_2$. Now using Theorem 3.3.4(a) again, the desired result follows immediately.

□

In the following theorem, we enumerate all Hermitian self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$.

Theorem 4.3.3. *Let r be even and $k = \frac{r}{2}$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Then the total number of distinct Hermitian self-orthogonal Λ-MT codes of length n over $\mathbb{F}_q$ is given by*

$$\mathfrak{M}_1 = \prod_{t=1}^{e_1} \mathcal{M}_t \prod_{\mu=e_1+1}^{e_2} \left(\sum_{k_0=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ k_0 \end{bmatrix}_{q^{d_\mu}} \Big(\sum_{k_1=0}^{\tau_\mu - k_0} \begin{bmatrix} \tau_\mu - k_0 \\ k_1 \end{bmatrix}_{q^{d_\mu}} \Big) \right),$$

where for $1 \leq t \leq e_1$,

$$\mathcal{M}_t = \begin{cases} \sum_{s=0}^{\epsilon_t/2} \Big(\prod_{a=\epsilon_t+1-2s}^{\epsilon_t} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) \Big/ \Big(\prod_{j=1}^{s} (q^{jd_t}-1) \Big) & \text{if } \epsilon_t \text{ is even;} \\ \sum_{s=0}^{(\epsilon_t-1)/2} \Big(\prod_{a=\epsilon_t+1-2s}^{\epsilon_t} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) \Big/ \Big(\prod_{j=1}^{s} (q^{jd_t}-1) \Big) & \text{if } \epsilon_t \text{ is odd.} \end{cases}$$

Proof. By Theorem 3.3.4(b), we see that to determine the number $\mathfrak{M}_1$, it is enough to determine the numbers $\mathcal{M}_t$ for $1 \leq t \leq e_1$ and $\mathcal{M}_\mu$ for $e_1+1 \leq \mu \leq e_2$.

To do this, for $1 \leq t \leq e_1$, by Lemma 4.3.1(a), we see that $\big(\mathcal{G}_t, [\cdot,\cdot]_{\frac{r}{2}} \restriction_{\mathcal{G}_t \times \mathcal{G}_t}\big)$ is a unitary space of dimension ϵ_t over F_t. Further, by Theorem 2.1.4(a), the Witt index of $\mathcal{G}_t$ is given by $\epsilon_t/2$ if ϵ_t is even, and by $(\epsilon_t - 1)/2$ if ϵ_t is odd. For $1 \leq t \leq e_1$, using this and by applying Theorem 2.1.4(b), we obtain

$$\mathcal{M}_t = \begin{cases} \sum\limits_{s=0}^{\epsilon_t/2} \Big(\prod\limits_{a=\epsilon_t+1-2s}^{\epsilon_t} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) \Big/ \Big(\prod\limits_{j=1}^{s} (q^{jd_t} - 1) \Big) & \text{if } \epsilon_t \text{ is even;} \\ \sum\limits_{s=0}^{(\epsilon_t-1)/2} \Big(\prod\limits_{a=\epsilon_t+1-2s}^{\epsilon_t} (q^{\frac{ad_t}{2}} - (-1)^a) \Big) \Big/ \Big(\prod\limits_{j=1}^{s} (q^{jd_t} - 1) \Big) & \text{if } \epsilon_t \text{ is odd.} \end{cases}$$

To determine the number $\mathcal{M}_\mu$ for $e_1 + 1 \leq \mu \leq e_2$, let $\mathcal{C}_\mu$ be an F_μ-subspace of $\mathcal{K}_\mu$ having dimension k_0, where $0 \leq k_0 \leq \tau_\mu$. Now by applying Lemma 4.3.1(b) and Theorem 2.1.1, we see that the F'_μ-dimension of $\mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$ is $\tau_\mu - k_0$. As $\mathcal{C}'_\mu \subseteq \mathcal{C}_\mu^{\perp_{\frac{r}{2}}} \cap \mathcal{K}'_\mu$, by Lemma 2.1.6, the subspace $\mathcal{C}'_\mu$ of $\mathcal{K}'_\mu$ has $\sum\limits_{k_1=0}^{\tau_\mu - k_0} \begin{bmatrix} \tau_\mu - k_0 \\ k_1 \end{bmatrix}_{q^{d_\mu}}$ choices if the F_μ-dimension of $\mathcal{C}_\mu$ is k_0. Further, by applying Lemma 2.1.6, we see that for $0 \leq k_0 \leq \tau_\mu$, the number of distinct k_0-dimensional F_μ-subspaces of $\mathcal{K}_\mu$ is given by $\begin{bmatrix} \tau_\mu \\ k_0 \end{bmatrix}_{q^{d_\mu}}$. From this, we obtain $\mathcal{M}_\mu = \sum\limits_{k_0=0}^{\tau_\mu} \begin{bmatrix} \tau_\mu \\ k_0 \end{bmatrix}_{q^{d_\mu}} \Big(\sum\limits_{k_1=0}^{\tau_\mu - k_0} \begin{bmatrix} \tau_\mu - k_0 \\ k_1 \end{bmatrix}_{q^{d_\mu}} \Big)$ for $e_1 + 1 \leq \mu \leq e_2$.

Now using Theorem 3.3.4(b) again, the desired result follows immediately. □

In the following theorem, we enumerate all Hermitian LCD Λ-MT codes of length n over $\mathbb{F}_q$ when $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$.

Theorem 4.3.4. *Let r be even and $k = \frac{r}{2}$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$. Then the total number of distinct Hermitian LCD Λ-MT codes of length n over $\mathbb{F}_q$ is given by*

$$\mathfrak{M}_2 = \prod_{t=1}^{e_1} \mathcal{D}_t \prod_{\mu=e_1+1}^{e_2} \left(2 + \sum_{\iota=1}^{\tau_\mu - 1} q^{\iota(\tau_\mu - \iota)d_\mu} \begin{bmatrix} \tau_\mu \\ \iota \end{bmatrix}_{q^{d_\mu}} \right) \prod_{u=e_2+1}^{e_3} \left(\sum_{b=0}^{\epsilon_u} \begin{bmatrix} \epsilon_u \\ b \end{bmatrix}_{q^{d_u}} \right),$$

where $\mathcal{D}_t = 2 + \sum\limits_{\vartheta=1}^{\epsilon_t - 1} q^{\frac{\vartheta(\epsilon_t - \vartheta)\eta_t}{2}} \prod\limits_{\tau=0}^{\vartheta-1} \left(\frac{q^{\frac{(\epsilon_t - \tau)\eta_t}{2}} - (-1)^{\epsilon_t - \tau}}{q^{\frac{(\vartheta - \tau)\eta_t}{2}} - (-1)^{\vartheta - \tau}} \right)$ *for* $1 \leq t \leq e_1$.

Proof. By Theorem 3.3.4(c), we see that to determine the number $\mathfrak{M}_2$, it is enough

to determine the numbers $\mathcal{D}_t$ for $1 \leq t \leq e_1$, $\mathcal{D}_\mu$ for $e_1 + 1 \leq \mu \leq e_2$ and $\mathcal{D}_u$ for $e_2 + 1 \leq u \leq e_3$.

To do this, for $1 \leq t \leq e_1$, working in a similar manner as in Proposition 3.5 of Sharma and Kaur [71], we get

$$\mathcal{D}_t = 2 + \sum_{\vartheta=1}^{\epsilon_t - 1} q^{\frac{\vartheta(\epsilon_t - \vartheta)d_t}{2}} \prod_{\tau=0}^{\vartheta-1} \left(\frac{q^{\frac{(\epsilon_t - \tau)d_t}{2}} - (-1)^{\epsilon_t - \tau}}{q^{\frac{(\vartheta - \tau)d_t}{2}} - (-1)^{\vartheta - \tau}} \right).$$

Further, for $e_1 + 1 \leq \mu \leq e_2$, working in a similar manner as in Proposition 3.8 of Sharma and Kaur [71], we obtain $\mathcal{D}_\mu = 2 + \sum_{\iota=1}^{\tau_\mu - 1} q^{\iota(\tau_\mu - \iota)d_\mu} \begin{bmatrix} \tau_\mu \\ \iota \end{bmatrix}_{q^{d_\mu}}$.

Moreover, by Lemma 2.1.6, we get $\mathcal{D}_u = \sum_{b=0}^{\epsilon_u} \begin{bmatrix} \epsilon_u \\ b \end{bmatrix}_{q^{d_u}}$ for $e_2 + 1 \leq u \leq e_3$. Now using Theorem 3.3.4(c) again, the desired result follows immediately. □

5

Hamming weights in multi-twisted codes over finite fields

5.1 Introduction

Let $\mathbb{F}_q$ denote the finite field of order q. Let ℓ be a positive integer, and let $m_1, m_2, \cdots, m_\ell$ be positive integers satisfying $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. Let $n = m_1 + m_2 + \cdots + m_\ell$, and let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. In this chapter, we shall explicitly determine all non-zero Hamming weights of codewords of several classes of Λ-multi-twisted (Λ-MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$. Using these results, we

shall explicitly determine Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights, which have applications in constructing association schemes, strongly regular graphs and authentication codes. Among these classes of few weight Λ-MT codes, we shall identify two classes of optimal equidistant Λ-MT codes meeting the Griesmer and Plotkin bounds, which have strong connections with combinatorial designs and projective geometry and are also useful in designing distributed storage systems. Besides this, we identify three other classes of few weight Λ-MT codes, which are useful in constructing secret sharing schemes with nice access structures.

Now let $q = \ell = 2$, $\Lambda = (1, 1)$, and let m_1, m_2 be odd positive integers such that the irreducible factorization of $x^{m_i} - 1$ over $\mathbb{F}_2$ is given by

$$x^{m_i} - 1 = (x - 1)f_i(x) \quad \text{for} \quad i \in \{1, 2\}. \tag{5.1}$$

Further, let $\alpha_i \in \mathbb{F}_{2^{m_i-1}}$ be a root of the polynomial $f_i(x)$, θ_i be a primitive element of $\mathbb{F}_{2^{m_i-1}}$, and let us write $\alpha_i^{-1} = \theta_i^{\ell_i}$ for some integer ℓ_i satisfying $0 \leq \ell_i \leq 2^{m_i-1} - 2$ for each i. Patanker and Singh [64] recently determined Hamming weight distributions of $(1, 1)$-MT codes of block lengths (m_1, m_2) over $\mathbb{F}_2$ (i.e., $\mathbb{F}_2$-double cyclic codes with block lengths (m_1, m_2)) under the assumption that there exists a least positive integer t_i satisfying

$$2^{t_i} \equiv -1 \pmod{\gcd(\ell_i, 2^{m_i-1} - 1)} \quad \text{for} \quad i \in \{1, 2\}. \tag{5.2}$$

Here under the conditions (5.1) and (5.2), we assert that $m_i \in \{3, 5\}$ for $i \in \{1, 2\}$. To prove this assertion, let $i \in \{1, 2\}$ be fixed. Now by (5.1), we observe that $m_i - 1$ is the least positive integer satisfying $2^{m_i-1} \equiv 1 \pmod{m_i}$, which further implies that m_i is a prime number. Since $\alpha_i^{m_i} = 1$ and $\alpha_i \neq 1$, we note that α_i is a primitive m_ith root of unity. Without any loss of generality, we can assume that $\alpha_i^{-1} = \theta_i^{\frac{2^{m_i-1}-1}{m_i}}$, i.e., we can take $\ell_i = \frac{2^{m_i-1}-1}{m_i}$ so that $\gcd(\ell_i, 2^{m_i-1} - 1) = \frac{2^{m_i-1}-1}{m_i}$. Now one can

easily see that conditions (5.1) and (5.2) hold for $m_i = 3$ or 5. Further, we see that $m_i = 7$ does not satisfy the condition (5.1). Furthermore, for $m_i \geq 11$, we note that $\frac{2^{m_i-1}-1}{m_i} \geq 3$ and the condition (5.2) implies that t_i divides $\frac{m_i-1}{2}$, which further implies that $2^{t_i}+1 \leq 2^{\frac{m_i-1}{2}}+1 < \frac{2^{m_i-1}-1}{m_i}$. From this, it follows that the condition (5.2) does not hold for any prime $m_i \geq 11$. This shows that conditions (5.1) and (5.2) are very heavy constraints and hold only when $m_i \in \{3, 5\}$. In the light of this, Patanker and Singh [64] essentially determined Hamming weight distributions of some $(1, 1)$-MT codes over $\mathbb{F}_2$ (i.e., $\mathbb{F}_2$-double cyclic codes) of block lengths $(3, 3), (3, 5)$ and $(5, 5)$ only, which one can easily determine by direct computations and without applying deeper results on Gauss sums.

The main goal of this chapter is to determine all non-zero Hamming weights of codewords of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, and to determine their Hamming weight distributions. As applications, several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with few weights and two classes of optimal equidistant (or equivalently, constant weight) Λ-MT codes meeting the Griesmer bound and the Plotkin bound are also identified.

This chapter is organized as follows: In Section 5.2, we explicitly determine Hamming weights of all the blocks of non-zero codewords of several classes of MT codes with at most two non-zero constituents (Theorems 5.2.2-5.2.10). Applying these results, one can determine all non-zero Hamming weights in these MT codes and their Hamming weight distributions. In Section 5.3, we determine Hamming weight distributions of several classes of few weights MT codes (Theorems 5.3.3-5.3.11). Among these classes of few weights MT codes, we identify two classes of optimal equidistant MT codes that attain both Griesmer and Plotkin bounds (Theorems 5.3.3-5.3.4). Besides this, we identify three different classes of few weight MT codes, which are useful in constructing secret sharing schemes with nice access structures (Theorems 5.3.3-5.3.5). Working in a similar manner as in Sections 5.2,

one can determine Hamming weight distributions of several other classes of MT codes with more than two non-zero constituents (see Remark 5.3.12 and Theorem 5.3.13).

From now on, throughout this chapter, let $q = p^r$, where p is a prime number and r is a positive integer. Here we shall follow the same notations as in Chapters 2 and 3.

5.2 Hamming weights of codewords of MT codes with at most two non-zero constituents

In this section, we shall determine Hamming weights of non-zero codewords of several classes of Λ-MT codes with at most two non-zero constituents. To do this, we recall that $F_w \simeq \mathbb{F}_{q^{d_w}}$ for $1 \leq w \leq \rho$. Without any loss of generality, we assume, throughout this chapter, that the constituents of Λ-MT codes corresponding to the irreducible factors $g_3(x), g_4(x), \cdots, g_\rho(x)$ are zero. Then by Theorems 3.2.2 and 3.5.2, each Λ-MT code of length n over $\mathbb{F}_q$ is given by

$$\begin{aligned}\mathcal{C} \;=\; \big\{\big(c_1(x_1,x_2), c_2(x_1,x_2), \cdots, c_\ell(x_1,x_2)\big) : x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w \\ \text{for } 1 \leq w \leq 2\big\},\end{aligned}$$

where $\mathcal{C}_1$ and $\mathcal{C}_2$ are subspaces of $\mathcal{G}_1$ and $\mathcal{G}_2$ over $\mathbb{F}_{q^{d_1}}$ and $\mathbb{F}_{q^{d_2}}$ respectively, and

$$\begin{aligned}c_i(x_1,x_2) \;=\; \frac{1}{m_i}\Big(\sum_{w=1}^{2} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}(x_{w,i}), \sum_{w=1}^{2} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}(x_{w,i}\delta_w^{-1}), \cdots, \\ \sum_{w=1}^{2} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}(x_{w,i}\delta_w^{-(m_i-1)})\Big) \qquad (5.3)\end{aligned}$$

is the ith block of the codeword $c(x_1,x_2) = \big(c_1(x_1,x_2), c_2(x_1,x_2), \cdots, c_\ell(x_1,x_2)\big)$ of the code $\mathcal{C}$ for $1 \leq i \leq \ell$. In view of this, we see that the Hamming weight

$W_H(c(x_1, x_2))$ of the codeword $c(x_1, x_2) \in \mathcal{C}$ is given by

$$W_H(c(x_1, x_2)) = W_H(c_1(x_1, x_2)) + W_H(c_2(x_1, x_2)) + \cdots + W_H(c_\ell(x_1, x_2)), \quad (5.4)$$

where $W_H(c_i(x_1, x_2))$ denotes the Hamming weight of the ith block $c_i(x_1, x_2)$ of the codeword $c(x_1, x_2) \in \mathcal{C}$ for $1 \leq i \leq \ell$. Therefore to determine the Hamming weight of the codeword $c(x_1, x_2) \in \mathcal{C}$, it is enough to determine Hamming weights $W_H(c_1(x_1, x_2)), W_H(c_2(x_1, x_2)), \cdots, W_H(c_\ell(x_1, x_2))$ of each of its ℓ blocks. For this, we shall first express Hamming weights $W_H(c_i(x_1, x_2))$ of the blocks $c_i(x_1, x_2)$, $1 \leq i \leq \ell$, in terms of certain character sums over finite fields. We assume, throughout this chapter, that χ, χ_1 and χ_2 are canonical additive characters of $\mathbb{F}_q$, $\mathbb{F}_{q^{d_1}}$ and $\mathbb{F}_{q^{d_2}}$, respectively.

From this point on, let $x_1 = (x_{1,1}, x_{1,2}, \cdots, x_{1,\ell}) \in \mathcal{C}_1$, $x_2 = (x_{2,1}, x_{2,2}, \cdots, x_{2,\ell}) \in \mathcal{C}_2$ and let $1 \leq i \leq \ell$ be fixed. Then we see, by (5.3), that

$$\begin{aligned} W_H(c_i(x_1, x_2)) &= |\{0 \leq j \leq m_i - 1 : Tr_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_q}(x_{1,i}\delta_1^{-j}) + Tr_{\mathbb{F}_{q^{d_2}}/\mathbb{F}_q}(x_{2,i}\delta_2^{-j}) \neq 0\}| \\ &= m_i - |\{0 \leq j \leq m_i - 1 : Tr_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_q}(x_{1,i}\delta_1^{-j}) + Tr_{\mathbb{F}_{q^{d_2}}/\mathbb{F}_q}(x_{2,i}\delta_2^{-j}) = 0\}|. \end{aligned}$$

This, by (2.1), can be rewritten as

$$\begin{aligned} W_H(c_i(x_1, x_2)) &= m_i - \frac{1}{q} \sum_{j=0}^{m_i-1} \sum_{y \in \mathbb{F}_q} \chi\left(y(Tr_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_q}(x_{1,i}\delta_1^{-j}) + Tr_{\mathbb{F}_{q^{d_2}}/\mathbb{F}_q}(x_{2,i}\delta_2^{-j}))\right) \\ &= m_i - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \sum_{j=0}^{m_i-1} \chi\left(yTr_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_q}(x_{1,i}\delta_1^{-j})\right) \chi\left(yTr_{\mathbb{F}_{q^{d_2}}/\mathbb{F}_q}(x_{2,i}\delta_2^{-j})\right). \end{aligned}$$

Now by using the fact that $Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}$ is an $\mathbb{F}_q$-linear map for $1 \leq w \leq 2$ and by (2.2), we observe that

$$W_H(c_i(x_1, x_2)) = m_i - \frac{1}{q} \sum_{y \in \mathbb{F}_q} \sum_{j=0}^{m_i-1} \chi_1(yx_{1,i}\delta_1^{-j})\chi_2(yx_{2,i}\delta_2^{-j}).$$

From this, we obtain

$$W_H(c_i(x_1,x_2)) = \begin{cases} 0 & \text{if } x_{1,i}=x_{2,i}=0; \\ m_i - \frac{m_i}{q} - \frac{1}{q}\sum\limits_{y\in\mathbb{F}_q^*}\sum\limits_{j=0}^{m_i-1}\chi_1(yx_{1,i}\delta_1^{-j}) & \text{if } x_{1,i}\neq 0 \text{ and } x_{2,i}=0; \\ m_i - \frac{m_i}{q} - \frac{1}{q}\sum\limits_{y\in\mathbb{F}_q^*}\sum\limits_{j=0}^{m_i-1}\chi_2(yx_{2,i}\delta_2^{-j}) & \text{if } x_{1,i}=0 \text{ and } x_{2,i}\neq 0; \\ m_i - \frac{m_i}{q} - \frac{1}{q}\sum\limits_{y\in\mathbb{F}_q^*}\sum\limits_{j=0}^{m_i-1}\chi_1(yx_{1,i}\delta_1^{-j})\chi_2(yx_{2,i}\delta_2^{-j}) & \\ & \text{if } x_{1,i}\neq 0 \text{ and } x_{2,i}\neq 0. \end{cases} \tag{5.5}$$

Now we proceed to determine the explicit value of the Hamming weight $W_H(c_i(x_1,x_2))$ by further expressing these character sums in terms of Gauss sums, whose explicit values are known only in certain special cases [11, 51]. To do this, we shall distinguish the following two cases: (i) either $x_{1,i}$ or $x_{2,i}$ is zero and (ii) both $x_{1,i}$ and $x_{2,i}$ are non-zero. From now on, throughout this chapter, we assume that ξ_1 and ξ_2 are primitive elements of $\mathbb{F}_{q^{d_1}}$ and $\mathbb{F}_{q^{d_2}}$, respectively. It is easy to see that $\xi_1^{\frac{q^{d_1}-1}{q-1}}$ and $\xi_2^{\frac{q^{d_2}-1}{q-1}}$ are primitive elements of $\mathbb{F}_q$. Now for $1\leq w\leq 2$, since $\delta_w\in\mathbb{F}_{q^{d_w}}^*$, we can write $\delta_w^{-1}=\xi_w^{\ell_w}$, where $0\leq\ell_w\leq q^{d_w}-2$. Further, let $\tau_w=\gcd\left(\frac{q^{d_w}-1}{q-1},\ell_w\right)$ and let ϕ_w be a generator of the multiplicative character group $\widehat{\mathbb{F}_{q^{d_w}}^*}$ of $\mathbb{F}_{q^{d_w}}$ for each w.

5.2.1 Determination of $W_H(c_i(x_1,x_2))$ when either $x_{1,i}$ or $x_{2,i}$ is zero

When $x_{1,i}=x_{2,i}=0$, by (5.5), we have $W_H(c_i(x_1,x_2))=0$. So we assume, throughout this section, that $x_{w,i}\neq 0$ and $x_{w',i}=0$, where $\{w,w'\}=\{1,2\}$. In the following lemma, we express the Hamming weight $W_H(c_i(x_1,x_2))$ in terms of certain Gauss sums.

Lemma 5.2.1. *We have*

$$W_H(c_i(x_1,x_2)) = m_i - \frac{m_i}{q} - \frac{m_i(q-1)}{q(q^{d_w}-1)} \sum_{b=0}^{\tau_w-1} \phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}(x_{w,i}) G(\overline{\phi}_w^{\frac{(q^{d_w}-1)b}{\tau_w}}, \chi_w).$$

Proof. To prove the result, we first note, by (5.5), that

$$W_H(c_i(x_1,x_2)) = m_i - \frac{m_i}{q} - \frac{1}{q} \sum_{y\in\mathbb{F}_q^*} \sum_{j=0}^{m_i-1} \chi_w(yx_{w,i}\delta_w^{-j}). \tag{5.6}$$

Now by (2.5) and by using the fact that $\widehat{\mathbb{F}_{q^{d_w}}^*} = \langle \phi_w \rangle$, we see that

$$\begin{aligned} \sum_{y\in\mathbb{F}_q^*} \sum_{j=0}^{m_i-1} \chi_w(yx_{w,i}\delta_w^{-j}) &= \frac{1}{q^{d_w}-1} \sum_{y\in\mathbb{F}_q^*} \sum_{u=0}^{q^{d_w}-2} \sum_{j=0}^{m_i-1} G(\overline{\phi}_w^u, \chi_w)\phi_w^u(yx_{w,i}\delta_w^{-j}) \\ &= \frac{1}{q^{d_w}-1} \sum_{j=0}^{m_i-1} \sum_{u=0}^{q^{d_w}-2} G(\overline{\phi}_w^u, \chi_w)\phi_w^u(x_{w,i}\delta_w^{-j}) \left(\sum_{y\in\mathbb{F}_q^*} \phi_w^u(y) \right). \end{aligned}$$

Further, for $0 \le u \le q^{d_w}-2$, one can easily observe that

$$\begin{aligned} \sum_{y\in\mathbb{F}_q^*} \phi_w^u(y) &= \sum_{k=0}^{q-2} \phi_w^u(\xi_w^{\frac{(q^{d_w}-1)k}{q-1}}) = \sum_{k=0}^{q-2} e^{\frac{2\pi\iota(q^{d_w}-1)uk}{(q^{d_w}-1)(q-1)}} \\ &= \sum_{k=0}^{q-2} e^{\frac{2\pi\iota uk}{q-1}} = \begin{cases} q-1 & \text{if } u \equiv 0 \pmod{q-1}; \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

In view of this, we get

$$\sum_{y\in\mathbb{F}_q^*} \sum_{j=0}^{m_i-1} \chi_w(yx_{w,i}\delta_w^{-j}) = \frac{q-1}{q^{d_w}-1} \sum_{a=0}^{\frac{q^{d_w}-1}{q-1}-1} G(\overline{\phi}_w^{(q-1)a}, \chi_w)\phi_w^{(q-1)a}(x_{w,i}) \left(\sum_{j=0}^{m_i-1} \phi_w^{(q-1)a}(\delta_w^{-j}) \right).$$

Further, if $\phi_w^{(q-1)a}(\delta_w^{-1}) \neq 1$ for some integer a satisfying $0 \le a < \frac{q^{d_w}-1}{q-1}$, then we see

that

$$\sum_{j=0}^{m_i-1} \phi_w^{(q-1)a}(\delta_w^{-j}) = \sum_{j=0}^{m_i-1} \phi_w^{(q-1)a}(\delta_w^{-1})^j = \frac{\phi_w^{(q-1)a}(\delta_w^{-m_i})-1}{\phi_w^{(q-1)a}(\delta_w^{-1})-1} = \frac{\phi_w^{(q-1)a}(\lambda_i^{-1})-1}{\phi_w^{(q-1)a}(\delta_w^{-1})-1} = 0,$$

as $\delta_w^{m_i} = \lambda_i$ and $\lambda_i^{q-1} = 1$. Therefore for $0 \leq a < \frac{q^{d_w}-1}{q-1}$, we have

$$\sum_{j=0}^{m_i-1} \phi_w^{(q-1)a}(\delta_w^{-j}) = \begin{cases} m_i & \text{if } \phi_w^{(q-1)a}(\delta_w^{-1}) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Further, for an integer a satisfying $0 \leq a < \frac{q^{d_w}-1}{q-1}$, we note that $\phi_w^{(q-1)a}(\delta_w^{-1}) = \phi_w^{(q-1)a}(\xi_w^{\ell_w}) = e^{\frac{2\pi\iota(q-1)a\ell_w}{q^{d_w}-1}} = 1$ if and only if $(q-1)a\ell_w \equiv 0 \pmod{q^{d_w}-1}$, which holds if and only if $a \equiv 0 \left(\mathrm{mod}\ \frac{(q^{d_w}-1)}{\tau_w(q-1)}\right)$. From this, we obtain

$$\sum_{y\in\mathbb{F}_q^*} \sum_{j=0}^{m_i-1} \chi_w(yx_{w,i}\delta_w^{-j}) = \frac{m_i(q-1)}{q^{d_w}-1} \sum_{b=0}^{\tau_w-1} \phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}(x_{w,i}) G(\overline{\phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}}, \chi_w).$$

Now on substituting the above value of the sum $\sum_{y\in\mathbb{F}_q^*} \sum_{j=0}^{m_i-1} \chi_w(yx_{w,i}\delta_w^{-j})$ in equation (5.6), we get the desired result. □

In the following theorem, we explicitly determine the Hamming weight $W_H(c_i(x_1, x_2))$.

Theorem 5.2.2. *Let $x_{w,i} = \xi_w^{s_{w,i}} \in \mathbb{F}_{q^{d_w}}^*$ and $x_{w',i} = 0$, where $0 \leq s_{w,i} \leq q^{d_w} - 2$.*

(a) When $\tau_w = 1$, we have $W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} + \frac{m_i(q-1)}{q(q^{d_w}-1)}$.

(b) When $\tau_w = 2$, the integer d_w is even, q is an odd prime power and

$$W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} + \frac{m_i(q-1)\left(1 + \iota^{\frac{rd_w(p-1)^2}{4}} q^{\frac{d_w}{2}} (-1)^{s_{w,i}}\right)}{q(q^{d_w}-1)}.$$

(c) Let $\tau_w \geq 3$. Suppose that there exists a positive integer u_w satisfying $p^{u_w} \equiv -1 \pmod{\tau_w}$. If s_w is the least positive integer satisfying $p^{s_w} \equiv -1 \pmod{\tau_w}$,

then we have $rd_w = 2s_w\nu_w$ *for some positive integer* ν_w.

- *If* τ_w *is even and* $\frac{p\nu_w(p^{s_w}+1)}{\tau_w}$ *is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} m_i - \frac{m_i}{q} - \frac{m_i(q-1)(-1+q^{\frac{d_w}{2}}(\tau_w-1))}{q(q^{d_w}-1)} & \text{if } \tau_w \mid \frac{\tau_w}{2} + s_{w,i}; \\ m_i - \frac{m_i}{q} + \frac{m_i(q-1)(1+q^{\frac{d_w}{2}})}{q(q^{d_w}-1)} & \text{if } \tau_w \nmid \frac{\tau_w}{2} + s_{w,i}. \end{cases}$$

- *If either* τ_w *is odd or* $\frac{p\nu_w(p^{s_w}+1)}{\tau_w}$ *is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} m_i - \frac{m_i}{q} - \frac{m_i(q-1)(-1+(-1)^{\nu_w-1}q^{\frac{d_w}{2}}(\tau_w-1))}{q(q^{d_w}-1)} & \text{if } \tau_w \mid s_{w,i}; \\ m_i - \frac{m_i}{q} + \frac{m_i(q-1)(1+(-1)^{\nu_w-1}q^{\frac{d_w}{2}})}{q(q^{d_w}-1)} & \text{if } \tau_w \nmid s_{w,i}. \end{cases}$$

Proof. To prove the result, we see, by Lemma 5.2.1, that

$$W_H(c_i(x_1,x_2)) = m_i - \frac{m_i}{q} - \frac{m_i(q-1)\Theta_i'(x_{w,i})}{q(q^{d_w}-1)}, \tag{5.7}$$

where $\Theta_i'(x_{w,i}) = \sum_{b=0}^{\tau_w-1} \phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}(x_{w,i})G(\overline{\phi}_w^{\frac{(q^{d_w}-1)b}{\tau_w}}, \chi_w)$. So to determine the Hamming weight $W_H(c_i(x_1,x_2))$, it is enough to determine the explicit value of the sum $\Theta_i'(x_{w,i})$. For this, we observe that $O(\overline{\phi}_w^{\frac{q^{d_w}-1}{\tau_w}}) = \tau_w$. Now we shall distinguish the following three cases: (a) $\tau_w = 1$, (b) $\tau_w = 2$, and (c) $\tau_w \geq 3$.

(a) When $\tau_w = 1$, by (2.4), we get $\Theta_i'(x_{w,i}) = -1$.

(b) When $\tau_w = 2$, we note that $\overline{\phi}_w^{\frac{q^{d_w}-1}{\tau_w}}$ is the quadratic character of $\mathbb{F}_{q^{d_w}}^*$. In this case, we see that $\tau_w = 2$ divides $\frac{q^{d_w}-1}{q-1} = 1 + q + \cdots + q^{d_w-1}$, which implies that q is odd and d_w is even. Hence by Theorem 2.2.1, we obtain

$$\Theta_i'(x_{w,i}) = -1 + \phi_w^{\frac{q^{d_w}-1}{\tau_w}}(x_{w,i})G(\overline{\phi}_w^{\frac{q^{d_w}-1}{\tau_w}}, \chi_w) = -1 - \iota^{\frac{rd_w(p-1)^2}{4}} q^{\frac{d_w}{2}} (-1)^{s_{w,i}}.$$

(c) Next let $\tau_w \geq 3$. Here by Theorem 2.2.2, for $1 \leq b \leq \tau_w - 1$, we see that

$$G(\overline{\phi}_w^{\frac{(q^{d_w}-1)b}{\tau_w}}, \chi_w) = \begin{cases} (-1)^b q^{\frac{d_w}{2}} & \text{if } \tau_w \text{ is even and } \frac{p\nu_w(p^{s_w}+1)}{\tau_w} \text{ is odd;} \\ (-1)^{\nu_w - 1} q^{\frac{d_w}{2}} & \text{otherwise.} \end{cases} \tag{5.8}$$

When τ_w is even and $\frac{p\nu_w(p^{s_w}+1)}{\tau_w}$ is odd, we see, by (5.8), that

$$\begin{aligned} \Theta_i'(x_{w,i}) &= -1 + q^{\frac{d_w}{2}} \sum_{b=1}^{\tau_w - 1} (-1)^b \phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}(x_{w,i}) \\ &= -1 + q^{\frac{d_w}{2}} \sum_{b=1}^{\tau_w - 1} e^{\left(\frac{2\pi\iota b(q^{d_w}-1)s_{w,i}}{\tau_w(q^{d_w}-1)} + \frac{2\pi\iota b\tau_w}{2\tau_w}\right)} \\ &= -1 + q^{\frac{d_w}{2}} \sum_{b=1}^{\tau_w - 1} e^{\frac{2\pi\iota b}{\tau_w}(s_{w,i} + \frac{\tau_w}{2})} \\ &= \begin{cases} -1 + q^{\frac{d_w}{2}}(\tau_w - 1) & \text{if } \tau_w \mid \frac{\tau_w}{2} + s_{w,i}; \\ -1 - q^{\frac{d_w}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

On the other hand, when either τ_w is odd or $\frac{p\nu_w(p^{s_w}+1)}{\tau_w}$ is even, we see, by (5.8), that

$$\begin{aligned} \Theta_i'(x_{w,i}) &= -1 + (-1)^{\nu_w - 1} q^{\frac{d_w}{2}} \sum_{b=1}^{\tau_w - 1} \phi_w^{\frac{(q^{d_w}-1)b}{\tau_w}}(x_{w,i}) \\ &= \begin{cases} -1 + (-1)^{\nu_w - 1} q^{\frac{d_w}{2}}(\tau_w - 1) & \text{if } \tau_w \mid s_{w,i}; \\ -1 - (-1)^{\nu_w - 1} q^{\frac{d_w}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

Now on substituting the values of $\Theta_i'(x_{w,i})$ in equation (5.7) in the respective cases, we get the desired result. □

5.2.2 Determination of $W_H(c_i(x_1, x_2))$ when $x_{1,i} \neq 0$ and $x_{2,i} \neq 0$

Throughout this section, we assume that $x_{1,i} \neq 0$ and $x_{2,i} \neq 0$. To determine the Hamming weight $W_H(c_i(x_1, x_2))$, throughout this chapter, let us first fix the following notations:

$d = \gcd(d_1, d_2)$	τ is the least positive integer satisfying $\frac{\tau \ell_1}{g_1 G} \equiv 1 \pmod{\frac{q^d-1}{G}}$
$g_w = \gcd\left(\frac{q^{d_w}-1}{q^d-1}, \ell_w\right)$ for $1 \leq w \leq 2$	τ' is the least positive integer satisfying $\frac{\tau'(q^d-1)\Delta_1}{G\lambda} \equiv 1 \pmod{\frac{q-1}{\lambda}}$
$\Delta_w = \frac{q^{d_w}-1}{(q^d-1)g_w}$ for $1 \leq w \leq 2$	L is the least positive integer satisfying $\xi_1^{\frac{q^{d_1}-1}{q-1}} = \xi_2^{\frac{(q^{d_2}-1)L}{q-1}}$
$G = \gcd\left(\frac{\ell_1}{g_1}, q^d-1\right)$	$\lambda' = \gcd(\lambda, \frac{\Delta_2 GL}{H} - \frac{\Delta_1 \tau \ell_2}{g_2 H})$
$H = \gcd\left(\frac{\ell_1}{g_1}, \frac{\ell_2}{g_2}, q^d-1\right)$	$K_1 = \frac{(q^d-1)(q-1)}{G\lambda}$
$\lambda = \gcd\left(\frac{\Delta_1(q^d-1)}{G}, q-1\right)$	$K_2 = -\frac{\lambda \tau \ell_2}{\lambda' g_2 H}\left(1 - \frac{(q^d-1)\tau'\Delta_1}{G\lambda}\right) - \frac{\tau'(q^{d_2}-1)L}{\lambda' H g_2}$
$M_1 = \frac{G\lambda g_1}{q-1}$	$M_2 = \frac{(q^d-1)\lambda' g_2 H}{G\lambda}$

Note that $K_2 = -\frac{\tau \ell_2 \lambda}{g_2 H \lambda'} - \frac{\tau'(q^d-1)}{G\lambda'}\left(\frac{\Delta_2 GL}{H} - \frac{\tau \ell_2 \Delta_1}{g_2 H}\right)$ and $M_2 = \frac{(q^d-1)\lambda' g_2 H}{G\lambda}$ are integers, and $\gcd(L, q-1) = 1$.

In the following lemma, we first express the Hamming weight $W_H(c_i(x_1, x_2))$ in terms of certain Gauss sums.

Lemma 5.2.3. *We have*

$$W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} - \frac{m_i(q-1)\Theta_i(x_{1,i}, x_{2,i})}{q(q^{d_1}-1)(q^{d_2}-1)}, \tag{5.9}$$

where

$$\Theta_i(x_{1,i}, x_{2,i}) = \sum_{z_2=0}^{M_2-1} \sum_{z_1=0}^{M_1-1} \Big(G(\overline{\phi_1}^{\Delta_1(K_2 z_2 + K_1 z_1)}, \chi_1) \phi_1^{\Delta_1(K_2 z_2 + K_1 z_1)}(x_{1,i})$$

$$G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})\Big). \quad (5.10)$$

Proof. To prove the result, we note, by (5.5), that

$$W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} - \frac{1}{q}\Omega_i(x_{1,i}, x_{2,i}), \quad (5.11)$$

where $\Omega_i(x_{1,i}, x_{2,i}) = \sum_{y\in\mathbb{F}_q^*}\sum_{j=0}^{m_i-1}\chi_1(yx_{1,i}\delta_1^{-j})\chi_2(yx_{2,i}\delta_2^{-j})$. Further, as $\widehat{\mathbb{F}^*_{q^{d_1}}} = \langle\phi_1\rangle$ and $\widehat{\mathbb{F}^*_{q^{d_2}}} = \langle\phi_2\rangle$, we see, by (2.5), that

$$\begin{aligned}
&\Omega_i(x_{1,i}, x_{2,i})\\
&= \frac{1}{(q^{d_1}-1)(q^{d_2}-1)}\sum_{y\in\mathbb{F}_q^*}\sum_{u_1=0}^{q^{d_1}-2}\sum_{u_2=0}^{q^{d_2}-2}\sum_{j=0}^{m_i-1} G(\overline{\phi}_1^{u_1}, \chi_1)\phi_1^{u_1}(yx_{1,i}\delta_1^{-j})G(\overline{\phi}_2^{u_2}, \chi_2)\phi_2^{u_2}(yx_{2,i}\delta_2^{-j})\\
&= \frac{1}{(q^{d_1}-1)(q^{d_2}-1)}\sum_{j=0}^{m_i-1}\sum_{u_1=0}^{q^{d_1}-2}\sum_{u_2=0}^{q^{d_2}-2} G(\overline{\phi}_1^{u_1}, \chi_1)\phi_1^{u_1}(x_{1,i}\delta_1^{-j})G(\overline{\phi}_2^{u_2}, \chi_2)\phi_2^{u_2}(x_{2,i}\delta_2^{-j})\Big(\\
&\qquad\qquad \sum_{y\in\mathbb{F}_q^*}\phi_1^{u_1}(y)\phi_2^{u_2}(y)\Big).
\end{aligned}$$

Further, for $0 \le u_1 \le q^{d_1}-2$ and $0 \le u_2 \le q^{d_2}-2$, one can easily observe that

$$\begin{aligned}
\sum_{y\in\mathbb{F}_q^*}\phi_1^{u_1}(y)\phi_2^{u_2}(y) &= \sum_{k=0}^{q-2}\phi_1^{u_1}(\xi_1^{\frac{(q^{d_1}-1)k}{q-1}})\phi_2^{u_2}(\xi_2^{\frac{(q^{d_2}-1)kL}{q-1}})\\
&= \sum_{k=0}^{q-2} e^{\frac{2\pi\iota(u_1+u_2L)k}{q-1}} = \begin{cases} q-1 & \text{if } u_1+u_2L \equiv 0 \pmod{q-1};\\ 0 & \text{otherwise.}\end{cases}
\end{aligned}$$

In view of this, we obtain

$$\begin{aligned}
\Omega_i(x_{1,i}, x_{2,i}) &= \frac{q-1}{(q^{d_1}-1)(q^{d_2}-1)}\sum_{u_1,u_2} G(\overline{\phi}_1^{u_1}, \chi_1)\phi_1^{u_1}(x_{1,i})G(\overline{\phi}_2^{u_2}, \chi_2)\phi_2^{u_2}(x_{2,i})\Big(\\
&\qquad\qquad \sum_{j=0}^{m_i-1}\phi_1^{u_1}(\delta_1^{-j})\phi_2^{u_2}(\delta_2^{-j})\Big).
\end{aligned}$$

where the summation $\sum_{u_1,u_2}$ runs over integers u_1 and u_2 satisfying $0 \le u_1 \le q^{d_1}-2$, $0 \le u_2 \le q^{d_2}-2$, and $u_1 + u_2 L \equiv 0 \pmod{q-1}$.

Further, for $0 \le u_1 \le q^{d_1}-2$ and $0 \le u_2 \le q^{d_2}-2$ satisfying $u_1 + u_2 L \equiv 0 \pmod{q-1}$, we assert that

$$\sum_{j=0}^{m_i-1} \phi_1^{u_1}(\delta_1^{-j})\phi_2^{u_2}(\delta_2^{-j}) = \begin{cases} m_i & \text{if } \phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1}) = 1; \\ 0 & \text{otherwise.} \end{cases} \tag{5.12}$$

To prove the above assertion, we see that if $\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1}) \neq 1$, then

$$\begin{aligned} \sum_{j=0}^{m_i-1} \phi_1^{u_1}(\delta_1^{-j})\phi_2^{u_2}(\delta_2^{-j}) &= \sum_{j=0}^{m_i-1} (\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1}))^j \\ &= \frac{\phi_1^{u_1}(\delta_1^{-m_i})\phi_2^{u_2}(\delta_2^{-m_i})-1}{\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1})-1} = \frac{\phi_1^{u_1}(\lambda_i^{-1})\phi_2^{u_2}(\lambda_i^{-1})-1}{\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1})-1}, \end{aligned}$$

as $\delta_1^{m_i} = \delta_2^{m_i} = \lambda_i$. Since $\lambda_i^{-1} \in \mathbb{F}_q^*$ and $\xi_1^{\frac{q^{d_1}-1}{q-1}} = \xi_2^{\frac{(q^{d_2}-1)L}{q-1}}$ is a primitive element of $\mathbb{F}_q$, we can write $\lambda_i^{-1} = \xi_1^{\frac{(q^{d_1}-1)T}{q-1}} = \xi_2^{\frac{(q^{d_2}-1)TL}{q-1}}$ for some integer T satisfying $0 \le T \le q-2$. From this, we observe that $\phi_1^{u_1}(\lambda_i^{-1})\phi_2^{u_2}(\lambda_i^{-1}) = e^{\frac{2\pi\iota T(u_1+u_2L)}{q-1}} = 1$, which further implies that $\sum_{j=0}^{m_i-1} \phi_1^{u_1}(\delta_1^{-j})\phi_2^{u_2}(\delta_2^{-j}) = 0$. On the other hand, when $\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1}) = 1$, it is easy to see that $\sum_{j=0}^{m_i-1} \phi_1^{u_1}(\delta_1^{-j})\phi_2^{u_2}(\delta_2^{-j}) = m_i$, which proves (5.12).

We further note that $\phi_1^{u_1}(\delta_1^{-1})\phi_2^{u_2}(\delta_2^{-1}) = e^{\frac{2\pi\iota u_1\ell_1}{q^{d_1}-1} + \frac{2\pi\iota u_2\ell_2}{q^{d_2}-1}} = 1$ if and only if $(q^{d_2}-1)u_1\ell_1 + (q^{d_1}-1)u_2\ell_2 \equiv 0 \pmod{(q^{d_1}-1)(q^{d_2}-1)}$. From this, we obtain

$$\Omega_i(x_{1,i}, x_{2,i}) = \frac{m_i(q-1)}{(q^{d_1}-1)(q^{d_2}-1)} \sum_{u_1,u_2} G(\overline{\phi}_1^{u_1}, \chi_1)\phi_1^{u_1}(x_{1,i})G(\overline{\phi}_2^{u_2}, \chi_2)\phi_2^{u_2}(x_{2,i}), \tag{5.13}$$

where the summation $\sum_{u_1,u_2}$ runs over integers u_1 and u_2 satisfying

$$\begin{aligned} &0 \le u_1 \le q^{d_1}-2, 0 \le u_2 \le q^{d_2}-2, \\ &(q^{d_2}-1)u_1\ell_1 + (q^{d_1}-1)u_2\ell_2 \equiv 0 \pmod{(q^{d_1}-1)(q^{d_2}-1)} \text{ and} \end{aligned}$$

$$u_1 + u_2 L \equiv 0 \pmod{q-1}. \tag{5.14}$$

Further, one can observe that all the distinct integers u_1, u_2 satisfying (5.14) are given by

$$u_1 = \Delta_1(K_2 z_2 + K_1 z_1) \text{ and } u_2 = \frac{\Delta_2 G \lambda z_2}{H\lambda'},$$

where z_1, z_2 are integers satisfying $0 \leq z_1 < M_1$ and $0 \leq z_2 < M_2$. This, by (5.13), gives $\Omega_i(x_{1,i}, x_{2,i}) = \frac{m_i(q-1)\Theta_i(x_{1,i},x_{2,i})}{(q^{d_1}-1)(q^{d_2}-1)}$. From this and by equation (5.11), the desired result follows immediately. □

Next to determine the explicit value of $W_H(c_i(x_1, x_2))$, we note that $O(\phi_1^{\Delta_1 K_1}) = M_1$ and $O(\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}) = M_2$. Now we shall consider the following three cases separately: (i) $M_2 = 1$, (ii) $M_2 = 2$, and (iii) $M_2 \geq 3$. Further, in each of these three cases, we shall distinguish the following three subcases: (i) $M_1 = 1$, (ii) $M_1 = 2$, and (iii) $M_1 \geq 3$.

In the following theorem, we consider the case $M_2 = 1$ and we determine the explicit value of $W_H(c_i(x_1, x_2))$.

Theorem 5.2.4. *Let $M_2 = 1$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \leq s_{1,i} \leq q^{d_1} - 2$ and $0 \leq s_{2,i} \leq q^{d_2} - 2$.*

(a) When $M_1 = 1$, we have $W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} - \frac{m_i(q-1)}{q(q^{d_2}-1)(q^{d_1}-1)}$.

(b) When $M_1 = 2$, the integer d_1 is even, q is an odd prime power and

$$W_H(c_i(x_1, x_2)) = m_i - \frac{m_i}{q} - \frac{m_i(q-1)\big(1 + \iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}} (-1)^{s_{1,i}}\big)}{q(q^{d_1}-1)(q^{d_2}-1)}.$$

(c) Let $M_1 \geq 3$. Suppose that there exists a positive integer u satisfying $p^u \equiv -1 \pmod{M_1}$. If t is the least positive integer satisfying $p^t \equiv -1 \pmod{M_1}$, then we have $rd_1 = 2t\gamma$ for some positive integer γ.

- *If M_1 is even and $\frac{p\gamma(p^t+1)}{M_1}$ is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} m_i - \frac{m_i}{q} - \frac{m_i(q-1)\left(1-q^{\frac{d_1}{2}}(M_1-1)\right)}{q(q^{d_2}-1)(q^{d_1}-1)} & \text{if } M_1 \mid \frac{M_1}{2} + s_{1,i}; \\ m_i - \frac{m_i}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}\right)}{q(q^{d_2}-1)(q^{d_1}-1)} & \text{if } M_1 \nmid \frac{M_1}{2} + s_{1,i}. \end{cases}$$

- *If either M_1 is odd or $\frac{p\gamma(p^t+1)}{M_1}$ is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} m_i - \frac{m_i}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma-1}q^{\frac{d_1}{2}}(M_1-1)\right)}{q(q^{d_2}-1)(q^{d_1}-1)} & \text{if } M_1 \mid s_{1,i}; \\ m_i - \frac{m_i}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_2}-1)(q^{d_1}-1)} & \text{if } M_1 \nmid s_{1,i}. \end{cases}$$

Proof. To prove this, we see, by Lemma 5.2.3, that to determine the Hamming weight $W_H(c_i(x_1,x_2))$, it is enough to determine the explicit value of

$$\Theta_i(x_{1,i},x_{2,i}) = -\sum_{z_1=0}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1},\chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}). \tag{5.15}$$

To do this, we shall distinguish the following three cases: (a) $M_1 = 1$, (b) $M_1 = 2$, and (c) $M_3 \geq 3$.

(a) When $M_1 = 1$, by (5.15) and (2.4), clearly we have $\Theta_i(x_{1,i},x_{2,i}) = 1$.

(b) When $M_1 = 2$, $\overline{\phi}_1^{\Delta_1 K_1}$ is a quadratic character of $\mathbb{F}_{q^{d_1}}$ and q is odd. Further, we note that $M_1 = 2 = \gcd(\frac{q^{d_1}-1}{q-1}, Gg_1)$, which implies that d_1 is even. Hence equation (5.15) can be rewritten as

$$\Theta_i(x_{1,i},x_{2,i}) = 1 - G(\overline{\phi}_1^{\Delta_1 K_1},\chi_1)\phi_1^{\Delta_1 K_1}(x_{1,i}). \tag{5.16}$$

From this and by Theorem 2.2.1, we obtain $\Theta_i(x_{1,i},x_{2,i}) = 1+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}(-1)^{s_{1,i}}$.

(c) Next let $M_1 \geq 3$. Here by Theorem 2.2.2, for $1 \leq z_1 \leq M_1 - 1$, we see that

$$G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1) = \begin{cases} (-1)^{z_1} q^{\frac{d_1}{2}} & \text{if } M_1 \text{ is even and } \frac{p\gamma(p^t+1)}{M_1} \text{ is odd;} \\ (-1)^{\gamma-1} q^{\frac{d_1}{2}} & \text{otherwise.} \end{cases} \tag{5.17}$$

When M_1 is even and $\frac{p\gamma(p^t+1)}{M_1}$ is odd, we see, by (5.17), that

$$\begin{aligned} \Theta_i(x_{1,i}, x_{2,i}) &= 1 - \sum_{z_1=1}^{M_1-1} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1) \\ &= 1 - q^{\frac{d_1}{2}} \sum_{z_1=1}^{M_1-1} (-1)^{z_1} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) \\ &= 1 - q^{\frac{d_1}{2}} \sum_{z_1=1}^{M_1-1} e^{\left(\frac{2\pi\iota z_1 s_{1,i}}{M_1} + \pi\iota z_1\right)} \\ &= 1 - q^{\frac{d_1}{2}} \sum_{z_1=1}^{M_1-1} e^{\left(\frac{2\pi\iota z_1}{M_1}(s_{1,i} + \frac{M_1}{2})\right)} \\ &= \begin{cases} 1 - q^{\frac{d_1}{2}}(M_1 - 1) & \text{if } M_1 \mid \frac{M_1}{2} + s_{1,i}; \\ 1 + q^{\frac{d_1}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

On the other hand, when either M_1 is odd or $\frac{p\gamma(p^t+1)}{M_1}$ is even, we see, by (5.15) and (5.17), that

$$\begin{aligned} \Theta_i(x_{1,i}, x_{2,i}) &= 1 - (-1)^{\gamma-1} q^{\frac{d_1}{2}} \sum_{z_1=1}^{M_1-1} e^{\left(\frac{2\pi\iota z_1 s_{1,i}}{M_1}\right)} \\ &= \begin{cases} 1 - (-1)^{\gamma-1} q^{\frac{d_1}{2}}(M_1 - 1) & \text{if } M_1 \mid s_{1,i}; \\ 1 + (-1)^{\gamma-1} p^{\frac{rd_1}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

Now on substituting the values of $\Theta_i(x_{1,i}, x_{2,i})$ in equation (5.15) in the respective cases, we get the desired result. □

In the following theorem, we determine the explicit value of $W_H(c_i(x_1, x_2))$ when $M_1 = 1$ and $M_2 = 2$.

Theorem 5.2.5. *Let $M_1 = 1$, $M_2 = 2$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \le s_{1,i} \le q^{d_1} - 2$ and $0 \le s_{2,i} \le q^{d_2} - 2$.*

(a) When d_2 is even, we have $W_H(c_i(x_1, x_2)) = \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}} (-1)^{s_{2,i}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)}$.

(b) When d_2 is odd, the integer d_1 is also odd and we have

$$W_H(c_i(x_1, x_2)) = \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+\iota^{\frac{r(d_1+d_2)(p-1)^2}{4}} q^{\frac{d_1+d_2}{2}} (-1)^{s_{1,i}+s_{2,i}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)}.$$

Proof. To determine the Hamming weight $W_H(c_i(x_1, x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 + G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2) G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1) \phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i}) \phi_1^{\Delta_1 K_2}(x_{1,i}).$$

To do this, we note that $O(\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}) = M_2 = 2$, so the character $\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}$ is the quadratic character of $\mathbb{F}_{q^{d_2}}$ and q is odd. Since $\gcd(L, q-1) = 1$, we see that L is odd. Further, $M_1 = 1$ implies that $g_1 = 1$ and $G\lambda = q - 1$. From this, it follows that $\frac{(q^d-1)\lambda' g_2 H}{q-1} = M_2 = 2$. This gives $d = 1$ and $\lambda' g_2 H = 2$. Further, it is easy to see that

$$\begin{aligned} \Delta_1 K_2 &= \frac{q^{d_1}-1}{q-1}\Big(- \frac{\lambda\tau\ell_2(1-\tau'\Delta_1)}{2} - \frac{\tau'(q^{d_2}-1)L}{2}\Big) \\ &= \frac{q^{d_1}-1}{2}\Big(- \frac{\tau\ell_2(1-\tau'\Delta_1)}{G} - \frac{\tau'(q^{d_2}-1)L}{q-1}\Big) \end{aligned} \tag{5.18}$$

and

$$\lambda' g_2 H = 2 = \gcd\Big(\lambda g_2 H, \frac{(q^{d_2}-1)GL}{q-1} - \Delta_1\ell_2\tau\Big). \tag{5.19}$$

Now we shall distinguish the following two cases: (a) d_2 is even and (b) d_2 is odd.

(a) Let d_2 be even. Here as $d = 1$, the integer d_1 must be odd. From this, we observe that the integer $\frac{q^{d_2}-1}{q-1}$ is even and the integer Δ_1 is odd. This, by (5.19), clearly implies that the integer $\tau\ell_2$ is even. Further, since G divides $1-\tau'\Delta_1$, by (5.18),

one can easily observe that $\phi_1^{\Delta_1 K_2}$ is the trivial multiplicative character of $\mathbb{F}_{q^{d_1}}$ in this case. From this and by Theorem 2.2.1, we obtain

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 - G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i}) = 1 + \iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}} (-1)^{s_{2,i}}.$$

(b) When d_2 is odd, we see that the integer $\frac{q^{d_2}-1}{q-1}$ is odd and $g_2 = 1$. Next as $\frac{G\lambda}{q-1} = \gcd(\Delta_1, G) = 1$, by (5.19), one can easily see that the integer Δ_1 must be odd. From this, we note that the integer d_1 is odd.

Now when G is even, we see, by (5.19), that the integer $\tau\ell_2$ is even. Further, as G divides $1 - \tau'\Delta_1$, we observe that the integer τ' is odd. This, by (5.18), implies that $\phi_1^{\Delta_1 K_2}$ is the quadratic character of $\mathbb{F}_{q^{d_1}}$.

On the other hand, when G is odd, we observe, by (5.19), that the integer $\tau\ell_2$ is odd. We further note that the integer τ' must be odd if the integer $\frac{1-\tau'\Delta_1}{G}$ is even, while the integer τ' is even if the integer $\frac{1-\tau'\Delta_1}{G}$ is odd. Now since both the integers $\frac{(q^{d_2}-1)L}{q-1}, \tau\ell_2$ are odd, we see, by (5.18), that $\phi_1^{\Delta_1 K_2}$ is the quadratic character of $\mathbb{F}_{q^{d_1}}$.

From this and by applying Theorem 2.2.1, we obtain

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 + \iota^{\frac{r(d_1+d_2)(p-1)^2}{4}} q^{\frac{d_1+d_2}{2}} (-1)^{s_{1,i}+s_{2,i}}.$$

□

In the following theorem, we determine the explicit value of $W_H(c_i(x_1, x_2))$ when $M_1 = M_2 = 2$.

Theorem 5.2.6. *Let $M_1 = M_2 = 2$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \leq s_{1,i} \leq q^{d_1} - 2$ and $0 \leq s_{2,i} \leq q^{d_2} - 2$. Here the integer $g_1 \in \{1, 2\}$ and p is an odd prime.*

(a) When $g_1 = 1$, we have $q = 3$, $G = \lambda = d = 2$ and

$$W_H(c_i(x_1, x_2)) = \begin{cases} \frac{2m_i}{3} - \frac{2m_i\left(1-3^{\frac{d_1}{2}}+2(-1)^{\frac{2s_{2,i}+s_{1,i}+d_2}{2}}3^{\frac{d_1+d_2}{2}}\right)}{3(3^{d_1}-1)(3^{d_2}-1)} & \text{if } 2 \mid s_{1,i}; \\ \frac{2m_i}{3} - \frac{2m_i(1+3^{\frac{d_1}{2}})}{3(3^{d_1}-1)(3^{d_2}-1)} & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

(b) Let $g_1 = 2$.

- *If $p \equiv 3 \pmod 4$, then we have*

$$W_H(c_i(x_1, x_2)) = \begin{cases} \frac{(q-1)m_i}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}+2(-1)^{\frac{2s_{2,i}+rd_2+s_{1,i}}{2}}q^{\frac{d_1+d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } 2 \mid s_{1,i}; \\ \frac{(q-1)m_i}{q} - \frac{m_i(q-1)(1-q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

- *If $p \equiv 1 \pmod 4$, then we have*

$$W_H(c_i(x_1, x_2)) = \begin{cases} \frac{(q-1)m_i}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}+2q^{\frac{d_1+2d_2}{4}}(-1)^{\frac{2(rd_2+s_{2,i})+s_{1,i}}{2}}\mathcal{R}_i\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad\qquad \text{if } 2 \mid s_{1,i}; & \\ \frac{(q-1)m_i}{q} - \frac{m_i(q-1)\left(1-q^{\frac{d_1}{2}}+2q^{\frac{d_1+2d_2}{4}}(-1)^{\frac{2(rd_2+s_{2,i})+1+s_{1,i}}{2}}\mathcal{I}_i\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad\qquad \text{if } 2 \nmid s_{1,i}, & \end{cases}$$

where $\mathcal{R}_i = Re\,(a+\iota b)^{\frac{rd_1}{2}}$ and $\mathcal{I}_i = Im\,(a+\iota b)^{\frac{rd_1}{2}}$ denote the real and imaginary parts of the complex number $(a+\iota b)^{\frac{rd_1}{2}}$, respectively (Here a and b are the integers determined uniquely by $p = a^2+b^2, a \equiv -1 \pmod 4$ and $b \equiv a\xi_1^{\frac{q^{d_1}-1}{4}} \pmod p$).

Proof. To determine the Hamming weight $W_H(c_i(x_1, x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\Theta_i(x_{1,i}, x_{2,i}) \;=\; 1 - G(\overline{\phi}_1^{\Delta_1 K_1}, \chi_1)\phi_1^{\Delta_1 K_1}(x_{1,i}) + G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i})F(x_{1,i}),$$

where $F(x_{1,i}) = \phi_1^{\Delta_1 K_2}(x_{1,i})\Big(G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1)+G(\overline{\phi}_1^{\Delta_1(K_1+K_2)}, \chi_1)\phi_1^{\Delta_1 K_1}(x_{1,i})\Big)$. As $M_1 =$

$M_2 = 2$, we note that $\phi_1^{\Delta_1 K_1}$ and $\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}$ are the quadratic characters of $\mathbb{F}_{q^{d_1}}$ and $\mathbb{F}_{q^{d_2}}$ respectively and q is odd. Since $\gcd(L, q-1) = 1$, the integer L must be odd. Further, since $M_1 = 2$ and $q-1$ divides $G\lambda$, we see that the integer g_1 divides 2. So we shall distinguish the following two cases: (a) $g_1 = 1$, and (b) $g_1 = 2$.

(a) Let $g_1 = 1$. Here we have $\frac{G\lambda}{q-1} = 2 = \gcd\left(\frac{q^{d_1}-1}{q-1}, G\right)$, which implies that both the integers d_1 and G are even. Since $G = \gcd(\ell_1, q^d - 1)$ is even and $g_1 = \gcd\left(\frac{q^{d_1}-1}{q^d-1}, \ell_1\right) = 1$, one can easily see that the integer $\frac{d_1}{d}$ is odd, which implies that the integer d is even. Further, as $\frac{G\lambda}{q-1} = 2$ and $M_2 = 2$, we see that $\frac{(q^d-1)\lambda' g_2 H}{q-1} = 4$. Next we note that $\frac{q^d-1}{q-1} = 1 + q + q^2 + \cdots + q^{d-1} \geq 4$. This implies that $\lambda' g_2 H = 1$ and $\frac{q^d-1}{q-1} = 4$, which further implies that $q = 3$ and $d = 2$. From this, we obtain $G\lambda = 4$. Since $\lambda = \gcd(2, \frac{3^{d_1}-1}{G})$ and the integer $\frac{3^d-1}{G}$ is even, we note that $\lambda = 2$, which gives $G = 2$. Further, it is easy to observe that

$$\begin{aligned}\Delta_1 K_2 &= \frac{(q^{d_1}-1)(-2\tau\ell_2(1-2\tau'\Delta_1) - \tau'(q^{d_2}-1)L)}{8} \\ &= \frac{(q^{d_1}-1)(-\tau\ell_2(1-2\tau'\Delta_1))}{4} - \frac{\tau'(q^{d_1}-1)(q^{d_2}-1)L}{8}.\end{aligned}$$

This implies that $\phi_1^{\Delta_1 K_2} = \overline{\phi}_1^{\frac{\tau\ell_2(q^{d_1}-1)(1-2\tau'\Delta_1)}{4}}$. Since $G = 2$ and $\lambda' = 1 = \gcd(2, \Delta_2 GL - \Delta_1\tau\ell_2)$, we note that the integer $\tau\ell_2$ is odd, which further implies that $O(\phi_1^{\Delta_1 K_2}) = 4$. Further, we note that $\Delta_1 K_1 = \frac{q^{d_1}-1}{2}$, and $\phi_1^{\Delta_1(K_1+K_2)} = \phi_1^{\frac{(q^{d_1}-1)(-\tau\ell_2(1-2\tau'\Delta_1)+2)}{4}}$. This gives $O(\phi_1^{\Delta_1(K_1+K_2)}) = 4$. Next since $p \equiv 3 \equiv -1 \pmod 4$, $r = 1$ and $\frac{d_1}{2}$ is odd, by Theorem 2.2.2, we see that $G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1) = G(\overline{\phi}_1^{\Delta_1(K_1+K_2)}) = -p^{\frac{d_1}{2}}$. This implies that the sum

$$\begin{aligned}F(x_{1,i}) &= -p^{\frac{d_1}{2}} \phi_1^{\Delta_1 K_2}(x_{1,i})(1 + \phi_1^{\Delta_1 K_1}(x_{1,i})) \\ &= -p^{\frac{d_1}{2}} e^{\left(\frac{-2\pi\iota\tau\ell_2(1-2\tau'\Delta_1)s_{1,i}}{4}\right)}(1 + e^{\pi\iota s_{1,i}})\end{aligned}$$

$$= \begin{cases} -2\, p^{\frac{d_1}{2}}(-1)^{\frac{s_{1,i}}{2}} & \text{if } 2 \mid s_{1,i}; \\ 0 & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

From this and by Theorem 2.2.1, we obtain

$$\Theta_i(x_{1,i}, x_{2,i}) = \begin{cases} 1 - 3^{\frac{d_1}{2}} + 2(-1)^{\frac{s_{1,i}+d_2+2s_{2,i}}{2}} 3^{\frac{d_1+d_2}{2}} & \text{if } 2 \mid s_{1,i}; \\ 1 + 3^{\frac{d_1}{2}} & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

(b) When $g_1 = 2 = \gcd\left(\frac{q^{d_1}-1}{q^d-1}, \ell_1\right)$, we see that $\frac{G\lambda}{q-1} = 1$ and both the integers d_1, ℓ_1 are even. Now as $M_2 = 2$, we observe that $\lambda' g_2 H = 2$ and $\frac{q^d-1}{q-1} = 1$, i.e., $d = 1$. Since $d = 1$ and d_1 is even, the integer d_2 must be odd and $g_2 = 1 = \gcd\left(\frac{q^{d_2}-1}{q-1}, \ell_2\right)$. This implies that the integer Δ_2 is odd and

$$\lambda' H = 2 = \gcd(\lambda H, \Delta_2 GL - \Delta_1 \tau \ell_2). \tag{5.20}$$

Further, since $\frac{g_1}{2} = \gcd\left(\Delta_1, \frac{\ell_1}{2}\right) = 1$ and $G = \gcd\left(\frac{\ell_1}{2}, q-1\right)$, by (5.20), one can easily observe that the integer Δ_1 is odd in this case. Next we see that

$$\Delta_1 K_2 = \frac{q^{d_1}-1}{2(q-1)}\Big(\frac{-\lambda\tau\ell_2(1-\tau'\Delta_1)}{2} - \frac{\tau'(q^{d_2}-1)L}{2}\Big) = \frac{(q^{d_1}-1)A}{4}, \tag{5.21}$$

where $A = \frac{-\tau\ell_2(1-\tau'\Delta_1)}{G} - \tau'\Delta_2 L$. Further, as Δ_1, Δ_2, L all are odd integers, we observe, by (5.20), that the integers G and $\tau\ell_2$ are of the same parity.

When G is even, the integer $\tau\ell_2$ is even. Since G divides $1 - \tau'\Delta_1$, we see that the integer τ' is odd. From this, it is easy to see that the integer A is odd. This, by (5.21), gives $O(\overline{\phi}_1^{\Delta_1 K_2}) = 4$.

On the other hand, when G is odd, we note that the integer $\tau\ell_2$ is odd. Next we observe that the integer τ' is odd if the integer $\frac{1-\tau'\Delta_1}{G}$ is even, while the integer τ' is even if the integer $\frac{1-\tau'\Delta_1}{G}$ is odd. That is, the integers $\frac{1-\tau'\Delta_1}{G}$ and τ' are of the opposite parity. Now as both the integers $\Delta_2 L$ and $\tau\ell_2$ are

odd, we see that the integer A is odd. This, by (5.21), gives $O(\overline{\phi}_1^{\Delta_1 K_2}) = 4$. Next we see that $\overline{\phi}_1^{\Delta_1(K_1+K_2)} = \overline{\phi}_1^{\frac{(q^{d_1}-1)(A+2)}{4}}$. In view of this, we observe that the characters $\overline{\phi}_1^{\Delta_1 K_2}$ and $\overline{\phi}_1^{\Delta_1(K_1+K_2)}$ are inverses of each other, which implies that $O(\overline{\phi}_1^{\Delta_1 K_2}) = O(\overline{\phi}_1^{\Delta_1(K_1+K_2)}) = 4$. Since $\Delta_1 = \frac{q^{d_1}-1}{2(q-1)}$ is odd, we note that $q \equiv 1 \pmod 4$ and $\frac{d_1}{2}$ is odd. So we shall distinguish the following two cases: (i) $p \equiv 3 \pmod 4$, and (ii) $p \equiv 1 \pmod 4$.

(i) When $p \equiv 3 \pmod 4$, the integer r must be even. That is, $p \equiv -1 \pmod 4$ and the integer $\frac{rd_1}{2}$ is even. Now by Theorem 2.2.2, we get $G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1) = G(\overline{\phi}_1^{\Delta_1(K_1+K_2)}, \chi_1) = (-1)^{\frac{rd_1}{2}-1} q^{\frac{d_1}{2}} = -q^{\frac{d_1}{2}}$.

This implies that

$$\begin{aligned} F(x_{1,i}) &= -q^{\frac{d_1}{2}} \phi_1^{\Delta_1 K_2}(x_{1,i})(1 + \phi_1^{\Delta_1 K_1}(x_{1,i})) \\ &= -q^{\frac{d_1}{2}} e^{\left(\frac{\pi \iota s_{1,i} A}{2}\right)}(1 + (-1)^{s_{1,i}}) = \begin{cases} -2\, q^{\frac{d_1}{2}} (-1)^{\frac{s_{1,i}}{2}} & \text{if } 2 \mid s_{1,i}; \\ 0 & \text{if } 2 \nmid s_{1,i}. \end{cases} \end{aligned}$$

From this and by Theorem 2.2.1, we obtain

$$\Theta_i(x_{1,i}, x_{2,i}) = \begin{cases} 1 + q^{\frac{d_1}{2}} + 2(-1)^{\frac{rd_2 + s_{1,i} + 2s_{2,i}}{2}} q^{\frac{d_1+d_2}{2}} & \text{if } 2 \mid s_{1,i}; \\ 1 - q^{\frac{d_1}{2}} & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

(ii) Let $p \equiv 1 \pmod 4$. Since $O(\overline{\phi}_1^{\Delta_1(K_1+K_2)}) = O(\overline{\phi}_1^{\Delta_1 K_2}) = 4$ divides $p-1$, by Theorem 11.4.4 of [11, p. 356], we see that there exists a multiplicative character ϕ of $\mathbb{F}_p$ having order 4 such that

$$\overline{\phi}_1^{\Delta_1(K_1+K_2)}(\alpha) = \phi(N_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_p}(\alpha)) \text{ and } \overline{\phi}_1^{\Delta_1 K_2}(\alpha) = \overline{\phi}(N_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_p}(\alpha)) \text{ for all } \alpha \in \mathbb{F}_{q^{d_1}}, \tag{5.22}$$

where $N_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_p}$ denotes the norm function from $\mathbb{F}_{q^{d_1}}$ onto $\mathbb{F}_p$. Further, by Davenport-Hasse's Theorem (see Theorem 11.5.2 of [11, p. 360]) and by using

the fact that the integer rd_1 is even, we get

$$G(\overline{\phi}_1^{\Delta_1(K_1+K_2)}, \chi_1) = -G(\phi, \chi')^{rd_1} \text{ and } G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1) = -G(\overline{\phi}, \chi')^{rd_1},$$

where χ' is the canonical additive character of $\mathbb{F}_p$. This implies that

$$F(x_{1,i}) = -\phi_1^{\Delta_1 K_2}(x_{1,i})\Big(G(\overline{\phi}, \chi')^{rd_1} + G(\phi, \chi')^{rd_1}(-1)^{s_{1,i}}\Big).$$

Since $\xi = \xi_1^{\frac{q^{d_1}-1}{p-1}}$ is a primitive element of $\mathbb{F}_p$, we see, by (5.22), that

$$\overline{\phi}_1^{\Delta_1 K_2}(\xi_1) = e^{\frac{2\pi\iota(q^{d_1}-1)A}{(q^{d_1}-1)4}} = \iota^A = \overline{\phi}(N_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_p}(\xi_1)) = \overline{\phi}(\xi_1^{\frac{q^{d_1}-1}{p-1}}) = \overline{\phi}(\xi)$$

and

$$\overline{\phi}_1^{\Delta_1(K_1+K_2)}(\xi_1) = e^{\frac{2\pi\iota(q^{d_1}-1)(A+2)}{(q^{d_1}-1)4}} = \iota^{(A+2)} = \phi(N_{\mathbb{F}_{q^{d_1}}/\mathbb{F}_p}(\xi_1)) = \phi(\xi_1^{\frac{q^{d_1}-1}{p-1}}) = \phi(\xi).$$

As the integer rd_1 is even and $\xi^{\frac{p-1}{2}} = -1$, by (2.4), we get

$$\begin{aligned} G(\overline{\phi}, \chi')^{rd_1} &= \phi^{rd_1}(-1)\overline{G(\phi, \chi')}^{rd_1} = \iota^{\frac{(A+2)(p-1)rd_1}{2}}\overline{G(\phi, \chi')}^{rd_1} \\ &= (-1)^{\frac{(A+2)(p-1)rd_1}{4}}\overline{G(\phi, \chi')}^{rd_1} = \overline{G(\phi, \chi')}^{rd_1}. \end{aligned} \tag{5.23}$$

We further assert that

$$F(x_{1,i}) = -\iota^{s_{1,i}} p^{\frac{rd_1}{4}}\Big((a+\iota b)^{\frac{rd_1}{2}} + (a-\iota b)^{\frac{rd_1}{2}}(-1)^{s_{1,i}}\Big).$$

To prove this assertion, we first note that $\phi_1^{\Delta_1 K_2}(x_{1,i}) = e^{\frac{2\pi\iota(q^{d_1}-1)As_{1,i}}{(q^{d_1}-1)4}} = \iota^{As_{1,i}}$, and we shall distinguish the following two cases: $A \equiv 1 \pmod 4$ and $A \equiv 3 \pmod 4$.

When $A \equiv 1 \pmod 4$, we have $\overline{\phi}(\xi) = \iota$. By Theorem 4.2.3 of [11, p. 163], we

see that $G(\overline{\phi}, \chi')^{rd_1} = p^{\frac{rd_1}{4}}(a+\iota b)^{\frac{rd_1}{2}}$. Now by (5.23), we obtain

$$F(x_{1,i}) = -\iota^{s_{1,i}} p^{\frac{rd_1}{4}} \Big((a+\iota b)^{\frac{rd_1}{2}} + (a-\iota b)^{\frac{rd_1}{2}} (-1)^{s_{1,i}} \Big).$$

When $A \equiv 3 \pmod 4$, we have $\phi(\xi) = \iota$. By Theorem 4.2.3 of [11, p. 163], we note that $G(\phi, \chi')^{rd_1} = p^{\frac{rd_1}{4}}(a+\iota b)^{\frac{rd_1}{2}}$. Now by (5.23), we get

$$\begin{aligned} F(x_{1,i}) &= -(-\iota)^{s_{1,i}} p^{\frac{rd_1}{4}} \Big((a-\iota b)^{\frac{rd_1}{2}} + (a+\iota b)^{\frac{rd_1}{2}} (-1)^{s_{1,i}} \Big) \\ &= -\iota^{s_{1,i}} p^{\frac{rd_1}{4}} \Big((a+\iota b)^{\frac{rd_1}{2}} + (a-\iota b)^{\frac{rd_1}{2}} (-1)^{s_{1,i}} \Big), \end{aligned}$$

which proves the assertion. This, by Theorem 2.2.1, implies that

$$\Theta_i(x_{1,i}, x_{2,i}) = \begin{cases} 1 + q^{\frac{d_1}{2}} + 2\, q^{\frac{d_1+2d_2}{4}} (-1)^{\frac{2(rd_2+s_{2,i})+s_{1,i}}{2}} \text{ Re } (a+\iota b)^{\frac{rd_1}{2}} & \text{if } 2 \mid s_{1,i}; \\ 1 - q^{\frac{d_1}{2}} + 2\, q^{\frac{d_1+2d_2}{4}} (-1)^{\frac{2(rd_2+s_{2,i})+1+s_{1,i}}{2}} \text{ Im } (a+\iota b)^{\frac{rd_1}{2}} & \text{if } 2 \nmid s_{1,i}. \end{cases}$$

□

In the following theorem, we determine the explicit value of $W_H(c_i(x_1, x_2))$ when $M_1 \geq 3$ and $M_2 = 2$.

Theorem 5.2.7. *Let $M_1 \geq 3$, $M_2 = 2$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \leq s_{1,i} \leq q^{d_1} - 2$ and $0 \leq s_{2,i} \leq q^{d_2} - 2$. Let $S = -\frac{\tau \ell_2 \lambda}{q-1}\big(1 - \frac{(q^d-1)\tau' \Delta_1}{G\lambda}\big) - \frac{\tau'(q^{d_2}-1)L}{q-1}$. Here S is an integer, the integer rd_2 is even and p is an odd prime.*

(a) Let S be even. Suppose that there exists a positive integer u satisfying $p^u \equiv -1 \pmod{M_1}$. If t is the least positive integer satisfying $p^t \equiv -1 \pmod{M_1}$, then we have $rd_1 = 2t\gamma$ for some positive integer γ.

- *If M_1 is even and $\frac{\gamma(p^t+1)}{M_1}$ is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} + \frac{m_i(q-1)\left(-1+q^{\frac{d_1}{2}}(M_1-1)\right)\left(1+(-1)^{s_{2,i}}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_1 \mid s_{1,i}+\frac{M_1}{2}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}\right)\left(1+(-1)^{s_{2,i}}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_1 \nmid s_{1,i}+\frac{M_1}{2}. \end{cases}$$

- *If either M_1 is odd or $\frac{\gamma(p^t+1)}{M_1}$ is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma}q^{\frac{d_1}{2}}(M_1-1)\right)\left(1+\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)\Big)} \\ \qquad\qquad \text{if } M_1 \mid s_{1,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma}q^{\frac{d_1}{2}}\right)\left(1+\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_1 \nmid s_{1,i}. \end{cases}$$

(b) Let S be odd. Suppose that there exists a positive integer u' satisfying $p^{u'} \equiv -1 \pmod{2M_1}$. If t and t' are the least positive integers satisfying $p^t \equiv -1 \pmod{M_1}$ and $p^{t'} \equiv -1 \pmod{2M_1}$, then we have $rd_1 = 2t\gamma = 2t'\gamma'$ for some positive integers γ and γ'.

- *If M_1 is even and $\frac{\gamma\gamma'(p^t+1)(p^{t'}+1)}{2M_1^2}$ is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}+(-1)^{\left(\frac{s_{1,i}}{M_1}+s_{2,i}\right)}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_1+d_2}{2}}M_1\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_1 \mid s_{1,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-q^{\frac{d_1}{2}}(M_1-1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \text{ if } M_1 \nmid s_{1,i} \ \&\ M_1 \mid s_{1,i}+\frac{M_1}{2}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} \text{ if } M_1 \nmid s_{1,i} \ \&\ M_1 \nmid s_{1,i}+\frac{M_1}{2}. \end{cases}$$

- *If both the integers $M_1, \frac{\gamma'(p^{t'}+1)}{2M_1}$ are even and the integer $\frac{\gamma(p^t+1)}{M_1}$ is odd,*

then we have

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+q^{\frac{d_1}{2}}+(-1)^{\left(\frac{s_{1,i}}{M_1}+\gamma'+s_{2,i}\right)}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_1+d_2}{2}}M_1\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } M_1 \mid s_{1,i}; & \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-q^{\frac{d_1}{2}}(M_1-1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \text{ if } M_1 \nmid s_{1,i} \ \&\ M_1 \mid s_{1,i}+\frac{M_1}{2}; & \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} \text{ if } M_1 \nmid s_{1,i} \ \&\ M_1 \nmid s_{1,i}+\frac{M_1}{2}. & \end{cases}$$

- *If either M_1 is odd or $\frac{\gamma(p^t+1)}{M_1}$ is even and $\frac{\gamma'(p^{t'}+1)}{2M_1}$ is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma-1}q^{\frac{d_1}{2}}(M_1-1)+\mathcal{X}_iM_1\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } M_1 \mid s_{1,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } M_1 \nmid s_{1,i}, \end{cases}$$

where $\mathcal{X}_i = (-1)^{\left(\frac{s_{1,i}}{M_1}+s_{2,i}\right)}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_1+d_2}{2}}$.

- *If $\frac{\gamma'(p^{t'}+1)}{2M_1}$ is even and either M_1 is odd or the integer $\frac{\gamma(p^t+1)}{M_1}$ is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma-1}q^{\frac{d_1}{2}}(M_1-1)+\mathcal{Y}_iM_1\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } M_1 \mid s_{1,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } M_1 \nmid s_{1,i}, \end{cases}$$

where $\mathcal{Y}_i = (-1)^{\left(\frac{s_{1,i}}{M_1}+\gamma'+s_{2,i}\right)}\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_1+d_2}{2}}$.

Proof. To determine the Hamming weight $W_H(c_i(x_1,x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\begin{aligned} \Theta_i(x_{1,i},x_{2,i}) &= 1+G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i})\Big(\sum_{z_1=0}^{M_1-1}G(\overline{\phi}_1^{\Delta_1(K_2+z_1K_1)},\chi_1) \\ &\qquad \phi_1^{\Delta_1(K_2+z_1K_1)}(x_{1,i})\Big) - \sum_{z_1=1}^{M_1-1}G(\overline{\phi}_1^{\Delta_1K_1z_1},\chi_1)\phi_1^{\Delta_1K_1z_1}(x_{1,i}). \quad (5.24) \end{aligned}$$

For this, since $M_2 = 2$, we note that $\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}$ is the quadratic character of $\mathbb{F}_{q^{d_2}}$ and q is odd. Since $\gcd(L, q-1) = 1$, the integer L must be odd. Further, for $0 \leq z_1 \leq M_1 - 1$, we see that

$$\Delta_1(K_2+z_1K_1) = \frac{q^{d_1}-1}{g_1(q^d-1)\lambda' g_2 H}\Big(-\lambda\tau\ell_2\Big(1-\frac{(q^d-1)\tau'\Delta_1}{G\lambda}\Big)-\tau'(q^{d_2}-1)L+z_1(q-1)M_2\Big).$$

Now as $M_2 = 2$, for $0 \leq z_1 \leq M_1 - 1$, we obtain

$$\begin{aligned}\Delta_1(K_2 + z_1K_1) &= \frac{q^{d_1}-1}{2G\lambda g_1}\Big(-\lambda\tau\ell_2\Big(1-\frac{(q^d-1)\tau'\Delta_1}{G\lambda}\Big)-\tau'(q^{d_2}-1)L+2z_1(q-1)\Big)\\ &= \frac{(q^{d_1}-1)(S+2z_1)}{2M_1}. \qquad (5.25)\end{aligned}$$

Note that S is an integer. Now we shall distinguish the following two cases: (a) S is even and (b) S is odd.

(a) Let S be even. Since $O(\phi_1^{\Delta_1 K_1}) = O(\phi_1^{\frac{q^{d_1}-1}{M_1}}) = M_1$, we note that $\phi_1^{\frac{(q^{d_1}-1)S}{2M_1}} \in \langle\phi_1^{\Delta_1 K_1}\rangle$. This, by (5.25), implies that $\{\phi_1^{\Delta_1(K_2+z_1K_1)} : 0 \leq z_1 \leq M_1 - 1\} = \langle\phi_1^{\Delta_1 K_1}\rangle$. Therefore equation (5.24) can be rewritten as

$$\begin{aligned}\Theta_i(x_{1,i}, x_{2,i}) &= \Big(-1+\sum_{z_1=1}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i})\Big)\times\Big(-1+\\ &\qquad G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i})\Big) \qquad (5.26)\end{aligned}$$

We next assert that the integer d_2 is even in this case.

To prove this assertion, we suppose, on the contrary, that the integer d_2 is odd. This implies that both the integers d and Δ_2 are odd. As $M_2 = 2$, we see that $g_2 \mid 2$. Since d_2 is odd, we must have $g_2 = 1$. This implies that $\frac{(q^d-1)\lambda' H}{G\lambda} = 2$, which gives $\frac{(q^d-1)\lambda' H}{q-1} = 2\big(\frac{G\lambda}{q-1}\big)$. From this, we see that $2 \mid \frac{(q^d-1)\lambda' H}{q-1}$, which implies that $2 \mid \lambda' H = \gcd(\lambda H, \Delta_2 GL - \Delta_1\tau\ell_2)$. Further, it is easy to observe that the integer Δ_1 must be odd, which implies that the integers G and $\tau\ell_2$

are of the same parity. Further, since both Δ_1 and d are odd, one can see that the integer $\frac{G\lambda}{q-1} = \gcd\left(\frac{\Delta_1(q^d-1)}{(q-1)}, G\right)$ is odd.

When G is even, both the integers $\frac{q-1}{\lambda}$ and $\tau\ell_2$ are even. Since $\frac{\tau'\Delta_1(q^d-1)}{G\lambda} \equiv 1 \pmod{\frac{q-1}{\lambda}}$, the integer τ' must be odd, which implies that the integer S is odd. This is a contradiction.

On the other hand, when G is odd, we note that both the integers $\frac{q-1}{\lambda}, \tau\ell_2$ are odd. Further, since $\frac{\tau'\Delta_1(q^d-1)}{G\lambda} \equiv 1 \pmod{\frac{q-1}{\lambda}}$ and $\frac{\Delta_1(q^d-1)}{G\lambda}$ is odd, we observe that τ' is odd if $\frac{\lambda}{q-1}\left(1-\frac{\tau'\Delta_1(q^d-1)}{G\lambda}\right)$ is even, while τ' is even if $\frac{\lambda}{q-1}\left(1-\frac{\tau'\Delta_1(q^d-1)}{G\lambda}\right)$ is odd. Now as both the integers $\frac{(q^{d_2}-1)L}{q-1}$ and $\tau\ell_2$ are odd, we see that the integer S is odd, which is a contradiction.

This proves the assertion that the integer d_2 is even. Next by Theorem 2.2.1, we note that

$$G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i}) = -\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}} (-1)^{s_{2,i}}. \tag{5.27}$$

Further, for $1 \leq z_1 \leq M_1 - 1$, by Theorem 2.2.2, we see that

$$G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1) = \begin{cases} (-1)^{z_1} q^{\frac{d_1}{2}} & \text{if } M_1 \text{ is even and } \frac{p\gamma(p^t+1)}{M_1} \text{ is odd;} \\ (-1)^{\gamma-1} q^{\frac{d_1}{2}} & \text{otherwise.} \end{cases} \tag{5.28}$$

When M_1 is even and $\frac{p\gamma(p^t+1)}{M_1}$ is odd, we see, by (5.28), that

$$\begin{aligned} \sum_{z_1=1}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) &= q^{\frac{d_1}{2}} \sum_{z_1=1}^{M_1-1} (-1)^{z_1} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) \\ &= q^{\frac{d_1}{2}} \sum_{z_1}^{M_1-1} e^{\pi\iota z_1} e^{\frac{2\pi\iota z_1 s_{1,i}}{M_1}} \\ &= q^{\frac{rd_1}{2}} \sum_{z_1=1}^{M_1-1} e^{\frac{2\pi\iota z_1}{M_1}\left(s_{1,i}+\frac{M_1}{2}\right)} \end{aligned}$$

$$= \begin{cases} q^{\frac{d_1}{2}}(M_1-1) & \text{if } M_1 \mid s_{1,i}+\frac{M_1}{2}; \\ -q^{\frac{d_1}{2}} & \text{if } M_1 \nmid s_{1,i}+\frac{M_1}{2}. \end{cases}$$

This, by (5.26) and (5.27), implies that

$$\Theta_i(x_{1,i},x_{2,i}) = \begin{cases} (-1+q^{\frac{d_1}{2}}(M_1-1))(-1-\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}) & \\ & \text{if } M_1 \mid s_{1,i}+\frac{M_1}{2}; \\ (-1-q^{\frac{d_1}{2}})(-1-\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}) & \text{if } M_1 \nmid s_{1,i}+\frac{M_1}{2}. \end{cases}$$

On the other hand, when either M_1 is odd or $\frac{\gamma(p^t+1)}{M_1}$ is even, we see, by (5.28), that

$$\begin{aligned} \sum_{z_1=1}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1},\chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) &= (-1)^{\gamma-1}q^{\frac{d_1}{2}}\sum_{z_1=1}^{M_1-1}\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) \\ &= (-1)^{\gamma-1}q^{\frac{d_1}{2}}\sum_{z_1=1}^{M_1-1} e^{\frac{2\pi\iota z_1 s_{1,i}}{M_1}} \\ &= \begin{cases} (-1)^{\gamma-1}q^{\frac{d_1}{2}}(M_1-1) & \text{if } M_1 \mid s_{1,i}; \\ -(-1)^{\gamma-1}q^{\frac{d_1}{2}} & \text{if } M_1 \nmid s_{1,i}. \end{cases} \end{aligned}$$

This, by (5.26) and (5.27), further implies that

$$\Theta_i(x_{1,i},x_{2,i}) = \begin{cases} (-1+(-1)^{\gamma-1}q^{\frac{d_1}{2}}(M_1-1))(-1-\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}) & \\ & \text{if } M_1 \mid s_{1,i}; \\ (-1-(-1)^{\gamma-1}q^{\frac{d_1}{2}})(-1-\iota^{\frac{rd_2(p-1)^2}{4}}q^{\frac{d_2}{2}}(-1)^{s_{2,i}}) & \text{if } M_1 \nmid s_{1,i}. \end{cases}$$

(b) Next let S be odd. Here as $O(\phi_1^{\frac{q^{d_1}-1}{2M_1}}) = 2M_1$, we note that $\phi_1^{\frac{(q^{d_1}-1)S}{2M_1}} \in \langle \phi_1^{\frac{q^{d_1}-1}{2M_1}} \rangle$. Further, by (5.25), one can easily observe that $\left\{\phi_1^{\Delta_1(K_2+z_1K_1)} : 0 \le z_1 \le M_1-1\right\} = \left\{\phi_1^{\frac{(q^{d_1}-1)(1+2z_1)}{2M_1}} : 0 \le z_1 \le M_1-1\right\}$. In view of this, equation (5.24)

can be rewritten as

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 - \sum_{z_1=1}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) + G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda}{H\lambda'}}(x_{2,i}) \times\Big(\sum_{z_1=0}^{M_1-1} G(\overline{\phi}_1^{\frac{(q^{d_1}-1)(1+2z_1)}{2M_1}}, \chi_1)\phi_1^{\frac{(q^{d_1}-1)(1+2z_1)}{2M_1}}(x_{1,i})\Big). \tag{5.29}$$

Here we assert that the integer rd_2 is even.

To prove this assertion, we suppose, on the contrary, that rd_2 is odd. Since d_2 is odd, the integer d is odd. Now working in a similar manner as in part (a), we see that the integer Δ_1 is odd. Further, as the integer rd_1 is even, we note that g_1 is even. Now since $p^{t'} \equiv -1 \pmod{2M_1}$ and $g_1 \mid M_1$, we observe that $p \equiv 3 \pmod 4$. Further, as $rd_1 = 2t'\gamma'$ and $2M_1 \mid p^{t'} + 1$, we see that the integer $\frac{q^{d_1}-1}{2M_1}$ is even. On the other hand, let s be the positive integer such that $2^s \mid\mid g_1$, i.e., $2^s \mid g_1$ but $2^{s+1} \nmid g_1$. Since both r, d are odd, we note that $2 \mid\mid q-1$ and $2 \mid\mid q^d - 1$. Further, as Δ_1 is odd, one can easily observe that $2^{s+1} \mid\mid q^{d_1} - 1$ and the integer $\frac{G\lambda}{q-1} = \gcd(\frac{\Delta_1(q^d-1)}{(q-1)}, G)$ is odd. From this, it follows that the integer $\frac{q^{d_1}-1}{2M_1}$ is odd, which is a contradiction.

This proves the assertion that the integer rd_2 is even. Further, for $1 \le k \le 2M_1 - 1$, by Theorem 2.2.2, we see that

$$G(\overline{\phi}_1^{\frac{(q^{d_1}-1)k}{2M_1}}, \chi_1) = \begin{cases} (-1)^k q^{\frac{d_1}{2}} & \text{if } \frac{p\gamma'(p^{t'}+1)}{2M_1} \text{ is odd;} \\ (-1)^{\gamma'-1} q^{\frac{d_1}{2}} & \text{otherwise.} \end{cases} \tag{5.30}$$

Now on substituting the values of Gauss sums from (5.27), (5.28) and (5.30) in equation (5.29) and after an easy computation, we obtain the desired values of the sum $\Theta_i(x_{1,i}, x_{2,i})$ in the respective cases.

□

Next we proceed to determine the explicit value of the Hamming weight $W_H(c_i(x_1,$

$x_2)$) when $M_2 \geq 3$. From now on, throughout this section, suppose that there exists a positive integer u_2 satisfying $p^{u_2} \equiv -1 \pmod{M_2}$. Further, let t_2 be the least positive integer satisfying $p^{t_2} \equiv -1 \pmod{M_2}$. Then by Theorem 2.2.2, we have $rd_2 = 2t_2\gamma_2$ for some positive integer γ_2, and for $1 \leq z_2 \leq M_2 - 1$, we have

$$G(\overline{\phi_2}^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}, \chi_2) = \begin{cases} (-1)^{z_2} q^{\frac{d_2}{2}} & \text{if } M_2 \text{ is even and } \frac{p\gamma_2(p^{t_2}+1)}{M_2} \text{ is odd;} \\ (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}} & \text{otherwise.} \end{cases} \tag{5.31}$$

In the following theorem, we determine the explicit value of $W_H(c_i(x_1, x_2))$ when $M_1 = 1$ and $M_2 \geq 3$.

Theorem 5.2.8. *Let $M_1 = 1$, $M_2 \geq 3$, $B = -\frac{\lambda\tau\ell_2}{G\lambda g_2}\big(1 - \frac{(q^d-1)\tau'\Delta_1}{G\lambda}\big) - \frac{\tau'(q^{d_2}-1)L}{g_2 G\lambda}$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \leq s_{1,i} \leq q^{d_1} - 2$ and $0 \leq s_{2,i} \leq q^{d_2} - 2$. Further, let us define the integers $T = \gcd\big(B, \frac{(q^d-1)\lambda' H}{G\lambda}\big)$ and $N = \frac{(q^d-1)\lambda' H}{G\lambda T}$, (note that $N \mid M_2$).*

(a) Let $N = 1$.

- *If Tg_2 is even and $\frac{p\gamma_2(p^{t_2}+1)}{Tg_2}$ is odd, then we have*

$$W_H(c_i(x_1, x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1 - q^{\frac{d_2}{2}}(Tg_2 - 1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i} + \frac{Tg_2}{2}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+q^{\frac{d_2}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i} + \frac{Tg_2}{2}. \end{cases}$$

- *If either Tg_2 is odd or $\frac{p\gamma_2(p^{t_2}+1)}{Tg_2}$ is even, then we have*

$$W_H(c_i(x_1, x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1 - (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}}(Tg_2 - 1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1 + (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i}. \end{cases}$$

(b) When $N = 2$, the integer rd_1 is even and p is an odd prime.

- *If* $\frac{\gamma_2(p^{t_2}+1)}{2Tg_2}$ *is odd, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-q^{\frac{d_2}{2}}(Tg_2-1)+\mathcal{U}_i Tg_2\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+q^{\frac{d_2}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i}, \end{cases}$$

where $\mathcal{U}_i = \iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{\left(\frac{s_{2,i}}{Tg_2}+s_{1,i}\right)} q^{\frac{d_1+d_2}{2}}$.

- *If* $\frac{\gamma_2(p^{t_2}+1)}{2Tg_2}$ *is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_2}q^{\frac{d_2}{2}}\left(Tg_2-1+\mathcal{V}_i Tg_2\right)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma_2}q^{\frac{d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i}, \end{cases}$$

where $\mathcal{V}_i = \iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}(-1)^{\left(\frac{s_{2,i}}{Tg_2}+s_{1,i}\right)}$.

(c) *Let* $N \geq 3$. *There exists a least positive integer* s' *satisfying* $p^{s'} \equiv -1 \ (mod\ N)$. *Here we have* $rd_1 = 2s'\nu'$ *for some positive integer* ν'.

- *If either the integer* TNg_2 *is odd or both the integers* $TNg_2, \frac{p\gamma_2(p^{t_2}+1)}{TNg_2}$ *are even and* N *is odd or both the integers* $\frac{p\nu'(p^{s'}+1)}{N}, \frac{p\gamma_2(p^{t_2}+1)}{TNg_2}$ *are of the same parity and* N *is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1-(-1)^{\gamma_2}q^{\frac{d_2}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_2}q^{\frac{d_2}{2}}(Tg_2-1+(-1)^{\nu'}Tg_2(N-1)q^{\frac{d_1}{2}})\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad \text{if } Tg_2 \mid s_{2,i} \ \&\ N \mid \frac{s_{2,i}}{Tg_2} + \frac{Bs_{1,i}}{T}; & \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_2}q^{\frac{d_2}{2}}(Tg_2-1-(-1)^{\nu'}Tg_2q^{\frac{d_1}{2}})\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad \text{if } Tg_2 \mid s_{2,i} \ \&\ N \nmid \frac{s_{2,i}}{Tg_2} + \frac{Bs_{1,i}}{T}. & \end{cases}$$

- *If* TNg_2 *is even,* $\frac{p\gamma_2(p^{t_2}+1)}{TNg_2}$ *is odd and either* N *is odd or* $\frac{p\nu'(p^{s'}+1)}{N}$ *is even,*

then we have

$$W_H(c_i(x_1,x_2))=\begin{cases}\frac{m_i(q-1)}{q}-\frac{m_i(q-1)(1+q^{\frac{d_2}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid \frac{M_2+2s_{2,i}}{2};\\ \frac{m_i(q-1)}{q}-\frac{m_i(q-1)\left(1-q^{\frac{d_2}{2}}(Tg_2(1+(N-1)(-1)^{\nu'}q^{\frac{d_1}{2}})-1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid \frac{M_2+2s_{2,i}}{2} \ \&\ N \mid \frac{M_2+2s_{2,i}}{2Tg_2}+\frac{Bs_{1,i}}{T};\\ \frac{m_i(q-1)}{q}-\frac{m_i(q-1)\left(1-q^{\frac{d_2}{2}}(Tg_2(1-q^{\frac{d_1}{2}}(-1)^{\nu'})-1)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid \frac{M_2+2s_{2,i}}{2} \ \&\ N \nmid \frac{M_2+2s_{2,i}}{2Tg_2}+\frac{Bs_{1,i}}{T}.\end{cases}$$

- *If* $\frac{p\nu'(p^{s'}+1)}{N}$ *is odd and both* $N, \frac{p\gamma_2(p^{t_2}+1)}{TNg_2}$ *are even, then we have*

$$W_H(c_i(x_1,x_2))=\begin{cases}\frac{m_i(q-1)}{q}-\frac{m_i(q-1)\left(1-(-1)^{\gamma_2}q^{\frac{d_2}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \nmid s_{2,i};\\ \frac{m_i(q-1)}{q}-\frac{m_i(q-1)\left(1+(-1)^{\gamma_2}q^{\frac{d_2}{2}}(Tg_2-1-q^{\frac{d_1}{2}}(N-1)Tg_2)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i} \ \&\ N \mid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T}+\frac{N}{2};\\ \frac{m_i(q-1)}{q}-\frac{m_i(q-1)\left(1+(-1)^{\gamma_2}q^{\frac{d_2}{2}}(Tg_2-1+q^{\frac{d_1}{2}}Tg_2)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } Tg_2 \mid s_{2,i} \ \&\ N \nmid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T}+\frac{N}{2}.\end{cases}$$

Proof. To determine the Hamming weight $W_H(c_i(x_1,x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\Theta_i(x_{1,i},x_{2,i})=1+\sum_{z_2=1}^{M_2-1}G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})G(\overline{\phi}_1^{\Delta_1 K_2 z_2},\chi_1)\phi_1^{\Delta_1 K_2 z_2}(x_{1,i}). \tag{5.32}$$

For this, we note that as $M_1=1$, we must have $g_1=1$ and $G\lambda=q-1$. Further, it is easy to see that

$$\Delta_1 K_2=\frac{(q^{d_1}-1)G\lambda}{(q^d-1)\lambda' g_2 H}\Big(-\frac{\lambda\tau\ell_2}{G\lambda}\Big(1-\frac{(q^d-1)\tau'\Delta_1}{G\lambda}\Big)-\frac{\tau'(q^{d_2}-1)L}{G\lambda}\Big)=\frac{(q^{d_1}-1)G\lambda B}{(q^d-1)\lambda' H}. \tag{5.33}$$

Note that B is an integer. Next by (5.33), we see that $O(\phi_1^{\Delta_1 K_2})=\frac{(q^d-1)\lambda' H}{G\lambda T}=N$. Now we shall distinguish the following three cases: (a) $N=1$, (b) $N=2$, and (c)

$N \geq 3$.

(a) Let $N = 1$. Here by (2.4) and (5.32), we note that

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 - \sum_{z_2=1}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}).$$

When Tg_2 is even and $\frac{p^{\gamma_2}(p^{t_2}+1)}{Tg_2}$ is odd, we see, by (5.31), that

$$\begin{aligned}
\Theta_i(x_{1,i}, x_{2,i}) &= 1 - q^{\frac{d_2}{2}} \sum_{z_2=1}^{Tg_2-1} (-1)^{z_2} \phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) \\
&= 1 - q^{\frac{d_2}{2}} \sum_{z_2=1}^{Tg_2-1} e^{\pi\iota z_2} e^{\frac{2\pi\iota z_2 s_{2,i}}{Tg_2}} \\
&= 1 - q^{\frac{d_2}{2}} \sum_{z_2=1}^{Tg_2-1} e^{\frac{2\pi\iota z_2}{Tg_2}\left(s_{2,i}+\frac{Tg_2}{2}\right)} \\
&= \begin{cases} 1 - q^{\frac{d_2}{2}}(Tg_2 - 1) & \text{if } Tg_2 \mid s_{2,i} + \frac{Tg_2}{2}; \\ 1 + q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i} + \frac{Tg_2}{2}. \end{cases}
\end{aligned}$$

On the other hand, when either Tg_2 is odd or $\frac{p^{\gamma_2}(p^{t_2}+1)}{Tg_2}$ is even, we see, by (5.31), that

$$\begin{aligned}
\Theta_i(x_{1,i}, x_{2,i}) &= 1 - (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}} \sum_{z_2=1}^{Tg_2-1} \phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) \\
&= \begin{cases} 1 - (-1)^{\gamma_2-1} q^{\frac{d_2}{2}}(Tg_2 - 1) & \text{if } Tg_2 \mid s_{2,i}; \\ 1 + (-1)^{\gamma_2-1} q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i}. \end{cases}
\end{aligned}$$

(b) Let $N = 2$. Here we note that $\phi_1^{\Delta_1 K_2}$ is the quadratic character of $\mathbb{F}_{q^{d_1}}$ and q is odd. Further, each integer z_2 satisfying $1 \leq z_2 < M_2 = 2Tg_2$ can be uniquely expressed as $z_2 = 2Q + R$, where $0 \leq Q < Tg_2$ when $R = 1$ and $0 < Q < Tg_2$

when $R = 0$. Hence equation (5.32) can be rewritten as

$$\Theta_i(x_{1,i}, x_{2,i}) = 1 - \sum_{Q=1}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda 2Q}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda 2Q}{H\lambda'}}(x_{2,i}) + G(\overline{\phi}_1^{\Delta_1 K_2}, \chi_1)\phi_1^{\Delta_1 K_2}(x_{1,i}) \times\Big(\sum_{Q=0}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda(2Q+1)}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda(2Q+1)}{H\lambda'}}(x_{2,i})\Big). \tag{5.34}$$

Now we assert that the integer rd_1 is even.

To prove this assertion, we suppose, on the contrary, that the integer rd_1 is odd. This implies that both the integers d and Δ_1 are odd. Since rd_2 is even, we note that the integer d_2 is even. Further, as $N = \frac{(q^d-1)\lambda' H}{G\lambda T} = 2$ and $G\lambda = q - 1$, we observe that $2 \mid \lambda' H = \gcd(\lambda H, \Delta_2 GL - \frac{\Delta_1 \tau \ell_2}{g_2})$. We note that $\gcd(\Delta_2, \frac{\ell_2}{g_2}) = 1$. Further, it is easy to show that the integer Δ_2 is odd, which implies that the integer g_2 is even. Next since $rd_2 = 2t_2\gamma_2$ and $p^{t_2} \equiv -1 \pmod{2Tg_2}$, we see that the integer $\frac{q^{d_2}-1}{2Tg_2}$ is even. On the other hand, as g_2 is even, there exists a positive integer s such that $2^s \mid\mid g_2$. Further, as $p^{t_2} \equiv -1 \pmod{2Tg_2}$, we note that $p \equiv 3 \pmod 4$. Since both r, d are odd, we see that $2 \mid\mid q - 1$ and $2 \mid\mid q^d - 1$. Now as $\Delta_2 = \frac{q^{d_2}-1}{(q^d-1)g_2}$ is odd, it is easy to observe that $2^{s+1} \mid\mid q^{d_2} - 1$. Since $\lambda' H \mid G\lambda = q - 1$, we note that $2 \mid\mid \lambda' H$. From this, it follows that the integer $T = \frac{(q^d-1)\lambda' H}{(q-1)2}$ is odd, which implies that the integer $\frac{q^{d_2}-1}{2Tg_2}$ is odd. This is a contradiction.

This proves the assertion that the integer rd_1 is even.

(i) Now when $\frac{\gamma_2(p^{t_2}+1)}{2Tg_2}$ is odd, by (5.31), we see that

$$\sum_{Q=0}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda(2Q+1)}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda(2Q+1)}{H\lambda'}}(x_{2,i}) = -q^{\frac{d_2}{2}} \sum_{Q=0}^{Tg_2-1} \phi_2^{\frac{\Delta_2 G\lambda(2Q+1)}{H\lambda'}}(x_{2,i}) = -q^{\frac{d_2}{2}} \sum_{Q=0}^{Tg_2-1} e^{\frac{\pi\iota s_{2,i}}{Tg_2} + \frac{2\pi\iota s_{2,i} Q}{Tg_2}}$$

$$= \begin{cases} -Tg_2 q^{\frac{d_2}{2}} (-1)^{\frac{s_{2,i}}{Tg_2}} & \text{if } Tg_2 \mid s_{2,i}; \\ 0 & \text{if } Tg_2 \nmid s_{2,i} \end{cases}$$

and

$$\begin{aligned} \sum_{Q=1}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda 2Q}{H\lambda'}}, \chi_2)\phi_2^{\frac{\Delta_2 G\lambda 2Q}{H\lambda'}}(x_{2,i}) &= q^{\frac{rd_2}{2}} \sum_{Q=1}^{Tg_2-1} \phi_2^{\frac{\Delta_2 G\lambda 2Q}{H\lambda'}}(x_{2,i}) \\ &= \begin{cases} q^{\frac{d_2}{2}}(Tg_2 - 1) & \text{if } Tg_2 \mid s_{2,i}; \\ -q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i}. \end{cases} \end{aligned}$$

This, by (5.34) and by Theorem 2.2.1, implies that

$$\Theta_i(x_{1,i}, x_{2,i}) = \begin{cases} 1 - q^{\frac{d_2}{2}}(Tg_2 - 1) + \iota^{\frac{rd_1(p-1)^2}{4}} (-1)^{\left(\frac{s_{2,i}}{Tg_2} + s_{1,i}\right)} q^{\frac{d_1+d_2}{2}} Tg_2 & \\ & \text{if } Tg_2 \mid s_{2,i}; \\ 1 + q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i}. \end{cases}$$

(ii) When $\frac{\gamma_2(p^{t_2}+1)}{2Tg_2}$ is even, working in a similar manner as in part (i), we obtain

$$\Theta_i(x_{1,i}, x_{2,i}) = \begin{cases} 1 - (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}} \left(Tg_2 - 1 + \iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}} (-1)^{\left(\frac{s_{2,i}}{Tg_2} + s_{1,i}\right)} Tg_2\right) & \\ & \text{if } Tg_2 \mid s_{2,i}; \\ 1 + (-1)^{\gamma_2 - 1} q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i}. \end{cases}$$

(c) Let $N \geq 3$. Here for $1 \leq u \leq N-1$, we see, by Theorem 2.2.2, that

$$G(\overline{\phi}_1^{\Delta_1 K_2 u}, \chi_1) = \begin{cases} (-1)^u q^{\frac{d_1}{2}} & \text{if } N \text{ is even and } \frac{p\nu'(p^{s'}+1)}{N} \text{ is odd}; \\ (-1)^{\nu'-1} q^{\frac{d_1}{2}} & \text{otherwise.} \end{cases} \tag{5.35}$$

In this case, it is easy to see that each integer z_1 satisfying $1 \leq z_1 < M_2 = TNg_2$ can be uniquely written as $z_1 = NQ + R$, where $0 \leq Q < Tg_2$ when $1 \leq R < N$ and $1 \leq Q < Tg_2$ when $R = 0$. Therefore equation (5.32) can be

rewritten as

$$\Theta_i(x_{1,i},x_{2,i}) = 1-\sum_{Q=1}^{Tg_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda NQ}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda NQ}{H\lambda'}}(x_{2,i}) + \sum_{Q=0}^{Tg_2-1}\sum_{R=1}^{N-1}\Big(G(\overline{\phi}_1^{\Delta_1 K_2 R},\chi_1) \phi_1^{\Delta_1 K_2 R}(x_{1,i}) G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda(NQ+R)}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda(NQ+R)}{H\lambda'}}(x_{2,i})\Big). \tag{5.36}$$

Here we shall consider the case when N is even and both the integers $\frac{p\gamma_2(p^{t_2}+1)}{TNg_2}$, $\frac{p\nu'(p^{s'}+1)}{N}$ are odd. In this case, by (5.31), (5.35) and (5.36), we obtain

$$\Theta_i(x_{1,i},x_{2,i}) = 1 - q^{\frac{d_2}{2}}U(x_{2,i}) + q^{\frac{d_1+d_2}{2}}V(x_{1,i},x_{2,i}), \tag{5.37}$$

where

$$U(x_{2,i}) = \sum_{Q=1}^{Tg_2-1}\phi_2^{\frac{\Delta_2 G\lambda NQ}{H\lambda'}}(x_{2,i})$$

and

$$V(x_{1,i},x_{2,i}) = \Big(1+U(x_{2,i})\Big)\Big(\sum_{R=1}^{N-1}\phi_2^{\frac{\Delta_2 G\lambda R}{H\lambda'}}(x_{2,i})\phi_1^{\Delta_1 K_2 R}(x_{1,i})\Big).$$

Next we observe that

$$U(x_{2,i}) = \sum_{Q=1}^{Tg_2-1} e^{\frac{2\pi\iota(q^{d_2}-1)G\lambda NQs_{2,i}}{(q^d-1)(q^{d_2}-1)g_2H\lambda'}} = \sum_{Q=1}^{Tg_2-1} e^{\frac{2\pi\iota Qs_{2,i}}{Tg_2}} = \begin{cases} Tg_2-1 & \text{if } Tg_2 \mid s_{2,i};\\ -1 & \text{otherwise.}\end{cases}$$

and

$$\begin{aligned}\sum_{R=1}^{N-1}\phi_2^{\frac{\Delta_2 G\lambda R}{H\lambda'}}(x_{2,i})\phi_1^{\Delta_1 K_2 R}(x_{1,i}) &= \sum_{R=1}^{N-1} e^{\frac{2\pi\iota Rs_{2,i}}{TNg_2}+\frac{2\pi\iota BRs_{1,i}}{TN}}\\ &= \begin{cases} N-1 & \text{if } Tg_2 \mid s_{2,i} \text{ and } N \mid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T};\\ -1 & \text{if } Tg_2 \mid s_{2,i} \text{ and } N \nmid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T}.\end{cases}\end{aligned}$$

From this, it follows that

$$V(x_{1,i},x_{2,i})=\begin{cases} Tg_2(N-1) & \text{if } Tg_2 \mid s_{2,i} \text{ and } N \mid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T};\\ -Tg_2 & \text{if } Tg_2 \mid s_{2,i} \text{ and } N \nmid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T};\\ 0 & \text{if } Tg_2 \nmid s_{2,i}. \end{cases}$$

This, by (5.37), further implies that

$$\Theta_i(x_{1,i},x_{2,i})=\begin{cases} 1+q^{\frac{d_2}{2}} & \text{if } Tg_2 \nmid s_{2,i};\\ 1-q^{\frac{d_2}{2}}(Tg_2-1-Tg_2q^{\frac{d_1}{2}}(N-1)) & \text{if } Tg_2 \mid s_{2,i} \ \&\ N \mid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T};\\ 1-q^{\frac{d_2}{2}}(Tg_2-1+Tg_2q^{\frac{d_1}{2}}) & \text{if } Tg_2 \mid s_{2,i} \ \&\ N \nmid \frac{s_{2,i}}{Tg_2}+\frac{Bs_{1,i}}{T} \end{cases}$$

when N is even and both the integers $\frac{p\gamma_2(p^{t_2}+1)}{TNg_2}, \frac{p\nu'(p^{s'}+1)}{N}$ are odd. Working in a similar manner as above, one can also determine explicit values of the sum $\Theta_i(x_{1,i},x_{2,i})$ in the remaining cases.

□

In the following theorem, we determine the Hamming weight $W_H(c_i(x_1,x_2))$ when $M_1=2$ and $M_2\geq 3$ with either $O(\phi_1^{\Delta_1K_2})=1$ or $O(\phi_1^{\Delta_1K_2})=2$.

Theorem 5.2.9. *Let $M_1=2$, $M_2\geq 3$, $x_{1,i}=\xi_1^{s_{1,i}}\in\mathbb{F}_{q^{d_1}}^*$ and $x_{2,i}=\xi_2^{s_{2,i}}\in\mathbb{F}_{q^{d_2}}^*$, where $0\leq s_{1,i}\leq q^{d_1}-2$ and $0\leq s_{2,i}\leq q^{d_2}-2$. Suppose that either $O(\phi_1^{\Delta_1K_2})=1$ or $O(\phi_1^{\Delta_1K_2})=2$. Then p is an odd prime, the integer rd_1 is even and the following hold.*

- *If M_2 is even and $\frac{\gamma_2(p^{t_2}+1)}{M_2}$ is odd, then we have*

$$W_H(c_i(x_1,x_2))=\begin{cases} \frac{m_i(q-1)}{q}+\frac{m_i(q-1)\left(-1+q^{\frac{d_2}{2}}(M_2-1)\right)\left(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad\qquad \text{if } M_2 \mid s_{2,i}+\frac{M_2}{2};\\ \frac{m_i(q-1)}{q}-\frac{m_i(q-1)(1+q^{\frac{d_2}{2}})\left(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad\qquad \text{if } M_2 \nmid s_{2,i}+\frac{M_2}{2}. \end{cases}$$

- *If either M_2 is odd or $\frac{\gamma_2(p^{t_2}+1)}{M_2}$ is even, then we have*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} + \frac{m_i(q-1)\left(-1+(-1)^{\gamma_2-1}q^{\frac{d_2}{2}}(M_2-1)\right)\left(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_2 \mid s_{2,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_2-1}q^{\frac{d_2}{2}}\right)\left(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} \\ \qquad\qquad \text{if } M_2 \nmid s_{2,i}. \end{cases}$$

Proof. To determine the Hamming weight $W_H(c_i(x_1,x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\begin{aligned} \Theta_i(x_{1,i},x_{2,i}) &= \sum_{z_2=0}^{M_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})\Big(G(\overline{\phi}_1^{\Delta_1 z_2 K_2},\chi_1)\phi_1^{\Delta_1 z_2 K_2}(x_{1,i}) \\ &\quad + G(\overline{\phi}_1^{\Delta_1(z_2K_2+K_1)},\chi_1)\phi_1^{\Delta_1(z_2K_2+K_1)}(x_{1,i})\Big) \end{aligned} \tag{5.38}$$

Since $O(\phi_1^{\Delta_1 K_1}) = M_1 = 2$, we note that $\phi_1^{\Delta_1 K_1}$ is a quadratic character of $\mathbb{F}_{q^{d_1}}$, q is odd and the integer d_1 is even. Further, by Theorem 2.2.1, equation (5.38) can be rewritten as

$$\Theta_i(x_{1,i},x_{2,i}) = \Big(-1+\sum_{z_2=1}^{M_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})\Big)\times\Big(-1-\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\Big). \tag{5.39}$$

Next when M_2 is even and $\frac{p\gamma_2(p^{t_2}+1)}{M_2}$ is odd, by (5.31), we see that

$$\begin{aligned} \sum_{z_2=1}^{M_2-1} G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) &= q^{\frac{d_2}{2}}\sum_{z_2=1}^{M_2-1}(-1)^{z_2}\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) \\ &= q^{\frac{d_2}{2}}\sum_{z_2=1}^{M_2-1} e^{\frac{2\pi\iota z_2}{M_2}\left(s_{2,i}+\frac{M_2}{2}\right)} \\ &= \begin{cases} q^{\frac{d_2}{2}}(M_2-1) & \text{if } M_2 \mid s_{2,i}+\frac{M_2}{2}; \\ -q^{\frac{d_2}{2}} & \text{if } M_2 \nmid s_{2,i}+\frac{M_2}{2}. \end{cases} \end{aligned}$$

This, by (5.39), implies that

$$\Theta_i(x_{1,i},x_{2,i})=\begin{cases} -(-1+q^{\frac{d_2}{2}}(M_2-1))\big(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\big) & \text{if } M_2 \mid s_{2,i}+\frac{M_2}{2};\\ (1+q^{\frac{d_2}{2}})\big(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\big) & \text{if } M_2 \nmid s_{2,i}+\frac{M_2}{2}.\end{cases}$$

On the other hand, when either M_2 is odd or $\frac{p\gamma_2(p^{t_2}+1)}{M_2}$ is even, we see, by (5.31), that

$$\begin{aligned}\sum_{z_2=1}^{M_2-1} G(\overline{\phi_2}^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}},\chi_2)\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) &= (-1)^{\gamma_2-1}q^{\frac{d_2}{2}}\sum_{z_2=1}^{M_2-1} e^{\frac{2\pi\iota z_2 s_{2,i}}{M_2}}\\ &= \begin{cases}(-1)^{\gamma_2-1}q^{\frac{d_2}{2}}(M_2-1) & \text{if } M_2\mid s_{2,i};\\ -(-1)^{\gamma_2-1}q^{\frac{d_2}{2}} & \text{if } M_2\nmid s_{2,i}.\end{cases}\end{aligned}$$

This, by (5.39), implies that

$$\Theta_i(x_{1,i},x_{2,i})=\begin{cases} -(-1+(-1)^{\gamma_2-1}q^{\frac{d_2}{2}}(M_2-1))\big(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\big) & \text{if } M_2 \mid s_{2,i};\\ (1+(-1)^{\gamma_2-1}q^{\frac{d_2}{2}})\big(1+\iota^{\frac{rd_1(p-1)^2}{4}}(-1)^{s_{1,i}}q^{\frac{d_1}{2}}\big) & \text{if } M_2 \nmid s_{2,i}.\end{cases}$$

□

Now we proceed to determine the Hamming weight $W_H(c_i(\delta_1,\delta_2)$ when both $M_1,M_2\geq 3$. To do this, we see, by Lemma 5.2.3, that we need to determine explicit values of the Gauss sums $G(\phi_1^{\Delta_1 j},\chi_1)$, where $1\leq j<(q^d-1)g_1$. Towards this, we note that $O(\phi_1^{\Delta_1})=(q^d-1)g_1\geq 3$. Now by Theorem 2.2.2, we see that the explicit values of the Gauss sums $G(\phi_1^{\Delta_1 j},\chi_1)$, $1\leq j<(q^d-1)g_1$, are known in the semi-primitive case, i.e., when there exists a least positive integer t_1 satisfying $p^{t_1}\equiv -1 \pmod{(q^d-1)g_1}$. In the semi-primitive case, by Theorem 2.2.2, we see that the integer rd_1 must be even. We also recall that there exists a least positive integer t_2 satisfying $p^{t_2}\equiv -1 \pmod{M_2}$, which gives $rd_2=2t_2\gamma_2$ for some positive integer γ_2. That is, the integer rd_2 is also even. This implies that the integer $rd=\gcd(rd_1,rd_2)$ is even. As $q^d-1=1$ or 2 implies that $rd=1$, we must have $q^d-1\geq 3$. Since we

have $p^{t_1} \equiv -1 \pmod{(q^d-1)g_1}$, there exists a least positive integer f satisfying $p^f \equiv -1 \pmod{q^d-1}$. This, by Theorem 11.6.2 of [11], implies that $rd = 2f$. This further implies that $q^d-1 = p^{rd}-1 = (p^f+1)(p^f-1)$, which gives $\left(\frac{p^f+1}{q^d-1}\right)(p^f-1) = 1$. From this, we get $p^f-1 = 1$, which holds if and only if $f = 1,\ p = 2$ and $rd = 2$. Therefore in the semi-primitive case, we must have $q = 2$ or 4. In the following theorem, we determine the Hamming weight $W_H(c_i(x_1, x_2))$ when $M_1 \geq 3$ and $M_2 \geq 3$ in the semi-primitive case.

Theorem 5.2.10. *Let $M_1 \geq 3$, $M_2 \geq 3$, $x_{1,i} = \xi_1^{s_{1,i}} \in \mathbb{F}_{q^{d_1}}^*$ and $x_{2,i} = \xi_2^{s_{2,i}} \in \mathbb{F}_{q^{d_2}}^*$, where $0 \leq s_{1,i} \leq q^{d_1}-2$ and $0 \leq s_{2,i} \leq q^{d_2}-2$. Suppose that there exist least positive integers t_1 and t_2 satisfying $p^{t_1} \equiv -1 \pmod{(q^d-1)g_1}$ and $p^{t_2} \equiv -1 \pmod{M_2}$. Then we have $q = 2$ or 4. Furthermore, we have $rd_1 = 2t_1\gamma_1$, $rd_2 = 2t_2\gamma_2$ for some positive integers γ_1, γ_2, and*

$$W_H(c_i(x_1,x_2)) = \begin{cases} \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(-1)^{\gamma_1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \text{if } M_1 \nmid s_{1,i}; \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_1}q^{\frac{d_1}{2}}\left((M_1-1)+(-1)^{\gamma_2}q^{\frac{d_2}{2}}M_1(M_2-1)\right)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad \text{if } M_1 \mid s_{1,i} \ \&\ M_2 \mid s_{2,i} + \frac{\lambda' g_2 H K_2 s_{1,i}}{G\lambda g_1}; & \\ \frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1+(-1)^{\gamma_1}q^{\frac{d_1}{2}}\left((M_1-1)-(-1)^{\gamma_2}q^{\frac{d_2}{2}}M_1\right)\right)}{q(q^{d_1}-1)(q^{d_2}-1)} & \\ \qquad \text{if } M_1 \mid s_{1,i} \ \&\ M_2 \nmid s_{2,i} + \frac{\lambda' g_2 H K_2 s_{1,i}}{G\lambda g_1}. & \end{cases}$$

Proof. To determine the Hamming weight $W_H(c_i(x_1, x_2))$, we see, by (5.9) and (5.10), that it is enough to determine the explicit value of the sum

$$\begin{aligned} \Theta_i(x_{1,i}, x_{2,i}) \ = \ & 1 - \sum_{z_1=1}^{M_1-1} G(\overline{\phi}_1^{\Delta_1 K_1 z_1}, \chi_1)\phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) + \sum_{z_2=1}^{M_2-1}\sum_{z_1=0}^{M_1-1}\Big(G(\overline{\phi}_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}, \chi_2) \\ & \phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})G(\overline{\phi}_1^{\Delta_1(K_2 z_2 + K_1 z_1)}, \chi_1)\phi_1^{\Delta_1(K_2 z_2 + K_1 z_1)}(x_{1,i})\Big). \end{aligned} \tag{5.40}$$

Further, for $1 \leq v \leq (q^d-1)g_1 - 1$, by Theorem 2.2.2, we see that

$$G(\overline{\phi}_1^{\Delta_1 v}, \chi_1) = (-1)^{\gamma_1 - 1} q^{\frac{d_1}{2}}.$$

From this and by (5.31), equation (5.40) can be rewritten as

$$\begin{aligned}
\Theta_i(x_{1,i}, x_{2,i}) &= 1 - \sum_{z_1=1}^{M_1-1} (-1)^{\gamma_1-1} q^{\frac{d_1}{2}} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) \\
&\quad + \sum_{z_2=1}^{M_2-1} \sum_{z_1=0}^{M_1-1} (-1)^{\gamma_2-1} q^{\frac{d_2}{2}} \phi_2^{\frac{\Delta_2 G \lambda z_2}{H\lambda'}}(x_{2,i}) (-1)^{\gamma_1-1} q^{\frac{d_1}{2}} \phi_1^{\Delta_1(K_2 z_2 + K_1 z_1)}(x_{1,i}) \\
&= 1 - q^{\frac{d_1}{2}} (-1)^{\gamma_1-1} X(x_{1,i}) + (-1)^{\gamma_1+\gamma_2} q^{\frac{(d_1+d_2)}{2}} Y(x_{1,i}, x_{2,i}), \qquad (5.41)
\end{aligned}$$

where

$$X(x_{1,i}) = \sum_{z_1=1}^{M_1-1} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i})$$

and

$$Y(x_{1,i}, x_{2,i}) = \Big(1 + X(x_{1,i})\Big)\Big(\sum_{z_2=1}^{M_2-1} \phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i}) \phi_1^{\Delta_1 K_2 z_2}(x_{1,i})\Big).$$

Next we see that

$$\begin{aligned}
\lambda' g_2 H K_2 &= \lambda' g_2 H \Big(- \frac{\lambda \tau \ell_2}{\lambda' g_2 H} \Big(1 - \frac{(q^d-1)\tau' \Delta_1}{G\lambda}\Big) - \frac{(q-1)\tau' \Delta_2 G L}{G\lambda' H}\Big) \\
&= -\tau \ell_2 \lambda \Big(1 - \frac{(q^d-1)\tau'\Delta_1}{G\lambda}\Big) - \tau'(q^{d_2}-1)L.
\end{aligned}$$

Further, since $\frac{q-1}{\lambda}$ divides $1 - \frac{(q^d-1)\tau'\Delta_1}{G\lambda}$ and $q-1$ divides $q^{d_2}-1$, we note that $\frac{\lambda' g_2 H K_2}{q-1}$ is an integer. Next we observe that

$$X(x_{1,i}) = \sum_{z_1=1}^{M_1-1} \phi_1^{\Delta_1 K_1 z_1}(x_{1,i}) = \sum_{z_1=1}^{M_1-1} e^{\frac{2\pi \iota s_{1,i} z_1}{M_1}} = \begin{cases} M_1 - 1 & \text{if } M_1 \mid s_{1,i}; \\ -1 & \text{otherwise.} \end{cases}$$

and

$$\begin{aligned}\sum_{z_2=1}^{M_2-1}\phi_2^{\frac{\Delta_2 G\lambda z_2}{H\lambda'}}(x_{2,i})\phi_1^{\Delta_1 K_2 z_2}(x_{1,i}) &= \sum_{z_2=1}^{M_2-1} e^{\frac{2\pi\iota z_2 s_{2,i}}{M_2}+\frac{2\pi\iota(q^{d_1}-1)K_2 z_2 s_{1,i}}{(q^d-1)(q^{d_1}-1)g_1}}\\ &= \sum_{z_2=1}^{M_2-1} e^{\frac{2\pi\iota z_2}{M_2}\left(s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1}\right)}\\ &= \begin{cases} M_2-1 & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \mid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1};\\ -1 & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \nmid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1}.\end{cases}\end{aligned}$$

From this, it follows that

$$Y(x_{1,i},x_{2,i}) = \begin{cases} M_1(M_2-1) & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \mid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1};\\ -M_1 & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \nmid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1};\\ 0 & \text{if } M_1 \nmid s_{1,i}.\end{cases}$$

Now on substituting the values of $X(x_{1,i})$ and $Y(x_{1,i},x_{2,i})$ in equation (5.41), we obtain

$$\Theta_i(x_{1,i},x_{2,i}) = \begin{cases} 1-(-1)^{\gamma_1}q^{\frac{d_1}{2}} & \text{if } M_1 \nmid s_{1,i};\\ 1+(-1)^{\gamma_1}q^{\frac{d_1}{2}}(M_1-1)+(-1)^{\gamma_1+\gamma_2}q^{\frac{(d_1+d_2)}{2}}M_1(M_2-1) & \\ & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \mid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1};\\ 1+(-1)^{\gamma_1}q^{\frac{d_1}{2}}(M_1-1)-(-1)^{\gamma_1+\gamma_2}q^{\frac{(d_1+d_2)}{2}}M_1 & \\ & \text{if } M_1 \mid s_{1,i} \text{ and } M_2 \nmid s_{2,i}+\frac{\lambda' g_2 HK_2 s_{1,i}}{G\lambda g_1}.\end{cases}$$

□

Remark 5.2.11. *By applying Theorems 5.2.2-5.2.10 and by* (5.4)*, one can determine all non-zero Hamming weights in some* Λ*-MT codes with at most two non-zero constituents, which we demonstrate in the following section by computing Hamming weight distributions of several classes of MT codes.*

5.3 Some applications

In this section, we will explicitly determine Hamming weight distributions of some classes of MT codes with at most two non-zero constituents. Using these results, we further identify two classes of optimal equidistant linear codes and several other classes of minimal linear codes within these classes of MT codes. Recall that the support of a vector $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_q^n$, denoted by $\mathrm{supp}(v)$, is defined as the set $\mathrm{supp}(v) = \{i : 0 \leq i \leq n-1, v_i \neq 0\}$. Further, a vector $u \in \mathbb{F}_q^n$ is said to cover another vector $v \in \mathbb{F}_q^n$ if $\mathrm{supp}(v) \subseteq \mathrm{supp}(u)$. A codeword $c \in \mathcal{C}$ is said to be minimal if c covers only the codewords $ac \in \mathcal{C}$ for all $a \in \mathbb{F}_q$, and c does not cover any other codeword of the code $\mathcal{C}$. The linear code $\mathcal{C}$ is said to be minimal if every codeword of $\mathcal{C}$ is minimal.

Next we first state a sufficient condition for a linear code over a finite field to be minimal, which was derived by Ashikhmin and Barg [1].

Lemma 5.3.1. *[1] A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is minimal if it satisfies*

$$\frac{W_{min}}{W_{max}} > \frac{q-1}{q}, \tag{5.42}$$

where W_{min} and W_{max} denote the minimum and the maximum among the Hamming weights of non-zero codewords of the code $\mathcal{C}$, respectively.

In view of the above lemma, we see that all equidistant linear codes over finite fields satisfy the inequality (5.42), and hence are minimal linear codes. It has been shown that minimal linear codes are useful in constructing secret sharing schemes with nice access structures [19, 23, 54, 60, 80] and in secure two-party computation [2, 22]. In addition, these codes can be effectively decoded with a minimum distance decoding algorithm [1].

Throughout this section, let $\mathscr{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathscr{C}_1 = \langle F_1 \rangle \subseteq \mathcal{G}_1$, $\mathscr{C}_2 = \langle F_2 \rangle \subseteq \mathcal{G}_2$ and $\mathscr{C}_3 = \cdots = \mathscr{C}_\rho = \{0\}$, where $F_1 = (F_{1,1}, F_{1,2}, \cdots, F_{1,\ell}) \in \mathcal{G}_1$ and $F_2 = (F_{2,1}, F_{2,2}, \cdots, F_{2,\ell}) \in \mathcal{G}_2$. Further, let us

define the sets $Z_1 = \{1 \leq i \leq \ell : F_{1,i} \neq 0\}, Z_2 = \{1 \leq i \leq \ell : F_{2,i} \neq 0\}, Z_3 = \{1 \leq i \leq \ell : F_{1,i} \neq 0 \text{ and } F_{2,i} = 0\}, Z_4 = \{1 \leq i \leq \ell : F_{1,i} = 0 \text{ and } F_{2,i} \neq 0\}$ and $Z_5 = \{1 \leq i \leq \ell : F_{1,i} \neq 0 \text{ and } F_{2,i} \neq 0\}$. We also recall that $M_1 = \frac{G\lambda g_1}{q-1}$, $M_2 = \frac{(q^d-1)\lambda' g_2 H}{G\lambda}$, $g_w = \gcd\left(\frac{q^{dw}-1}{q^d-1}, \ell_w\right)$ and $\tau_w = \gcd\left(\frac{q^{dw}-1}{q-1}, \ell_w\right)$ for $1 \leq w \leq 2$.

In the following result, we state the Griesmer and Plotkin bounds for a linear code over $\mathbb{F}_q$.

Theorem 5.3.2. *[44] Let $\mathcal{C}$ be a linear code of length n, dimension k and Hamming distance d over $\mathbb{F}_q$.*

(a) (Griesmer bound) The parameters $[n, k, d]$ of the code $\mathcal{C}$ satisfy $n \geq \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil$.

(b) (Plotkin bound) The parameters $[n, k, d]$ of the code $\mathcal{C}$ satisfy $q^k \leq \left\lfloor \frac{qd}{qd-n(q-1)} \right\rfloor$ provided $qd > n(q-1)$.

In the following theorem, we obtain a class of equidistant optimal Λ-MT codes that attain Griesmer and Plotkin bounds.

Theorem 5.3.3. *If $\tau_1 = 1$, $F_1 \neq 0$ and $F_2 = 0$, then the Λ-MT code $\mathscr{C}$ is an equidistant code of length n over $\mathbb{F}_q$ with the only non-zero Hamming weight as $\sum_{i \in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$. In particular, if $Z_1 = \{1, 2, \cdots, \ell\}$, then the code $\mathscr{C}$ has parameters $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and is an optimal code that attains both the Griesmer and Plotkin bounds.*

Proof. Since $\tau_1 = 1$, by (5.4) and by applying Theorem 5.2.2(a), we see that each non-zero codeword of $\mathscr{C}$ has Hamming weight $\sum_{i \in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$. Further, for each $i \in Z_1$, since $\xi_1^{\ell_1 m_i} = \delta_1^{-m_i} = \lambda_i^{-1}$, we see that $\xi_1^{\ell_1 m_i (q-1)} = 1$, which implies that $\frac{q^{d_1}-1}{q-1} \mid m_i$. Now when $Z_1 = \{1, 2, \cdots, \ell\}$, one can easily see that the code $\mathscr{C}$ has parameters $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and attains both the Griesmer and Plotkin bounds. □

From this point on, in Tables 5.1-5.9, we assume that $A_0 = 1$ and $A_j = 0$ for all other non-zero Hamming weights j's. In the following theorem, we obtain another class of equidistant optimal Λ-MT codes, which attain Griesmer and Plotkin bounds.

Hamming weight j	Frequency A_j
$\sum_{i\in S_1} \frac{m_i(q-1)\left(q^{d_1}+\iota\frac{rd_1(p-1)^2}{4}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in S_2} \frac{m_i(q-1)\left(q^{d_1}-\iota\frac{rd_1(p-1)^2}{4}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in S_1} \frac{m_i(q-1)\left(q^{d_1}-\iota\frac{rd_1(p-1)^2}{4}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in S_2} \frac{m_i(q-1)\left(q^{d_1}+\iota\frac{rd_1(p-1)^2}{4}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$

Table 5.1: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.4

Theorem 5.3.4. *Let $F_1 \neq 0$ and $F_2 = 0$. If $S_1 = \{i \in Z_1 : F_{1,i}$ is a square in $\mathbb{F}_{q^{d_1}}\}$, $S_2 = \{i \in Z_1 : F_{1,i}$ is a non-square in $\mathbb{F}_{q^{d_1}}\}$ and $\tau_1 = 2$, then the Λ-MT code $\mathscr{C}$ has at most two non-zero Hamming weights and its Hamming weight distribution is given by Table 5.1. In particular, let $Z_1 = \{1, 2, \cdots, \ell\}$ and $m_1 = m_2 = \cdots = m_\ell$ so that $n = m_1\ell$. Now if ℓ is even and $|S_1| = |S_2| = \frac{\ell}{2}$, then the code $\mathscr{C}$ has parameters $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and is an optimal equidistant code that attains Griesmer and Plotkin bounds.*

Proof. By applying Theorem 5.2.2(b) and working in a similar manner as in Theorem 5.3.3, the desired result follows immediately. □

In the following theorems, we identify some more classes of few weight Λ-MT codes.

Theorem 5.3.5. *Let $\tau_1 \geq 3$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = 0$. Suppose that there exists a least positive integer s_1 satisfying $p^{s_1} \equiv -1 \pmod{\tau_1}$. Then we have $rd_1 = 2\nu_1 s_1$ for some positive integer ν_1. The Λ-MT code $\mathscr{C}$ is a 2-weight code of length n over $\mathbb{F}_q$, whose Hamming weight distribution is given by Table 5.2. Furthermore, if ν_1 is odd, then the Λ-MT code $\mathscr{C}$ is minimal when $q^{\frac{d_1}{2}} - q\tau_1 + 1 > 0$, while if ν_1 is even, then the Λ-MT code $\mathscr{C}$ is minimal when $q^{\frac{d_1}{2}} - q\tau_1 + \tau_1 - 1 > 0$.*

Proof. It follows immediately from (5.4) and by applying Theorem 5.2.2(c). □

Theorem 5.3.6. *If $M_1 = M_2 = 1$, then the Λ-MT code $\mathscr{C}$ has at most three non-zero Hamming weights and its Hamming weight distribution is given by Table 5.3.*

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)\left(q^{d_1}-(-1)^{\nu_1-1}q^{\frac{d_1}{2}}(\tau_1-1)\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{\tau_1}$
$\sum_{i\in Z_1} \frac{m_i(q-1)\left(q^{d_1}+(-1)^{\nu_1-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{(q^{d_1}-1)(\tau_1-1)}{\tau_1}$

Table 5.2: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.5

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}+\sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}+\sum_{i\in Z_5} \frac{m_i(q-1)((q^{d_1}-1)(q^{d_2}-1)-1)}{q(q^{d_1}-1)(q^{d_2}-1)}$	$(q^{d_1}-1)(q^{d_2}-1)$

Table 5.3: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.6

Proof. Here it is easy to see that $\tau_1 = g_1 = \tau_2 = g_2 = 1$. Now the desired result follows by equation (5.4) and by applying Theorems 5.2.2(a) and 5.2.4(a). □

Theorem 5.3.7. *If $M_1 = 2$, $M_2 = 1$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = (\epsilon_{2,1}, \epsilon_{2,2}, \cdots, \epsilon_{2,\ell})$, then the Λ-MT code $\mathscr{C}$ has at most five non-zero Hamming weights and its Hamming weight distribution is given by Table 5.4.*

Proof. Here one can easily observe that $\tau_1 = g_1 = 2$ and $\tau_2 = g_2 = 1$. Now the desired result follows by equation (5.4) and by applying Theorems 5.2.2(a), 5.2.2(b) and 5.2.4(b). □

Theorem 5.3.8. *Let $M_1 \geq 3$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = (\epsilon_{2,1}, \epsilon_{2,2}, \cdots, \epsilon_{2,\ell})$. Suppose that there exists a least positive integer t satisfying $p^t \equiv -1 \pmod{M_1}$. Then we have $rd_1 = 2t\gamma$ for some positive integer γ. Furthermore, if $\tau_1 = \tau_2 = M_2 = 1$, then the Λ-MT code $\mathscr{C}$ has at most four non-zero Hamming weights and its Hamming weight distribution is given by Table 5.5.*

Proof. The desired result follows by (5.4) and by applying Theorems 5.2.2(a) and 5.2.4(c). □

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in Z_1} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in Z_3} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$
$\sum_{i\in Z_3} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$

Table 5.4: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.7

Theorem 5.3.9. *If $M_1 = 1$, $M_2 = g_2 = 2$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = (\epsilon_{2,1}, \epsilon_{2,2}, \cdots, \epsilon_{2,\ell})$, then the Λ-MT code $\mathscr{C}$ has at most five non-zero Hamming weights and its Hamming weight distribution is given by Table 5.6.*

Proof. Here one can easily see that $\tau_2 = g_2 = 2$ and $g_1 = \tau_1 = 1$. Now the desired result follows by (5.4) and by applying Theorems 5.2.2(a), 5.2.2(b) and 5.2.5(a). □

Theorem 5.3.10. *If $M_1 = g_2 = 1$, $M_2 = 2$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = (\epsilon_{2,1}, \epsilon_{2,2}, \cdots, \epsilon_{2,\ell})$, then the Λ-MT code $\mathscr{C}$ has at most four non-zero Hamming weights and its Hamming weight distribution is given by Table 5.7.*

Proof. Here we note that $\tau_2 = g_2 = g_1 = \tau_1 = 1$. Now the desired result follows by (5.4) and by applying Theorems 5.2.2(a) and 5.2.5(b). □

Theorem 5.3.11. *If $F_1 \neq 0, F_2 \neq 0, \tau_1 = \tau_2 = 1$ and Z_5 is the empty set, then the Λ-MT code $\mathscr{C}$ has at most three non-zero Hamming weights and its Hamming weight distribution is given by Table 5.8.*

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)\left(1-(M_1-1)(-1)^{\gamma-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{M_1}$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+(-1)^{\gamma-1}q^{\frac{d_1}{2}})}{q(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)(M_1-1)}{M_1}$

Table 5.5: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.8

Proof. It follows immediately by (5.4) and by applying Theorem 5.2.2(a). □

Remark 5.3.12. *Working in a similar manner as in Sections 5.2 and 5.3, one can also determine Hamming weight distributions of several classes of MT codes with more than two non-zero constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$, all of whose codewords $(\delta_{w,1}, \delta_{w,2}, \cdots, \delta_{w,\ell}) \in \mathcal{C}_w$ satisfy the following condition:*

For $1 \le i \le \ell$, there exist integers a_i, b_i such that $1 \le a_i < b_i \le \rho$ and $x_{w,i} = 0$ for

$$1 \le w(\neq a_i, b_i) \le \rho. \qquad (*)$$

In the following theorem, we determine Hamming weight distributions of a class of MT codes with three non-zero constituents whose codewords satisfy the condition $(*)$.

Theorem 5.3.13. *Let $\mathscr{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathscr{C}_1 = \langle(1,1,0,\cdots,0)\rangle \subseteq \mathcal{G}_1$, $\mathscr{C}_2 = \langle(0,0,1,1,0,\cdots,0)\rangle \subseteq \mathcal{G}_2$, $\mathscr{C}_3 = \langle(0,0,0,0,1,\cdots \cdots,1)\rangle \subseteq \mathcal{G}_3$ and $\mathscr{C}_4 = \cdots = \mathscr{C}_\rho = \{0\}$. Let $\mathbb{F}^*_{q^{d_3}} = \langle\xi_3\rangle$ and $\tau_3 = \gcd\left(\frac{q^{d_3}-1}{q-1}, \ell_3\right)$, where $\delta_3^{-1} = \xi_3^{\ell_3}$ for some integer ℓ_3 satisfying $0 \le \ell_3 \le q^{d_3}-2$. If $\tau_1 = \tau_2 = \tau_3 = 1$, then the Λ-MT code $\mathscr{C}$ has at most seven non-zero Hamming weights and its Hamming weight distribution is given by Table 5.9.*

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in Z_2} \frac{m_i(q-1)\left(q^{d_2}+\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}}\right)}{q(q^{d_2}-1)}$	$\frac{q^{d_2}-1}{2}$
$\sum_{i\in Z_2} \frac{m_i(q-1)\left(q^{d_2}-\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}}\right)}{q(q^{d_2}-1)}$	$\frac{q^{d_2}-1}{2}$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)\left(q^{d_2}+\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}}\right)}{q(q^{d_2}-1)}$ $+ \sum_{i\in Z_5} \frac{m_i(q-1)}{q}\left(1 - \frac{\left(1+\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)\left(q^{d_2}-\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_2}{2}}\right)}{q(q^{d_2}-1)}$ $+ \sum_{i\in Z_5} \frac{m_i(q-1)}{q}\left(1 - \frac{\left(1-\iota^{\frac{rd_2(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{(q^{d_1}-1)(q^{d_2}-1)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$

Table 5.6: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.9

Hamming weight j	FrequencyA_j
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)}{q(q^{d_1}-1)(q^{d_2}-1)}\left(1+\iota^{\frac{r(d_1+d_2)(p-1)^2}{4}} q^{\frac{(d_1+d_2)}{2}}\right)\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$
$\sum_{i\in Z_3} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_4} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$ $+ \sum_{i\in Z_5} \left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)}{q(q^{d_1}-1)(q^{d_2}-1)}\left(1-\iota^{\frac{r(d_1+d_2)(p-1)^2}{4}} q^{\frac{(d_1+d_2)}{2}}\right)\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$

Table 5.7: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.10

Hamming weight j	Frequency A_j
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in Z_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in Z_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$(q^{d_1}-1)(q^{d_2}-1)$

Table 5.8: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.11

Hamming weight j	Frequency A_j
$\frac{(m_1+m_2)(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\frac{(m_3+m_4)(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\frac{(m_5+\cdots+m_\ell)(q-1)q^{d_3-1}}{q^{d_3}-1}$	$q^{d_3}-1$
$\frac{(m_1+m_2)(q-1)q^{d_1-1}}{q^{d_1}-1}+\frac{(m_3+m_4)(q-1)q^{d_2-1}}{q^{d_2}-1}$	$(q^{d_1}-1)(q^{d_2}-1)$
$\frac{(m_1+m_2)(q-1)q^{d_1-1}}{q^{d_1}-1}+\frac{(m_5+\cdots+m_\ell)(q-1)q^{d_3-1}}{q^{d_3}-1}$	$(q^{d_1}-1)(q^{d_3}-1)$
$\frac{(m_3+m_4)(q-1)q^{d_2-1}}{q^{d_2}-1}+\frac{(m_5+\cdots+m_\ell)(q-1)q^{d_3-1}}{q^{d_3}-1}$	$(q^{d_2}-1)(q^{d_3}-1)$
$\frac{(m_1+m_2)(q-1)q^{d_1-1}}{q^{d_1}-1}+\frac{(m_3+m_4)(q-1)q^{d_2-1}}{q^{d_2}-1}+\frac{(m_5+\cdots+m_\ell)(q-1)q^{d_3-1}}{q^{d_3}-1}$	$(q^{d_1}-1)(q^{d_2}-1)(q^{d_3}-1)$

Table 5.9: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 5.3.13

Proof. By applying Theorem 3.5.2 and by working in a similar manner as in Theorem 5.2.2(a), the desired result follows. □

6

A generalization of multi-twisted codes over finite fields, their Galois duals and Type II codes

6.1 Introduction

In Chapters 3-5, we studied MT codes over $\mathbb{F}_q$, whose block lengths are positive integers coprime to q. In this chapter, we shall extend this family of codes and study MT codes over $\mathbb{F}_q$, whose block lengths are arbitrary positive integers not necessarily coprime to q. To do this, we assume, throughout this chapter, that $q = p^r$, where

p is a prime number and r is a positive integer. Let $m_1, m_2, \cdots, m_\ell$ be arbitrary positive integers (not necessarily coprime to q), and let $n = m_1 + m_2 + \cdots + m_\ell$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$.

In this chapter, we shall study algebraic structures of Λ-multi-twisted (MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and their Galois duals (i.e., their orthogonal complements with respect to the Galois inner product on $\mathbb{F}_q^n$). We shall derive necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois linear with complementary dual (LCD). We shall also provide a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by using the generalized discrete Fourier transform (GDFT), which gives rise to a method to construct these codes. We shall further provide necessary and sufficient conditions under which a Euclidean self-dual Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_{2^r}$ is a Type II code when $\lambda_i = 1$ and $m_i = n_i 2^a$ for $1 \leq i \leq \ell$, where $a \geq 0$ is an integer and $n_1, n_2, \cdots, n_\ell$ are odd positive integers satisfying $n_1 \equiv n_2 \equiv \cdots \equiv n_\ell \pmod 4$. We shall also develop generator theory for Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and show that each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ has a unique normalized generating set. With the help of a normalized generating set, we shall explicitly determine the dimension and a generating set of the Galois dual of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$. Besides this, we shall obtain several linear codes with best-known and optimal parameters from 1-generator Λ-MT codes over $\mathbb{F}_q$, where $2 \leq q \leq 7$.

This chapter is organized as follows: In Section 6.2, we study Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and their dual codes with respect to the Galois inner product on $\mathbb{F}_q^n$ (Theorems 6.2.2-6.2.6). We also derive necessary and sufficient conditions for a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ to be (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois

linear with complementary-dual (LCD) (Theorem 6.2.8). In Section 6.3, we provide a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ by using the generalized discrete Fourier transform (GDFT), which gives rise to a construction method for these codes (Theorem 6.3.2). In Section 6.4, we derive necessary and sufficient conditions for a Euclidean self-dual Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_{2^r}$ to be a Type II code when $\lambda_i = 1$ and $m_i = n_i 2^a$ for $1 \leq i \leq \ell$, where $a \geq 0$ is an integer and $n_1, n_2, \cdots, n_\ell$ are odd positive integers satisfying $n_1 \equiv n_2 \equiv \cdots \equiv n_\ell \pmod 4$ (Theorem 6.4.4). In Section 6.5, we show that each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ has a unique normalized generating set (Theorem 6.5.3). We also explicitly determine the dimension and a generating set of the Galois dual of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ (Corollary 6.5.4 and Theorem 6.5.6). Besides this, we identify several linear codes with best-known and optimal parameters from 1-generator Λ-MT codes over $\mathbb{F}_q$, where $2 \leq q \leq 7$ (Tables 6.1 and 6.2). It is worth mentioning that these code parameters can not be attained by any of their subclasses (such as constacyclic and quasi-twisted codes) containing record breaker codes. This shows that this generalized family of MT codes over finite fields is more promising to find codes with better parameters than the current best-known codes.

6.2 MT codes over finite fields and their Galois duals

In Chapters 3-5, we studied MT codes over $\mathbb{F}_q$ whose block lengths are coprime to q. In this section, we shall extend the definition of MT codes, and we shall study MT codes over $\mathbb{F}_q$ whose block lengths are arbitrary positive integers (not necessarily coprime to q). To do this, we recall that $\mathbb{F}_q$ is the finite field of order $q = p^r$, where p is a prime and r is a positive integer. Here we have $n = m_1 + m_2 + \cdots + m_\ell$,

where $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers, not necessarily coprime to q. For $1 \leq i \leq \ell$, let us write

$$m_i = n_i p^{a_i}, \tag{6.1}$$

where $a_i \geq 0$ is an integer and n_i is a positive integer coprime to q. Let $\mathbb{F}_q^n$ denote the vector space consisting of all n-tuples over $\mathbb{F}_q$. We also recall that $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. For $1 \leq i \leq \ell$, one can show that there exists a non-zero element $\alpha_i \in \mathbb{F}_q$ such that $\lambda_i = \alpha_i^{p^{a_i}}$, which implies that $x^{m_i} - \lambda_i = (x^{n_i} - \alpha_i)^{p^{a_i}}$ in $\mathbb{F}_q[x]$. Now a Λ-multi-twisted (MT) module V is an $\mathbb{F}_q[x]$-module of the form $V = \prod_{i=1}^{\ell} V_i$, where $V_i = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \lambda_i \rangle} = \frac{\mathbb{F}_q[x]}{\langle (x^{n_i} - \alpha_i)^{p^{a_i}} \rangle}$ for $1 \leq i \leq \ell$. From this point on, we shall represent each element $c \in \mathbb{F}_q^n$ as $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots, c_{\ell,m_\ell-1})$ and the corresponding element $c(x) \in V$ as $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x))$, where $c_i(x) = \sum_{j=0}^{m_i-1} c_{i,j} x^j \in V_i$ for $1 \leq i \leq \ell$. Note that the map $c \mapsto c(x)$ is an $\mathbb{F}_q$-linear vector space isomorphism from $\mathbb{F}_q^n$ onto V.

Definition 6.2.1. *[5] A Λ-multi-twisted (Λ-MT) code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is defined as an $\mathbb{F}_q[x]$-submodule of the Λ-MT module V. Equivalently, a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called a Λ-MT code if $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots\cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots, c_{\ell,m_\ell-1})$ is a codeword of $\mathcal{C}$, then its Λ-MT shift $T_\Lambda(c) = (\lambda_1 c_{1,m_1-1}, c_{1,0}, \cdots, c_{1,m_1-2}; \lambda_2 c_{2,m_2-1}, c_{2,0}, \cdots, c_{2,m_2-2}; \cdots; \lambda_\ell c_{\ell,m_\ell-1}, c_{\ell,0}, \cdots, c_{\ell,m_\ell-2})$ is also a codeword of $\mathcal{C}$.*

Now let $g_1(x), g_2(x), \cdots, g_\rho(x)$ be all the distinct irreducible factors of the polynomials $x^{n_1} - \alpha_1, x^{n_2} - \alpha_2, \cdots, x^{n_\ell} - \alpha_\ell$ over $\mathbb{F}_q$. Further, for $1 \leq i \leq \ell$ and $1 \leq w \leq \rho$, let us define

$$\epsilon_{w,i} = \begin{cases} 1 & \text{if } g_w(x) \text{ divides } x^{n_i} - \alpha_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise.} \end{cases}$$

Therefore for $1 \leq i \leq \ell$, the irreducible factorization of the polynomial $x^{n_i} - \alpha_i$ over

$\mathbb{F}_q$ is given by

$$x^{n_i} - \alpha_i = g_1(x)^{\epsilon_{1,i}} g_2(x)^{\epsilon_{2,i}} \cdots g_\rho(x)^{\epsilon_{\rho,i}}, \tag{6.2}$$

which further implies that the irreducible factorization of the polynomial $x^{m_i} - \lambda_i$ over $\mathbb{F}_q$ is given by

$$x^{m_i} - \lambda_i = (x^{n_i} - \alpha_i)^{p^{a_i}} = g_1(x)^{\epsilon_{1,i}p^{a_i}} g_2(x)^{\epsilon_{2,i}p^{a_i}} \cdots g_\rho(x)^{\epsilon_{\rho,i}p^{a_i}}.$$

Next for each i, we see, by applying the Chinese Remainder Theorem, that

$$V_i \simeq \bigoplus_{w=1}^{\rho} \epsilon_{w,i} \frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_i}} \rangle},$$

where the ring isomorphism is given by $a_i(x) \mapsto \sum_{w=1}^{\rho} \epsilon_{w,i} \left(a_i(x) + \langle g_w(x)^{p^{a_i}} \rangle \right)$ for each $a_i(x) \in V_i$. This implies that

$$V = \prod_{i=1}^{\ell} V_i \simeq \bigoplus_{w=1}^{\rho} \Bigg(\underbrace{\epsilon_{w,1} \frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_1}} \rangle}, \epsilon_{w,2} \frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_2}} \rangle}, \cdots, \epsilon_{w,\ell} \frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_\ell}} \rangle}}_{\mathcal{G}_w} \Bigg), \tag{6.3}$$

and the corresponding ring isomorphism from V onto $\bigoplus_{w=1}^{\rho} \mathcal{G}_w$ is given by

$$c(x) \mapsto \sum_{w=1}^{\rho} \Big(\epsilon_{w,1}\big(c_1(x) + \langle g_w(x)^{p^{a_1}} \rangle\big), \epsilon_{w,2}\big(c_2(x) + \langle g_w(x)^{p^{a_2}} \rangle\big), \cdots, \epsilon_{w,\ell}\big(c_\ell(x) + \langle g_w(x)^{p^{a_\ell}} \rangle\big) \Big)$$

for each $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \in V$. Furthermore, for $1 \leq w \leq \rho$, let us define

$$\mathcal{S}_w = \left\{ \left(\alpha(x) + \langle g_w(x)^{p^{a_1}} \rangle, \alpha(x) + \langle g_w(x)^{p^{a_2}} \rangle, \cdots, \alpha(x) + \langle g_w(x)^{p^{a_\ell}} \rangle \right) : \alpha(x) \in \mathbb{F}_q[x] \right\}.$$

Here for each w, one can observe that the set $\mathcal{S}_w$ is a commutative ring with unity with respect to the component wise addition and the component wise multiplication,

and we shall view the set $\mathcal{G}_w = \left(\epsilon_{w,1}\frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_1}}\rangle}, \epsilon_{w,2}\frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_2}}\rangle}, \cdots, \epsilon_{w,\ell}\frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_\ell}}\rangle}\right)$ as an $\mathcal{S}_w$-module. In particular, when $a_1 = a_2 = \cdots = a_\ell$, the set $\mathcal{G}_w$ can also be viewed as a $\frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_1}}\rangle}$-module for each w. From the above discussion, we deduce the following:

Theorem 6.2.2. *(a) Each Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as*

$$\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w,$$

where $\mathcal{C}_w = \{\big(\epsilon_{w,1}(c_1(x) + \langle g_w(x)^{p^{a_1}}\rangle), \cdots, \epsilon_{w,\ell}(c_\ell(x) + \langle g_w(x)^{p^{a_\ell}}\rangle)\big) \in \mathcal{G}_w : (c_1(x), c_2(x), \cdots, c_\ell(x)) \in \mathcal{C}\}$ is an $\mathcal{S}_w$-submodule of $\mathcal{G}_w$ for each w. (The codes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ are called the constituents of $\mathcal{C}$ corresponding to the polynomials $g_1(x), g_2(x), \cdots, g_\rho(x)$, respectively.)

(b) Conversely, if $\mathcal{D}_w$ is an $\mathcal{S}_w$-submodule of $\mathcal{G}_w$ for $1 \leq w \leq \rho$, then the direct sum $\mathcal{D} = \bigoplus_{w=1}^{\rho} \mathcal{D}_w$ is a Λ-MT code of length n over $\mathbb{F}_q$.

Next we proceed to study dual codes of Λ-MT codes of length n over $\mathbb{F}_q$ with respect to the Galois inner product on $\mathbb{F}_q^n$, which is first defined and studied by Fan and Zhang [36]. For this, let k be a fixed integer satisfying $0 \leq k < r$. Then the k-Galois inner product on $\mathbb{F}_q^n$ is a map $\langle \cdot, \cdot \rangle_k : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, defined as

$$\langle d, c \rangle_k = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i - 1} d_{i,j} c_{i,j}^{p^k} \quad \text{for all } d, c \in \mathbb{F}_q^n.$$

Note that the map $\langle \cdot, \cdot \rangle_k$ is a non-degenerate σ_k-sesquilinear form on $\mathbb{F}_q^n$, where σ_k is an automorphism of $\mathbb{F}_q$, defined as $\sigma_k(b) = b^{p^k}$ for each $b \in \mathbb{F}_q$. In particular, the k-Galois inner product coincides with the Euclidean inner product on $\mathbb{F}_q^n$ when $k = 0$, while the k-Galois inner product matches with the Hermitian inner product on $\mathbb{F}_q^n$ when r is even and $k = \frac{r}{2}$.

Now for a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$, the k-Galois dual $\mathcal{C}^{\perp_k}$ of the code

$\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp_k} = \{d \in \mathbb{F}_q^n : \langle d, c\rangle_k = 0 \text{ for all } c \in \mathcal{C}\}.$$

Next let $m = \text{lcm}[m_1O(\lambda_1), m_2O(\lambda_2), \cdots, m_\ell O(\lambda_\ell)]$, where $O(\lambda_i)$ denotes the multiplicative order of λ_i for each i. It is easy to see that $T_\Lambda^m = I$, where I is the identity operator on $\mathbb{F}_q^n$. From this, we see that the k-Galois dual $\mathcal{C}^{\perp_k}$ of the code $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_q$ satisfying the following: if $d = (d_{1,0}, d_{1,1}, \cdots, d_{1,m_1-1}; d_{2,0}, d_{2,1}, \cdots, d_{2,m_2-1}; \cdots; d_{\ell,0}, d_{\ell,1}, \cdots, d_{\ell,m_\ell-1})$ is a codeword of $\mathcal{C}^{\perp_k}$, then its Λ^{-p^k}-MT shift $T_{\Lambda^{-p^k}}(d)$=$(\lambda_1^{-p^k} d_{1,m_1-1}, d_{1,0}, \cdots, d_{1,m_1-2}; \lambda_2^{-p^k} d_{2,m_2-1}, d_{2,0}, \cdots, d_{2,m_2-2}; \cdots; \lambda_\ell^{-p^k} d_{\ell,m_\ell-1}, d_{\ell,0}, \cdots, d_{\ell,m_\ell-2})$ is also a codeword of $\mathcal{C}^{\perp_k}$, where $\Lambda^{-p^k} = (\lambda_1^{-p^k}, \lambda_2^{-p^k}, \cdots, \lambda_\ell^{-p^k})$. Therefore $\mathcal{C}^{\perp_k}$ is a Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$. Equivalently, $\mathcal{C}^{\perp_k}$ is an $\mathbb{F}_q[x]$-submodule of the Λ^{-p^k}-MT module $V' = \prod_{i=1}^{\ell} V_i'$, where $V_i' = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \lambda_i^{-p^k}\rangle} = \frac{\mathbb{F}_q[x]}{\langle (x^{n_i} - \alpha_i^{-p^k})^{p^{a_i}}\rangle}$ for $1 \le i \le \ell$.

In order to further study algebraic structures of k-Galois duals of Λ-MT codes, let us define a map $\mathscr{T}_k : \mathbb{F}_q[x] \to \mathbb{F}_q[x]$ as

$$\mathscr{T}_k(f(x)) = a_0^{p^k} x^t + a_1^{p^k} x^{t-1} + \cdots + a_{t-1}^{p^k} x + a_t^{p^k}$$

for each $f(x) = a_0 + a_1 x + \cdots + a_t x^t \in \mathbb{F}_q[x]$ with $a_t \neq 0$. Then we observe the following:

Lemma 6.2.3. *Let $a(x) = a_0 + a_1 x + \cdots + a_t x^t$, $d(x) = d_0 + d_1 x + \cdots + d_\mu x^\mu \in \mathbb{F}_q[x]$, where a_0, a_t, d_μ are non-zero elements of $\mathbb{F}_q$ and $t, \mu \ge 0$ are integers. Then for $0 \le k < r$, we have the following:*

(a) $(\mathscr{T}_k \circ \mathscr{T}_{r-k})(a(x)) = (\mathscr{T}_{r-k} \circ \mathscr{T}_k)(a(x)) = a(x)$.

(b) $\mathscr{T}_k(a(x)d(x)) = \mathscr{T}_k(a(x))\mathscr{T}_k(d(x))$.

Proof. Proof is trivial. □

Now we make the following observation.

Lemma 6.2.4. *For $0 \leq k < r$, the map $\mathcal{T}_k : \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle} \to \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$, defined as*

$$\mathcal{T}_k(d(x)) = \sum_{j=0}^{m-1} d_j^{p^k} x^{-j} \text{ for each } d(x) = \sum_{j=0}^{m-1} d_j x^j \in \frac{\mathbb{F}_q[x]}{\langle x^m - 1\rangle},$$

is a ring automorphism. (Here we have $x^{-1} = x^{m-1} \in \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$.)

Proof. Its proof is straightforward. □

Next for $0 \leq k < r$ and $1 \leq i \leq \ell$, let us define the map $\mathcal{T}_k^{(i)} : V_i \to V_i'$ as $\mathcal{T}_k^{(i)}(c_i(x)) = \sum_{j=0}^{m_i-1} c_{i,j}^{p^k} x^{-j}$ for each $c_i(x) = \sum_{j=0}^{m_i-1} c_{i,j} x^j \in V_i$, where $x^{-1} = \lambda_i^{p^k} x^{m_i-1} \in V_i'$. We see that the map $\mathcal{T}_k^{(i)}$ is a ring isomorphism, and its inverse is a map $\mathcal{S}_k^{(i)} : V_i' \to V_i$, defined as $\mathcal{S}_k^{(i)}(d_i(x)) = \sum_{j=0}^{m_i-1} d_{i,j}^{p^{r-k}} x^{-j}$ for each $d_i(x) = \sum_{j=0}^{m_i-1} d_{i,j} x^j \in V_i'$, where $x^{-1} = \lambda_i^{-1} x^{m_i-1} \in V_i$. One can easily show that the map $\mathcal{S}_k^{(i)}$ is also a ring isomorphism. Now let us define the maps $(\cdot,\cdot)_k : V' \times V \longrightarrow \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$ and $\{\cdot,\cdot\}_k : V \times V' \longrightarrow \frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$ as

$$(d(x), c(x))_k = \sum_{i=1}^{\ell} \lambda_i^{-p^k} \left(\frac{x^m - 1}{x^{m_i} - \lambda_i^{-p^k}} \right) d_i(x) \mathcal{T}_k^{(i)}(c_i(x))$$

and

$$\{c(x), d(x)\}_k := \sum_{i=1}^{\ell} \lambda_i \left(\frac{x^m - 1}{x^{m_i} - \lambda_i} \right) c_i(x) \mathcal{S}_k^{(i)}(d_i(x))$$

for $d(x) = (d_1(x), d_2(x), \cdots, d_\ell(x)) \in V'$ and $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \in V$, where V and V' are viewed as $\frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}$-modules. From this, we make the following observation.

Lemma 6.2.5. *For $0 \leq k < r$, the following hold.*

(a) If $d(x) \in V'$ and $c(x) \in V$, then we have

$$(d(x), c(x))_k = \langle d, c\rangle_k + \langle d, T_\Lambda(c)\rangle_k \, x + \left\langle d, T_\Lambda^2(c)\right\rangle_k x^2 + \cdots + \left\langle d, T_\Lambda^{m-1}(c)\right\rangle_k x^{m-1}$$

and

$$\{c(x), d(x)\}_k = \langle c, d\rangle_{r-k} + \left\langle c, T_{\Lambda^{-p^k}}(d)\right\rangle_{r-k} x + \cdots + \left\langle c, T^{m-1}_{\Lambda^{-p^k}}(d)\right\rangle_{r-k} x^{m-1} \text{ in } \frac{\mathbb{F}_q[x]}{\langle x^m - 1\rangle}.$$

(b) For $d(x) \in V'$ and $c(x) \in V$, $(d(x), c(x))_k = 0$ if and only if $\{c(x), d(x)\}_k = 0$.

(c) The mapping $(\cdot,\cdot)_k$ is a non-degenerate $\mathcal{T}_k$-sesquilinear form on $V' \times V$, and the mapping $\{\cdot,\cdot\}_k$ is a non-degenerate $\mathcal{T}_{r-k}$-sesquilinear form on $V \times V'$.

Proof. Proof is trivial. □

In the following theorem, we show that the k-Galois dual of a Λ-MT code of length n over $\mathbb{F}_q$ can also be viewed as the orthogonal complement of the code with respect to the $\mathcal{T}_k$-sesquilinear form $(\cdot,\cdot)_k$.

Theorem 6.2.6. *If $\mathcal{C}$ $(\subseteq V)$ is a Λ-MT code of length n over $\mathbb{F}_q$, then its k-Galois dual $\mathcal{C}^{\perp_k} (\subseteq V')$ is a Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$ and is given by*

$$\mathcal{C}^{\perp_k} = \{d(x) \in V' : (d(x), c(x))_k = 0 \text{ for all } c(x) \in \mathcal{C}\}.$$

Proof. It follows immediately from Lemma 6.2.5(a). □

Further, a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is said to be

(i) k-Galois self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp_k}$.

(ii) k-Galois self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_k}$.

(iii) k-Galois linear with complementary-dual (LCD) if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_k} = \{0\}$.

We now proceed to study algebraic structures of k-Galois self-dual, k-Galois self-orthogonal and k-Galois LCD Λ-MT codes of length n over $\mathbb{F}_q$. Towards this, we first recall that $g_1(x), g_2(x), \cdots, g_\rho(x)$ are all the distinct irreducible factors of the polynomials $x^{n_1} - \alpha_1, x^{n_2} - \alpha_2, \cdots, x^{n_\ell} - \alpha_\ell$ in $\mathbb{F}_q[x]$. Further, by Lemma 6.2.3,

one can easily observe that $\mathscr{T}_k(g_1(x)), \mathscr{T}_k(g_2(x)), \cdots, \mathscr{T}_k(g_\rho(x))$ are all the distinct irreducible factors appearing in the factorizations of the polynomials $x^{n_1}-\alpha_1^{-p^k}, x^{n_2}-\alpha_2^{-p^k}, \cdots, x^{n_\ell}-\alpha_\ell^{-p^k}$ in $\mathbb{F}_q[x]$. Next for $1 \leq w \leq \rho$, we note that there exists a largest non-negative integer t_w satisfying the following two conditions:

(i) $g_w(x), \mathscr{T}_k(g_w(x)), \cdots, \mathscr{T}_k^{t_w}(g_w(x)) \in \mathbb{F}_q[x]$ are distinct irreducible factors of the polynomials $x^{n_1}-\alpha_1, x^{n_2}-\alpha_2, \cdots, x^{n_\ell}-\alpha_\ell$ in $\mathbb{F}_q[x]$.

(ii) Either $\langle \mathscr{T}_k^{t_w+1}(g_w(x))\rangle \neq \langle g_{w'}(x)\rangle$ for $1 \leq w' \leq \rho$ or $\langle \mathscr{T}_k^{t_w+1}(g_w(x))\rangle = \langle g_w(x)\rangle$ holds.

Accordingly, we classify the irreducible polynomials $g_1(x), g_2(x), \cdots, g_\rho(x)$ as follows:

Definition 6.2.7. *For $1 \leq w \leq \rho$, we say that an irreducible factor $g_w(x)$ of the polynomials $x^{n_1}-\alpha_1, x^{n_2}-\alpha_2, \cdots, x^{n_\ell}-\alpha_\ell$ in $\mathbb{F}_q[x]$ is of the*

- *Type I if $t_w = 0$ and $\langle \mathscr{T}_k(g_w(x))\rangle = \langle g_w(x)\rangle$.*
- *Type II if $t_w = 0$ and $\langle \mathscr{T}_k(g_w(x))\rangle \neq \langle g_w(x)\rangle$.*
- *Type III if $t_w \geq 1$ and $\langle \mathscr{T}_k^{t_w+1}(g_w(x))\rangle = \langle g_w(x)\rangle$.*
- *Type IV if $t_w \geq 1$ and $\langle \mathscr{T}_k^{t_w+1}(g_w(x))\rangle \neq \langle g_w(x)\rangle$.*

Now we assume, by relabelling $g_w(x)$'s if required, that $g_1(x), g_2(x), \cdots, g_{s_1}(x)$ are all the distinct Type I irreducible factors, $g_{s_1+1}(x), g_{s_1+2}(x), \cdots, g_{s_2}(x)$ are all the distinct Type II irreducible factors, $g_{s_2+1}(x), g_{s_2+2}(x), \cdots, g_{s_3}(x)$ are all the distinct Type III irreducible factors and $g_{s_3+1}(x), g_{s_3+2}(x), \cdots, g_{s_4}(x)$ are all the distinct Type IV irreducible factors of the polynomials $x^{n_1}-\alpha_1, x^{n_2}-\alpha_2, \cdots, x^{n_\ell}-\alpha_\ell$ in $\mathbb{F}_q[x]$. Here we note that $\rho = s_2 + \sum_{\vartheta=s_2+1}^{s_4} (t_\vartheta+1)$. Further, for $1 \leq \alpha \leq s_4$, $0 \leq b \leq t_\alpha+1$ and $1 \leq i \leq \ell$, let us define

$$R_{\alpha,i}^{(b)} = \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k^b(g_\alpha(x))^{p^{a^i}}\rangle} \quad \text{and} \quad \epsilon_{\alpha,i}^{(b)} = \begin{cases} 1 & \text{if } \mathscr{T}_k^b(g_\alpha(x)) \text{ divides } x^{n_i}-\alpha_i \text{ in } \mathbb{F}_q[x]; \\ 0 & \text{otherwise,} \end{cases}$$

(note that $R_{\alpha,i}^{(t_\alpha+1)} = R_{\alpha,i}^{(0)}$ for $\alpha \in \{1, 2, \cdots, s_1\} \cup \{s_2+1, s_2+2, \cdots, s_3\}$ and $1 \leq i \leq \ell$).

For $1 \leq \alpha \leq s_4, 0 \leq b \leq t_\alpha$ and $1 \leq i \leq \ell$, we observe that if $\epsilon_{\alpha,i}^{(b)} = 1$, then $\mathscr{T}_k^{b+1}(g_\alpha(x))$ divides $x^{n_i} - \alpha_i^{-p^k}$ in $\mathbb{F}_q[x]$. Now by applying the Chinese Remainder Theorem again, we obtain

$$\begin{aligned} V \simeq & \left(\bigoplus_{t=1}^{s_1} \mathcal{G}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=s_1+1}^{s_2} \mathcal{G}_\mu^{(0)}\right) \oplus \left(\bigoplus_{z=s_2+1}^{s_3} \Big(\underbrace{\mathcal{G}_z^{(0)} \oplus \mathcal{G}_z^{(1)} \oplus \cdots \oplus \mathcal{G}_z^{(t_z)}}_{G_z}\Big)\right) \oplus \\ & \left(\bigoplus_{v=s_3+1}^{s_4} \Big(\underbrace{\mathcal{G}_v^{(0)} \oplus \mathcal{G}_v^{(1)} \oplus \cdots \oplus \mathcal{G}_v^{(t_v)}}_{G_v}\Big)\right), \end{aligned}$$

and

$$\begin{aligned} V' \simeq & \left(\bigoplus_{t=1}^{s_1} \mathcal{G}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=s_1+1}^{s_2} \mathcal{H}_\mu^{(1)}\right) \oplus \left(\bigoplus_{z=s_2+1}^{s_3} \Big(\underbrace{\mathcal{H}_z^{(0)} \oplus \mathcal{H}_z^{(1)} \oplus \cdots \oplus \mathcal{H}_z^{(t_z)}}_{H_z}\Big)\right) \oplus \\ & \left(\bigoplus_{v=s_3+1}^{s_4} \Big(\underbrace{\mathcal{H}_v^{(t_v+1)} \oplus \mathcal{H}_v^{(1)} \oplus \cdots \oplus \mathcal{H}_v^{(t_v)}}_{H_v}\Big)\right), \end{aligned}$$

where

$$\begin{aligned} \mathcal{G}_\alpha^{(b)} &= \big(\epsilon_{\alpha,1}^{(b)} R_{\alpha,1}^{(b)}, \epsilon_{\alpha,2}^{(b)} R_{\alpha,2}^{(b)}, \cdots, \epsilon_{\alpha,\ell}^{(b)} R_{\alpha,\ell}^{(b)}\big) \text{ for } 1 \leq \alpha \leq s_4 \text{ and } 0 \leq b \leq t_\alpha, \\ \mathcal{H}_\mu^{(1)} &= \big(\epsilon_{\mu,1}^{(0)} R_{\mu,1}^{(1)}, \epsilon_{\mu,2}^{(0)} R_{\mu,2}^{(1)}, \cdots, \epsilon_{\mu,\ell}^{(0)} R_{\mu,\ell}^{(1)}\big) \text{ for } s_1+1 \leq \mu \leq s_2, \\ \mathcal{H}_z^{(0)} &= \big(\epsilon_{z,1}^{(t_z)} R_{z,1}^{(0)}, \epsilon_{z,2}^{(t_z)} R_{z,2}^{(0)}, \cdots, \epsilon_{z,\ell}^{(t_z)} R_{z,\ell}^{(0)}\big) \text{ for } s_2+1 \leq z \leq s_3, \\ \mathcal{H}_\omega^{(s)} &= \big(\epsilon_{\omega,1}^{(s-1)} R_{\omega,1}^{(s)}, \epsilon_{\omega,2}^{(s-1)} R_{\omega,2}^{(s)}, \cdots, \epsilon_{\omega,\ell}^{(s-1)} R_{\omega,\ell}^{(s)}\big) \text{ for } s_2+1 \leq \omega \leq s_4 \text{ and } 1 \leq s \leq t_\omega+1, \end{aligned}$$

(note that $\mathcal{H}_z^{(t_z+1)} = \mathcal{H}_z^{(0)}$, as $R_{z,i}^{(t_z+1)} = R_{z,i}^{(0)}$ for $s_2+1 \leq z \leq s_3$ and $1 \leq i \leq \ell$).

In view of this, from now on, we shall identify each element $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \in V$ as $C = (C_1, C_2, \cdots, C_{s_1}, C_{s_1+1}, C_{s_1+2}, \cdots, C_{s_2}, C_{s_2+1}, C_{s_2+2}, \cdots, C_{s_3}, C_{s_3+1},$

$C_{s_3+2}, \cdots, C_{s_4})$, where

$$\begin{aligned} C_t &= (C_{t,1}^{(0)}, C_{t,2}^{(0)}, \cdots, C_{t,\ell}^{(0)}) \in \mathcal{G}_t^{(0)}, C_\mu = (C_{\mu,1}^{(0)}, C_{\mu,2}^{(0)}, \cdots, C_{\mu,\ell}^{(0)}) \in \mathcal{G}_\mu^{(0)} \text{ and} \\ C_\omega &= (C_{\omega,1}^{(0)}, C_{\omega,2}^{(0)}, \cdots, C_{\omega,\ell}^{(0)}, C_{\omega,1}^{(1)}, C_{\omega,2}^{(1)}, \cdots, C_{\omega,\ell}^{(1)}, \cdots, C_{\omega,1}^{(t_\omega)}, C_{\omega,2}^{(t_\omega)}, \cdots, C_{\omega,\ell}^{(t_\omega)}) \in G_\omega \end{aligned}$$

for $1 \leq t \leq s_1, s_1+1 \leq \mu \leq s_2$ and $s_2+1 \leq \omega \leq s_4$ with

$$C_{\alpha,i}^{(b)} := \epsilon_{\alpha,i}^{(b)}\big(c_i(x) + \big\langle \mathscr{T}_k^b(g_\alpha(x))^{p^{a_i}} \big\rangle\big) \in \epsilon_{\alpha,i}^{(b)} R_{\alpha,i}^{(b)}$$

for $1 \leq \alpha \leq s_4, 0 \leq b \leq t_\alpha$ and $1 \leq i \leq \ell$.

Analogously, we shall identify each element $d(x) = (d_1(x), d_2(x), \cdots, d_\ell(x)) \in V'$ as $D = (D_1, D_2, \cdots, D_{s_1}, D_{s_1+1}, D_{s_1+2}, \cdots, D_{s_2}, D_{s_2+1}, D_{s_2+2}, \cdots, D_{s_3}, D_{s_3+1}, D_{s_3+2}, \cdots, D_{s_4})$, where

$$\begin{aligned} D_t &= (D_{t,1}^{(0)}, D_{t,2}^{(0)}, \cdots, D_{t,\ell}^{(0)}) \in \mathcal{G}_t^{(0)}, \quad D_\mu = (D_{\mu,1}^{(1)}, D_{\mu,2}^{(1)}, \cdots, D_{\mu,\ell}^{(1)}) \in \mathcal{H}_\mu^{(1)}, \\ D_z &= (D_{z,1}^{(0)}, D_{z,2}^{(0)}, \cdots, D_{z,\ell}^{(0)}, D_{z,1}^{(1)}, D_{z,2}^{(1)}, \cdots, D_{z,\ell}^{(1)}, \cdots, D_{z,1}^{(t_z)}, D_{z,2}^{(t_z)}, \cdots, D_{z,\ell}^{(t_z)}) \in H_z \text{ and} \\ D_v &= (D_{v,1}^{(t_v+1)}, D_{v,2}^{(t_v+1)}, \cdots, D_{v,\ell}^{(t_v+1)}, D_{v,1}^{(1)}, D_{v,2}^{(1)}, \cdots, D_{v,\ell}^{(1)}, \cdots, D_{v,1}^{(t_v)}, D_{v,2}^{(t_v)}, \cdots, D_{v,\ell}^{(t_v)}) \in H_v \end{aligned}$$

with

$$\begin{aligned} D_{t,i}^{(0)} &:= \epsilon_{t,i}^{(0)}\big(d_i(x) + \big\langle g_t(x)^{p^{a_i}} \big\rangle\big), \qquad D_{\mu,i}^{(1)} := \epsilon_{\mu,i}^{(0)}\big(d_i(x) + \big\langle \mathscr{T}_k(g_\mu(x))^{p^{a_i}} \big\rangle\big), \\ D_{z,i}^{(0)} &:= \epsilon_{z,i}^{(t_z)}\big(d_i(x) + \big\langle g_z(x)^{p^{a_i}} \big\rangle\big), \qquad D_{z,i}^{(j)} := \epsilon_{z,i}^{(j-1)}\big(d_i(x) + \big\langle \mathscr{T}_k^j(g_z(x))^{p^{a_i}} \big\rangle\big) \text{ and} \\ D_{v,i}^{(j')} &:= \epsilon_{v,i}^{(j'-1)}\big(d_i(x) + \big\langle \mathscr{T}_k^{j'}(g_v(x))^{p^{a_i}} \big\rangle\big) \end{aligned}$$

for $1 \leq j \leq t_z$, $1 \leq j' \leq t_v+1$, $1 \leq t \leq s_1$, $s_1+1 \leq \mu \leq s_2$, $s_2+1 \leq z \leq s_3$, $s_3+1 \leq v \leq s_4$ and $1 \leq i \leq \ell$.

Next for $1 \leq \alpha \leq s_4$ and $0 \leq b \leq t_\alpha+1$, we note that the set $\mathcal{S}_\alpha^{(b)} = \Big\{\Big(f(x) + \big\langle \mathscr{T}_k^b(g_\alpha(x))^{p^{a_1}} \big\rangle, f(x) + \big\langle \mathscr{T}_k^b(g_\alpha(x))^{p^{a_2}} \big\rangle, \cdots, f(x) + \big\langle \mathscr{T}_k^b(g_\alpha(x))^{p^{a_\ell}} \big\rangle\Big) : f(x) \in \mathbb{F}_q[x]\Big\}$ is a finite commutative ring with unity with respect to the component wise addition

and the component wise multiplication. Further, since V and V' are $\mathbb{F}_q[x]$-modules, we shall view the set $\mathcal{G}_\alpha^{(b)}$ (resp. $\mathcal{H}_\mu^{(1)}$, $\mathcal{H}_z^{(0)}$ and $\mathcal{H}_\omega^{(s)}$) as an $\mathcal{S}_\alpha^{(b)}$-module (resp. $\mathcal{S}_\mu^{(1)}$-module, $\mathcal{S}_z^{(0)}$-module and $\mathcal{S}_\omega^{(s)}$-module) for $1 \leq \alpha \leq s_4$ and $0 \leq b \leq t_\alpha$ (resp. for $s_1+1 \leq \mu \leq s_2$, $s_2+1 \leq z \leq s_3$, $s_2+1 \leq \omega \leq s_4$ and $1 \leq s \leq t_\omega+1$). From this, one can observe that a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as

$$\begin{aligned}\mathcal{C} \;=\; & \left(\bigoplus_{t=1}^{s_1} \mathcal{C}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=s_1+1}^{s_2} \mathcal{C}_\mu^{(0)}\right) \oplus \left(\bigoplus_{z=s_2+1}^{s_3} \left(\mathcal{C}_z^{(0)} \oplus \mathcal{C}_z^{(1)} \oplus \cdots \oplus \mathcal{C}_z^{(t_z)}\right)\right) \oplus \\ & \left(\bigoplus_{v=s_3+1}^{s_4} \left(\mathcal{C}_v^{(0)} \oplus \mathcal{C}_v^{(1)} \oplus \cdots \oplus \mathcal{C}_v^{(t_v)}\right)\right), \end{aligned} \tag{6.4}$$

where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}$, $\mathcal{C}_z^{(j)}$ and $\mathcal{C}_v^{(j')}$) is an $\mathcal{S}_t^{(0)}$-submodule of $\mathcal{G}_t^{(0)}$ (resp. $\mathcal{S}_\mu^{(0)}$-submodule of $\mathcal{G}_\mu^{(0)}$, $\mathcal{S}_z^{(j)}$-submodule of $\mathcal{G}_z^{(j)}$ and $\mathcal{S}_v^{(j')}$-submodule of $\mathcal{G}_v^{(j')}$) for $1 \leq t \leq s_1$ (resp. for $s_1+1 \leq \mu \leq s_2$, $s_2+1 \leq z \leq s_3$, $0 \leq j \leq t_z$, $s_3+1 \leq v \leq s_4$ and $0 \leq j' \leq t_v$).

Now for $1 \leq w \leq \rho$, let $\deg g_w(x) = d_w$. Further, note that $\deg \mathscr{T}_k(g_w(x)) = d_w$, as $g_w(x)$ is an irreducible polynomial over $\mathbb{F}_q$.

For $1 \leq \alpha \leq s_4$, $0 \leq b \leq t_\alpha$ and $1 \leq i \leq \ell$, let $^- : \epsilon_{\alpha,i}^{(b)} R_{\alpha,i}^{(b)} \to \epsilon_{\alpha,i}^{(b)} R_{\alpha,i}^{(b+1)}$ be the map, defined as

$$\overline{h_{\alpha,i}^{(b)}(x)} = \begin{cases} \displaystyle\sum_{\vartheta=0}^{d_\alpha p^{a_i}-1} h_\vartheta^{p^k} x^{-\vartheta} & \text{if } \epsilon_{\alpha,i}^{(b)} = 1; \\ 0 & \text{if } \epsilon_{\alpha,i}^{(b)} = 0 \end{cases} \tag{6.5}$$

for all $h_{\alpha,i}^{(b)}(x) = \displaystyle\sum_{\vartheta=0}^{d_\alpha p^{a_i}-1} h_\vartheta x^\vartheta \in R_{\alpha,i}^{(b)} (\subseteq V_i)$ when $\epsilon_{\alpha,i}^{(b)} = 1$, (note that $R_{\alpha,i}^{(t_\alpha+1)} = R_{\alpha,i}^{(0)}$ for $\alpha \in \{1, 2, \cdots, s_1\} \cup \{s_2+1, s_2+2, \cdots, s_3\}$ and $1 \leq i \leq \ell$).

For $1 \leq t \leq s_1$ and $1 \leq i \leq \ell$ satisfying $\epsilon_{t,i}^{(0)} = 1$, we observe that the conjugation map $^-$ is the identity map when $d_t = 1, k = 0$ and $p^{a_i} = 1$, while it is an automorphism of $R_{t,i}^{(0)}$ when either $d_t > 1$ or $0 < k < r$ or $p^{a_i} > 1$. In view of this, we note that for each $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \in V$, the element $\overline{c(x)} \in V'$ is identified

as

$$(\overline{C_1}, \overline{C_2}, \cdots, \overline{C_{s_1}}, \overline{C_{s_1+1}}, \overline{C_{s_1+2}}, \cdots, \overline{C_{s_2}}, \overline{C_{s_2+1}}, \overline{C_{s_2+2}}, \cdots, \overline{C_{s_3}}, \overline{C_{s_3+1}}, \overline{C_{s_3+2}}, \cdots, \overline{C_{s_4}}),$$

where

$$\begin{aligned}
\overline{C_t} &= (\overline{C_{t,1}^{(0)}}, \overline{C_{t,2}^{(0)}}, \cdots, \overline{C_{t,\ell}^{(0)}}) \in \mathcal{G}_t^{(0)}, \quad \overline{C_\mu} = (\overline{C_{\mu,1}^{(0)}}, \overline{C_{\mu,2}^{(0)}}, \cdots, \overline{C_{\mu,\ell}^{(0)}}) \in \mathcal{H}_\mu^{(1)}, \\
\overline{C_z} &= (\overline{C_{z,1}^{(t_z)}}, \overline{C_{z,2}^{(t_z)}}, \cdots, \overline{C_{z,\ell}^{(t_z)}}, \overline{C_{z,1}^{(0)}}, \overline{C_{z,2}^{(0)}}, \cdots, \overline{C_{z,\ell}^{(0)}}, \cdots, \overline{C_{z,1}^{(t_z-1)}}, \overline{C_{z,2}^{(t_z-1)}}, \cdots, \overline{C_{z,\ell}^{(t_z-1)}}) \in H_z, \\
\overline{C_v} &= (\overline{C_{v,1}^{(t_v)}}, \overline{C_{v,2}^{(t_v)}}, \cdots, \overline{C_{v,\ell}^{(t_v)}}, \overline{C_{v,1}^{(0)}}, \overline{C_{v,2}^{(0)}}, \cdots, \overline{C_{v,\ell}^{(0)}}, \cdots, \overline{C_{v,1}^{(t_v-1)}}, \overline{C_{v,2}^{(t_v-1)}}, \cdots, \overline{C_{v,\ell}^{(t_v-1)}}) \in H_v
\end{aligned}$$

for $1 \le t \le s_1, s_1+1 \le \mu \le s_2, s_2+1 \le z \le s_3$ and $s_3+1 \le v \le s_4$ with

$$\overline{C_{\alpha,i}^{(b)}} := \epsilon_{\alpha,i}^{(b)}\big(\overline{c_i(x)} + \big\langle \mathscr{T}_k^{b+1}(g_\alpha(x))^{p^{a_i}} \big\rangle\big) \in \epsilon_{\alpha,i}^{(b)} R_{\alpha,i}^{(b+1)}$$

for all $1 \le \alpha \le s_4,\ 0 \le b \le t_\alpha$ and $1 \le i \le \ell$.

From this point on, let $a = \max\{a_1, a_2, \cdots, a_\ell\}$. Then it is easy to see that if $\epsilon_{\alpha,i}^{(b)} = 1$ for some $1 \le \alpha \le s_4$, $0 \le b \le t_\alpha$ and $1 \le i \le \ell$, then $x^{m_i} = \lambda_i^{-p^k}$ in $R_{\alpha,i}^{(b+1)}$, which implies that $\lambda_i^{-p^k}(x^m-1)/(x^{m_i}-\lambda_i^{-p^k}) = m/m_i = 0$ in $R_{\alpha,i}^{(b+1)}$ when $a_i \ne a$, while $\lambda_i^{-p^k}(x^m-1)/(x^{m_i}-\lambda_i^{-p^k}) = m/m_i \ne 0$ in $R_{\alpha,i}^{(b+1)}$ when $a_i = a$. In view of this, one can easily observe that the sesquilinear form corresponding to $(\cdot,\cdot)_k$ is a mapping $[\cdot,\cdot]_k$ from $V' \times V$ into $\left(\bigoplus_{t=1}^{s_1} \frac{\mathbb{F}_q[x]}{\langle g_t(x)^{p^a}\rangle}\right) \oplus \left(\bigoplus_{\mu=s_1+1}^{s_2} \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k(g_\mu(x))^{p^a}\rangle}\right) \oplus \left(\bigoplus_{z=s_2+1}^{s_3} \left(\frac{\mathbb{F}_q[x]}{\langle g_z(x)^{p^a}\rangle} \oplus \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k(g_z(x))^{p^a}\rangle} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k^{t_z}(g_z(x))^{p^a}\rangle}\right)\right) \oplus \left(\bigoplus_{v=s_3+1}^{s_4} \left(\frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k^{t_v+1}(g_v(x))^{p^a}\rangle} \oplus \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k(g_v(x))^{p^a}\rangle} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{\langle \mathscr{T}_k^{t_v}(g_v(x))^{p^a}\rangle}\right)\right)$, defined as

$$\begin{aligned}
[D,C]_k = \Bigg(&\sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{1,i}^{(0)} D_{1,i}^{(0)} \overline{C_{1,i}^{(0)}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{2,i}^{(0)} D_{2,i}^{(0)} \overline{C_{2,i}^{(0)}}, \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{s_1,i}^{(0)} D_{s_1,i}^{(0)} \overline{C_{s_1,i}^{(0)}}, \\
&\sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{s_1+1,i}^{(0)} D_{s_1+1,i}^{(1)} \overline{C_{s_1+1,i}^{(0)}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{s_1+2,i}^{(0)} D_{s_1+2,i}^{(1)} \overline{C_{s_1+2,i}^{(0)}}, \cdots,
\end{aligned}$$

$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_2,i}^{(0)}D_{s_2,i}^{(1)}\overline{C_{s_2,i}^{(0)}},\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_2+1,i}^{(t_{s_2+1})}D_{s_2+1,i}^{(0)}\overline{C_{s_2+1,i}^{(t_{s_2+1})}},\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_2+1,i}^{(0)}D_{s_2+1,i}^{(1)}\overline{C_{s_2+1,i}^{(0)}},$$
$$\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_2+1,i}^{(t_{s_2+1}-1)}D_{s_2+1,i}^{(t_{s_2+1})}\overline{C_{s_2+1,i}^{(t_{s_2+1}-1)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3,i}^{(t_{s_3})}D_{s_3,i}^{(0)}\overline{C_{s_3,i}^{(t_{s_3})}},$$
$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3,i}^{(0)}D_{s_3,i}^{(1)}\overline{C_{s_3,i}^{(0)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3,i}^{(t_{s_3}-1)}D_{s_3,i}^{(t_{s_3})}\overline{C_{s_3,i}^{(t_{s_3}-1)}},\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3+1,i}^{t_{s_3+1}}D_{s_3+1,i}^{t_{s_3+1}+1}\overline{C_{s_3+1,i}^{t_{s_3+1}}},$$
$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3+1,i}^{(0)}D_{s_3+1,i}^{(1)}\overline{C_{s_3+1,i}^{(0)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_3+1,i}^{(t_{s_3+1}-1)}D_{s_3+1,i}^{(t_{s_3+1})}\overline{C_{s_3+1,i}^{(t_{s_3+1}-1)}},\cdots,$$
$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_4,i}^{(t_{s_4})}D_{s_4,i}^{(t_{s_4}+1)}\overline{C_{s_4,i}^{(t_{s_4})}},\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_4,i}^{(0)}D_{s_4,i}^{(1)}\overline{C_{s_4,i}^{(0)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{s_4,i}^{(t_{s_4}-1)}D_{s_4,i}^{(t_{s_4})}\overline{C_{s_4,i}^{(t_{s_4}-1)}}\Bigg). \tag{6.6}$$

for each $C \in V$ and $D \in V'$. Furthermore, with respect to the sesquilinear form $[\cdot,\cdot]_k$ (as defined by (6.6)), we observe that the k-Galois dual $\mathcal{C}^{\perp_k}$ of the code $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_k}=\Bigg(\bigoplus_{t=1}^{s_1}\mathcal{C}_t^{(0)\perp_k}\Bigg)\oplus\Bigg(\bigoplus_{\mu=s_1+1}^{s_2}\mathcal{C}_\mu^{(0)\perp_k}\Bigg)\oplus\Bigg(\bigoplus_{z=s_2+1}^{s_3}\mathcal{C}_z{}^{(t_z)\perp_k}\oplus\mathcal{C}_z{}^{(0)\perp_k}\oplus\cdots\oplus\mathcal{C}_z{}^{(t_z-1)\perp_k}\Bigg)$$
$$\oplus\Bigg(\bigoplus_{v=s_3+1}^{s_4}\mathcal{C}_v{}^{(t_v)\perp_k}\oplus\mathcal{C}_v{}^{(0)\perp_k}\oplus\cdots\oplus\mathcal{C}_v{}^{(t_v-1)\perp_k}\Bigg), \tag{6.7}$$

where

- $\mathcal{C}_t^{(0)\perp_k}(\subseteq\mathcal{G}_t^{(0)})$ is the orthogonal complement of $\mathcal{C}_t^{(0)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}}$ for $1\le t\le s_1$;
- $\mathcal{C}_\mu^{(0)\perp_k}(\subseteq\mathcal{H}_\mu^{(1)})$ is the orthogonal complement of $\mathcal{C}_\mu^{(0)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}}$ for $s_1+1\le\mu\le s_2$;
- $\mathcal{C}_z^{(t_z)\perp_k}(\subseteq\mathcal{H}_z^{(0)})$ is the orthogonal complement of $\mathcal{C}_z^{(t_z)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_z^{(0)}\times\mathcal{G}_z^{(t_z)}}$ and $\mathcal{C}_z^{(j)\perp_k}(\subseteq\ \mathcal{H}_z^{(j+1)})$ is the orthogonal complement of $\mathcal{C}_z^{(j)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_z^{(j+1)}\times\mathcal{G}_z^{(j)}}$ for $0\le j\le t_z-1$ and $s_2+1\le z\le s_3$;

- $\mathcal{C}_v^{(j')\perp_k}(\subseteq \mathcal{H}_v^{(j'+1)})$ is the orthogonal complement of $\mathcal{C}_v^{(j')}$ with respect to $[\cdot,\cdot]_k \restriction_{\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}}$ for $s_3+1 \leq v \leq s_4$ and $0 \leq j' \leq t_v$.

Here $[\cdot,\cdot]_k \restriction_{\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}}$ (resp. $[\cdot,\cdot]_k \restriction_{\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}}$, $[\cdot,\cdot]_k \restriction_{\mathcal{H}_z^{(j+1)}\times\mathcal{G}_z^{(j)}}$, $[\cdot,\cdot]_k \restriction_{\mathcal{H}_z^{(0)}\times\mathcal{G}_z^{(t_z)}}$ and $[\cdot,\cdot]_k \restriction_{\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}}$) is the restriction of the sesquilinear form $[\cdot,\cdot]_k$ (as defined by (6.6)) to $\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}$ (resp. $\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}$, $\mathcal{H}_z^{(j+1)}\times\mathcal{G}_z^{(j)}$, $\mathcal{H}_z^{(0)}\times\mathcal{G}_z^{(t_z)}$ and $\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}$) for each t (resp. μ, z, v, j and j'). Further, for $s_2+1 \leq z \leq s_3$ and $s_3+1 \leq v \leq s_4$, let us define $\mathcal{K}_z^{(j)} = \mathcal{G}_z^{(j)} \cap \mathcal{H}_z^{(j)}$ and $\mathcal{K}_v^{(j')} = \mathcal{G}_v^{(j')} \cap \mathcal{H}_v^{(j')}$, where $0 \leq j \leq t_z$ and $1 \leq j' \leq t_v$.

Now as a consequence of the above discussion, we have the following theorem, which provides necessary and sufficient conditions under which a Λ-MT code is (i) k-Galois self-dual, (ii) k-Galois self-orthogonal and (iii) k-Galois LCD.

Theorem 6.2.8. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Let*

$$\begin{aligned}\mathcal{C} \;=\; & \left(\bigoplus_{t=1}^{s_1}\mathcal{C}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=s_1+1}^{s_2}\mathcal{C}_\mu^{(0)}\right) \oplus \left(\bigoplus_{z=s_2+1}^{s_3}\left(\mathcal{C}_z^{(0)} \oplus \mathcal{C}_z^{(1)} \oplus \cdots \oplus \mathcal{C}_z^{(t_z)}\right)\right) \\ & \oplus \left(\bigoplus_{v=s_3+1}^{s_4}\left(\mathcal{C}_v^{(0)} \oplus \mathcal{C}_v^{(1)} \oplus \cdots \oplus \mathcal{C}_v^{(t_v)}\right)\right)\end{aligned}$$

be a Λ-MT code of length n over $\mathbb{F}_q$, where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}$, $\mathcal{C}_z^{(j)}$ and $\mathcal{C}_\nu^{(j')}$) is an $\mathcal{S}_t^{(0)}$-submodule of $\mathcal{G}_t^{(0)}$ (resp. $\mathcal{S}_\mu^{(0)}$-submodule of $\mathcal{G}_\mu^{(0)}$, $\mathcal{S}_z^{(j)}$-submodule of $\mathcal{G}_z^{(j)}$ and $\mathcal{S}_v^{(j')}$-submodule of $\mathcal{G}_v^{(j')}$) for $1 \leq t \leq s_1$ (resp. for $s_1+1 \leq \mu \leq s_2, s_2+1 \leq z \leq s_3, 0 \leq j \leq t_z, s_3+1 \leq v \leq s_4$ and $0 \leq j' \leq t_v$). Then for $0 \leq k < r$, the following hold.

(a) The code $\mathcal{C}$ is k-Galois self-dual if and only if the following conditions are satisfied:

- *None of the polynomials $x^{n_1}-\alpha_1, x^{n_2}-\alpha_2, \cdots, x^{n_\ell}-\alpha_\ell$ has an irreducible factor of the Type II in $\mathbb{F}_q[x]$.*

- $\mathcal{C}_t^{(0)} = \mathcal{C}_t^{(0)\perp_k}$ *for* $1 \leq t \leq s_1$.
- *For* $s_2 + 1 \leq z \leq s_3$ *and* $0 \leq j \leq t_z$, $\mathcal{C}_z^{(j)}$ *is an* $\mathcal{S}_z^{(j)}$*-submodule of* $\mathcal{K}_z^{(j)}$ *satisfying* $\mathcal{C}_z^{(0)} = \mathcal{C}_z^{(t_z)\perp_k}$, $\mathcal{C}_z^{(1)} = \mathcal{C}_z^{(0)\perp_k}$, $\mathcal{C}_z^{(2)} = \mathcal{C}_z^{(1)\perp_k}$, $\cdots$, $\mathcal{C}_z^{(t_z)} = \mathcal{C}_z^{(t_z-1)\perp_k}$.
- *For* $s_3+1 \leq v \leq s_4$, $\mathcal{C}_v^{(0)} = \{0\}$, $\mathcal{C}_v^{(1)} = \mathcal{K}_v^{(1)}$ *and* $\mathcal{C}_v^{(j')}$ *is an* $\mathcal{S}_v^{(j')}$*-submodule of* $\mathcal{K}_v^{(j')}$ *satisfying* $\mathcal{C}_v^{(j')} = \mathcal{C}_v^{(j'-1)\perp_k}$ *and* $\mathcal{C}_v^{(t_v)\perp_k} = \{0\}$, *where* $2 \leq j' \leq t_v$.

(b) The code $\mathcal{C}$ *is* k*-Galois self-orthogonal if and only if the following conditions are satisfied:*

- $\mathcal{C}_t^{(0)} \subseteq \mathcal{C}_t^{(0)\perp_k}$ *for* $1 \leq t \leq s_1$.
- $\mathcal{C}_\mu^{(0)} = \{0\}$ *for* $s_1 + 1 \leq \mu \leq s_2$.
- *For* $s_2 + 1 \leq z \leq s_3$ *and* $0 \leq j \leq t_z$, $\mathcal{C}_z^{(j)}$ *is an* $\mathcal{S}_z^{(j)}$*-submodule of* $\mathcal{K}_z^{(j)}$ *satisfying* $\mathcal{C}_z^{(0)} \subseteq \mathcal{C}_z^{(t_z)\perp_k}$, $\mathcal{C}_z^{(1)} \subseteq \mathcal{C}_z^{(0)\perp_k}$, $\mathcal{C}_z^{(2)} \subseteq \mathcal{C}_z^{(1)\perp_k}$, $\cdots$, $\mathcal{C}_z^{(t_z)} \subseteq \mathcal{C}_z^{(t_z-1)\perp_k}$.
- *For* $s_3 + 1 \leq v \leq s_4$, $\mathcal{C}_v^{(0)} = \{0\}$, $\mathcal{C}_v^{(1)}$ *is any* $\mathcal{S}_v^{(1)}$*-submodule of* $\mathcal{K}_v^{(1)}$ *and* $\mathcal{C}_v^{(j')}$ *is an* $\mathcal{S}_v^{(j')}$*-submodule of* $\mathcal{K}_v^{(j')}$ *satisfying* $\mathcal{C}_v^{(j')} \subseteq \mathcal{C}_v^{(j'-1)\perp_k}$, *where* $2 \leq j' \leq t_v$.

(c) The code $\mathcal{C}$ *is* k*-Galois LCD if and only if the following conditions are satisfied:*

- $\mathcal{C}_t^{(0)} \cap \mathcal{C}_t^{(0)\perp_k} = \{0\}$ *for* $1 \leq t \leq s_1$.
- $\mathcal{C}_\mu^{(0)}$ *is any* $\mathcal{S}_\mu^{(0)}$*-submodule of* $\mathcal{G}_\mu^{(0)}$ *for* $s_1 + 1 \leq \mu \leq s_2$.
- *For* $s_2 + 1 \leq z \leq s_3$ *and* $0 \leq j \leq t_z$, $\mathcal{C}_z^{(0)} \cap \mathcal{C}_z^{(t_z)\perp_k} = \{0\}$, $\mathcal{C}_z^{(1)} \cap \mathcal{C}_z^{(0)\perp_k} = \{0\}, \cdots, \mathcal{C}_z^{(t_z)} \cap \mathcal{C}_z^{(t_z-1)\perp_k} = \{0\}$.
- *For* $s_3 + 1 \leq v \leq s_4$, $\mathcal{C}_v^{(0)}$ *is any* $\mathcal{S}_v^{(0)}$*-submodule of* $\mathcal{G}_v^{(0)}$ *and* $\mathcal{C}_v^{(j')} \cap \mathcal{C}_v^{(j'-1)\perp_k} = \{0\}$, *where* $1 \leq j' \leq t_v$.

When either $k = 0$ or r is even and $k = r/2$, we see that $\mathscr{T}_k^2(g_w(x)) = g_w(x)$, which implies that $t_w \leq 1$ for $1 \leq w \leq \rho$. This further implies that the polynomials

$x^{n_1}-\alpha_1, x^{n_2}-\alpha_2, \cdots, x^{n_\ell}-\alpha_\ell$ do not have an irreducible factor of the Type IV in $\mathbb{F}_q[x]$. From this and by (6.4), we note that a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as

$$\mathcal{C} = \Big(\bigoplus_{t=1}^{s_1} \mathcal{C}_t^{(0)}\Big) \oplus \Big(\bigoplus_{\mu=s_1+1}^{s_2} \mathcal{C}_\mu^{(0)}\Big) \oplus \Big(\bigoplus_{z=s_2+1}^{s_3} (\mathcal{C}_z^{(0)} \oplus \mathcal{C}_z^{(1)})\Big), \tag{6.8}$$

where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}$ and $\mathcal{C}_z^{(j)}$) is an $\mathcal{S}_t^{(0)}$-submodule of $\mathcal{G}_t^{(0)}$ (resp. $\mathcal{S}_\mu^{(0)}$-submodule of $\mathcal{G}_\mu^{(0)}$ and $\mathcal{S}_z^{(j)}$-submodule of $\mathcal{G}_z^{(j)}$) for $1 \le t \le s_1$ (resp. for $s_1+1 \le \mu \le s_2$ and $s_2+1 \le z \le s_3$ with $0 \le j \le 1$).

6.3 Trace description of MT codes

In this section, we will provide a trace description for all Λ-MT codes of length n over $\mathbb{F}_q$. For this, we first recall the definition of the Hasse derivative of a polynomial in $\mathbb{F}_q[x]$.

Definition 6.3.1. *[51] For an integer $j \ge 0$, the j-th Hasse derivative (or the j-th hyperderivative) of the polynomial $g(x) = \sum_{i=0}^{h} g_i x^i \in \mathbb{F}_q[x]$ is defined as*

$$g^{[j]}(x) = \sum_{i=j}^{h} \binom{i}{j} g_i x^{i-j}.$$

We next recall the definition of the classical discrete Fourier transform (DFT). For this, let θ be a positive integer satisfying $\gcd(\theta, p) = 1$, and let λ be a non-zero element of $\mathbb{F}_q$. Further, let ξ be a primitive θ-th root of unity in some field extension of $\mathbb{F}_q$, and let β be an element in some field extension of $\mathbb{F}_q$ satisfying $\beta^\theta = \lambda$. One can easily observe that all the distinct roots of $x^\theta - \lambda$ over $\mathbb{F}_q$ are given by $\beta, \beta\xi, \beta\xi^2, \cdots, \beta\xi^{\theta-1}$. Now the classical DFT maps the element $c(x) = \sum_{\nu=0}^{\theta-1} c_\nu x^\nu \in$

$\frac{\mathbb{F}_q[x]}{\langle x^\theta - \lambda \rangle}$ to the sequence $(\hat{c}_0, \hat{c}_1, \cdots, \hat{c}_{\theta-1})$, where

$$\hat{c}_\nu = c(\beta\xi^\nu) = \sum_{j=0}^{\theta-1} c_j(\beta\xi^\nu)^j \text{ for } 0 \leq \nu \leq \theta - 1.$$

On the other hand, the inverse DFT is given by

$$c_\kappa = \frac{\beta^{-\kappa}}{\theta} \sum_{h=0}^{\theta-1} \hat{c}_h(\xi^{-\kappa})^h \text{ for } 0 \leq \kappa \leq \theta - 1.$$

We refer to [57, p. 239] for more details.

Next let $M = \text{lcm}\,[n_1O(\alpha_1), n_2O(\alpha_2), \cdots, n_\ell O(\alpha_\ell)]$, where $O(\alpha_i)$ denotes the multiplicative order of α_i in $\mathbb{F}_q$ for $1 \leq i \leq \ell$. We note that $\gcd(M, q) = 1$, and hence there exists a field extension $\mathbb{F}_Q$ of $\mathbb{F}_q$, which contains a primitive M-th root of unity. From this, we observe that there exist elements $\beta_1, \beta_2, \cdots, \beta_\ell, \xi_1, \xi_2, \cdots, \xi_\ell$ in $\mathbb{F}_Q$ such that

$$\beta_i^{n_i} = \alpha_i \text{ and } O(\xi_i) = n_i \text{ for } 1 \leq i \leq \ell.$$

Therefore for $1 \leq i \leq \ell$, we have

$$x^{n_i} - \alpha_i = (x - \beta_i)(x - \beta_i\xi_i) \cdots (x - \beta_i\xi_i^{n_i-1}) \text{ in } \mathbb{F}_Q[x],$$

which gives

$$x^{m_i} - \lambda_i = (x^{n_i} - \alpha_i)^{p^{a_i}} = (x - \beta_i)^{p^{a_i}}(x - \beta_i\xi_i)^{p^{a_i}} \cdots (x - \beta_i\xi_i^{n_i-1})^{p^{a_i}} \text{ in } \mathbb{F}_Q[x].$$

Further, recall that $g_1(x), g_2(x), \cdots, g_\rho(x)$ are all the distinct irreducible factors of the polynomials $x^{n_1} - \alpha_1, x^{n_2} - \alpha_2, \cdots, x^{n_\ell} - \alpha_\ell$ in $\mathbb{F}_q[x]$. For $1 \leq w \leq \rho$, if d_w is the degree of the irreducible polynomial $g_w(x)$, then we have $\frac{\mathbb{F}_q[x]}{\langle g_w(x) \rangle} \simeq \mathbb{F}_{q^{d_w}}$. Next let δ_w be a root of $g_w(x)$ in $\mathbb{F}_{q^{d_w}}$ for $1 \leq w \leq \rho$. Now for $1 \leq i \leq \ell$ and $1 \leq w \leq \rho$ satisfying

$\epsilon_{w,i} = 1$, we note that there exists an integer $\tau_w^{(i)}$ satisfying $0 \leq \tau_w^{(i)} \leq n_i - 1$ and

$$\beta_i \xi_i^{\tau_w^{(i)}} = \delta_w.$$

Furthermore, for $1 \leq i \leq \ell$, we note that $\beta_i^{n_i} = \alpha_i$, which implies that $\beta_i^{(q-1)n_i} = 1$. This further implies that $\beta_i^{q-1} = \xi_i^{\varepsilon_i}$ for some integer ε_i satisfying $0 \leq \varepsilon_i \leq n_i - 1$. Next if $\epsilon_{w,i} = 1$ and $\beta_i \xi_i^{t_i}$ is a root of $g_w(x)$ for some integer t_i satisfying $0 \leq t_i \leq n_i - 1$, then one can observe that $\beta_i \xi_i^{t_i q + \varepsilon_i}$ is also a root of $g_w(x)$ for $1 \leq i \leq \ell$ and $1 \leq w \leq \rho$. Further, for $1 \leq i \leq \ell$, let us define a map $\chi_i : \mathbb{Z}/n_i\mathbb{Z} \longrightarrow \mathbb{Z}/n_i\mathbb{Z}$ as $h \mapsto qh + \varepsilon_i$ for each $h \in \mathbb{Z}/n_i\mathbb{Z}$. Here for each i, we see that the map χ_i is a bijection and induces an equivalence relation $\sim$ on $\mathbb{Z}/n_i\mathbb{Z}$, which is given by $h_1 \sim h_2$ if and only if $h_1 = \chi_i^d(h_2)$ for some integer d. Therefore for each i, there is a 1-1 correspondence between the equivalence classes of $\mathbb{Z}/n_i\mathbb{Z}$ with respect to the relation $\sim$ and the irreducible factors of $x^{n_i} - \alpha_i$ in $\mathbb{F}_q[x]$. These equivalence classes are called orbits of χ_i for each i. Further, if $\epsilon_{w,i} = 1$ for some w and i, then we choose the integer $\tau_w^{(i)}$ as a representative of the orbit corresponding to the irreducible factor $g_w(x)$ of $x^{n_i} - \alpha_i$. Now let us define the sets

$$T_i = \{w : 1 \leq w \leq \rho \text{ and } \epsilon_{w,i} = 1\} \text{ for } 1 \leq i \leq \ell$$

and

$$U_w = \{i : 1 \leq i \leq \ell \text{ and } \epsilon_{w,i} = 1\} \text{ for } 1 \leq w \leq \rho.$$

In order to provide a trace description for Λ-MT codes, we will use the concept of the generalized discrete Fourier transform (GDFT) in a manner similar to that of Theorem 6.2 of Ling et al. [52] and Theorem 7 of Jia [47]. To do this, we see that for $1 \leq i \leq \ell$, the generalized discrete Fourier transform (GDFT) of the element

$c_i(x) = \sum_{j=0}^{m_i-1} c_{i,j}x^j \in V_i$ is given by the following matrix

$$\hat{c}_i = \begin{bmatrix} \hat{c}_{0,0}^{(i)} & \hat{c}_{0,1}^{(i)} & \cdots & \hat{c}_{0,n_i-1}^{(i)} \\ \hat{c}_{1,0}^{(i)} & \hat{c}_{1,1}^{(i)} & \cdots & \hat{c}_{1,n_i-1}^{(i)} \\ \vdots & \vdots & \vdots & \vdots \\ \hat{c}_{p^{a_i}-1,0}^{(i)} & \hat{c}_{p^{a_i}-1,1}^{(i)} & \cdots & \hat{c}_{p^{a_i}-1,n_i-1}^{(i)} \end{bmatrix},$$

where

$$\hat{c}_{g_i,h_i}^{(i)} = c_i^{[g_i]}(\beta_i\xi_i^{h_i}) = \sum_{j=0}^{m_i-1} \binom{j}{g_i} c_{i,j}(\beta_i\xi_i^{h_i})^{j-g_i}$$

for $0 \le g_i \le p^{a_i} - 1$ and $0 \le h_i \le n_i - 1$.

Further, for $1 \le i \le \ell$, $0 \le g_i \le p^{a_i} - 1$ and $0 \le h_i \le n_i - 1$, we observe that

$$(\hat{c}_{g_i,h_i}^{(i)})^q = \sum_{j=0}^{m_i-1} \binom{j}{g_i} c_{i,j}(\beta_i\xi_i^{h_i})^{q(i-j)} = \sum_{j=0}^{m_i-1} \binom{j}{g_i} c_{i,j}(\beta_i\xi_i^{qh_i+\varepsilon_i})^{i-j} = \hat{c}_{g_i,qh_i+\varepsilon_i}^{(i)}, \quad (6.9)$$

where ε_i is an integer satisfying $0 \le \varepsilon_i \le n_i - 1$ and $\beta_i^{q-1} = \xi_i^{\varepsilon_i}$. Now if $f(x)$ is an irreducible polynomial of degree d in $\mathbb{F}_q[x]$ and $b \ge 0$ is an integer, then one can show that the quotient ring $\frac{\mathbb{F}_q[x]}{\langle f(x)^{p^b}\rangle}$ is isomorphic to the finite commutative chain ring $\frac{\mathbb{F}_{q^d}[u]}{\langle u^{p^b}\rangle} \simeq \mathbb{F}_{q^d} + u\mathbb{F}_{q^d} + \cdots + u^{p^b-1}\mathbb{F}_{q^d}$ with $u^{p^b} = 0$. In fact, the ring isomorphism from $\frac{\mathbb{F}_q[x]}{\langle f(x)^{p^b}\rangle}$ onto $\frac{\mathbb{F}_{q^d}[u]}{\langle u^{p^b}\rangle}$ is given by $r(x) \mapsto r(\alpha(1-u))$ for each $r(x) \in \frac{\mathbb{F}_q[x]}{\langle f(x)^{p^b}\rangle}$, where $u^{p^b} = 0$ and α is a root of $f(x)$ in $\mathbb{F}_{q^d}$. In view of this, for $1 \le w \le \rho$ and $1 \le i \le \ell$, we observe that

$$\epsilon_{w,i}\frac{\mathbb{F}_q[x]}{\langle g_w(x)^{p^{a_i}}\rangle} \simeq \epsilon_{w,i}\frac{\mathbb{F}_{q^{d_w}}[u_i]}{\langle u_i^{p^{a_i}}\rangle} \simeq \epsilon_{w,i}\left(\mathbb{F}_{q^{d_w}} + u_i\mathbb{F}_{q^{d_w}} + \cdots + u_i^{p^{a_i}-1}\mathbb{F}_{q^{d_w}}\right) \text{ with } u_i^{p^{a_i}} = 0.$$

In view of this, for $1 \le w \le \rho$, we see that

$$\mathcal{G}_w \simeq \left(\epsilon_{w,1}\frac{\mathbb{F}_{q^{d_w}}[u_1]}{\langle u_1^{p^{a_1}}\rangle}, \epsilon_{w,2}\frac{\mathbb{F}_{q^{d_w}}[u_2]}{\langle u_2^{p^{a_2}}\rangle}, \cdots, \epsilon_{w,\ell}\frac{\mathbb{F}_{q^{d_w}}[u_\ell]}{\langle u_\ell^{p^{a_\ell}}\rangle}\right) = \mathcal{L}_w,$$

where $u_i^{p^{a_i}} = 0$ for $1 \leq i \leq \ell$. Further, let us define a map $\psi : V \to \bigoplus_{w=1}^{\rho} \mathcal{L}_w$ as

$$\psi\big(c_1(x), c_2(x), \cdots, c_\ell(x)\big) = \sum_{w=1}^{\rho} \left(\sum_{j_1=0}^{p^{a_1}-1} u_1^{j_1} \hat{c}^{(1)}_{j_1,\tau_w^{(1)}}, \sum_{j_2=0}^{p^{a_2}-1} u_2^{j_2} \hat{c}^{(2)}_{j_2,\tau_w^{(2)}}, \cdots, \sum_{j_\ell=0}^{p^{a_\ell}-1} u_\ell^{j_\ell} \hat{c}^{(\ell)}_{j_\ell,\tau_w^{(\ell)}} \right)$$

for all $(c_1(x), c_2(x), \cdots, c_\ell(x)) \in V$, where for $1 \leq w \leq \rho, 1 \leq i \leq \ell$ and $0 \leq j_i \leq p^{a_i} - 1$,

$$\hat{c}^{(i)}_{j_i,\tau_w^{(i)}} = \begin{cases} c_i^{[j_i]}(\delta_w) = c_i^{[j_i]}(\beta_i \xi_i^{\tau_w^{(i)}}) & \text{if } \epsilon_{w,i} = 1; \\ 0 & \text{if } \epsilon_{w,i} = 0. \end{cases}$$

One can easily show that the map Ψ is the ring isomorphism from V onto $\bigoplus_{w=1}^{\rho} \mathcal{L}_w$. Now for $1 \leq w \leq \rho$, let us define

$$\mathcal{F}_w = \left\{ \left(\sum_{j_1=0}^{p^{a_1}-1} u_1^{j_1} \alpha^{[j_1]}(\delta_w), \sum_{j_2=0}^{p^{a_2}-1} u_2^{j_2} \alpha^{[j_2]}(\delta_w), \cdots, \sum_{j_\ell=0}^{p^{a_\ell}-1} u_\ell^{j_\ell} \alpha^{[j_\ell]}(\delta_w) \right) : \alpha(x) \in \mathbb{F}_q[x] \right\},$$

where $u_i^{p^{a_i}} = 0$ for $1 \leq i \leq \ell$. Here for each w, we see that the set $\mathcal{F}_w$ is a finite commutative ring with unity with respect to the component wise addition and the component wise multiplication, and we shall view the set $\mathcal{L}_w$ as an $\mathcal{F}_w$-module. From the above discussion and by Theorem 6.2.2, we observe that a Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as $\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w$, where $\mathcal{C}_w$ is an $\mathcal{F}_w$-submodule of $\mathcal{L}_w$ for each w. The codes $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ are called the constituents of $\mathcal{C}$ corresponding to the polynomials $g_1(x), g_2(x), \cdots, g_\rho(x)$, respectively. Conversely, if $\mathcal{D}_w$ is an $\mathcal{F}_w$-submodule of $\mathcal{L}_w$ for $1 \leq w \leq \rho$, then the direct sum $\mathcal{D} = \bigoplus_{w=1}^{\rho} \mathcal{D}_w$ is a Λ-MT code of length n over $\mathbb{F}_q$.

Now to explicitly derive the inverse transform of the GDFT, let us define $c_{(i,t_i)}(x) = c_{i,t_i} + c_{i,t_i+p^{a_i}} x + \cdots + c_{i,t_i+(n_i-1)p^{a_i}} x^{n_i-1}$ for $0 \leq t_i \leq p^{a_i} - 1$ and $1 \leq i \leq \ell$. Further, for each i, we note that there exists a positive integer k_i satisfying $k_i r - a_i > 0$. Now for $1 \leq i \leq \ell$ and $0 \leq t_i \leq p^{a_i} - 1$, let us define $d_{(i,t_i)}(x) = c_{i,t_i}^{p^{k_i r - a_i}} +$

$c_{i,t_i+p^{a_i}}^{p^{k_i r-a_i}} x+\cdots+c_{i,t_i+(n_i-1)p^{a_i}}^{p^{k_i r-a_i}} x^{n_i-1}$. Then for each i, by using the DFT, we see that $\hat{d}_{(i,t_i)}(x)=\hat{c}_{i,t_i}^{p^{k_i r-a_i}}+\hat{c}_{i,t_i+p^{a_i}}^{p^{k_i r-a_i}} x+\cdots+\hat{c}_{i,t_i+(n_i-1)p^{a_i}}^{p^{k_i r-a_i}} x^{n_i-1}$, where $\hat{c}_{i,t_i+v_i p^{a_i}}^{p^{k_i r-a_i}}=d_{(i,t_i)}(\beta_i\xi_i^{v_i})$ with $0\le t_i\le p^{a_i}-1$ and $0\le v_i\le n_i-1$. Further, for each i, by using the inverse DFT, one can easily observe that $c_{i,t_i+v_i p^{a_i}}^{p^{k_i r-a_i}}=\frac{\beta_i^{-v_i}}{n_i}\hat{d}_{(i,t_i)}(\xi_i^{-v_i})$, where $0\le v_i\le n_i-1$. This implies that

$$c_{i,t_i+v_i p^{a_i}}=\frac{\beta_i^{-v_i p^{a_i}}}{n_i}\sum_{h_i=0}^{n_i-1} c_{(i,t_i)}\left((\beta_i\xi_i^{h_i})^{p^{a_i}}\right)\left(\xi_i^{-v_i p^{a_i}}\right)^{h_i} \text{ for each relevant } i, v_i \text{ and } t_i. \tag{6.10}$$

Now for $1\le i\le \ell$, let $H_i(x)$ be the $p^{a_i}\times p^{a_i}$ matrix whose (s_i,μ_i)-th entry is $\binom{\mu_i}{s_i}x^{\mu_i-s_i}$, where the rows and columns of $H_i(x)$ are indexed from 0 to $p^{a_i}-1$. It is easy to see that the matrix $H_i(x)$ is invertible and its inverse is given by $H_i(-x)$ for each i. Further, for each i, we observe that

$$H_i(\beta_i\xi_i^{h_i})\begin{bmatrix} c_{(i,0)}((\beta_i\xi_i^{h_i})^{p^{a_i}}) \\ c_{(i,1)}((\beta_i\xi_i^{h_i})^{p^{a_i}}) \\ \vdots \\ c_{(i,p^{a_i}-1)}((\beta_i\xi_i^{h_i})^{p^{a_i}}) \end{bmatrix}=\begin{bmatrix} \hat{c}_{0,h_i}^{(i)} \\ \hat{c}_{1,h_i}^{(i)} \\ \vdots \\ \hat{c}_{p^{a_i}-1,h_i}^{(i)} \end{bmatrix}, \text{ where } 0\le h_i\le n_i-1. \tag{6.11}$$

Now for each v_i, t_i and i, by (6.9)-(6.11), we get

$$\begin{aligned} c_{i,t_i+v_i p^{a_i}} &= \frac{\beta_i^{-v_i p^{a_i}}}{n_i}\sum_{h_i=0}^{n_i-1}\left(\sum_{j_i=0}^{p^{a_i}-1}\binom{j_i}{t_i}\left(-\beta_i\xi_i^{h_i}\right)^{j_i-t_i}\hat{c}_{j_i,h_i}^{(i)}\right)\left(\xi_i^{-v_i p^{a_i}}\right)^{h_i} \\ &= \frac{1}{n_i}\sum_{j_i=0}^{p^{a_i}-1}\binom{j_i}{t_i}(-1)^{j_i-t_i}\left(\sum_{h_i=0}^{n_i-1}\left(\beta_i\xi_i^{h_i}\right)^{j_i-t_i-v_i p^{a_i}}\hat{c}_{j_i,h_i}^{(i)}\right) \\ &= \frac{1}{n_i}\sum_{j_i=0}^{p^{a_i}-1}\binom{j_i}{t_i}(-1)^{j_i-t_i}\left(\sum_{w\in T_i} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}\left(\left(\beta_i\xi_i^{\tau_w^{(i)}}\right)^{j_i-t_i-v_i p^{a_i}}\hat{c}_{j_i,\tau_w^{(i)}}^{(i)}\right)\right), \end{aligned}$$

where $Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}$ is the trace function from $\mathbb{F}_{q^{d_w}}$ onto $\mathbb{F}_q$ for each w.

From the above discussion, we have the following theorem, which provides a trace description for all Λ-MT codes of length n over $\mathbb{F}_q$ using the GDFT.

Theorem 6.3.2. *(a) For $1 \leq w \leq \rho$, let $\mathcal{C}_w$ be an $\mathcal{F}_w$-submodule of $\mathcal{L}_w$, and let us write each word $x_w \in \mathcal{C}_w$ as $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell})$, where*

$$x_{w,i} = \begin{cases} x_{0,w}^{(i)} + x_{1,w}^{(i)} u_i + \cdots + x_{p^{a_i}-1,w}^{(i)} u_i^{p^{a_i}-1} & \text{if } \epsilon_{w,i} = 1; \\ 0 & \text{otherwise,} \end{cases}$$

with $x_{j_i,w}^{(i)} \in \mathbb{F}_{q^{d_w}}$ for $1 \leq w \leq \rho$, $1 \leq i \leq \ell$ and $0 \leq j_i \leq p^{a_i} - 1$. Further, for $1 \leq i \leq \ell$, let us define

$$\begin{aligned} c_i(x_1, x_2, \cdots, x_\rho) &= \big(c_{i,0}(x_1, x_2, \cdots, x_\rho), c_{i,1}(x_1, x_2, \cdots, x_\rho), \cdots \\ &\qquad \cdots, c_{i,m_i-1}(x_1, x_2, \cdots, x_\rho)\big), \end{aligned}$$

where for $0 \leq t_i \leq p^{a_i} - 1$ and $0 \leq v_i \leq n_i - 1$,

$$c_{i,t_i+v_i p^{a_i}}(x_1, x_2, \cdots, x_\rho) = \frac{1}{n_i} \left(\sum_{j_i=0}^{p^{a_i}-1} \binom{j_i}{t_i} (-1)^{j_i - t_i} \sum_{w \in T_i} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q} \left(x_{j_i,w}^{(i)} \, (\delta_w)^{j_i - t_i - v_i p^{a_i}} \right) \right) \tag{6.12}$$

with $\delta_w = \beta_i \xi_i^{\tau_w^{(i)}}$. Then the code

$$\begin{aligned} \mathcal{C} &= \Big\{ (c_1(x_1, x_2, \cdots, x_\rho); c_2(x_1, x_2, \cdots, x_\rho); \cdots; c_\ell(x_1, x_2, \cdots, x_\rho)) : \\ &\qquad x_w \in \mathcal{C}_w \text{ for } 1 \leq w \leq \rho \Big\} \end{aligned}$$

is a Λ-MT code of length n over $\mathbb{F}_q$.

(b) Conversely, each Λ-MT code of length n over $\mathbb{F}_q$ can be obtained from its constituents (that are $\mathcal{F}_w$-submodules of $\mathcal{L}_w$) through this construction.

Remark 6.3.3. *(a) The above theorem also provides a method to construct all Λ-MT codes of length n over $\mathbb{F}_q$.*

(b) Theorem 3.5.2 follows, as a special case, on taking $a_1 = a_2 = \cdots = a_\ell = 0$ in Theorem 6.3.2.

6.4 Type II MT codes

Type II codes over finite fields form an interesting class of linear codes. These codes are useful in constructing unimodular lattices and in the determination of modular forms [37, 44]. In this section, we shall also study Type II codes within the family of Λ-MT codes over finite fields. For this, we assume, throughout this section, that $q = 2^r$ and $a_1 = a_2 = \cdots = a_\ell = a$. Here $n_1, n_2, \cdots, n_\ell$ are odd positive integers. We also recall that $U_1 = \{i : 1 \leq i \leq \ell, \epsilon_{1,i} = 1\}$. Moreover, for all $i \in U_1$, we assume that $n_i \equiv n' \pmod 4$ for some odd integer n'. We also note that there exists a trace-orthogonal basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$ ([51, p. 75]). Now let $B = \{b_1, b_2, \cdots, b_r\}$ be a trace-orthogonal basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$. That is, for $1 \leq u, v \leq r$, we have

$$Tr_{\mathbb{F}_{2^r}/\mathbb{F}_2}(b_u b_v) = \begin{cases} 1 & \text{if } u = v; \\ 0 & \text{otherwise,} \end{cases}$$

where $Tr_{\mathbb{F}_{2^r}/\mathbb{F}_2}$ is the trace function from $\mathbb{F}_{2^r}$ onto $\mathbb{F}_2$. Since B is a trace-orthogonal basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$, each element $y \in \mathbb{F}_{2^r}$ can be uniquely written as $y = \sum_{j=1}^{r} y_j b_j$, where $y_j \in \mathbb{F}_2 = \{0, 1\}$ for $1 \leq j \leq r$. Now the Lee weight of the element $y \in \mathbb{F}_{2^r}$ with respect to the basis B is defined as the sum $wt_L^B(y) = \sum_{j=1}^{r} y_j$. Further, the Lee weight of a vector $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathbb{F}_{2^r}^n$ with respect to the basis B is defined as the sum $wt_L^B(c) = \sum_{i=0}^{n-1} wt_L^B(c_i)$, i.e., the sum of the Lee weights of its individual components. Now a Euclidean self-dual code of length n over $\mathbb{F}_{2^r}$ is said to be a Type II code if the Lee weight of each of its codewords is a multiple of 4. This definition of Type II codes is shown to be independent of the choice of the trace-orthogonal basis [12].

In order to study Type II Λ-MT codes of length n over $\mathbb{F}_{2^r}$, we see, by Theorem 6.2.2, that a Λ-MT code of length n over $\mathbb{F}_{2^r}$ can be uniquely expressed as $\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w$, where $\mathcal{C}_w (\subseteq \mathcal{G}_w)$ is a linear code of length ℓ over the finite commutative chain ring $\frac{\mathbb{F}_{2^r}[x]}{\langle g_w(x)^{2^a} \rangle}$ for $1 \leq w \leq \rho$. Further, we know that the GDFT gives rise to the ring

isomorphism from $\frac{\mathbb{F}_{2^r}[x]}{\langle (x-1)^{2^a}\rangle}$ onto $\frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle} \simeq \mathbb{F}_{2^r} + u\mathbb{F}_{2^r} + \cdots + u^{2^a-1}\mathbb{F}_{2^r}$ with $u^{2^a} = 0$, given by $b(x) \mapsto b(1) + ub^{[1]}(1) + \cdots + u^{2^a-1}b^{[2^a-1]}(1)$ for each $b(x) = b_0 + b_1x + \cdots + b_{2^a-1}x^{2^a-1} \in \frac{\mathbb{F}_{2^r}[x]}{\langle (x-1)^{2^a}\rangle}$. Further, the inverse map from $\frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle}$ onto $\frac{\mathbb{F}_{2^r}[x]}{\langle (x-1)^{2^a}\rangle}$ is given by $A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1} \mapsto B_0 + B_1x + \cdots + B_{2^a-1}x^{2^a-1}$ for each $A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1} \in \frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle}$, where $B_\varsigma = A_\varsigma + \binom{\varsigma+1}{\varsigma}A_{\varsigma+1} + \cdots + \binom{2^a-1}{\varsigma}A_{2^a-1}$ for $0 \le \varsigma \le 2^a - 1$. This gives rise to a Gray map $\phi : \frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle} \to \mathbb{F}_{2^r}^{2^a}$, which is defined as

$$\phi(A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1}) = (B_0, B_1, \cdots, B_{2^a-1}) \tag{6.13}$$

for each $A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1} \in \frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle}$. Therefore with respect to the trace-orthogonal basis B of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$, the Lee weight of the element $A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1} \in \frac{\mathbb{F}_{2^r}[u]}{\langle u^{2^a}\rangle}$ is defined as the Lee weight of its Gray image $\phi(A_0 + uA_1 + \cdots + u^{2^a-1}A_{2^a-1}) = (B_0, B_1, \cdots, B_{2^a-1})$, where $B_\varsigma = A_\varsigma + \binom{\varsigma+1}{\varsigma}A_{\varsigma+1} + \cdots + \binom{2^a-1}{\varsigma}A_{2^a-1}$ for $0 \le \varsigma \le 2^a - 1$.

Now we make the following observation.

Lemma 6.4.1. *Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_{2^r}$. Let $\lambda_i = 1$ for some integer i satisfying $1 \le i \le \ell$, and let $\mathcal{C}_1$ be the constituent of $\mathcal{C}$ corresponding to the irreducible factor $g_1(x) = x - 1$ of $x^{m_i} - \lambda_i = x^{m_i} - 1$ in $\mathbb{F}_{2^r}[x]$. Suppose that there is an (odd) integer n' such that $n_i \equiv n' \pmod 4$ for all $i \in U_1$. If the Lee weight of every codeword of $\mathcal{C}$ is a multiple of 4, then the Lee weight of every word of the constituent $\mathcal{C}_1$ is a multiple of 4. Conversely, if the Lee weight of every word of the constituent $\mathcal{C}_1$ is a multiple of 4, then the Lee weight of every codeword of $\mathcal{C}$ corresponding to the direct sum $\mathcal{C}_1 \oplus \{0\} \oplus \cdots \oplus \{0\}$ is a multiple of 4.*

Proof. Let $x_1 = (x_{1,1}, x_{1,2}, \cdots, x_{1,\ell}) \in \mathcal{C}_1$ be fixed. Let us write

$$x_{1,i} = \begin{cases} x_{0,1}^{(i)} + x_{1,1}^{(i)}u + \cdots + x_{2^a-1,1}^{(i)}u^{2^a-1} & \text{if } \epsilon_{1,i} = 1; \\ 0 & \text{otherwise,} \end{cases}$$

where $x_{j,1}^{(i)} \in \mathbb{F}_{2^r}$ for $1 \le i \le \ell$ and $0 \le j \le 2^a - 1$. As $U_1 = \{i : 1 \le i \le \ell \text{ and } \epsilon_{1,i} =$

$1\}$, we see that $wt_L^B(x_1) = \sum_{i=1}^{\ell} wt_L^B(\phi(x_{1,i})) = \sum_{i \in U_1} wt_L^B(\phi(x_{1,i}))$.

Now by applying Theorem 6.3.2, the codeword $c \in \mathcal{C}$ corresponding to the element $(x_1, 0, \cdots, 0) \in \mathcal{C}_1 \oplus \{0\} \oplus \cdots \oplus \{0\}$ is given by $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots, c_{\ell,m_\ell-1})$, where for $0 \leq t \leq 2^a - 1, 1 \leq i \leq \ell$ and $0 \leq v_i \leq n_i - 1$,

$$c_{i,t+v_i 2^a} = \begin{cases} x_{t,1}^{(1)} + \binom{t+1}{t} x_{t+1,1}^{(1)} + \cdots + \binom{2^a-1}{t} x_{2^a-1,1}^{(1)} & \text{if } i \in U_1; \\ 0 & \text{otherwise.} \end{cases}$$

We further observe that

$$\begin{aligned} wt_L^B(c) &= \sum_{i \in U_1} wt_L^B(c_{i,0}, c_{i,1}, \cdots, c_{i,m_i-1}) = \sum_{i \in U_1} \sum_{v_i=0}^{n_i-1} wt_L^B(c_{i,v_i 2^a}, c_{i,1+v_i 2^a}, \cdots, c_{i,2^a-1+v_i 2^a}) \\ &= \sum_{i \in U_1} \sum_{v_i=0}^{n_i-1} wt_L^B(\phi(x_{1,i})) = \sum_{i \in U_1} n_i wt_L^B(\phi(x_{1,i})) \\ &\equiv \; n' \sum_{i \in U_1} wt_L^B(\phi(x_{1,i})) \equiv n' wt_L^B(x_1) \pmod 4. \end{aligned}$$

From this, the desired result follows immediately. □

Now we state Lemma 7.1 of Ling et al. [52] on the Lee weight of vectors over $\mathbb{F}_{2^r}$ with respect to the basis B.

Lemma 6.4.2. *[52] Let B be a trace-orthogonal basis of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$, and let wt_L^B denote the Lee weight function with respect to the basis B. Then for $y = (y_0, y_1, \cdots, y_{n-1}), y' = (y'_0, y'_1, \cdots, y'_{n-1}) \in \mathbb{F}_{2^r}^n$, we have*

$$wt_L^B(y + y') \equiv wt_L^B(y) + wt_L^B(y') - 2wt_L^B(y * y') \ (mod\ 4),$$

where $y * y' = (y_0 y'_0, y_1 y'_1, \cdots, y_{n-1} y'_{n-1})$. Furthermore, if $\langle y, y' \rangle_0 = 0$, then $wt_L^B(y + y') \equiv wt_L^B(y) + wt_L^B(y')$ $(mod\ 4)$.

The following lemma generalizes Lemma 7.3 of Ling et al. [52].

Lemma 6.4.3. *Let $\lambda_i = 1$ for $1 \leq i \leq \ell$. Let $\mathcal{C} = \bigoplus_{w'=1}^{\rho} \mathcal{C}_{w'}$ be a Euclidean self-orthogonal Λ-MT code (i.e., a GQC code) of length n over $\mathbb{F}_{2^r}$, where $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ are the respective constituents of the code $\mathcal{C}$ corresponding to the irreducible factors $g_1(x), g_2(x), \cdots, g_\rho(x)$ of the polynomials $x^{m_1} - 1, x^{m_2} - 1, \cdots, x^{m_\ell} - 1$ in $\mathbb{F}_{2^r}[x]$. Let w be an integer satisfying $1 \leq w \leq \rho$ and $g_w(x) \neq x - 1$. Then the Lee weights of all the codewords of $\mathcal{C}$ corresponding to the elements of the direct sum $\{0\} \oplus \cdots \oplus \{0\} \oplus \mathcal{C}_w \oplus \{0\} \oplus \cdots \oplus \{0\}$ are multiples of 4.*

Proof. To prove the result, let $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w$ be fixed. Let us write

$$x_{w,i} = \begin{cases} x_{0,w}^{(i)} + x_{1,w}^{(i)} u + \cdots + x_{2^a-1,w}^{(i)} u^{2^a-1} & \text{if } \epsilon_{w,i} = 1; \\ 0 & \text{otherwise,} \end{cases}$$

where $x_{j,w}^{(i)} \in \mathbb{F}_{2^{rd_w}}$ for $1 \leq i \leq \ell$ and $0 \leq j \leq 2^a - 1$. Next by Theorem 6.3.2, we see that the codeword $c \in \mathcal{C}$ corresponding to the element $(0, \cdots, 0, x_w, 0, \cdots, 0) \in \{0\} \oplus \cdots \oplus \{0\} \oplus \mathcal{C}_w \oplus \{0\} \oplus \cdots \oplus \{0\}$ is given by $c = (c_{1,0}, c_{1,1}, \cdots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \cdots, c_{2,m_2-1}; \cdots; c_{\ell,0}, c_{\ell,1}, \cdots, c_{\ell,m_\ell-1})$, where for $0 \leq t \leq 2^a - 1, 1 \leq i \leq \ell$ and $0 \leq v_i \leq n_i - 1$,

$$c_{i,t+v_i 2^a} = 0 \text{ if } i \notin U_w \tag{6.14}$$

and

$$c_{i,t+v_i 2^a} = \sum_{j=t}^{2^a-1} \binom{j}{t} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}(x_{j,w}^{(i)} \delta_w^{j-t-v_i 2^a}) \text{ if } i \in U_w. \tag{6.15}$$

Further, consider the minimal polynomial $P(x)$ of $\delta_w^{-2^a}$ over $\mathbb{F}_2$. Now as $\delta_w^{-2^a} \neq 1$, we note that the minimal polynomial $P(x)$ of $\delta_w^{-2^a}$ must have an odd number of non-zero monomials. Let us write $P(x) = 1 + x^{j_1} + x^{j_2} + \cdots + x^{j_{d-1}}$, where d is an odd integer. From this, we have

$$1 + \delta_w^{-j_1 2^a} + \delta_w^{-j_2 2^a} + \cdots + \delta_w^{-j_{d-1} 2^a} = 0. \tag{6.16}$$

Next for $i \in U_w, 0 \le v_i \le n_i - 1$ and $0 \le t \le 2^a - 1$, we see, by (6.15) and (6.16), that

$$c_{i,t+v_i 2^a} + c_{i,t+(v_i+j_1)2^a} + \cdots + c_{i,t+(v_i+j_{d-1})2^a} = 0.$$

Further, for $i \in U_w, 0 \le v_i \le n_i - 1$ and $0 \le t \le 2^a - 1$, let us define

$$\begin{aligned}
A^{(0)}_{t,v_i} &= c_{i,t+v_i 2^a}, \\
A^{(1)}_{t,v_i} &= c_{i,t+v_i 2^a} + c_{i,t+(v_i+j_1)2^a}, \\
A^{(2)}_{t,v_i} &= c_{i,t+v_i 2^a} + c_{i,t+(v_i+j_1)2^a} + c_{i,t+(v_i+j_2)2^a}, \\
&\vdots \\
A^{(d-2)}_{t,v_i} &= c_{i,t+v_i 2^a} + c_{i,t+(v_i+j_1)2^a} + \cdots + c_{i,t+(v_i+j_{d-2})2^a}.
\end{aligned}$$

From this, it follows that

$$\begin{aligned}
c_{i,t+v_i 2^a} &= A^{(0)}_{t,v_i}, \\
c_{i,t+(v_i+j_1)2^a} &= A^{(1)}_{t,v_i} + A^{(0)}_{t,v_i}, \\
c_{i,t+(v_i+j_2)2^a} &= A^{(2)}_{t,v_i} + A^{(1)}_{t,v_i}, \\
&\vdots \\
c_{i,t+(v_i+j_{d-2})2^a} &= A^{(d-2)}_{t,v_i} + A^{(d-3)}_{t,v_i}, \\
c_{i,t+(v_i+j_{d-1})2^a} &= A^{(d-2)}_{t,v_i}.
\end{aligned}$$

Next we observe that

$$\begin{aligned}
d\ wt^B_L(c) &= \sum_{i \in U_w} d\ wt^B_L(c_{i,0}, c_{i,1}, \cdots, c_{i,m_i-1}) \\
&= \sum_{i \in U_w} \sum_{v_i=0}^{n_i-1} \sum_{t=0}^{2^a-1} wt^B_L(c_{i,t+v_i 2^a}, c_{i,t+(v_i+j_1)2^a}, \cdots, c_{i,t+(v_i+j_{d-1})2^a}) \\
&= \sum_{i \in U_w} \sum_{v_i=0}^{n_i-1} \sum_{t=0}^{2^a-1} wt^B_L\left(A^{(0)}_{t,v_i}, A^{(1)}_{t,v_i} + A^{(0)}_{t,v_i}, \cdots, A^{(d-2)}_{t,v_i} + A^{(d-3)}_{t,v_i}, A^{(d-2)}_{t,v_i}\right).
\end{aligned}$$

Further, by applying Lemma 6.4.2, we get

$$\begin{aligned} d\ wt_L^B(c) &\equiv 2\sum_{i\in U_w}\sum_{v_i=0}^{n_i-1}\sum_{t=0}^{2^a-1}\Big(\sum_{b_1=0}^{d-2} wt_L^B\big(A_{t,v_i}^{(b_1)}\big) - \sum_{b_2=0}^{d-3} wt_L^B\big(A_{t,v_i}^{(b_2)} * A_{t,v_i}^{(b_2+1)}\big)\Big) \pmod 4 \\ &\equiv 2\sum_{b_1=0}^{d-2}\Big(\sum_{i\in U_w}\sum_{v_i=0}^{n_i-1}\sum_{t=0}^{2^a-1} wt_L^B\big(A_{t,v_i}^{(b_1)}\big)\Big) - 2\sum_{b_2=0}^{d-3}\Big(\sum_{i\in U_w}\sum_{v_i=0}^{n_i-1}\sum_{t=0}^{2^a-1} \\ &\qquad wt_L^B\big(A_{t,v_i}^{(b_2)} * A_{t,v_i}^{(b_2+1)}\big)\Big) \pmod 4. \end{aligned}$$

From this, we obtain

$$\begin{aligned} d\ wt_L^B(c) \equiv\ & 2\Big(wt_L^B(c) + wt_L^B\big(c + T_\Lambda^{-j_1 2^a}(c)\big) + \cdots + wt_L^B\big(c + T_\Lambda^{-j_1 2^a}(c) + \cdots + \\ & T_\Lambda^{-j_{d-2} 2^a}(c)\big)\Big) - 2\Big(wt_L^B\big(c * \big(c + T_\Lambda^{-j_1 2^a}(c)\big) + wt_L^B\big(\big(c + T_\Lambda^{-j_1 2^a}(c)\big) * \\ & \big(c + T_\Lambda^{-j_1 2^a}(c) + T_\Lambda^{-j_2 2^a}(c)\big) + \cdots + wt_L^B\big(\big(c + T_\Lambda^{-j_1 2^a}(c) + \cdots + T_\Lambda^{-j_{d-3} 2^a}(c)\big) \\ & *\big(c + T_\Lambda^{-j_1 2^a}(c) + \cdots + T_\Lambda^{-j_{d-2} 2^a}(c)\big)\Big) \pmod 4. \end{aligned} \tag{6.17}$$

Since $\mathcal{C}$ is a Euclidean self-orthogonal Λ-MT code, by applying Lemma 6.4.2, we note that $2\ wt_L^B(c') \equiv 0 \pmod 4$ for all $c' \in \mathcal{C}$. From this and by (6.17), one can easily observe that $d\ wt_L^B(c) \equiv 0 \pmod 4$, which implies that $wt_L^B(c) \equiv 0 \pmod 4$. From this, the desired result follows. □

In the following example, we show that Lemma 6.4.3 does not hold for Euclidean self-orthogonal Λ-MT codes of length n over $\mathbb{F}_{2^r}$ when $\lambda_i \neq 1$ for some integer i satisfying $1 \leq i \leq \ell$.

Example 6.4.1. *Let $q = 4$, $\ell = 2$, $m_1 = m_2 = 5$, and let $\Lambda = (b^2, b^2)$, where b is a primitive element of $\mathbb{F}_4$ satisfying $1 + b + b^2 = 0$. Here we have $V = \frac{\mathbb{F}_4[x]}{\langle x^5 - b^2\rangle} \times \frac{\mathbb{F}_4[x]}{\langle x^5 - b^2\rangle}$. It is easy to see that the set $B = \{b, b^2\}$ is a trace-orthogonal basis of $\mathbb{F}_4$ over $\mathbb{F}_2$. From this, we get $wt_L^B(0) = 0, wt_L^B(1) = 2$ and $wt_L^B(b) = wt_L^B(b^2) = 1$. Now let $\mathcal{C}$ be a 1-generator Euclidean self-orthogonal Λ-MT code of length 10 over $\mathbb{F}_4$ with the generating set $\{(b + bx + b^2x^2 + x^3, b + bx + b^2x^2 + x^3)\}$. Further, we observe that*

$x^5-b^2=(x-b)(x^2+x+b^2)(x^2+b^2x+b^2)$ is the irreducible factorization of x^5-b^2 over $\mathbb{F}_4$. Let us take $g_1(x)=x-b$, $g_2(x)=x^2+x+b^2$ and $g_3(x)=x^2+b^2x+b^2$. Now by applying Theorem 6.2.2, we get $\mathcal{C}=\bigoplus_{w=1}^{3}\mathcal{C}_w$, where $\mathcal{C}_1=\langle(b,b)\rangle$ is a $\frac{\mathbb{F}_4[x]}{\langle g_1(x)\rangle}$-submodule of $\mathcal{G}_1$, $\mathcal{C}_2=\langle(b^2+b^2\delta_2,b^2+b^2\delta_2)\rangle$ is a $\frac{\mathbb{F}_4[x]}{\langle g_2(x)\rangle}$-submodule of $\mathcal{G}_2$ with $\delta_2^2+\delta_2+b^2=0$ and $\mathcal{C}_3=\langle(b+\delta_3,b+\delta_3)\rangle$ is a $\frac{\mathbb{F}_4[x]}{\langle g_3(x)\rangle}$-submodule of $\mathcal{G}_3$ with $\delta_3^2+b^2\delta_3+b^2=0$. Next let us take $x_1=(b,b)\in\mathcal{C}_1, x_2=(b^2+b^2\delta_2,b^2+b^2\delta_2)\in\mathcal{C}_2$ and $x_3=(b+\delta_3,b+\delta_3)\in\mathcal{C}_3$. Now by Theorem 6.3.2, we see that the codewords $c_1,c_2,c_3\in\mathcal{C}$ corresponding to the elements $(x_1,0,0)\in\mathcal{C}_1\oplus\{0\}\oplus\{0\},(0,x_2,0)\in\{0\}\oplus\mathcal{C}_2\oplus\{0\},(0,0,x_3)\in\{0\}\oplus\{0\}\oplus\mathcal{C}_3$ are given by $c_1=(b+x+b^2x^2+bx^3+x^4,b+x+b^2x^2+bx^3+x^4), c_2=(b^2+x+b^2x^2+b^2x^3,b^2+x+b^2x^2+b^2x^3)$ and $c_3=(b^2+bx+b^2x^2+x^4,b^2+bx+b^2x^2+x^4)$, respectively. Here it easy to see that $wt_L^B(c_1)=14\not\equiv 0\ (mod\ 4)$ and $wt_L^B(c_2)=wt_L^B(c_3)=10\not\equiv 0\ (mod\ 4)$. This shows that the Lee weights (with respect to the basis B) of the codewords of $\mathcal{C}$ corresponding to the elements of $\mathcal{C}_1\oplus\{0\}\oplus\{0\},\{0\}\oplus\mathcal{C}_2\oplus\{0\}$ and $\{0\}\oplus\{0\}\oplus\mathcal{C}_3$ need not be multiples of 4. This shows that Lemma 6.4.3 does not hold when $\lambda_i\neq 1$ for some integer i satisfying $1\leq i\leq\ell$.

Now in the following theorem, we assume that $\lambda_i=1$ for $1\leq i\leq\ell$, and we derive necessary and sufficient conditions under which a Euclidean self-dual Λ-MT code of length n over $\mathbb{F}_{2^r}$ is a Type II code.

Theorem 6.4.4. *Let $\mathcal{C}$ be a Euclidean self-dual Λ-MT code of length n over $\mathbb{F}_{2^r}$. Let $\lambda_i=1$ for $1\leq i\leq\ell$, and let $\mathcal{C}_1$ be the constituent of $\mathcal{C}$ corresponding to the irreducible factor $g_1(x)=x-1$. Suppose that there is an odd integer n' satisfying $n_i\equiv n'\ (mod\ 4)$ for all $i\in U_1$. Then the code $\mathcal{C}$ is a Type II code over $\mathbb{F}_{2^r}$ if and only if the Lee weight of each word in the constituent $\mathcal{C}_1$ is a multiple of 4.*

Proof. To prove the result, it suffices to show that $wt_L^B(c)\equiv 0\ (\text{mod } 4)$ for all $c\in\mathcal{C}$ if and only if $wt_L^B(x_1)\equiv 0\ (\text{mod } 4)$ for all $x_1\in\mathcal{C}_1$.

To do this, let $c\in\mathcal{C}$ be fixed arbitrarily. As $\mathcal{C}\simeq\bigoplus_{w=1}^{\rho}\mathcal{C}_w$, in view of Theorem 6.3.2, we see that there exist $x_1\in\mathcal{C}_1$, $x_2\in\mathcal{C}_2,\cdots,x_\rho\in\mathcal{C}_\rho$ such that c is the codeword

corresponding to the element $(x_1, x_2, \cdots, x_\rho) \in \bigoplus_{w=1}^{\rho} \mathcal{C}_w$. We further note that

$$(x_1, x_2, \cdots, x_\rho) = (x_1, 0, \cdots, 0) + (0, x_2, 0, \cdots, 0) + \cdots + (0, 0, \cdots, 0, x_\rho).$$

Now for $1 \leq w \leq \rho$, by Theorem 6.3.2 again, let $c_w \in \mathcal{C}$ be the codeword corresponding to the element $(0, \cdots, 0, x_w, 0, \cdots, 0) \in \{0\} \oplus \cdots \oplus \{0\} \oplus \mathcal{C}_w \oplus \{0\} \oplus \cdots \oplus \{0\}$. Since $\mathcal{C} \simeq \bigoplus_{w=1}^{\rho} \mathcal{C}_w$, we must have $c = c_1 + c_2 + \cdots + c_\rho$. Next as $\mathcal{C}$ is a Euclidean self-dual Λ-MT code, by Lemma 6.4.2, we see that $wt_L^B(c) \equiv \sum_{w=1}^{\rho} wt_L^B(c_w) \pmod 4$. Further, by Lemma 6.4.3, we note that $wt_L^B(c_w) \equiv 0 \pmod 4$ for $2 \leq w \leq \rho$. From this, we obtain

$$wt_L^B(c) \equiv wt_L^B(c_1) \pmod 4,$$

where c_1 is the codeword of $\mathcal{C}$ corresponding to the element $(x_1, 0, \cdots, 0)$ of the direct sum $\mathcal{C}_1 \oplus \{0\} \oplus \cdots \oplus \{0\}$. Now by applying Lemma 6.4.1, the desired result follows immediately. □

In the following example, we illustrate the above theorem to find a Type II MT code over $\mathbb{F}_2$.

Example 6.4.2. *Let $q = 2$, $\ell = 2$, $m_1 = 20$, $m_2 = 4$, and let $\Lambda = (1, 1)$. Here we have $V = \frac{\mathbb{F}_2[x]}{\langle x^{20}-1\rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^4-1\rangle}$. Let us take $g_1(x) = x - 1$ and $g_2(x) = 1 + x + x^2 + x^3 + x^4$. Now let $\mathcal{C}$ be a 1-generator Λ-MT code of length 24 over $\mathbb{F}_2$ with the generating set $\{(x^3 + x^4 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{16} + x^{17}, 1 + x^2 + x^3)\}$. Let $\mathcal{C}_1$ be the constituent of $\mathcal{C}$ corresponding to the irreducible factor $g_1(x) = x - 1$ of the polynomials $x^{20} - 1$ and $x^4 - 1$ in $\mathbb{F}_2[x]$. It is easy to see that $\mathcal{C}_1 = \langle (1 + u^2, 1 + u + u^3) \rangle$ is a linear code of length 2 over $\mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2 + u^3\mathbb{F}_2$, where $u^4 = 0$. Since $q = 2$, we note that $B = \{1\}$ is the trace-orthogonal basis of $\mathbb{F}_2$ over $\mathbb{F}_2$, which implies that $wt_L^B(0) = 0$ and $wt_L^B(1) = 1$, (i.e., the Lee weight is the same as the Hamming weight here). By using the Magma Computational Algebra System, we see that the code $\mathcal{C}$ is a self-dual Λ-MT code of length 24 over $\mathbb{F}_2$ and that the Lee weight of each word of*

the constituent $\mathcal{C}_1$ is a multiple of 4. Now by applying Theorem 6.4.4, we see that the code $\mathcal{C}$ is a Type II code over $\mathbb{F}_2$.

6.5 Generating sets of MT codes and their Galois duals

Let $\mathcal{C}(\subseteq V)$ be a Λ-MT code of length n over $\mathbb{F}_q$. A set $S = \{y_1(x), y_2(x), \cdots, y_\varrho(x)\}$ consisting of the codewords of $\mathcal{C}$ is called a generating set of the code $\mathcal{C}$ if each codeword $c(x) \in \mathcal{C}$ can be expressed as $c(x) = f_1(x)y_1(x) + f_2(x)y_2(x) + \cdots + f_\varrho(x)y_\varrho(x)$ for some $f_1(x), f_2(x), \cdots, f_\varrho(x) \in \mathbb{F}_q[x]$, and we write $\mathcal{C} = \langle y_1(x), y_2(x), \cdots, y_\varrho(x)\rangle$. The code $\mathcal{C}$ is called a ϱ-generator code if ϱ is the cardinality of a minimal generating set of the code $\mathcal{C}$.

Furthermore, a generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ of the code $\mathcal{C}$ is called a normalized generating set of the code $\mathcal{C}$ if it satisfies exactly one of the following two conditions for each integer i satisfying $1 \le i \le \ell$:

I. $b_i(x) = (0, 0, \cdots, 0) \in V$ when there does not exist a codeword $c(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ in $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$.

II. $b_i(x) = (F_{i,1}(x), F_{i,2}(x), \cdots, F_{i,i}(x), 0, \cdots, 0)$, where $F_{i,i}(x)(\neq 0) \in V_i$ is a monic polynomial satisfying $\deg F_{i,i}(x) \le \deg c_{i,i}(x)$ for all the codewords $c(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ of $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$.

Now in the following theorem, we will show that each Λ-MT code of length n over $\mathbb{F}_q$ has a normalized generating set. It also extends Theorem 2.1 of Bae et al. [9].

Theorem 6.5.1. *Every Λ-MT code of length n over $\mathbb{F}_q$ has a normalized generating set.*

Proof. To prove the result, let $\mathcal{C}(\subseteq V)$ be a Λ-MT code of length n over $\mathbb{F}_q$. Now for $1 \leq i \leq \ell$, let us take $b_i(x) = (0, 0, \cdots, 0) \in \mathcal{C}$ if there does not exist a codeword in $\mathcal{C}$ of the form $c_i(x) = (c_{i,1}(x), c_{i,2}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ with $c_{i,i}(x) \neq 0$, otherwise take $b_i(x) = (F_{i,1}(x), F_{i,2}(x), \cdots, F_{i,i}(x), 0, \cdots, 0)$, where $F_{i,i}(x)(\neq 0) \in V_i$ is a monic polynomial satisfying $\deg F_{i,i}(x) \leq \deg c_{i,i}(x)$ for all the codewords $c_i(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0) \in \mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$. We will show that $\mathcal{C} = \langle b_1(x), b_2(x), \cdots, b_\ell(x) \rangle$.

For this, let $1 \leq i \leq \ell$ be fixed, and let $d_i(x) = (d_{i,1}(x), d_{i,2}(x), \cdots, d_{i,i}(x), 0, \cdots, 0)$ be an arbitrary codeword of $\mathcal{C}$ with $d_{i,i}(x)(\neq 0) \in V_i$. Here we assert that $F_{i,i}(x)$ divides $d_{i,i}(x)$ in $\mathbb{F}_q[x]$. To prove the assertion, by the division algorithm in $\mathbb{F}_q[x]$, there exist unique polynomials $q_i(x), r_i(x) \in \mathbb{F}_q[x]$ satisfying $d_{i,i}(x) = q_i(x)F_{i,i}(x) + r_i(x)$, where either $r_i(x) = 0$ or $\deg r_i(x) < \deg F_{i,i}(x)$. If $r_i(x) \neq 0$, then there exists a codeword $d_i(x) - q_i(x)b_i(x) = (d_{i,1}(x) - q_i(x)F_{i,1}(x), d_{i,2}(x) - q_i(x)F_{i,2}(x), \cdots, d_{i,i-1}(x) - q_i(x)F_{i,i-1}(x), r_i(x), 0, \cdots, 0)$ in $\mathcal{C}$ with $\deg r_i(x) < \deg F_{i,i}(x)$, which is a contradiction. So we must have $r_i(x) = 0$, from which the assertion follows immediately.

Now let $c(x) = (c_1(x), c_2(x), \cdots, c_\ell(x)) \in \mathcal{C}$ be an arbitrary non-zero codeword. Let j be the largest integer satisfying $1 \leq j \leq \ell$ and $c_j(x)(\neq 0) \in V_j$. Then we have $c(x) = (c_1(x), c_2(x), \cdots, c_j(x), 0, \cdots, 0)$. Here we will show that

$$c(x) = f_1(x)b_1(x) + f_2(x)b_2(x) + \cdots + f_j(x)b_j(x) \tag{6.18}$$

for some $f_1(x), f_2(x), \cdots, f_j(x) \in \mathbb{F}_q[x]$. To prove this, we will apply induction on $j \geq 1$. When $j = 1$, we have $c(x) = (c_1(x), 0, \cdots, 0) \in \mathcal{C}$, where $c_1(x)(\neq 0) \in V_1$. By the above assertion, we see that $F_{1,1}(x)$ divides $c_1(x)$ in $\mathbb{F}_q[x]$, which implies that $c_1(x) = f_1(x)F_{1,1}(x)$, where $f_1(x) \in \mathbb{F}_q[x]$. This implies that $c(x) = (f_1(x)F_{1,1}(x), 0, \cdots, 0) = f_1(x)b_1(x)$. Hence equation (6.18) holds when $j = 1$. Now let $h \geq 2$ be an integer, and let us suppose that equation (6.18) holds for $1 \leq j \leq h - 1$. We will now show that the equation (6.18) holds when $j = h$.

For this, let $c(x) = (c_1(x), c_2(x), \cdots, c_h(x), 0, \cdots, 0) \in \mathcal{C}$, where $c_h(x)(\neq 0) \in V_h$. By the above assertion again, we see that $F_{h,h}(x)$ divides $c_h(x)$ in $\mathbb{F}_q[x]$, which implies that $c_h(x) = f_h(x)F_{h,h}(x)$ for some $f_h(x) \in \mathbb{F}_q[x]$. Further, we observe that $c(x) - f_h(x)b_h(x) = (c_1(x) - f_h(x)F_{h,1}(x), c_2(x) - f_h(x)F_{h,2}(x), \cdots, c_{h-1}(x) - f_h(x)F_{h,h-1}(x), 0, \cdots, 0) = d(x)(\text{say}) \in \mathcal{C}$. If $d(x) = 0$, then we have $c(x) = f_h(x)b_h(x)$. On the other hand, if $d(x)(\neq 0) \in \mathcal{C}$, then by the induction hypothesis, we see that there exist $f_1(x), f_2(x), \cdots, f_{h-1}(x) \in \mathbb{F}_q[x]$ such that $c(x) - f_h(x)b_h(x) = d(x) = f_1(x)b_1(x) + f_2(x)b_2(x) + \cdots + f_{h-1}(x)b_{h-1}(x)$, where $f_1(x), f_2(x), \cdots, f_{h-1}(x) \in \mathbb{F}_q[x]$. From this, we get $c(x) = f_1(x)b_1(x) + f_2(x)b_2(x) + \cdots + f_h(x)b_h(x)$, which proves equation (6.18) when $j = h$.

Now by (6.18), the desired result follows immediately. □

We further observe the following:

Lemma 6.5.2. *Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ having a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ satisfying conditions I and II. If $b_i(x)$ is non-zero for some integer i satisfying $1 \leq i \leq \ell$, then $F_{i,i}(x)$ divides $x^{m_i} - \lambda_i$ in $\mathbb{F}_q[x]$.*

Proof. To prove the result, let $1 \leq i \leq \ell$ be fixed. By the division algorithm in $\mathbb{F}_q[x]$, there exist unique polynomials $Q_i(x), R_i(x) \in \mathbb{F}_q[x]$ such that $x^{m_i} - \lambda_i = Q_i(x)F_{i,i}(x) + R_i(x)$, where either $R_i(x) = 0$ or $\deg R_i(x) < \deg F_{i,i}(x)$. From this, it follows that $Q_i(x)F_{i,i}(x) = -R_i(x)$ in V_i. Now we see that $Q_i(x)b_i(x)$ is a codeword of $\mathcal{C}$ and that $Q_i(x)b_i(x) = (Q_i(x)F_{i,1}(x), Q_i(x)F_{i,2}(x), \cdots, Q_i(x)F_{i,i-1}(x), Q_i(x)F_{i,i}(x), 0, \cdots, 0) = (Q_i(x)F_{i,1}(x), Q_i(x)F_{i,2}(x), \cdots, Q_i(x)F_{i,i-1}(x), -R_i(x), 0, \cdots, 0)$. If $R_i(x)$ is a non-zero polynomial in V_i, then $\deg R_i(x) < \deg F_{i,i}(x)$ and $Q_i(x)b_i(x) = (Q_i(x)F_{i,1}(x), Q_i(x)F_{i,2}(x), \cdots, Q_i(x)F_{i,i-1}(x), -R_i(x), 0, \cdots, 0) \in \mathcal{C}$, which contradicts our choice of $F_{i,i}(x)$. Therefore we must have $R_i(x) = 0$, which implies that $F_{i,i}(x)$ divides $x^{m_i} - \lambda_i$ in $\mathbb{F}_q[x]$. □

Further, a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ (satisfying conditions I and II) of the Λ-MT code $\mathcal{C}$ is said to be nice if for $i + 1 \leq j \leq \ell$, either

$F_{j,i}(x) = 0$ or $\deg F_{j,i}(x) < \deg F_{i,i}(x)$, where $1 \leq i \leq \ell$.

In the following theorem, we show that each Λ-MT code of length n over $\mathbb{F}_q$ has a unique nice normalized generating set.

Theorem 6.5.3. *Every Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ has a unique nice normalized generating set.*

Proof. By Theorem 6.5.1, we see that the code $\mathcal{C}$ has a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ satisfying conditions I and II. Now to produce a nice normalized generating set for the code $\mathcal{C}$, let us take $d_1(x) = b_1(x)$. Further, if $b_1(x)(\neq 0) \in V_1$, then by applying the division algorithm in $\mathbb{F}_q[x]$, we see that there exist unique polynomials $Q_{2,1}(x), R_{2,1}(x) \in \mathbb{F}_q[x]$ such that $F_{2,1}(x) = Q_{2,1}(x)F_{1,1}(x) + R_{2,1}(x)$, where either $R_{2,1}(x) = 0$ or $\deg R_{2,1}(x) < \deg F_{1,1}(x)$.

Now let us define

$$d_2(x) = b_2(x) - Q_{2,1}(x)b_1(x) = (R_{2,1}(x), F_{2,2}(x), 0, \cdots, 0).$$

Further, if $b_2(x)(\neq 0) \in V_2$, then by applying the division algorithm in $\mathbb{F}_q[x]$, there exist unique polynomials $Q_{3,2}(x), R_{3,2}(x) \in \mathbb{F}_q[x]$ such that $F_{3,2}(x) = Q_{3,2}(x)F_{2,2}(x)+ R_{3,2}(x)$, where either $R_{3,2}(x) = 0$ or $\deg R_{3,2}(x) < \deg F_{2,2}(x)$. Moreover, if $b_1(x) \neq 0$, then for $F_{3,1}(x) - Q_{3,2}(x)F_{2,1}(x) \in \mathbb{F}_q[x]$, by the division algorithm in $\mathbb{F}_q[x]$, there exist unique polynomials $Q_{3,1}(x), R_{3,1}(x) \in \mathbb{F}_q[x]$ such that $F_{3,1}(x)-Q_{3,2}(x)F_{2,1}(x) = Q_{3,1}(x)F_{1,1}(x) + R_{3,1}(x)$, where either $R_{3,1}(x) = 0$ or $\deg R_{3,1}(x) < \deg F_{1,1}(x)$.

Now let

$$d_3(x) = b_3(x) - Q_{3,2}(x)b_2(x) - Q_{3,1}(x)b_1(x) = (R_{3,1}(x), R_{3,2}(x), F_{3,3}(x), 0, \cdots, 0).$$

Further, proceeding like this for $2 \leq i \leq \ell$ and $1 \leq j \leq i-1$, and by applying the division algorithm again, we can recursively choose unique polynomials

$Q_{i,j}(x), R_{i,j}(x) \in \mathbb{F}_q[x]$ such that

$$F_{i,j}(x) - Q_{i,i-1}(x)F_{i-1,j}(x) - \cdots - Q_{i,j+1}(x)F_{j+1,j}(x) = Q_{i,j}(x)F_{j,j}(x) + R_{i,j}(x),$$

where either $R_{i,j}(x) = 0$ or $\deg R_{i,j}(x) < \deg\, F_{j,j}(x)$.

Furthermore, for $3 \leq i \leq \ell$, let us define

$$\begin{aligned} d_i(x) &= b_i(x) - Q_{i,i-1}(x)b_{i-1}(x) - \cdots - Q_{i,1}(x)b_1(x) \\ &= (R_{i,1}(x), R_{i,2}(x), \cdots, R_{i,i-1}(x), F_{i,i}(x), 0, \cdots, 0). \end{aligned}$$

Now it is easy to observe that the set $\{d_1(x), d_2(x), \cdots, d_\ell(x)\}$ is a nice normalized generating set of the code $\mathcal{C}$.

Next let $\{t_1(x), t_2(x), \cdots, t_\ell(x)\}$ be another nice normalized generating set of the code $\mathcal{C}$ satisfying exactly one of the following two conditions:

A. $t_i(x) = (0, 0, \cdots, 0) \in V$ when there does not exist a codeword $c_i(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ in $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$.

B. $t_i(x) = (H_{i,1}(x), H_{i,2}(x), \cdots, H_{i,i}(x), 0, \cdots, 0)$, where $H_{i,i}(x)(\neq 0) \in V_i$ is a monic polynomial satisfying $\deg H_{i,i}(x) \leq \deg c_{i,i}(x)$ for all the codewords $c_i(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ of $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$, and for $i+1 \leq j \leq \ell$, either $H_{j,i}(x) = 0$ or $\deg H_{j,i}(x) < \deg H_{i,i}(x)$, where $1 \leq i \leq \ell$.

Now we will show that $d_i(x) = t_i(x)$ for $1 \leq i \leq \ell$. Towards this, let $1 \leq i \leq \ell$ be fixed.

If there does not exist any codeword $c_i(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ in $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$, then we have $d_i(x) = (0, 0, \cdots, 0) = t_i(x)$.

Now suppose that there exists a codeword $c_i(x) = (c_{i,1}(x), \cdots, c_{i,i}(x), 0, \cdots, 0)$ in $\mathcal{C}$ with $c_{i,i}(x)(\neq 0) \in V_i$. In this case, we note that $d_i(x) = (R_{i,1}(x), R_{i,2}(x), \cdots, R_{i,i-1}(x), F_{i,i}(x), 0, \cdots, 0)$ and $t_i(x) = (H_{i,1}(x), H_{i,2}(x), \cdots, H_{i,i-1}(x), H_{i,i}(x), 0, \cdots$

$\cdots, 0)$. We also note that both $F_{i,i}(x), H_{i,i}(x)$ are monic polynomials in $\mathbb{F}_q[x]$ of the same degree.

If $F_{i,i}(x) - H_{i,i}(x)(\neq 0) \in V_i$, then deg $(F_{i,i}(x) - H_{i,i}(x)) <$ deg $F_{i,i}(x)$. This implies that there exists a non-zero codeword $d_i(x) - t_i(x) = (R_{i,1}(x) - H_{i,1}(x), R_{i,2}(x) - H_{i,2}(x), \cdots, R_{i,i-1}(x) - H_{i,i-1}(x), F_{i,i}(x) - H_{i,i}(x), 0, \cdots, 0)$ in the code $\mathcal{C}$ satisfying deg $(F_{i,i}(x) - H_{i,i}(x)) <$ deg $F_{i,i}(x)$, which contradicts our choice of $F_{i,i}(x)$.

Therefore we must have $F_{i,i}(x) = H_{i,i}(x)$, which gives $d_i(x) - t_i(x) = (R_{i,1}(x) - H_{i,1}(x), R_{i,2}(x) - H_{i,2}(x), \cdots, R_{i,i-1}(x) - H_{i,i-1}(x), 0, 0, \cdots, 0) \in \mathcal{C}$. Here we assert that

$$R_{i,j}(x) = H_{i,j}(x) \text{ for } \ 1 \leq j \leq i-1. \tag{6.19}$$

Suppose, on the contrary, that the assertion (6.19) is not true. Let $1 \leq k \leq i-1$ be the largest integer such that $R_{i,k}(x) - H_{i,k}(x) \neq 0$. Then we note that $d_i(x) - t_i(x) = (R_{i,1}(x) - H_{i,1}(x), R_{i,2}(x) - H_{i,2}(x), \cdots, R_{i,k}(x) - H_{i,k}(x), 0, 0, \cdots, 0) \in \mathcal{C}$ and deg $(R_{i,k}(x) - H_{i,k}(x)) <$ deg $F_{k,k}(x)$, which contradicts our choice of $F_{k,k}(x)$.

Now by the assertion (6.19), we get $d_i(x) = t_i(x)$ for $1 \leq i \leq \ell$, which completes the proof of the theorem. □

In the following corollary, we explicitly determine the dimension of each Λ-MT code of length n over $\mathbb{F}_q$.

Corollary 6.5.4. *If $\mathcal{C}$ is a Λ-MT code of length n over $\mathbb{F}_q$ with a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ satisfying conditions I and II, then we have*

$$dim_{\mathbb{F}_q}\mathcal{C} = \sum_{i=1}^{\ell} (m_i - deg\ F_{i,i}(x)).$$

(Here we take $F_{i,i}(x) = x^{m_i} - \lambda_i$ if $F_{i,i}(x) = 0 \in V_i$ for $1 \leq i \leq \ell$.)

Proof. One can easily show that the set $\{x^j b_i(x) : 0 \leq j < m_i - \text{deg } F_{i,i}(x) \text{ and } 1 \leq i \leq \ell\}$ is a basis set of $\mathcal{C}$ over $\mathbb{F}_q$. From this, the desired result follows immediately. □

Now we proceed to explicitly determine a generating set of the k-Galois dual code of each Λ-MT code of length n over $\mathbb{F}_q$ from its normalized generating set. For this, let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$, and let $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ be a normalized generating set of the code $\mathcal{C}$ satisfying conditions I and II. From this point on, we shall take $F_{i,i}(x) = x^{m_i} - \lambda_i$ when $F_{i,i}(x) = 0$ in V_i for $1 \leq i \leq \ell$. Now for $1 \leq \eta \leq \ell$, let us define

$$\begin{aligned} A^{(0)}_{\eta,\eta}(x) &= F^{(0)}_{\eta,\eta}(x) = F_{\eta,\eta}(x), \quad B^{(0)}_{\eta,\eta}(x) = 0 \text{ and} \\ b^{(0)}_{\eta}(x) &= (F^{(0)}_{\eta,1}(x), F^{(0)}_{\eta,2}(x), \cdots, F^{(0)}_{\eta,\eta}(x), 0, \cdots, 0) = b_\eta(x). \end{aligned}$$

Further, for $2 \leq \eta \leq \ell$ and $1 \leq i \leq \eta - 1$, let us define

$$b^{(i)}_{\eta}(x) = A^{(i)}_{\eta,\eta-i}(x) b^{(i-1)}_{\eta}(x) - B^{(i)}_{\eta,\eta-i}(x) b_{\eta-i}(x) = (F^{(i)}_{\eta,1}(x), F^{(i)}_{\eta,2}(x), \cdots, F^{(i)}_{\eta,\eta}(x), 0, \cdots, 0),$$

where $A^{(i)}_{\eta,\eta-i}(x) = \dfrac{F^{(0)}_{\eta-i,\eta-i}(x)}{\gcd(F^{(0)}_{\eta-i,\eta-i}(x), F^{(i-1)}_{\eta,\eta-i}(x))}$ and $B^{(i)}_{\eta,\eta-i}(x) = \dfrac{F^{(i-1)}_{\eta,\eta-i}(x)}{\gcd(F^{(0)}_{\eta-i,\eta-i}(x), F^{(i-1)}_{\eta,\eta-i}(x))}$.

Next it is easy to observe that

$$F^{(i)}_{\eta,\eta}(x) = A^{(0)}_{\eta,\eta}(x) A^{(1)}_{\eta,\eta-1}(x) \cdots A^{(i)}_{\eta,\eta-i}(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } \mathbb{F}_q[x]$$

and

$$F^{(i)}_{\eta,j}(x) = 0$$

for $2 \leq \eta \leq \ell, 1 \leq i \leq \eta - 1$ and $\eta - i \leq j \leq \eta - 1$. Then we make the following observation.

Lemma 6.5.5. *For $1 \leq i \leq \ell$, let us take $F_{i,i}(x) = x^{m_i} - \lambda_i$ when $F_{i,i}(x) = 0$ in V_i. For $2 \leq \eta \leq \ell$ and $1 \leq i \leq \eta - 1$, the following hold.*

(a) $$\frac{B^{(\eta-i)}_{\eta,i}(x)}{A^{(\eta-i)}_{\eta,i}(x) A^{(\eta-i-1)}_{\eta,i+1}(x) \cdots A^{(1)}_{\eta,\eta-1}(x)} = \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta-1,i}(x) B^{(1)}_{\eta,\eta-1}(x)}{F_{i,i}(x) A^{(1)}_{\eta,\eta-1}(x)} - \cdots - \frac{F_{i+1,i}(x) B^{(\eta-i-1)}_{\eta,i+1}(x)}{F_{i,i}(x) A^{(\eta-i-1)}_{\eta,i+1}(x) A^{(\eta-i-2)}_{\eta,i+2}(x) \cdots A^{(1)}_{\eta,\eta-1}(x)}.$$

$$(b)\frac{B_{\eta,i}^{(\eta-i)}(x)}{A_{\eta,i}^{(\eta-i)}(x)A_{\eta,i+1}^{(\eta-i-1)}(x)\cdots A_{\eta,\eta-1}^{(1)}(x)} = \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta,i+1}(x)B_{i+1,i}^{(1)}(x)}{F_{i+1,i+1}^{(1)}(x)} - \cdots - \frac{F_{\eta,\eta-1}(x)B_{\eta-1,i}^{(\eta-i-1)}(x)}{F_{\eta-1,\eta-1}^{(\eta-i-1)}(x)}.$$

Proof. (a) To prove this, for $2 \leq \eta \leq \ell$, we see that

$$\begin{aligned} b_{\eta}^{(\eta-2)}(x) &= (F_{\eta,1}^{(\eta-2)}(x), 0, \cdots, 0, F_{\eta,\eta}^{(\eta-2)}(x), 0, \cdots, 0) \\ &= A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots A_{\eta,\eta-1}^{(1)}(x)b_{\eta}(x) - A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots \\ &\quad A_{\eta,\eta-2}^{(2)}(x)B_{\eta,\eta-1}^{(1)}(x)b_{\eta-1}(x) - \cdots - A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)B_{\eta,4}^{(\eta-4)}(x)b_4(x) \\ &\quad -A_{\eta,2}^{(\eta-2)}(x)B_{\eta,3}^{(\eta-3)}(x)b_3(x) - B_{\eta,2}^{(\eta-2)}(x)b_2(x). \end{aligned}$$

This further implies that

$$\begin{aligned} F_{\eta,1}^{(\eta-2)}(x) = {} & A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots A_{\eta,\eta-1}^{(1)}(x)F_{\eta,1}(x) - A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots \\ & A_{\eta,\eta-2}^{(2)}(x)B_{\eta,\eta-1}^{(1)}(x)F_{\eta-1,1}(x) - \cdots - A_{\eta,2}^{(\eta-2)}(x)B_{\eta,3}^{(\eta-3)}(x)F_{3,1}(x) - \\ & B_{\eta,2}^{(\eta-2)}(x)F_{2,1}(x) \end{aligned}$$

and

$$\begin{aligned} F_{\eta,i}^{(\eta-2)}(x) = 0 = {} & A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots A_{\eta,\eta-1}^{(1)}(x)F_{\eta,i}(x) - A_{\eta,2}^{(\eta-2)}(x)A_{\eta,3}^{(\eta-3)}(x)\cdots \\ & A_{\eta,\eta-2}^{(2)}(x)B_{\eta,\eta-1}^{(1)}(x)F_{\eta-1,i}(x) - \cdots - A_{\eta,2}^{(\eta-2)}(x)\cdots A_{\eta,i}^{(\eta-i)}(x) \\ & B_{\eta,i+1}^{(\eta-i-1)}(x)F_{i+1,i}(x) - A_{\eta,2}^{(\eta-2)}(x)\cdots A_{\eta,i-1}^{(\eta-i+1)}(x)B_{\eta,i}^{(\eta-i)}(x)F_{i,i}(x) \end{aligned}$$

for $2 \leq i \leq \eta - 1$. From this, the desired result follows immediately.

(b) To prove (b), let $2 \leq \eta \leq \ell$ be fixed. Here we will apply the strong mathematical induction on $\eta - i$, where $1 \leq i \leq \eta - 1$. Towards this, by part (a), we see that $\frac{B_{\eta,\eta-1}^{(1)}(x)}{A_{\eta,\eta-1}^{(1)}(x)} = \frac{F_{\eta,\eta-1}(x)}{F_{\eta-1,\eta-1}(x)}$, and hence the result holds when $\eta - i = 1$. Further, let $2 \leq \eta \leq \ell$ and $1 \leq i \leq \eta - 1$ be fixed integers, and let us assume

that the result holds for $1 \leq j \leq \eta - i - 1$, i.e., we have

$$\frac{B^{(j)}_{\eta,\eta-j}(x)}{A^{(j)}_{\eta,\eta-j}(x)A^{(j-1)}_{\eta,\eta-j+1}(x)\cdots A^{(1)}_{\eta,\eta-1}(x)} = \frac{F_{\eta,\eta-j}(x)}{F_{\eta-j,\eta-j}(x)} - \frac{F_{\eta,\eta-j+1}(x)B^{(1)}_{\eta-j+1,\eta-j}(x)}{F^{(1)}_{\eta-j+1,\eta-j+1}(x)} - \cdots - \frac{F_{\eta,\eta-1}(x)B^{(j-1)}_{\eta-1,\eta-j}(x)}{F^{(j-1)}_{\eta-1,\eta-1}(x)} \tag{6.20}$$

for $1 \leq j \leq \eta - i - 1$. Now we shall prove the result for $j = \eta - i$, i.e.,

$$\frac{B^{(\eta-i)}_{\eta,i}(x)}{A^{(\eta-i)}_{\eta,i}(x)A^{(\eta-i-1)}_{\eta,i+1}(x)\cdots A^{(1)}_{\eta,\eta-1}(x)} = \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta,i+1}(x)B^{(1)}_{i+1,i}(x)}{F^{(1)}_{i+1,i+1}(x)} - \cdots - \frac{F_{\eta,\eta-1}(x)B^{(\eta-i-1)}_{\eta-1,i}(x)}{F^{(\eta-i-1)}_{\eta-1,\eta-1}(x)}.$$

For this, we see, by part (a) and by (6.20), that

$$\begin{aligned}
&\frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta,i+1}(x)B^{(1)}_{i+1,i}(x)}{F^{(1)}_{i+1,i+1}(x)} - \cdots - \frac{F_{\eta,\eta-1}(x)B^{(\eta-i-1)}_{\eta-1,i}(x)}{F^{(\eta-i-1)}_{\eta-1,\eta-1}(x)} \\
&= \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta,i+1}(x)F_{i+1,i}(x)}{F_{i+1,i+1}(x)F_{i,i}(x)} - \cdots - \frac{F_{\eta,\eta-1}(x)}{F_{\eta-1,\eta-1}(x)}\left(\frac{F_{\eta-1,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta-2,i}(x)B^{(1)}_{\eta-1,\eta-2}(x)}{F_{i,i}(x)A^{(1)}_{\eta-1,\eta-2}(x)}\right. \\
&\quad \left. - \cdots - \frac{F_{i+1,i}(x)B^{(\eta-i-2)}_{\eta-1,i+1}(x)}{F_{i,i}(x)A^{(\eta-i-2)}_{\eta-1,i+1}(x)A^{(\eta-i-3)}_{\eta-1,i+2}(x)\cdots A^{(1)}_{\eta-1,\eta-2}(x)}\right) \\
&= \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta-1,i}(x)F_{\eta,\eta-1}(x)}{F_{i,i}(x)F_{\eta-1,\eta-1}(x)} - \cdots - \frac{F_{i+1,i}(x)}{F_{i,i}(x)}\left(\frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta,i+1}(x)B^{(1)}_{i+1,i}(x)}{F_{i+1,i+1}(x)A^{(1)}_{i+1,i}(x)} - \right. \\
&\quad \left. \cdots - \frac{F_{\eta,\eta-1}(x)B^{(\eta-i-1)}_{\eta-1,i}(x)}{F_{\eta-1,\eta-1}(x)A^{(\eta-i-1)}_{\eta-1,i}(x)A^{(\eta-i-2)}_{\eta-1,i+1}(x)\cdots A^{(1)}_{\eta-1,\eta-2}(x)}\right) \\
&= \frac{F_{\eta,i}(x)}{F_{i,i}(x)} - \frac{F_{\eta-1,i}(x)B^{(1)}_{\eta,\eta-1}(x)}{F_{i,i}(x)A^{(1)}_{\eta,\eta-1}(x)} - \cdots - \frac{F_{i+1,i}(x)B^{(\eta-i-1)}_{\eta,i+1}(x)}{F_{i,i}(x)A^{(\eta-i-1)}_{\eta,i+1}(x)A^{(\eta-i-2)}_{\eta,i+2}(x)\cdots A^{(1)}_{\eta,\eta-1}(x)} \\
&= \frac{B^{(\eta-i)}_{\eta,i}(x)}{A^{(\eta-i)}_{\eta,i}(x)A^{(\eta-i-1)}_{\eta,i+1}(x)\cdots A^{(1)}_{\eta,\eta-1}(x)}.
\end{aligned}$$

Hence the result follows by strong mathematical induction.

□

Bae et al. [9, Th. 3.11] tried to determine a normalized generating set of the Euclidean dual code of a binary GQC code from the normalized generating set of the code. However, we noticed an error in Theorem 3.11 of Bae et al. [9], which we illustrate in the following example.

Example 6.5.1. *Let $q = 2, \ell = 3$ and $m_1 = m_2 = m_3 = 3$. Here we have $V = V_1 \times V_2 \times V_3 = \frac{\mathbb{F}_2[x]}{\langle x^3-1\rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^3-1\rangle} \times \frac{\mathbb{F}_2[x]}{\langle x^3-1\rangle}$. Let $\mathcal{C}$ be a GQC code of length 9 over $\mathbb{F}_2$ with a normalized generating set $\{b_1(x), b_2(x), b_3(x)\}$, where $b_1(x) = (1, 0, 0), b_2(x) = (1, 1 + x + x^2, 0)$ and $b_3(x) = (1, x + 1, x + 1)$. Now by Lemma 3.7, Theorem 3.11 and Example 3.12 of Bae et al. [9], we see that the Euclidean dual code $\mathcal{C}^{\perp_0}$ of the code $\mathcal{C}$ is a GQC code of length 9 over $\mathbb{F}_2$ with a normalized generating set $\{e_1(x), e_2(x), e_3(x)\}$, where $e_1(x) = e_2(x) = (0, 0, 0)$ and $e_3(x) = (0, (x+1)\lambda_{3,2}(x), 1)$ with $\lambda_{3,2}(x) \equiv x^{-1} \pmod 1$. This implies that $\mathcal{C}^{\perp_0} = \langle(0, (x + 1)\lambda_{3,2}(x), 1)\rangle$ for any $\lambda_{3,2}(x) \in \frac{\mathbb{F}_2[x]}{\langle x^3-1\rangle}$. However, one can easily observe that $(0, (x + 1)\lambda_{3,2}(x), 1) \notin \mathcal{C}^{\perp_0}$ whenever $\lambda_{3,2}(x) \not\equiv x \pmod{1+x+x^2}$. This shows that there is an error in Theorem 3.11 of Bae et al. [9], and hence in the method provided by Bae et al. [9] to determine generating sets of the Euclidean dual codes of GQC codes over $\mathbb{F}_2$ from their normalized generating sets.*

Now in the following theorem, we explicitly determine generating sets of the k-Galois duals of all Λ-MT codes over $\mathbb{F}_q$ from normalized generating sets of these codes. It also rectifies errors in Theorem 3.11 of Bae et al. [9] for binary GQC codes.

Theorem 6.5.6. *If $\mathcal{C}$ is a Λ-MT code of length n over $\mathbb{F}_q$ with a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ satisfying conditions I and II, then a generating set of the k-Galois dual code $\mathcal{C}^{\perp_k}$ of the code $\mathcal{C}$ is given by $\{a_1(x), a_2(x), \cdots, a_\ell(x)\}$, where*

$$a_i(x) = (0, \cdots, 0, \mathcal{T}_k^{(i)}(E_{i,i}(x)), \mathcal{T}_k^{(i+1)}(E_{i,i+1}(x)), \cdots, \mathcal{T}_k^{(\ell)}(E_{i,\ell}(x))) \tag{6.21}$$

with $E_{i,i}(x) = \frac{\lambda_i^{-1}(x^{m_i}-\lambda_i)}{F_{i,i}(x)}$ and $E_{i,j} = -\frac{\lambda_j^{-1}(x^{m_j}-\lambda_j)B_{j,i}^{(j-i)}(x)}{F_{j,j}^{(j-i)}(x)}$ for $1 \le i \le \ell$ and

$i < j \leq \ell$. (Here we take $F_{i,i}(x) = x^{m_i} - \lambda_i$ if $F_{i,i}(x) = 0 \in V_i$ for $1 \leq i \leq \ell$.)

Proof. In order to prove this, we will first show that $a_1(x), a_2(x), \cdots, a_\ell(x) \in \mathcal{C}^{\perp_k}$, i.e., $(a_j(x), b_i(x))_k = 0$ for all $1 \leq i, j \leq \ell$. To do this, let $1 \leq i, j \leq \ell$ be fixed.

First of all, for $i \leq j$, one can easily observe that $\{b_i(x), a_j(x)\}_k = 0$.

Next for $j < i$, we consider

$$\begin{aligned}\{b_i(x), a_j(x)\}_k &= E_{j,j}(x)F_{i,j}(x)\lambda_j\Big(\frac{x^m-1}{x^{m_j}-\lambda_j}\Big) + E_{j,j+1}(x)F_{i,j+1}(x)\lambda_{j+1}\Big(\frac{x^m-1}{x^{m_{j+1}}-\lambda_{j+1}}\Big) + \\ &\qquad \cdots + E_{j,i}(x)F_{i,i}(x)\lambda_i\Big(\frac{x^m-1}{x^{m_i}-\lambda_i}\Big) \\ &= \Bigg(\frac{F_{i,j}(x)}{F_{j,j}(x)} - \frac{F_{i,j+1}(x)B^{(1)}_{j+1,j}(x)}{F^{(1)}_{j+1,j+1}(x)} - \cdots - \frac{F_{i,i-1}(x)B^{(i-j-1)}_{i-1,j}(x)}{F^{(i-j-1)}_{i-1,i-1}(x)} \\ &\qquad - \frac{B^{(i-j)}_{i,j}(x)}{A^{(1)}_{i,i-1}(x)\cdots A^{(i-j)}_{i,j}(x)}\Bigg)(x^m-1).\end{aligned}$$

This, by Lemma 6.5.5(b), implies that $\{b_i(x), a_j(x)\}_k = 0$ for $j < i$. Further, by Lemma 6.2.5(b), we get $a_1(x), a_2(x), \cdots, a_\ell(x) \in \mathcal{C}^{\perp_k}$, which further implies that

$$\langle a_1(x), a_2(x), \cdots\cdots, a_\ell(x)\rangle \subseteq \mathcal{C}^{\perp_k}. \tag{6.22}$$

On the other hand, let $(d_1(x), d_2(x), \cdots, d_\ell(x)) \in \mathcal{C}^{\perp_k}$. This, by Theorem 8.3.2 and Lemma 6.2.5(b), implies that

$$\begin{aligned}&F_{1,1}(x)\mathcal{S}^{(1)}_k(d_1(x))\lambda_1\Big(\frac{x^m-1}{x^{m_1}-\lambda_1}\Big) \equiv 0 \pmod{x^m-1}, \\ &F_{2,1}(x)\mathcal{S}^{(1)}_k(d_1(x))\lambda_1\Big(\frac{x^m-1}{x^{m_1}-\lambda_1}\Big) + F_{2,2}(x)\mathcal{S}^{(2)}_k(d_2(x))\lambda_2\Big(\frac{x^m-1}{x^{m_2}-\lambda_2}\Big) \equiv 0 \pmod{x^m-1}, \\ &\quad\vdots \\ &F_{\ell,1}(x)\mathcal{S}^{(1)}_k(d_1(x))\lambda_1\Big(\frac{x^m-1}{x^{m_1}-\lambda_1}\Big) + F_{\ell,2}(x)\mathcal{S}^{(2)}_k(d_2(x))\lambda_2\Big(\frac{x^m-1}{x^{m_2}-\lambda_2}\Big) + \\ &\qquad \cdots + F_{\ell,\ell}(x)\mathcal{S}^{(\ell)}_k(d_\ell(x))\lambda_\ell\Big(\frac{x^m-1}{x^{m_\ell}-\lambda_\ell}\Big) \equiv 0 \pmod{x^m-1}.\end{aligned}$$

From this, we observe that

$$\begin{aligned}
&\mathcal{S}_k^{(1)}(d_1(x)) = y_1(x)E_{1,1}(x),\\
&\mathcal{S}_k^{(2)}(d_2(x)) = y_1(x)E_{1,2}(x) + y_2(x)E_{2,2}(x),\\
&\mathcal{S}_k^{(3)}(d_3(x)) = y_1(x)E_{1,3}(x) + y_2(x)E_{2,3}(x) + y_3(x)E_{3,3}(x),\\
&\vdots\\
&\mathcal{S}_k^{(\ell)}(d_\ell(x)) = y_1(x)E_{1,\ell}(x) + y_2(x)E_{2,\ell}(x) + \cdots + y_\ell(x)E_{\ell,\ell}(x),
\end{aligned}$$

where $y_1(x), y_2(x), \cdots, y_\ell(x) \in \mathbb{F}_q[x]$. This implies that $(\mathcal{S}_k^{(1)}(d_1(x)), \mathcal{S}_k^{(2)}(d_2(x)), \cdots \cdots, \mathcal{S}_k^{(\ell)}(d_\ell(x))) \in \langle (E_{1,1}(x), E_{1,2}(x), \cdots, E_{1,\ell}(x)), (0, E_{2,2}(x), \cdots, E_{2,\ell}(x)), \cdots, (0, 0, \cdots, 0, E_{\ell,\ell}(x))\rangle \subseteq V$. As $\mathcal{T}_k^{(i)}$ is the inverse of $\mathcal{S}_k^{(i)}$ for $1 \leq i \leq \ell$, we see that $(d_1(x), d_2(x), \cdots, d_\ell(x)) \in \langle a_1(x), a_2(x), \cdots, a_\ell(x)\rangle (\subseteq V')$. From this, we obtain

$$\mathcal{C}^{\perp_k} \subseteq \langle a_1(x), a_2(x), \cdots, a_\ell(x)\rangle . \tag{6.23}$$

Now by (6.22) and (6.23), the desired result follows immediately. □

Now we provide an example to illustrate Theorem 6.5.6.

Example 6.5.2. *Let $\mathcal{C}$ be the GQC code of length 9 over $\mathbb{F}_2$ (as considered in Example 6.5.1) with a normalized generating set $\{b_1(x), b_2(x), b_3(x)\}$, where $b_1(x) = (1, 0, 0), b_2(x) = (1, 1 + x + x^2, 0)$ and $b_3(x) = (1, x + 1, x + 1)$. Now by applying Theorem 6.5.6, we see that a generating set of the Euclidean dual code $\mathcal{C}^{\perp_0}$ of the code $\mathcal{C}$ is given by $\{a_1(x), a_2(x), a_3(x)\}$, where $a_1(x) = (0, 1 + x^2, x), a_2(x) = (0, 1 + x^2, 1 + x^2)$ and $a_3(x) = (0, 0, 1 + x + x^2)$. Since $a_1(x) = a_2(x) + a_3(x)$, we see that $\mathcal{C}^{\perp_0} = \langle a_2(x), a_3(x)\rangle$.*

Remark 6.5.7. *(a) Let $\mathcal{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with a normalized generating set $\{b_1(x), b_2(x), \cdots, b_\ell(x)\}$ satisfying conditions I and II. By applying Theorem 6.5.6 and by working in a similar manner as in Theorem 6.5.3,*

one can determine a unique generating set $S = \{R_1(x), R_2(x), \cdots, R_\ell(x)\}$ *for the dual code* $\mathcal{C}^{\perp_k}$ *with* $R_i(x) = (0, \cdots, 0, R_{i,i}(x), R_{i,i+1}(x), \cdots, R_{i,\ell}(x))$, *where* $R_{i,i}(x) = \kappa_i\Big(\mathcal{T}_k^{(i)}\Big(\frac{\lambda_i^{-1}(x^{m_i}-\lambda_i)}{F_{i,i}(x)}\Big)\Big)$ *is a monic polynomial for some* $\kappa_i \in \mathbb{F}_q$ *and either* $R_{j,i}(x) = 0$ *or deg* $R_{j,i}(x) <$ *deg* $R_{i,i}(x)$ *for* $1 \leq j < i \leq \ell$.

(b) The results derived in Section 3.4 can be similarly extended to this generalized family of MT codes over $\mathbb{F}_q$, *whose block lengths* $m_1, m_2, \cdots, m_\ell$ *are arbitrary positive integers, not necessarily coprime to* q.

In the database maintained by Grassl [39], many linear codes with best-known and optimal parameters $[n, k, d_{\min}]$ have been listed over $\mathbb{F}_q$ when $2 \leq q \leq 9$. In Tables 6.1 and 6.2, we also identify several linear codes with best-known and optimal parameters $[n, k, d_{\min}]$ from 1-generator Λ-MT codes over $\mathbb{F}_q$ with the generating set $\{(b_1(x), b_2(x), \cdots, b_\ell(x))\}$ by carrying out computations in the Magma Computational Algebra System, where $2 \leq q \leq 7$. It is worth noting that these code parameters cannot be attained by constacyclic and QT codes. In Tables 6.1 and 6.2, the element $b_i(x) = b_{i,0} + b_{i,1}x + b_{i,2}x^2 + \cdots + b_{i,m_i-1}x^{m_i-1} \in V_i$ is represented by the sequence $b_{i,0}b_{i,1}\cdots b_{i,m_i-1}$ for $1 \leq i \leq \ell$, and b is a primitive element of $\mathbb{F}_4$.

q	$(m_1, m_2, \cdots, m_\ell)$	Λ	$(b_1(x), b_2(x), \cdots, b_\ell(x))$	$[n, k, d_{\min}]$
2	$(21, 1, 1)$	$(1, 1, 1)$	$(10101101010101010110010, 1, 0)$	$[23, 16, 4]$
2	$(21, 1, 1)$	$(1, 1, 1)$	$(10111001111010110100110, 1, 1)$	$[23, 15, 4]$
2	$(15, 5, 3)$	$(1, 1, 1)$	$(010011110111011, 10111, 011)$	$[23, 10, 8]$
2	$(14, 7, 2)$	$(1, 1, 1)$	$(10011010000110, 0010001, 00)$	$[23, 9, 8]$
2	$(14, 7, 2)$	$(1, 1, 1)$	$(10111010111111, 1010011, 10)$	$[23, 8, 8]$
2	$(24, 4, 1)$	$(1, 1, 1)$	$(100111110011110011111100, 1000, 1)$	$[29, 20, 4]$
2	$(21, 7, 1)$	$(1, 1, 1)$	$(001111000001110010011, 1001101, 0)$	$[29, 12, 8]$
2	$(24, 3, 2)$	$(1, 1, 1)$	$(001111110110111100011011, 00110)$	$[29, 21, 4]$
2	$(28, 2, 1)$	$(1, 1, 1)$	$(111000101011110110011000010 0, 11, 0)$	$[31, 22, 4]$
2	$(28, 2, 1)$	$(1, 1, 1)$	$(001011010101011011101101111, 10, 1)$	$[31, 23, 4]$
2	$(28, 2, 1)$	$(1, 1, 1)$	$(111010011101001001011101 1100, 10, 1)$	$[31, 24, 4]$
2	$(20, 10, 1)$	$(1, 1, 1)$	$(0010111010100010 1110, 0111111010, 1)$	$[31, 14, 8]$
2	$(30, 1)$	$(1, 1)$	$(001101100111011101011101010100, 1)$	$[31, 18, 6]$
2	$(35, 2)$	$(1, 1)$	$(11010010000100000110001100010011110, 00)$	$[37, 27, 4]$
2	$(40, 1)$	$(1, 1)$	$(1010111011110001001010001000101001100100, 0)$	$[41, 31, 4]$
2	$(35, 5, 1)$	$(1, 1, 1)$	$(0100001101110001010011001010101 1000, 01100, 0)$	$[41, 32, 4]$
2	$(42, 1)$	$(1, 1)$	$(1110011101001110101110001100001010 11010100, 0)$	$[43, 33, 4]$
2	$(42, 1)$	$(1, 1)$	$(0000011100001010111001111111000011 01110011, 0)$	$[43, 34, 4]$
2	$(42, 1)$	$(1, 1)$	$(0110101100110010111000010111111101 01011111, 0)$	$[43, 35, 4]$
2	$(21, 21, 1)$	$(1, 1, 1)$	$(1010101000110110000 10, 0110110000101 00101101, 1)$	$[43, 21, 10]$
2	$(42, 4, 1)$	$(1, 1, 1)$	$(0110101011010000110000010001101000 00110011, 1100, 1)$	$[47, 37, 4]$
2	$(42, 4, 1)$	$(1, 1, 1)$	$(0111011110111000000011110100000101 10001000, 1100, 0)$	$[47, 38, 4]$
2	$(42, 3, 2)$	$(1, 1, 1)$	$(0011111100011011110101001001101011 10110110, 001, 10)$	$[47, 39, 4]$
3	$(11, 11, 1)$	$(2, 2, 1)$	$(11012110120, 00022201121, 0)$	$[23, 10, 9]$
3	$(11, 11, 1)$	$(2, 2, 2)$	$(22012201200, 11122121102, 2)$	$[23, 11, 9]$
3	$(26, 2, 1)$	$(1, 1, 2)$	$(012211021011022112111 00210, 10, 2)$	$[29, 20, 6]$
3	$(24, 3, 2)$	$(1, 1, 2)$	$(121221120202111212100112, 211, 11)$	$[29, 19, 6]$
5	$(24, 5)$	$(1, 3)$	$(322143404240332412004122, 24224)$	$[29, 5, 3]$
5	$(30, 1)$	$(4, 2)$	$(400032102243414411401230334141, 1)$	$[31, 26, 4]$
7	$(16, 1)$	$(2, 2)$	$(3365356202240515, 6)$	$[17, 13, 4]$
7	$(8, 8, 1)$	$(4, 4, 5)$	$(13460303, 36344311, 2)$	$[17, 8, 8]$

Table 6.1: Linear codes with optimal parameters $[n, k, d_{\min}]$ over $\mathbb{F}_q$ obtained as 1-generator Λ-MT codes

q	$(m_1, m_2, \cdots, m_\ell)$	Λ	$(b_1(x), b_2(x), \cdots, b_\ell(x))$	$[n, k, d_{\min}]$
2	$(33, 2, 2)$	$(1, 1, 1)$	$(00101011101110010001001010110101110,$ $11, 11)$	$[37, 23, 6]$
2	$(30, 5, 2)$	$(1, 1, 1)$	$(11001000101101101000001011010 0,$ $00110, 10)$	$[37, 18, 8]$
2	$(18, 18, 1)$	$(1, 1, 1)$	$(100000001101110110,$ $011011001111000110, 1)$	$[37, 15, 10]$
2	$(20, 20, 1)$	$(1, 1, 1)$	$(10000000111001000111,$ $11000010001111010011, 0)$	$[41, 19, 10]$
2	$(28, 14, 1)$	$(1, 1, 1)$	$(10001101011001001010000 10110,$ $10110011001010, 1)$	$[43, 23, 8]$
2	$(21, 21, 1)$	$(1, 1, 1)$	$(000001010000100111111,$ $101111100100101000000, 1)$	$[43, 16, 12]$
2	$(30, 15, 2)$	$(1, 1, 1)$	$(10010100101111111110010110010 01,$ $111000000101111, 10)$	$[47, 26, 8]$
2	$(42, 8, 3)$	$(1, 1, 1)$	$(10001110110010100001110111111001 11$ $110110000, 01111000, 101)$	$[53, 42, 4]$
3	$(14, 14, 1)$	$(2, 2, 1)$	$(22020002020202, 00001022110010, 0)$	$[29, 14, 9]$
3	$(24, 4, 1)$	$(1, 2, 1)$	$(10202021000211200020210 2, 0201, 1)$	$[29, 22, 4]$
3	$(20, 5, 4)$	$(1, 2, 1)$	$(11211020200200001200, 11222, 2022)$	$[29, 15, 8]$
3	$(24, 4, 1)$	$(1, 1, 2)$	$(20012110102022012101 2120, 2021, 2)$	$[29, 18, 6]$
3	$(14, 14, 1)$	$(1, 1, 2)$	$(21121011001201, 12221202100101, 1)$	$[29, 14, 9]$
3	$(24, 4, 3)$	$(1, 2, 1)$	$(21122011202110221022 1110, 0012, 200)$	$[31, 20, 6]$
3	$(24, 4, 3)$	$(1, 2, 1)$	$(02112222221221021122 0122, 0202, 212)$	$[31, 24, 4]$
4	$(9, 9, 1)$	$(1, 1, b^2)$	$(b^2 1 b^2 0 b 11 b 1, 010 b^2 b^2 0100, 1)$	$[19, 8, 8]$
4	$(7, 7, 7, 2)$	$(1, 1, 1, 1)$	$(bb10000, 10b1b1b^2, 1b^2bb^2b^2b^2b^2, b^2b^2)$	$[23, 7, 12]$
4	$(20, 2, 1)$	(b, b, b^2)	$(b^2b^2001b^2bb01b^21b^210b^2bbb^21, 10, b^2)$	$[23, 17, 4]$
4	$(18, 18, 1)$	$(1, 1, b^2)$	$(011bb^2b^2bb1b11b11b00,$ $000bbb^2bb11b0b1bbb^2b, b^2)$	$[37, 17, 12]$
5	$(11, 11, 1)$	$(3, 3, 2)$	$(41013412110, 34442312433, 3)$	$[23, 11, 9]$
5	$(20, 5, 4)$	$(1, 1, 1)$	$(20410204030400122031, 40023, 3414)$	$[29, 17, 8]$
7	$(16, 2, 1)$	$(1, 6, 1)$	$(5332356045155140, 63, 5)$	$[19, 14, 4]$
7	$(21, 1, 1)$	$(1, 2, 4)$	$(6326222521456610232 30, 5, 5)$	$[23, 18, 4]$

Table 6.2: Linear codes with best-known parameters $[n, k, d_{\min}]$ over $\mathbb{F}_q$ obtained as 1-generator Λ-MT codes

7

Hamming weight distributions of multi-twisted codes over finite fields

7.1 Introduction

Let $\mathbb{F}_q$ denote the finite field of order q, and let $n = m_1 + m_2 + \cdots + m_\ell$, where $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers (not necessarily coprime to q). Let

$\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. In this chapter, we shall explicitly determine Hamming weights of all non-zero codewords of several classes of Λ-multi-twisted (Λ-MT) codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$. Using these results, we shall explicitly determine Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights, which have applications in constructing strongly regular graphs, association schemes and authentication codes. We shall also identify two classes of optimal equidistant Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ meeting the Griesmer as well as Plotkin bounds, which have nice connections with projective geometry and combinatorial designs and are useful in constructing distributed storage systems. Besides this, we shall obtain three different classes of few weight Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$, which are useful in constructing secret sharing schemes with nice access structures.

This chapter is organized as follows: In Section 7.2, we explicitly determine Hamming weights of all the blocks of non-zero codewords of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ (Theorems 7.2.2-7.2.10). Using these results, one can explicitly determine Hamming weights of all non-zero codewords in these Λ-MT codes and their Hamming weight distributions. In Section 7.3, we explicitly determine Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights (Theorems 7.3.1-7.3.9). Among these classes of few weight MT codes, we obtain two classes of optimal equidistant Λ-MT codes that attain both Griesmer and Plotkin bounds (Theorems 7.3.1-7.3.2). Besides this, we identify three different classes of few weight Λ-MT codes, which are useful in designing secret sharing schemes with nice access structures (Theorems 7.3.1-7.3.3).

From now on, throughout this chapter, let $\mathbb{F}_q$ denote the finite field of order $q = p^r$, where p is a prime number and r is a positive integer. Let $m_1, m_2, \cdots, m_\ell$ be

arbitrary positive integers, not necessarily coprime to q. Let $n = m_1 + m_2 + \cdots + m_\ell$, and let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Here we shall follow the same notations as in Chapters 2 and 6.

7.2 Hamming weights of codewords of MT codes

In this section, we shall determine Hamming weights of non-zero codewords of several classes of Λ-MT codes over finite fields. To do this, let $\mathcal{C}$ be a Λ-MT code of length $n = m_1 + m_2 + \cdots + m_\ell$ over $\mathbb{F}_q$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$, whose codewords $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w$ satisfy the following condition:

$$\begin{aligned}&\text{For } 1 \le i \le \ell, \text{ there exist integers } i_1, i_2 \text{ such that } 1 \le i_1 < i_2 \le \rho \text{ and } x_{w,i} = 0\\ &\text{for } 1 \le w(\neq i_1, i_2) \le \rho,\end{aligned} \tag{7.1}$$

(note that the integers i_1 and i_2 depend upon i). Now let us write each word $x_w \in \mathcal{C}_w$ as $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell})$, where

$$x_{w,i} = \begin{cases} x_{0,w}^{(i)} + x_{1,w}^{(i)} u_i + \cdots + x_{p^{a_i}-1,w}^{(i)} u_i^{p^{a_i}-1} & \text{if } \epsilon_{w,i} = 1; \\ 0 & \text{otherwise,} \end{cases}$$

with $x_{j_i,w}^{(i)} \in \mathbb{F}_{q^{d_w}}$ for $1 \le w \le \rho$, $1 \le i \le \ell$ and $0 \le j_i \le p^{a_i} - 1$. Next we see, by Theorem 6.3.2, that the codeword of $\mathcal{C}$ corresponding to the words $x_1 \in \mathcal{C}_1, x_2 \in \mathcal{C}_2, \cdots, x_\rho \in \mathcal{C}_\rho$ is given by

$$c(x_1, x_2, \cdots, x_\rho) = \big(c_1(x_1, x_2, \cdots, x_\rho); c_2(x_1, x_2, \cdots, x_\rho); \cdots; c_\ell(x_1, x_2, \cdots, x_\rho)\big)$$

with $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w$ for $1 \le w \le \rho$, where

$$c_i(x_1, x_2, \cdots, x_\rho) = (c_{i,0}(x_1, x_2, \cdots, x_\rho), c_{i,1}(x_1, x_2, \cdots, x_\rho), \cdots, c_{i,m_i-1}(x_1, x_2, \cdots, x_\rho))$$

is the ith block of the codeword $c(x_1, x_2, \cdots, x_\rho)$ of the code $\mathcal{C}$ with

$$c_{i,t_i+v_ip^{a_i}}(x_1, x_2, \cdots, x_\rho) = \frac{1}{n_i}\left(\sum_{j_i=0}^{p^{a_i}-1}\binom{j_i}{t_i}(-1)^{j_i-t_i}\sum_{w=1}^{\rho} Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}\left(x_{j_i,w}^{(i)}\delta_w^{j_i-t_i-v_ip^{a_i}}\right)\right) \tag{7.2}$$

for $1 \leq i \leq \ell$, $0 \leq t_i \leq p^{a_i} - 1$ and $0 \leq v_i \leq n_i - 1$.

From now on, for $1 \leq w \leq \rho$, let $x_w = (x_{w,1}, x_{w,2}, \cdots, x_{w,\ell}) \in \mathcal{C}_w$ be fixed. In view of this, we see that the Hamming weight $W_H(c(x_1, x_2, \cdots, x_\rho))$ of the codeword $c(x_1, x_2, \cdots, x_\rho) \in \mathcal{C}$ is given by

$$W_H(c(x_1, x_2, \cdots, x_\rho)) = \sum_{i=1}^{\ell} W_H(c_i(x_1, x_2, \cdots, x_\rho)), \tag{7.3}$$

where $W_H(c_i(x_1, x_2, \cdots, x_\rho))$ denotes the Hamming weight of the ith block $c_i(x_1, x_2, \cdots, x_\rho)$ of the codeword $c(x_1, x_2, \cdots, x_\rho) \in \mathcal{C}$ for $1 \leq i \leq \ell$. Therefore to determine the Hamming weight of the codeword $c(x_1, x_2, \cdots, x_\rho) \in \mathcal{C}$, it is enough to determine the Hamming weights $W_H(c_1(x_1, x_2, \cdots, x_\rho)), W_H(c_2(x_1, x_2, \cdots, x_\rho)), \cdots, W_H(c_\ell(x_1, x_2, \cdots, x_\rho))$ of each of its ℓ blocks. Towards this, we note that

$$\begin{aligned} W_H(c_i(x_1, x_2, \cdots, x_\rho)) &= \sum_{t_i=0}^{p^{a_i}-1}\sum_{v_i=0}^{n_i-1} W_H(c_{i,t_i+v_ip^{a_i}}(x_1, x_2, \cdots, x_\rho)) \\ &= \sum_{t_i=0}^{p^{a_i}-1} \Delta_i^{(t_i)}(x_1, x_2 \cdots, x_\rho), \end{aligned} \tag{7.4}$$

where $\Delta_i^{(t_i)}(x_1, x_2 \cdots, x_\rho) = \sum_{v_i=0}^{n_i-1} W_H(c_{i,t_i+v_ip^{a_i}}(x_1, x_2, \cdots, x_\rho))$ for $0 \leq t_i \leq p^{a_i} - 1$ and $1 \leq i \leq \ell$. In order to determine the Hamming weight $W_H(c_i(x_1, x_2, \cdots, x_\rho))$ of the ith block $c_i(x_1, x_2, \cdots, x_\rho)$ of the codeword $c(x_1, x_2, \cdots, x_\rho) \in \mathcal{C}$ for $1 \leq i \leq \ell$, it is enough to determine the number $\Delta_i^{(t_i)}(x_1, x_2, \cdots, x_\rho)$ for $0 \leq t_i \leq p^{a_i} - 1$.

From this point on, let $1 \leq i \leq \ell$ and $0 \leq t_i \leq p^{a_i} - 1$ be fixed. Further, by (7.1), there exist integers i_1, i_2 satisfying $1 \leq i_1 < i_2 \leq \rho$ and $x_{w,i} = 0$ for $1 \leq w \leq \rho$ and

$w \notin \{i_1, i_2\}$. In view of this and by (7.2), we see that

$$\Delta_i^{(t_i)}(x_1, x_2 \cdots, x_\rho) = n_i - \big|\{0 \le v_i \le n_i - 1 : Tr_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_q}(y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}}) + Tr_{\mathbb{F}_{q^{d_{i_2}}}/\mathbb{F}_q}(y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}}) = 0\}\big|,$$

where

$$y_{t_i,i_1}^{(i)} = \sum_{j_i=t_i}^{p^{a_i}-1} \binom{j_i}{t_i} x_{j_i,i_1}^{(i)} (-\delta_{i_1})^{j_i - t_i} \in \mathbb{F}_{q^{d_{i_1}}} \quad \text{and} \quad y_{t_i,i_2}^{(i)} = \sum_{j_i=t_i}^{p^{a_i}-1} \binom{j_i}{t_i} x_{j_i,i_2}^{(i)} (-\delta_{i_2})^{j_i - t_i} \in \mathbb{F}_{q^{d_{i_2}}}.$$

From this point on, let us define

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \Delta_i^{(t_i)}(x_1, x_2 \cdots, x_\rho). \tag{7.5}$$

Now we shall first express the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ in terms of certain character sums over finite fields. For this, we assume, throughout this chapter, that χ and χ_w are canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_{q^{d_w}}$ for $1 \le w \le \rho$, respectively. Then by (2.1), the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ can be rewritten as

$$\begin{aligned} & D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) \\ = \; & n_i - \frac{1}{q} \sum_{v_i=0}^{n_i-1} \sum_{z \in \mathbb{F}_q} \chi\Big(z(Tr_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_q}(y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}}) + Tr_{\mathbb{F}_{q^{d_{i_2}}}/\mathbb{F}_q}(y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}}))\Big) \\ = \; & n_i - \frac{n_i}{q} - \frac{1}{q} \sum_{z \in \mathbb{F}_q^*} \sum_{v_i=0}^{n_i-1} \chi\Big(zTr_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_q}(y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}})\Big) \chi\Big(zTr_{\mathbb{F}_{q^{d_{i_2}}}/\mathbb{F}_q}(y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}})\Big). \end{aligned}$$

Further, by using the fact that $Tr_{\mathbb{F}_{q^{d_w}}/\mathbb{F}_q}$ is an $\mathbb{F}_q$-linear map for $1 \le w \le \rho$ and by (2.2), we observe that

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = n_i - \frac{n_i}{q} - \frac{1}{q} \sum_{z \in \mathbb{F}_q^*} \sum_{v_i=0}^{n_i-1} \chi_{i_1}(z y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}}) \chi_{i_2}(z y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}}).$$

From this, we obtain

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 0 & \text{if } y_{t_i,i_1}^{(i)} = y_{t_i,i_2}^{(i)} = 0; \\ \frac{n_i(q-1)}{q} - \frac{1}{q} \sum\limits_{z \in \mathbb{F}_q^*} \sum\limits_{v_i=0}^{n_i-1} \chi_{i_1}(z y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}}) & \text{if } y_{t_i,i_1}^{(i)} \neq 0 \ \& \ y_{t_i,i_2}^{(i)} = 0; \\ \frac{n_i(q-1)}{q} - \frac{1}{q} \sum\limits_{z \in \mathbb{F}_q^*} \sum\limits_{v_i=0}^{n_i-1} \chi_{i_2}(z y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}}) & \text{if } y_{t_i,i_1}^{(i)} = 0 \ \& \ y_{t_i,i_2}^{(i)} \neq 0; \\ \frac{n_i(q-1)}{q} - \frac{1}{q} \sum\limits_{z \in \mathbb{F}_q^*} \sum\limits_{v_i=0}^{n_i-1} \chi_{i_1}(z y_{t_i,i_1}^{(i)} \delta_{i_1}^{-v_i p^{a_i}}) \chi_{i_2}(z y_{t_i,i_2}^{(i)} \delta_{i_2}^{-v_i p^{a_i}}) & \\ & \text{if } y_{t_i,i_1}^{(i)} \neq 0 \ \& \ y_{t_i,i_2}^{(i)} \neq 0. \end{cases} \tag{7.6}$$

In order to explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we further proceed to express the above character sums in terms of Gauss sums, whose explicit values are known only in certain special cases [11, 51]. For this, we shall distinguish the following two cases: (i) either $y_{t_i,i_1}^{(i)}$ or $y_{t_i,i_2}^{(i)}$ is zero and (ii) both $y_{t_i,i_1}^{(i)}$ and $y_{t_i,i_2}^{(i)}$ are non-zero. From this point on, throughout this chapter, we assume that ζ_w is a primitive element of $\mathbb{F}_{q^{d_w}}$ for $1 \leq w \leq \rho$. It is easy to observe that $\zeta_w^{\frac{q^{d_w}-1}{q-1}}$ is a primitive element of $\mathbb{F}_q$ for each w. Now for $1 \leq w \leq \rho$, since $\delta_w \in \mathbb{F}_{q^{d_w}}^*$, we can write $\delta_w^{-1} = \zeta_w^{\ell_w}$ for some integer ℓ_w satisfying $0 \leq \ell_w \leq q^{d_w} - 2$. Further, let $\tau_w = \gcd\left(\frac{q^{d_w}-1}{q-1}, \ell_w\right)$, and let ϕ_w be a generator of the multiplicative character group $\widehat{\mathbb{F}_{q^{d_w}}^*}$ of $\mathbb{F}_{q^{d_w}}$ for each w.

7.2.1 Determination of the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when either $y_{t_i,i_1}^{(i)}$ or $y_{t_i,i_2}^{(i)}$ is zero

When $y_{t_i,i_1}^{(i)} = y_{t_i,i_2}^{(i)} = 0$, by (7.6), we have $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 0$. So we assume, throughout this section, that $y_{t_i,s_i}^{(i)} \neq 0$ and $y_{t_i,s_i'}^{(i)} = 0$, where $\{s_i, s_i'\} = \{i_1, i_2\}$. In the following lemma, we express the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ in terms of certain Gauss sums.

Lemma 7.2.1. *We have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q} - \frac{n_i(q-1)}{q(q^{d_{s_i}}-1)} \sum_{b_i=0}^{\tau_{s_i}-1} G(\overline{\phi}_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}, \chi_{s_i}) \phi_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)}).$$

Proof. To prove this, we see, by (7.6), that

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q} - \frac{1}{q} \sum_{z\in\mathbb{F}_q^*} \sum_{v_i=0}^{n_i-1} \chi_{s_i}(z y_{t_i,s_i}^{(i)} \delta_{s_i}^{-v_i p^{a_i}}). \tag{7.7}$$

Next by (2.5) and by using the fact that $\widehat{\mathbb{F}^*_{q^{d_{s_i}}}} = \langle \phi_{s_i} \rangle$, we note that

$$\sum_{z\in\mathbb{F}_q^*} \sum_{v_i=0}^{n_i-1} \chi_{s_i}(z y_{t_i,s_i}^{(i)} \delta_{s_i}^{-v_i p^{a_i}}) = \frac{1}{q^{d_{s_i}}-1} \sum_{z\in\mathbb{F}_q^*} \sum_{h_i=0}^{q^{d_{s_i}}-2} \sum_{v_i=0}^{n_i-1} G(\overline{\phi}_{s_i}^{h_i}, \chi_{s_i}) \phi_{s_i}^{h_i}(z y_{t_i,s_i}^{(i)} \delta_{s_i}^{-v_i p^{a_i}})$$

Furthermore, for $0 \le h_i \le q^{d_{s_i}} - 2$, one can observe that

$$\begin{aligned} \sum_{z\in\mathbb{F}_q^*} \phi_{s_i}^{h_i}(z) &= \sum_{k=0}^{q-2} \phi_{s_i}^{h_i}(\zeta_{s_i}^{\frac{(q^{d_{s_i}}-1)k}{q-1}}) = \sum_{k=0}^{q-2} e^{\frac{2\pi\iota(q^{d_{s_i}}-1)h_i k}{(q^{d_{s_i}}-1)(q-1)}} \\ &= \sum_{k=0}^{q-2} e^{\frac{2\pi\iota h_i k}{q-1}} = \begin{cases} q-1 & \text{if } h_i \equiv 0 \pmod{q-1}; \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

From this, we get

$$\begin{aligned} &\sum_{z\in\mathbb{F}_q^*} \sum_{v_i=0}^{n_i-1} \chi_{s_i}(z y_{t_i,s_i}^{(i)} \delta_{s_i}^{-v_i p^{a_i}}) \\ = \ & \frac{q-1}{q^{d_{s_i}}-1} \Bigg(\sum_{z_i=0}^{\frac{q^{d_{s_i}}-1}{q-1}-1} G(\overline{\phi}_{s_i}^{(q-1)z_i}, \chi_{s_i}) \phi_{s_i}^{(q-1)z_i}(y_{t_i,s_i}^{(i)}) \Bigg(\sum_{v_i=0}^{n_i-1} \phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-v_i p^{a_i}}) \Bigg) \Bigg). \end{aligned}$$

Next if $\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}}) \ne 1$ for some integer z_i satisfying $0 \le z_i < \frac{q^{d_{s_i}}-1}{q-1}$, then we

observe that

$$\begin{aligned}\sum_{v_i=0}^{n_i-1}\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-v_ip^{a_i}}) &= \sum_{v_i=0}^{n_i-1}\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}})^{v_i} = \frac{\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-m_i})-1}{\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}})-1}\\ &= \frac{\phi_{s_i}^{(q-1)z_i}(\lambda_i^{-1})-1}{\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}})-1} = 0,\end{aligned}$$

as $\delta_{s_i}^{m_i}=\lambda_i$ and $\lambda_i^{q-1}=1$. Therefore for $0\le z_i<\frac{q^{d_{s_i}}-1}{q-1}$, we get

$$\sum_{v_i=0}^{n_i-1}\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-v_ip^{a_i}}) = \begin{cases} n_i & \text{if } \phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}})=1;\\ 0 & \text{otherwise.}\end{cases}$$

Further, for an integer z_i satisfying $0\le z_i<\frac{q^{d_{s_i}}-1}{q-1}$, we note that $\phi_{s_i}^{(q-1)z_i}(\delta_{s_i}^{-p^{a_i}}) = \phi_{s_i}^{(q-1)z_i}(\zeta_{s_i}^{\ell_{s_i}p^{a_i}}) = e^{\frac{2\pi\iota(q-1)z_ip^{a_i}\ell_{s_i}}{q^{d_{s_i}}-1}} = 1$ if and only if $(q-1)z_ip^{a_i}\ell_{s_i}\equiv 0 \pmod{q^{d_{s_i}}-1}$, which holds if and only if $z_i\equiv 0 \pmod{\frac{(q^{d_{s_i}}-1)}{\tau_{s_i}(q-1)}}$. From this, we obtain

$$\sum_{z\in\mathbb{F}_q^*}\sum_{v_i=0}^{n_i-1}\chi_{s_i}(zy_{t_i,s_i}^{(i)}\delta_{s_i}^{-v_ip^{a_i}}) = \frac{n_i(q-1)}{q^{d_{s_i}}-1}\sum_{b_i=0}^{\tau_{s_i}-1}G(\overline{\phi}_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}},\chi_{s_i})\phi_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)}).$$

Now on substituting the above value of the sum $\sum_{z\in\mathbb{F}_q^*}\sum_{v_i=0}^{n_i-1}\chi_{s_i}(zy_{t_i,s_i}^{(i)}\delta_{s_i}^{-v_ip^{a_i}})$ in equation (7.7), the desired result follows immediately. □

In the following theorem, we explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)},y_{t_i,i_2}^{(i)})$.

Theorem 7.2.2. *Let* $y_{t_i,s_i}^{(i)}=\zeta_{s_i}^{b_{t_i,s_i}^{(i)}}\in\mathbb{F}_{q^{d_{s_i}}}^*$ *and* $y_{t_i,s_i'}^{(i)}=0$, *where* $0\le b_{t_i,s_i}^{(i)}\le q^{d_{s_i}}-2$.

(a) If $\tau_{s_i}=1$, *then we have* $D_i^{(t_i)}(y_{t_i,i_1}^{(i)},y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q}+\frac{n_i(q-1)}{q(q^{d_{s_i}}-1)}$.

(b) If $\tau_{s_i}=2$, *then the integer* d_{s_i} *is even and*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)},y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q}+\frac{n_i(q-1)\big(1+\iota^{\frac{rd_{s_i}(p-1)^2}{4}}q^{\frac{d_{s_i}}{2}}(-1)^{b_{t_i,s_i}^{(i)}}\big)}{q(q^{d_{s_i}}-1)}.$$

(c) Let $\tau_{s_i} \geq 3$. Suppose that there exists a positive integer ν'_{s_i} satisfying $p^{\nu'_{s_i}} \equiv -1 \ (mod\ \tau_{s_i})$. If z_{s_i} is the least positive integer satisfying $p^{z_{s_i}} \equiv -1 \ (mod\ \tau_{s_i})$, then we have $rd_{s_i} = 2z_{s_i}\nu_{s_i}$ for some positive integer ν_{s_i}.

- *When τ_{s_i} is even and $\frac{p\nu_{s_i}(p^{z_{s_i}}+1)}{\tau_{s_i}}$ is odd, we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(-1+q^{\frac{d_{s_i}}{2}}(\tau_{s_i}-1))}{q(q^{d_{s_i}}-1)} & \text{if } \tau_{s_i} \mid \frac{\tau_{s_i}}{2} + b_{t_i,s_i}^{(i)}; \\ \frac{n_i(q-1)}{q} + \frac{n_i(q-1)(1+q^{\frac{d_{s_i}}{2}})}{q(q^{d_{s_i}}-1)} & \text{if } \tau_{s_i} \nmid \frac{\tau_{s_i}}{2} + b_{t_i,s_i}^{(i)}. \end{cases}$$

- *When either τ_{s_i} is odd or $\frac{p\nu_{s_i}(p^{z_{s_i}}+1)}{\tau_{s_i}}$ is even, we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(-1+(-1)^{\nu_{s_i}-1}q^{\frac{d_{s_i}}{2}}(\tau_{s_i}-1))}{q(q^{d_{s_i}}-1)} & \text{if } \tau_{s_i} \mid b_{t_i,s_i}^{(i)}; \\ \frac{n_i(q-1)}{q} + \frac{n_i(q-1)(1+(-1)^{\nu_{s_i}-1}q^{\frac{d_{s_i}}{2}})}{q(q^{d_{s_i}}-1)} & \text{if } \tau_{s_i} \nmid b_{t_i,s_i}^{(i)}. \end{cases}$$

Proof. To prove the result, we first note, by Lemma 7.2.1, that

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\Theta'_i(y_{t_i,s_i}^{(i)})}{q(q^{d_{s_i}}-1)}, \tag{7.8}$$

where $\Theta'_i(y_{t_i,s_i}^{(i)}) = \sum_{b_i=0}^{\tau_{s_i}-1} \phi_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)}) G(\overline{\phi}_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}, \chi_{s_i})$. So to determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, it is enough to determine the explicit value of the sum $\Theta'_i(y_{t_i,s_i}^{(i)})$. To do this, we note that $O(\overline{\phi}_{s_i}^{\frac{q^{d_{s_i}}-1}{\tau_{s_i}}}) = \tau_{s_i}$. Now we shall consider the following three cases separately: (a) $\tau_{s_i} = 1$, (b) $\tau_{s_i} = 2$, and (c) $\tau_{s_i} \geq 3$.

(a) When $\tau_{s_i} = 1$, by (2.4), we note that $\Theta'_i(y_{t_i,s_i}^{(i)}) = -1$.

(b) When $\tau_{s_i} = 2$, we note that $\overline{\phi}_{s_i}^{\frac{q^{d_{s_i}}-1}{\tau_{s_i}}}$ is the quadratic character of $\mathbb{F}^*_{q^{d_{s_i}}}$. We also observe that $\tau_{s_i} = 2$ divides $\frac{q^{d_{s_i}}-1}{q-1} = 1 + q + \cdots + q^{d_{s_i}-1}$, which implies that q

is odd and d_{s_i} is even. Now by Theorem 2.2.1, we get

$$\Theta_i'(y_{t_i,s_i}^{(i)}) = -1 + \phi_{s_i}^{\frac{q^{d_{s_i}}-1}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)})G(\overline{\phi}_{s_i}^{\frac{q^{d_{s_i}}-1}{\tau_{s_i}}}, \chi_{s_i}) = -1 - \iota^{\frac{rd_{s_i}(p-1)^2}{4}} q^{\frac{d_{s_i}}{2}} (-1)^{b_{t_i,s_i}^{(i)}}.$$

(c) Next let $\tau_{s_i} \geq 3$. Here by Theorem 2.2.2, for $1 \leq b_i \leq \tau_{s_i} - 1$, we note that

$$G(\overline{\phi}_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}, \chi_{s_i}) = \begin{cases} (-1)^{b_i} q^{\frac{d_{s_i}}{2}} & \text{if } \tau_{s_i} \text{ is even and } \frac{p\nu_{s_i}(p^{z_{s_i}}+1)}{\tau_{s_i}} \text{ is odd;} \\ (-1)^{\nu_{s_i}-1} q^{\frac{d_{s_i}}{2}} & \text{otherwise.} \end{cases} \tag{7.9}$$

When τ_{s_i} is even and $\frac{p\nu_{s_i}(p^{z_{s_i}}+1)}{\tau_{s_i}}$ is odd, we observe, by (7.9), that

$$\begin{aligned} \Theta_i'(y_{t_i,s_i}^{(i)}) &= -1 + q^{\frac{d_{s_i}}{2}} \sum_{b_i=1}^{\tau_{s_i}-1} (-1)^{b_i} \phi_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)}) \\ &= -1 + q^{\frac{d_{s_i}}{2}} \sum_{b_i=1}^{\tau_{s_i}-1} e^{\left(\frac{2\pi\iota b_i(q^{d_{s_i}}-1)b_{t_i,s_i}^{(i)}}{\tau_{s_i}(q^{d_{s_i}}-1)} + \frac{2\pi\iota b_i \tau_{s_i}}{2\tau_{s_i}}\right)} \\ &= -1 + q^{\frac{d_{s_i}}{2}} \sum_{b_i=1}^{\tau_{s_i}-1} e^{\frac{2\pi\iota b_i}{\tau_{s_i}}(b_{t_i,s_i}^{(i)} + \frac{\tau_{s_i}}{2})} \\ &= \begin{cases} -1 + q^{\frac{d_{s_i}}{2}}(\tau_{s_i}-1) & \text{if } \tau_{s_i} \mid \frac{\tau_{s_i}}{2} + b_{t_i,s_i}^{(i)}; \\ -1 - q^{\frac{d_{s_i}}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

On the other hand, when either τ_{s_i} is odd or $\frac{p\nu_{s_i}(p^{z_{s_i}}+1)}{\tau_{s_i}}$ is even, we observe, by (7.9), that

$$\begin{aligned} \Theta_i'(y_{t_i,s_i}^{(i)}) &= -1 + (-1)^{\nu_{s_i}-1} q^{\frac{d_{s_i}}{2}} \sum_{b_i=1}^{\tau_{s_i}-1} \phi_{s_i}^{\frac{(q^{d_{s_i}}-1)b_i}{\tau_{s_i}}}(y_{t_i,s_i}^{(i)}) \\ &= \begin{cases} -1 + (-1)^{\nu_{s_i}-1} q^{\frac{d_{s_i}}{2}}(\tau_{s_i}-1) & \text{if } \tau_{s_i} \mid b_{t_i,s_i}^{(i)}; \\ -1 - (-1)^{\nu_{s_i}-1} q^{\frac{d_{s_i}}{2}} & \text{otherwise.} \end{cases} \end{aligned}$$

Now on substituting the values of $\Theta_i'(y_{t_i,s_i}^{(i)})$ in equation (7.8) in the respective cases,

we get the desired result. □

7.2.2 Determination of $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $y_{t_i,i_1}^{(i)} \neq 0$ and $y_{t_i,i_2}^{(i)} \neq 0$

Throughout this section, we assume that $y_{t_i,i_1}^{(i)} \neq 0$ and $y_{t_i,i_2}^{(i)} \neq 0$. To determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we shall first fix the following notations:

$\eta_i = \gcd(d_{i_1}, d_{i_2})$	$g_{s_i} = \gcd\big(\frac{q^{d_{s_i}}-1}{q^{\eta_i}-1}, \ell_{s_i}\big)$ for $s_i \in \{i_1, i_2\}$
$\Delta_{s_i} = \frac{q^{d_{s_i}}-1}{(q^{\eta_i}-1)g_{s_i}}$ for $s_i \in \{i_1, i_2\}$	τ_i is the least positive integer satisfying $\frac{\tau_i \ell_{i_1}}{g_{i_1} G_i} \equiv 1 \left(\mathrm{mod} \frac{q^{\eta_i}-1}{G_i}\right)$
$G_i = \gcd\big(\frac{\ell_{i_1}}{g_{i_1}}, q^{\eta_i}-1\big)$	τ_i' is the least positive integer satisfying $\frac{\tau_i'(q^{\eta_i}-1)\Delta_{i_1}}{G_i \Lambda_i} \equiv 1 \left(\mathrm{mod}\ \frac{q-1}{\Lambda_i}\right)$
$H_i = \gcd\big(\frac{\ell_{i_1}}{g_{i_1}}, \frac{\ell_{i_2}}{g_{i_2}}, q^{\eta_i}-1\big)$	L_i is the least positive integer satisfying $\zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{q-1}} = \zeta_{i_2}^{\frac{(q^{d_{i_2}}-1)L_i}{q-1}}$
$\Lambda_i = \gcd\big(\frac{\Delta_{i_1}(q^{\eta_i}-1)}{G_i}, q-1\big)$	$\Lambda_i' = \gcd(\Lambda_i, \frac{\Delta_{i_2} G_i L_i}{H_i} - \frac{\Delta_{i_1}\tau_i \ell_{i_2}}{g_{i_2} H_i})$
$K_i = \frac{(q^{\eta_i}-1)(q-1)}{G_i \Lambda_i}$	$K_i' = -\frac{\Lambda_i \tau_i \ell_{i_2}}{\Lambda_i' g_{i_2} H_i}\big(1 - \frac{(q^{\eta_i}-1)\tau_i' \Delta_{i_1}}{G_i \Lambda_i}\big) - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{\Lambda_i' H_i g_{i_2}}$
$M_i = \frac{G_i \Lambda_i g_{i_1}}{q-1}$	$M_i' = \frac{(q^{\eta_i}-1)\Lambda_i' g_{i_2} H_i}{G_i \Lambda_i}$

Note that $K_i' = -\frac{\tau_i \ell_{i_2} \Lambda_i}{g_{i_2} H_i \Lambda_i'} - \frac{\tau_i'(q^{\eta_i}-1)}{G_i \Lambda_i'}\big(\frac{\Delta_{i_2} G_i L_i}{H_i} - \frac{\tau_i \ell_{i_2} \Delta_{i_1}}{g_{i_2} H_i}\big)$ and $M_i' = \frac{(q^{\eta_i}-1)\Lambda_i' g_{i_2} H_i}{G_i \Lambda_i}$ are integers, and $\gcd(L_i, q-1) = 1$.

In the following lemma, we first express the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ in terms of certain Gauss sums.

Lemma 7.2.3. *We have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)},$$

where

$$\Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \sum_{z_2=0}^{M_i'-1}\sum_{z_1=0}^{M_i-1}\Big(G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i'z_2+K_iz_1)}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}(K_i'z_2+K_iz_1)}(y^{(i)}_{t_i,i_1})G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_iz_2}{H_i\Lambda_i'}}, \chi_{i_2}) \phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_iz_2}{H_i\Lambda_i'}}(y^{(i)}_{t_i,i_2})\Big).$$

Proof. To prove the result, we see, by (7.6), that

$$D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \frac{n_i(q-1)}{q} - \frac{1}{q}\Omega_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}), \tag{7.10}$$

where $\Omega_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \sum\limits_{z\in\mathbb{F}_q^*}\sum\limits_{v_i=0}^{n_i-1}\chi_{i_1}(zy^{(i)}_{t_i,i_1}\delta_{i_1}^{-v_ip^{a_i}})\chi_{i_2}(zy^{(i)}_{t_i,i_2}\delta_{i_2}^{-v_ip^{a_i}})$. Now since $\widehat{\mathbb{F}^*_{q^{d_{i_1}}}} = \langle\phi_{i_1}\rangle$ and $\widehat{\mathbb{F}^*_{q^{d_{i_2}}}} = \langle\phi_{i_2}\rangle$, we note, by (2.5), that

$$\begin{aligned}\Omega_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) &= \frac{1}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\sum_{z\in\mathbb{F}_q^*}\sum_{\mu_1=0}^{q^{d_{i_1}}-2}\sum_{\mu_2=0}^{q^{d_{i_2}}-2}\sum_{v_i=0}^{n_i-1}\Big(G(\overline{\phi}_{i_1}^{\mu_1}, \chi_{i_1})\phi_{i_1}^{\mu_1}(zy^{(i)}_{t_i,i_1}\delta_{i_1}^{-v_ip^{a_i}}) \\ &\qquad G(\overline{\phi}_{i_2}^{\mu_2}, \chi_{i_2})\phi_{i_2}^{\mu_2}(zy^{(i)}_{t_i,i_2}\delta_{i_2}^{-v_ip^{a_i}})\Big).\end{aligned}$$

Further, for $0 \le \mu_1 \le q^{d_{i_1}}-2$ and $0 \le \mu_2 \le q^{d_{i_2}}-2$, one can easily observe that

$$\begin{aligned}\sum_{z\in\mathbb{F}_q^*}\phi_{i_1}^{\mu_1}(z)\phi_{i_2}^{\mu_2}(z) &= \sum_{k=0}^{q-2}\phi_{i_1}^{\mu_1}(\zeta_{i_1}^{\frac{(q^{d_{i_1}}-1)k}{q-1}})\phi_{i_2}^{\mu_2}(\zeta_{i_2}^{\frac{(q^{d_{i_2}}-1)kL_i}{q-1}}) \\ &= \sum_{k=0}^{q-2}e^{\frac{2\pi\iota(\mu_1+\mu_2L_i)k}{q-1}} = \begin{cases} q-1 \text{ if } \mu_1+\mu_2L_i \equiv 0 \pmod{q-1}; \\ 0 \qquad \text{otherwise.}\end{cases}\end{aligned}$$

From this, we obtain

$$\begin{aligned}\Omega_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) &= \frac{q-1}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\sum_{\mu_1,\mu_2}G(\overline{\phi}_{i_1}^{\mu_1}, \chi_{i_1})\phi_{i_1}^{\mu_1}(y^{(i)}_{t_i,i_1})G(\overline{\phi}_{i_2}^{\mu_2}, \chi_{i_2})\phi_{i_2}^{\mu_2}(y^{(i)}_{t_i,i_2}) \\ &\qquad \times\Big(\sum_{v_i=0}^{n_i-1}\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-v_ip^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-v_ip^{a_i}})\Big),\end{aligned}$$

where the summation $\sum_{\mu_1,\mu_2}$ runs over the integers μ_1 and μ_2 satisfying $0 \le \mu_1 \le q^{d_{i_1}}-2$, $0 \le \mu_2 \le q^{d_{i_2}}-2$ and $\mu_1+\mu_2 L_i \equiv 0 \pmod{q-1}$. Next for $0 \le \mu_1 \le q^{d_{i_1}}-2$ and $0 \le \mu_2 \le q^{d_{i_2}}-2$ satisfying $\mu_1+\mu_2 L_i \equiv 0 \pmod{q-1}$, we assert that

$$\sum_{v_i=0}^{n_i-1} \phi_{i_1}^{\mu_1}(\delta_{i_1}^{-v_i p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-v_i p^{a_i}}) = \begin{cases} n_i & \text{if } \phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}}) = 1; \\ 0 & \text{otherwise.} \end{cases} \tag{7.11}$$

To prove this, we note that if $\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}}) \ne 1$, then

$$\sum_{v_i=0}^{n_i-1} \phi_{i_1}^{\mu_1}(\delta_{i_1}^{-v_i p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-v_i p^{a_i}}) = \frac{\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-m_i})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-m_i})-1}{\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}})-1} = \frac{\phi_{i_1}^{\mu_1}(\lambda_i^{-1})\phi_{i_2}^{\mu_2}(\lambda_i^{-1})-1}{\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}})-1},$$

as $\delta_{i_1}^{m_i} = \delta_{i_2}^{m_i} = \lambda_i$. Since $\lambda_i^{-1} \in \mathbb{F}_q^*$ and $\zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{q-1}} = \zeta_{i_2}^{\frac{(q^{d_{i_2}}-1)L_i}{q-1}}$ is a primitive element of $\mathbb{F}_q$, one can write $\lambda_i^{-1} = \zeta_{i_1}^{\frac{(q^{d_{i_1}}-1)J}{q-1}} = \zeta_{i_2}^{\frac{(q^{d_{i_2}}-1)JL_i}{q-1}}$ for some integer J satisfying $0 \le J \le q-2$. In view of this, we obtain $\phi_{i_1}^{\mu_1}(\lambda_i^{-1})\phi_{i_2}^{\mu_2}(\lambda_i^{-1}) = e^{\frac{2\pi\iota J(\mu_1+\mu_2 L_i)}{q-1}} = 1$, which further implies that $\sum_{v_i=0}^{n_i-1} \phi_{i_1}^{\mu_1}(\delta_{i_1}^{-v_i p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-v_i p^{a_i}}) = 0$. On the other hand, when $\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}}) = 1$, we have $\sum_{v_i=0}^{n_i-1} \phi_{i_1}^{\mu_1}(\delta_{i_1}^{-v_i p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-v_i p^{a_i}}) = n_i$, which proves (7.11).

We further note that $\phi_{i_1}^{\mu_1}(\delta_{i_1}^{-p^{a_i}})\phi_{i_2}^{\mu_2}(\delta_{i_2}^{-p^{a_i}}) = e^{\frac{2\pi\iota\mu_1\ell_{i_1}p^{a_i}}{q^{d_{i_1}}-1}+\frac{2\pi\iota\mu_2\ell_{i_2}p^{a_i}}{q^{d_{i_2}}-1}} = 1$ if and only if $(q^{d_{i_2}}-1)\mu_1\ell_{i_1} + (q^{d_{i_1}}-1)\mu_2\ell_{i_2} \equiv 0 \pmod{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}$. From this, we get

$$\Omega_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \sum_{\mu_1,\mu_2} G(\overline{\phi}_{i_1}^{\mu_1}, \chi_{i_1})\phi_{i_1}^{\mu_1}(y_{t_i,i_1}^{(i)})G(\overline{\phi}_{i_2}^{\mu_2}, \chi_{i_2})\phi_{i_2}^{\mu_2}(y_{t_i,i_2}^{(i)}), \tag{7.12}$$

where the summation $\sum_{\mu_1,\mu_2}$ runs over the integers μ_1 and μ_2 satisfying

$$\begin{aligned} &0 \le \mu_1 \le q^{d_{i_1}}-2, 0 \le \mu_2 \le q^{d_{i_2}}-2, \\ &(q^{d_{i_2}}-1)\mu_1\ell_{i_1} + (q^{d_{i_1}}-1)\mu_2\ell_{i_2} \equiv 0 \pmod{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \text{ and} \\ &\mu_1+\mu_2 L_i \equiv 0 \pmod{q-1}. \end{aligned} \tag{7.13}$$

Furthermore, one can observe that all the distinct integers μ_1, μ_2 satisfying (7.13) are given by

$$\mu_1 = \Delta_{i_1}(K_i' z_2 + K_i z_1) \text{ and } \mu_2 = \frac{\Delta_{i_2} G_i \Lambda_i z_2}{H_i \Lambda_i'},$$

where z_1, z_2 are integers satisfying $0 \leq z_1 < M_i$ and $0 \leq z_2 < M_i'$. This, by (7.12), gives $\Omega_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \frac{n_i(q-1)\Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2})}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}$. From this and by equation (7.10), the desired result follows immediately. □

Next to determine the explicit value of $D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2})$, we note that $O(\phi_{i_1}^{\Delta_{i_1} K_i}) = M_i$ and $O(\phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i}{H_i \Lambda_i'}}) = M_i'$. Now we shall distinguish the following three cases: (i) $M_i' = 1$, (ii) $M_i' = 2$, and (iii) $M_i' \geq 3$. Further, in each of these three cases, we shall consider the following three subcases separately: (i) $M_i = 1$, (ii) $M_i = 2$, and (iii) $M_i \geq 3$.

In the following theorem, we consider the case $M_i' = 1$, and we explicitly determine the number $D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2})$.

Theorem 7.2.4. *Let $M_i' = 1$, $y^{(i)}_{t_i,i_1} = \zeta_{i_1}^{b^{(i)}_{t_i,i_1}} \in \mathbb{F}^*_{q^{d_{i_1}}}$ and $y^{(i)}_{t_i,i_2} \in \mathbb{F}^*_{q^{d_{i_2}}}$, where $0 \leq b^{(i)}_{t_i,i_1} \leq q^{d_{i_1}} - 2$.*

(a) If $M_i = 1$, then we have $D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \frac{n_i(q-1)}{q} - \frac{n_i(q-1)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}$.

(b) If $M_i = 2$, then the integer d_{i_1} is even and

$$D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\big(1 + \iota^{\frac{r d_{i_1} (p-1)^2}{4}} q^{\frac{d_{i_1}}{2}} (-1)^{b^{(i)}_{t_i,i_1}}\big)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}.$$

(c) Let $M_i \geq 3$. Suppose that there exists a positive integer μ_i' satisfying $p^{\mu_i'} \equiv -1 \pmod{M_i}$. If θ_i is the least positive integer satisfying $p^{\theta_i} \equiv -1 \pmod{M_i}$, then we have $r d_{i_1} = 2\theta_i \gamma_i$ for some positive integer γ_i.

- *When M_i is even and $\frac{p\gamma_i(p^{\theta_i}+1)}{M_i}$ is odd, we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-q^{\frac{d_{i_1}}{2}}(M_i-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \mid \frac{M_i}{2} + b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \nmid \frac{M_i}{2} + b_{t_i,i_1}^{(i)}. \end{cases}$$

- *When either M_i is odd or $\frac{p\gamma_i(p^{\theta_i}+1)}{M_i}$ is even, we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}(M_i-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

Proof. By applying Lemma 7.2.3 and working in a similar manner as in Theorem 7.2.2, the desired result follows immediately. □

In the following theorem, we explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $M_i = 1$ and $M_i' = 2$.

Theorem 7.2.5. *Let $M_i = 1$, $M_i' = 2$, $y_{t_i,i_1}^{(i)} = \zeta_{i_1}^{b_{t_i,i_1}^{(i)}} \in \mathbb{F}_{q^{d_{i_1}}}^*$ and $y_{t_i,i_2}^{(i)} = \zeta_{i_2}^{b_{t_i,i_2}^{(i)}} \in \mathbb{F}_{q^{d_{i_2}}}^*$, where $0 \le b_{t_i,i_1}^{(i)} \le q^{d_{i_1}} - 2$ and $0 \le b_{t_i,i_2}^{(i)} \le q^{d_{i_2}} - 2$.*

(a) When d_{i_2} is even, we have $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q}\left(1 - \frac{1+\iota^{\frac{rd_{i_2}(p-1)^2}{4}} q^{\frac{d_{i_2}}{2}} (-1)^{b_{t_i,i_2}^{(i)}}}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\right)$.

(b) When d_{i_2} is odd, the integer d_{i_1} is odd and

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \frac{n_i(q-1)}{q}\left(1 - \frac{1+\iota^{\frac{r(d_{i_1}+d_{i_2})(p-1)^2}{4}} q^{\frac{d_{i_1}+d_{i_2}}{2}} (-1)^{b_{t_i,i_1}^{(i)}+b_{t_i,i_2}^{(i)}}}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\right).$$

Proof. To determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we note, by Lemma 7.2.3, that it is enough to determine the explicit value of the sum

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 + G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i}{H_i \Lambda_i'}}, \chi_{i_2}) G(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i'}, \chi_{i_1}) \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i}{H_i \Lambda_i'}}(y_{t_i,i_2}^{(i)}) \phi_{i_1}^{\Delta_{i_1} K_i'}(y_{t_i,i_1}^{(i)}).$$

Towards this, we see that $O(\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}) = M_i' = 2$, so the character $\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_2}}}$ and q is odd. Since $\gcd(L_i, q-1) = 1$, we see that L_i is odd. Further, $M_i = 1$ implies that $g_{i_1} = 1$ and $G_i\Lambda_i = q-1$. From this, we obtain $\frac{(q^{\eta_i}-1)\Lambda_i' g_{i_2} H_i}{q-1} = M_i' = 2$, which further implies that $\eta_i = 1$ and $\Lambda_i' g_{i_2} H_i = 2$. Furthermore, it is easy to see that

$$\begin{aligned}\Delta_{i_1}K_i' &= \frac{q^{d_{i_1}}-1}{q-1}\Big(-\frac{\Lambda_i\tau_i\ell_{i_2}(1-\tau_i'\Delta_{i_1})}{2} - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{2}\Big)\\ &= \frac{q^{d_{i_1}}-1}{2}\Big(-\frac{\tau_i\ell_{i_2}(1-\tau_i'\Delta_{i_1})}{G_i} - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{q-1}\Big) \qquad (7.14)\end{aligned}$$

and

$$\Lambda_i' g_{i_2} H_i = 2 = \gcd\Big(\Lambda_i g_{i_2} H_i, \frac{(q^{d_{i_2}}-1)G_iL_i}{q-1} - \Delta_{i_1}\ell_{i_2}\tau_i\Big). \qquad (7.15)$$

Now we shall consider the following two cases separately: (a) d_{i_2} is even and (b) d_{i_2} is odd.

(a) When d_{i_2} is even, we note that the integer d_{i_1} is odd, as $\eta_i = 1$. From this, we see that the integer $\frac{q^{d_{i_2}}-1}{q-1}$ is even and the integer Δ_{i_1} is odd. This, by (7.15), clearly implies that the integer $\tau_i\ell_{i_2}$ is even. Further, since G_i divides $1-\tau_i'\Delta_{i_1}$, by (7.14), we observe that $\phi_{i_1}^{\Delta_{i_1}K_i'}$ is the trivial multiplicative character of $\mathbb{F}_{q^{d_{i_1}}}$. This, by Theorem 2.2.1, implies that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 - G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}) = 1 + \iota^{\frac{rd_{i_2}(p-1)^2}{4}} q^{\frac{d_{i_2}}{2}} (-1)^{b_{t_i,i_2}^{(i)}}.$$

(b) When d_{i_2} is odd, we note that the integer $\frac{q^{d_{i_2}}-1}{q-1}$ is odd and $g_{i_2} = 1$. Now as $\frac{G_i\Lambda_i}{q-1} = \gcd(\Delta_{i_1}, G_i) = 1$, by (7.15), one can observe that the integer Δ_{i_1} must be odd, which further implies that the integer d_{i_1} is odd.

Now when G_i is even, we note, by (7.15), that the integer $\tau_i\ell_{i_2}$ is even. Further,

as G_i divides $1-\tau_i'\Delta_{i_1}$, we observe that the integer τ_i' is odd. This, by (7.14), implies that $\phi_{i_1}^{\Delta_{i_1}K_i'}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_1}}}$.

On the other hand, when G_i is odd, we see, by (7.15), that the integer $\tau_i\ell_{i_2}$ is odd. Further, one can easily observe that the integer τ_i' must be odd if the integer $\frac{1-\tau_i'\Delta_{i_1}}{G_i}$ is even, while the integer τ_i' is even if the integer $\frac{1-\tau_i'\Delta_{i_1}}{G_i}$ is odd. Now since both the integers $\frac{(q^{d_{i_2}}-1)L_i}{q-1}, \tau_i\ell_{i_2}$ are odd, we note, by (7.14), that $\phi_{i_1}^{\Delta_{i_1}K_i'}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_1}}}$.

This, by Theorem 2.2.1, implies that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1+\iota^{\frac{r(d_{i_1}+d_{i_2})(p-1)^2}{4}} q^{\frac{d_{i_1}+d_{i_2}}{2}} (-1)^{b_{t_i,i_1}^{(i)}+b_{t_i,i_2}^{(i)}}. \qquad \square$$

In the following theorem, we explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $M_i = M_i' = 2$.

Theorem 7.2.6. *Let $M_i = M_i' = 2$, $y_{t_i,i_1}^{(i)} = \zeta_{i_1}^{b_{t_i,i_1}^{(i)}} \in \mathbb{F}_{q^{d_{i_1}}}^*$ and $y_{t_i,i_2}^{(i)} = \zeta_{i_2}^{b_{t_i,i_2}^{(i)}} \in \mathbb{F}_{q^{d_{i_2}}}^*$, where $0 \le b_{t_i,i_1}^{(i)} \le q^{d_{i_1}}-2$ and $0 \le b_{t_i,i_2}^{(i)} \le q^{d_{i_2}}-2$. Here the integer $g_{i_1} \in \{1,2\}$ and p is an odd prime.*

(a) When $g_{i_1}=1$, we have $q=3$, $G_i = \lambda_i = \eta_i = 2$ and

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{2n_i}{3} - \frac{2n_i\left(1-3^{\frac{d_{i_1}}{2}}+2(-1)^{\frac{2b_{t_i,i_2}^{(i)}+b_{t_i,i_1}^{(i)}+d_{i_2}}{2}} 3^{\frac{d_{i_1}+d_{i_2}}{2}}\right)}{3(3^{d_{i_1}}-1)(3^{d_{i_2}}-1)} & \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ \frac{2n_i}{3} - \frac{2n_i(1+3^{\frac{d_{i_1}}{2}})}{3(3^{d_{i_1}}-1)(3^{d_{i_2}}-1)} & \text{if } 2 \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

(b) Let $g_{i_1}=2$.

- *If $p \equiv 3 \pmod 4$, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\left(1 - \frac{1+q^{\frac{d_{i_1}}{2}}+2(-1)^{\frac{2b_{t_i,i_2}^{(i)}+rd_{i_2}+b_{t_i,i_1}^{(i)}}{2}} q^{\frac{d_{i_1}+d_{i_2}}{2}}}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\right) & \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q}\left(1 - \frac{1-q^{\frac{d_{i_1}}{2}}}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\right) & \text{if } 2 \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

- *If $p \equiv 1 \pmod 4$, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\Big(1 - \frac{1+q^{\frac{d_{i_1}}{2}}+2q^{\frac{d_{i_1}+2d_{i_2}}{4}}(-1)^{\frac{2(rd_{i_2}+b_{t_i,i_2}^{(i)})+b_{t_i,i_1}^{(i)}}{2}}\mathcal{R}_i}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \\ \qquad\qquad \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q}\Big(1 - \frac{1-q^{\frac{d_{i_1}}{2}}+2q^{\frac{d_{i_1}+2d_{i_2}}{4}}(-1)^{\frac{2(rd_{i_2}+b_{t_i,i_2}^{(i)})+1+b_{t_i,i_1}^{(i)}}{2}}\mathcal{I}_i}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \\ \qquad\qquad \text{if } 2 \nmid b_{t_i,i_1}^{(i)}, \end{cases}$$

where $\mathcal{R}_i = Re\,(e_i + \iota f_i)^{\frac{rd_{i_1}}{2}}$ and $\mathcal{I}_i = Im\,(e_i + \iota f_i)^{\frac{rd_{i_1}}{2}}$ denote the real and imaginary parts of the complex number $(e_i + \iota f_i)^{\frac{rd_{i_1}}{2}}$, respectively (Here e_i and f_i are the integers determined uniquely by $p = e_i^2 + f_i^2, e_i \equiv -1 \pmod 4$ and $f_i \equiv e_i \zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{4}} \pmod p$).

Proof. To determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we note, by Lemma 7.2.3, that it is enough to determine the explicit value of the sum

$$\begin{aligned} \Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) &= 1 - G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K_i}(y_{t_i,i_1}^{(i)}) \\ &\quad + G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)})F_i(y_{t_i,i_1}^{(i)}), \end{aligned}$$

where $F_i(y_{t_i,i_1}^{(i)}) = \phi_{i_1}^{\Delta_{i_1}K_i'}(y_{t_i,i_1}^{(i)})\Big(G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}, \chi_{i_1}) + G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K_i}(y_{t_i,i_1}^{(i)})\Big)$. Since $M_i = M_i' = 2$, we see that $\phi_{i_1}^{\Delta_{i_1}K_i}$ and $\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}$ are the quadratic characters of $\mathbb{F}_{q^{d_{i_1}}}$ and $\mathbb{F}_{q^{d_{i_2}}}$ respectively, and q is odd. As $\gcd(L_i, q-1) = 1$, the integer L_i must be odd. Further, since $M_i = 2$ and $q-1$ divides $G_i\Lambda_i$, one can observe that the integer g_{i_1} divides 2. So we shall consider the following two cases separately: (a) $g_{i_1} = 1$, and (b) $g_{i_1} = 2$.

(a) When $g_{i_1} = 1$, we see that $\frac{G_i\Lambda_i}{q-1} = 2 = \gcd\left(\frac{q^{d_{i_1}}-1}{q-1}, G_i\right)$, which implies that both the integers d_{i_1} and G_i are even. As $G_i = \gcd(\ell_{i_1}, q^{\eta_i} - 1)$ is even and $g_{i_1} = \gcd\left(\frac{q^{d_{i_1}}-1}{q^{\eta_i}-1}, \ell_{i_1}\right) = 1$, one can easily observe that the integer $\frac{d_{i_1}}{\eta_i}$ is odd, which

implies that the integer η_i is even. Further, since $\frac{G_i\Lambda_i}{q-1} = 2$ and $M_i' = 2$, we note that $\frac{(q^{\eta_i}-1)\Lambda_i' g_{i_2} H_i}{q-1} = 4$. Next we see that $\frac{q^{\eta_i}-1}{q-1} = 1+q+q^2+\cdots+q^{\eta_i-1} \geq 4$. From this, we obtain $\Lambda_i' g_{i_2} H_i = 1$ and $\frac{q^{\eta_i}-1}{q-1} = 4$, which further implies that $q = 3$ and $\eta_i = 2$. This gives $G_i\Lambda_i = 4$. Since $\Lambda_i = \gcd(2, \frac{3^{d_{i_1}}-1}{G_i})$ and the integer $\frac{3^{\eta_i}-1}{G_i}$ is even, we see that $\Lambda_i = 2$, which implies that $G_i = 2$. Further, it is easy to see that

$$\Delta_{i_1} K_i' = \frac{(q^{d_{i_1}}-1)(-2\tau_i \ell_{i_2}(1-2\tau_i'\Delta_{i_1}) - \tau_i'(q^{d_{i_2}}-1)L_i)}{8}.$$

This further implies that $\phi_{i_1}^{\Delta_{i_1}K_i'} = \overline{\phi}_{i_1}^{\frac{\tau_i \ell_{i_2}(q^{d_{i_1}}-1)(1-2\tau_i'\Delta_{i_1})}{4}}$. As $G_i = 2$ and $\Lambda_i' = 1 = \gcd(2, \Delta_{i_2} G_i L_i - \Delta_{i_1}\tau_i\ell_{i_2})$, we see that the integer $\tau_i\ell_{i_2}$ is odd, which further implies that $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = 4$. Next we observe that $\Delta_{i_1}K_i = \frac{q^{d_{i_1}}-1}{2}$ and $\phi_{i_1}^{\Delta_{i_1}(K_i+K_i')} = \phi_{i_1}^{\frac{(q^{d_{i_1}}-1)(-\tau_i\ell_{i_2}(1-2\tau_i'\Delta_{i_1})+2)}{4}}$. This implies that $O(\phi_{i_1}^{\Delta_{i_1}(K_i+K_i')}) = 4$. Now since $p \equiv 3 \equiv -1 \pmod 4$, $r = 1$ and $\frac{d_{i_1}}{2}$ is odd, by Theorem 2.2.2, we note that $G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}, \chi_{i_1}) = G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}) = -p^{\frac{d_{i_1}}{2}}$. From this, we obtain

$$\begin{aligned}
F_i(y_{t_i,i_1}^{(i)}) &= -p^{\frac{d_{i_1}}{2}} \phi_{i_1}^{\Delta_{i_1}K_i'}(y_{t_i,i_1}^{(i)})(1+\phi_{i_1}^{\Delta_{i_1}K_i}(y_{t_i,i_1}^{(i)})) \\
&= -p^{\frac{d_{i_1}}{2}} e\Big(\frac{-2\pi\iota\tau_i\ell_{i_2}(1-2\tau_i'\Delta_{i_1})b_{t_i,i_1}^{(i)}}{4}\Big)(1+e^{\pi\iota b_{t_i,i_1}^{(i)}}) \\
&= \begin{cases} -2\, p^{\frac{d_{i_1}}{2}}(-1)^{\frac{b_{t_i,i_1}^{(i)}}{2}} & \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ 0 & \text{if } 2 \nmid b_{t_i,i_1}^{(i)}. \end{cases}
\end{aligned}$$

This, by Theorem 2.2.1, implies that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 1-3^{\frac{d_{i_1}}{2}} + 2(-1)^{\frac{b_{t_i,i_1}^{(i)}+d_{i_2}+2b_{t_i,i_2}^{(i)}}{2}} 3^{\frac{d_{i_1}+d_{i_2}}{2}} & \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ 1+3^{\frac{d_{i_1}}{2}} & \text{if } 2 \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

(b) Let $g_{i_1} = 2 = \gcd\big(\frac{q^{d_{i_1}}-1}{q^{\eta_i}-1}, \ell_{i_1}\big)$. Here we see that $\frac{G_i\Lambda_i}{q-1} = 1$ and both the integers d_{i_1}, ℓ_{i_1} are even. Since $M_i' = 2$, we observe that $\Lambda_i' g_{i_2} H_i = 2$ and $\frac{q^{\eta_i}-1}{q-1} = 1$,

i.e., $\eta_i = 1$. Now as $\eta_i = 1$ and d_{i_1} is even, the integer d_{i_2} must be odd and $g_{i_2} = 1 = \gcd\left(\frac{q^{d_{i_2}}-1}{q-1}, \ell_{i_2}\right)$. This implies that the integer Δ_{i_2} is odd and

$$\Lambda_i' H_i = 2 = \gcd(\Lambda_i H_i, \Delta_{i_2} G_i L_i - \Delta_{i_1} \tau_i \ell_{i_2}). \tag{7.16}$$

Further, as $\frac{g_{i_1}}{2} = \gcd\left(\Delta_{i_1}, \frac{\ell_{i_1}}{2}\right) = 1$ and $G_i = \gcd\left(\frac{\ell_{i_1}}{2}, q-1\right)$, by (7.16), we observe that the integer Δ_{i_1} is odd in this case. Next we note that

$$\Delta_{i_1} K_i' = \frac{q^{d_{i_1}}-1}{2(q-1)}\Big(\frac{-\Lambda_i \tau_i \ell_{i_2}(1-\tau_i'\Delta_{i_1})}{2} - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{2}\Big) = \frac{(q^{d_{i_1}}-1)A_i}{4}, \tag{7.17}$$

where $A_i = \frac{-\tau_i \ell_{i_2}(1-\tau_i'\Delta_{i_1})}{G_i} - \tau_i'\Delta_{i_2} L_i$. Further, since $\Delta_{i_1}, \Delta_{i_2}, L_i$ all are odd integers, one can easily observe, by (7.16), that the integers G_i and $\tau_i \ell_{i_2}$ are of the same parity.

When G_i is even, we observe that the integer $\tau_i \ell_{i_2}$ is even. Since G_i divides $1 - \tau_i'\Delta_{i_1}$, we note that the integer τ_i' is odd. From this, one can easily see that the integer A_i is odd. This, by (7.17), gives $O(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i'}) = 4$.

On the other hand, when G_i is odd, we see that the integer $\tau_i \ell_{i_2}$ is odd. Next we note that the integer τ_i' is odd if the integer $\frac{1-\tau_i'\Delta_{i_1}}{G_i}$ is even, while the integer τ_i' is even if the integer $\frac{1-\tau_i'\Delta_{i_1}}{G_i}$ is odd. That is, the integers $\frac{1-\tau_i'\Delta_{i_1}}{G_i}$ and τ_i' are of the opposite parity. Now as both the integers $\Delta_{i_2} L_i$ and $\tau_i \ell_{i_2}$ are odd, we note that the integer A_i is odd. This, by (7.17), implies that $O(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i'}) = 4$. Next we note that $\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')} = \overline{\phi}_{i_1}^{\frac{(q^{d_{i_1}}-1)(A_i+2)}{4}}$. From this, one can easily observe that the characters $\overline{\phi}_{i_1}^{\Delta_{i_1} K_i'}$ and $\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}$ are inverses of each other, which implies that $O(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i'}) = O(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}) = 4$. As $\Delta_{i_1} = \frac{q^{d_{i_1}}-1}{2(q-1)}$ is odd, we see that $q \equiv 1 \pmod 4$ and $\frac{d_{i_1}}{2}$ is odd. So we shall consider the following two cases separately: (i) $p \equiv 3 \pmod 4$, and (ii) $p \equiv 1 \pmod 4$.

(i) When $p \equiv 3 \pmod 4$, we note that the integer r must be even. That is, $p \equiv -1 \pmod 4$ and the integer $\frac{r d_{i_1}}{2}$ is even. Further, by Theorem 2.2.2, we get

$G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}, \chi_{i_1}) = G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}, \chi_{i_1}) = (-1)^{\frac{rd_{i_1}}{2}-1} q^{\frac{d_{i_1}}{2}} = -q^{\frac{d_{i_1}}{2}}$. Now working in a similar manner as in part (a), we get

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 1 + q^{\frac{d_{i_1}}{2}} + 2(-1)^{\frac{rd_{i_2}+b_{t_i,i_1}^{(i)}+2b_{t_i,i_2}^{(i)}}{2}} q^{\frac{d_{i_1}+d_{i_2}}{2}} & \text{if } 2 \mid b_{t_i,i_1}^{(i)}; \\ 1 - q^{\frac{d_{i_1}}{2}} & \text{if } 2 \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

(ii) Let $p \equiv 1 \pmod 4$. As $O(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}) = O(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}) = 4$ divides $p-1$, by Theorem 11.4.4 of [11, p. 356], we note that there exists a multiplicative character ϕ of $\mathbb{F}_p$ having order 4 such that

$$\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}(\alpha) = \phi(N_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_p}(\alpha)) \text{ and } \overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}(\alpha) = \overline{\phi}(N_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_p}(\alpha)) \tag{7.18}$$

for all $\alpha \in \mathbb{F}_{q^{d_{i_1}}}$, where $N_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_p}$ denotes the norm function from $\mathbb{F}_{q^{d_{i_1}}}$ onto $\mathbb{F}_p$. Further, by Davenport-Hasse's Theorem (see Theorem 11.5.2 of [11, p. 360]) and by using the fact that the integer rd_{i_1} is even, we obtain

$$G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}, \chi_{i_1}) = -G(\phi, \chi')^{rd_{i_1}} \text{ and } G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}, \chi_{i_1}) = -G(\overline{\phi}, \chi')^{rd_{i_1}},$$

where χ' is the canonical additive character of $\mathbb{F}_p$. This gives

$$F_i(y_{t_i,i_1}^{(i)}) = -\phi_{i_1}^{\Delta_{i_1}K_i'}(y_{t_i,i_1}^{(i)}) \Big(G(\overline{\phi}, \chi')^{rd_{i_1}} + G(\phi, \chi')^{rd_{i_1}} (-1)^{b_{t_i,i_1}^{(i)}} \Big).$$

As $\zeta = \zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{p-1}}$ is a primitive element of $\mathbb{F}_p$, we note, by (7.18), that

$$\overline{\phi}_{i_1}^{\Delta_{i_1}K_i'}(\zeta_{i_1}) = e^{\frac{2\pi\iota(q^{d_{i_1}}-1)A_i}{(q^{d_{i_1}}-1)4}} = \iota^{A_i} = \overline{\phi}(N_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_p}(\zeta_{i_1})) = \overline{\phi}(\zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{p-1}}) = \overline{\phi}(\zeta)$$

and

$$\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i+K_i')}(\zeta_{i_1}) = e^{\frac{2\pi\iota(q^{d_{i_1}}-1)(A_i+2)}{(q^{d_{i_1}}-1)4}} = \iota^{A_i+2} = \phi(N_{\mathbb{F}_{q^{d_{i_1}}}/\mathbb{F}_p}(\zeta_{i_1})) = \phi(\zeta_{i_1}^{\frac{q^{d_{i_1}}-1}{p-1}}) = \phi(\zeta).$$

Since the integer rd_{i_1} is even and $\zeta^{\frac{p-1}{2}} = -1$, by (2.4), we see that

$$G(\overline{\phi}, \chi')^{rd_{i_1}} = \phi^{rd_{i_1}}(-1)\overline{G(\phi, \chi')}^{rd_{i_1}} = \iota^{\frac{(A_i+2)(p-1)rd_{i_1}}{2}}\overline{G(\phi, \chi')}^{rd_{i_1}} = \overline{G(\phi, \chi')}^{rd_{i_1}}. \tag{7.19}$$

Next we assert that

$$F_i(y^{(i)}_{t_i,i_1}) = -\iota^{b^{(i)}_{t_i,i_1}} p^{\frac{rd_{i_1}}{4}} \Big((e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} + (e_i - \iota f_i)^{\frac{rd_{i_1}}{2}} (-1)^{b^{(i)}_{t_i,i_1}} \Big).$$

To prove this assertion, we first see that $\phi_{i_1}^{\Delta_{i_1} K_i'}(y^{(i)}_{t_i,i_1}) = e^{\frac{2\pi\iota(q^{d_{i_1}}-1)A_i b^{(i)}_{t_i,i_1}}{(q^{d_{i_1}}-1)4}} = \iota^{A_i b^{(i)}_{t_i,i_1}}$, and we shall consider the following two cases separately: $A_i \equiv 1 \pmod 4$ and $A_i \equiv 3 \pmod 4$.

When $A_i \equiv 1 \pmod 4$, we see that $\overline{\phi}(\zeta) = \iota$. By Theorem 4.2.3 of [11, p. 163], we note that $G(\overline{\phi}, \chi')^{rd_{i_1}} = p^{\frac{rd_{i_1}}{4}}(e_i + \iota f_i)^{\frac{rd_{i_1}}{2}}$. This, by (7.19), implies that

$$F_i(y^{(i)}_{t_i,i_1}) = -\iota^{b^{(i)}_{t_i,i_1}} p^{\frac{rd_{i_1}}{4}} \Big((e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} + (e_i - \iota f_i)^{\frac{rd_{i_1}}{2}} (-1)^{b^{(i)}_{t_i,i_1}} \Big).$$

When $A_i \equiv 3 \pmod 4$, we note that $\phi(\zeta) = \iota$. By Theorem 4.2.3 of [11, p. 163], we see that $G(\phi, \chi')^{rd_{i_1}} = p^{\frac{rd_{i_1}}{4}}(e_i + \iota f_i)^{\frac{rd_{i_1}}{2}}$. This, by (7.19), implies that

$$\begin{aligned} F_i(y^{(i)}_{t_i,i_1}) &= -(-\iota)^{b^{(i)}_{t_i,i_1}} p^{\frac{rd_{i_1}}{4}} \Big((e_i - \iota f_i)^{\frac{rd_{i_1}}{2}} + (e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} (-1)^{b^{(i)}_{t_i,i_1}} \Big) \\ &= -\iota^{b^{(i)}_{t_i,i_1}} p^{\frac{rd_{i_1}}{4}} \Big((e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} + (e_i - \iota f_i)^{\frac{rd_{i_1}}{2}} (-1)^{b^{(i)}_{t_i,i_1}} \Big), \end{aligned}$$

which proves the assertion. From this and by Theorem 2.2.1, we obtain

$$\Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \begin{cases} 1 + q^{\frac{d_{i_1}}{2}} + 2\, q^{\frac{d_{i_1}+2d_{i_2}}{4}} (-1)^{\frac{2(rd_{i_2} + b^{(i)}_{t_i,i_2}) + b^{(i)}_{t_i,i_1}}{2}} \text{ Re } (e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} \\ \qquad\qquad \text{if } 2 \mid b^{(i)}_{t_i,i_1}; \\ 1 - q^{\frac{d_{i_1}}{2}} + 2\, q^{\frac{d_{i_1}+2d_{i_2}}{4}} (-1)^{\frac{2(rd_{i_2} + b^{(i)}_{t_i,i_2}) + 1 + b^{(i)}_{t_i,i_1}}{2}} \text{ Im } (e_i + \iota f_i)^{\frac{rd_{i_1}}{2}} \\ \qquad\qquad \text{if } 2 \nmid b^{(i)}_{t_i,i_1}. \end{cases}$$

□

In the following theorem, we explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $M_i \geq 3$ and $M_i' = 2$.

Theorem 7.2.7. *Let $M_i \geq 3$, $M_i' = 2$, $y_{t_i,i_1}^{(i)} = \zeta_{i_1}^{b_{t_i,i_1}^{(i)}} \in \mathbb{F}_{q^{d_{i_1}}}^*$ and $y_{t_i,i_2}^{(i)} = \zeta_{i_2}^{b_{t_i,i_2}^{(i)}} \in \mathbb{F}_{q^{d_{i_2}}}^*$, where $0 \leq b_{t_i,i_1}^{(i)} \leq q^{d_{i_1}} - 2$ and $0 \leq b_{t_i,i_2}^{(i)} \leq q^{d_{i_2}} - 2$. Let $S_i = -\frac{\tau_i \ell_{i_2} \Lambda_i}{q-1}\big(1 - \frac{(q^{\eta_i}-1)\tau_i' \Delta_{i_1}}{G_i \Lambda_i}\big) - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{q-1}$. Here S_i is an integer, the integer rd_{i_2} is even and p is an odd prime.*

(a) Let S_i be even. Suppose that there exists a positive integer μ_i' satisfying $p^{\mu_i'} \equiv -1 \pmod{M_i}$. If θ_i is the least positive integer satisfying $p^{\theta_i} \equiv -1 \pmod{M_i}$, then we have $rd_{i_1} = 2\theta_i\gamma_i$ for some positive integer γ_i.

- *If M_i is even and $\frac{\gamma_i(p^{\theta_i}+1)}{M_i}$ is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} + \frac{n_i(q-1)\left(-1+q^{\frac{d_{i_1}}{2}}(M_i-1)\right)\left(1+(-1)^{b_{t_i,i_2}^{(i)}}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_2}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad\qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)} + \frac{M_i}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+q^{\frac{d_{i_1}}{2}}\right)\left(1+(-1)^{b_{t_i,i_2}^{(i)}}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_2}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad\qquad \text{if } M_i \nmid b_{t_i,i_1}^{(i)} + \frac{M_i}{2}. \end{cases}$$

- *If either M_i is odd or $\frac{\gamma_i(p^{\theta_i}+1)}{M_i}$ is even, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\gamma_i}q^{\frac{d_{i_1}}{2}}(M_i-1)\right)\left(1+\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_2}}{2}}(-1)^{b_{t_i,i_2}^{(i)}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)\big)} \\ \qquad\qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\gamma_i}q^{\frac{d_{i_1}}{2}}\right)\left(1+\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_2}}{2}}(-1)^{b_{t_i,i_2}^{(i)}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad\qquad \text{if } M_i \nmid b_{t_i,i_1}^{(i)}. \end{cases}$$

(b) Let S_i be odd. Suppose that there exists a positive integer μ_i satisfying $p^{\mu_i} \equiv -1 \pmod{2M_i}$. If θ_i and θ_i' are the least positive integers satisfying $p^{\theta_i} \equiv$

$-1 \ (mod\ M_i)$ *and* $p^{\theta'_i} \equiv -1 \ (mod\ 2M_i)$, *then we have* $rd_{i_1} = 2\theta_i\gamma_i = 2\theta'_i\gamma'_i$ *for some positive integers* γ_i *and* γ'_i.

- *If* M_i *is even and* $\frac{\gamma_i\gamma'_i(p^{\theta_i}+1)(p^{\theta'_i}+1)}{2M_i^2}$ *is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\Big(1 - \frac{\Big(1+q^{\frac{d_{i_1}}{2}}+(-1)^{\Big(\frac{b_{t_i,i_1}^{(i)}}{M_i}+b_{t_i,i_2}^{(i)}\Big)}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_1}+d_{i_2}}{2}}M_i\Big)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q}\Big(1 - \frac{1-q^{\frac{d_{i_1}}{2}}(M_i-1)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \text{ if } M_i \nmid b_{t_i,i_1}^{(i)} \ \&\ M_i \mid \frac{2b_{t_i,i_1}^{(i)}+M_i}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_1}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \quad \text{if } M_i \nmid b_{t_i,i_1}^{(i)} \ \&\ M_i \nmid \frac{2b_{t_i,i_1}^{(i)}+M_i}{2}. \end{cases}$$

- *If both the integers* $M_i, \frac{\gamma'_i(p^{\theta'_i}+1)}{2M_i}$ *are even and the integer* $\frac{\gamma_i(p^{\theta_i}+1)}{M_i}$ *is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\Big(1 - \frac{\Big(1+q^{\frac{d_{i_1}}{2}}+(-1)^{\Big(\frac{b_{t_i,i_1}^{(i)}}{M_i}+\gamma'_i+b_{t_i,i_2}^{(i)}\Big)}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_1}+d_{i_2}}{2}}M_i\Big)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q}\Big(1 - \frac{1-q^{\frac{d_{i_1}}{2}}(M_i-1)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \text{ if } M_i \nmid b_{t_i,i_1}^{(i)} \ \&\ M_i \mid \frac{2b_{t_i,i_1}^{(i)}+M_i}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_1}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \ \text{if } M_i \nmid b_{t_i,i_1}^{(i)} \ \&\ M_i \nmid \frac{2b_{t_i,i_1}^{(i)}+M_i}{2}. \end{cases}$$

- *If either* M_i *is odd or* $\frac{\gamma_i(p^{\theta_i}+1)}{M_i}$ *is even and* $\frac{\gamma'_i(p^{\theta'_i}+1)}{2M_i}$ *is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\Big(1 - \frac{\Big(1-(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}(M_i-1)+\mathcal{X}_iM_i\Big)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) \text{ if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\Big(1+(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}\Big)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \qquad \text{if } M_i \nmid b_{t_i,i_1}^{(i)}, \end{cases}$$

  where $\mathcal{X}_i = (-1)^{\Big(\frac{b_{t_i,i_1}^{(i)}}{M_i}+b_{t_i,i_2}^{(i)}\Big)}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_1}+d_{i_2}}{2}}$.

- *If* $\frac{\gamma'_i(p^{\theta'_i}+1)}{2M_i}$ *is even and either* M_i *is odd or the integer* $\frac{\gamma_i(p^{\theta_i}+1)}{M_i}$ *is even,*

then we have

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q}\Big(1 - \frac{\left(1-(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}(M_i-1)+\mathcal{Y}_iM_i\right)}{(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)}\Big) & \text{if } M_i \mid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \nmid b_{t_i,i_1}^{(i)}, \end{cases}$$

where $\mathcal{Y}_i = (-1)^{\left(\frac{b_{t_i,i_1}^{(i)}}{M_i}+\gamma_i'+b_{t_i,i_2}^{(i)}\right)}\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_1}+d_{i_2}}{2}}$.

Proof. To determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we note, by Lemma 7.2.3, that it is enough to determine the explicit value of the sum

$$\begin{aligned}\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 &- \sum_{z_1=1}^{M_i-1} G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_iz_1}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K_iz_1}(y_{t_i,i_1}^{(i)}) \\ &+ G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)})\Bigg(\sum_{z_1=0}^{M_i-1} G(\overline{\phi}_{i_1}^{\Delta_{i_1}(K_i'+z_1K_i)}, \chi_{i_1}) \\ &\times \phi_{i_1}^{\Delta_{i_1}(K_i'+z_1K_i)}(y_{t_i,i_1}^{(i)})\Bigg).\end{aligned} \tag{7.20}$$

Towards this, as $M_i' = 2$, we see that $\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_2}}}$ and q is odd. Since $\gcd(L_i, q-1) = 1$, one can easily observe that the integer L_i is odd. Further, for $0 \le z_1 \le M_i - 1$, we note that

$$\begin{aligned}\Delta_{i_1}(K_i' + z_1K_i) &= \frac{q^{d_{i_1}}-1}{g_{i_1}(q^{\eta_i}-1)\Lambda_i'g_{i_2}H_i}\Bigg(-\Lambda_i\tau_i\ell_{i_2}\Big(1 - \frac{(q^{\eta_i}-1)\tau_i'\Delta_{i_1}}{G_i\Lambda_i}\Big) \\ &\quad -\tau_i'(q^{d_{i_2}}-1)L_i + \frac{z_1(q^{\eta_i}-1)(q-1)\Lambda_i'g_{i_2}H_i}{G_i\Lambda_i}\Bigg).\end{aligned}$$

Now as $M_i' = 2$, for $0 \le z_1 \le M_i - 1$, we get

$$\Delta_{i_1}(K_i' + z_1K_i) = \frac{(q^{d_{i_1}}-1)(S_i+2z_1)}{2M_i}. \tag{7.21}$$

Note that S_i is an integer. Now we shall distinguish the following two cases: (a) S_i is even and (b) S_i is odd.

(a) Let S_i be even. As $O(\phi_{i_1}^{\Delta_{i_1}K_i}) = O(\phi_{i_1}^{\frac{q^{d_{i_1}}-1}{M_i}}) = M_i$, we see that $\phi_{i_1}^{\frac{(q^{d_{i_1}}-1)S_i}{2M_i}} \in \langle \phi_{i_1}^{\Delta_{i_1}K_i} \rangle$. This, by (7.21), gives $\{\phi_{i_1}^{\Delta_{i_1}(K_i'+z_1K_i)} : 0 \leq z_1 \leq M_i - 1\} = \langle \phi_{i_1}^{\Delta_{i_1}K_i} \rangle$. Therefore equation (7.20) can be rewritten as

$$\begin{aligned}\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) &= \Big(-1 + \sum_{z_1=1}^{M_i-1} G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_iz_1}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K_iz_1}(y_{t_i,i_1}^{(i)}) \Big) \\ &\quad \times \Big(-1 + G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}) \Big) \quad (7.22)\end{aligned}$$

Next we assert that the integer d_{i_2} is even in this case.

To prove this, we suppose, on the contrary, that the integer d_{i_2} is odd. This implies that both the integers η_i and Δ_{i_2} are odd. Since $M_i' = 2$, we note that $g_{i_2} \mid 2$. As d_{i_2} is odd, we must have $g_{i_2} = 1$. This gives $\frac{(q^{\eta_i}-1)\Lambda_i'H_i}{G_i\Lambda_i} = 2$, which implies that $\frac{(q^{\eta_i}-1)\Lambda_i'H_i}{q-1} = 2\big(\frac{G_i\Lambda_i}{q-1}\big)$. From this, we note that $2 \mid \frac{(q^{\eta_i}-1)\Lambda_i'H_i}{q-1}$, which implies that $2 \mid \Lambda_i'H_i = \gcd(\Lambda_iH_i, \Delta_{i_2}G_iL_i - \Delta_{i_1}\tau_i\ell_{i_2})$. Further, it is easy to see that the integer Δ_{i_1} must be odd, which implies that the integers G_i and $\tau_i\ell_{i_2}$ are of the same parity. Further, since both Δ_{i_1} and η_i are odd, one can observe that the integer $\frac{G_i\Lambda_i}{q-1} = \gcd\big(\frac{\Delta_{i_1}(q^{\eta_i}-1)}{q-1}, G_i\big)$ is odd.

When G_i is even, both the integers $\frac{q-1}{\Lambda_i}$ and $\tau_i\ell_{i_2}$ are even. As $\frac{\tau_i'\Delta_{i_1}(q^{\eta_i}-1)}{G_i\Lambda_i} \equiv 1 \pmod{\frac{q-1}{\Lambda_i}}$, the integer τ_i' must be odd, which implies that the integer S_i is odd. This is a contradiction.

On the other hand, when G_i is odd, we see that both the integers $\frac{q-1}{\Lambda_i}, \tau_i\ell_{i_2}$ are odd. Further, since $\frac{\tau_i'\Delta_{i_1}(q^{\eta_i}-1)}{G_i\Lambda_i} \equiv 1 \pmod{\frac{q-1}{\Lambda_i}}$ and $\frac{\Delta_{i_1}(q^{\eta_i}-1)}{G_i\Lambda_i}$ is odd, we note that τ_i' is odd if $\frac{\Lambda_i}{q-1}\big(1 - \frac{\tau_i'\Delta_{i_1}(q^{\eta_i}-1)}{G_i\Lambda_i}\big)$ is even, while τ_i' is even if $\frac{\Lambda_i}{q-1}\big(1 - \frac{\tau_i'\Delta_{i_1}(q^{\eta_i}-1)}{G_i\Lambda_i}\big)$ is odd. Now as both the integers $\frac{(q^{d_{i_2}}-1)L_i}{q-1}$ and $\tau_i\ell_{i_2}$ are odd, we note that the integer S_i is odd, which is a contradiction.

This proves the assertion that the integer d_{i_2} is even. Now by Theorem 2.2.1, we see that

$$G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}},\chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}) = -\iota^{\frac{rd_{i_2}(p-1)^2}{4}}q^{\frac{d_{i_2}}{2}}(-1)^{b_{t_i,i_2}^{(i)}}. \tag{7.23}$$

Further, for $1 \leq z_1 \leq M_i - 1$, by Theorem 2.2.2, we note that

$$G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_iz_1},\chi_{i_1}) = \begin{cases} (-1)^{z_1}q^{\frac{d_{i_1}}{2}} & \text{if } M_i \text{ is even and } \frac{p\gamma_i(p^{\theta_i}+1)}{M_i} \text{ is odd;} \\ (-1)^{\gamma_i-1}q^{\frac{d_{i_1}}{2}} & \text{otherwise.} \end{cases} \tag{7.24}$$

Now on substituting the values of Gauss sums from (7.23) and (7.24) in equation (7.22) and after an easy computation, we obtain the desired values of $\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ in the respective cases.

(b) Next let S_i be odd. Since $O(\phi_{i_1}^{\frac{q^{d_{i_1}}-1}{2M_i}}) = 2M_i$, we see that $\phi_{i_1}^{\frac{(q^{d_{i_1}}-1)S_i}{2M_i}} \in \langle \phi_1^{\frac{q^{d_{i_1}}-1}{2M_i}} \rangle$. Further, by (7.21), we note that $\left\{\phi_{i_1}^{\Delta_{i_1}(K_i'+z_1K_i)} : 0 \leq z_1 \leq M_i - 1\right\} = \left\{\phi_{i_1}^{\frac{(q^{d_{i_1}}-1)(1+2z_1)}{2M_i}} : 0 \leq z_1 \leq M_i - 1\right\}$. In view of this, equation (7.20) can be rewritten as

$$\begin{aligned}\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 &- \sum_{z_1=1}^{M_i-1} G(\overline{\phi}_{i_1}^{\Delta_{i_1}K_iz_1},\chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K_iz_1}(y_{t_i,i_1}^{(i)}) \\ &+ G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}},\chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)})\Bigg(\sum_{z_1=0}^{M_i-1} G(\overline{\phi}_{i_1}^{\frac{(q^{d_{i_1}}-1)(1+2z_1)}{2M_i}},\chi_{i_1}) \\ &\times \phi_{i_1}^{\frac{(q^{d_{i_1}}-1)(1+2z_1)}{2M_i}}(y_{t_i,i_1}^{(i)})\Bigg).\end{aligned} \tag{7.25}$$

We next assert that the integer rd_{i_2} is even.

To prove this assertion, we suppose, on the contrary, that rd_{i_2} is odd. As d_{i_2} is odd, the integer η_i is odd. Now working in a similar manner as in part (a),

one can easily observe that the integer Δ_{i_1} is odd. Further, since the integer rd_{i_1} is even, we see that the integer g_{i_1} is even. Now as $p^{\theta_i'} \equiv -1 \pmod{2M_i}$ and $g_{i_1} \mid M_i$, we note that $p \equiv 3 \pmod 4$. Further, since $rd_{i_1} = 2\theta_i'\gamma_i'$ and $2M_i \mid p^{\theta_i'} + 1$, we observe that the integer $\frac{q^{d_{i_1}}-1}{2M_i}$ is even. On the other hand, let $\varkappa_i$ be the positive integer such that $2^{\varkappa_i} \mid\mid g_{i_1}$, i.e., $2^{\varkappa_i} \mid g_{i_1}$ but $2^{\varkappa_i+1} \nmid g_{i_1}$. Since both r, η_i are odd, we see that $2 \mid\mid q-1$ and $2 \mid\mid q^{\eta_i}-1$. Further, since Δ_{i_1} is odd, one can easily observe that $2^{\varkappa_i+1} \mid\mid q^{d_{i_1}}-1$ and the integer $\frac{G_i\Lambda_i}{q-1} = \gcd(\frac{\Delta_{i_1}(q^{\eta_i}-1)}{q-1}, G_i)$ is odd. From this, it follows that the integer $\frac{q^{d_{i_1}}-1}{2M_i}$ is odd, which is a contradiction.

This proves the assertion that the integer rd_{i_2} is even. Further, for $1 \leq \kappa \leq 2M_i - 1$, by Theorem 2.2.2, we note that

$$G(\overline{\phi}_{i_1}^{\frac{(q^{d_{i_1}}-1)\kappa}{2M_i}}, \chi_{i_1}) = \begin{cases} (-1)^{\kappa} q^{\frac{d_{i_1}}{2}} & \text{if } \frac{p\gamma_i'(p^{\theta_i'}+1)}{2M_i} \text{ is odd;} \\ (-1)^{\gamma_i'-1} q^{\frac{d_{i_1}}{2}} & \text{otherwise.} \end{cases} \tag{7.26}$$

Now on substituting the values of Gauss sums from (7.23), (7.24) and (7.26) in equation (7.25) and after an easy computation, we obtain the desired values of the sum $\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ in the respective cases.

□

Now we proceed to explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $M_i' \geq 3$. From this point on, throughout this section, suppose that there exists a positive integer e_i' satisfying $p^{e_i'} \equiv -1 \pmod{M_i'}$. Further, let e_i be the least positive integer satisfying $p^{e_i} \equiv -1 \pmod{M_i'}$. Then by Theorem 2.2.2, we have $rd_{i_2} = 2e_i\varrho_i$ for some positive integer ϱ_i, and for $1 \leq z_2 \leq M_i' - 1$, we have

$$G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i z_2}{H_i\Lambda_i'}}, \chi_{i_2}) = \begin{cases} (-1)^{z_2} q^{\frac{d_{i_2}}{2}} & \text{if } M_i' \text{ is even and } \frac{p\varrho_i(p^{e_i}+1)}{M_i'} \text{ is odd;} \\ (-1)^{\varrho_i-1} q^{\frac{d_{i_2}}{2}} & \text{otherwise.} \end{cases} \tag{7.27}$$

In the following theorem, we explicitly determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$

when $M_i = 1$ and $M_i' \geq 3$.

Theorem 7.2.8. *Let $M_i = 1$, $M_i' \geq 3$, $B_i = -\frac{\Lambda_i \tau_i \ell_{i_2}}{G_i \Lambda_i g_{i_2}}\big(1 - \frac{(q^{\eta_i}-1)\tau_i' \Delta_{i_1}}{G_i \Lambda_i}\big) - \frac{\tau_i'(q^{d_{i_2}}-1)L_i}{g_{i_2} G_i \Lambda_i}$, $y_{t_i,i_1}^{(i)} = \zeta_{i_1}^{b_{t_i,i_1}^{(i)}} \in \mathbb{F}_{q^{d_{i_1}}}^*$ and $y_{t_i,i_2}^{(i)} = \zeta_{i_2}^{b_{t_i,i_2}^{(i)}} \in \mathbb{F}_{q^{d_{i_2}}}^*$, where $0 \leq b_{t_i,i_1}^{(i)} \leq q^{d_{i_1}} - 2$ and $0 \leq b_{t_i,i_2}^{(i)} \leq q^{d_{i_2}} - 2$. Further, let us define the integers $T_i = \gcd\big(B_i, \frac{(q^{\eta_i}-1)\Lambda_i' H_i}{G_i \Lambda_i}\big)$ and $N_i = \frac{(q^{\eta_i}-1)\Lambda_i' H_i}{G_i \Lambda_i T_i}$, (note that $N_i \mid M_i'$).*

(a) Let $N_i = 1$.

- *If $T_i g_{i_2}$ is even and $\frac{p\varrho_i(p^{e_i}+1)}{T_i g_{i_2}}$ is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)} + \frac{T_i g_{i_2}}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_2}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \nmid b_{t_i,i_2}^{(i)} + \frac{T_i g_{i_2}}{2}. \end{cases}$$

- *If either $T_i g_{i_2}$ is odd or $\frac{p\varrho_i(p^{e_i}+1)}{T_i g_{i_2}}$ is even, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \nmid b_{t_i,i_2}^{(i)}. \end{cases}$$

(b) When $N_i = 2$, the integer rd_{i_1} is even and p is an odd prime.

- *If $\frac{\varrho_i(p^{e_i}+1)}{2T_i g_{i_2}}$ is odd, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1)+\mathcal{U}_i T_i g_{i_2}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_2}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \nmid b_{t_i,i_2}^{(i)}, \end{cases}$$

where $\mathcal{U}_i = \iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{\left(\frac{b_{t_i,i_2}^{(i)}}{T_i g_{i_2}} + b_{t_i,i_1}^{(i)}\right)} q^{\frac{d_{i_1}+d_{i_2}}{2}}$.

- *If* $\frac{\varrho_i(p^{e_i}+1)}{2T_ig_{i_2}}$ *is even, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})=\begin{cases}\frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}\left(T_ig_{i_2}-1+\mathcal{V}_iT_ig_{i_2}\right)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)};\\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)},\end{cases}$$

where $\mathcal{V}_i = \iota^{\frac{rd_{i_1}(p-1)^2}{4}} q^{\frac{d_{i_1}}{2}} (-1)^{\left(\frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}}+b_{t_i,i_1}^{(i)}\right)}$.

(c) *Let* $N_i \geq 3$. *There exists a least positive integer* ω_i *satisfying* $p^{\omega_i} \equiv -1 \pmod{N_i}$. *Here we have* $rd_{i_1} = 2\omega_i\vartheta_i$ *for some positive integer* ϑ_i.

- *If either the integer* $T_iN_ig_{i_2}$ *is odd or both the integers* $T_iN_ig_{i_2}$, $\frac{p\varrho_i(p^{e_i}+1)}{T_iN_ig_{i_2}}$ *are even and* N_i *is odd or both the integers* $\frac{p\vartheta_i(p^{\omega_i}+1)}{N_i}$, $\frac{p\varrho_i(p^{e_i}+1)}{T_iN_ig_{i_2}}$ *are of the same parity and* N_i *is even, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})=\begin{cases}\frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1-(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)};\\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}(T_ig_{i_2}-1+(-1)^{\vartheta_i}T_ig_{i_2}(N_i-1)q^{\frac{d_{i_1}}{2}})\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)} \ \&\ N_i \mid \frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}} + \frac{B_ib_{t_i,i_1}^{(i)}}{T_i};\\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}(T_ig_{i_2}-1-(-1)^{\vartheta_i}T_ig_{i_2}q^{\frac{d_{i_1}}{2}})\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)} \ \&\ N_i \nmid \frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}} + \frac{B_ib_{t_i,i_1}^{(i)}}{T_i}.\end{cases}$$

- *If* $T_iN_ig_{i_2}$ *is even,* $\frac{p\varrho_i(p^{e_i}+1)}{T_iN_ig_{i_2}}$ *is odd and either* N_i *is odd or* $\frac{p\vartheta_i(p^{\omega_i}+1)}{N_i}$ *is*

even, then we have

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_2}}{2}})}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \nmid \frac{M_i'+2b_{t_i,i_2}^{(i)}}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}(1+(N_i-1)(-1)^{\vartheta_i}q^{\frac{d_{i_1}}{2}})-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } T_i g_{i_2} \mid \frac{M_i'+2b_{t_i,i_2}^{(i)}}{2} \ \&\ N_i \mid \frac{M_i'+2b_{t_i,i_2}^{(i)}}{2T_i g_{i_2}} + \frac{B_i b_{t_i,i_1}^{(i)}}{T_i}; & \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}(1-q^{\frac{d_{i_1}}{2}}(-1)^{\vartheta_i})-1)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } T_i g_{i_2} \mid \frac{M_i'+2b_{t_i,i_2}^{(i)}}{2} \ \&\ N_i \nmid \frac{M_i'+2b_{t_i,i_2}^{(i)}}{2T_i g_{i_2}} + \frac{B_i b_{t_i,i_1}^{(i)}}{T_i}. \end{cases}$$

- *If* $\frac{p\vartheta_i(p^{\omega_i}+1)}{N_i}$ *is odd and both* $N_i, \frac{p\varrho_i(p^{e_i}+1)}{T_i N_i g_{i_2}}$ *are even, then we have*

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } T_i g_{i_2} \nmid b_{t_i,i_2}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1-q^{\frac{d_{i_1}}{2}}(N_i-1)T_i g_{i_2})\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)} \ \&\ N_i \mid \frac{b_{t_i,i_2}^{(i)}}{T_i g_{i_2}} + \frac{B_i b_{t_i,i_1}^{(i)}}{T_i} + \frac{N_i}{2}; & \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1+q^{\frac{d_{i_1}}{2}}T_i g_{i_2})\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)} \ \&\ N_i \nmid \frac{b_{t_i,i_2}^{(i)}}{T_i g_{i_2}} + \frac{B_i b_{t_i,i_1}^{(i)}}{T_i} + \frac{N_i}{2}. \end{cases}$$

Proof. To determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$, we note, by Lemma 7.2.3, that it is enough to determine the explicit value of the sum

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 + \sum_{z_2=1}^{M_i'-1} \Big(G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i z_2}{H_i \Lambda_i'}}, \chi_{i_2}) \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i z_2}{H_i \Lambda_i'}}(y_{t_i,i_2}^{(i)}) G(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i' z_2}, \chi_{i_1}) \phi_{i_1}^{\Delta_{i_1} K_i' z_2}(y_{t_i,i_1}^{(i)}) \Big). \tag{7.28}$$

Towards this, we note that as $M_i = 1$, we must have $g_{i_1} = 1$ and $G_i \Lambda_i = q - 1$.

Further, it is easy to observe that

$$\begin{aligned}\Delta_{i_1}K_i' &= \frac{(q^{d_{i_1}}-1)G_i\Lambda_i}{(q^{\eta_i}-1)\Lambda_i' g_{i_2}H_i}\Big(-\frac{\Lambda_i\tau_i\ell_{i_2}}{G_i\Lambda_i}\Big(1-\frac{(q^{\eta_i}-1)\tau_i'\Delta_{i_1}}{G_i\Lambda_i}\Big)-\frac{\tau_i'(q^{d_{i_2}}-1)L_i}{G_i\Lambda_i}\Big)\\ &= \frac{(q^{d_{i_1}}-1)G_i\Lambda_i B_i}{(q^{\eta_i}-1)\Lambda_i' H_i}. \qquad (7.29)\end{aligned}$$

Note that B_i is an integer. Next by (7.29), we note that $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = \frac{(q^{\eta_i}-1)\Lambda_i'H_i}{G_i\Lambda_i T_i} = N_i$. Now we shall consider the following three cases separately: (a) $N_i = 1$, (b) $N_i = 2$, and (c) $N_i \geq 3$.

(a) Let $N_i = 1$. Here by (2.4) and (7.28), we see that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 - \sum_{z_2=1}^{T_i g_{i_2}-1} G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i z_2}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i z_2}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}).$$

When $T_i g_{i_2}$ is even and $\frac{p\varrho_i(p^{e_i}+1)}{T_i g_{i_2}}$ is odd, we observe, by (7.27), that

$$\begin{aligned}\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) &= 1 - q^{\frac{d_{i_2}}{2}} \sum_{z_2=1}^{T_i g_{i_2}-1} (-1)^{z_2}\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i z_2}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)})\\ &= 1 - q^{\frac{d_{i_2}}{2}} \sum_{z_2=1}^{T_i g_{i_2}-1} e^{\pi\iota z_2} e^{\frac{2\pi\iota z_2 b_{t_i,i_2}^{(i)}}{T_i g_{i_2}}}\\ &= 1 - q^{\frac{d_{i_2}}{2}} \sum_{z_2=1}^{T_i g_{i_2}-1} e^{\frac{2\pi\iota z_2}{T_i g_{i_2}}\left(b_{t_i,i_2}^{(i)} + \frac{T_i g_{i_2}}{2}\right)}\\ &= \begin{cases} 1 - q^{\frac{d_{i_2}}{2}}(T_i g_{i_2}-1) & \text{if } T_i g_{i_2} \mid b_{t_i,i_2}^{(i)} + \frac{T_i g_{i_2}}{2};\\ 1 + q^{\frac{d_{i_2}}{2}} & \text{if } T_i g_{i_2} \nmid b_{t_i,i_2}^{(i)} + \frac{T_i g_{i_2}}{2}. \end{cases}\end{aligned}$$

On the other hand, when either $T_i g_{i_2}$ is odd or $\frac{p\varrho_i(p^{e_i}+1)}{T_i g_{i_2}}$ is even, we observe, by (7.27), that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 - (-1)^{\varrho_i - 1} q^{\frac{d_{i_2}}{2}} \sum_{z_2=1}^{T_i g_{i_2}-1} \phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i z_2}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)})$$

$$= \begin{cases} 1-(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}}(T_ig_{i_2}-1) & \text{if } T_ig_{i_2} \mid b^{(i)}_{t_i,i_2}; \\ 1+(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}} & \text{if } T_ig_{i_2} \nmid b^{(i)}_{t_i,i_2}. \end{cases}$$

(b) Let $N_i = 2$. Here we see that $\phi_{i_1}^{\Delta_{i_1}K'_i}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_1}}}$ and q is odd. Further, each integer z_2 satisfying $1 \le z_2 < M'_i = 2T_ig_{i_2}$ can be uniquely expressed as $z_2 = 2Q+R$, where $0 \le Q < T_ig_{i_2}$ when $R = 1$ and $0 < Q < T_ig_{i_2}$ when $R = 0$. In view of this, equation (7.28) can be rewritten as

$$\begin{aligned} \Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) &= 1 - \sum_{Q=1}^{T_ig_{i_2}-1} G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i 2Q}{H_i\Lambda'_i}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i 2Q}{H_i\Lambda'_i}}(y^{(i)}_{t_i,i_2}) \\ &\quad + G(\overline{\phi}_{i_1}^{\Delta_{i_1}K'_i}, \chi_{i_1})\phi_{i_1}^{\Delta_{i_1}K'_i}(y^{(i)}_{t_i,i_1})\Bigg(\sum_{Q=0}^{T_ig_{i_2}-1} G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i(2Q+1)}{H_i\Lambda'_i}}, \chi_{i_2}) \\ &\quad \times \phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i(2Q+1)}{H_i\Lambda'_i}}(y^{(i)}_{t_i,i_2})\Bigg). \end{aligned} \tag{7.30}$$

We further assert that the integer rd_{i_1} is even.

To prove this assertion, we suppose, on the contrary, that the integer rd_{i_1} is odd. From this, it follows that both the integers η_i and Δ_{i_1} are odd. As rd_{i_2} is even, we see that the integer d_{i_2} is even. Further, since $N_i = \frac{(q^{\eta_i}-1)\Lambda'_iH_i}{G_i\Lambda_iT_i} = 2$ and $G_i\Lambda_i = q-1$, we observe that $2 \mid \Lambda'_iH_i = \gcd(\Lambda_iH_i, \Delta_{i_2}G_iL_i - \frac{\Delta_{i_1}\tau_i\ell_{i_2}}{g_{i_2}})$. Now we see that $\gcd(\Delta_{i_2}, \frac{\ell_{i_2}}{g_{i_2}}) = 1$. Further, it is easy to observe that the integer Δ_{i_2} is odd, which implies that the integer g_{i_2} is even. Next as $rd_{i_2} = 2e_i\varrho_i$ and $p^{e_i} \equiv -1 \pmod{2T_ig_{i_2}}$, we note that the integer $\frac{q^{d_{i_2}}-1}{2T_ig_{i_2}}$ is even. On the other hand, since g_{i_2} is even, there exists a positive integer ς_i such that $2^{\varsigma_i} \mid\mid g_{i_2}$. Further, since $p^{e_i} \equiv -1 \pmod{2T_ig_{i_2}}$, we note that $p \equiv 3 \pmod 4$. As both r, η_i are odd, we observe that $2 \mid\mid q-1$ and $2 \mid\mid q^{\eta_i}-1$. Now as $\Delta_{i_2} = \frac{q^{d_{i_2}}-1}{(q^{\eta_i}-1)g_{i_2}}$ is odd, it is easy to see that $2^{\varsigma_i+1} \mid\mid q^{d_{i_2}}-1$. Since $\Lambda'_iH_i \mid G_i\Lambda_i = q-1$, we get $2 \mid\mid \Lambda'_iH_i$. From this, we see that the integer $T_i = \frac{(q^{\eta_i}-1)\Lambda'_iH_i}{(q-1)2}$ is odd, which

further implies that the integer $\frac{q^{d_{i_2}}-1}{2T_ig_{i_2}}$ is odd. This is a contradiction.

This proves the assertion that the integer rd_{i_1} is even.

(i) Now when $\frac{\varrho_i(p^{e_i}+1)}{2T_ig_{i_2}}$ is odd, by (7.27), we note that

$$\begin{aligned}\sum_{Q=0}^{T_ig_{i_2}-1} G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i(2Q+1)}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i(2Q+1)}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}) &= -q^{\frac{d_{i_2}}{2}} \sum_{Q=0}^{T_ig_{i_2}-1} e^{\frac{\pi\iota b_{t_i,i_2}^{(i)}}{T_ig_{i_2}}+\frac{2\pi\iota b_{t_i,i_2}^{(i)}Q}{T_ig_{i_2}}} \\ &= \begin{cases} -T_ig_{i_2}q^{\frac{d_{i_2}}{2}}(-1)^{\frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}}} & \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)}; \\ 0 & \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)} \end{cases}\end{aligned}$$

and

$$\sum_{Q=1}^{T_ig_{i_2}-1} G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i 2Q}{H_i\Lambda_i'}}, \chi_{i_2})\phi_{i_2}^{\frac{\Delta_{i_2}G_i\Lambda_i 2Q}{H_i\Lambda_i'}}(y_{t_i,i_2}^{(i)}) = \begin{cases} q^{\frac{d_{i_2}}{2}}(T_ig_{i_2}-1) & \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)}; \\ -q^{\frac{d_{i_2}}{2}} & \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)}. \end{cases}$$

From this and by (7.30) and by Theorem 2.2.1, we obtain

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 1-q^{\frac{d_{i_2}}{2}}(T_ig_{i_2}-1)+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{\left(\frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}}+b_{t_i,i_1}^{(i)}\right)}q^{\frac{d_{i_1}+d_{i_2}}{2}}T_ig_{i_2} & \\ \qquad\qquad \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)}; & \\ 1+q^{\frac{d_{i_2}}{2}} \qquad\qquad \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)}. & \end{cases}$$

(ii) When $\frac{\varrho_i(p^{e_i}+1)}{2T_ig_{i_2}}$ is even, working in a similar manner as in case (i), we obtain

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 1+(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}}\left(T_ig_{i_2}-1+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}q^{\frac{d_{i_1}}{2}}(-1)^{\left(\frac{b_{t_i,i_2}^{(i)}}{T_ig_{i_2}}+b_{t_i,i_1}^{(i)}\right)}T_ig_{i_2}\right) & \\ \qquad\qquad \text{if } T_ig_{i_2} \mid b_{t_i,i_2}^{(i)}; & \\ 1-(-1)^{\varrho_i}q^{\frac{d_{i_2}}{2}} \qquad\qquad \text{if } T_ig_{i_2} \nmid b_{t_i,i_2}^{(i)}. & \end{cases}$$

(c) Let $N_i \geq 3$. Here for $1 \leq u \leq N_i - 1$, we see, by Theorem 2.2.2, that

$$G(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i' u}, \chi_{i_1}) = \begin{cases} (-1)^u q^{\frac{d_{i_1}}{2}} & \text{if } N_i \text{ is even and } \frac{p\vartheta_i(p^{\omega_i}+1)}{N_i} \text{ is odd;} \\ (-1)^{\vartheta_i - 1} q^{\frac{d_{i_1}}{2}} & \text{otherwise.} \end{cases} \tag{7.31}$$

Further, we note that each integer z_1 satisfying $1 \leq z_1 < M_i' = T_i N_i g_{i_2}$ can be uniquely written as $z_1 = N_i Q + R$, where $0 \leq Q < T_i g_{i_2}$ when $1 \leq R < N_i$, while $1 \leq Q < T_i g_{i_2}$ when $R = 0$. In view of this, equation (7.28) can be rewritten as

$$\begin{aligned} \Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 + \sum_{Q=0}^{T_i g_{i_2}-1} \sum_{R=1}^{N_i - 1} \Big(& G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i (N_i Q + R)}{H_i \Lambda_i'}}, \chi_{i_2}) \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i (N_i Q + R)}{H_i \Lambda_i'}}(y_{t_i,i_2}^{(i)}) \\ & G(\overline{\phi}_{i_1}^{\Delta_{i_1} K_i' R}, \chi_{i_1}) \phi_{i_1}^{\Delta_{i_1} K_i' R}(y_{t_i,i_1}^{(i)}) \Big) - \sum_{Q=1}^{T_i g_{i_2}-1} \Big(G(\overline{\phi}_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i N_i Q}{H_i \Lambda_i'}}, \chi_{i_2}) \\ & \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i N_i Q}{H_i \Lambda_i'}}(y_{t_i,i_2}^{(i)}) \Big). \end{aligned} \tag{7.32}$$

Here we shall consider the case when N_i is even and both the integers $\frac{p\varrho_i(p^{e_i}+1)}{T_i N_i g_{i_2}}$, $\frac{p\vartheta_i(p^{\omega_i}+1)}{N_i}$ are odd. In this case, by (7.27), (7.31) and (7.32), we observe that

$$\Theta_i(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = 1 - q^{\frac{d_{i_2}}{2}} U(y_{t_i,i_2}^{(i)}) + q^{\frac{d_{i_1}+d_{i_2}}{2}} V(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}), \tag{7.33}$$

where

$$U(y_{t_i,i_2}^{(i)}) = \sum_{Q=1}^{T_i g_{i_2}-1} \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i N_i Q}{H_i \Lambda_i'}}(y_{t_i,i_2}^{(i)})$$

and

$$V(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \big(1 + U(y_{t_i,i_2}^{(i)})\big) V'(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$$

with $V'(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \sum_{R=1}^{N_i-1} \phi_{i_2}^{\frac{\Delta_{i_2} G_i \Lambda_i R}{H_i \Lambda_i'}}(y^{(i)}_{t_i,i_2}) \phi_{i_1}^{\Delta_{i_1} K_i' R}(y^{(i)}_{t_i,i_1})$. Next we see that

$$\begin{aligned} U(y^{(i)}_{t_i,i_2}) &= \sum_{Q=1}^{T_i g_{i_2}-1} e^{\frac{2\pi\iota(q^{d_{i_2}}-1) G_i \Lambda_i N_i Q b^{(i)}_{t_i,i_2}}{(q^{\eta_i}-1)(q^{d_{i_2}}-1) g_{i_2} H_i \Lambda_i'}} \\ &= \sum_{Q=1}^{T_i g_{i_2}-1} e^{\frac{2\pi\iota Q b^{(i)}_{t_i,i_2}}{T_i g_{i_2}}} \\ &= \begin{cases} T_i g_{i_2} - 1 & \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2}; \\ -1 & \text{otherwise} \end{cases} \end{aligned}$$

and

$$\begin{aligned} V'(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) &= \sum_{R=1}^{N_i-1} e^{\frac{2\pi\iota R b^{(i)}_{t_i,i_2}}{T_i N_i g_{i_2}} + \frac{2\pi\iota B_i R b^{(i)}_{t_i,i_1}}{T_i N_i}} \\ &= \begin{cases} N_i - 1 & \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \mid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i}; \\ -1 & \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \nmid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i}. \end{cases} \end{aligned}$$

This implies that

$$V(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \begin{cases} T_i g_{i_2}(N_i - 1) & \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \mid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i}; \\ -T_i g_{i_2} & \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \nmid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i}; \\ 0 & \text{if } T_i g_{i_2} \nmid b^{(i)}_{t_i,i_2}. \end{cases}$$

From this and by (7.33), we obtain

$$\Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \begin{cases} 1 + q^{\frac{d_{i_2}}{2}} & \text{if } T_i g_{i_2} \nmid b^{(i)}_{t_i,i_2}; \\ 1 - q^{\frac{d_{i_2}}{2}}(T_i g_{i_2} - 1 - T_i g_{i_2} q^{\frac{d_{i_1}}{2}}(N_i - 1)) & \\ \qquad \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \mid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i}; & \\ 1 - q^{\frac{d_{i_2}}{2}}(T_i g_{i_2} - 1 + T_i g_{i_2} q^{\frac{d_{i_1}}{2}}) & \\ \qquad \text{if } T_i g_{i_2} \mid b^{(i)}_{t_i,i_2} \text{ and } N_i \nmid \frac{b^{(i)}_{t_i,i_2}}{T_i g_{i_2}} + \frac{B_i b^{(i)}_{t_i,i_1}}{T_i} & \end{cases}$$

when N_i is even and both the integers $\frac{p\varrho_i(p^{e_i}+1)}{T_iN_ig_{i_2}}$, $\frac{p\vartheta_i(p^{\omega_i}+1)}{N_i}$ are odd. Working in a similar manner as above, one can also determine explicit values of the sum $\Theta_i(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2})$ in the remaining cases.

□

In the following theorem, we determine the number $D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2})$ when $M_i = 2$ and $M_i' \geq 3$ with either $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = 1$ or $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = 2$.

Theorem 7.2.9. *Let $M_i = 2$, $M_i' \geq 3$, $y^{(i)}_{t_i,i_1} = \zeta_{i_1}^{b^{(i)}_{t_i,i_1}} \in \mathbb{F}^*_{q^{d_{i_1}}}$ and $y^{(i)}_{t_i,i_2} = \zeta_{i_2}^{b^{(i)}_{t_i,i_2}} \in \mathbb{F}^*_{q^{d_{i_2}}}$, where $0 \leq b^{(i)}_{t_i,i_1} \leq q^{d_{i_1}} - 2$ and $0 \leq b^{(i)}_{t_i,i_2} \leq q^{d_{i_2}} - 2$. Suppose that either $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = 1$ or $O(\phi_{i_1}^{\Delta_{i_1}K_i'}) = 2$. Then p is an odd prime, the integer rd_{i_1} is even and the following hold.*

- *If M_i' is even and $\frac{\varrho_i(p^{e_i}+1)}{M_i'}$ is odd, then we have*

$$D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \begin{cases} \frac{n_i(q-1)}{q} + \frac{n_i(q-1)\left(-1+q^{\frac{d_{i_2}}{2}}(M_i'-1)\right)\left(1+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{b^{(i)}_{t_i,i_1}}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad \text{if } M_i' \mid b^{(i)}_{t_i,i_2} + \frac{M_i'}{2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)(1+q^{\frac{d_{i_2}}{2}})\left(1+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{b^{(i)}_{t_i,i_1}}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad \text{if } M_i' \nmid b^{(i)}_{t_i,i_2} + \frac{M_i'}{2}. \end{cases}$$

- *If either M_i' is odd or $\frac{\varrho_i(p^{e_i}+1)}{M_i'}$ is even, then we have*

$$D_i^{(t_i)}(y^{(i)}_{t_i,i_1}, y^{(i)}_{t_i,i_2}) = \begin{cases} \frac{n_i(q-1)}{q} + \frac{n_i(q-1)\left(-1+(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}}(M_i'-1)\right)\left(1+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{b^{(i)}_{t_i,i_1}}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad \text{if } M_i' \mid b^{(i)}_{t_i,i_2}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i-1}q^{\frac{d_{i_2}}{2}}\right)\left(1+\iota^{\frac{rd_{i_1}(p-1)^2}{4}}(-1)^{b^{(i)}_{t_i,i_1}}q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} \\ \qquad \text{if } M_i' \nmid b^{(i)}_{t_i,i_2}. \end{cases}$$

Proof. As $M_i = 2$, we note that $\phi_{i_1}^{\Delta_{i_1}K_i}$ is the quadratic character of $\mathbb{F}_{q^{d_{i_1}}}$ and q

is odd. Now by applying Theorem 2.2.1 and working in a similar manner as in Theorem 7.2.8(a), the desired result follows immediately. □

Next we proceed to determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when both $M_i, M_i' \geq 3$. Towards this, we see, by Lemma 7.2.3, that we need to determine explicit values of the Gauss sums $G(\phi_{i_1}^{\Delta_{i_1} j}, \chi_{i_1})$, where $1 \leq j < (q^{\eta_i} - 1)g_{i_1}$. To do this, we observe that $O(\phi_{i_1}^{\Delta_{i_1}}) = (q^{\eta_i} - 1)g_{i_1} \geq 3$. Now by Theorem 2.2.2, we note that the explicit values of the Gauss sums $G(\phi_{i_1}^{\Delta_{i_1} j}, \chi_{i_1})$, $1 \leq j < (q^{\eta_i} - 1)g_{i_1}$, are known in the semi-primitive case, i.e., when there exists a least positive integer ε_i satisfying $p^{\varepsilon_i} \equiv -1 \pmod{(q^{\eta_i} - 1)g_{i_1}}$. In the semi-primitive case, by Theorem 2.2.2, we note that the integer rd_{i_1} must be even. We also recall that there exists a least positive integer e_i satisfying $p^{e_i} \equiv -1 \pmod{M_i'}$, which implies that $rd_{i_2} = 2e_i\varrho_i$ for some positive integer ϱ_i. That is, the integer rd_{i_2} is also even. From this, it follows that the integer $r\eta_i = \gcd(rd_{i_1}, rd_{i_2})$ is even. Since $q^{\eta_i} - 1 = 1$ or 2 implies that $r\eta_i = 1$, we must have $q^{\eta_i} - 1 \geq 3$. As we have $p^{\varepsilon_i} \equiv -1 \pmod{(q^{\eta_i} - 1)g_{i_1}}$, there exists a least positive integer f_i satisfying $p^{f_i} \equiv -1 \pmod{q^{\eta_i} - 1}$. This, by Theorem 11.6.2 of [11], gives $r\eta_i = 2f_i$. From this, we obtain $q^{\eta_i} - 1 = p^{r\eta_i} - 1 = (p^{f_i} + 1)(p^{f_i} - 1)$, which implies that $\left(\frac{p^{f_i}+1}{q^{\eta_i}-1}\right)(p^{f_i} - 1) = 1$. This gives $p^{f_i} - 1 = 1$, which holds if and only if $f_i = 1$, $p = 2$ and $r\eta_i = 2$. Therefore in the semi-primitive case, we must have $q = 2$ or 4. In the following theorem, we determine the number $D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)})$ when $M_i \geq 3$ and $M_i' \geq 3$ in the semi-primitive case.

Theorem 7.2.10. *Let $M_i \geq 3$, $M_i' \geq 3$, $y_{t_i,i_1}^{(i)} = \zeta_{i_1}^{b_{t_i,i_1}^{(i)}} \in \mathbb{F}_{q^{d_{i_1}}}^*$ and $y_{t_i,i_2}^{(i)} = \zeta_{i_2}^{b_{t_i,i_2}^{(i)}} \in \mathbb{F}_{q^{d_{i_2}}}^*$, where $0 \leq b_{t_i,i_1}^{(i)} \leq q^{d_{i_1}} - 2$ and $0 \leq b_{t_i,i_2}^{(i)} \leq q^{d_{i_2}} - 2$. Suppose that there exist least positive integers ε_i and e_i satisfying $p^{\varepsilon_i} \equiv -1 \pmod{(q^{\eta_i} - 1)g_{i_1}}$ and $p^{e_i} \equiv -1 \pmod{M_i'}$. Then we have $q = 2$ or 4. Furthermore, we have $rd_{i_1} = 2\varepsilon_i\varrho_i'$,*

$rd_{i_2} = 2e_i\varrho_i$ for some positive integers ϱ_i, ϱ_i', and

$$D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1-(-1)^{\varrho_i'} q^{\frac{d_{i_1}}{2}}\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \text{if } M_i \nmid b_{t_i,i_1}^{(i)}; \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i'} q^{\frac{d_{i_1}}{2}}\left((M_i-1)+(-1)^{\varrho_i} q^{\frac{d_{i_2}}{2}} M_i(M_i'-1)\right)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)} \ \&\ M_i' \mid b_{t_i,i_2}^{(i)} + \frac{\Lambda_i' g_{i_2} H_i K_i' b_{t_i,i_1}^{(i)}}{G_i \Lambda_i g_{i_1}}; & \\ \frac{n_i(q-1)}{q} - \frac{n_i(q-1)\left(1+(-1)^{\varrho_i'} q^{\frac{d_{i_1}}{2}}\left((M_i-1)-(-1)^{\varrho_i} q^{\frac{d_{i_2}}{2}} M_i\right)\right)}{q(q^{d_{i_1}}-1)(q^{d_{i_2}}-1)} & \\ \qquad \text{if } M_i \mid b_{t_i,i_1}^{(i)} \ \&\ M_i' \nmid b_{t_i,i_2}^{(i)} + \frac{\Lambda_i' g_{i_2} H_i K_i' b_{t_i,i_1}^{(i)}}{G_i \Lambda_i g_{i_1}}. & \end{cases}$$

Proof. As $p = 2$, by Theorem 2.2.2, we see that $G(\overline{\phi}_{i_1}^{\Delta_{i_1} v}, \chi_{i_1}) = (-1)^{\varrho_i'-1} q^{\frac{d_{i_1}}{2}}$ for $1 \le v < (q^{\eta_i}-1)g_{i_1}$. Further, one can easily observe that $\frac{\Lambda_i' g_{i_2} H_i K_i'}{q-1}$ is an integer. Now working in a similar manner as in Theorem 7.2.8(c), the desired result follows immediately. □

Remark 7.2.11. *By applying Theorems 7.2.2-7.2.10 and by* (7.3)-(7.5)*, one can determine Hamming weights of all non-zero codewords of several classes of Λ-MT codes and their Hamming weight distributions, which we demonstrate in the following section by computing Hamming weight distributions of several classes of MT codes.*

7.3 Hamming weight distributions of MT codes

In this section, we will explicitly determine Hamming weight distributions of several classes of MT codes with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$, whose codewords satisfy the condition (7.1). Using these results, we further identify two classes of optimal equidistant linear codes meeting the Griesmer bound and the Plotkin bound and several other classes of minimal linear codes within these classes of MT codes.

Recall that the support of a vector $v = (v_0, v_1, \cdots, v_{n-1}) \in \mathbb{F}_q^n$, denoted by $\mathrm{supp}(v)$, is defined as the set $\mathrm{supp}(v) = \{i : 0 \le i \le n-1, v_i \ne 0\}$. Further, a vector $u \in \mathbb{F}_q^n$ is said to cover another vector $v \in \mathbb{F}_q^n$ if $\mathrm{supp}(v) \subseteq \mathrm{supp}(u)$. A codeword

$c \in \mathcal{C}$ is said to be minimal if c covers only the codewords $ac \in \mathcal{C}$ for all $a \in \mathbb{F}_q$, and c does not cover any other codeword of the code $\mathcal{C}$. The linear code $\mathcal{C}$ is said to be minimal if every codeword of $\mathcal{C}$ is minimal. It has been shown that minimal linear codes are useful in constructing secret sharing schemes with nice access structures [19, 23, 54, 60, 80] and in secure two-party computation [2, 22]. In addition, these codes can be effectively decoded with a minimum distance decoding algorithm [1].

Throughout this section, let $\mathscr{C}$ be a Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathscr{C}_1, \mathscr{C}_2, \cdots, \mathscr{C}_\rho$ such that $\mathscr{C}_w = \langle F_w \rangle$ is an $\mathcal{F}_w$-submodule of $\mathcal{L}_w$. Further, let us assume that $F_w = (F_{w,1}, F_{w,2}, \cdots, F_{w,\ell})$, where

$$F_{w,i} = \begin{cases} F_{0,w}^{(i)} + F_{1,w}^{(i)} u_i \cdots + F_{p^{a_i}-1,w}^{(i)} u_i^{p^{a_i}-1} & \text{if } \epsilon_{w,i} = 1; \\ 0 & \text{otherwise,} \end{cases}$$

with $F_{j_i,w}^{(i)} \in \mathbb{F}_{q^{d_w}}$ for $1 \le w \le \rho$, $1 \le i \le \ell$ and $0 \le j_i \le p^{a_i} - 1$. Further, for each w, let us define $E_w = \{1 \le i \le \ell : F_{w,i} \neq 0\}$.

In the following theorem, we identify a class of optimal equidistant linear codes over finite fields within the family of Λ-MT codes.

Theorem 7.3.1. *Let $F_1 = (b_{1,1}u_1^{p^{a_1}-1}, b_{1,2}u_2^{p^{a_2}-1}, \cdots, b_{1,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0$ and $F_2 = F_3 = \cdots = F_\rho = 0$, where $b_{1,i} \in \mathbb{F}_{q^{d_1}}$ for $1 \le i \le \ell$. If $\tau_1 = 1$, then the Λ-MT code $\mathscr{C}$ is an equidistant linear $\left[n, d_1, \sum_{i \in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$-code over $\mathbb{F}_q$. In particular, if $E_1 = \{1, 2, \cdots, \ell\}$, then the code $\mathscr{C}$ has parameters $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and is an optimal code that attains both the Griesmer and Plotkin bounds.*

Proof. Since $\mathscr{C}_1 = \langle F_1 \rangle$, we have $\mathscr{C}_1 = \{(\nu b_{1,1}u_1^{p^{a_1}-1}, \nu b_{1,2}u_2^{p^{a_2}-1}, \cdots, \nu b_{1,\ell}u_\ell^{p^{a_\ell}-1}) : \nu \in \mathbb{F}_{q^{d_1}}\}$, which implies that $|\mathscr{C}| = q^{d_1}$. Note that the code $\mathscr{C}$ satisfies the condition (7.1) with $i_1 = 1$ and i_2 to be any integer satisfying $1 < i_2 \le \rho$ for $1 \le i \le \ell$. Further, for $1 \le i \le \ell$ and $0 \le t_i \le p^{a_i} - 1$, it is easy to see that $\binom{p^{a_i}-1}{t_i} \neq 0$. From this, for each t_i, we see that $y_{t_i,1}^{(i)} = \binom{p^{a_i}-1}{t_i} \nu b_{1,i}(-\delta_1)^{p^{a_i}-1-t_i} \neq 0$ for $i \in E_1$ and $x_1 = (\nu b_{1,1}u_1^{p^{a_1}-1}, \nu b_{1,2}u_2^{p^{a_2}-1}, \cdots, \nu b_{1,\ell}u_\ell^{p^{a_\ell}-1}) (\neq 0) \in \mathscr{C}_1$. Now for each $i \in E_1$, by

equations (7.1), (7.4) and (7.5) and by Theorem 7.2.2(a), we see that the Hamming weight of the ith block $c_i(x_1, x_2, \cdots, x_\rho)$ of the codeword $c(x_1, x_2, \cdots, x_\rho) \in \mathscr{C}$ is given by

$$W_H(c_i(x_1, x_2, \cdots, x_\rho)) = \sum_{t_i=0}^{p^{a_i}-1} D_i^{(t_i)}(y_{t_i,i_1}^{(i)}, y_{t_i,i_2}^{(i)}) = \begin{cases} 0 & \text{if } x_1 = 0; \\ \frac{p^{a_i} n_i (q-1) q^{d_1-1}}{q^{d_1}-1} & \text{otherwise,} \end{cases}$$

where $x_w \in \mathscr{C}_w$ for $1 \leq w \leq \rho$. Further, by (7.3), we note that each non-zero codeword of $\mathscr{C}$ has Hamming weight $\sum_{i \in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$. Furthermore, for $i \in E_1$, since $\zeta_1^{\ell_1 m_i} = \delta_1^{-m_i} = \lambda_i^{-1}$, we see that $\zeta_1^{\ell_1 m_i (q-1)} = 1$, which implies that $\frac{q^{d_1}-1}{q-1} \mid m_i$. Now when $E_1 = \{1, 2, \cdots, \ell\}$, one can easily observe that the code $\mathscr{C}$ has parameters $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and attains both the Griesmer and Plotkin bounds. □

From this point on, in Tables 7.5-7.8, we assume that $A_0 = 1$ and $A_j = 0$ for all other non-zero Hamming weights j'. In the following theorem, we explicitly determine Hamming weight distributions of the codes belonging to a class of Λ-MT codes having at most two non-zero Hamming weights. We also identify two different classes of optimal equidistant linear codes and 2-weight minimal linear codes within these classes of MT codes.

Theorem 7.3.2. *Let* $F_1 = (b_{1,1}u_1^{p^{a_1}-1}, b_{1,2}u_2^{p^{a_2}-1}, \cdots, b_{1,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0$ *and* $F_2 = F_3 = \cdots = F_\rho = 0$, *where* $b_{1,i} \in \mathbb{F}_{q^{d_1}}$ *for* $1 \leq i \leq \ell$. *If* $S_1 = \{i \in E_1 : b_{1,i}$ *is a square in* $\mathbb{F}_{q^{d_1}}\}$, $S_2 = \{i \in E_1 : b_{1,i}$ *is a non-square in* $\mathbb{F}_{q^{d_1}}\}$ *and* $\tau_1 = 2$, *then* d_1 *is an even integer,* q *is an odd prime power, and the* Λ*-MT code* $\mathscr{C}$ *is a linear code of length* n *and dimension* d_1 *over* $\mathbb{F}_q$ *having at most two non-zero Hamming weights and its Hamming weight distribution is given by Table 7.1. Furthermore, the code* $\mathscr{C}$ *is a 2-weight code over* $\mathbb{F}_q$ *if* $\sum_{i \in S_1} m_i \neq \sum_{i \in S_2} m_i$, *while the code* $\mathscr{C}$ *is an equidistant code if* $\sum_{i \in S_1} m_i = \sum_{i \in S_2} m_i$.

In particular, let $E_1 = \{1, 2, \cdots, \ell\}$ *and* $m_1 = m_2 = \cdots = m_\ell$ *so that* $n = m_1\ell$. *Now if* ℓ *is even and* $|S_1| = |S_2| = \frac{\ell}{2}$, *then the code* $\mathscr{C}$ *is an optimal equidistant*

Hamming weight j	Frequency A_j
$\sum_{i\in S_1} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in S_2} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in S_1} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in S_2} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$

Table 7.1: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.2

linear $\left[n, d_1, \frac{n(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$*-code over* $\mathbb{F}_q$ *that attains both the Griesmer and Plotkin bounds. On the other hand, if either* $S_1 = \{1, 2, \cdots, \ell\}$ *or* $S_2 = \{1, 2, \cdots, \ell\}$*, then the code* $\mathscr{C}$ *is a 2-weight linear* $\left[n, d_1, \frac{n(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}\right]$*-code over* $\mathbb{F}_q$*, which is a minimal linear code when either* $2 \mid\mid \frac{rd_1(p-1)^2}{4}$ *or* $4 \mid \frac{rd_1(p-1)^2}{4}$ *and* $d_1 \geq 4$*, (note that* $2 \mid \frac{rd_1(p-1)^2}{4}$*).*

Proof. Since $\mathbb{F}_{q^{d_1}}^* = \langle \zeta_1 \rangle$, it is easy to see that $\zeta_1^{\frac{q^{d_1}-1}{p-1}}$ is a primitive element of $\mathbb{F}_p$. Also for $1 \leq i \leq \ell$ and $0 \leq t_i \leq p^{a_i} - 1$, we note that $\binom{p^{a_i}-1}{t_i} = \zeta_1^{\frac{(q^{d_1}-1)r_i}{p-1}}$ for some integer r_i satisfying $0 \leq r_i \leq p-2$, which implies that $2 \mid \frac{(q^{d_1}-1)r_i}{p-1}$, as $\tau_1 = 2 = \gcd\left(\frac{q^{d_1}-1}{q-1}, \ell_1\right)$. Further, for $i \in E_1, 0 \leq t_i \leq p^{a_i} - 1$ and $x_1 = (\zeta_1^h b_{1,1} u_1^{p^{a_1}-1}, \zeta_1^h b_{1,2} u_2^{p^{a_2}-1}, \cdots, \zeta_1^h b_{1,\ell} u_\ell^{p^{a_\ell}-1}) \in \mathscr{C}_1$ with $0 \leq h \leq q^{d_1} - 2$, one can observe that

$$y_{t_i,1}^{(i)} = \binom{p^{a_i}-1}{t_i} \zeta_1^h b_{1,i} (-\delta_1)^{p^{a_i}-1-t_i} = \binom{p^{a_i}-1}{t_i} \zeta_1^h b_{1,i} \zeta_1^{\frac{(q^{d_1}-1)(p^{a_i}-1-t_i)}{2}} \zeta_1^{-\ell_1(p^{a_i}-1-t_i)}$$

is a square in $\mathbb{F}_q^{d_1}$ when $\zeta_1^h b_{1,i}$ is a square in $\mathbb{F}_q^{d_1}$, as $2 \mid \ell_1$ and $2 \mid \frac{q^{d_1}-1}{2}$. Now by applying Theorem 7.2.2(b) and working in a similar manner as in Theorem 7.3.1, the desired result follows immediately. □

In the following theorem, we explicitly determine the Hamming weight distribution of the code $\mathscr{C}$ when $\tau_1 \geq 3$, $F_1 = (\epsilon_{1,1} u_1^{p^{a_1}-1}, \epsilon_{1,2} u_2^{p^{a_2}-1}, \cdots, \epsilon_{1,\ell} u_\ell^{p^{a_\ell}-1})$ and $F_2 = F_3 = \cdots = F_\kappa = 0$ in the semi-primitive case. We also derive sufficient conditions under which the code $\mathscr{C}$ is minimal.

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}-(-1)^{\nu_1-1}q^{\frac{d_1}{2}}(\tau_1-1)\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{\tau_1}$
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}+(-1)^{\nu_1-1}q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{(q^{d_1}-1)(\tau_1-1)}{\tau_1}$

Table 7.2: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.3

Theorem 7.3.3. *Let $\tau_1 \geq 3$, $F_1 = (\epsilon_{1,1}u_1^{p^{a_1}-1}, \epsilon_{1,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{1,\ell}u_\ell^{p^{a_\ell}-1})$ and $F_2 = F_3 = \cdots = F_\rho = 0$. Suppose that there exists a least positive integer z_1 satisfying $p^{z_1} \equiv -1 \ (mod\ \tau_1)$. Then we have $rd_1 = 2z_1\nu_1$ for some positive integer ν_1.*

(a) When ν_1 is even, the Λ-MT code $\mathscr{C}$ is a 2-weight linear $\left[n, d_1, \sum_{i\in E_1} \frac{m_i(q-1)(q^{d_1}-q^{\frac{d_1}{2}})}{q(q^{d_1}-1)}\right]$-code over $\mathbb{F}_q$, whose Hamming weight distribution is given by Table 7.2. Further, the code $\mathscr{C}$ is minimal when $q^{\frac{d_1}{2}} - q\tau_1 + \tau_1 - 1 > 0$.

(b) When ν_1 is odd, the Λ-MT code $\mathscr{C}$ is a 2-weight linear $\left[n, d_1, \sum_{i\in E_1} \frac{m_i(q-1)(q^{d_1}-(R_1-1)q^{\frac{d_1}{2}})}{q(q^{d_1}-1)}\right]$-code over $\mathbb{F}_q$, whose Hamming weight distribution is given by Table 7.2. The code $\mathscr{C}$ is minimal when $q^{\frac{d_1}{2}} - q\tau_1 + 1 > 0$.

Proof. By applying Theorem 7.2.2(c) and working in a similar manner as in Theorems 7.3.1 and 7.3.2, the desired result follows immediately. □

In the following two theorems, we identify several 2-weight and 3-weight codes within the family of MT codes, and explicitly determine their Hamming weight distributions.

Theorem 7.3.4. *Let $q = 2^r$, $a_1 = a_2 = \cdots = a_\ell = 1$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = F_3 = \cdots = F_\rho = 0$. If $\tau_1 = 1$, then the Λ-MT code $\mathscr{C}$ has parameters $\left[n, 2d_1, \sum_{i\in E_1} \frac{n_i(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and is a 2-weight code, whose Hamming weight distribution is given by Table 7.3.*

Proof. The desired result follows by equations (7.1), (7.3)-(7.5) and by applying Theorem 7.2.2(a). □

Hamming weight j	Frequency A_j	Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{n_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$2(q^{d_1}-1)$	$\sum_{i\in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$(q^{d_1}-1)^2$

Table 7.3: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.4

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{n_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$3(q^{d_1}-1)$
$\sum_{i\in E_1} \frac{2n_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$2(q^{d_1}-1)+2(q^{d_1}-1)(q^{d_1}-2)+(q^{d_1}-1)^2$
$\sum_{i\in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1+2(q^{d_1}-1)(q^{d_1}-2)+(q^{d_1}-1)(q^{d_1}-2)^2$

Table 7.4: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.5

Theorem 7.3.5. *Let $q = 3^r$, $a_1 = a_2 = \cdots = a_\ell = 1$, $F_1 = (\epsilon_{1,1}, \epsilon_{1,2}, \cdots, \epsilon_{1,\ell})$ and $F_2 = F_3 = \cdots = F_\rho = 0$. If $\tau_1 = 1$, then the Λ-MT code $\mathscr{C}$ has parameters $\left[n, 3d_1, \sum_{i\in E_1} \frac{n_i(q-1)q^{d_1-1}}{q^{d_1}-1}\right]$ and is a 3-weight code, whose Hamming weight distribution is given by Table 7.4.*

Proof. The desired result follows by equations (7.1), (7.3)-(7.5) and by applying Theorem 7.2.2(a). □

In the following theorem, we explicitly determine Hamming weight distributions of the codes belonging to a class of Λ-MT codes having at most three non-zero Hamming weights. We also identify a class of 3-weight minimal linear codes within this class of MT codes.

Theorem 7.3.6. *Suppose that $F_1 = (b_{1,1}u_1^{p^{a_1}-1}, b_{1,2}u_2^{p^{a_2}-1}, \cdots, b_{1,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0, F_2 = (b_{2,1}u_1^{p^{a_1}-1}, b_{2,2}u_2^{p^{a_2}-1}, \cdots, b_{2,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0$ and $F_3 = F_4 = \cdots = F_\rho = 0$, where $b_{1,i} \in \mathbb{F}_{q^{d_1}}$ and $b_{2,i} \in \mathbb{F}_{q^{d_2}}$ for $1 \leq i \leq \ell$. Then we have $i_1 = 1$ and $i_2 = 2$ for $1 \leq i \leq \ell$. Furthermore, if $E_1 \cap E_2$ is a non-empty set and $M_i = M_i' = 1$ for some i satisfying $1 \leq i \leq \ell$, then the Λ-MT code $\mathscr{C}$ is a linear code of length n and dimension $d_1 + d_2$ over $\mathbb{F}_q$ having at most three non-zero Hamming weights and its Hamming weight distribution is given by Table 7.5. In particular, if $E_1 = E_2 = \{1, 2, \cdots, \ell\}$,*

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in E_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1} + \sum_{i\in E_1\cap E_2} \frac{m_i(q-1)((q^{d_1}-1)(q^{d_2}-1)-1)}{q(q^{d_1}-1)(q^{d_2}-1)}$	$(q^{d_1}-1)(q^{d_2}-1)$

Table 7.5: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.6

then the Λ-MT code $\mathscr{C}$ is a 3-weight linear $\left[n, d_1+d_2, \frac{n(q-1)\left((q^{d_1}-1)(q^{d_2}-1)-1\right)}{q(q^{d_1}-1)(q^{d_2}-1)}\right]$-code over $\mathbb{F}_q$, which is minimal when both $d_1, d_2 \geq 2$ and $\gcd(d_1, d_2) = 1$.

Proof. Since $i_1 = 1$ and $i_2 = 2$ for $1 \leq i \leq \ell$, we note that $M_1 = M_2 = \cdots = M_\ell$ and $M'_1 = M'_2 = \cdots = M'_\ell$. Further, one can easily observe that $\tau_1 = g_1 = \tau_2 = g_2 = 1$, as $M_1 = M_2 = \cdots = M_\ell = M'_1 = M'_2 = \cdots = M'_\ell = 1$. Now the desired result follows by equations (7.1), (7.3)-(7.5) and by applying Theorems 7.2.2(a) and 7.2.4(a). □

In the following theorem, we explicitly determine the Hamming weight distribution of the code $\mathscr{C}$ when $F_1 = (\epsilon_{1,1}u_1^{p^{a_1}-1}, \epsilon_{1,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{1,\ell}u_\ell^{p^{a_\ell}-1})$, $F_2 = (\epsilon_{2,1}u_1^{p^{a_1}-1}, \epsilon_{2,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{2,\ell}u_\ell^{p^{a_\ell}-1})$, $F_3 = F_4 = \cdots = F_\rho = 0$, and $M_i = 2$ and $M'_i = 1$ for some integer i satisfying $1 \leq i \leq \ell$. We also derive sufficient conditions under which the code $\mathscr{C}$ is minimal.

Theorem 7.3.7. *Suppose that $F_1 = (\epsilon_{1,1}u_1^{p^{a_1}-1}, \epsilon_{1,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{1,\ell}u_\ell^{p^{a_\ell}-1})$, $F_2 = (\epsilon_{2,1}u_1^{p^{a_1}-1}, \epsilon_{2,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{2,\ell}u_\ell^{p^{a_\ell}-1})$ and $F_3 = F_4 = \cdots = F_\rho = 0$. Then we have $i_1 = 1$ and $i_2 = 2$ for $1 \leq i \leq \ell$. Furthermore, if $M_i = 2$ and $M'_i = 1$ for some i satisfying $1 \leq i \leq \ell$, then d_1 is an even integer, q is an odd prime power, and the Λ-MT code $\mathscr{C}$ is a linear code of length n and dimension $d_1 + d_2$ over $\mathbb{F}_q$ having at most five non-zero Hamming weights and its Hamming weight distribution is given by Table 7.6. In particular, if $E_1 = E_2 = \{1, 2, \cdots, \ell\}$, $d_1 \neq 2d_2$ and $\gcd(d_1, d_2) = 1$, then the code $\mathscr{C}$ is a 5-weight linear $\left[n, d_1+d_2, \frac{n(q-1)(q^{d_1}-q^{\frac{d_1}{2}})}{q(q^{d_1}-1)}\right]$-code over $\mathbb{F}_q$, which*

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in E_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1} + \sum_{i\in E_1\cap E_2}\left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}}{q(q^{d_1}-1)(q^{d_2}+2)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1} + \sum_{i\in E_1\cap E_2}\left(\frac{m_i(q-1)}{q} - \frac{m_i(q-1)(1-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}}{q(q^{d_1}-1)(q^{d_2}+2)}\right)$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$

Table 7.6: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.7

is minimal when either $d_1 > 2d_2$ *and* $q^{d_2-1}(q^{\frac{d_1}{2}}+1) > q^{\frac{d_1}{2}} + q^{d_2}$ *or* $d_1 < 2d_2$ *and* $d_1 \geq 4$.

Proof. Here it is easy to see that $M_1 = M_2 = \cdots = M_\ell$ and $M'_1 = M'_2 = \cdots = M'_\ell$. Since $M_1 = 2$ and $M'_1 = 1$, we note that $\tau_1 = g_1 = 2$ and $\tau_2 = g_2 = 1$. The desired result follows by equations (7.1), (7.3)-(7.5) and by applying Theorems 7.2.2(a), 7.2.2(b) and 7.2.4(b). □

In the following two theorems, we identify two more classes with few weights within the family of MT codes, and explicitly determine their Hamming weight distributions.

Theorem 7.3.8. *Suppose that* $F_1 = (b_{1,1}u_1^{p^{a_1}-1}, b_{1,2}u_2^{p^{a_2}-1}, \cdots, b_{1,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0, F_2 = (b_{2,1}u_1^{p^{a_1}-1}, b_{2,2}u_2^{p^{a_2}-1}, \cdots, b_{2,\ell}u_\ell^{p^{a_\ell}-1}) \neq 0$ *and* $F_3 = F_4 = \cdots = F_\rho = 0$, *where* $b_{1,i} \in \mathbb{F}_{q^{d_1}}$ *and* $b_{2,i} \in \mathbb{F}_{q^{d_2}}$ *for* $1 \leq i \leq \ell$. *Then we have* $i_1 = 1$ *and* $i_2 = 2$ *for* $1 \leq i \leq \ell$. *Furthermore, if* $E_1 \cap E_2$ *is the empty set and* $\tau_1 = \tau_2 = 1$, *then the* Λ*-MT code* $\mathscr{C}$ *is a linear code of length* n *and dimension* $d_1 + d_2$ *over* $\mathbb{F}_q$ *having at most*

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1}$	$q^{d_1}-1$
$\sum_{i\in E_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)q^{d_1-1}}{q^{d_1}-1} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$(q^{d_1}-1)(q^{d_2}-1)$

Table 7.7: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.8

three non-zero Hamming weights and its Hamming weight distribution is given by Table 7.7.

Proof. The desired result follows immediately by equations (7.1), (7.3)-(7.5) and by Theorem 7.2.2(a). □

Theorem 7.3.9. *Suppose that* $F_1 = (\epsilon_{1,1}u_1^{p^{a_1}-1}, \epsilon_{1,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{1,\ell}u_\ell^{p^{a_\ell}-1}), F_2 = (\epsilon_{2,1}u_1^{p^{a_1}-1}, \epsilon_{2,2}u_2^{p^{a_2}-1}, \cdots, \epsilon_{2,\ell}u_\ell^{p^{a_\ell}-1})$ *and* $F_3 = F_4 = \cdots = F_\rho = 0$. *Then we have* $i_1 = 1$ *and* $i_2 = 2$ *for* $1 \le i \le \ell$. *Furthermore, if* $E_1 \cap E_2$ *is the empty set and* $\tau_1 = 2$ *and* $\tau_2 = 1$, *then the* Λ*-MT code* $\mathscr{C}$ *is a linear code of length* n *and dimension* $d_1 + d_2$ *over* $\mathbb{F}_q$ *having at most five non-zero Hamming weights and its Hamming weight distribution is given by Table 7.8.*

Proof. It follows immediately by equations (7.1), (7.3)-(7.5) and by applying Theorems 7.2.2(a) and 7.2.2(b). □

Hamming weight j	Frequency A_j
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in E_1} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)}$	$\frac{q^{d_1}-1}{2}$
$\sum_{i\in E_2} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$q^{d_2}-1$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)\left(q^{d_1}+\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$
$\sum_{i\in E_1\setminus E_2} \frac{m_i(q-1)\left(q^{d_1}-\iota^{\frac{rd_1(p-1)^2}{4}} q^{\frac{d_1}{2}}\right)}{q(q^{d_1}-1)} + \sum_{i\in E_2\setminus E_1} \frac{m_i(q-1)q^{d_2-1}}{q^{d_2}-1}$	$\frac{(q^{d_1}-1)(q^{d_2}-1)}{2}$

Table 7.8: Hamming weight distribution of the code $\mathscr{C}$ considered in Theorem 7.3.9

8

Skew multi-twisted codes over finite fields and their Galois duals

8.1 Introduction

In this chapter, we shall introduce a new class of linear codes over finite fields, *viz.* skew multi-twisted (skew MT) codes (or skew generalized quasi-twisted codes), which is a generalization of some well-known classes of linear codes such as cyclic codes, generalized quasi-cyclic codes and MT codes. We shall also study algebraic structures of skew multi-twisted codes and their Galois duals (i.e., orthogonal complements with respect to the Galois inner product). We shall view skew multi-twisted

codes as direct sums of certain concatenated codes, which gives rise to a method to construct these codes. We shall obtain a lower bound on their minimum Hamming distances using their multilevel concatenated structure. Besides this, we shall determine the parity-check polynomial of each skew multi-twisted code, and obtain BCH type bounds on their minimum Hamming distances. We shall determine generating sets of Galois duals of some skew multi-twisted codes from generating sets of these codes. We shall also derive necessary and sufficient conditions under which a skew multi-twisted code is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD (linear with complementary dual). We shall also obtain many linear codes with best known and optimal parameters from 1-generator skew multi-twisted codes over finite fields $\mathbb{F}_8$ and $\mathbb{F}_9$.

This chapter is organized as follows: In Section 8.2, we state some basic definitions and results that are needed to derive our main results. In Section 8.3, we introduce a new class of linear codes over finite fields, *viz.* skew multi-twisted (MT) codes and study their algebraic structures (Theorem 8.3.3). In Section 8.4, we show that each skew MT code is a direct sum of certain concatenated codes (Theorem 8.4.2). We also determine a lower bound on their minimum Hamming distances using their multilevel concatenated structure (Theorems 8.4.3 and 8.4.4). In Section 8.5, we study their dual codes with respect to the Galois inner product (Theorem 8.5.5). We also derive necessary and sufficient conditions under which a skew MT code is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD (Theorem 8.5.7). In Section 8.6, we obtain the parity-check polynomial of each skew MT code, determine generating sets of Galois duals of some skew MT codes from generating sets of the corresponding skew MT codes, and derive BCH type lower bounds on their minimum Hamming distances (Theorem 8.6.2). We list several linear codes with best known and optimal parameters obtained from 1-generator skew MT codes (Tables 8.1 and 8.2).

8.2 Preliminaries

In this section, we shall state some basic results on skew polynomial rings that we need to derive our main results. For this, throughout this chapter, let $\mathbb{F}_q$ be the finite field of order $q = p^r$, where p is a prime and r is a positive integer. Let σ be an automorphism of $\mathbb{F}_q$ having the order as α, and let $\mathbb{F}_q^\sigma$ be the fixed field of σ. Let

$$\mathcal{R} = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_0, a_1, \cdots, a_n \in \mathbb{F}_q \text{ and } n \geq 0\}$$

be the set of all formal polynomials in the indeterminate x over $\mathbb{F}_q$, where the coefficients are written on the left of the indeterminate x and its higher powers. One can easily observe that the set $\mathcal{R}$ forms a ring with unity under the usual addition of polynomials and under the multiplication defined using the distributive law and the rule

$$(ax^i)(bx^j) = a\sigma^i(b)x^{i+j} \text{ for each } a, b \in \mathbb{F}_q \text{ and integers } i, j \geq 0.$$

The ring $\mathcal{R}$ is called a skew polynomial ring over $\mathbb{F}_q$ and elements of $\mathcal{R}$ are called skew polynomials. Note that the ring $\mathcal{R}$ is non-commutative unless σ is the identity automorphism. Now the following result is well-known.

Theorem 8.2.1. *[18, 31] In the skew polynomial ring $\mathcal{R}$, the following hold.*

(a) The ring $\mathcal{R}$ has no non-zero zero divisors.

(b) The units of $\mathcal{R}$ are the units of $\mathbb{F}_q$.

(c) The center of $\mathcal{R}$ is given by $Z(\mathcal{R}) = \mathbb{F}_q^\sigma[x^\alpha] = \{a_0 + a_1x^\alpha + \cdots + a_dx^{d\alpha} : a_0, a_1, \cdots, a_d \in \mathbb{F}_q^\sigma$ and $d \geq 0\}$.

(d) If $f(x), g(x) \in \mathcal{R}$ are such that $f(x)g(x) \in Z(\mathcal{R})$, then we have $f(x)g(x) = g(x)f(x)$.

In the following theorem, we state the right division algorithm in $\mathcal{R}$, and the corresponding result holds regarding the left division in $\mathcal{R}$.

Theorem 8.2.2. *[61, Th. II.11] (Right Division Algorithm) For $f(x), g(x) \in \mathcal{R}$ with $f(x) \neq 0$, there exist unique skew polynomials $q(x), r(x) \in \mathcal{R}$ such that $g(x) = q(x)f(x) + r(x)$, where either $r(x) = 0$ or deg $r(x) <$ deg $f(x)$. When $r(x) = 0$, we say that $f(x)$ is a right divisor of $g(x)$ or $g(x)$ is a left multiple of $f(x)$.*

Further, by applying the right (left) division algorithm, one can show that the ring $\mathcal{R}$ is a left (right) principal ideal ring, i.e., each left (right) ideal of $\mathcal{R}$ is principal. That is, for each left ideal I of $\mathcal{R}$, there exists an element $a(x) \in I$ such that $I = \{f(x)a(x) : f(x) \in \mathcal{R}\}$, and we shall write $I = \langle a(x) \rangle_L$. Similarly, for each right ideal J of $\mathcal{R}$, there exists an element $b(x) \in J$ such that $J = \{b(x)f(x) : f(x) \in \mathcal{R}\}$, and we shall write $J = \langle b(x) \rangle_R$.

Let $f(x), g(x) \in \mathcal{R}$ be such that either $f(x)$ or $g(x)$ is non-zero. Then a monic skew polynomial $d(x) \in \mathcal{R}$ is called the greatest common right divisor (gcrd) of $f(x)$ and $g(x)$, written as $d(x) = \text{gcrd}(f(x), g(x))$, if it satisfies the following two conditions:

(i) $d(x)$ is a right divisor of both $f(x)$ and $g(x)$.

(ii) If $e(x)$ is another right divisor of both $f(x)$ and $g(x)$, then $e(x)$ is a right divisor of $d(x)$.

We say that the skew polynomials $f(x), g(x) \in \mathcal{R}$ are right coprime if they satisfy $\text{gcrd}(f(x), g(x)) = 1$.

Theorem 8.2.3. *[3, Th. 7] Let $f(x), g(x) \in \mathcal{R}$ be such that either $f(x)$ or $g(x)$ is non-zero. If gcrd$(f(x), g(x)) = d(x)$, then there exist skew polynomials $a(x), b(x) \in \mathcal{R}$ such that $d(x) = a(x)f(x) + b(x)g(x)$.*

Further, let $f(x), g(x)$ be non-zero skew polynomials in $\mathcal{R}$. Then a monic skew polynomial $\ell(x) \in \mathcal{R}$ is called the least common right multiple (lcrm) of $f(x)$ and $g(x)$, written as $\ell(x) = \text{lcrm}\,[f(x), g(x)]$, if it satisfies the following two conditions:

(i) $\ell(x)$ is a right multiple of both $f(x)$ and $g(x)$.

(ii) If $k(x)$ is another right multiple of both $f(x)$ and $g(x)$, then $k(x)$ is a right multiple of $\ell(x)$.

The greatest common left divisor (gcld) and the least common left multiple (lclm) are defined in an analogous manner. Further, if $f(x), g(x) \in \mathcal{R}$ are such that either $f(x)$ or $g(x)$ is non-zero and $\text{gcld}(f(x), g(x)) = h(x)$, then there exist skew polynomials $A(x), B(x) \in \mathcal{R}$ such that $h(x) = f(x)A(x) + g(x)B(x)$.

An element $f(x) \in \mathcal{R}$ is called a 2-sided element of $\mathcal{R}$ if it satisfies $\langle f(x)\rangle_L = \langle f(x)\rangle_R = \langle f(x)\rangle$. It is easy to see that a 2-sided ideal of $\mathcal{R}$ is generated by a 2-sided element of $\mathcal{R}$. Further, a 2-sided element $f(x) \in \mathcal{R}$ is called a maximal element of $\mathcal{R}$ if the 2-sided ideal $\langle f(x)\rangle$ is a maximal ideal of $\mathcal{R}$.

Theorem 8.2.4. *[46, Th. 1.1.22] Each 2-sided element of $\mathcal{R}$ is of the form $c\big(1 + a_1x^{\alpha} + \cdots + a_dx^{d\alpha}\big)x^e$, where $c \in \mathbb{F}_q$, $a_1, \cdots, a_d \in \mathbb{F}_q^{\sigma}$ and $d, e \geq 0$ are integers.*

The following theorem states that each non-zero non-unit 2-sided element of $\mathcal{R}$ can be expressed as a product of 2-sided maximal elements of $\mathcal{R}$.

Theorem 8.2.5. *[46, Th. 1.2.17] Let $f(x)$ be a non-zero, non-unit and a 2-sided element of $\mathcal{R}$. Then $f(x)$ can be expressed as $f(x) = g_1(x)g_2(x)\cdots g_t(x)$, where $g_1(x), g_2(x), \cdots, g_t(x)$ are 2-sided maximal elements of $\mathcal{R}$. Such a factorization is unique up to the order and up to unit multipliers.*

Further, for each 2-sided element $f(x) \in \mathcal{R}$, the set $\frac{\mathcal{R}}{\langle f(x)\rangle} = \{r(x) + \langle f(x)\rangle : r(x) \in \mathcal{R}\}$ can be viewed as a ring. From now on, we shall represent elements of the quotient ring $\frac{\mathcal{R}}{\langle f(x)\rangle}$ by skew polynomials in $\mathcal{R}$ of degree less than $\deg f(x)$.

8.3 Algebraic structures of skew multi-twisted codes over finite fields

In this section, we will introduce a new class of linear codes over finite fields, viz. skew multi-twisted codes, which is a generalization of MT codes. To do this, throughout this chapter, let $n = m_1 + m_2 + \cdots + m_\ell$, where $m_1, m_2, \cdots, m_\ell$ are positive integers such that $\gcd(m_i, q) = 1$ and α divides m_i for $1 \leq i \leq \ell$. Let $\mathbb{F}_q^n$ denote the vector space consisting of all n-tuples over $\mathbb{F}_q$. Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ and $\Lambda^{-p^k} = (\lambda_1^{-p^k}, \lambda_2^{-p^k}, \cdots, \lambda_\ell^{-p^k})$ for each integer k satisfying $0 \leq k < r$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q^\sigma$. Under these conditions, by Theorem 8.2.1(c), we see that the skew polynomial $x^{m_i} - \lambda_i \in Z(\mathcal{R})$, which implies that $\langle x^{m_i} - \lambda_i \rangle$ is a 2-sided ideal of $\mathcal{R}$ for $1 \leq i \leq \ell$. This further implies that $V_i = \frac{\mathcal{R}}{\langle x^{m_i} - \lambda_i \rangle}$ is a quotient ring for each i. Then a skew Λ-multi-twisted (MT) module V is a left $\mathcal{R}$-module of the form $V = \prod_{i=1}^{\ell} V_i$. We further observe that there exists an $\mathbb{F}_q$-linear vector space isomorphism from $\mathbb{F}_q^n$ onto V. From now on, we shall represent each element $b \in \mathbb{F}_q^n$ as $b = (b_{1,0}, b_{1,1}, \cdots, b_{1,m_1-1}; b_{2,0}, b_{2,1}, \cdots, b_{2,m_2-1}; \cdots; b_{\ell,0}, b_{\ell,1}, \cdots, b_{\ell,m_\ell-1})$ and the corresponding element $b(x) \in V$ as $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x))$, where $b_i(x) = \sum_{j=0}^{m_i-1} b_{i,j} x^j \in V_i$ for $1 \leq i \leq \ell$. Further, the skew Λ-MT shift operator $T_{\Lambda,\sigma}$ on $\mathbb{F}_q^n$ is defined as $T_{\Lambda,\sigma}(b) = (\sigma(\lambda_1 b_{1,m_1-1}), \sigma(b_{1,0}), \cdots, \sigma(b_{1,m_1-2}); \sigma(\lambda_2 b_{2,m_2-1}), \sigma(b_{2,0}), \cdots, \sigma(b_{2,m_2-2}); \cdots; \sigma(\lambda_\ell b_{\ell,m_\ell-1}), \sigma(b_{\ell,0}), \cdots, \sigma(b_{\ell,m_\ell-2}))$ for each $b \in \mathbb{F}_q^n$. Next let

$$m = \operatorname{lcm}\left[m_1 O(\lambda_1), m_2 O(\lambda_2), \cdots, m_\ell O(\lambda_\ell)\right],$$

where $O(\lambda_i)$ denotes the multiplicative order of λ_i in $\mathbb{F}_q$ for $1 \leq i \leq \ell$. One can show that $T_{\Lambda,\sigma}^m = I$, where I is the identity operator on $\mathbb{F}_q^n$.

Definition 8.3.1. *A skew Λ-multi-twisted (MT) code (or a skew generalized Λ-quasi-twisted code) of length n over $\mathbb{F}_q$ is defined as a left $\mathcal{R}$-submodule of the skew Λ-MT module V. Equivalently, a linear code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called a skew*

Λ-MT (or a skew Λ-GQT) code if $T_{\Lambda,\sigma}(c) \in \mathcal{C}$ for each codeword $c \in \mathcal{C}$, (i.e., if the skew Λ-multi-twisted shift of each codeword of $\mathcal{C}$ is also a codeword of $\mathcal{C}$).

In particular, skew Λ-MT (or skew Λ-GQT) codes of length $n = m_1+m_2+\cdots+m_\ell$ over $\mathbb{F}_q$ are

- Λ-MT (or Λ-GQT) codes of length n over $\mathbb{F}_q$ when $\sigma = I$ (the identity automorphism on $\mathbb{F}_q$) [5, 69].
- permutation-equivalent to QT codes of length $m_1\ell$ over $\mathbb{F}_q$ when $\lambda_1 = \lambda_2 = \cdots = \lambda_\ell$, $\sigma = I$ and $m_1 = m_2 = \cdots = m_\ell$ [47].
- skew GQC codes of length n over $\mathbb{F}_q$ when $\lambda_i = 1$ for $1 \leq i \leq \ell$ [48].
- permutation-equivalent to QC codes of length $m_1\ell$ over $\mathbb{F}_q$ when $\sigma = I$, $m_1 = m_2 = \cdots = m_\ell$ and $\lambda_1 = \lambda_2 = \cdots = \lambda_\ell = 1$ [77].
- skew λ_1-constacyclic codes of length m_1 over $\mathbb{F}_q$ when $\ell = 1$ [31].
- λ_1-constacyclic codes of length m_1 over $\mathbb{F}_q$ when $\ell = 1$ and $\sigma = I$ [10].

Now to study algebraic structures of skew Λ-MT codes, we first prove the following:

Proposition 8.3.2. *Let t be a positive integer such that α divides t and $\gcd(t, q) = 1$, and let λ be a non-zero element of $\mathbb{F}_q^\sigma$. Then the following hold.*

(a) The skew polynomial $x^t - \lambda \in Z(\mathcal{R})$ can be uniquely expressed (up to order) as

$$x^t - \lambda = f_1(x)f_2(x)\cdots f_s(x), \tag{8.1}$$

where $f_1(x), f_2(x), \cdots, f_s(x)$ are monic, pairwise coprime and irreducible polynomials in $Z(\mathcal{R})$. Furthermore, equation (8.1) also gives the factorization of $x^t - \lambda$ into 2-sided maximal elements of $\mathcal{R}$.

(b) There exist $\epsilon_1(x), \epsilon_2(x), \cdots, \epsilon_s(x) \in Z(\mathcal{R})$ *satisfying* $\epsilon_j(x)\epsilon_u(x) = \delta_{j,u}\epsilon_j(x)$ *for* $1 \leq j, u \leq s$ *and* $\epsilon_1(x) + \epsilon_2(x) + \cdots + \epsilon_s(x) = 1$ *in* $\frac{\mathcal{R}}{\langle x^t - \lambda \rangle}$, *where* $\delta_{j,u}$ *is the Kronecker* δ*-function. Furthermore, for* $1 \leq j \leq s$, $\langle \epsilon_j(x) \rangle$ *is a 2-sided ideal of* $\frac{\mathcal{R}}{\langle x^t - \lambda \rangle}$ *with the unity as* $\epsilon_j(x)$. *As a consequence, we have* $\frac{\mathcal{R}}{\langle x^t - \lambda \rangle} \simeq \bigoplus_{j=1}^{s} \langle \epsilon_j(x) \rangle$.

(c) For $1 \leq j \leq s$, *the map* $\psi_j : \frac{\mathcal{R}}{\langle f_j(x) \rangle} \to \langle \epsilon_j(x) \rangle$, *defined as* $\psi_j(g_j(x)) = g_j(x)\epsilon_j(x)$ *for each* $g_j(x) \in \frac{\mathcal{R}}{\langle f_j(x) \rangle}$, *is a ring isomorphism.*

(d) $\frac{\mathcal{R}}{\langle x^t - \lambda \rangle} \simeq \bigoplus_{j=1}^{s} \frac{\mathcal{R}}{\langle f_j(x) \rangle}$.

Proof. Here by Theorem 8.2.1(c), we see that $x^t - \lambda \in Z(\mathcal{R}) = \mathbb{F}_q^{\sigma}[x^{\alpha}]$, which is a unique factorization domain. Now using the fact that $\gcd(t, q) = 1$, we can write

$$x^t - \lambda = f_1(x) f_2(x) \cdots f_s(x), \tag{8.2}$$

where $f_1(x), f_2(x), \cdots, f_s(x)$ are monic, pairwise coprime and irreducible polynomials in $Z(\mathcal{R})$. Next we assert that $f_1(x), f_2(x), \cdots, f_s(x)$ are also 2-sided maximal elements of $\mathcal{R}$.

To prove this assertion, we see that $x^t - \lambda \in Z(\mathcal{R})$ is a 2-sided element of $\mathcal{R}$. So by Theorem 8.2.5, we can write

$$x^t - \lambda = h_1(x) h_2(x) \cdots h_v(x), \tag{8.3}$$

where $h_1(x), h_2(x), \cdots, h_v(x)$ are 2-sided maximal elements of $\mathcal{R}$. Further, for $1 \leq i \leq v$, by Theorem 8.2.4, we note that $h_i(x) = c_i \hat{h}_i(x) x^{e_i}$, where $c_i \in \mathbb{F}_q$, $e_i \geq 0$, and $\hat{h}_i(x) = h_{i,0} + h_{i,1}x^{\alpha} + h_{i,2}x^{2\alpha} + \cdots + h_{i,\eta_i - 1}x^{(\eta_i - 1)\alpha} + x^{\eta_i \alpha}$ with $h_{i,0}, h_{i,1}, \cdots, h_{i,\eta_i - 1} \in \mathbb{F}_q^{\sigma}$ and $\eta_i \geq 1$. On comparing coefficients in (8.3), we get $e_i = 0$ for each i, and $c_1 c_2 \cdots c_v = 1$. This gives

$$x^t - \lambda = \prod_{i=1}^{v} \hat{h}_i(x). \tag{8.4}$$

Note that $\hat{h}_i(x)$ belongs to $Z(\mathcal{R})$ for each i. Furthermore, since $h_i(x)$ is a maximal

element of $\mathcal{R}$, we see that $\hat{h}_i(x)$ is an irreducible polynomial in $Z(\mathcal{R})$. Hence equation (8.4) also gives the factorization of $x^t-\lambda$ into monic, pairwise coprime and irreducible polynomials in $Z(\mathcal{R})$. By (8.2) and (8.4) and by uniqueness of such a factorization, we have $s = v$ and $f_i(x) = \hat{h}_i(x)$ for $1 \leq i \leq s$ (on relabelling $\hat{h}_i(x)$'s if required). For each i, as $h_i(x) = c_i\hat{h}_i(x)$ is a maximal element of $\mathcal{R}$ and $\hat{h}_i(x) \in Z(\mathcal{R})$, we see that $f_i(x) = \hat{h}_i(x)$ is a 2-sided maximal element of $\mathcal{R}$, which proves the assertion.

Next we define $\hat{f}_j(x) = \prod_{\substack{u=1 \\ u\neq j}}^{s} f_u(x)$ for $1 \leq j \leq s$. We observe that the skew polynomials $f_j(x)$ and $\hat{f}_j(x)$ are coprime in $Z(\mathcal{R}) = \mathbb{F}_q^{\sigma}[x^{\alpha}]$ for $1 \leq j \leq s$. So for each j, by Euclidean algorithm in $Z(\mathcal{R}) = \mathbb{F}_q^{\sigma}[x]$, there exist skew polynomials $A_j(x), B_j(x) \in Z(\mathcal{R})$ satisfying $A_j(x)f_j(x)+B_j(x)\hat{f}_j(x) = 1$. Now on taking $\epsilon_j(x) = B_j(x)\hat{f}_j(x)$ for $1 \leq j \leq s$ and working in a similar manner as in Theorem 2.11 of Gao et al. [48], the desired result follows. □

Now we recall that $\gcd(m_i, q) = 1$, α divides m_i and $\sigma(\lambda_i) = \lambda_i$ for $1 \leq i \leq \ell$. By Proposition 8.3.2(a), we see that each skew polynomial $x^{m_i} - \lambda_i \in Z(\mathcal{R})$ can be uniquely expressed (up to order) as a product of monic, pairwise coprime and irreducible polynomials in $Z(\mathcal{R})$. Let $g_1(x), g_2(x), \cdots, g_\rho(x) \in Z(\mathcal{R})$ be all such distinct irreducible factors of the skew polynomials $x^{m_1} - \lambda_1$, $x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $Z(\mathcal{R})$. Further, for $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$, let us define

$$\epsilon_{w,i} = \begin{cases} 1 & \text{if } g_w(x) \text{ divides } x^{m_i} - \lambda_i \text{ in } Z(\mathcal{R}); \\ 0 & \text{otherwise.} \end{cases}$$

Then for $1 \leq i \leq \ell$, we observe that

$$x^{m_i} - \lambda_i = g_1(x)^{\epsilon_{1,i}} g_2(x)^{\epsilon_{2,i}} \cdots g_\rho(x)^{\epsilon_{\rho,i}}. \tag{8.5}$$

Now for each i, by applying Proposition 8.3.2, we see that

$$V_i \simeq \bigoplus_{w=1}^{\rho} \frac{\mathcal{R}}{\langle g_w(x)^{\epsilon_{w,i}} \rangle} \simeq \bigoplus_{w=1}^{\rho} \epsilon_{w,i} F_w$$

with $F_w = \frac{\mathcal{R}}{\langle g_w(x) \rangle}$ for $1 \leq w \leq \rho$, and the corresponding ring isomorphism is given by

$$a_i(x) \mapsto \sum_{w=1}^{\rho} a_{w,i} \text{ for each } a_i(x) \in V_i,$$

where $a_{w,i} := \epsilon_{w,i}\big(a_i(x) + \langle g_w(x) \rangle\big)$ for $1 \leq w \leq \rho$. From this, it follows that

$$V = \prod_{i=1}^{\ell} V_i \simeq \bigoplus_{w=1}^{\rho} \Big(\underbrace{\epsilon_{w,1} F_w, \epsilon_{w,2} F_w, \cdots, \epsilon_{w,\ell} F_w}_{\mathcal{G}_w} \Big), \tag{8.6}$$

and the corresponding ring isomorphism is given by

$$a(x) \mapsto \sum_{w=1}^{\rho} \Big(a_{w,1}, a_{w,2}, \cdots, a_{w,\ell} \Big)$$

for each $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V$, where $a_{w,i} = \epsilon_{w,i}(a_i(x) + \langle g_w(x) \rangle)$ for $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$. Further, since V is a left $\mathcal{R}$-module, we shall view $\mathcal{G}_w = (\epsilon_{w,1} F_w, \epsilon_{w,2} F_w, \cdots, \epsilon_{w,\ell} F_w)$ as a left F_w-module for each w. In view of the above, we have the following:

Theorem 8.3.3. *Each skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as*

$$\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w,$$

where $\mathcal{C}_w = \{(a_{w,1}, a_{w,2}, \cdots, a_{w,\ell}) \in \mathcal{G}_w : (a_1(x), a_2(x), \cdots, a_\ell(x)) \in \mathcal{C}\}$ is a left F_w-submodule of $\mathcal{G}_w$ for each w. (The left modules $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ are called constituents of the skew Λ-MT code $\mathcal{C}$.)

Gao et al. [48, p.60] remarked that each constituent of a 1-generator skew GQC

code is either $\{0\}$ or 1-dimensional, and hence a free module. However, this is not true in general, which we illustrate in the following example.

Example 8.3.1. *Let $q = 3^2, m_1 = 4, m_2 = 2$, $\Lambda = (1,1)$, and let $\sigma = \sigma_1$ be the Frobenius automorphism of $\mathbb{F}_{3^2}$, (i.e., $\sigma(b) = b^3$ for all $b \in \mathbb{F}_{3^2}$). Here we have $V = V_1 \times V_2 = \frac{\mathcal{R}}{\langle x^4-1\rangle} \times \frac{\mathcal{R}}{\langle x^2-1\rangle}$. We first note that $\mathbb{F}_{3^2}^{\sigma} = \mathbb{F}_3$ and $O(\sigma) = 2$, which, by Theorem 8.2.1(c), gives $Z(\mathcal{R}) = \mathbb{F}_3[x^2]$. Further, we observe that $x^4 - 1 = (x^2-1)(x^2+1) = (x^2+1)(x^2-1)$ is the factorization of the skew polynomial $x^4 - 1$ into 2-sided maximal elements of $\mathcal{R}$. Let us take $g_1(x) = x^2 - 1$ and $g_2(x) = x^2 + 1$, so that we have $F_w = \frac{\mathcal{R}}{\langle g_w(x)\rangle}$ for $1 \leq w \leq 2$. By applying Proposition 8.3.2, we get $V \simeq \underbrace{(F_1, F_1)}_{\mathcal{G}_1} \oplus \underbrace{(F_2, \{0\})}_{\mathcal{G}_2}$. Now let $\mathcal{C}$ be a skew Λ-MT code of length $6 = 4 + 2$ over $\mathbb{F}_{3^2}$ with the generating set $\{(x + x^2, x + 1)\}$. By Theorem 8.3.3, we see that the constituents of $\mathcal{C}$ are given by $\mathcal{C}_1 = \langle (x + 1, x + 1)\rangle$ and $\mathcal{C}_2 = \langle (x - 1, 0)\rangle$. One can easily observe that any other generator of the constituent $\mathcal{C}_1$ is of the form $B(x + 1, x + 1)$, where $B(\neq 0) \in \mathbb{F}_{3^2}$. Further, there exists $(x - 1)B^{-1}(\neq 0) \in F_1$ such that $(x - 1)B^{-1}B(x + 1, x + 1) = 0$ in $\mathcal{G}_1$, which implies that the constituent $\mathcal{C}_1$ is not a free left F_1-submodule of $\mathcal{G}_1$. One can show that the constituent $\mathcal{C}_2$ is a free left F_2-submodule of $\mathcal{G}_2$ with the free basis as $\{(x - 1, 0)\}$. This shows that each constituent of a 1-generator skew GQC code need not be a free module.*

8.4 Concatenated structure of skew MT codes

In this section, we will view skew Λ-MT codes of length n over $\mathbb{F}_q$ as direct sums of certain concatenated codes. Using their multilevel concatenated structure, we will also determine a lower bound on their minimum Hamming distances. To do this, by (8.5), we see that $x^{m_i} - \lambda_i = \prod_{w=1}^{\rho} g_w(x)^{\epsilon_{w,i}}$, where for $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$, $\epsilon_{w,i} = 1$ if $g_w(x)$ divides $x^{m_i} - \lambda_i$, and $\epsilon_{w,i} = 0$ otherwise.

Now let $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$ be fixed. If $\epsilon_{w,i} = 1$, then we see that $g_w(x)$ and $\frac{x^{m_i}-\lambda_i}{g_w(x)}$ are coprime in $Z(\mathcal{R})$, and hence there exist skew polynomials

$A_{w,i}(x), B_{w,i}(x) \in Z(\mathcal{R})$ such that $A_{w,i}(x)g_w(x)+B_{w,i}(x)\left(\frac{x^{m_i}-\lambda_i}{g_w(x)}\right) = 1$. Let us define $e_{w,i}(x) = B_{w,i}(x)\left(\frac{x^{m_i}-\lambda_i}{g_w(x)}\right)$. Further, we observe that $e_{w,i}(x)+\langle g_w(x)\rangle = 1+\langle g_w(x)\rangle$ in $\frac{\mathcal{R}}{\langle g_w(x)\rangle}$. On the other hand, if $\epsilon_{w,i} = 0$, then we define $e_{w,i}(x) = 0$. One can show that $\langle e_{w,i}(x)\rangle = \left\langle \epsilon_{w,i}\left(\frac{x^{m_i}-\lambda_i}{g_w(x)}\right)\right\rangle$ for $1 \leq w \leq \rho$ and $1 \leq i \leq \ell$. Further, for each i, working as in Proposition 8.3.2, we observe that the following hold in the ring $\frac{\mathcal{R}}{\langle x^{m_i}-\lambda_i\rangle}$:

(i) For $1 \leq w, w' \leq \rho$, we have $e_{w,i}(x)e_{w',i}(x) = \delta_{w,w'}e_{w,i}(x)$.

(ii) $e_{1,i}(x) + e_{2,i}(x) + \cdots + e_{r,i}(x) = 1$.

(iii) $\frac{\mathcal{R}}{\langle x^{m_i}-\lambda_i\rangle} = \bigoplus_{w=1}^{\rho}\langle e_{w,i}(x)\rangle$.

(iv) $\langle e_{w,i}(x)\rangle \simeq \epsilon_{w,i}F_w$ for each w and i.

Now let $\psi_{w,i}$ be the ring isomorphism from $\epsilon_{w,i}F_w$ onto $\langle e_{w,i}(x)\rangle$, which is given by $\epsilon_{w,i}\delta_w(x) \mapsto \delta_w(x)e_{w,i}(x)$ for each $\delta_w(x) \in \frac{\mathcal{R}}{\langle g_w(x)\rangle}$. The inverse of $\psi_{w,i}$ is the ring isomorphism $\phi_{w,i}$ from $\langle e_{w,i}(x)\rangle$ onto $\epsilon_{w,i}F_w$, defined as $a(x) \mapsto \epsilon_{w,i}(a(x)+\langle g_w(x)\rangle)$ for each $a(x) \in \langle e_{w,i}(x)\rangle$. Further, for each w, we recall that $\mathcal{G}_w = (\epsilon_{w,1}F_w, \epsilon_{w,2}F_w, \cdots\cdots, \epsilon_{w,\ell}F_w)$ is a left F_w-module, where $F_w = \frac{\mathcal{R}}{\langle g_w(x)\rangle}$. We shall view both V and $\mathcal{G}_w$ $(1 \leq w \leq \rho)$ as rings with respect to the component wise addition, denoted by $+$, and the component wise multiplication, denoted by $\odot$. If 1_w is the unity of F_w, then $1_{\mathcal{G}_w} := (\epsilon_{w,1}1_w, \epsilon_{w,2}1_w, \cdots, \epsilon_{w,\ell}1_w)$ and $1_V := (1, 1, \cdots, 1)$ are the unities of $\mathcal{G}_w$ and V respectively.

Next we define the maps $\Phi_w : V \to \mathcal{G}_w$ and $\Psi_w : \mathcal{G}_w \to V$ as

$$\begin{aligned}\Phi_w\big(a_1(x), a_2(x), \cdots, a_\ell(x)\big) \;=\; &\big(\epsilon_{w,1}(a_1(x)+\langle g_w(x)\rangle), \epsilon_{w,2}(a_2(x)+\langle g_w(x)\rangle), \cdots,\\ &\epsilon_{w,\ell}(a_\ell(x)+\langle g_w(x)\rangle)\big)\end{aligned}$$

for all $\big(a_1(x), a_2(x), \cdots, a_\ell(x)\big) \in V$, and

$$\Psi_w\big(\delta_1(x), \delta_2(x), \cdots, \delta_\ell(x)\big) = \big(\psi_{w,1}(\delta_1(x)), \psi_{w,2}(\delta_2(x)), \cdots, \psi_{w,\ell}(\delta_\ell(x))\big)$$

for all $\big(\delta_1(x), \delta_2(x), \cdots, \delta_\ell(x)\big) \in \mathcal{G}_w$.

For $1 \leq w \leq \rho$, let $E_w = \big(e_{w,1}(x), e_{w,2}(x), \cdots, e_{w,\ell}(x)\big) \in V$. One can show that $\Psi_w(1_{\mathcal{G}_w}) = E_w$ and $\langle E_w \rangle = \langle e_{w,1}(x) \rangle \times \langle e_{w,2}(x) \rangle \times \cdots \times \langle e_{w,\ell}(x) \rangle$. We further note that the restriction map $\Phi_w \restriction_{\langle E_w \rangle}$ and Ψ_w are inverses of each other for each w. From the above discussion, we deduce the following:

Lemma 8.4.1. *(a)* $\Psi_w(\mathcal{G}_w) = \langle E_w \rangle$ *for* $1 \leq w \leq \rho$.

(b) For $1 \leq w, w' \leq \rho$, *we have* $E_w \odot E_{w'} = \delta_{w,w'} E_w$.

(c) $\sum_{w=1}^{\rho} E_w = 1_V$ *and* $V = \bigoplus_{w=1}^{\rho} \langle E_w \rangle$.

Proof. For each $w \in \{1, 2, \cdots, \rho\}$, clearly we have $\Psi_w(\mathcal{G}_w) \subseteq \langle E_w \rangle$. For the converse let $a(x) \in \langle E_w \rangle$, where $a(x) = r(x) \odot E_w$ for some $r(x) = (r_1(x), r_2(x), \cdots, r_\ell(x)) \in V$. Thus we get, $a(x) = (r_1(x)e_{w,1}(x), r_2(x)e_{w,2}(x), \cdots, r_\ell(x)e_{w,\ell}(x)) = \Psi_w(\epsilon_{w,1}r_1(x), \epsilon_{w,2}r_2(x), \cdots, \epsilon_{w,\ell}r_\ell(x))$ for $(\epsilon_{w,1}r_1(x), \epsilon_{w,2}r_2(x), \cdots, \epsilon_{w,\ell}r_\ell(x)) \in \mathcal{G}_w$ as Ψ_w is onto, which further implies that $\langle E_w \rangle \subseteq \Psi_w(\mathcal{G}_w)$. Other two identities follows immediately by the defination. Now to prove $V = \bigoplus_{w=1}^{\rho} \langle E_w \rangle$, firstly we prove that sum is direct. Now for $1 \leq w \leq \rho$, let us suppose that $y_w(x) \in \langle E_w \rangle$ such that $y_1(x) + y_2(x) + \cdots + y_\rho(x) = 0$. On right multiplication by E_w, we get $y_w(x) = 0$ for each $1 \leq w \leq \rho$. Thus the sum is direct. Also for each $r(x) \in V$, we have $r(x) = \sum_{w=1}^{\rho} r(x) \odot E_w \in \bigoplus_{w=1}^{\rho} \langle E_w \rangle$, which implies that $V \subseteq \bigoplus_{w=1}^{\rho} \langle E_w \rangle$. Hence we get $V = \bigoplus_{w=1}^{\rho} \langle E_w \rangle$. □

Now for $1 \leq w \leq \rho$, the concatenation of $\langle E_w \rangle$ and a left F_w-submodule $\mathcal{D}$ of $\mathcal{G}_w$ is defined as

$$\langle E_w \rangle \square \mathcal{D} = \Big\{ \big(\psi_{w,1}(\delta_1(x)), \psi_{w,1}(\delta_2(x)), \cdots, \psi_{w,1}(\delta_\ell(x))\big) : \big(\delta_1(x), \delta_2(x), \cdots, \delta_\ell(x)\big) \in \mathcal{D} \Big\}.$$

In the following theorem, we show that each skew Λ-MT code of length n over $\mathbb{F}_q$ can be expressed as a direct sum of certain concatenated codes.

Theorem 8.4.2. *(a) Let $\mathcal{C}$ be a skew Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$. Then the code $\mathcal{C}$ has a concatenated structure*

$$\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle E_w \rangle \,\square\, \Phi_w\big(\mathcal{C} \odot E_w\big),$$

where $\Phi_w\big(\mathcal{C} \odot E_w\big) = \mathcal{C}_w$ for each w. As a consequence, we have $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle E_w \rangle \,\square\, \mathcal{C}_w$.

(b) Conversely, let $\mathfrak{C}_w$ be a left F_w-submodule of $\mathcal{G}_w$ for $1 \leq w \leq \rho$. Then the direct sum $\mathcal{C} = \bigoplus_{w=1}^{\rho} \langle E_w \rangle \,\square\, \mathfrak{C}_w$ is a skew Λ-MT code of length n over $\mathbb{F}_q$.

Proof. (a) To prove the result, we note that

$$\mathcal{C} = \mathcal{C} \odot 1_V = \mathcal{C} \odot \Big(\sum_{w=1}^{\rho} E_w \Big) = \bigoplus_{w=1}^{\rho} \mathcal{C} \odot E_w.$$

For $1 \leq w \leq \rho$, we see that $\mathcal{C} \odot E_w = \big\{ \big(c_1(x)e_{w,1}(x), c_2(x)e_{w,2}(x), \cdots, c_\ell(x)e_{w,\ell}(x)\big) : \big(c_1(x), c_2(x), \cdots, c_\ell(x)\big) \in \mathcal{C} \big\}$, which implies that

$$\begin{aligned}
\Phi_w(\mathcal{C} \odot E_w) &= \big\{ \big(\phi_{w,1}(c_1(x)e_{w,1}(x)), \phi_{w,2}(c_2(x)e_{w,2}(x)), \cdots, \phi_{w,\ell}(c_\ell(x)e_{w,\ell}(x))\big) \\
&\qquad : (c_1(x), c_2(x), \cdots, c_\ell(x)) \in \mathcal{C} \big\} \\
&= \big\{ \big(\epsilon_{w,1}(c_1(x) + \langle g_w(x) \rangle), \epsilon_{w,2}(c_2(x) + \langle g_w(x) \rangle), \cdots, \epsilon_{w,\ell}(c_\ell(x) \\
&\qquad + \langle g_w(x) \rangle)\big) : \big(c_1(x), c_2(x), \cdots, c_\ell(x)\big) \in \mathcal{C} \big\} \\
&= \mathcal{C}_w,
\end{aligned}$$

as $\phi_{w,i}(e_{w,i}(x)) = \epsilon_{w,i}(1 + \langle g_w(x) \rangle)$ for each i and w. Further, since the restriction map $\Phi_w \restriction_{\langle E_w \rangle}$ and the map Ψ_w are inverses of each other, we see that $\langle E_w \rangle \,\square\, \Phi_w(\mathcal{C} \odot E_w) = \mathcal{C} \odot E_w$ for each w. From this, part (a) follows.

(b) To prove this, it is enough to prove that $\langle E_w \rangle \,\square\, \mathfrak{C}_w$ is a skew Λ-MT code of length n over $\mathbb{F}_q$ for $1 \leq w \leq \rho$. For this, we observe that $\langle E_w \rangle \,\square\, \mathfrak{C}_w = \{\Psi_w\big(\delta_w(x)\big) : \delta_w(x) \in \mathfrak{C}_w\}$. It is easy to see that $\Psi_w\big(\delta_w(x)\big) + \Psi_w\big(c_w(x)\big) =$

$\Psi_w\big(\delta_w(x) + c_w(x)\big) \in \langle E_w\rangle \,\square\, \mathfrak{C}_w$ for each $\delta_w(x), c_w(x) \in \mathfrak{C}_w$. Further, for each $f(x) \in \mathcal{R}$, we note that $f_w(x) = f(x) + \langle g_w(x)\rangle \in F_w$ and that $f_w(x)\delta_w(x) \in \mathfrak{C}_w$ for each $\delta_w(x) = \big(\delta_{w,1}(x), \delta_{w,2}(x), \cdots, \delta_{w,\ell}(x)\big) \in \mathfrak{C}_w$. This implies that

$$\begin{aligned}
\Psi_w\big(f_w(x)\delta_w(x)\big) &= \big(\psi_{w,1}(f_w(x))\psi_{w,1}(\delta_{w,1}(x)), \psi_{w,2}(f_w(x))\psi_{w,2}(\delta_{w,2}(x)), \cdots \\
&\qquad \cdots, \psi_{w,\ell}(f_w(x))\psi_{w,\ell}(\delta_{w,\ell}(x))\big) \\
&= \big(f(x)e_{w,1}(x)\psi_{w,1}(\delta_{w,1}(x)), f(x)e_{w,2}(x)\psi_{w,2}(\delta_{w,2}(x)), \cdots \\
&\qquad \cdots, f(x)e_{w,\ell}(x)\psi_{w,\ell}(\delta_{w,\ell}(x))\big) \\
&= \big(f(x)\psi_{w,1}(\delta_{w,1}(x)), f(x)\psi_{w,2}(\delta_{w,2}(x)), \cdots, f(x)\psi_{w,\ell}(\delta_{w,\ell}(x))\big) \\
&= f(x)\Psi_w(\delta_w(x)),
\end{aligned}$$

as $\psi_{w,i}(\delta_{w,i}(x)) \in \langle e_{w,i}(x)\rangle$ and $e_{w,i}(x)$ is the unity of $\langle e_{w,i}(x)\rangle$ for $1 \le i \le \ell$. This shows that $f(x)\Psi_w(\delta_w(x)) \in \langle E_w\rangle \,\square\, \mathfrak{C}_w$ for each $f(x) \in \mathcal{R}$ and $\delta_w(x) \in \mathfrak{C}_w$. Therefore $\langle E_w\rangle \,\square\, \mathfrak{C}_w$ is a left $\mathcal{R}$-submodule of V for each w. From this, part (b) follows immediately.

□

Next we will show that each skew Λ-MT code of length n over $\mathbb{F}_q$ has a multilevel concatenated structure. To do this, let $\mathcal{C}$ be a skew Λ-MT code of length n over $\mathbb{F}_q$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$. Let us define

$$B_{\mathcal{C}} = \left\{ \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,\ell} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,\ell} \\ \vdots & \vdots & \vdots & \vdots \\ c_{\rho,1} & c_{\rho,2} & \cdots & c_{\rho,\ell} \end{bmatrix} : (c_{w,1}, c_{w,2}, \cdots, c_{w,\ell}) \in \mathcal{C}_w \text{ for } 1 \le w \le \rho \right\}.$$

Note that $|B_{\mathcal{C}}| = \prod_{i=1}^{\ell} |\mathcal{C}_w|$. From now on, we shall write each element $c \in B_{\mathcal{C}}$ as $c = (c^{(1)}, c^{(2)}, \cdots, c^{(\ell)})$, where $c^{(i)} = (c_{1,i}, c_{2,i}, \cdots, c_{\rho,i})^T$ denotes the ith column of c for

$1 \leq i \leq \ell$. We further note that the ith column $c^{(i)}$ of $c \in B_{\mathcal{C}}$ belongs to the mixed alphabet set $(\epsilon_{1,i}F_1, \epsilon_{2,i}F_2, \cdots, \epsilon_{\rho,i}F_\rho)^T$ for each i. In view of this, one can view $B_{\mathcal{C}}$ as an $\mathbb{F}_q$-linear code of length ℓ over the mixed alphabet set $(\epsilon_{1,1}F_1, \epsilon_{2,1}F_2, \cdots, \epsilon_{\rho,1}F_\rho)^T \times (\epsilon_{1,2}F_1, \epsilon_{2,2}F_2, \cdots, \epsilon_{\rho,2}F_\rho)^T \times \cdots \times (\epsilon_{1,\ell}F_1, \epsilon_{2,\ell}F_2, \cdots, \epsilon_{\rho,\ell}F_\rho)^T$.

Now for $1 \leq i \leq \ell$, define a map $\Upsilon_i : (\epsilon_{1,i}F_1, \epsilon_{2,i}F_2, \cdots, \epsilon_{\rho,i}F_\rho) \to \langle e_{1,i}(x)\rangle \oplus \langle e_{2,i}(x)\rangle \oplus \cdots \oplus \langle e_{\rho,i}(x)\rangle$ as

$$\Upsilon_i(c_{1,i}, c_{2,i}, \cdots, c_{\rho,i}) = \psi_{1,i}(c_{1,i}) + \psi_{2,i}(c_{2,i}) + \cdots + \psi_{\rho,i}(c_{\rho,i})$$

for each $(c_{1,i}, c_{2,i}, \cdots, c_{\rho,i}) \in (\epsilon_{1,i}F_1, \epsilon_{2,i}F_2, \cdots, \epsilon_{\rho,i}F_\rho)$.

For each i, we see that Υ_i is a left $\mathbb{F}_q$-module isomorphism, as $\psi_{w,i}$ is a ring isomorphism for $1 \leq w \leq \rho$. Further, considering $B_{\mathcal{C}}$ as an outer code, we define multilevel concatenation of $B_{\mathcal{C}}$ with $\prod_{i=1}^{\ell} \langle e_{1,i}(x)\rangle \oplus \langle e_{2,i}(x)\rangle \oplus \cdots \oplus \langle e_{\rho,i}(x)\rangle$ as

$$\Upsilon(B_{\mathcal{C}}) := \left\{ \left(\Upsilon_1(c^{(1)}), \Upsilon_2(c^{(2)}), \cdots, \Upsilon_\ell(c^{(\ell)})\right) : (c^{(1)}, c^{(2)}, \cdots, c^{(\ell)}) \in B_{\mathcal{C}} \right\}.$$

In the following theorem, we show that each skew Λ-MT code of length n over $\mathbb{F}_q$ has a multilevel concatenated structure.

Theorem 8.4.3. *For a skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$, we have $\mathcal{C} = \Upsilon(B_{\mathcal{C}})$.*

Proof. Let $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_\rho$ be the constituents of the code $\mathcal{C}$. Here in view of Theorem 8.4.2(a), it suffices to show that $\Upsilon(B_{\mathcal{C}}) = \bigoplus_{w=1}^{\rho} \langle E_w\rangle \,\square\, \mathcal{C}_w$. To prove this, we consider

$$\begin{aligned}
\Upsilon(B_{\mathcal{C}}) &= \left\{\Upsilon(b^{(1)}, b^{(2)}, \cdots, b^{(\ell)}) : (b^{(1)}, b^{(2)}, \cdots, b^{(\ell)}) \in B_{\mathcal{C}}\right\} \\
&= \left\{(\Upsilon_1(b^{(1)}), \Upsilon_2(b^{(2)}), \cdots, \Upsilon_\ell(b^{(\ell)})) : (b^{(1)}, b^{(2)}, \cdots, b^{(\ell)}) \in B_{\mathcal{C}}\right\} \\
&= \left\{\sum_{w=1}^{\rho} (\psi_{w,1}(b_{w,1}), \psi_{w,2}(b_{w,2}), \cdots, \psi_{w,\ell}(b_{w,\ell})) : (b^{(1)}, b^{(2)}, \cdots, b^{(\ell)}) \in B_{\mathcal{C}}\right\} \\
&= \bigoplus_{w=1}^{\rho} \langle E_w\rangle \,\square\, \mathcal{C}_w.
\end{aligned}$$

This proves the theorem. □

Now using the multilevel concatenated structure of skew Λ-MT codes of length n over $\mathbb{F}_q$, we also determine a lower bound on their minimum Hamming distances in the following theorem.

Theorem 8.4.4. *Let $\mathcal{C}$ be a skew Λ-MT code of length n over $\mathbb{F}_q$ with the non-zero constituents as $\mathcal{C}_{w_1}, \mathcal{C}_{w_2}, \cdots, \mathcal{C}_{w_t}$, where $1 \leq w_1, w_2, \cdots, w_t \leq \rho$. Let $\mathfrak{d}_j$ be the minimum Hamming distance of the code $\mathcal{C}_{w_j}$ for $1 \leq j \leq t$. Let us assume that $\mathfrak{d}_1 \leq \mathfrak{d}_2 \leq \cdots \leq \mathfrak{d}_t$. Let us define $\mathfrak{K}_v = \min_{\substack{I \subseteq \{1,2,\cdots,\ell\} \\ |I| = \mathfrak{d}_v}} \Big\{ \sum_{g \in I} d_{\min}(\langle e_{w_1,g}(x) \rangle \oplus \langle e_{w_2,g}(x) \rangle \oplus \cdots \oplus \langle e_{w_t,g}(x) \rangle) \Big\}$ for $v \in \{1, 2, \cdots, t\}$. Then the minimum Hamming distance $d_{\min}(\mathcal{C})$ of the code $\mathcal{C}$ satisfies*

$$d_{\min}(\mathcal{C}) \geq min\{\mathfrak{K}_1, \mathfrak{K}_2, \cdots, \mathfrak{K}_t\}.$$

Proof. Working in a similar manner as in Theorem 4.2 of Güneri et al. [41] and by applying Theorem 8.4.3, the desired result follows. □

8.5 Galois duals of skew MT codes over finite fields

Next we proceed to study dual codes of skew Λ-MT codes over finite fields with respect to the Galois inner product on $\mathbb{F}_q^n$. To do this, let k be a fixed integer satisfying $0 \leq k < r$. Let σ_k be an automorphism of $\mathbb{F}_q$, defined as $\sigma_k(b) = b^{p^k}$ for each $b \in \mathbb{F}_q$. Recall that the k-Galois inner product on $\mathbb{F}_q^n$ is a map $\langle \cdot, \cdot \rangle_k : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_k = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i - 1} a_{i,j} b_{i,j}^{p^k} \quad \text{for all } a, b \in \mathbb{F}_q^n.$$

Here we observe that $\langle \cdot, \cdot \rangle_k$ is a non-degenerate σ_k-sesquilinear form on $\mathbb{F}_q^n$. In particular, the k-Galois inner product coincides with the Euclidean inner product on $\mathbb{F}_q^n$ when $k = 0$, while the k-Galois inner product matches with the Hermitian inner product on $\mathbb{F}_q^n$ when r is even and $k = \frac{r}{2}$.

Now if $\mathcal{C}$ is a linear code of length n over $\mathbb{F}_q$, then its k-Galois dual is defined as

$$\mathcal{C}^{\perp_k} = \{a \in \mathbb{F}_q^n : \langle a, b \rangle_k = 0 \text{ for all } b \in \mathcal{C}\}.$$

In order to study the k-Galois dual $\mathcal{C}^{\perp_k}$ of the code $\mathcal{C}$, let us define $\mathcal{C}^{p^k} = \big\{\big(b_{1,0}^{p^k}, b_{1,1}^{p^k}, \cdots, b_{1,m_1-1}^{p^k}; b_{2,0}^{p^k}, b_{2,1}^{p^k}, \cdots, b_{2,m_2-1}^{p^k}; \cdots; b_{\ell,0}^{p^k}, b_{\ell,1}^{p^k}, \cdots, b_{\ell,m_\ell-1}^{p^k}\big) : (b_{1,0}, b_{1,1}, \cdots, b_{1,m_1-1}; b_{2,0}, b_{2,1}, \cdots, b_{2,m_2-1}; \cdots; b_{\ell,0}, b_{\ell,1}, \cdots, b_{\ell,m_\ell-1}) \in \mathcal{C}\big\}$, which is also a linear code of length n over $\mathbb{F}_q$. It is easy to see that $\mathcal{C}^{\perp_k} = (\mathcal{C}^{p^k})^{\perp_0}$. Furthermore, if $\mathcal{C}$ is a skew Λ-MT code, then one can show that the code $\mathcal{C}^{p^k}$ is a skew Λ^{p^k}-MT code, where $\Lambda^{p^k} = (\lambda_1^{p^k}, \lambda_2^{p^k}, \cdots, \lambda_\ell^{p^k})$. Now using the fact that $T_{\Lambda,\sigma}^m = I$, we see that $\mathcal{C}^{\perp_k}$ is a skew Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$, i.e., $\mathcal{C}^{\perp_k}$ is a linear code of length n over $\mathbb{F}_q$ satisfying the following: if $a = (a_{1,0}, a_{1,1}, \cdots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \cdots, a_{2,m_2-1}; \cdots; a_{\ell,0}, a_{\ell,1}, \cdots, a_{\ell,m_\ell-1}) \in \mathcal{C}^{\perp_k}$, then its Λ^{-p^k}-multi-twisted shift $T_{\Lambda^{-p^k},\sigma}(a) = (\lambda_1^{-p^k}\sigma(a_{1,m_1-1}), \sigma(a_{1,0}), \cdots, \sigma(a_{1,m_1-2}); \lambda_2^{-p^k}\sigma(a_{2,m_2-1}), \sigma(a_{2,0}), \cdots, \sigma(a_{2,m_2-2}); \cdots; \lambda_\ell^{-p^k}\sigma(a_{\ell,m_\ell-1}), \sigma(a_{\ell,0}), \cdots, \sigma(a_{\ell,m_\ell-2})) \in \mathcal{C}^{\perp_k}$. Equivalently, $\mathcal{C}^{\perp_k}$ is a left $\mathcal{R}$-submodule of the skew Λ^{-p^k}-MT module $V' = \prod_{i=1}^{\ell} V_i'$, where $V_i' = \frac{\mathcal{R}}{\langle x^{m_i} - \lambda_i^{-p^k} \rangle}$ for $1 \leq i \leq \ell$.

Now we make the following observation.

Lemma 8.5.1. *For $0 \leq k < r$ and $a, b \in \mathbb{F}_q^n$, we have*

(a) $\langle a, b \rangle_k = \langle b, a \rangle_{r-k}^{p^k}$.

(b) $\langle T_{\Lambda^{-p^k},\sigma}^j(a), b \rangle_k = \sigma^j\big(\langle a, T_{\Lambda,\sigma}^{m-j}(b) \rangle_k\big)$, *where* $0 \leq j \leq m-1$.

Proof. Proof is trivial. □

For $0 \leq k < r$, define a map $\mathscr{T}_k : \mathcal{R} \to \mathcal{R}$ as

$$\mathscr{T}_k(f(x)) = \sigma^t(a_0^{p^k})x^t + \sigma^{t-1}(a_1^{p^k})x^{t-1} + \cdots + \sigma(a_{t-1}^{p^k})x + a_t^{p^k}$$

for each $f(x) = a_0 + a_1x + \cdots + a_tx^t \in \mathcal{R}$ with $a_t \neq 0$.

Then we observe the following:

Lemma 8.5.2. *Let $a(x) = a_0 + a_1x^\alpha + a_2x^{2\alpha} + \cdots + a_tx^{t\alpha}$ be an element of $\mathcal{R}$, where $t \geq 0$ is an integer and a_0, a_t are non-zero elements of $\mathbb{F}_q$. Then for $0 \leq k < r$, we have the following:*

(a) $(\mathscr{T}_k \circ \mathscr{T}_{r-k})(a(x)) = (\mathscr{T}_{r-k} \circ \mathscr{T}_k)(a(x)) = a(x)$.

(b) If $d(x) = d_0 + d_1x + \cdots + d_\mu x^\mu \in \mathcal{R}$ and $a(x) \in Z(\mathcal{R})$, then $\mathscr{T}_k(a(x)d(x)) = \mathscr{T}_k(a(x))\mathscr{T}_k(d(x))$.

Proof. Its proof is straightforward. □

Next we say that the skew polynomial $f(x) \in Z(\mathcal{R})$ is

(i) $\mathscr{T}_k$-self-conjugate if it satisfies $\langle f(x)\rangle = \langle \mathscr{T}_k(f(x))\rangle$ in $\mathcal{R}$.

(ii) $\mathscr{T}_k$-conjugate to the skew polynomial $g(x) \in Z(\mathcal{R})$ if $\langle f(x)\rangle \neq \langle g(x)\rangle$ and $\langle f(x)\rangle = \langle \mathscr{T}_k(g(x))\rangle$.

In particular, when r is even and $k = \frac{r}{2}$, by using Lemma 8.5.2, we note that $f(x) \in Z(\mathcal{R})$ is $\mathscr{T}_{\frac{r}{2}}$-conjugate to $g(x) \in Z(\mathcal{R})$ if and only if $g(x) \in Z(\mathcal{R})$ is $\mathscr{T}_{\frac{r}{2}}$-conjugate to $f(x) \in Z(\mathcal{R})$. In view of this, we say that two skew polynomials $f(x), g(x) \in Z(\mathcal{R})$ form a $\mathscr{T}_{\frac{r}{2}}$-conjugate pair if they satisfy $\langle f(x)\rangle \neq \langle g(x)\rangle$ and $\langle f(x)\rangle = \langle \mathscr{T}_{\frac{r}{2}}(g(x))\rangle$.

Lemma 8.5.3. *For $0 \leq k < r$, the map $\mathcal{T}_k : \frac{\mathcal{R}}{\langle x^m-1\rangle} \to \frac{\mathcal{R}}{\langle x^m-1\rangle}$, defined as*

$$\mathcal{T}_k(d(x)) = \sum_{j=0}^{m-1} \sigma^{-j}(d_j^{p^k})x^{-j} \text{ for each } d(x) = \sum_{j=0}^{m-1} d_jx^j \in \frac{\mathcal{R}}{\langle x^m - 1\rangle},$$

is a ring anti-automorphism. (Here we have $x^{-1} = x^{m-1} \in \frac{\mathcal{R}}{\langle x^m-1\rangle}$.*)*

Proof. First of all, we will show that $\mathcal{T}_k$ is a well-defined map. For this, let $f(x), h(x) \in \frac{\mathcal{R}}{\langle x^m-1\rangle}$ be such that $f(x) = h(x)$ in $\frac{\mathcal{R}}{\langle x^m-1\rangle}$, which implies that $f(x) - h(x) = (x^m - 1)r(x)$ for some $r(x) = r_0 + r_1x + r_2x^2 + \cdots + r_tx^t \in \mathcal{R}$ with $r_t \neq 0$. Since $x^m - 1 \in Z(\mathcal{R})$, by Lemma 8.5.2(b), we get $\mathscr{T}_k(f(x) - h(x)) = \mathscr{T}_k(x^m - 1)\mathscr{T}_k(r(x)) = -(x^m - 1)\mathscr{T}_k(r(x))$, which further implies that $\mathscr{T}_k(f(x) - h(x)) = x^{\deg(f(x)-h(x))}\mathcal{T}_k(f(x) - h(x)) = 0$ in $\frac{\mathcal{R}}{\langle x^m-1\rangle}$. From this, it follows that $\mathcal{T}_k(f(x)) - \mathcal{T}_k(h(x)) = \mathcal{T}_k(f(x) - h(x)) = 0$ in $\frac{\mathcal{R}}{\langle x^m-1\rangle}$. This shows that $\mathcal{T}_k$ is a well-defined map. Further, we observe that $\mathcal{T}_k$ is a ring anti-homomorphism, and $(\mathcal{T}_{r-k} \circ \mathcal{T}_k)(d(x)) = (\mathcal{T}_k \circ \mathcal{T}_{r-k})(d(x)) = d(x)$ for each $d(x) \in \frac{\mathcal{R}}{\langle x^m-1\rangle}$. This implies that the ring anti-homomorphisms $\mathcal{T}_k$ and $\mathcal{T}_{r-k}$ of $\frac{\mathcal{R}}{\langle x^m-1\rangle}$ are inverses of each other. From this, the desired result follows. □

Next, for $0 \leq k < r$ and $1 \leq i \leq \ell$, let us define the map $\mathcal{T}_k^{(i)} : V_i \to V_i'$ as $\mathcal{T}_k^{(i)}(b_i(x)) = \sum_{j=0}^{m_i-1} \sigma^{-j}(b_{i,j}^{p^k})x^{-j}$ for each $b_i(x) = \sum_{j=0}^{m_i-1} b_{i,j}x^j \in V_i$, where $x^{-1} = \lambda_i^{p^k}x^{m_i-1} \in V_i'$. We see that the map $\mathcal{T}_k^{(i)}$ is a ring anti-isomorphism, and its inverse is a map $\mathcal{S}_k^{(i)} : V_i' \to V_i$, defined as $\mathcal{S}_k^{(i)}(a_i(x)) = \sum_{j=0}^{m_i-1} \sigma^{-j}(a_{i,j}^{p^{r-k}})x^{-j}$ for each $a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j}x^j \in V_i'$, where $x^{-1} = \lambda_i^{-1}x^{m_i-1} \in V_i$. One can easily show that the map $\mathcal{S}_k^{(i)}$ is also a ring anti-isomorphism.

Now let us define the maps $(\cdot,\cdot)_k : V' \times V \longrightarrow \frac{\mathcal{R}}{\langle x^m-1\rangle}$ and $\{\cdot,\cdot\}_k : V \times V' \longrightarrow \frac{\mathcal{R}}{\langle x^m-1\rangle}$ as

$$(a(x), b(x))_k = \sum_{i=1}^{\ell} \lambda_i^{-p^k} \left(\frac{x^m - 1}{x^{m_i} - \lambda_i^{-p^k}} \right) a_i(x)\mathcal{T}_k^{(i)}(b_i(x))$$

and

$$\{b(x), a(x)\}_k := \sum_{i=1}^{\ell} \lambda_i \left(\frac{x^m - 1}{x^{m_i} - \lambda_i} \right) b_i(x)\mathcal{S}_k^{(i)}(a_i(x))$$

for $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V'$ and $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in V$, where V and V' are viewed as left $\frac{\mathcal{R}}{\langle x^m-1\rangle}$-modules. Now we make the following

observation.

Lemma 8.5.4. *Let $a(x) \in V'$ and $b(x) \in V$.*

(a) We have

$$(a(x), b(x))_k = \langle a, b\rangle_k + \langle a, T_{\Lambda,\sigma}(b)\rangle_k\, x + \left\langle a, T^2_{\Lambda,\sigma}(b)\right\rangle_k x^2 + \cdots + \left\langle a, T^{m-1}_{\Lambda,\sigma}(b)\right\rangle_k x^{m-1}$$

and

$$\{b(x), a(x)\}_k = \langle b, a\rangle_{r-k} + \left\langle b, T_{\Lambda^{-p^k},\sigma}(a)\right\rangle_{r-k} x + \cdots + \left\langle b, T^{m-1}_{\Lambda^{-p^k},\sigma}(a)\right\rangle_{r-k} x^{m-1} \text{ in } \frac{\mathcal{R}}{\langle x^m - 1\rangle}.$$

(b) $(a(x), b(x))_k = 0$ if and only if $\{b(x), a(x)\}_k = 0$.

(c) The mapping $(\cdot,\cdot)_k$ is a non-degenerate $\mathcal{T}_k$-sesquilinear form on $V' \times V$, and the mapping $\{\cdot,\cdot\}_k$ is a non-degenerate $\mathcal{T}_{r-k}$-sesquilinear form on $V \times V'$.

Proof. To prove the result, let us write $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V'$ and $b(x) = (b_1(x), b_2(x), \cdots, b_\ell(x)) \in V$, where $a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j}x^j \in V_i'$ and $b_i(x) = \sum_{j=0}^{m_i-1} b_{i,j}x^j \in V_i$ for $1 \le i \le \ell$.

(a) Here we observe that

$$a_i(x)\mathcal{T}_k^{(i)}(b_i(x)) = \langle a_i, b_i\rangle_k + \langle a_i, T_{\lambda_i,\sigma}(b_i)\rangle_k\, x + \cdots + \left\langle a_i, T^{m_i-1}_{\lambda_i,\sigma}(b_i)\right\rangle_k x^{m_i-1}$$

and $\lambda_i^{-p^k}\left(\frac{x^m-1}{x^{m_i}-\lambda_i^{-p^k}}\right) = 1+\lambda_i^{p^k}x^{m_i}+\lambda_i^{2p^k}x^{2m_i}+\cdots+\lambda_i^{\left(\frac{m}{m_i}-1\right)p^k}x^{\left(\frac{m}{m_i}-1\right)m_i}$, where $T_{\lambda_i,\sigma}(b_i) = (\lambda_i\sigma(b_{i,m_i-1}), \sigma(b_{i,0}), \cdots, \sigma(b_{i,m_i-2}))$ is the skew λ_i-constacyclic shift of b_i for each i. From this, we get $(a(x), b(x))_k = \langle a, b\rangle_k + \langle a, T_{\Lambda,\sigma}(b)\rangle_k\, x + \left\langle a, T^2_{\Lambda,\sigma}(b)\right\rangle_k x^2 + \cdots + \left\langle a, T^{m-1}_{\Lambda,\sigma}(b)\right\rangle_k x^{m-1}$ in $\frac{\mathcal{R}}{\langle x^m-1\rangle}$. Working in a similar manner, one can show that $\{b(x), a(x)\}_k = \langle b, a\rangle_{r-k} + \left\langle b, T_{\Lambda^{-p^k},\sigma}(a)\right\rangle_{r-k} x + \cdots + \left\langle b, T^{m-1}_{\Lambda^{-p^k},\sigma}(a)\right\rangle_{r-k} x^{m-1}$ in $\frac{\mathcal{R}}{\langle x^m-1\rangle}$.

(b) By part (a), we note that $(a(x), b(x))_k = 0$ if and only if $\left\langle a, T^j_{\Lambda,\sigma}(b)\right\rangle_k = 0$ for $0 \leq j \leq m-1$. Further, for $0 \leq j \leq m-1$, by Lemma 8.5.1(a) and (b), we see that $\left\langle a, T^j_{\Lambda,\sigma}(b)\right\rangle_k = 0$ if and only if $\left\langle T^{m-j}_{\Lambda^{-p^k},\sigma}(a), b\right\rangle_k = 0$, which holds if and only if $\left\langle b, T^{m-j}_{\Lambda^{-p^k},\sigma}(a)\right\rangle_{r-k} = 0$. From this and by part (a) again, part (b) follows immediately.

(c) For this, we first observe that $(a(x), b(x)+d(x))_k = (a(x), b(x))_k + (a(x), d(x))_k$ and $(a(x)+e(x), b(x))_k = (a(x), b(x))_k + (e(x), b(x))_k$ for all $a(x), e(x) \in V'$ and $b(x), d(x) \in V$. Further, by part (a), we see that

$$\begin{aligned}(a(x), xb(x))_k &= \langle a, T_{\Lambda,\sigma}(b)\rangle_k + \left\langle a, T^2_{\Lambda,\sigma}(b)\right\rangle_k x + \cdots + \langle a, b\rangle_k x^{m-1} \\ &= (a(x), b(x))_k x^{m-1}\end{aligned}$$

and

$$\begin{aligned}(a(x), ub(x))_k &= \langle a, b\rangle_k u^{p^k} + \langle a, T_{\Lambda,\sigma}(b)\rangle_k \sigma(u^{p^k})x + \cdots \\ &\qquad \cdots + \left\langle a, T^{m-1}_{\Lambda,\sigma}(b)\right\rangle_k \sigma^{m-1}(u^{p^k})x^{m-1} \\ &= (a(x), b(x))_k u^{p^k}\end{aligned}$$

for each $u \in \mathbb{F}_q$. This implies that $(a(x), r(x)b(x))_k = (a(x), b(x))_k \mathcal{T}_k(r(x))$ for each $r(x) \in \frac{\mathcal{R}}{\langle x^m-1\rangle}$. On the other hand, since $\lambda_i^{-p^k}\left(\frac{x^m-1}{x^{m_i}-\lambda_i^{-p^k}}\right) \in Z(\mathcal{R})$ for $1 \leq i \leq \ell$, we have $(r(x)a(x), b(x))_k = r(x)\,(a(x), b(x)))_k$ for each $r(x) \in \frac{\mathcal{R}}{\langle x^m-1\rangle}$. This shows that the map $(\cdot,\cdot)_k$ is a $\mathcal{T}_k$-sesquilinear form on $V' \times V$.

Next to show that the sesquilinear form $(\cdot,\cdot)_k$ is non-degenerate, suppose that $(a(x), b(x))_k = 0$ for all $a(x) \in V'$, which, by part (a), implies that $\langle a, b\rangle_k = 0$ for all $a \in \mathbb{F}_q^n$. Now as $\langle\cdot,\cdot\rangle_k$ is a non-degenerate sesquilinear form on $\mathbb{F}_q^n$, we must have $b = 0$, and hence $b(x) = 0$. Working in a similar manner, one can show that if $(a(x), b(x))_k = 0$ for all $b(x) \in V$, then $a(x) = 0$.

Working in a similar way as above, we see that the mapping $\{\cdot,\cdot\}_k$ is a non-degenerate $\mathcal{T}_{r-k}$-sesquilinear form on $V \times V'$.

□

From the above discussion, we deduce the following:

Theorem 8.5.5. *Let $\mathcal{C}$ $(\subseteq V)$ be a skew Λ-MT code of length n over $\mathbb{F}_q$. The k-Galois dual $\mathcal{C}^{\perp_k}(\subseteq V')$ of the code $\mathcal{C}$ is a skew Λ^{-p^k}-MT code of length n over $\mathbb{F}_q$ and is given by*

$$\mathcal{C}^{\perp_k} = \{a(x) \in V' : (a(x), b(x))_k = 0 \text{ for all } b(x) \in \mathcal{C}\}.$$

A skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called (i) a k-Galois self-dual code if it satisfies $\mathcal{C}^{\perp_k} = \mathcal{C}$, (ii) a k-Galois self-orthogonal code if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_k}$, and (iii) a k-Galois LCD (linear with complementary dual) code if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_k} = 0$. To study these three classes of skew Λ-MT codes, we proceed as follows:

For $1 \leq i \leq \ell$, we see that $\mathscr{T}_k(x^{m_i} - \lambda_i) = 1 - \lambda_i^{p^k} x^{m_i} = -\lambda_i^{p^k}(x^{m_i} - \lambda_i^{-p^k})$. On the other hand, we note, by (8.5) and Lemma 8.5.2(b), that $\mathscr{T}_k(x^{m_i} - \lambda_i) = \mathscr{T}_k(g_1(x))^{\epsilon_{1,i}} \mathscr{T}_k(g_2(x))^{\epsilon_{2,i}} \cdots \mathscr{T}_k(g_\rho(x))^{\epsilon_{\rho,i}}$ for each i. From this, we obtain $x^{m_i} - \lambda_i^{-p^k} = -\lambda_i^{-p^k} \mathscr{T}_k(g_1(x))^{\epsilon_{1,i}} \mathscr{T}_k(g_2(x))^{\epsilon_{2,i}} \cdots \mathscr{T}_k(g_\rho(x))^{\epsilon_{\rho,i}}$ for $1 \leq i \leq \ell$. By Lemma 8.5.2, one can easily observe that the skew polynomials $\mathscr{T}_k(g_1(x)), \mathscr{T}_k(g_2(x)), \cdots\cdots, \mathscr{T}_k(g_\rho(x))$ are also irreducible elements of $Z(\mathcal{R})$. From this, it follows that $\mathscr{T}_k(g_1(x)), \mathscr{T}_k(g_2(x)), \cdots, \mathscr{T}_k(g_\rho(x)) \in Z(\mathcal{R})$ are all the distinct irreducible elements appearing in the factorizations of the skew polynomials $x^{m_1} - \lambda_1^{-p^k}, x^{m_2} - \lambda_2^{-p^k}, \cdots, x^{m_\ell} - \lambda_\ell^{-p^k} \in Z(\mathcal{R})$. Further, for $1 \leq w \leq \rho$, there exists a largest non-negative integer d_w satisfying the following two conditions:

(i) $g_w(x), \mathscr{T}_k(g_w(x)), \cdots, \mathscr{T}_k^{d_w}(g_w(x)) \in Z(\mathcal{R})$ are distinct irreducible factors of the skew-polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $Z(\mathcal{R})$.

(ii) Either $\langle \mathscr{T}_k^{d_w+1}(g_w(x))\rangle \neq \langle g_{w'}(x)\rangle$ for $1 \leq w' \leq \rho$ or $\langle \mathscr{T}_k^{d_w+1}(g_w(x))\rangle = \langle g_w(x)\rangle$ holds.

Definition 8.5.6. *For $1 \leq w \leq \rho$, we say that an irreducible factor $g_w(x)$ of $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $Z(\mathcal{R})$ is of*

- *Type I if $d_w = 0$ and $\langle \mathscr{T}_k(g_w(x))\rangle = \langle g_w(x)\rangle$.*
- *Type II if $d_w = 0$ and $\langle \mathscr{T}_k(g_w(x))\rangle \neq \langle g_w(x)\rangle$.*
- *Type III if $d_w \geq 1$ and $\langle \mathscr{T}_k^{d_w+1}(g_w(x))\rangle = \langle g_w(x)\rangle$.*
- *Type IV if $d_w \geq 1$ and $\langle \mathscr{T}_k^{d_w+1}(g_w(x))\rangle \neq \langle g_w(x)\rangle$.*

Now by relabelling $g_w(x)$'s (if required), we assume that $g_1(x), g_2(x), \cdots, g_{e_1}(x)$ are all the distinct Type I irreducible factors, $g_{e_1+1}(x), g_{e_1+2}(x), \cdots, g_{e_2}(x)$ are all the distinct Type II irreducible factors, $g_{e_2+1}(x), g_{e_2+2}(x), \cdots, g_{e_3(x)}$ are all the distinct Type III irreducible factors and $g_{e_3+1}(x), g_{e_3+2}(x), \cdots, g_{e_4}(x)$ are all the distinct Type IV irreducible factors of the skew polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ in $Z(\mathcal{R})$.

Note that

$$\rho = e_2 + \sum_{s=e_2+1}^{e_4} (d_s + 1).$$

For $1 \leq a \leq e_4$, $0 \leq b \leq d_a + 1$ and $1 \leq i \leq \ell$, let us define

$$R_{a,b} = \frac{\mathcal{R}}{\langle \mathscr{T}_k^b(g_a(x))\rangle} \quad \text{and} \quad \epsilon_{a,i}^{(b)} = \begin{cases} 1 & \text{if } \mathscr{T}_k^b(g_a(x)) \text{ divides } x^{m_i} - \lambda_i \text{ in } Z(\mathcal{R}); \\ 0 & \text{otherwise,} \end{cases}$$

(note that $R_{a,d_a+1} = R_{a,0}$ for $1 \leq a \leq e_1$ and $e_2 + 1 \leq a \leq e_3$). In view of the above, (8.6) can be rewritten as

$$V \simeq \left(\bigoplus_{t=1}^{e_1} \mathcal{G}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=e_1+1}^{e_2} \mathcal{G}_\mu^{(0)}\right) \oplus \left(\bigoplus_{u=e_2+1}^{e_3} \Big(\underbrace{\mathcal{G}_u^{(0)} \oplus \mathcal{G}_u^{(1)} \oplus \cdots \oplus \mathcal{G}_u^{(d_u)}}_{G_u}\Big)\right) \oplus$$

$$\Bigg(\bigoplus_{v=e_3+1}^{e_4} \Big(\underbrace{\mathcal{G}_v^{(0)} \oplus \mathcal{G}_v^{(1)} \oplus \cdots \oplus \mathcal{G}_v^{(d_v)}}_{G_v} \Big) \Bigg),$$

where $\mathcal{G}_a^{(b)} = \Big(\epsilon_{a,1}^{(b)} R_{a,b}, \epsilon_{a,2}^{(b)} R_{a,b}, \cdots, \epsilon_{a,\ell}^{(b)} R_{a,b} \Big)$ for $1 \leq a \leq e_4$ and $0 \leq b \leq d_a$.

For $1 \leq a \leq e_4, 0 \leq b \leq d_a$ and $1 \leq i \leq \ell$, we observe that if $\epsilon_{a,i}^{(b)} = 1$, then $\mathscr{T}_k^{b+1}(g_a(x))$ divides $x^{m_i} - \lambda_i^{-p^k}$ in $Z(\mathcal{R})$. Therefore by applying Proposition 8.3.2 and working as above, we see that

$$\begin{aligned} V' \simeq & \Bigg(\bigoplus_{t=1}^{e_1} \mathcal{G}_t^{(0)} \Bigg) \oplus \Bigg(\bigoplus_{\mu=e_1+1}^{e_2} \mathcal{H}_\mu^{(1)} \Bigg) \oplus \Bigg(\bigoplus_{u=e_2+1}^{e_3} \Big(\underbrace{\mathcal{H}_u^{(0)} \oplus \mathcal{H}_u^{(1)} \oplus \cdots \oplus \mathcal{H}_u^{(d_u)}}_{H_u} \Big) \Bigg) \oplus \\ & \Bigg(\bigoplus_{v=e_3+1}^{e_4} \Big(\underbrace{\mathcal{H}_v^{(d_v+1)} \oplus \mathcal{H}_v^{(1)} \oplus \cdots \oplus \mathcal{H}_v^{(d_v)}}_{H_v} \Big) \Bigg), \end{aligned}$$

where $\mathcal{G}_t^{(0)} = \big(\epsilon_{t,1}^{(0)} R_{t,0}, \epsilon_{t,2}^{(0)} R_{t,0}, \cdots, \epsilon_{t,\ell}^{(0)} R_{t,0} \big), \mathcal{H}_\mu^{(1)} = \big(\epsilon_{\mu,1}^{(0)} R_{\mu,1}, \epsilon_{\mu,2}^{(0)} R_{\mu,1}, \cdots, \epsilon_{\mu,\ell}^{(0)} R_{\mu,1} \big)$, $\mathcal{H}_u^{(0)} = \big(\epsilon_{u,1}^{(d_u)} R_{u,0}, \epsilon_{u,2}^{(d_u)} R_{u,0}, \cdots, \epsilon_{u,\ell}^{(d_u)} R_{u,0} \big), \mathcal{H}_s^{(\omega)} = \big(\epsilon_{s,1}^{(\omega-1)} R_{s,\omega}, \epsilon_{s,2}^{(\omega-1)} R_{s,\omega}, \cdots, \epsilon_{s,\ell}^{(\omega-1)} R_{s,\omega} \big)$ for $1 \leq t \leq e_1$, $e_1+1 \leq \mu \leq e_2$, $e_2+1 \leq u \leq e_3$, $e_2+1 \leq s \leq e_4$ and $1 \leq \omega \leq d_s+1$, (note that $\mathcal{H}_u^{(d_u+1)} = \mathcal{H}_u^{(0)}$, as $R_{u,d_u+1} = R_{u,0}$ for $e_2+1 \leq u \leq e_3$).

In view of this, from now on, we shall identify each element $b(x) = (b_1(x), b_2(x), \cdots \cdots, b_\ell(x)) \in V$ as $B = (B_1, B_2, \cdots, B_{e_1}, B_{e_1+1}, B_{e_1+2}, \cdots, B_{e_2}, B_{e_2+1}, B_{e_2+2}, \cdots, B_{e_3}, B_{e_3+1}, B_{e_3+2}, \cdots, B_{e_4})$, where

$$\begin{aligned} B_t &= (B_{t,1}^{(0)}, B_{t,2}^{(0)}, \cdots, B_{t,\ell}^{(0)}) \in \mathcal{G}_t^{(0)}, B_\mu = (B_{\mu,1}^{(0)}, B_{\mu,2}^{(0)}, \cdots, B_{\mu,\ell}^{(0)}) \in \mathcal{G}_\mu^{(0)} \\ B_s &= (B_{s,1}^{(0)}, B_{s,2}^{(0)}, \cdots, B_{s,\ell}^{(0)}, B_{s,1}^{(1)}, B_{s,2}^{(1)}, \cdots, B_{s,\ell}^{(1)}, \cdots, B_{s,1}^{(d_s)}, B_{s,2}^{(d_s)}, \cdots, B_{s,\ell}^{(d_s)}) \in G_s \end{aligned}$$

for $1 \leq t \leq e_1, e_1+1 \leq \mu \leq e_2, e_2+1 \leq s \leq e_4$ with $B_{a,i}^{(b)} := \epsilon_{a,i}^{(b)} \big(b_i(x) + \big\langle \mathscr{T}_k^b(g_a(x)) \big\rangle \big) \in \epsilon_{a,i}^{(b)} R_{a,b}$ for $1 \leq a \leq e_4$, $0 \leq b \leq d_a$ and $1 \leq i \leq \ell$.

Apart from this, we shall identify each element $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in V'$ as $A = (A_1, A_2, \cdots, A_{e_1}, A_{e_1+1}, A_{e_1+2}, \cdots, A_{e_2}, A_{e_2+1}, A_{e_2+2}, \cdots, A_{e_3}, A_{e_3+1}, A_{e_3+2},$

$\cdots, A_{e_4})$, where

$$A_t = (A_{t,1}^{(0)}, A_{t,2}^{(0)}, \cdots, A_{t,\ell}^{(0)}) \in \mathcal{G}_t^{(0)}, A_\mu = (A_{\mu,1}^{(1)}, A_{\mu,2}^{(1)}, \cdots, A_{\mu,\ell}^{(1)}) \in \mathcal{H}_\mu^{(1)},$$
$$A_u = (A_{u,1}^{(0)}, A_{u,2}^{(0)}, \cdots, A_{u,\ell}^{(0)}, A_{u,1}^{(1)}, A_{u,2}^{(1)}, \cdots, A_{u,\ell}^{(1)}, \cdots, A_{u,1}^{(d_u)}, A_{u,2}^{(d_u)}, \cdots, A_{u,\ell}^{(d_u)}) \in H_u \text{ and}$$
$$A_v = (A_{v,1}^{(d_v+1)}, A_{v,2}^{(d_v+1)}, \cdots, A_{v,\ell}^{(d_v+1)}, A_{v,1}^{(1)}, A_{v,2}^{(1)}, \cdots, A_{v,\ell}^{(1)}, \cdots, A_{v,1}^{(d_v)}, A_{v,2}^{(d_v)}, \cdots, A_{v,\ell}^{(d_v)}) \in H_v$$

with $A_{t,i}^{(0)} := \epsilon_{t,i}^{(0)}\big(a_i(x)+\langle g_t(x)\rangle\big)$, $A_{\mu,i}^{(1)} := \epsilon_{\mu,i}^{(0)}\big(a_i(x)+\langle \mathscr{T}_k(g_\mu(x))\rangle\big)$, $A_{u,i}^{(0)} := \epsilon_{u,i}^{(d_u)}\big(a_i(x)+\langle g_u(x)\rangle\big)$, $A_{u,i}^{(j)} := \epsilon_{u,i}^{(j-1)}\big(a_i(x) + \big\langle \mathscr{T}_k^j(g_u(x))\big\rangle\big)$ with $1 \le j \le d_u$ and $A_{v,i}^{(j')} := \epsilon_{v,i}^{(j'-1)}\big(a_i(x) + \big\langle \mathscr{T}_k^{j'}(g_v(x))\big\rangle\big)$ for $1 \le j' \le d_v+1$, $1 \le t \le e_1$, $e_1+1 \le \mu \le e_2$, $e_2+1 \le u \le e_3$, $e_3+1 \le v \le e_4$ and $1 \le i \le \ell$.

Now for $1 \le w \le \rho$, let $\deg g_w(x) = \eta_w$. Further, note that $\deg \mathscr{T}_k(g_w(x)) = \eta_w$, as $g_w(x)$ is an irreducible element of $Z(\mathcal{R})$. For $1 \le a \le e_4$, $0 \le b \le d_a$ and $1 \le i \le \ell$, let $- : \epsilon_{a,i}^{(b)} R_{a,b} \to \epsilon_{a,i}^{(b)} R_{a,b+1}$ be the map, defined as

$$\overline{h_a(x)} = \begin{cases} \sum_{s=0}^{\eta_a-1} \sigma^{-s}(h_{as}^{p^k}) x^{-s} & \text{if } \epsilon_{a,i}^{(b)} = 1; \\ 0 & \text{if } \epsilon_{a,i}^{(b)} = 0 \end{cases} \tag{8.7}$$

for all $h_a(x) = \sum_{s=0}^{\eta_a-1} h_{as}x^s \in \epsilon_{a,i}^{(b)} R_{a,b} (\subseteq V_i)$, (note that $R_{a,d_a+1} = R_{a,0}$ when $1 \le a \le e_1$ and $e_2+1 \le a \le e_3$).

We further observe that for each $B \in V$, the corresponding element $\overline{B} \in V'$ is identified as

$$(\overline{B_1}, \overline{B_2}, \cdots, \overline{B_{e_1}}, \overline{B_{e_1+1}}, \overline{B_{e_1+2}}, \cdots, \overline{B_{e_2}}, \overline{B_{e_2+1}}, \overline{B_{e_2+2}}, \cdots, \overline{B_{e_3}}, \overline{B_{e_3+1}}, \overline{B_{e_3+2}}, \cdots, \overline{B_{e_4}}),$$

where $\overline{B_t} = (\overline{B_{t,1}^{(0)}}, \overline{B_{t,2}^{(0)}}, \cdots, \overline{B_{t,\ell}^{(0)}}) \in \mathcal{G}_t^{(0)}$ for $1 \le t \le e_1$, $\overline{B_\mu} = (\overline{B_{\mu,1}^{(0)}}, \overline{B_{\mu,2}^{(0)}}, \cdots, \overline{B_{\mu,\ell}^{(0)}}) \in \mathcal{H}_\mu^{(1)}$ for $e_1+1 \le \mu \le e_2$, $\overline{B_u} = (\overline{B_{u,1}^{(d_u)}}, \overline{B_{u,2}^{(d_u)}}, \cdots, \overline{B_{u,\ell}^{(d_u)}}, \overline{B_{u,1}^{(0)}}, \overline{B_{u,2}^{(0)}}, \cdots, \overline{B_{u,\ell}^{(0)}}, \cdots, \overline{B_{u,1}^{(d_u-1)}}, \overline{B_{u,2}^{(d_u-1)}}, \cdots, \overline{B_{u,\ell}^{(d_u-1)}}) \in H_u$ for $e_2+1 \le u \le e_3$ and $\overline{B_v} = (\overline{B_{v,1}^{(d_v)}}, \overline{B_{v,2}^{(d_v)}}, \cdots, \overline{B_{v,\ell}^{(d_v)}}, \overline{B_{v,1}^{(0)}}, \overline{B_{v,2}^{(0)}}, \cdots, \overline{B_{v,\ell}^{(0)}}, \cdots, \overline{B_{v,1}^{(d_v-1)}}, \overline{B_{v,2}^{(d_v-1)}}, \cdots, \overline{B_{v,\ell}^{(d_v-1)}}) \in H_v$ for $e_3+1 \le v \le e_4$ with

$\overline{B_{a,i}^{(b)}} := \epsilon_{a,i}^{(b)}\big(\overline{b_i(x)} + \big\langle \mathscr{T}_k^{b+1}(g_a(x))\big\rangle\big) \in \epsilon_{a,i}^{(b)} R_{a,b+1}$ for all $1 \le a \le e_4$, $0 \le b \le d_a$ and $1 \le i \le \ell$.

In view of this, a skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely written as

$$\begin{aligned}\mathcal{C} \;=\; & \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t^{(0)}\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} \mathcal{C}_\mu^{(0)}\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \Big(\mathcal{C}_u^{(0)} \oplus \mathcal{C}_u^{(1)} \oplus \cdots \oplus \mathcal{C}_u^{(d_u)}\Big)\Big) \oplus \\ & \Big(\bigoplus_{v=e_3+1}^{e_4} \Big(\mathcal{C}_v^{(0)} \oplus \mathcal{C}_v^{(1)} \oplus \cdots \oplus \mathcal{C}_v^{(d_v)}\Big)\Big), \end{aligned} \tag{8.8}$$

where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}, \mathcal{C}_u^{(j)}$ and $\mathcal{C}_v^{(j')}$) is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ for $1 \le t \le e_1$ (resp. left $R_{\mu,0}$-submodule of $\mathcal{G}_\mu^{(0)}$, left $R_{u,j}$-submodule of $\mathcal{G}_u^{(j)}$ and left $R_{v,j'}$-submodule of $\mathcal{G}_v^{(j')}$ for $e_1+1 \le \mu \le e_2$, $e_2+1 \le u \le e_3$, $e_3+1 \le v \le e_4$, $0 \le j \le d_u$ and $0 \le j' \le d_v$).

Next we see that if for some a, b and i, $\epsilon_{a,i}^{(b)} = 1$, then $x^{m_i} = \lambda_i^{-p^k}$ in $R_{a,b+1}$, which implies that $\lambda_i^{-p^k}\Big(\frac{x^m-1}{x^{m_i}-\lambda_i^{-p^k}}\Big) = \frac{m}{m_i}$ in $R_{a,b+1}$. Further, the sesquilinear form corresponding to $(\cdot,\cdot)_k$ is the map $[\cdot,\cdot]_k$ from $V' \times V$ into the direct sum $\Big\{\Big(\bigoplus_{t=1}^{e_1} R_{t,0}\Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} R_{\mu,1}\Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \big(R_{u,0} \oplus R_{u,1} \oplus \cdots \oplus R_{u,d_u}\big)\Big) \oplus \Big(\bigoplus_{v=e_3+1}^{e_4} \big(R_{v,d_v+1} \oplus R_{v,1} \oplus \cdots \oplus R_{v,d_v}\big)\Big)\Big\}$, which is defined as

$$\begin{aligned}[A,B]_k = \Big(& \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{1,i}^{(0)} A_{1,i}^{(0)} \overline{B_{1,i}^{(0)}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{2,i}^{(0)} A_{2,i}^{(0)} \overline{B_{2,i}^{(0)}}, \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_1,i}^{(0)} A_{e_1,i}^{(0)} \overline{B_{e_1,i}^{(0)}}, \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_1+1,i}^{(0)} A_{e_1+1,i}^{(1)} \overline{B_{e_1+1,i}^{(0)}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_1+2,i}^{(0)} A_{e_1+2,i}^{(1)} \overline{B_{e_1+2,i}^{(0)}}, \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2,i}^{(0)} A_{e_2,i}^{(1)} \overline{B_{e_2,i}^{(0)}}, \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2+1,i}^{(d_{e_2+1})} A_{e_2+1,i}^{(0)} \overline{B_{e_2+1,i}^{(d_{e_2+1})}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2+1,i}^{(0)} A_{e_2+1,i}^{(1)} \overline{B_{e_2+1,i}^{(0)}}, \cdots, \\ & \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_2+1,i}^{(d_{e_2+1}-1)} A_{e_2+1,i}^{(d_{e_2+1})} \overline{B_{e_2+1,i}^{(d_{e_2+1}-1)}}, \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_3,i}^{(d_{e_3})} A_{e_3,i}^{(0)} \overline{B_{e_3,i}^{(d_{e_3})}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_3,i}^{(0)} A_{e_3,i}^{(1)} \overline{B_{e_3,i}^{(0)}}, \\ & \cdots, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_3,i}^{(d_{e_3}-1)} A_{e_3,i}^{(d_{e_3})} \overline{B_{e_3,i}^{(d_{e_3}-1)}}, \sum_{i=1}^{\ell} \frac{m}{m_i} \epsilon_{e_3+1,i}^{d_{e_3+1}} A_{e_3+1,i}^{d_{e_3+1}+1} \overline{B_{e_3+1,i}^{d_{e_3+1}}}, \end{aligned}$$

$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{e_3+1,i}^{(0)}A_{e_3+1,i}^{(1)}\overline{B_{e_3+1,i}^{(0)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{e_3+1,i}^{(d_{e_3+1}-1)}A_{e_3+1,i}^{(d_{e_3+1})}\overline{B_{e_3+1,i}^{(d_{e_3+1}-1)}},\cdots,$$
$$\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{e_4,i}^{(d_{e_4})}A_{e_4,i}^{(d_{e_4}+1)}\overline{B_{e_4,i}^{(d_{e_4})}},\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{e_4,i}^{(0)}A_{e_4,i}^{(1)}\overline{B_{e_4,i}^{(0)}},\cdots,\sum_{i=1}^{\ell}\frac{m}{m_i}\epsilon_{e_4,i}^{(d_{e_4}-1)}A_{e_4,i}^{(d_{e_4})}\overline{B_{e_4,i}^{(d_{e_4}-1)}}\Big).$$

Moreover, with respect to form defined by $(*)$, we observe that the k-Galois dual $\mathcal{C}^{\perp_k}$ of $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp_k}=\Big(\bigoplus_{t=1}^{e_1}\mathcal{C}_t^{(0)\perp_k}\Big)\oplus\Big(\bigoplus_{\mu=e_1+1}^{e_2}\mathcal{C}_\mu^{(0)\perp_k}\Big)\oplus\Big(\bigoplus_{u=e_2+1}^{e_3}\big(\mathcal{C}_u{}^{(d_u)\perp_k}\oplus\mathcal{C}_u{}^{(0)\perp_k}\oplus\cdots\oplus\mathcal{C}_u{}^{(d_u-1)\perp_k}\big)\Big)$$
$$\oplus\Big(\bigoplus_{v=e_3+1}^{e_4}\big(\mathcal{C}_v{}^{(d_v)\perp_k}\oplus\mathcal{C}_v{}^{(0)\perp_k}\oplus\cdots\oplus\mathcal{C}_v{}^{(d_v-1)\perp_k}\big)\Big),\tag{8.9}$$

where

- $\mathcal{C}_t^{(0)\perp_k}(\subseteq\mathcal{G}_t^{(0)})$ is the orthogonal complement of $\mathcal{C}_t^{(0)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}}$ for $1\le t\le e_1$;
- $\mathcal{C}_\mu^{(0)\perp_k}(\subseteq\mathcal{H}_\mu^{(1)})$ is the orthogonal complement of $\mathcal{C}_\mu^{(0)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}}$ for $e_1+1\le\mu\le e_2$;
- $\mathcal{C}_u^{(j)\perp_k}(\subseteq\mathcal{H}_u^{(j+1)})$ is the orthogonal complement of $\mathcal{C}_u^{(j)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_u^{(j+1)}\times\mathcal{G}_u^{(j)}}$ for $0\le j\le d_u-1$ and $\mathcal{C}_u^{(d_u)\perp_k}(\subseteq\mathcal{H}_u^{(0)})$ is the orthogonal complement of $\mathcal{C}_u^{(d_u)}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_u^{(0)}\times\mathcal{G}_u^{(d_u)}}$ for $e_2+1\le u\le e_3$; and
- $\mathcal{C}_v^{(j')\perp_k}(\subseteq\mathcal{H}_v^{(j'+1)})$ is the orthogonal complement of $\mathcal{C}_v^{(j')}$ with respect to $[\cdot,\cdot]_k\restriction_{\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}}$ for $e_3+1\le v\le e_4$ and $1\le j'\le d_v$.

Here $[\cdot,\cdot]_k\restriction_{\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}}$ (resp. $[\cdot,\cdot]_k\restriction_{\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}}$, $[\cdot,\cdot]_k\restriction_{\mathcal{H}_u^{(j+1)}\times\mathcal{G}_u^{(j)}}$, $[\cdot,\cdot]_k\restriction_{\mathcal{H}_u^{(0)}\times\mathcal{G}_u^{(d_u)}}$ and $[\cdot,\cdot]_k\restriction_{\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}}$) denotes the restriction of the form $[\cdot,\cdot]_k$ (as defined by $(*)$) to $\mathcal{G}_t^{(0)}\times\mathcal{G}_t^{(0)}$ (resp. $\mathcal{H}_\mu^{(1)}\times\mathcal{G}_\mu^{(0)}$, $\mathcal{H}_u^{(j+1)}\times\mathcal{G}_u^{(j)}$, $\mathcal{H}_u^{(0)}\times\mathcal{G}_u^{(d_u)}$ and $\mathcal{H}_v^{(j'+1)}\times\mathcal{G}_v^{(j')}$) for each t (resp. μ, u, j, v and j').

For $e_2+1\le u\le e_3$ and $e_3+1\le v\le e_4$, let $\mathcal{K}_u^{(j)}=\mathcal{G}_u^{(j)}\cap\mathcal{H}_u^{(j)}$ and $\mathcal{K}_v^{(j')}=\mathcal{G}_v^{(j')}\cap\mathcal{H}_v^{(j')}$, where $0\le j\le d_u$ and $1\le j'\le d_v$. In the following theorem, we derive

necessary and sufficient conditions under which a skew Λ-MT code is (i) k-Galois self-dual, (ii) k-Galois self-orthogonal and (iii) k-Galois LCD.

Theorem 8.5.7. *Let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$ be fixed, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q^\sigma$. Let*

$$\mathcal{C} = \left(\bigoplus_{t=1}^{e_1} \mathcal{C}_t^{(0)}\right) \oplus \left(\bigoplus_{\mu=e_1+1}^{e_2} \mathcal{C}_\mu^{(0)}\right) \oplus \left(\bigoplus_{u=e_2+1}^{e_3} \left(\mathcal{C}_u^{(0)} \oplus \mathcal{C}_u^{(1)} \oplus \cdots \oplus \mathcal{C}_u^{(d_u)}\right)\right) \oplus \left(\bigoplus_{v=e_3+1}^{e_4} \left(\mathcal{C}_v^{(0)} \oplus \mathcal{C}_v^{(1)} \oplus \cdots \oplus \mathcal{C}_v^{(d_v)}\right)\right)$$

be a skew Λ-MT code of length n over $\mathbb{F}_q$, where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}$, $\mathcal{C}_u^{(j)}$ and $\mathcal{C}_v^{(j')}$) is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ for $1 \leq t \leq e_1$ (resp. left $R_{\mu,0}$-submodule of $\mathcal{G}_\mu^{(0)}$, left $R_{u,j}$-submodule of $\mathcal{G}_u^{(j)}$ and left $R_{v,j'}$-submodule of $\mathcal{G}_v^{(j')}$ for $e_1 + 1 \leq \mu \leq e_2$, $e_2 + 1 \leq u \leq e_3$, $e_3 + 1 \leq v \leq e_4$, $0 \leq j \leq d_u$ and $0 \leq j' \leq d_v$). Then for $0 \leq k < r$, the following hold.

(a) The code $\mathcal{C}$ is k-Galois self-dual if and only if the following conditions are satisfied:

- *None of the skew polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ has an irreducible factor of the Type II in $Z(\mathcal{R})$.*
- *For $1 \leq t \leq e_1$, $\mathcal{C}_t^{(0)}$ is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ satisfying $\mathcal{C}_t^{(0)} = \mathcal{C}_t^{(0)\perp_k}$.*
- *For $e_2 + 1 \leq u \leq e_3$ and $0 \leq j \leq d_u$, $\mathcal{C}_u^{(j)}$ is a left $R_{u,j}$-submodule of $\mathcal{K}_u^{(j)}$ satisfying $\mathcal{C}_u^{(0)} = \mathcal{C}_u^{(d_u)\perp_k}$, $\mathcal{C}_u^{(1)} = \mathcal{C}_u^{(0)\perp_k}$, $\mathcal{C}_u^{(2)} = \mathcal{C}_u^{(1)\perp_k}$, $\cdots$, $\mathcal{C}_u^{(d_u)} = \mathcal{C}_u^{(d_u-1)\perp_k}$.*
- *For $e_3 + 1 \leq v \leq e_4$, $\mathcal{C}_v^{(0)} = \{0\}, \mathcal{C}_v^{(1)} = \mathcal{K}_v^{(1)}$ and $\mathcal{C}_v^{(j')}$ is a left $R_{v,j'}$-submodule of $\mathcal{K}_v^{(j')}$ satisfying $\mathcal{C}_v^{(j')} = \mathcal{K}_v^{(j')} \cap \mathcal{C}_v^{(j'-1)\perp_k}$ and $\mathcal{C}_v^{(d_v)\perp_k} = \{0\}$, where $2 \leq j' \leq d_v$.*

(b) The code $\mathcal{C}$ is k-Galois self-orthogonal if and only if the following conditions are satisfied:

- *For $1 \leq t \leq e_1$, $\mathcal{C}_t^{(0)}$ is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ satisfying $\mathcal{C}_t^{(0)} \subseteq \mathcal{C}_t^{(0)\perp_k}$.*
- *For $e_1 + 1 \leq \mu \leq e_2$, $\mathcal{C}_\mu^{(0)} = \{0\}$.*
- *For $e_2 + 1 \leq u \leq e_3$ and $0 \leq j \leq d_u$, $\mathcal{C}_u^{(j)}$ is a left $R_{u,j}$-submodule of $\mathcal{K}_u^{(j)}$ satisfying $\mathcal{C}_u^{(0)} \subseteq \mathcal{C}_u^{(d_u)\perp_k}$, $\mathcal{C}_u^{(1)} \subseteq \mathcal{C}_u^{(0)\perp_k}$, $\mathcal{C}_u^{(2)} \subseteq \mathcal{C}_u^{(1)\perp_k}, \cdots, \mathcal{C}_u^{(d_u)} \subseteq \mathcal{C}_u^{(d_u-1)\perp_k}$.*
- *For $e_3 + 1 \leq v \leq e_4$, $\mathcal{C}_v^{(0)} = \{0\}$, $\mathcal{C}_v^{(1)}$ is any left $R_{v,1}$-submodule of $\mathcal{K}_v^{(1)}$ and $\mathcal{C}_v^{(j')}$ is a left $R_{v,j'}$-submodule of $\mathcal{K}_v^{(j')}$ satisfying $\mathcal{C}_v^{(j')} \subseteq \mathcal{C}_v^{(j'-1)\perp_k}$, where $2 \leq j' \leq d_v$.*

(c) The code $\mathcal{C}$ is k-Galois LCD if and only if the following conditions are satisfied:

- *For $1 \leq t \leq e_1$, $\mathcal{C}_t^{(0)}$ is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ satisfying $\mathcal{C}_t^{(0)} \cap \mathcal{C}_t^{(0)\perp_k} = \{0\}$.*
- *For $e_1 + 1 \leq \mu \leq e_2$, $\mathcal{C}_\mu^{(0)}$ is any left $R_{\mu,0}$-submodule of $\mathcal{G}_\mu^{(0)}$.*
- *For $e_2 + 1 \leq u \leq e_3$ and $0 \leq j \leq d_u$, $\mathcal{C}_u^{(j)}$ is a left $R_{u,j}$-submodule of $\mathcal{G}_u^{(j)}$ satisfying $\mathcal{C}_u^{(0)} \cap \mathcal{C}_u^{(d_u)\perp_k} = \{0\}$, $\mathcal{C}_u^{(1)} \cap \mathcal{C}_u^{(0)\perp_k} = \{0\}, \cdots, \mathcal{C}_u^{(d_u)} \cap \mathcal{C}_u^{(d_u-1)\perp_k} = \{0\}$.*
- *For $e_3 + 1 \leq v \leq e_4$, $\mathcal{C}_v^{(0)}$ is any left $R_{v,0}$-submodule of $\mathcal{G}_v^{(0)}$ and $\mathcal{C}_v^{(j')}$ is a left $R_{v,j'}$-submodule of $\mathcal{G}_v^{(j')}$ satisfying $\mathcal{C}_v^{(j')} \cap \mathcal{C}_v^{(j'-1)\perp_k} = \{0\}$, where $1 \leq j' \leq d_v$.*

Proof. By (8.8) and (8.9), the desired result follows. □

When either $k = 0$ or r is even and $k = \frac{r}{2}$, we see that $\mathscr{T}_k^2(g_w(x)) = g_w(x)$, which implies that $d_w \leq 1$ for $1 \leq w \leq \rho$. This further implies that the skew polynomials $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ do not have an irreducible factor of the Type IV

in $Z(\mathcal{R})$. In view of this and by (8.8), we note that a skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ can be uniquely expressed as

$$\mathcal{C} = \Big(\bigoplus_{t=1}^{e_1} \mathcal{C}_t^{(0)} \Big) \oplus \Big(\bigoplus_{\mu=e_1+1}^{e_2} \mathcal{C}_\mu^{(0)} \Big) \oplus \Big(\bigoplus_{u=e_2+1}^{e_3} \big(\mathcal{C}_u^{(0)} \oplus \mathcal{C}_u^{(1)} \big) \Big), \tag{8.10}$$

where $\mathcal{C}_t^{(0)}$ (resp. $\mathcal{C}_\mu^{(0)}$ and $\mathcal{C}_u^{(j)}$) is a left $R_{t,0}$-submodule of $\mathcal{G}_t^{(0)}$ for $1 \leq t \leq e_1$ (resp. left $R_{\mu,0}$-submodule of $\mathcal{G}_\mu^{(0)}$ and left $R_{u,j}$-submodule of $\mathcal{G}_u^{(j)}$ for $e_1 + 1 \leq \mu \leq e_2$, $e_2 + 1 \leq u \leq e_3$ and $0 \leq j \leq 1$). Furthermore, when $\sigma = I$, we see that each constituent of a Λ-MT code of length n over $\mathbb{F}_q$ is a free module.

8.6 Generator theory for skew MT codes

In this section, we will extend the results derived in Section 3.4 and develop generator theory for skew Λ-MT codes. We will also derive a BCH type lower bound on their minimum Hamming distances. The other results derived in Section 3.4 can be similarly extended to skew Λ-MT codes.

A skew Λ-MT code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is called a ϱ-generator code if ϱ is the smallest positive integer satisfying the following property: There exist ϱ number of distinct codewords $b_1(x), b_2(x), \cdots, b_\varrho(x) \in \mathcal{C}$ such that each codeword $c(x) \in \mathcal{C}$ can be expressed as $c(x) = f_1(x)b_1(x) + f_2(x)b_2(x) + \cdots + f_\varrho(x)b_\varrho(x)$ for some $f_1(x), f_2(x), \cdots, f_\varrho(x) \in \mathcal{R}$. The set $\{b_1(x), b_2(x), \cdots, b_\varrho(x)\}$ is called a generating set of $\mathcal{C}$, and we shall write $\mathcal{C} = \langle b_1(x), b_2(x), \cdots, b_\varrho(x) \rangle_L$. The annihilator of $\mathcal{C}$ is defined as $\mathrm{Ann}(\mathcal{C}) = \{f(x) \in \mathcal{R} : b_\varsigma(x)f(x) = 0 \text{ in } V \text{ for } 1 \leq \varsigma \leq \varrho\}$. It is easy to see that $\prod_{i=1}^{\ell} (x^{m_i} - \lambda_i) \in \mathrm{Ann}(\mathcal{C})$, and that $\mathrm{Ann}(\mathcal{C})$ is a non-zero right ideal of $\mathcal{R}$. As $\mathcal{R}$ is a right principal ideal ring, there exists a unique smallest degree monic skew polynomial $h(x)$ in $\mathcal{R}$ such that $Ann(\mathcal{C}) = \langle h(x) \rangle_R$. The skew polynomial $h(x)$ is called the parity-check polynomial of $\mathcal{C}$.

In Example 8.3.1, we have shown that constituents of a skew Λ-MT code need

not be free modules, and hence the rank (or dimension) can not be defined for such constituents. However, by Well-ordering principle, we can choose a minimal generating set (i.e., a generating set of the smallest cardinality) for each constituent. In the following theorem, we determine the cardinality of a minimal generating set of a skew Λ-MT code from cardinalities of minimal generating sets of its constituents, which generalizes Theorem 3.5 of Gao et al. [48].

Theorem 8.6.1. *Let $\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w$ be a skew Λ-MT code of length n over $\mathbb{F}_q$, where each constituent $\mathcal{C}_w$ is a left F_w-submodule of $\mathcal{G}_w$ for each w. Let $\mathcal{K} = \max\{k_1, k_2, \cdots, k_\rho\}$, where k_w is the cardinality of a minimal generating set of $\mathcal{C}_w$ for $1 \leq w \leq \rho$. Then $\mathcal{C}$ is a ϱ-generator skew Λ-MT code if and only if $\varrho = \mathcal{K}$.*

Proof. Working in a similar manner as in Theorem 3.5 of Gao et al. [48], the desired result follows. □

Theorem 5.3(i) of Gao et el. [48] states that if $\mathcal{C} = \bigoplus_{w=1}^{\rho} \mathcal{C}_w$ is a $\mathcal{K}$-generator skew QC code with each constituent as a free module of rank k_w, then its Euclidean dual $\mathcal{C}^{\perp_0}$ is an $(\ell - \mathcal{K}')$-generator skew QC code, where $\mathcal{K} = \max\{k_1, k_2, \cdots, k_\rho\}$ and $\mathcal{K}' = \min\{k_1, k_2, \cdots, k_\rho\}$. In the following example, we show that this theorem does not hold in general.

Example 8.6.1. *Let $q = 3^2$, $\ell = 3$, $m_1 = m_2 = m_3 = 2$, $\Lambda = (1, 1, 1)$, and let $\sigma = \sigma_1$ be the Frobenius automorphism of $\mathbb{F}_{3^2}$. Here we have $V = V_1 \times V_2 \times V_3 = \frac{\mathcal{R}}{\langle x^2-1\rangle} \times \frac{\mathcal{R}}{\langle x^2-1\rangle} \times \frac{\mathcal{R}}{\langle x^2-1\rangle}$. We first note that $\mathbb{F}_{3^2}^{\sigma} = \mathbb{F}_3$ and $O(\sigma) = 2$, which, by Theorem 8.2.1(c), gives $Z(\mathcal{R}) = \mathbb{F}_3[x^2]$. We next observe that the skew polynomial $x^2 - 1$ is irreducible in $Z(\mathcal{R})$. Thus we have $\rho = 1$, which gives $\mathcal{K} = \mathcal{K}'$.*

(i) Let $\mathcal{C}$ be a 1-generator skew QC code of length $6 = 2 + 2 + 2$ over $\mathbb{F}_{3^2}$ with the generating set $\{(x + 1, 0, 0)\}$. Here we have $\mathcal{K} = \mathcal{K}' = 1$ and $\ell - \mathcal{K}' = 3 - 1 = 2$. By Theorem 8.5.5, we see that the Euclidean dual of $\mathcal{C}$ is given by $\mathcal{C}^{\perp_0} = \{(a(x + 1), b_0 + b_1 x, c_0 + c_1 x) : a, b_0, b_1, c_0, c_1 \in \mathbb{F}_{3^2}\}$. Here we observe

that $\mathcal{C}^{\perp_0}(\subseteq V)$ is a 3-generator skew QC code of length 6 over $\mathbb{F}_{3^2}$. This shows that the Euclidean dual of a $\mathcal{K}$-generator skew QC code need not be an $(\ell-\mathcal{K}')$-generator code

(ii) Let a be a primitive element of $\mathbb{F}_{3^2}$, let $F_1 = \frac{\mathcal{R}}{\langle x^2-1\rangle}$, and let $\mathcal{C}$ be a 1-generator skew QC code of length $6 = 2+2+2$ over $\mathbb{F}_{3^2}$ with the generating set $\{(a(x+1), x+1, 0)\}$. Here we have $\mathcal{K} = \mathcal{K}' = 1$ and $\ell - \mathcal{K}' = 3-1 = 2$. Note that $\mathcal{C} = \mathcal{C}_1$ is a free left F_1-submodule of $\mathcal{G}_1$ with rank 1. By Theorem 8.5.5, we see that the Euclidean dual of $\mathcal{C}$ is given by $\mathcal{C}^{\perp_0} = \{(-a_1a^2 - b_0a^{-1} - b_1a^{-1} + a_1x, b_0+b_1x, c_0+c_1x) : a_1, b_0, b_1, c_0, c_1 \in \mathbb{F}_{3^2}\}$. From this, one can easily observe that $|\mathcal{C}^{\perp_0}| = 9^5$, which implies that $\mathcal{C}^{\perp_0}(\subseteq V)$ is not a free left F_1-submodule of $\mathcal{G}_1$ with rank $\ell - \mathcal{K}' = 2$.

In the following theorem, we obtain the parity-check polynomial of a ϱ-generator skew Λ-MT code of length n over $\mathbb{F}_q$. We also determine the dimension of a 1-generator skew Λ-MT code of length n over $\mathbb{F}_q$. We also obtain generating sets of k-Galois duals of some ϱ-generator skew Λ-MT codes. Apart from this, we derive a BCH type lower bound on minimum Hamming distances of ϱ-generator skew Λ-MT codes.

Theorem 8.6.2. *Let $\mathcal{C} = \langle b_1(x), b_2(x), \cdots, b_\varrho(x)\rangle_L$ be a ϱ-generator skew Λ-MT code of length n over $\mathbb{F}_q$, where $b_\varsigma(x) = (b_{\varsigma,1}(x), b_{\varsigma,2}(x), \cdots, b_{\varsigma,\ell}(x))$ for $1 \le \varsigma \le \varrho$. For $1 \le i \le \ell$, let us define $w_i(x) = gcrd(b_{1,i}(x), b_{2,i}(x), \cdots, b_{\varrho,i}(x), x^{m_i} - \lambda_i)$ and $W_i(x) = gcld(b_{1,i}(x), b_{2,i}(x), \cdots, b_{\varrho,i}(x), x^{m_i} - \lambda_i)$. Let η_i be the maximum number of consecutive exponents of right zeros of $w_i(x)$ over $\mathbb{F}_q$ for each i.*

(a) For $1 \le i \le \ell$, if π_i is the projection of V onto V_i, then $\pi_i(\mathcal{C})$ is a skew λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ (i.e., $\pi_i(\mathcal{C})$ is a left ideal of V_i). Furthermore, we have $\pi_i(\mathcal{C}) = \langle w_i(x)\rangle_L$ for each i.

(b) The parity-check polynomial $h(x)$ of $\mathcal{C}$ is given by $h(x) = \underset{1\le i\le \ell}{lcrm}\left[\frac{x^{m_i}-\lambda_i}{w_i(x)}\right]$.

(c) When $\varrho = 1$, we have $dim_{\mathbb{F}_q}\mathcal{C} = deg \underset{1\le i\le \ell}{lclm}\left[\frac{x^{m_i}-\lambda_i}{gcld(b_{1,i}(x),x^{m_i}-\lambda_i)}\right]$.

(d) When $x^{m_1}-\lambda_1, x^{m_2}-\lambda_2, \cdots, x^{m_\ell}-\lambda_\ell \in Z(\mathcal{R})$ are pairwise coprime polynomials in $\mathcal{R}$, we have

$$\mathcal{C}^{\perp_k} = \langle H_1(x), H_2(x), \cdots, H_\ell(x)\rangle_L,$$

where $H_i(x) = (0, \cdots, 0, \underbrace{\mathcal{T}_k^{(i)}\left(\frac{x^{m_i}-\lambda_i}{w_i(x)}\right)}_{i^{th}\ position}, 0, \cdots, 0)$ *for* $1 \le i \le \ell$.

(e) The minimum Hamming distance $d_{\min}(\mathcal{C})$ of the code $\mathcal{C}$ satisfies

$$d_{\min}(\mathcal{C}) \ge \min_{1\le i\le \ell}(\eta_i + 1).$$

(f) When $\varrho = 1$, the minimum Hamming distance $d_{\min}(\mathcal{C})$ of the code $\mathcal{C}$ satisfies

$$d_{\min}(\mathcal{C}) \ge \sum_{i\notin K}(\eta_i + 1),$$

where $K \subseteq \{1, 2, \cdots, \ell\}$ is a set of maximum cardinality such that $\underset{i\in K}{lclm}\left[\frac{x^{m_i}-\lambda_i}{W_i(x)}\right] \neq \underset{1\le i\le \ell}{lclm}\left[\frac{x^{m_i}-\lambda_i}{W_i(x)}\right]$.

In particular, when $\frac{x^{m_1}-\lambda_1}{W_1(x)} = \frac{x^{m_2}-\lambda_2}{W_2(x)} = \cdots = \frac{x^{m_\ell}-\lambda_\ell}{W_\ell(x)}$, we have

$$d_{\min}(\mathcal{C}) \ge \sum_{1\le i\le \ell}(\eta_i + 1).$$

Proof. For $1 \le i \le \ell$, since $w_i(x) = \text{gcrd}(b_{1,i}(x), b_{2,i}(x), \cdots, b_{\varrho,i}(x), x^{m_i} - \lambda_i)$, by Theorem 8.2.3, we see that there exist $A_{1,i}(x), A_{2,i}(x), \cdots, A_{\varrho+1,i}(x) \in \mathcal{R}$ such that

$$w_i(x) = A_{1,i}(x)b_{1,i}(x) + A_{2,i}(x)b_{2,i}(x) + \cdots + A_{\varrho,i}(x)b_{\varrho,i}(x) + A_{\varrho+1,i}(x)(x^{m_i} - \lambda_i). \tag{8.11}$$

Further, for each i, we can write

$$b_{\varsigma,i}(x) = \alpha_{\varsigma,i}(x)w_i(x) \tag{8.12}$$

for some $\alpha_{\varsigma,i}(x) \in \mathcal{R}$, where $1 \leq \varsigma \leq \varrho$.

(a) To prove this, let $1 \leq i \leq \ell$ be fixed. It is easy to see that $\pi_i(\mathcal{C})$ is a left ideal of V_i. Now to prove the second part, we see, by (8.11), that $w_i(x) = A_{1,i}(x)b_{1,i}(x)+A_{2,i}(x)b_{2,i}(x)+\cdots+A_{\varrho,i}(x)b_{\varrho,i}(x) = \pi_i(A_{1,i}(x)b_1(x)+A_{2,i}(x)b_2(x) + \cdots + A_{\varrho,i}(x)b_\varrho(x)) \in \pi_i(\mathcal{C})$ in V_i, which implies that

$$\langle w_i(x)\rangle_L \subseteq \pi_i(\mathcal{C}). \tag{8.13}$$

On the other hand, for each $a(x) \in \pi_i(\mathcal{C})$, there exists $c(x) \in \mathcal{C}$ such that $\pi_i(c(x)) = a(x)$. As $\mathcal{C} = \langle b_1(x), b_2(x), \cdots, b_\varrho(x)\rangle_L$, there exist $f_1(x), f_2(x), \cdots, f_\varrho(x) \in \mathcal{R}$ such that $c(x) = \sum_{\varsigma=1}^{\varrho} f_\varsigma(x)b_\varsigma(x)$. From this and by (8.12), we obtain $a(x) = \pi_i(c(x)) = \sum_{\varsigma=1}^{\varrho} f_\varsigma(x)b_{\varsigma,i}(x) = \sum_{\varsigma=1}^{\varrho} f_\varsigma(x)\alpha_{\varsigma,i}(x)w_i(x) \in \langle w_i(x)\rangle_L$, which implies that

$$\pi_i(\mathcal{C}) \subseteq \langle w_i(x)\rangle_L. \tag{8.14}$$

By (8.13) and (8.14), we get $\pi_i(\mathcal{C}) = \langle w_i(x)\rangle_L$.

(b) For $1 \leq i \leq \ell$, we see that $x^{m_i} - \lambda_i \in Z(\mathcal{R})$ and $w_i(x)$ is a right divisor of $x^{m_i} - \lambda_i$ in $\mathcal{R}$, so by Theorem 8.2.1(d), there exists $p_i(x) \in \mathcal{R}$ such that

$$x^{m_i} - \lambda_i = w_i(x)p_i(x) = p_i(x)w_i(x). \tag{8.15}$$

Further, let us define $L(x) = \text{lcrm}\,[p_1(x), p_2(x), \cdots, p_\ell(x)]$. Here we will show that $h(x) = L(x)$.

As $\text{Ann}(\mathcal{C}) = \langle h(x)\rangle_R$, we have $b_\varsigma(x)h(x) = 0$ for $1 \leq \varsigma \leq \varrho$. This implies

that $b_{\varsigma,i}(x)h(x) = 0$ in V_i for each i and ς. From this and by (8.11), it follows that $w_i(x)h(x) = \sum_{\varsigma=1}^{\varrho} A_{\varsigma,i}(x)b_{\varsigma,i}(x)h(x) = 0$ in V_i for each i. This implies that $w_i(x)h(x) = (x^{m_i} - \lambda_i)\beta_i(x) = w_i(x)p_i(x)\beta_i(x)$ in $\mathcal{R}$ for some $\beta_i(x) \in \mathcal{R}$, which further implies, by Theorem 8.2.1(a), that $h(x) = p_i(x)\beta_i(x)$ for each i. From this, we see that

$$h(x) = L(x)\beta(x) \text{ for some } \beta(x) \in \mathcal{R}. \tag{8.16}$$

On the other hand, as $L(x) = \text{lcrm}\left[p_1(x), p_2(x), \cdots, p_\ell(x)\right]$, we can write

$$L(x) = p_i(x)\alpha_i(x), \tag{8.17}$$

where $\alpha_i(x) \in \mathcal{R}$ for each i. Now for $1 \leq \varsigma \leq \varrho$, we observe, by (8.12) and (8.17), that $b_{\varsigma,i}(x)L(x) = \alpha_{\varsigma,i}(x)w_i(x)p_i(x)\alpha_i(x) = \alpha_{\varsigma,i}(x)(x^{m_i} - \lambda_i)\alpha_i(x) = 0$ in V_i for each i. This implies that

$$b_\varsigma(x)L(x) = (b_{\varsigma,1}(x)L(x), b_{\varsigma,2}(x)L(x), \cdots, b_{\varsigma,\ell}(x)L(x)) = 0$$

in V for each ς. That is, we have $L(x) \in Ann(\mathcal{C}) = \langle h(x)\rangle_R$, which implies that

$$L(x) = h(x)K(x) \text{ for some } K(x) \in \mathcal{R}. \tag{8.18}$$

By (8.16) and (8.18), we get $h(x) = L(x)\beta(x) = h(x)K(x)\beta(x)$. Now by Theorem 8.2.1(a), we get $K(x)\beta(x) = 1$ in $\mathcal{R}$, which implies that both $K(x), \beta(x) \in \mathbb{F}_q$. As both $h(x)$ and $L(x)$ are monic skew polynomials in $\mathcal{R}$, we get $h(x) = L(x)$.

(c) Here we have $\varrho = 1$ so that $\mathcal{C} = \langle b_1(x)\rangle_L$. Let us define a map $\phi : \mathcal{R} \to V$ as $\phi(f(x)) = f(x)b_1(x)$ for each $f(x) \in \mathcal{R}$. It is easy to see that ϕ is a left $\mathcal{R}$-module homomorphism with the image as $\phi(\mathcal{R}) = \mathcal{C}$. Further, the kernel of

ϕ is given by $\mathcal{D} = \{f(x) \in \mathcal{R} : f(x)b_1(x) = 0\}$. Note that $\mathcal{D}$ is a left ideal of $\mathcal{R}$, and that $\frac{\mathcal{R}}{\mathcal{D}} \simeq \mathcal{C}$. Further, working in a similar manner as in part (b), one can show that $\mathcal{D} = \left\langle \underset{1\leq i\leq \ell}{\text{lclm}} \left[\frac{x^{m_i}-\lambda_i}{\text{gcld}(b_{1,i}(x), x^{m_i}-\lambda_i)} \right] \right\rangle_L$. From this, part (c) follows.

(d) To prove this, we will first show that $H_1(x), H_2(x), \cdots, H_\ell(x) \in \mathcal{C}^{\perp_k}$, i.e., $(H_j(x), b_\varsigma(x))_k = 0$ for $1 \leq j \leq \ell$ and $1 \leq \varsigma \leq \varrho$.

To do this, for $1 \leq j \leq \ell$, we consider $\{b_\varsigma(x), H_j(x)\}_k = \lambda_j \left(\frac{x^m-1}{x^{m_j}-\lambda_j} \right) b_{\varsigma,j}(x) \mathcal{S}_k^{(j)} \Big(\mathcal{T}_k^{(j)} \left(\frac{x^{m_j}-\lambda_j}{w_j(x)} \right) \Big) = \lambda_j \left(\frac{x^m-1}{x^{m_j}-\lambda_j} \right) b_{\varsigma,j}(x) \left(\frac{x^{m_j}-\lambda_j}{w_j(x)} \right)$, as $\mathcal{S}_k^{(j)} \circ \mathcal{T}_k^{(j)}$ is the identity map on V_j. Further, by (8.12), we see that $b_{\varsigma,j}(x) \left(\frac{x^{m_j}-\lambda_j}{w_j(x)} \right) = \alpha_{\varsigma,j}(x)(x^{m_j} - \lambda_j)$ for each j. From this and using the fact that $x^{m_j} - \lambda_j \in Z(\mathcal{R})$, we get $\{b_\varsigma(x), H_j(x)\}_k = \lambda_j \left(\frac{x^m-1}{x^{m_j}-\lambda_j} \right) \alpha_{\varsigma,j}(x)(x^{m_j} - \lambda_j) = \lambda_j(x^m - 1)\alpha_{\varsigma,j}(x) = 0$ in $\frac{\mathcal{R}}{\langle x^m-1 \rangle}$ for each j and ς. Now by Lemma 8.5.4(b), we get $(H_j(x), b_\varsigma(x))_k = 0$ for each j and ς. This implies that $H_1(x), H_2(x), \cdots, H_\ell(x) \in \mathcal{C}^{\perp_k}$, which further implies that

$$\langle H_1(x), H_2(x), \cdots, H_\ell(x) \rangle_L \subseteq \mathcal{C}^{\perp_k}. \tag{8.19}$$

On the other hand, let $a(x) = (a_1(x), a_2(x), \cdots, a_\ell(x)) \in \mathcal{C}^{\perp_k}$, i.e., $(a(x), b_\varsigma(x))_k = 0$ in $\frac{\mathcal{R}}{\langle x^m-1 \rangle}$ for $1 \leq \varsigma \leq \varrho$. From this and by Lemma 8.5.4(b), we get $\{b_\varsigma(x), a(x)\}_k = \sum_{i=1}^{\ell} \lambda_i \left(\frac{x^m-1}{x^{m_i}-\lambda_i} \right) b_{\varsigma,i}(x) \mathcal{S}_k^{(i)}(a_i(x)) = 0$ in $\frac{\mathcal{R}}{\langle x^m-1 \rangle}$ for each ς. Further, one can observe that

$$\mathcal{S}_k^{(i)}(a_i(x)) = x^{-\deg\, a_i(x)} \mathscr{T}_{r-k}(a_i(x)) = (\lambda_i^{-1} x^{m_i-1})^{\deg\, a_i(x)} \mathscr{T}_{r-k}(a_i(x)) \text{ in } V_i.$$

Let us denote $f_i(x) = (\lambda_i^{-1} x^{m_i-1})^{\deg\, a_i(x)} \mathscr{T}_{r-k}(a_i(x))$ for $1 \leq i \leq \ell$. This implies that $x^m - 1$ divides $\sum_{i=1}^{\ell} \lambda_i \left(\frac{x^m-1}{x^{m_i}-\lambda_i} \right) b_{\varsigma,i}(x) f_i(x)$ in $\mathcal{R}$, which further implies that $x^{m_j} - \lambda_j$ divides $\sum_{i=1}^{\ell} \lambda_i \left(\frac{x^m-1}{x^{m_i}-\lambda_i} \right) b_{\varsigma,i}(x) f_i(x)$ in $\mathcal{R}$ for $1 \leq j \leq \ell$ and $1 \leq \varsigma \leq \varrho$. From this and using the fact that $x^{m_1} - \lambda_1, x^{m_2} - \lambda_2, \cdots, x^{m_\ell} - \lambda_\ell$ are pairwise

coprime in $\mathcal{R}$, we see that $x^{m_j}-\lambda_j$ divides $\lambda_j\left(\frac{x^m-1}{x^{m_j}-\lambda_j}\right)b_{\varsigma,j}(x)f_j(x)$ for each ς and j. As $\gcd(m,q)=1$, we note that $\gcd\left(\frac{x^m-1}{x^{m_j}-\lambda_j}, x^{m_j}-\lambda_j\right)=1$ in $Z(\mathcal{R})$ for each j. From this, it follows that $x^{m_j}-\lambda_j$ divides $b_{\varsigma,j}(x)f_j(x)$ for each ς and j. Now by (8.11), we see that $x^{m_j}-\lambda_j$ divides $\sum_{\varsigma=1}^{\varrho} A_{\varsigma,j}(x)b_{\varsigma,j}f_j(x)+A_{\varsigma+1,j}(x)(x^{m_j}-\lambda_j)f_j(x) = w_j(x)f_j(x)$ for each j. This implies that $w_j(x)f_j(x) = (x^{m_j}-\lambda_j)A_j(x)$ for some $A_j(x)\in\mathcal{R}$, which further implies that $f_j(x)=\left(\frac{x^{m_j}-\lambda_j}{w_j(x)}\right)A_j(x)$ in $\mathcal{R}$ and hence in V_j. From this and using the fact that $\mathcal{T}_k^{(j)}\circ\mathcal{S}_k^{(j)}$ is the identity map on V_j', we get $a_j(x)=\mathcal{T}_k^{(j)}(A_j(x))\mathcal{T}_k^{(j)}\left(\frac{x^{m_j}-\lambda_j}{w_j(x)}\right)$ in V_j'. If $\deg A_j(x)=t_j$ for $1\le j\le \ell$, then we can write $a(x)=\lambda_1^{t_1p^k}x^{t_1(m_1-1)}\mathscr{T}_k(A_1(x))H_1(x)+\lambda_2^{t_2p^k}x^{t_2(m_2-1)}\mathscr{T}_k(A_2(x))H_2(x)+\cdots+\lambda_\ell^{t_\ell p^k}x^{t_\ell(m_\ell-1)}\mathscr{T}_k(A_\ell(x))H_\ell(x)$, which implies that

$$\mathcal{C}^{\perp_k}\subseteq\langle H_1(x),H_2(x),\cdots,H_\ell(x)\rangle_L. \tag{8.20}$$

Now by (8.19) and (8.20), part (d) follows immediately.

(e) For $1\le i\le\ell$, if π_i is the projection of V onto V_i, then $\pi_i(\mathcal{C})$ is a skew λ_i-constacyclic code of length m_i over $\mathbb{F}_q$ having the generator polynomial $w_i(x)$. Further, as η_i is the maximum number of consecutive exponents of right zeros of $w_i(x)$, working as in Theorem 4 of Bhaintwal [13], we obtain $d_{\min}(\pi_i(\mathcal{C}))\ge\eta_i+1$ for each i. Next we observe that if the ith block $c_i\in\mathbb{F}_q^{m_i}$ of a codeword $c=(c_1,c_2,\cdots,c_\ell)\in\mathcal{C}$ is non-zero, then the Hamming weight $w_H(c_i)$ of c_i satisfies $w_H(c_i)\ge\eta_i+1$. This implies that $w_H(c)\ge\min\limits_{1\le i\le\ell}(\eta_i+1)$ for each $c(\neq 0)\in\mathcal{C}$. From this, we obtain the desired result.

(f) For $1\le i\le\ell$, working as in part (e), we obtain $d_{\min}(\pi_i(\mathcal{C}))\ge\eta_i+1$. Now working in a similar manner as in Theorem 4.3 of Gao et al. [48], the desired result follows immediately.

□

In the following example, we show that Theorem 8.6.2(c) does not hold for a

ϱ-generator skew Λ-MT code of length n over $\mathbb{F}_q$ when $\varrho \geq 2$.

Example 8.6.2. *Let $q = 2^3, m_1 = m_2 = 3$ and $\Lambda = (1, 1)$. Let σ be an automorphism of $\mathbb{F}_{2^3}$, defined as $\sigma(b) = b^4$ for all $b \in \mathbb{F}_{2^3}$. Note that $\mathbb{F}_{2^3}^{\sigma} = \mathbb{F}_2$ and $O(\sigma) = 3$. Further, we have $V = V_1 \times V_2 = \frac{\mathcal{R}}{\langle x^3-1\rangle} \times \frac{\mathcal{R}}{\langle x^3-1\rangle}$. Let $\mathcal{C}(\subseteq V)$ be a skew Λ-MT code of length 6 over $\mathbb{F}_{2^3}$ with the generating set $\{(x^2 + x + 1, 1), (x^2, x + 1)\}$. Here we observe that $dim_{\mathbb{F}_{2^3}}\mathcal{C} = 6$. Now by applying the left division algorithm, we get $A_1(x) = gcld(x^2 + x + 1, x^2, x^3 - 1) = 1$ and $A_2(x) = gcld(x + 1, 1, x^3 - 1) = 1$, which further implies that $H(x) = lclm\,[x^3 - 1, x^3 - 1] = x^3 - 1$. From this, we get deg $H(x) = 3 \neq dim_{\mathbb{F}_{2^3}}\mathcal{C}$.*

In [39], many linear codes with best known and optimal parameters $[n, k, d_{\min}]$ have been listed over $\mathbb{F}_q$ when $2 \leq q \leq 9$. Here also, by using the Magma Computational Algebra System, we obtain linear codes with best known and optimal parameters $[n, k, d_{\min}]$ over $\mathbb{F}_q$ from 1-generator skew Λ-MT codes with the generating set $\{(b_1, b_2, \cdots, b_\ell)\}$, which are listed in Tables 8.1 and 8.2, respectively. In Tables 8.1 and 8.2, a is a primitive element of $\mathbb{F}_q$, $\sigma = \sigma_1$ is the Frobenius automorphism of $\mathbb{F}_q$, and the element $a_0 + a_1x + a_2x^2 + \cdots + a_{m_i-1}x^{m_i-1} \in V_i$ is represented by the sequence $a_0a_1a_2 \cdots a_{m_i-1}$ for $1 \leq i \leq \ell$.

q	$(m_1, m_2, \cdots, m_\ell)$	Λ	$(b_1, b_2, \cdots, b_\ell)$	$[n, k, d_{\min}]$
8	$(9, 9, 3)$	$(1, 1, 1)$	$b_1 = a^4a^2a^6a1a^5a^2a^2a$, $b_2 = 0a^4a^4a^2a^3a^5aa^40$, $b_3 = a^3aa^6$	$[21, 9, 10]$
8	$(15, 15, 3)$	$(1, 1, 1)$	$b_1 = a^2a^2a^210aa^5a^4a^6a^6a^31aa^5$, $b_2 = a^5a11a^3a^4aa^5a^2a^3a^5aa^510$, $b_3 = a^6a^5a^5$	$[33, 15, 13]$
8	$(21, 21, 3)$	$(1, 1, 1)$	$b_1 = aa^5a^5a^60a^5a^6aa^6aa^410aa^2a^3a^31a^200$, $b_2 = 0a^6a^30a^50a^61aa^40a^6a^3a^3a^3a^4a^20a0a$, $b_3 = aa^3a^4$	$[45, 21, 16]$
9	$(10, 10, 2)$	$(1, 1, 1)$	$b_1 = a^212a0aa^611a^3$, $b_2 = a^2a^6aa^3a^6a^3a^72a^3a^5$, $b_3 = a^60$	$[22, 10, 10]$
9	$(16, 8)$	$(2, 2)$	$b_1 = 222a^32a^5a^7210a2012a$, $b_2 = a2a^5a^5a^62a^72$	$[24, 16, 6]$
9	$(20, 10)$	$(1, 1)$	$b_1 = a^7a1a^6a^22a^220a^6a^2a^511a^21a^3a^712$, $b_2 = 2a12aa2a^3a^5a^3$	$[30, 20, 7]$
9	$(16, 16, 2)$	$(1, 1, 1)$	$b_1 = a^62a^30a^5a^7a0a^7a^2002a^7a^5a$, $b_2 = a^22122a^300a^52a^5a^2a^3a^20a$, $b_3 = a^3a^2$	$[34, 16, 13]$
9	$(22, 22, 2)$	$(1, 1, 1)$	$b_1 = a^520a^5a^32a^61220a^30a^3021a^5a^20a^6a^3$, $b_2 = 1a^7a00a^2a^72a^6a^6a^3a^22a^5a^5a^3a^5a^602$ $a^30, b_3 = 20$	$[46, 22, 16]$
9	$(22, 22, 2)$	$(2, 2, 2)$	$b_1 = 0aa^71a^62a^310a^3a^71a^200a2a^7a^21aa^3$, $b_2 = a^5aa^601a1a12a^3a^5a^6a^72a^7a^3101a^52$, $b_3 = a^3a$	$[46, 22, 16]$

Table 8.1: *Linear codes with best known parameters $[n, k, d_{\min}]$ over $\mathbb{F}_q$ obtained as 1-generator skew Λ-MT codes

q	(m_1, m_2)	Λ	$(b_1, b_2, \cdots, b_\ell)$	$[n, k, d_{\min}]$
8	$(9, 9)$	$(1, 1)$	$b_1 = aa^61a1aa^41a^5, b_2 = a0a0a^20aa^20$	$[18, 9, 8]$
9	$(16, 4)$	$(2, 2)$	$b_1 = a^31a^3a^5aa^6a^3a^2a^6a^7aa^6a^7a^5a^3a^5, b_2 = a^2a^2a^3a^2$	$[20, 16, 4]$
9	$(32, 2)$	$(1, 1)$	$b_1 = a^5aa^3a^511a^51aa^52a^3a^60022a21a02222a^5a^6a^6a^21a^2$, $b_2 = a^7a^6$	$[34, 32, 2]$
9	$(46, 2)$	$(2, 2)$	$b_1 = a^5a^5a^3020a^6a^2a^7a10a^3a^21a^3a1aa^2210a^20aa^2a^50a0$ $1a^5a^6a^3a^7202a^6a^2a^3a^7a^3a^6a^5, b_2 = 1a$	$[48, 46, 2]$
9	$(50, 2)$	$(2, 2)$	$b_1 = 1a^6a^7a^6a^6a^52a^6211a1a^2a^7a^2a^2a^5aa^2aaa0a^6a^5a^6a^5$ $a^5a^5a^3aa^2a^7a^62a^5a^7aa^70a0a^31a^5a^3a^300, b_2 = 1a^5$	$[52, 50, 2]$

Table 8.2: *Linear codes with optimal parameters $[n, k, d_{\min}]$ over $\mathbb{F}_q$ obtained as 1-generator skew Λ-MT codes

9

Conclusion and future work

9.1 Introduction

Nowadays error-correcting codes are widely used in communication systems, returning pictures from deep space, designing registration numbers, and storage of data in memory systems. An important family of error-correcting codes is that of linear codes, which contains many well-known codes such as Hamming codes, Hadamard codes, cyclic codes and quasi-cyclic codes. In a recent work, a new family of linear codes, *viz.* multi-twisted (MT) codes over $\mathbb{F}_q$ with block lengths coprime to q, has been introduced and studied by Aydin and Halilović [5]. These codes are generalizations of well-known classes of linear codes (such as constacyclic

codes and generalized quasi-cyclic codes) having rich algebraic structures and containing record-breaker codes. They obtained subcodes of MT codes with best-known parameters $[33, 12, 12]$ over $\mathbb{F}_3$, $[53, 18, 21]$ over $\mathbb{F}_5$, $[23, 7, 13]$ over $\mathbb{F}_7$ and optimal parameters $[54, 4, 44]$ over $\mathbb{F}_7$, and proved that the code parameters $[53, 18, 21]$ over $\mathbb{F}_5$ and $[33, 12, 12]$ over $\mathbb{F}_3$ can not be attained by constacyclic and quasi-cyclic codes. This suggests that the family of MT codes over finite fields is more promising to find codes with better parameters than the current best known linear codes. This inspired us to further study MT codes over finite fields.

9.2 Conclusion

Let $\mathbb{F}_q$ denote the finite field of order q. Let ℓ be a positive integer, and let $m_1, m_2, \cdots, m_\ell$ be positive integers. Let $n = m_1 + m_2 + \cdots + m_\ell$, and let $\Lambda = (\lambda_1, \lambda_2, \cdots, \lambda_\ell)$, where $\lambda_1, \lambda_2, \cdots, \lambda_\ell$ are non-zero elements of $\mathbb{F}_q$. Below we summarize some of the main results derived in the thesis.

In this thesis, algebraic structures of all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ and their dual codes with respect to Euclidean and Hermitian inner products are studied, where $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$. Necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) Euclidean self-dual, (ii) Euclidean self-orthogonal, (iii) Euclidean LCD, (iv) Hermitian self-dual, (v) Hermitian self-orthogonal and (vi) Hermitian LCD are derived. Some sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is either Euclidean LCD or Hermitian LCD are also derived. Besides this, enumeration formulae for all Euclidean and Hermitian self-dual and self-orthogonal Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are provided. All Euclidean and Hermitian LCD Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are also

enumerated when $\lambda_i \in \{1, -1\}$ for $1 \leq i \leq \ell$. These enumeration formulae are useful in the determination of complete lists of inequivalent Euclidean and Hermitian self-dual, self-orthogonal and LCD Λ-MT codes. The parity-check polynomial of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is explicitly determined and a BCH type lower bound on their minimum Hamming distances is also derived. Generating sets of Euclidean and Hermitian dual codes of some Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are expressed in terms of generating sets of the corresponding Λ-MT codes. Apart from this, a trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is provided by viewing these codes as direct sums of certain concatenated codes. Another lower bound on their minimum Hamming distances is obtained by using their multilevel concatenated structure. All non-zero Hamming weights of codewords of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with at most two non-zero constituents are determined. As applications, Hamming weight distributions of several classes of few weight Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are also determined. Among these classes of Λ-MT codes, two classes of optimal equidistant Λ-MT codes over $\mathbb{F}_q$ meeting both Griesmer and Plotkin bounds and three other classes of few weight Λ-MT codes that are useful in constructing secret sharing schemes with nice access structures are identified.

The family of MT codes is further extended and algebraic structures of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are studied, where the block lengths $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers, not necessarily coprime to q. Their dual codes with respect to the Galois inner product are studied, and necessary and sufficient conditions under which a Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD are also derived. A trace description for all Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ is provided

by using the generalized discrete Fourier transform (GDFT), which gives rise to a method to construct these codes. Necessary and sufficient conditions under which a Euclidean self-dual Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_{2^r}$ is a Type II code are derived when $\lambda_i = 1$ and $m_i = 2^a n_i$ for $1 \leq i \leq \ell$, where $n_1, n_2, \cdots, n_\ell$ are odd positive integers satisfying $n_1 \equiv n_2 \equiv \cdots \equiv n_\ell \pmod 4$. It is also shown that each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ has a unique normalized generating set. With the help of a normalized generating set, the dimension and the corresponding generating set of the Galois dual code of each Λ-MT code of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are explicitly determined. Besides this, several linear codes with best-known and optimal parameters from 1-generator Λ-MT codes over $\mathbb{F}_q$ are obtained, where $2 \leq q \leq 7$. It is worth mentioning that these code parameters can not be attained by any of their subclasses (such as constacyclic and quasi-twisted codes) containing record breaker codes. This shows that this generalized family of MT codes over finite fields is more promising to find codes with better parameters than the current best-known codes. Moreover, explicit Hamming weights of all non-zero codewords of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ are determined, where $m_1, m_2, \cdots, m_\ell$ are arbitrary positive integers, not necessarily coprime to q. Using these results, explicit Hamming weight distributions of several classes of Λ-MT codes of block lengths $(m_1, m_2, \cdots, m_\ell)$ and length n over $\mathbb{F}_q$ with a few weights are determined. Among these classes of few weight Λ-MT codes, two classes of optimal equidistant Λ-MT codes that attain the Griesmer as well as Plotkin bounds are obtained. Three other classes of Λ-MT codes of length n over $\mathbb{F}_q$ that are useful in constructing secret sharing schemes with nice access structures are also identified.

Finally, skew analogues of MT codes over finite fields, *viz.* skew multi-twisted (MT) codes, are studied. These codes are linear codes and are generalizations of MT codes. Algebraic structures of these codes and their Galois duals are thoroughly

investigated. Necessary and sufficient conditions under which a skew MT code is (i) Galois self-dual, (ii) Galois self-orthogonal and (iii) Galois LCD are also derived. A method to construct skew MT codes is also provided by viewing these codes as direct sums of certain concatenated codes. A generator theory for these codes is also developed, and two lower bounds on their minimum Hamming distances are obtained. Many linear codes with best known and optimal parameters are obtained from 1-generator skew MT codes over $\mathbb{F}_8$ and $\mathbb{F}_9$.

9.3 Future work

It would be interesting to study MT codes over chain rings and to determine their Hamming weight distributions. Another interesting problem would be to further extend the class of MT codes over finite chain rings to skew MT codes over chain rings.

Bibliography

[1] Ashikhmin, A. and Barg, A.: Minimal vectors in linear codes, *IEEE Trans. Inf. Theory* 44 (5), pp. 2010-2017, 1998.

[2] Ashikhmin, A., Barg, A., Cohen, G. and Huguet, L.: Variations on minimal codewords in linear codes, Lecture Notes in Computer Science 948, AAECC-11, Springer-Verlag, Berlin, pp. 96-105, (1995).

[3] Abualrub, T., Ghrayeb, A., Aydin, N. and Siap, I.: On the construction of skew quasi-cyclic codes, *IEEE Trans. Inf. Theory* 56(5), pp. 183-195, 2010.

[4] Abualrub, T., Ezerman, F. M., Seneviratne, P. and Solé, P.: Skew generalized quasi-cyclic codes, *TWMS J. Pure Appl. Math.* 9(2), pp. 123-134, 2018.

[5] Aydin, N. and Haliović, A.: A generalization of quasi-twisted codes: Multi-twisted codes, *Finite Fields Appl.* 45, pp. 96-106, 2017.

[6] Aydin, N., Connolly, N., Grassl, M.: Some results on the structure of consta-cyclic codes and new linear codes over GF(7) from quasi-twisted codes, *Adv. Math. Commun.* 11(1), pp. 245-258, 2017.

[7] Aydin, N., Connolly, N., Muphree, J.: New binary linear codes from quasi-cyclic codes and an augmentation algorithm, *Appl. Algebra Eng. Commun. Comput.* 28, pp. 339-350, 2017.

[8] Aydin, N., Siap, I., Ray-Chaudhuri, D.K.: The structure of 1-generator quasi-twisted codes and new linear codes, *Des. Codes Cryptogr.* 23(3), pp. 313-326, 2001.

[9] Bae, S., Kang, P. L. and Li, C.: On normalized generating sets for GQC codes over $\mathbb{Z}_2$, *Finite Fields Appl.* 45, pp. 285-300, 2017.

[10] Berlekamp, E.R.: *Algebraic coding theory*, McGraw -Hill Book Company, New York, 1968.

[11] Berndt, B. C., Evans, R. J. and Williams, K. S.: *Gauss and Jacobi sums*, John Wiley & Sons Inc., New York, 1997.

[12] Betsumiya, K.: The Type II property for self-dual codes over finite fields of characteristic two, preprint, 2001.

[13] Bhaintwal, M.: Skew quasi-cyclic codes over Galois rings, *Des. Codes and Cryptogr.* 62, pp. 85-101, 2012.

[14] Blahut, R. E.: *Algebraic codes for data transmission*, Cambridge University Press, 2003.

[15] Bonisoli, A.: Every equidistant linear code is a sequence of dual Hamming codes, *Ars Combin.* 18, pp. 181186, 1984.

[16] Boucher, D., Gaborit, P., Geiselmann, W. and Ulmer, F.: Key exchange and encryption schemes based on non-commutative skew polynomials, *PQCrypto* 6061, pp. 126-141, 2010.

[17] Boucher, D., Geiselmann, W. and Ulmer, F.: Skew cyclic codes, *Appl. Alg. Eng. Commun. and Comput.* 18, pp. 379-389, 2007.

[18] Boucher, D. and Ulmer, F.: Coding with skew polynomial rings, *J. Symb. Comput.* 44, pp. 1644-1656, 2009.

[19] Carlet, C., Ding, C. and Yuan, J.: Linear codes from highly nonlinear functions and their secret sharing schemes, *IEEE Trans. Inf. Theory* 51 (6), pp. 2089-2102, 2005.

[20] Calderbank, A. R. and Goethals, J. M.: Three-weight codes and association schemes, *Philips J. Res.* 39, pp. 143-152, 1984.

[21] Calderbank, R. and Kantor, W. M.: The geometry of two-weight codes, *Bull. Lond. Math. Soc.* 18(2), pp. 97-122, 1986.

[22] Cohen, G. D., Mesnager, S. and Patey, A.: On minimal and quasi-minimal linear codes, Lecture Notes in Computer Science 8308, IMACC 2013, Springer, Heidelberg, pp. 85-98, 2013.

[23] Ding, K. and Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Trans. Inf. Theory* 61(11), pp. 5835-5842, 2015.

[24] Daraiseh, A. G. A. and Baum, C. W.: Decoder error and failure probabilities for Reed-Solomon codes: Decodable vectors method, *IEEE Trans. Communications* 46(7), pp. 857-859, 1998.

[25] Daskalov, R. and Hristov, P.: Some new quasi-twisted ternary linear codes, *J. Algebra Comb. Discret. Struct. Appl.* 2(3), pp. 211-216, 2016.

[26] Daskalov, R. and Hristov, P.: New binary one-generator QC codes, *IEEE Trans. Inf. Theory* 49(11), pp. 3001-3005, 2003.

[27] Daskalov, R. and Hristov, P.: New quasi-twisted degenerate ternary linear codes, *IEEE Trans. Inf. Theory* 49(9), pp. 2259-2263, 2003.

[28] Ding, C.: The weight distribution of some irreducible cyclic codes, *IEEE Trans. Inf. Theory* 55(3), pp. 955-960, 2009.

[29] Ding, C. and Wang, X.: A coding theory construction of new systematic authentication codes, *Theoretical Computer Science* 330(1), pp. 81-99, 2005.

[30] Ding, K. and Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing, *IEEE Trans. Inf. Theory* 61(11), pp. 5835-5842, 2015.

[31] Dinh, H.Q., Nguyen, B.T. and Sriboonchitta, S.: Skew constacyclic codes over finite fields and finite chain rings, *Mathematical Problems in Engineering* 2016, Article ID 3965789, 17 Pages, 2016.

[32] Dinh, H.Q.: On repeated-root constacyclic codes of length $4p^s$, *Asian Eur. J. Math. 6*, 1350020, 2013.

[33] Dinh, H. Q, Li, C. and Yue, Q.: Recent progress on weight distributions of cyclic codes over finite fields, *J. Algebra Comb. Discrete Appl.* 2(1), pp. 39-63, 2014.

[34] Esmaeili, M. and Yari, S.: Generalized quasi-cyclic codes: structural properties and code construction, *Appl. Algebra Eng. Commun. Comput.* 20(2), pp. 159-173, 2009.

[35] Etzion, T. and Storme, L.: Galois geometries and coding theory, *Des. Codes Cryptogr.* 78, pp. 311-350, 2016.

[36] Fan, Y. and Zhang, L.: Galois self-dual constacyclic codes, *Des. Codes Cryptogr.* 84, pp. 473-492, 2017.

[37] Gaborit, P., Pless, V., Solé, P. and Atkin, O.: Type II codes over $\mathbb{F}_4$, *Finite Fields Appl.* 8, pp. 171-183, 2002.

[38] Gao, J., Shen, L. and Fang-Wei, P.: A Chinese remainder theorem approach to skew generalized quasi-cyclic codes over finite fields , *Cryptogr. Commun.* 8, pp. 51-66, 2016.

[39] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, accessed on May 2020.

[40] Grove, L. C.: *Classical Groups and Geometric Algebra*, American Mathematical Society, Providence, Rhode Island, 2008.

[41] Güneri, C., Özbudak, F., Özkaya, B., Sacikara, E., Sepasdar, Z., Sole, P.: Structure and performance of generalized quasi-cyclic codes, *Finite Fields Appl.* 47, pp. 183-202, 2017.

[42] Heng, Z. and Yue, Q.: Several classes of cyclic codes with either optimal three weights or a few weights, *IEEE Trans. Inf. Theory* 62(8), pp. 4501-4513, 2016.

[43] Heng, Z., Ding, C. and Zhou, Z.: Minimal linear codes over finite fields, *Finite Fields Appl.* 54, pp. 176-196, 2018.

[44] Huffman, W. C. and Pless, V.: *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[45] Huffman, W. C.: Cyclic $\mathbb{F}_q$-linear $\mathbb{F}_{q^t}$-codes, *Int. J. Inform. Coding Theory* 1(3), pp. 249-284, 2010.

[46] Jacobson, N.: *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996.

[47] Jia, Y.: On quasi-twisted codes over finite fields, *Finite Fields Appl.* 18, pp. 237-257, 2012.

[48] Jian, G., Lin, Z. and Feng, R.: Two-weight and three-weight linear codes based on Weil sums, *Finite Fields Appl.* 57, pp. 92-107, 2019.

[49] Kasami, T.: A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2, *IEEE Trans. Inf. Theory* 20(5), pp. 679, 1974.

[50] Li, F., Yue, Q. and Liu, F.: The weight distribution of a class of cyclic codes containing a subclass with optimal parameters, *Finite Fields Appl.* 45, pp. 183-202, 2017.

[51] Lidl, R. and Niederreiter, H.: *Finite fields*, Cambridge University Press, 1997.

[52] Ling, S., Niederreiter, H. and Solé, P.: On the algebraic structure of quasi-cyclic codes IV: Repeated roots, *Des. Codes Cryptogr.* 38, pp. 337-361, 2006.

[53] Ling, S. and Solé, P.: On the algebraic structure of quasi-cyclic codes I: Finite fields, *IEEE Trans. Inf. Theory* 47(7), pp. 2751-2760, 2001.

[54] Li, Z., Sun, J. and Li, J.: A novel secret sharing scheme based on minimal linear codes, *Wuhan Univ. J. Natural Sci.* 18, pp. 407-412, 2013.

[55] Ling, S. and Solé, P.: On the algebraic structure of quasi-cyclic codes III: Generator theory, *IEEE Trans. Inf. Theory* 51(7), pp. 2692-2700, 2005.

[56] Luo, J. and Feng, K.: On the weight distributions of two classes of cyclic codes, *IEEE Trans. Inf. Theory* 54(12), pp. 5332-5344, 2008.

[57] MacWilliams, F.J. and Sloane, N.J.A.: *The theory of error-correcting codes*, North-Holland, 1977.

[58] MacWilliams, F. J. and Seery, J.: The weight distributions of some minimal cyclic codes, *IEEE Trans. Inf. Theory* 27(6), pp. 796-806, 1981.

[59] Massey, J. L.: Minimal codewords and secret sharing, Proc. 6th Joint SwedishRussian Int. Workshop on Info. Theory, pp. 276-279, 1993.

[60] Mesnager, S. and Sinak, A.: Several classes of minimal linear codes with few weights from weakly regular Plateaued functions, *IEEE Trans. Inf. Theory* 66(4), pp. 2296-2310, 2020.

[61] McDonald, B.R.: *Finite rings with identity*, Marcel Dekker press, New York, 1974.

[62] Morelos-Zaragoza, R. H.: *The art of error correcting coding*, John Wiley & Sons, 2006.

[63] Ore, O.: Theory of non-commutative polynomials, *Ann. Math.* 34, pp. 480-508, 1933.

[64] Patanker, N. and Singh, S. K.: Weight distribution of a subclass of $\mathbb{Z}_2$-double cyclic codes, *Finite Fields Appl.* 57, pp. 287-308, 2019.

[65] Pless, V.: On the uniqueness of Golay codes, *J. Combin. Theory* 5, pp. 215-228, 1968.

[66] Prange, E.: Cyclic error-correcting codes in two symbols, *Air force Cambridge research center*, pp. 103, 1957.

[67] Raviv, N. and Etzion, T.: Distributed storage systems based on equidistant subspace codes, *Proc. IEEE International Symposium on Information Theory*, Hong Kong, China, pp. 1462-1466, June 2015.

[68] Saleh, A. and Easmaeili, M.: On complementary dual quasi-twisted codes, *J. Appl. Math. Comput.* 56, pp. 115-129, 2018.

[69] Sharma, A., Chauhan, V. and Singh, H.: Multi-twisted codes over finite fields and their dual codes, *Finite Fields Appl.* 51, pp. 270-297, 2018.

[70] Sharma, A. and Chauhan, V.: Skew multi-twisted codes over finite fields and their Galois dual codes, *Finite Fields Appl.* 59, pp. 297-334, 2019.

[71] Sharma, A. and Kaur, T.: Enumeration formulae for self-dual, self-orthogonal and complementary-dual quasi-cyclic codes over finite fields, *Cryptogr. Commun.* 10, pp. 401-435, 2018.

[72] Sharma, A. and Rani, S.: Trace description and Hamming weights of irreducible constacyclic codes, *Adv. Math. Commun.* 12(1), pp. 123-141, 2018.

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

[74] Smith, D. H., Hughes, L. A. and Perkins, S.: A new table of constant weight codes of length greater than 28, *The Electronic Journal of Combinatorics* 13, 2006.

[75] Solomon, G. and Tilborg, H.C.A.V.: A connection between block codes and convolutional codes, *SIAM J. Appl. Math.* 37(2), pp. 358-369, 1979.

[76] Stinson, D. R. and Rees, G. H. J. V.: The equivalence of certain equidistant binary codes and symmetric bibds, *Combinatorica* 4(4), pp. 357-362, 1984.

[77] Townsend, R.L. and Weldon, E.J., Jr.: Self-orthogonal quasi-cyclic codes, *IEEE Trans. Inf. Theory* 13(2), pp. 183-195, 1967.

[78] Taylor, D.E.: *The geometry of classical groups*, Heldermann-Verlag, 2009.

[79] Weldon, E.J.: Long quasi-cyclic codes are good, *IEEE Trans. Inf. Theory* 16(1), pp. 130, 1970.

[80] Yuan, J. and Ding, C.: Secret sharing schemes from three classes of linear codes, *IEEE Trans. Inf. Theory* 52(1), pp. 206-212, 2006.

[81] Zhang, Y.: A secret sharing scheme via skew polynomials, *Int. Conf. on Comp. Sci. and Appl. (ICCSA),* pp. 33-38, 2010.