



**On Some Special Classes of Additive Codes
Over Finite Fields**

A Ph.D. Thesis

by

**Sandeep Sharma
(PhD18303)**

**Under the Supervision of Prof. Anuradha Sharma
Indraprastha Institute of Information Technology, Delhi
May 2024**



On Some Special Classes of Additive Codes
Over Finite Fields

A Thesis

*Submitted in partial fulfillment of the requirements for the
degree of*

Doctor of Philosophy

by

Sandeep Sharma
(PhD18303)

Department of Mathematics

to the

Indraprastha Institute of Information Technology Delhi
New Delhi, Delhi 110020, India
May 2024

Dedicated to my family

Certificate

This is to certify that the thesis entitled “**On Some Special Classes of Additive Codes Over Finite Fields**” being submitted by “**Mr. Sandeep Sharma**” to the **Indraprastha Institute of Information Technology Delhi**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bonafide research work carried out by him 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.

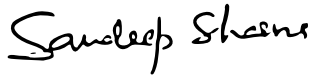
New Delhi
May 2024


Anuradha Sharma
Professor
Department of Mathematics
IIIT-Delhi

Candidate's Declaration

The author hereby declares that the work presented in this thesis entitled “**On Some Special Classes of Additive Codes Over Finite Fields**”, submitted as partial fulfillment for the degree of **Doctor of Philosophy** to Indraprastha Institute of Information Technology, Delhi, has been carried out under the supervision of Prof. Anuradha Sharma.

The work done in this thesis is original and has not been submitted earlier as a whole or in part for a degree or diploma at this or any other Institution or University.



Signature of the candidate

Sandeep Sharma

Date: May 31, 2024

Acknowledgements

With immense gratitude and pleasure, I extend my heartfelt acknowledgment to those who have played a pivotal role in the completion of my Ph.D. journey.

First and foremost, my sincere appreciation goes to my Ph.D. advisor, Prof. Anuradha Sharma. I am deeply grateful for her expertise, cooperation, and persistent encouragement throughout the planning and development of this work. Her availability to discuss my doubts, advice, and guidance has been invaluable. Her mentorship has not only shaped my research but also enriched my growth as a scholar.

I would also like to acknowledge the University Grants Commission (UGC) and IIIT Delhi for providing financial support, which allowed me to focus on my research without financial constraints.

I am also grateful to my doctoral committee members, Dr. Donghoon Chang and Dr. Subhabrata Samajder, for their generous support and encouragement. I also appreciate the expertise and feedback provided by Dr. Shanta Laisharam (Indian Statistical Institute, New Delhi, India), the external examiner during my fellowship enhancement seminar.

I extend my heartfelt gratitude to my friends and research fellows at IIIT-Delhi. Among them, I wish to mention my friend Monika Yadav. Her engaging discussions and the exchange of valuable ideas have been instrumental in enriching my understanding of the concepts explored in this research. My gratitude extends to the supporting staff whose contributions, direct or indirect, facilitated the smooth completion of my work.

I am extremely grateful to my thesis evaluation committee members, Prof. Nuh

Aydin (Kenyon College, Gambier, Ohio, USA), Prof. Yonglin Cao (Shandong University of Technology, Zibo, Shandong, China), and Prof. Ashish Kumar Upadhyay (Banaras Hindu University (BHU), Varanasi, India), for their valuable time and consideration.

I would also like to thank my teachers, Mr. Rashtrapal Yadav, Dr. Avinash Chand Yadav, and Dr. Yogesh Kumar, who consistently motivated and inspired me throughout my journey. Thanks to my senior, Dr. Kamlesh Kumar, and my friends Gitesh, Balram, and Raj Kumar for their timely help and support.

A special mention is reserved for my family members, particularly my parents, Mr. Suresh Sharma and Mrs. Laxmi Devi, whose consistent support has been my pillar of strength. Their encouragement and love have been instrumental in navigating the challenges of this journey. I also thank my siblings for their unwavering belief in me and constant support throughout this challenging path.

To everyone mentioned above, I dedicate this work. Your collective support and encouragement have been crucial to my success story. Thank you for being an integral part of this significant achievement.

New Delhi
May 2024

Sandeep Sharma

Abstract

In this thesis, we define and study a new class of additive codes over finite fields, *viz.* multi-twisted (MT) additive codes, which is a generalization of constacyclic additive codes and an extension of MT (linear) codes introduced by Aydin and Halilović [5]. We study their algebraic structures by writing a canonical form decomposition of these codes using the Chinese Remainder Theorem and provide an enumeration formula for these codes. With the help of their canonical form decomposition, we also provide a trace description for all MT additive codes over finite fields. We further apply probabilistic methods to study the asymptotic properties of the rates and relative Hamming distances of a special subclass of 1-generator MT additive codes. We show that there exists an asymptotically good infinite sequence of MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with rate $\frac{v}{p^\eta \ell t}$ and relative Hamming distance at least δ , where $\ell \geq 1$ and $t \geq 2$ are integers, q is a prime power, $\mathbb{F}_{q^t}$ is the finite field of order q^t , p is an odd prime satisfying $\gcd(p, q) = 1$, $v = \text{ord}_p(q)$ is the multiplicative order of q modulo p , η is the largest positive integer such that $p^\eta \mid (q^v - 1)$ and δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, (here $h_{q^t}(\cdot)$ denotes the q^t -ary entropy function). This shows that the family of MT additive codes over finite fields is asymptotically good. As special cases, we deduce that the families of constacyclic and cyclic additive codes over finite fields are asymptotically good.

By placing ordinary, Hermitian and $*$ trace bilinear forms, we study the dual codes of MT additive codes over finite fields and derive necessary and sufficient conditions under which an MT additive code is (i) self-orthogonal, (ii) self-dual and (iii)

an additive code with complementary dual (or an ACD code). We also derive a necessary and sufficient condition for the existence of a self-dual MT additive code over a finite field and provide enumeration formulae for all self-orthogonal, self-dual and ACD MT additive codes over finite fields with respect to the aforementioned trace bilinear forms. We further employ probabilistic methods and results from groups and geometry to study the asymptotic behavior of the rates and relative Hamming distances of self-orthogonal, self-dual and ACD MT additive codes over finite fields with respect to the aforementioned trace bilinear forms. We establish the existence of asymptotically good infinite sequences of self-orthogonal and ACD MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with relative Hamming distance at least δ and rates $\frac{v}{p^n \ell t}$ and $\frac{2v}{p^n \ell t}$ with respect to the aforementioned trace bilinear forms, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, p is an odd prime coprime to q , $v = \text{ord}_p(q)$ is the multiplicative order of q modulo p , and n is the largest positive integer satisfying $p^n \mid (q^v - 1)$. This shows that self-orthogonal and ACD MT additive codes over finite fields are asymptotically good. As special cases, we deduce that self-orthogonal and ACD constacyclic additive codes over finite fields are asymptotically good. We also establish the existence of asymptotically good infinite sequences of self-dual MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with relative Hamming distance at least δ and rate $\frac{1}{2}$ with respect to the aforementioned trace bilinear forms, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$, p is an odd prime coprime to q such that $v = \text{ord}_p(q)$ is even. As special cases, we deduce that self-dual cyclic and negacyclic additive codes over finite fields are asymptotically good. We also define and study a special class of self-dual MT additive codes over $\mathbb{F}_{q^t}$ with respect to the ordinary trace bilinear form, *viz.* doubly-even self-dual MT additive codes and characterize a special class of these codes in terms of their constituents with the help of their trace description, where q is an even prime power. With the help of this characterization and using probabilistic methods and results from groups and geometry, we further study the asymptotic behaviour of their relative Hamming distances and show that doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ are asymptotically good. As a special case, we also deduce that doubly-even self-dual cyclic additive codes over $\mathbb{F}_{2^t}$ are asymptotically good.

We next define and study a new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, which is a generalization of a special class of MT additive codes over finite fields and an extension of linear QA codes over finite fields. We study the algebraic structures of these codes and their dual codes with respect to ordinary, Hermitian and $*$ trace bilinear forms. We further express these codes as direct sums of additive codes over finite fields and derive necessary and sufficient conditions under which an additive QA code is (i) self-orthogonal, (ii) self-dual and (iii) ACD. We also derive necessary and sufficient conditions for the existence of a self-dual additive QA code over finite fields. Besides this, we obtain explicit enumeration formulae for all self-orthogonal, self-dual and ACD additive QA codes over finite fields. We also list several MDS and almost MDS codes belonging to the family of additive QA codes over finite fields, which shows that additive QA codes over finite fields is a promising class of codes to find codes with good and optimal parameters.

Research Publications

Published Articles:

1. Chauhan, V., Sharma, A., **Sharma, S.** and Yadav, M.: Hamming weight distributions of multi-twisted codes over finite fields, *Des. Codes Cryptogr.* 89(8), pp. 1787–1837, 2021.
2. **Sharma, S.** and Sharma, A.: Multi-twisted additive codes over finite fields, *Beitr. Algebra Geom.* 63(2), pp. 287-320, 2022.
3. **Sharma, S.** and Sharma, A.: Multi-twisted additive codes over finite fields with complementary duals, *Probl. Inf. Transm.* 58(1), pp. 32-57, 2022.
4. **Sharma, S.** and Sharma, A.: Multi-twisted additive codes over finite fields are asymptotically good, *Cryptogr. Commun.* 15(1), pp. 17-33, 2023.
5. **Sharma, S.** and Sharma, A.: Multi-twisted additive self-orthogonal and ACD codes are asymptotically good, *Finite Fields Appl.* 93, Article No. 102319, 2024.

Communicated Articles:

1. **Sharma, S.**, Yadav, M. and Sharma, A.: On additive quasi-Abelian codes over finite fields and their duality properties, under review.
2. **Sharma, S.** and Sharma, A.: On some asymptotically good classes of self-dual multi-twisted additive codes, under review.

Contents

Certificate	i
Candidate's Declaration	iii
Acknowledgements	v
Abstract	vii
Research Publications	xi
List of Symbols	xvii
1 Introduction	1
1.1 Introduction	2
1.2 Multi-twisted additive codes over finite fields and their dual codes . .	6
1.3 Additive quasi-Abelian codes over finite fields and their dual codes . .	9
1.4 Conclusion and future work	10
2 Some Preliminaries	11
2.1 Linear and additive codes over finite fields	11
2.2 Some basic results from groups and geometry	18
2.3 Some basic results from probability theory	29
3 Multi-twisted additive codes over finite fields	31
3.1 Introduction	31
3.2 Multi-twisted additive codes over finite fields	32

3.3	A canonical decomposition of MT additive codes using the Chinese Remainder Theorem	34
3.4	Trace description of MT additive codes	37
3.5	MT additive codes over finite fields are asymptotically good	40
4	Characterization of self-orthogonal, self-dual and ACD multi-twisted additive codes	53
4.1	Introduction	53
4.2	Dual codes of MT additive codes	54
4.3	Canonical decomposition of σ -dual codes of MT additive codes	58
4.4	Self-orthogonal, self-dual and ACD MT additive codes	63
5	Enumeration formulae for σ -self-orthogonal, σ -self-dual and σ -ACD multi-twisted additive codes over finite fields	75
5.1	Introduction	75
5.2	Enumeration of σ -self-orthogonal MT additive codes	76
5.3	Enumeration of σ -self-dual MT additive codes	88
5.4	Enumeration of σ -ACD MT additive codes	96
5.4.1	Determination of the number $\mathfrak{L}_u$ when $u \in \mathcal{J}_1$	98
5.4.2	Determination of the number $\mathfrak{L}_u$ when $u \in \mathcal{J}_2$	117
5.4.3	Determination of the number $\mathfrak{L}_v$ when $e_1 + 1 \leq v \leq e_2$	119
5.4.4	Determination of the number $\mathfrak{L}_w$ when $e_2 + 1 \leq w \leq e_3$	123
6	Self-orthogonal and ACD multi-twisted additive codes are asymptotically good	127
6.1	Introduction	127
6.2	A class of MT additive codes over $\mathbb{F}_{q^t}$	128
6.3	Asymptotically good σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ exist	130
6.3.1	The case $-1 \in Q$	131
6.3.2	The case $-1 \notin Q$ and $\omega = \omega^{-1}$	139
6.3.3	The case $-1 \notin Q$ and $\omega \neq \omega^{-1}$	151

7 Self-dual multi-twisted additive codes are asymptotically good	155
7.1 Introduction	155
7.2 Asymptotically good σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ exist	156
7.3 Doubly-even self-dual multi-twisted additive codes	173
7.4 Doubly-even self-dual multi-twisted additive codes are asymptotically good	178
8 Additive quasi-Abelian codes over finite fields and their dual codes	187
8.1 Introduction	187
8.2 Some preliminaries	188
8.3 Additive quasi-Abelian codes over finite fields and their dual codes	190
8.4 Canonical decompositions of additive H -QA codes over $\mathbb{F}_{q^t}$ and their σ -dual codes	196
8.5 σ -Self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes over $\mathbb{F}_{q^t}$	207
8.6 Enumeration of σ -self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes over finite fields	214
8.6.1 Enumeration formula for σ -self-orthogonal additive H -QA codes	215
8.6.2 Enumeration formula for σ -self-dual additive H -QA codes	224
8.6.3 Enumeration formula for σ -ACD H -QA codes	225
8.7 Determination of the parameters r_1, r_2 and r_3 when H is an arbitrary finite Abelian group	233
8.8 MDS and almost MDS additive H -QA codes	241
9 Conclusion and future work	245
Bibliography	249

List of Symbols

Symbol	Meaning
$ A $	<i>Cardinality</i> of the set A
$\min\{a, b\}$	<i>Minimum</i> of a and b
$\dim_F V$	The <i>dimension</i> of a finite-dimensional vector space V over the field F
$\mathbb{N}$	The set of <i>positive integers</i>
$\gcd(a, b)$	The <i>greatest common divisor</i> of a and b
$\text{lcm}[a, b]$	The <i>least common multiple</i> of a and b
$a \equiv b \pmod{n}$	The integers a and b are congruent modulo a positive integer n
$\nu_2(n)$	The <i>highest power of 2</i> dividing n
$\text{ord}(a)$	The <i>order</i> of the group element a
$\text{ord}_n(a)$	The <i>multiplicative order</i> of the integer a modulo n
$\langle a \rangle$	The <i>cyclic group</i> generated by the element a
$\langle a \rangle_R$	The <i>principal ideal</i> generated by the element a of the ring R
$[\cdot]_q$	The <i>q-binomial coefficient</i>
$\mathbb{F}_q$	The <i>finite field</i> of order q
$\text{Tr}_{q^t, q}$	The <i>trace map</i> from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$

$[\cdot, \cdot] \upharpoonright_{U \times U}$	The <i>restriction</i> of the map $[\cdot, \cdot]$ to $U \times U$
$\lceil \cdot \rceil$	The <i>Ceiling</i> function
$\lfloor \cdot \rfloor$	The <i>Floor</i> function
$d(\mathcal{C})$	The minimum <i>Hamming distance</i> of the code $\mathcal{C}$
$h_q(\cdot)$	The <i>q-ary entropy function</i>
$C_i(q)$	The <i>q-cyclotomic coset</i> containing i

1

Introduction

The objectives of this thesis are

- to define and study a new class of additive codes over finite fields, *viz.* multi-twisted (MT) additive codes over finite fields, which is a generalization of cyclic and constacyclic additive codes and an extension of MT (linear) codes introduced by Aydin and Halilović [5].
- to show that MT additive codes over finite fields are asymptotically good by applying probabilistic methods.
- to study the dual codes of MT additive codes over finite fields and their three special classes such as self-orthogonal, self-dual and additive codes with complementary duals (ACD codes).
- to count all self-orthogonal, self-dual and ACD MT additive codes over finite fields.

- to show that self-orthogonal, self-dual and ACD MT additive codes over finite fields are asymptotically good by applying probabilistic methods and results from groups and geometry.
- to define and study another new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, which is a generalization of a special class of MT additive codes and an extension of linear QA codes introduced by Wasan [67].
- to study dual codes of additive QA codes over finite fields and their three special classes such as self-orthogonal, self-dual and ACD codes.

1.1 Introduction

In 1948, Claude Shannon [54] published a manuscript entitled “A Mathematical Theory of Communication”, where it is shown that there exist encoding and decoding schemes using which reliable communication can be achieved at any rate below the capacity of the channel. This led to the birth of coding theory, which deals with the design and study of such encoding and decoding schemes. Nowadays, encoding schemes are called error-correcting codes, or simply called codes. Error-correcting codes have found various applications in data compression, cryptography, error detection and correction, data transmission and data storage. Linear codes over finite fields constitute the most important and extensively studied family of error-correcting codes, which contains many well-known classes of error-correcting codes such as Hamming codes, Golay codes, BCH codes, Reed-Solomon codes, cyclic codes, and quasi-cyclic codes. Prange [51] introduced and studied cyclic codes over finite fields, which have rich algebraic structures and can be effectively encoded and decoded using shift registers. A natural generalization of cyclic codes is that of constacyclic codes, which are introduced and studied in [10] and have nice algebraic structures. In another direction, Townsend and Weldon [68] generalized cyclic codes over finite fields to quasi-cyclic (QC) codes. Hill and Greenough [30] further generalized QC codes to quasi-twisted (QT) codes. Further, Aydin *et al.* [4] studied the structural properties of QT codes and also obtained a BCH type lower bound

on Hamming distances of 1-generator QT codes. Later, Siap and Kulhan [62] generalized QC codes to generalized quasi-cyclic (GQC) codes and studied 1-generator GQC over finite fields. In a recent work [5], Aydin and Halilović introduced and studied multi-twisted (MT) codes over finite fields, which are generalizations of constacyclic codes, QC codes, QT codes and GQC codes. In the same work, they studied 1-generator MT codes over finite fields. They also presented several methods to construct these codes and obtained several bounds on their Hamming distances. Later, Sharma *et al.* [55, 56] thoroughly investigated the algebraic structures of MT codes over finite fields and their dual codes with respect to the Euclidean and Hermitian sesquilinear forms. They also derived a necessary and sufficient condition for the existence of a self-dual MT code and provided enumeration formulae for all self-orthogonal, self-dual and linear codes with complementary duals (LCD codes) belonging to the family of MT codes over finite fields. They also showed that MT codes over finite fields can be viewed as direct sums of certain concatenated codes, which gives rise to a method to construct these codes. They also derived a lower bound on their Hamming distances using their multilevel concatenated structures. Later, Chauhan *et al.* [18, 19] determined Hamming weight distributions of several classes of MT codes over finite fields. They also identified several classes of codes with a few weights within the family of MT codes.

Linear codes over finite fields are generalized to additive codes. These codes have rich algebraic structures and are useful in constructing quantum error-correcting codes. Calderbank *et al.* [16] first introduced and studied additive codes over the finite field $\mathbb{F}_4$ of order 4. In the same work, they studied their dual codes with respect to the ordinary trace bilinear form and provided methods to construct quantum stabilizer codes from self-orthogonal additive codes over $\mathbb{F}_4$. Subsequently, Bierbrauer and Edel [13] and Rains [52] studied additive codes over arbitrary finite fields. Huffman [32] introduced and studied cyclic additive codes of odd lengths over $\mathbb{F}_4$ by writing a canonical form decomposition for these codes and enumerated all such codes. Besides this, he provided explicit enumeration formulae for all self-orthogonal and self-dual cyclic additive codes over $\mathbb{F}_4$ with respect to the ordinary trace bilinear form. In a subsequent work [33], he extended this work to cyclic additive codes of even lengths over $\mathbb{F}_4$. Later, Huffman [34] generalized this work for cyclic additive

codes of an arbitrary length n over the finite field $\mathbb{F}_{q^t}$, where $t \geq 2$ is an integer, q is a prime power, and n is a positive integer with $\gcd(n, q) = 1$. By placing ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^t}^n$, he studied their dual codes, derived necessary and sufficient conditions for the existence of a self-dual cyclic additive code of length n over $\mathbb{F}_{q^t}$ and provided enumeration formulae for all self-orthogonal and self-dual cyclic additive codes of length n over $\mathbb{F}_{q^t}$. Moreover, when $t = 2$, he explicitly determined the bases of all self-dual and self-orthogonal cyclic additive codes of length n over $\mathbb{F}_{q^2}$ with respect to both ordinary and Hermitian trace bilinear forms on $\mathbb{F}_{q^2}^n$. If p is the characteristic of the finite field $\mathbb{F}_{q^t}$, then for any positive integer $t \geq 2$ satisfying $t \not\equiv 1 \pmod{p}$, Sharma and Kaur [57] introduced a new trace bilinear form on $\mathbb{F}_{q^t}^n$, which is called the $*$ trace bilinear form. They studied the dual codes of cyclic additive codes of length n over $\mathbb{F}_{q^t}$ and provided enumeration formulae for all self-orthogonal and self-dual cyclic additive codes over $\mathbb{F}_{q^t}$ with respect to the $*$ trace bilinear form. In another work, Sharma and Kaur [58] studied cyclic additive codes with complementary duals (or ACD cyclic additive codes) of length n over $\mathbb{F}_{q^t}$ and obtained enumeration formulae for all ACD cyclic additive codes over $\mathbb{F}_{q^t}$ with respect to ordinary, Hermitian and $*$ trace bilinear forms. Cao *et al.* [17] further generalized cyclic additive codes to constacyclic additive codes of length n over $\mathbb{F}_{q^t}$ when t is a prime number and $\gcd(n, q) = 1$. They also studied their dual codes with respect to the ordinary trace bilinear form on $\mathbb{F}_{q^t}^n$. In the same work, they investigated the existence of a self-orthogonal and a self-dual negacyclic additive code of length n over $\mathbb{F}_{q^t}$ and derived necessary and sufficient conditions for a negacyclic additive code of length n over $\mathbb{F}_{q^2}$ to be self-dual or self-orthogonal. Further, for any integer $t \geq 2$ (not necessarily a prime number), Kaur and Sharma [41] developed the theory of constacyclic additive codes over $\mathbb{F}_{q^t}$ by writing a canonical form decomposition for these codes. They also studied their dual codes and provided explicit enumeration formulae for all self-orthogonal, self-dual and ACD constacyclic additive codes over $\mathbb{F}_{q^t}$ with respect to ordinary, Hermitian and $*$ trace bilinear forms on $\mathbb{F}_{q^t}^n$. Recently, Shi *et al.* [60] studied ACD cyclic additive codes of odd length n over $\mathbb{F}_4$ with respect to ordinary and Hermitian trace bilinear forms and characterized subfield subcodes and trace codes of these codes in terms of their generators as binary cyclic codes. Later, Shi *et al.* [61] studied ACD codes of odd

length n over $\mathbb{F}_4$ with respect to ordinary and Hermitian trace bilinear forms and provided methods to construct ACD codes over $\mathbb{F}_4$ from binary codes. This motivated us to extend the class of MT (linear) codes over finite fields to MT additive codes over finite fields.

In a related work, Kabatiansky [40] showed that if q is a primitive root modulo an odd prime p satisfying $q^{p-1} \not\equiv 1 \pmod{p^2}$, then for any integer $a \geq 1$, there exists a cyclic additive code of length p^a over $\mathbb{F}_{q^t}$ with rate $R_k = \frac{k}{t}$ and relative Hamming distance δ_k satisfying $h_q(\delta_k) \geq (1 - R_k)(\frac{p-1}{p})$ for $1 \leq k \leq t - 1$, where $h_q(\cdot)$ denotes the q -ary entropy function. Further, assuming the unresolved Artin's conjecture on primitive roots, he proved that cyclic additive codes of prime power length p^a over $\mathbb{F}_{q^t}$ are asymptotically good, where $p \rightarrow \infty$. However, this asymptotically good class of cyclic additive codes over $\mathbb{F}_{q^t}$ do not satisfy the asymptotic Gilbert-Varshamov (GV) bound, as the relative Hamming distance δ_k satisfies the inequality $h_q(\delta_k) \geq 1 - R_k$ instead of the asymptotic GV bound $h_{q^t}(\delta_k) \geq 1 - R_k$. Recall that the Artin's conjecture on primitive roots states that for an integer a , which is neither a perfect square nor equal to -1 , there are infinitely many primes p for which a is a primitive root modulo p [42]. Hooley [31] provided a conditional proof of this conjecture for an integer a under the assumption that the Riemann Hypothesis holds for the Dedekind-Zeta function of each field $\mathbb{Q}(\sqrt[p]{a})$, where p runs over the set of all primes. Later, Heath-Brown [29] showed that at least one of 2, 3, or 5 is a primitive root modulo infinitely many primes and that there are at most two primes for which the Artin's conjecture fails. However, the Artin's conjecture is still an unresolved problem in general [3, 47]. In fact, the Artin's conjecture is not yet resolved for any specific value of the integer a . Later, by applying the Chebyshev's Theorem on prime numbers, Chepyzhov [21] proved that there exists an infinite sequence of cyclic additive codes of prime lengths $p \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with rate $R_k = \frac{k}{t}$ and relative Hamming distance δ_k satisfying the asymptotic Gilbert-Varshamov bound for $1 \leq k \leq t - 1$. From this, it follows that cyclic additive codes of prime lengths over finite fields are asymptotically good. In a recent work [59], Shi *et al.* established a relation between ω -QT codes of length nt and index t over $\mathbb{F}_q$ and ω -constacyclic additive codes of length n over $\mathbb{F}_{q^t}$, where ω is a non-zero element of $\mathbb{F}_q$. They

further applied Theorem 5.4 of Alahmadi *et al.* [1] to show that the class of ω -constacyclic additive codes of length $n \rightarrow \infty$ over $\mathbb{F}_{q^t}$ is asymptotically good when the polynomial $x^n - \omega \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$. Besides this, they applied Theorem 5.6 of Alahmadi *et al.* [1] to show that the class of cyclic additive codes of prime length $p \rightarrow \infty$ over $\mathbb{F}_{q^t}$ is asymptotically good by assuming the unresolved Artin's conjecture on primitive roots. Therefore, it is a natural question to ask whether MT additive codes and their three special classes such as self-orthogonal, self-dual and ACD MT additive codes over finite fields are asymptotically good. In this thesis, we answer this question in affirmative and show that MT additive codes and their three special classes such as self-orthogonal, self-dual and ACD MT additive codes over finite fields are asymptotically good by employing probabilistic methods and results from groups and geometry.

In this thesis, we define and study two new classes of additive codes over finite fields, *viz.* multi-twisted (MT) additive codes over finite fields and additive quasi-Abelian (QA) codes over finite fields. We also study their dual codes with respect to ordinary, Hermitian and $*$ trace bilinear forms. We now proceed to describe the problems explored in this thesis.

1.2 Multi-twisted additive codes over finite fields and their dual codes

In this thesis, we define and study multi-twisted (MT) additive codes over finite fields and their dual codes with respect to ordinary, Hermitian and $*$ trace bilinear forms. To describe the problems explored in this thesis, we assume, throughout this thesis, that q is a power of the prime number $\mathfrak{p}$, $t \geq 2$ is an integer and $\mathbb{F}_q$ and $\mathbb{F}_{q^t}$ are finite fields of order q and q^t , respectively. Let n, ℓ be positive integers, and let $m_1, m_2, \dots, m_\ell$ be positive integers coprime to q satisfying $n = m_1 + m_2 + \dots + m_\ell$. Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed, where $\omega_1, \omega_2, \dots, \omega_\ell$ are non-zero elements of $\mathbb{F}_q$.

In Chapter 3, we define and study a new class of additive codes over finite fields, *viz.* Ω -multi-twisted (Ω -MT) additive codes, which is a generalization of cyclic and constacyclic additive codes and is an extension of MT (linear) codes over finite fields. We study the algebraic structures of Ω -MT additive codes of length

$n = m_1 + m_2 + \cdots + m_\ell$ and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. We provide a canonical form decomposition for these codes using the Chinese Remainder Theorem. We also provide a trace description for Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with the help of their canonical form decomposition. Further, by employing the probabilistic methods, we study the asymptotic behaviour of the rates and relative Hamming distances of a certain special subclass of 1-generator MT additive codes over finite fields. We also establish the existence of asymptotically good infinite sequences of MT additive codes of prime power block lengths over finite fields. This shows that the class of MT additive codes over finite fields is asymptotically good. As a special case, we deduce that ω -constacyclic additive codes of prime power length n over $\mathbb{F}_{q^t}$ are asymptotically good when the polynomial $x^n - \omega$ is reducible over $\mathbb{F}_q$. We also deduce, as a special case, that cyclic additive codes of prime power lengths over finite fields are asymptotically good without assuming the unresolved Artin's conjecture on primitive roots and without applying Chebyshev's Theorem on prime numbers.

In Chapter 4, we place ordinary, Hermitian and $*$ trace bilinear forms on $\mathbb{F}_{q^t}^n$ and study the dual codes of Ω -MT additive codes of length $n = m_1 + m_2 + \cdots + m_\ell$ and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. We also derive necessary and sufficient conditions under which an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is (i) self-orthogonal, (ii) self-dual and (iii) an additive code with complementary dual (or an ACD code) with respect to the aforementioned trace bilinear forms.

In Chapter 5, we first derive a necessary and sufficient condition for the existence of a self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with respect to ordinary, Hermitian and $*$ trace bilinear forms. We further apply the results derived in Chapter 4 and enumerate all self-orthogonal, self-dual and ACD Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with respect to each of the three above-mentioned trace bilinear forms.

In Chapter 6, we study a special class of 1-generator MT additive codes over finite fields on which our probabilistic methods can work well. By applying probabilistic methods and results from groups and geometry, we study the asymptotic properties of the rates and relative Hamming distances of self-orthogonal and ACD

codes belonging to this special class of MT additive codes over finite fields with respect to ordinary, Hermitian and $*$ trace bilinear forms. We also establish the existence of asymptotically good infinite sequences of self-orthogonal and ACD MT additive codes of prime power block lengths over finite fields. This shows that self-orthogonal and ACD MT additive codes over finite fields are asymptotically good. As a consequence, we deduce that self-orthogonal and ACD constacyclic additive codes over finite fields are asymptotically good.

In Chapter [7](#), we consider a special class of self-dual MT additive codes over finite fields with respect to the ordinary, Hermitian and $*$ trace bilinear forms and study the asymptotic behavior of their relative Hamming distances using probabilistic methods and results from groups and geometry. We further establish the existence of asymptotically good infinite sequences of self-dual MT additive codes of prime power block lengths over finite fields. This shows that self-dual MT additive codes over finite fields are asymptotically good. As a special case, we deduce that self-dual cyclic and negacyclic additive codes over finite fields are asymptotically good. We also define and study a special class of self-dual MT additive codes over finite fields of even characteristic with respect to the ordinary trace bilinear form, *viz.* doubly-even self-dual MT additive codes. We provide a characterization of a special class of doubly-even self-dual MT additive codes in terms of their constituents with the help of their trace description. Besides this, we derive a necessary and sufficient condition for the existence of a doubly-even self-dual MT additive code over $\mathbb{F}_{q^t}$, where q is an even prime power. Finally, we consider a special class of doubly-even self-dual MT additive codes of prime power block lengths over $\mathbb{F}_{2^t}$ on which our probabilistic methods work well and show that there exists an asymptotically good infinite sequence of doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ by using result from groups and geometry. This shows that doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ are asymptotically good. As a consequence, we deduce that doubly-even self-dual cyclic additive codes over $\mathbb{F}_{2^t}$ are asymptotically good.

1.3 Additive quasi-Abelian codes over finite fields and their dual codes

Quasi-abelian (QA) codes over finite fields constitute an important class of linear codes and are generalizations of several well-known classes of linear codes such as Abelian group codes, cyclic codes and QC codes [9, 14, 38, 45]. Wasan [67] first introduced and studied these codes and showed that each QA code can be written as a direct sum of Abelian group codes. Jitman and Ling [38] further studied these codes and gave a structural characterization of H -quasi-Abelian (H -QA) codes over $\mathbb{F}_q$ using the Discrete Fourier Transform, where H is an Abelian group of order m with $\gcd(m, q) = 1$. They also derived necessary and sufficient conditions under which an H -QA code over $\mathbb{F}_q$ is Euclidean self-dual. They further obtained enumeration formulae for all Euclidean self-dual H -QA codes over $\mathbb{F}_q$ in terms of the parameters r_1 , r_2 and r_3 that depend on q and the structure of H . They also obtained explicit values of the parameters r_1 , r_2 and r_3 when H is an elementary p -group, where p is a prime. In a recent work [50], Palines *et al.* obtained an enumeration formula for all Hermitian self-dual H -QA codes over $\mathbb{F}_q$ in terms of the parameters s_1 and s_2 , whose values depend on q and the structure of H . They also obtained explicit values of the parameters s_1 and s_2 when $H \simeq (\mathbb{Z}_{p^k})^s$, where p is a prime and k, s are positive integers. Fan and Lin [24] showed that there exist numerous asymptotically good QA codes over finite fields that attain the Gilbert-Varshamov (GV) bound. Jitman *et al.* [39] characterized all LCD QA codes over finite fields with respect to the Euclidean and Hermitian sesquilinear forms. They also showed that the class of Euclidean LCD QA codes of index 3 over finite fields is asymptotically good. Recently, Zhang and Chen [70] proved that the class of Euclidean self-orthogonal QA codes over finite fields is asymptotically good. Borello *et al.* [14] gave a concatenated decomposition of QA codes over finite fields. With the help of this concatenated structure, they derived a lower bound on the Hamming distances of QA codes and constructed some optimal codes. They also showed that the class of LCD strictly QA codes over finite fields is asymptotically good.

In Chapter 8 we define and study a new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, which is a generalization of a special

class of MT additive codes and is an extension of linear QA codes over finite fields introduced by Wasan [67]. We also study their duality properties with respect to ordinary, Hermitian and $*$ trace bilinear forms. More specifically, let H be an additive Abelian group of order m and $\gcd(m, q) = 1$. We provide canonical decompositions of additive H -QA codes over $\mathbb{F}_{q^t}$ and their dual codes with respect to the aforementioned trace bilinear forms. We also provide necessary and sufficient conditions under which an additive H -QA code over $\mathbb{F}_{q^t}$ is (i) self-orthogonal, (ii) self-dual and (iii) ACD. We also derive a necessary and sufficient condition for the existence of a self-dual additive H -QA code over $\mathbb{F}_{q^t}$. We further obtain explicit enumeration formulae for all self-orthogonal, self-dual and ACD additive H -QA codes over $\mathbb{F}_{q^t}$ in terms of the parameters r_1 , r_2 and r_3 , whose values depend on q and the structure of the group H . We also derive formulae to determine the parameters r_1 , r_2 and r_3 when H is an arbitrary finite Abelian group. With the help of these results, one can obtain explicit enumeration formulae for all self-orthogonal, self-dual and ACD additive H -QA codes over $\mathbb{F}_{q^t}$, which are useful in classifying these three classes of additive codes up to monomial equivalence [35, Sec. 9.6 and 9.7]. We also list several maximum distance separable (MDS) and almost maximum distance separable (almost MDS) codes belonging to the class of 1-generator additive H -QA codes over $\mathbb{F}_{q^t}$, which suggests that this new class of additive codes is a promising class of codes to find codes with good and optimal parameters.

1.4 Conclusion and future work

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

2

Some Preliminaries

In this chapter, we will first state some basic properties of linear and additive codes over finite fields. We will further state some fundamental results on the geometry of symplectic, unitary and orthogonal spaces over finite fields. We will also recall some basic definitions and results from probability theory needed to prove our results.

To begin with, we will recall the definitions of linear and additive codes over finite fields and state their basic properties in the following section.

2.1 Linear and additive codes over finite fields

Let n be a positive integer, q be a prime power, and let $\mathbb{F}_q$ be the finite field of order q . Let $\mathbb{F}_q^n$ denote the n -dimensional vector space consisting of all n -tuples over $\mathbb{F}_q$. We will refer to the elements of $\mathbb{F}_q^n$ as words. Let us define a function

$d : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{N} \cup \{0\}$ as

$$d(a, b) = |\{i \in \mathbb{Z} : 1 \leq i \leq n, a_i \neq b_i\}|$$

for all $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n$. Note that the function d is a metric on $\mathbb{F}_q^n$ and is called the Hamming distance function. For $a, b \in \mathbb{F}_q^n$, the number $d(a, b)$ is called the *Hamming distance* between the words a and b . The *Hamming weight* of a word $a \in \mathbb{F}_q^n$ is defined as $wt(a) = d(a, \mathbf{0}) = |\{i \in \mathbb{Z} : 1 \leq i \leq n, a_i \neq 0\}|$. One can easily see that $d(a, b) = wt(a - b)$ for all $a, b \in \mathbb{F}_q^n$. Moreover, the *relative Hamming weight* of a word $a \in \mathbb{F}_q^n$, denoted by $\widehat{wt}(a)$, is defined as $\widehat{wt}(a) = \frac{wt(a)}{n}$.

A code C of length n over $\mathbb{F}_q$ is defined as a non-empty subset of $\mathbb{F}_q^n$. Elements of the code C are called codewords. The size of the code C , denoted by $|C|$, is defined as the number of codewords in C . The Hamming distance of the code C , denoted by $d(C)$, is defined as

$$d(C) = \min\{d(a, b) : a, b \in C, a \neq b\}.$$

The Hamming weight of the code C , denoted by $wt(C)$, is defined as

$$wt(C) = \min\{wt(a) : \mathbf{0} \neq a \in C\}.$$

For example, for the binary code $C_1 = \{(0, 0, 0, 0, 0), (0, 0, 1, 1, 1), (1, 1, 1, 1, 1)\}$ of length 5, we see that $d(C_1) = 2$ and $wt(C_1) = 3$, i.e., $d(C_1) \neq wt(C_1)$. Thus $d(C) = wt(C)$ need not hold for a code C in general. By Theorems 2.5.6 and 2.5.7 of [46], respectively, we note that a code C with Hamming distance d can detect up to $d - 1$ errors in any codeword and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors in any codeword. Thus the Hamming distance of a code is a measure of its error-detecting and error-correcting capabilities. A code C of length n , size M and Hamming distance d over $\mathbb{F}_q$ is referred to as a q -ary (n, M, d) -code. Linear and additive codes are two algebraically rich families of codes over finite fields.

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 *dimension* of the linear code $\mathcal{C}$, denoted by $\dim_{\mathbb{F}_q} \mathcal{C}$, is defined as the dimension of $\mathcal{C}$ as a vector space over $\mathbb{F}_q$. Thus the size of the linear code $\mathcal{C}$ is given by $|\mathcal{C}| = q^{\dim_{\mathbb{F}_q} \mathcal{C}}$.

For a linear code $\mathcal{C}$, we see, by Theorem 4.3.8 of [46], that $d(\mathcal{C}) = wt(\mathcal{C})$. A linear code $\mathcal{C}$ of length n , dimension k and Hamming distance d over $\mathbb{F}_q$ is referred to as a q -ary linear $[n, k, d]$ -code. In particular, the code $\mathcal{C}$ is called (i) a *binary linear code* if $q = 2$, (ii) a *ternary linear code* if $q = 3$, and (iii) a *quaternary linear code* if $q = 4$.

Example 2.1.1. The code $\mathcal{C}_1 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1)\}$ is a binary linear $[3, 2, 1]$ -code.

Cyclic codes, Hamming codes, Reed-Solomon codes, BCH codes and Golay codes constitute some of the notable and extensively studied families of linear codes.

To define additive codes, let $t \geq 2$ be an integer, and let $\mathbb{F}_{q^t}$ denote the finite field of order q^t . Let $\mathbb{F}_{q^t}^n$ denote the set of all n -tuples over $\mathbb{F}_{q^t}$. One can view the set $\mathbb{F}_{q^t}^n$ as an nt -dimensional vector space over $\mathbb{F}_q$ under the component-wise addition and the component-wise scalar multiplication. Now an *additive code* $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$ is defined as an $\mathbb{F}_q$ -linear subspace of $\mathbb{F}_{q^t}^n$. The *dimension* of the additive code $\mathcal{C}$, denoted by $\dim_{\mathbb{F}_q} \mathcal{C}$, is defined as $\dim_{\mathbb{F}_q} \mathcal{C} = \log_q |\mathcal{C}|$. Thus the size of the code $\mathcal{C}$ is given by $|\mathcal{C}| = q^{t \dim_{\mathbb{F}_q} \mathcal{C}}$. Note that the dimension of an additive code need not be an integer. For an additive code $\mathcal{C}$, we note, by Lemma 3 of Ball *et al.* [6], that $d(\mathcal{C}) = wt(\mathcal{C})$. From now on, we will refer to an additive code of length n , dimension k and Hamming distance d over $\mathbb{F}_{q^t}$ as an additive $[n, k, d]$ -code over $\mathbb{F}_{q^t}$.

Example 2.1.2. Let $q = t = 2$. Here we have $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_4 = \mathbb{F}_2(\omega) = \{0, 1, \omega, \omega^2\}$, where ω is a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$. The set

$$\mathfrak{C} = \{(0, 0, 0), (0, \omega, 0), (1, 0, \omega^2), (0, 0, \omega), (1, \omega, \omega^2), (0, \omega, \omega), (1, 0, 1), (1, \omega, 1)\}$$

is an additive $[3, \frac{3}{2}, 1]$ -code over $\mathbb{F}_4$.

Theorem 2.1.1. [36, Th. 10] (*Singleton bound for additive codes*): If $\mathcal{C}$ is an additive $[n, k, d]$ -code over $\mathbb{F}_{q^t}$, then we have $d \leq n - \lceil k \rceil + 1$.

An additive $[n, k, d]$ code $\mathcal{C}$ over $\mathbb{F}_{q^t}$ is said to be *maximum distance separable* (MDS) if its parameters satisfy $d = n - \lceil k \rceil + 1$, whereas the code $\mathcal{C}$ is said to be *almost MDS* if its parameters satisfy $d = n - \lceil k \rceil$.

The *rate* of an additive code $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$, denoted by $R(\mathcal{C})$, is defined as

$$R(\mathcal{C}) = \frac{\dim_{\mathbb{F}_{q^t}} \mathcal{C}}{n} = \frac{\log_{q^t} |\mathcal{C}|}{n},$$

and the *relative Hamming distance* of an additive code $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$, denoted by $\Delta(\mathcal{C})$, is defined as

$$\Delta(\mathcal{C}) = \frac{d(\mathcal{C})}{n} = \frac{wt(\mathcal{C})}{n} = \frac{1}{n} \min\{wt(a) : \mathbf{0} \neq a \in \mathcal{C}\} = \min\{\widehat{wt}(a) : \mathbf{0} \neq a \in \mathcal{C}\}.$$

Now let $\mathcal{F} = \{\mathcal{C}_i\}_{i \geq 1}$ be an infinite sequence of additive codes $\mathcal{C}_i$'s over $\mathbb{F}_{q^t}$, where for $i \geq 1$, the code $\mathcal{C}_i$ is an additive $[n_i, k_i, d_i]$ -code over $\mathbb{F}_{q^t}$ with $\lim_{i \rightarrow \infty} \{n_i\} = \infty$. The *rate* of the sequence $\mathcal{F}$, denoted by $R_{\mathcal{F}}$, is defined as

$$R_{\mathcal{F}} = \limsup_{i \rightarrow \infty} \{R(\mathcal{C}_i)\} = \limsup_{i \rightarrow \infty} \left\{ \frac{k_i}{n_i} \right\},$$

and the *relative Hamming distance* of the sequence $\mathcal{F}$, denoted by $\Delta_{\mathcal{F}}$, is defined as

$$\Delta_{\mathcal{F}} = \liminf_{i \rightarrow \infty} \{\Delta(\mathcal{C}_i)\} = \liminf_{i \rightarrow \infty} \left\{ \frac{d_i}{n_i} \right\}.$$

The sequence $\mathcal{F}$ of additive codes over $\mathbb{F}_{q^t}$ is said to be *asymptotically good* if it satisfies $R_{\mathcal{F}} \Delta_{\mathcal{F}} > 0$, i.e., if both its rate $R_{\mathcal{F}}$ and relative Hamming distance $\Delta_{\mathcal{F}}$ are positive. A class of additive codes over $\mathbb{F}_{q^t}$ is said to be *asymptotically good* if there exists an asymptotically good infinite sequence of additive codes over $\mathbb{F}_{q^t}$ belonging to this class.

Note that every linear code is inherently additive, but not all additive codes are necessarily linear. For instance, the additive code $\mathfrak{C}$ (considered in Example 2.1.2) is not a linear code, as the word $\omega(0, \omega, 0) = (0, \omega^2, 0) \notin \mathfrak{C}$. Thus, additive codes provide a broader framework as compared to linear codes and constitute an important family of codes. Kabatyansky [40] established a connection between linear and additive codes over finite fields. To recall this connection, let $\mathcal{B} = \{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_t\}$ be a basis of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$. Each element $a \in \mathbb{F}_{q^t}$ can be uniquely expressed as

$$a = a^{(1)}\mathbf{f}_1 + a^{(2)}\mathbf{f}_2 + \dots + a^{(t)}\mathbf{f}_t,$$

where $a^{(k)} \in \mathbb{F}_q$ for $1 \leq k \leq t$. Further, the map $\Phi_{\mathcal{B}} : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_q^t$, defined as

$$\Phi_{\mathcal{B}}(a) = (a^{(1)}, a^{(2)}, \dots, a^{(t)})$$

for all $a = a^{(1)}\mathbf{f}_1 + a^{(2)}\mathbf{f}_2 + \dots + a^{(t)}\mathbf{f}_t \in \mathbb{F}_{q^t}$ with $a^{(k)} \in \mathbb{F}_q$ for $1 \leq k \leq t$, is an $\mathbb{F}_q$ -linear vector space isomorphism. Furthermore, for any positive integer n , the isomorphism $\Phi_{\mathcal{B}}$ can be naturally extended to an $\mathbb{F}_q$ -linear vector space isomorphism from $\mathbb{F}_{q^t}^n$ onto $\mathbb{F}_q^{nt}$ as

$$a \mapsto (a_1^{(1)}, a_2^{(1)}, \dots, a_n^{(1)}, a_1^{(2)}, a_2^{(2)}, \dots, a_n^{(2)}, \dots, a_1^{(t)}, a_2^{(t)}, \dots, a_n^{(t)})$$

for all $a = (a_1, a_2, \dots, a_n) \in \mathbb{F}_{q^t}^n$, where $a_i = a_i^{(1)}\mathbf{f}_1 + a_i^{(2)}\mathbf{f}_2 + \dots + a_i^{(t)}\mathbf{f}_t \in \mathbb{F}_{q^t}$ with $a_i^{(k)} \in \mathbb{F}_q$ for $1 \leq i \leq n$ and $1 \leq k \leq t$, which we shall denote by $\Phi_{\mathcal{B}}$ itself for the sake of simplicity. In view of this, one can easily see that a non-empty subset $\mathcal{C}$ of $\mathbb{F}_{q^t}^n$ is an additive code of length n over $\mathbb{F}_{q^t}$ if and only if its image $\Phi_{\mathcal{B}}(\mathcal{C})$ is a linear code of length nt over $\mathbb{F}_q$. Now the following lemma relates the Hamming distance of an additive code $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$ with the Hamming distance of the corresponding linear code $\Phi_{\mathcal{B}}(\mathcal{C})$ of length nt over $\mathbb{F}_q$.

Lemma 2.1.1. *For an additive code $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$, we have*

$$d(\mathcal{C}) \geq \left\lceil \frac{d(\Phi_{\mathcal{B}}(\mathcal{C}))}{t} \right\rceil.$$

Proof. Its proof is similar to that of Lemma 2 of Shi *et al.* [59]. □

For a real number r satisfying $0 \leq r \leq n$, the Hamming ball of radius r centered at $a \in \mathbb{F}_q^n$ is defined as

$$S_a(n, r) = \{b \in \mathbb{F}_q^n : d(a, b) \leq r\}.$$

One can easily see that the volume $\text{Vol}_q(n, r)$ of the Hamming ball $S_a(n, r)$ is independent of the center a and is given by

$$\text{Vol}_q(n, r) = \sum_{j=0}^r \binom{n}{j} (q-1)^j.$$

Now for a prime power q , let $A_q(n, d)$ denote the largest positive integer M such that there exists a q -ary (n, M, d) -code. The Sphere Packing Bound (see [35, Th. 1.12.1]) is a well-known upper bound on $A_q(n, d)$, which is as stated below:

$$A_q(n, d) \leq \frac{q^n}{\text{Vol}_q(n, r)}, \quad \text{where } r = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Further, it is well-known [35, Lem. 2.10.3] that as $n \rightarrow \infty$, the volume $\text{Vol}_q(n, r)$ of the Hamming ball can be approximated in terms of the q -ary entropy function, which is as defined below.

Definition 2.1.1. [28, Sec. 3.3] *For any integer $q \geq 2$, the q -ary entropy function is the function $h_q : [0, 1] \rightarrow \mathbb{R}$, defined as*

$$h_q(y) = \begin{cases} 0 & \text{if } y = 0; \\ y \log_q(q-1) - y \log_q y - (1-y) \log_q(1-y) & \text{if } 0 < y < 1; \\ \log_q(q-1) & \text{if } y = 1. \end{cases}$$

Note that the function h_q is continuous, strictly increasing and concave in the interval $[0, 1 - q^{-1}]$ and satisfies $h_q(1 - q^{-1}) = 1$. The inverse of the entropy function h_q is the function $h_q^{-1} : [0, 1] \rightarrow [0, 1 - q^{-1}]$, defined as follows: For each $z \in [0, 1]$, $h_q^{-1}(z)$ is the unique real number $y \in [0, 1 - q^{-1}]$ satisfying $h_q(y) = z$.

Further, if δ is a real number satisfying $\delta \in [0, 1 - q^{-1}]$, then by [35, Lem. 2.10.3], we note that

$$\lim_{n \rightarrow \infty} \left\{ \frac{\text{Vol}_q(n, \delta n)}{q^{h_q(\delta)n}} \right\} = 1.$$

For $0 < \delta \leq 1 - q^{-1}$, let us define

$$\alpha_q(\delta) = \limsup_{n \rightarrow \infty} \left\{ \frac{\log_q A_q(n, \delta n)}{n} \right\}.$$

Theorem 2.1.2. [35, Th. 2.10.8] *(Asymptotic Gilbert-Varshamov (GV) bound) For $0 < \delta \leq 1 - q^{-1}$, we have*

$$\alpha_q(\delta) \geq 1 - h_q(\delta).$$

This bound guarantees the existence of a family of codes with relative distances

approaching δ and rates approaching $1 - h_q(\delta)$ as their lengths approach infinity.

In Chapters 3, 6 and 7, we will identify some asymptotically good classes of additive codes over finite fields by applying some basic results on balanced codes derived by Fan and Lin [24]. To define *balanced codes*, let $I = \{1, 2, \dots, n\}$ be an index set, and let us define $\mathbb{F}_q^I = \mathbb{F}_q^n$. Now for any subset $J = \{i_1, i_2, \dots, i_d\}$ of I satisfying $1 \leq i_1 < i_2 < \dots < i_d \leq n$, let $\rho : \mathbb{F}_q^I \rightarrow \mathbb{F}_q^J$ be a projection map, defined as $\rho(a) = (a_{i_1}, a_{i_2}, \dots, a_{i_d})$ for all $a = (a_1, a_2, \dots, a_n) \in \mathbb{F}_q^I$.

Definition 2.1.2. [24] *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_q$. If $I_1, I_2, \dots, I_s$ are subsets of the index set I (with repetition allowed) with each I_j of cardinality d and there exists an integer k such that*

- (i) *for any index $i \in I$, there are exactly k sets among I_j 's that contain i , and*
- (ii) *for each $j = 1, 2, \dots, s$, the projection map $\rho_j : \mathbb{F}_q^I \rightarrow \mathbb{F}_q^{I_j}$ bijectively maps the code $\mathcal{C}$ onto $\mathbb{F}_q^{I_j}$,*

then we say that the linear code $\mathcal{C}$ is a balanced code of length n over $\mathbb{F}_q$ with information length d . The sets $I_1, I_2, \dots, I_s$ are said to form a balanced system of information index set of $\mathcal{C}$.

We need the following two results derived by Fan and Lin [24] to show that MT additive codes over finite fields and their special classes such as self-orthogonal, self-dual and ACD codes are asymptotically good.

Theorem 2.1.3. [24, Cor. 3.4] *Let $\mathcal{C}$ be a balanced code of length n over $\mathbb{F}_q$ with information length d . Let us define*

$$\mathcal{C}^{\leq \delta} = \{c \in \mathcal{C} : \widehat{wt}(c) \leq \delta\}.$$

For $0 \leq \delta \leq 1 - q^{-1}$, we have

$$|\mathcal{C}^{\leq \delta}| \leq q^{dh_q(\delta)}.$$

Theorem 2.1.4. [24, Cor. 3.5] *Let $\mathcal{C}$ be a balanced code of length n over $\mathbb{F}_q$ with information length d . Then the code*

$$\mathcal{D} = \mathcal{C}^m = \mathcal{C} \times \mathcal{C} \times \dots \times \mathcal{C} = \{(c_1, c_2, \dots, c_m) : c_i \in \mathcal{C}, i = 1, 2, \dots, m\}$$

is also a balanced code of length mn over $\mathbb{F}_q$ with information length md . Further, for $0 \leq \delta \leq 1 - q^{-1}$, we have

$$|\mathcal{D}^{\leq \delta}| \leq q^{mdh_q(\delta)}.$$

In the following section, we will state some fundamental results from groups and geometry, which are needed to count some special classes of additive codes over finite fields.

2.2 Some basic results from groups and geometry

Throughout this section, let V be a finite-dimensional vector space over $\mathbb{F}_q$, and let θ be an automorphism of $\mathbb{F}_q$. A map $B : V \times V \rightarrow \mathbb{F}_q$ is called a θ -sesquilinear form on V if it satisfies the following four conditions for all vectors $u, v, w \in V$ and scalars $a, b \in \mathbb{F}_q$:

- (i) $B(u + v, w) = B(u, w) + B(v, w)$.
- (ii) $B(u, v + w) = B(u, v) + B(u, w)$.
- (iii) $B(au, v) = aB(u, v)$.
- (iv) $B(u, bv) = \theta(b)B(u, v)$.

In particular, if θ is the identity automorphism of $\mathbb{F}_q$, then the θ -sesquilinear form B is called a *bilinear form* on V . Further, the θ -sesquilinear form B on V is said to be

- (i) *reflexive* if $B(u, v) = 0$ for some $u, v \in V$, then $B(v, u) = 0$.
- (ii) *left non-degenerate* if $B(u, v) = 0$ for all $v \in V$, then $u = 0$.
- (iii) *right non-degenerate* if $B(u, v) = 0$ for all $u \in V$, then $v = 0$.
- (iv) *alternating* if θ is the identity automorphism of $\mathbb{F}_q$ and $B(u, u) = 0$ for all $u \in V$.
- (v) *symmetric* if θ is the identity automorphism of $\mathbb{F}_q$ and $B(u, v) = B(v, u)$ for all $u, v \in V$.

(vi) *Hermitian* if θ is the automorphism of $\mathbb{F}_q$ of order 2 and $B(u, v) = \theta(B(v, u))$ for all $u, v \in V$.

(vii) *skew-Hermitian* if θ is the automorphism of $\mathbb{F}_q$ of order 2 and

$$B(u, v) = -\theta(B(v, u)) \quad \text{for all } u, v \in V.$$

If a θ -sesquilinear form B is reflexive, then B is left non-degenerate if and only if it is right non-degenerate, and such a θ -sesquilinear form is simply referred to as a *non-degenerate θ -sesquilinear form*.

A pair (V, B) , where V is a finite-dimensional vector space over $\mathbb{F}_q$ and B is a θ -sesquilinear form on V , is called a *formed space* over $\mathbb{F}_q$. The *dimension* of the formed space (V, B) , denoted by $\dim_{\mathbb{F}_q} V$, is defined as the dimension of the vector space V over $\mathbb{F}_q$. In particular, if θ is the identity automorphism of $\mathbb{F}_q$, then the formed space (V, B) is called a *bilinear space*. If U is a subspace of V and $B_U = B|_{U \times U}$, then the pair (U, B_U) is called a subspace of the formed space (V, B) .

A formed space (V, B) is said to be *reflexive* (*resp. non-degenerate*) if the θ -sesquilinear form B on V is *reflexive* (*resp. non-degenerate*). The formed space (V, B) is called

- a *symplectic space* if B is an alternating, reflexive and non-degenerate bilinear form on V .
- a *unitary space* if B is a Hermitian (and hence reflexive) and non-degenerate form on V .
- an *orthogonal space* or a *finite geometry* if B is a symmetric (and hence reflexive) and non-degenerate bilinear form on V .

From now on, we assume, throughout this section, that the formed space (V, B) is reflexive and non-degenerate. Two vectors u, v in the formed space (V, B) are said to be *orthogonal* if they satisfy $B(u, v) = 0$. The *radical* of the formed space (V, B) , denoted by $\text{Rad}_B(V)$, is defined as the set

$$\text{Rad}_B(V) = \{v \in V : B(u, v) = 0 \text{ for all } u \in V\}.$$

Note that a formed space $(V, \mathbf{B})$ is *non-degenerate* if and only if $\text{Rad}_{\mathbf{B}}(V) = \{\mathbf{0}\}$.

Let us suppose that the formed space $(V, \mathbf{B})$ has dimension n . Then the Gram matrix of the formed space $(V, \mathbf{B})$ with respect to the ordered basis $\{v_1, v_2, \dots, v_n\}$ of V , denoted by $\mathfrak{G}(v_1, v_2, \dots, v_n)$, is defined as an $n \times n$ matrix, whose (i, j) th entry is given by $\mathbf{B}(v_i, v_j)$ for $1 \leq i, j \leq n$. By Theorem 24 of [23, Ch. 11], we see that the determinant $\det \mathfrak{G}(v_1, v_2, \dots, v_n)$ of the Gram matrix $\mathfrak{G}(v_1, v_2, \dots, v_n)$ can be expressed as

$$\det \mathfrak{G}(v_1, v_2, \dots, v_n) = \sum_{\pi \in S_n} \text{sgn}(\pi) \mathbf{B}(v_1, v_{\pi(1)}) \mathbf{B}(v_2, v_{\pi(2)}) \cdots \mathbf{B}(v_n, v_{\pi(n)}),$$

where S_n is the symmetric group of $\{1, 2, \dots, n\}$ and $\text{sgn} : S_n \rightarrow \{1, -1\}$ is the signum function, defined as

$$\text{sgn}(\pi) = \begin{cases} 1 & \text{if } \pi \text{ is the even permutation;} \\ -1 & \text{if } \pi \text{ is the odd permutation} \end{cases}$$

for all $\pi \in S_n$. We next recall the following well-known result.

Theorem 2.2.1. [64, Th. 5.1.1] *A finite-dimensional formed space $(V, \mathbf{B})$ is non-degenerate if and only if the Gram matrix of $(V, \mathbf{B})$ with respect to any ordered basis of V is non-singular.*

Further, a non-zero vector v in the formed space $(V, \mathbf{B})$ is said to be *isotropic* if it satisfies $\mathbf{B}(v, v) = 0$, otherwise v is called an *anisotropic vector*. A *hyperbolic pair* in $(V, \mathbf{B})$ is defined as a pair (u, v) of isotropic vectors $u, v \in V$ satisfying $\mathbf{B}(u, v) = 1$. If (u, v) is a hyperbolic pair in $(V, \mathbf{B})$, then one can easily see that the vectors u, v are linearly independent over $\mathbb{F}_q$. The 2-dimensional subspace $\langle u, v \rangle$ of V , generated by a hyperbolic pair (u, v) in $(V, \mathbf{B})$ is called a *hyperbolic line*.

For a subspace $(U, \mathbf{B}_U)$ of the formed space $(V, \mathbf{B})$, the *orthogonal complement* of U with respect to the form $\mathbf{B}$, denoted by $U^\perp$, is defined as

$$U^\perp = \{v \in V : \mathbf{B}(u, v) = 0 \text{ for all } u \in U\}.$$

Now a subspace $(U, \mathbf{B}_U)$ of the formed space $(V, \mathbf{B})$ is said to be

- (i) *isotropic* if it contains an isotropic vector.

- (ii) *anisotropic* if it contains no isotropic vector.
- (iii) *self-orthogonal* (or *totally isotropic*) if it satisfies $U \subseteq U^\perp$.
- (iv) *self-dual* if it satisfies $U = U^\perp$.
- (v) *non-degenerate* if it satisfies $U \cap U^\perp = \{0\}$.

Let U_1 and U_2 be two subspaces of V such that $V = U_1 \oplus U_2$ is the direct sum of U_1 and U_2 . Then the formed space (V, B) is said to be an *orthogonal direct sum* of U_1 and U_2 , written as $V = U_1 \perp U_2$, if it satisfies $B(u_1, u_2) = 0$ for all $u_1 \in U_1$ and $u_2 \in U_2$. Then the following holds.

Theorem 2.2.2. [27, 65] *Let (V, B) be a finite-dimensional reflexive and non-degenerate formed space over $\mathbb{F}_q$. If U is a subspace of V , then the orthogonal complement $U^\perp$ of U is also a subspace of V . Furthermore, we have*

$$\dim_{\mathbb{F}_q} U^\perp = \dim_{\mathbb{F}_q} V - \dim_{\mathbb{F}_q} U.$$

Additionally, if U is non-degenerate (or equivalently, $B_U = B \upharpoonright_{U \times U}$ is non-degenerate), then we have

$$V = U \perp U^\perp.$$

A self-orthogonal subspace U of a formed space (V, B) is said to be maximal if it is not properly contained in any other self-orthogonal subspace of (V, B) . By Theorem 7.4 of [65], we note that any two maximal self-orthogonal (or maximal totally isotropic) subspaces of a formed space (V, B) have the same dimension, which is called the *Witt index* of the formed space (V, B) . By applying Theorem 2.2.2, one can easily see that the Witt index of the formed space (V, B) is at most $\frac{1}{2} \dim_{\mathbb{F}_q} V$. From now on, let $I_{m, n-2m}$ and $H_{m, n-2m}$ denote the number of isotropic vectors and the number of hyperbolic pairs in an n -dimensional formed space of Witt index m , respectively. We next recall the following well-known result.

Lemma 2.2.1. *For a positive integer $k \leq n$, the number of distinct k -dimensional subspaces of an n -dimensional vector space over $\mathbb{F}_q$ is given by the q -binomial coefficient*

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

(Recall that $\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$.)

As a consequence, the total number of distinct subspaces of an n -dimensional vector space over $\mathbb{F}_q$ is given by

$$N(n, q) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}_q = 1 + \sum_{k=1}^n \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

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

Theorem 2.2.3. [65] *Let (V, B) be an n -dimensional symplectic space over $\mathbb{F}_q$. Then the dimension n of the space V is necessarily even. Further, the following hold.*

- (a) *The Witt index of (V, B) is $\frac{n}{2}$.*
- (b) *Every non-zero vector of V is isotropic. Thus the number of isotropic vectors in V is given by*

$$I_{\frac{n}{2}, 0} = q^n - 1.$$

- (c) *The number of hyperbolic pairs in V is given by*

$$H_{\frac{n}{2}, 0} = q^{n-1}(q^n - 1).$$

- (d) *The symplectic space (V, B) admits the Witt decomposition:*

$$V = \langle u_1, v_1 \rangle \perp \langle u_2, v_2 \rangle \perp \dots \perp \langle u_{\frac{n}{2}}, v_{\frac{n}{2}} \rangle,$$

where $(u_1, v_1), (u_2, v_2), \dots, (u_{\frac{n}{2}}, v_{\frac{n}{2}})$ are hyperbolic pairs in V . The corresponding basis $\{u_1, v_1, u_2, v_2, \dots, u_{\frac{n}{2}}, v_{\frac{n}{2}}\}$ is called a Witt basis (or a symplectic basis) of V .

- (e) *For $0 \leq k \leq \frac{n}{2}$, the number of distinct k -dimensional self-orthogonal (or totally isotropic) subspaces of V is given by*

$$\begin{bmatrix} n/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} \left(q^{\frac{n-2j}{2}} + 1 \right).$$

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

Theorem 2.2.4. [65] *For an n -dimensional unitary space $(V, \mathbf{B})$ over $\mathbb{F}_{q^2}$, the following hold.*

(a) *The Witt index $\mathfrak{m}$ of $(V, \mathbf{B})$ is given by*

$$\mathfrak{m} = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even;} \\ \frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

(b) *If $n \geq 2$, then V contains an isotropic vector.*

(c) *The number of isotropic vectors in V is given by*

$$\mathbf{I}_{\mathfrak{m}, n-2\mathfrak{m}} = (q^{n-1} - (-1)^{n-1})(q^n - (-1)^n).$$

(d) *The number of hyperbolic pairs in V is given by*

$$\mathbf{H}_{\mathfrak{m}, n-2\mathfrak{m}} = q^{2n-3}(q^{n-1} - (-1)^{n-1})(q^n - (-1)^n).$$

(e) *The unitary space $(V, \mathbf{B})$ admits the Witt decomposition:*

$$V = \begin{cases} \langle u_1, v_1 \rangle \perp \langle u_2, v_2 \rangle \perp \dots \perp \langle u_{\mathfrak{m}}, v_{\mathfrak{m}} \rangle & \text{if } n = 2\mathfrak{m}; \\ \langle u_1, v_1 \rangle \perp \langle u_2, v_2 \rangle \perp \dots \perp \langle u_{\mathfrak{m}}, v_{\mathfrak{m}} \rangle \perp \langle \beta \rangle & \text{if } n = 2\mathfrak{m} + 1, \end{cases}$$

where $(u_1, v_1), (u_2, v_2), \dots, (u_{\mathfrak{m}}, v_{\mathfrak{m}})$ are hyperbolic pairs in V and β is an anisotropic vector of V . The corresponding basis $\{u_1, v_1, u_2, v_2, \dots, u_{\mathfrak{m}}, v_{\mathfrak{m}}\} \cup \{\beta\}$ is called a Witt basis (or a unitary basis) of V .

(f) *For $0 \leq k \leq \mathfrak{m}$, the number of distinct k -dimensional self-orthogonal (or totally isotropic) subspaces of V is given by*

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

Definition 2.2.1. Let V be a finite-dimensional vector space over $\mathbb{F}_q$. The map $\varphi : V \rightarrow \mathbb{F}_q$ is called a quadratic map on V if it satisfies the following two conditions:

(i) $\varphi(au) = a^2\varphi(u)$ for all $a \in \mathbb{F}_q$ and $u \in V$.

(ii) The mapping $B_\varphi : V \times V \rightarrow \mathbb{F}_q$, defined as

$$B_\varphi(u, v) = \varphi(u + v) - \varphi(u) - \varphi(v) \text{ for all } u, v \in V, \quad (2.1)$$

is a symmetric bilinear form on V .

We refer to the pair (V, φ) as a *quadratic space* over $\mathbb{F}_q$ with the associated symmetric bilinear form B_φ . A quadratic space (V, φ) is said to be *non-degenerate* if it satisfies $\varphi^{-1}(0) \cap \text{Rad}_{B_\varphi}(V) = \{\mathbf{0}\}$, where $\text{Rad}_{B_\varphi}(V)$ denotes the *radical* of V with respect to the symmetric bilinear form B_φ . A non-zero vector v in the quadratic space (V, φ) is said to be *singular* if it satisfies $\varphi(v) = 0$, otherwise v is called a *non-singular* vector. Further, a *hyperbolic pair* in (V, φ) is defined as a pair (u, v) of singular vectors $u, v \in V$ satisfying $B_\varphi(u, v) = 1$. If (u, v) is a hyperbolic pair in (V, φ) , then one can easily see that the vectors u, v are linearly independent over $\mathbb{F}_q$ and the 2-dimensional subspace $\langle u, v \rangle$ of V , generated by the hyperbolic pair (u, v) , is called a *hyperbolic line*. A subspace of the quadratic space (V, φ) is defined as a pair (U, φ_U) , where U is a subspace of V and $\varphi_U = \varphi|_U$, and we will simply say that U is a subspace of the quadratic space (V, φ) . Now a subspace U of the quadratic space (V, φ) is said to be

(i) *singular* if it contains a singular vector.

(ii) *non-singular* if it contains no singular vector.

(iii) *self-orthogonal* (or *totally singular*) if $\varphi(u) = 0$ for all $u \in U$.

A self-orthogonal subspace U of the quadratic space (V, φ) is said to be maximal if it is not properly contained in any other self-orthogonal subspace of (V, φ) . By Corollaries 5.3 and 12.11 of [27], we note that all maximal self-orthogonal subspaces of the quadratic space (V, φ) have the same dimension, which is called the *Witt index* of (V, φ) .

Now let q be an odd prime power, and let (V, φ) be a quadratic space over $\mathbb{F}_q$ with the associated symmetric bilinear form B_φ . Note that the symmetric bilinear form B_φ can be uniquely determined from the quadratic map φ by using (2.1). Additionally, one can easily observe that the quadratic space (V, φ) is non-degenerate if and only if the formed space (V, B_φ) is non-degenerate. Thus one can associate an orthogonal space (V, B_φ) with every non-degenerate quadratic space (V, φ) . On the other hand, with every symmetric bilinear form B on a vector space V over $\mathbb{F}_q$, one can associate the quadratic map $Q_B : V \rightarrow \mathbb{F}_q$, defined as

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

Thus one can associate a non-degenerate quadratic space (V, Q_B) with every orthogonal space (V, B) over $\mathbb{F}_q$. From this, it follows that when q is odd, every non-degenerate quadratic space over $\mathbb{F}_q$ can be viewed as an orthogonal space, and vice versa.

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

Theorem 2.2.5. [65] *Let q be an odd prime power. Let (V, φ) be an n -dimensional non-degenerate quadratic space over $\mathbb{F}_q$ with the Witt index $\mathfrak{m}$. We have the following:*

(a) *If $n \geq 3$, then V contains a singular vector.*

(b) *The total number of singular vectors in V is given by*

$$I_{\mathfrak{m}, n-2\mathfrak{m}} = (q^{\mathfrak{m}} - 1)(q^{n-\mathfrak{m}-1} + 1).$$

(c) *The total number of hyperbolic pairs in V is given by*

$$H_{\mathfrak{m}, n-2\mathfrak{m}} = q^{n-2}(q^{\mathfrak{m}} - 1)(q^{n-\mathfrak{m}-1} + 1).$$

(d) *The quadratic space (V, φ) admits a Witt decomposition:*

$$V = \langle u_1, v_1 \rangle \perp \langle u_2, v_2 \rangle \perp \dots \perp \langle u_{\mathfrak{m}}, v_{\mathfrak{m}} \rangle \perp W,$$

where $(u_1, v_1), (u_2, v_2), \dots, (u_m, v_m)$ are hyperbolic pairs in V and W is a non-singular subspace of V having dimension $n - 2m \leq 2$. The corresponding basis $\{u_1, v_1, u_2, v_2, \dots, u_m, v_m\} \cup \beta_W$ with β_W as a basis of W is called a Witt basis (or a quadratic basis) of V .

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

$$\begin{bmatrix} m \\ k \end{bmatrix}_q \prod_{a=0}^{k-1} (q^{n-m-a-1} + 1).$$

We next recall, from Section 2.1, that the set $\mathbb{F}_{q^t}^n$ is an nt -dimensional vector space over $\mathbb{F}_q$. In particular, let $V = \mathbb{F}_{q^t}^n$, and let $\langle \cdot, \cdot \rangle : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_q$ be a reflexive, non-degenerate and symmetric bilinear form. That is, the pair $(\mathbb{F}_{q^t}^n, \langle \cdot, \cdot \rangle)$ is an nt -dimensional orthogonal space over $\mathbb{F}_q$. When q is odd, the orthogonal space $(\mathbb{F}_{q^t}^n, \langle \cdot, \cdot \rangle)$ can also be viewed as a non-degenerate quadratic space $(\mathbb{F}_{q^t}^n, \mathbf{Q})$ over $\mathbb{F}_q$, where the corresponding quadratic form $\mathbf{Q} : \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_q$ is defined as

$$\mathbf{Q}(v) = \frac{1}{2} \langle v, v \rangle \quad \text{for all } v \in \mathbb{F}_{q^t}^n.$$

In the following theorem, we assume that q is an odd prime power and obtain the Witt index of the quadratic space $(\mathbb{F}_{q^t}^n, \mathbf{Q})$ over $\mathbb{F}_q$.

Theorem 2.2.6. [36, Th. 7] *Let q be an odd prime power, and let $(\mathbb{F}_{q^t}^n, \mathbf{Q})$ be an nt -dimensional non-degenerate quadratic space over $\mathbb{F}_q$. The Witt index m of the quadratic space $(\mathbb{F}_{q^t}^n, \mathbf{Q})$ is given by*

$$m = \begin{cases} \frac{nt-1}{2} & \text{if } nt \text{ is odd;} \\ \frac{nt-2}{2} & \text{if either } n \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } n \text{ is odd, } t \equiv 0 \pmod{4} \\ & \text{and } q \equiv 3 \pmod{4} \text{ or } n \equiv 2 \pmod{4}, t \text{ is odd and } q \equiv 3 \pmod{4}; \\ \frac{nt}{2} & \text{if either } n \text{ is even and } q \equiv 1 \pmod{4} \text{ or } n \text{ is even, } nt \equiv 0 \pmod{4} \text{ and} \\ & q \equiv 3 \pmod{4} \text{ or } n \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases}$$

Now two quadratic spaces $(V_1, \mathbf{Q}_1)$ and $(V_2, \mathbf{Q}_2)$ are said to be *isometric* if there exists a vector space isomorphism $\phi : V_1 \rightarrow V_2$ satisfying $\mathbf{Q}_2(\phi(v)) = \mathbf{Q}_1(v)$ for all

$v \in V_1$. If such an isomorphism exists, we say that the quadratic spaces (V_1, Q_1) and (V_2, Q_2) are isometric and that the corresponding quadratic forms Q_1 and Q_2 are equivalent, which we denote by $V_1 \simeq V_2$.

Theorem 2.2.7. [27, Th. 5.1] (*Witt's Cancellation Theorem*) *Let q be an odd prime power. Let U_1 and U_2 be two non-degenerate subspaces of a finite-dimensional quadratic space (V, Q) over $\mathbb{F}_q$. If $U_1 \simeq U_2$, then $U_1^\perp \simeq U_2^\perp$.*

Finally, let q be an even prime power, and let (V, φ) be a quadratic space over $\mathbb{F}_q$ with the associated symmetric bilinear form B_φ . Here we observe that

$$B_\varphi(u, u) = \varphi(u + u) + \varphi(u) + \varphi(u) = 0 \text{ for all } u \text{ in } V,$$

which implies that the symmetric bilinear form B_φ is necessarily an alternating form. Consequently, the symmetric bilinear form B_φ is not uniquely determined by φ , and hence we can not associate an orthogonal space with a quadratic space. To study quadratic spaces over finite fields of even characteristic, we need to define the following:

A quadratic space (V, φ) is said to be *non-defective* if $\text{Rad}_{B_\varphi}(V) = \{0\}$, otherwise it is said to be *defective*. The quadratic form φ is said to be *regular* if it satisfies $\ker(\varphi \upharpoonright_{\text{Rad}_{B_\varphi}(V)}) = \{0\}$.

Theorem 2.2.8. [27, Th. 12.9] *Let q be an even prime power, and let (V, φ) be an n -dimensional regular quadratic space over $\mathbb{F}_q$ with the Witt index m . There exists a basis $\{v_1, v_2, \dots, v_n\}$ of V relative to which the quadratic form φ can take one of the following three forms:*

I. *When $n = 2m + 1$, the quadratic map φ is given by*

$$\varphi \left(\sum_{i=1}^n a_i v_i \right) = a_1 a_{m+1} + a_2 a_{m+2} + \dots + a_m a_{2m} + a_{2m+1}^2$$

for all $a_1, a_2, \dots, a_n \in \mathbb{F}_q$.

II. *When n is an even integer, there are two possible forms for the quadratic map φ accordingly as the Witt index m of the quadratic space (V, φ) is $\frac{n}{2}$ or $\frac{n-2}{2}$.*

(a) If $n = 2\mathfrak{m}$, we have

$$\varphi \left(\sum_{i=1}^n a_i v_i \right) = a_1 a_{\mathfrak{m}+1} + a_2 a_{\mathfrak{m}+2} + \cdots + a_{\mathfrak{m}} a_{2\mathfrak{m}}$$

for all $a_1, a_2, \dots, a_n \in \mathbb{F}_q$.

(b) If $n = 2\mathfrak{m} + 2$, we have

$$\varphi \left(\sum_{i=1}^n a_i v_i \right) = a_1 a_{\mathfrak{m}} + a_2 a_{\mathfrak{m}+1} + \cdots + a_{\mathfrak{m}-1} a_{2\mathfrak{m}-2} + a_{2\mathfrak{m}-1}^2 + a_{2\mathfrak{m}-1} a_{2\mathfrak{m}} + b a_{2\mathfrak{m}}^2$$

for all $a_1, a_2, \dots, a_n \in \mathbb{F}_q$, where $b \in \mathbb{F}_q$ is chosen in such a way that the polynomial $x^2 + x + b$ is irreducible over $\mathbb{F}_q$.

In the following theorem, we state some basic properties of regular quadratic spaces over a finite field of even characteristic.

Theorem 2.2.9. [27] *Let q be an even prime power, and let (V, φ) be an n -dimensional regular quadratic space over $\mathbb{F}_q$ with the Witt index $\mathfrak{m}$. Then we have the following:*

(a) *If $n \geq 2$ and V is defective, then V contains a singular vector.*

(b) *If $n \geq 3$ and V is non-defective, then V contains a singular vector.*

(c) *The number of singular vectors in V is given by*

$$I_{\mathfrak{m}, n-2\mathfrak{m}} = \begin{cases} (q^{n-1} - 1) & \text{if } n = 2\mathfrak{m} + 1; \\ (q^{\mathfrak{m}} - 1)(q^{\mathfrak{m}-1} + 1) & \text{if } n = 2\mathfrak{m}; \\ (q^{\mathfrak{m}} - 1)(q^{\mathfrak{m}+1} + 1) & \text{if } n = 2\mathfrak{m} + 2. \end{cases}$$

(d) *The number of hyperbolic pairs in V is given by*

$$H_{\mathfrak{m}, n-2\mathfrak{m}} = \begin{cases} q^{n-2}(q^{n-1} - 1) & \text{if } n = 2\mathfrak{m} + 1; \\ q^{n-2}(q^{\mathfrak{m}} - 1)(q^{\mathfrak{m}-1} + 1) & \text{if } n = 2\mathfrak{m}; \\ q^{n-2}(q^{\mathfrak{m}} - 1)(q^{\mathfrak{m}+1} + 1) & \text{if } n = 2\mathfrak{m} + 2. \end{cases}$$

Theorem 2.2.10. [27, Cor. 12.12] (*Witt's Cancellation Theorem*) Let q be an even prime power, and let (V, φ) be a non-defective quadratic space over $\mathbb{F}_q$. If U_1 and U_2 are subspaces of the quadratic space (V, φ) such that $U_1 \simeq U_2$, then $U_1^\perp \simeq U_2^\perp$.

In the following section, we state some basic results from probability theory, which are needed to study the asymptotic properties of the rates and relative Hamming distances of certain special classes of additive codes over finite fields.

2.3 Some basic results from probability theory

A *random variable* X defined on a sample space S is a function $X : S \rightarrow \mathbb{R}$. A *discrete random variable* is a random variable that takes only finitely many or countably many values. The *expectation* of a discrete random variable X , denoted by $E[X]$, is defined as

$$E[X] = \sum_x x \Pr(X = x),$$

where the summation $\sum_x$ runs over all possible values x taken by the random variable X and $\Pr(X = x)$ is the probability that the random variable X takes the value x .

Suppose an experiment succeeds with probability p and fails with probability $1 - p$. Let X be a discrete random variable defined as

$$X = \begin{cases} 1 & \text{if the experiment succeeds;} \\ 0 & \text{otherwise.} \end{cases}$$

Here note that $\Pr(X = 1) = p$ and $\Pr(X = 0) = 1 - p$. Such a random variable X is called a *Bernoulli* or an *indicator random variable*. For a Bernoulli random variable X , we have

$$E[X] = 1 \cdot p + 0 \cdot (1 - p) = p = \Pr(X = 1).$$

Theorem 2.3.1. [66, Th. 2.1] (*Linearity of Expectation*) For a finite collection of discrete random variables $X_1, X_2, \dots, X_n$ with finite expectations $E[X_1], E[X_2], \dots, E[X_n]$ respectively, we have

$$E\left[\sum_{i=1}^n X_i\right] = \sum_{i=1}^n E[X_i].$$

Theorem 2.3.2. [66, Th. 3.1]/(Markov's Inequality) *Let X be a non-negative random variable. Then for all $a > 0$, we have*

$$\Pr(X \geq a) \leq \frac{E[X]}{a}.$$

In Chapters [3, 7] we will define and study a new family of additive codes over finite fields, *viz.* multi-twisted additive codes, which is an extension of multi-twisted (linear) codes introduced by Aydin and Halilović [5]. We will apply these results to show that multi-twisted additive codes over finite fields and their special subclasses consisting of all self-orthogonal, self-dual and additive codes with complementary duals (ACD codes) are asymptotically good. We will also provide enumeration formulae for the aforementioned classes of MT additive codes over finite fields. Later, in Chapter [8] we will apply these results to study additive quasi-Abelian codes over finite fields, which is a generalization of a special class of MT additive codes over finite fields and an extension of linear quasi-Abelian codes introduced by Wasan [67]. We will apply the results on the geometry of symplectic, unitary and orthogonal spaces to enumerate all self-orthogonal, self-dual, and additive codes with complementary duals (ACD codes) belonging to the family of additive quasi-abelian codes over finite fields.

3

Multi-twisted additive codes over finite fields

3.1 Introduction

In this chapter, we will define and study a new class of additive codes over finite fields, *viz.* multi-twisted (MT) additive codes, which is a generalization of constacyclic additive codes and an extension of MT (linear) codes introduced by Aydin and Halilović [5]. We will study their algebraic structures by writing a canonical form decomposition of these codes using the Chinese Remainder Theorem and provide an enumeration formula for these codes. We will also provide a trace description of these codes using their canonical form decomposition. We will further study the asymptotic properties of the rates and relative Hamming distances of a certain special subclass of MT additive codes over finite fields on which probabilistic methods can work well. By applying probabilistic methods, we will show that the family of

MT additive codes over finite fields is asymptotically good.

This chapter is organized as follows: In Section 3.2, we define and study multi-twisted (MT) additive codes over finite fields. In Section 3.3, we provide a canonical form decomposition of these codes using the Chinese Remainder Theorem (Theorem 3.3.1). In Section 3.4, we provide a trace description for all MT additive codes over finite fields in terms of their constituents (Theorem 3.4.1). In Section 3.5, we study a suitable subclass of MT additive codes over finite fields on which probabilistic methods can work well. Further, by using probabilistic methods, we study the asymptotic properties of the rates and the relative Hamming distances of this particular class of codes (Theorems 3.5.1 and 3.5.2), and show that there exists an infinite sequence of asymptotically good MT additive codes over finite fields (Theorem 3.5.3). As a consequence, we deduce that the families of constacyclic and cyclic additive codes over finite fields are asymptotically good (Corollaries 3.5.1 and 3.5.2).

3.2 Multi-twisted additive codes over finite fields

Throughout this thesis, let $\mathbb{F}_q$ denote the finite field of order q and characteristic p . Let $t \geq 2$ be an integer, and let $\mathbb{F}_{q^t}$ denote the finite field of order q^t . Let n be a positive integer, and let $\mathbb{F}_{q^t}^n$ denote the set of all n -tuples over $\mathbb{F}_{q^t}$. One can view the set $\mathbb{F}_{q^t}^n$ as an (nt) -dimensional vector space over $\mathbb{F}_q$ under the component-wise addition and the component-wise scalar multiplication. Recall that an additive code of length n over $\mathbb{F}_{q^t}$ is defined as an $\mathbb{F}_q$ -linear subspace of $\mathbb{F}_{q^t}^n$.

To define multi-twisted additive codes, let us write $n = m_1 + m_2 + \cdots + m_\ell$, where $m_1, m_2, \dots, m_\ell$ are positive integers coprime to q . From now on, we shall represent each element $a \in \mathbb{F}_{q^t}^n$ as

$$a = (a_{1,0}, a_{1,1}, \dots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \dots, a_{2,m_2-1}; \dots; a_{\ell,0}, a_{\ell,1}, \dots, a_{\ell,m_\ell-1}),$$

where $a_{i,j} \in \mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$ and $0 \leq j \leq m_i - 1$. Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$, where $\omega_1, \omega_2, \dots, \omega_\ell$ are non-zero elements of $\mathbb{F}_q$. Now let us define a map $T_\Omega : \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_{q^t}^n$ by

$$T_\Omega(a) = (\omega_1 a_{1,m_1-1}, a_{1,0}, \dots, a_{1,m_1-2}; \omega_2 a_{2,m_2-1}, a_{2,0}, \dots, a_{2,m_2-2}; \dots; \omega_\ell a_{\ell,m_\ell-1}, a_{\ell,0}, \dots, a_{\ell,m_\ell-2})$$

for all $a = (a_{1,0}, a_{1,1}, \dots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \dots, a_{2,m_2-1}; \dots; a_{\ell,0}, a_{\ell,1}, \dots, a_{\ell,m_\ell-1}) \in \mathbb{F}_{q^t}^n$. It is easy to see that the map T_Ω is an $\mathbb{F}_q$ -linear vector space isomorphism and is called the Ω -multi-twisted (Ω -MT) shift operator on $\mathbb{F}_{q^t}^n$. It is easy to observe that

$$M = \text{lcm}[m_1 \text{ord}(\omega_1), m_2 \text{ord}(\omega_2), \dots, m_\ell \text{ord}(\omega_\ell)]$$

is the least positive integer satisfying $T_\Omega^M = I$, where I is the identity operator on $\mathbb{F}_{q^t}^n$ and $\text{ord}(\omega_i)$ denotes the multiplicative order of ω_i for $1 \leq i \leq \ell$. Also, it is easy to see that M is the least positive integer such that $x^{m_i} - \omega_i$ divides $x^M - 1$ in $\mathbb{F}_q[x]$ for $1 \leq i \leq \ell$.

Definition 3.2.1. An additive code $\mathcal{C}$ of length n over $\mathbb{F}_{q^t}$ is called an Ω -multi-twisted (Ω -MT) additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ if it is invariant under the Ω -MT shift operator T_Ω on $\mathbb{F}_{q^t}^n$, i.e., if it satisfies $T_\Omega(\mathcal{C}) = \mathcal{C}$.

Example 3.2.1. Let $q = 3$ and $t = 2$. Here we have $\mathbb{F}_3 = \{0, 1, 2\}$ and $\mathbb{F}_9 = \mathbb{F}_3(\xi)$, where ξ is a root of $x^2 + 2x + 2 \in \mathbb{F}_3[x]$. The set

$$\mathfrak{C}_1 = \left\{ (a + 2b\xi^7 + 2c + d\xi^7, a\xi^7 + b + 2c\xi^7 + 2d; a\xi^5 + c\xi^6 + d\xi^7, a\xi^7 + b\xi^5 + d\xi^6, \right. \\ \left. a\xi^6 + b\xi^7 + c\xi^5, b\xi^6 + c\xi^7 + d\xi^5) : a, b, c, d \in \mathbb{F}_3 \right\}$$

is an additive $[6, \frac{3}{2}, 4]$ -code over $\mathbb{F}_9$. It is easy to observe that the code $\mathfrak{C}_1$ is a $(2, 1)$ -MT additive code of length 6 and block lengths $(2, 4)$ over $\mathbb{F}_9$.

In particular, Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ coincide with ω_1 -constacyclic additive codes of length m_1 over $\mathbb{F}_{q^t}$ when $\ell = 1$ [17, 41], while these codes coincide with cyclic additive codes of length m_1 over $\mathbb{F}_{q^t}$ when $\ell = 1$ and $\omega_1 = 1$ [32–34, 57, 58].

We now proceed to study the algebraic structure of Ω -MT additive codes over $\mathbb{F}_{q^t}$. To do this, throughout this thesis, for a finite field $\mathbb{F}_\Omega$ of order Ω and a non-zero, non-constant polynomial $F(x)$ in $\mathbb{F}_\Omega[x]$, we shall represent elements of the quotient ring $\mathbb{F}_\Omega[x]/\langle F(x) \rangle$ by their representatives in $\mathbb{F}_\Omega[x]$ of degree strictly less than the degree of $F(x)$, and we shall perform their addition and multiplication modulo $F(x)$. Let us define the quotient ring $\mathfrak{R}_M = \frac{\mathbb{F}_q[x]}{\langle x^M - 1 \rangle}$. Note that $\mathfrak{R}_M$ is a principal ideal ring. Furthermore, for a non-zero element $\omega \in \mathbb{F}_q$ and a positive integer m , let $\mathcal{R}_{m,\omega}$

be the quotient ring $\frac{\mathbb{F}_{q^t}[x]}{\langle x^m - \omega \rangle}$. Next, let us define

$$\mathcal{R} = \prod_{i=1}^{\ell} \mathcal{R}_{m_i, \omega_i}.$$

Note that the set $\mathcal{R}$ can be viewed as an $\mathbb{F}_q[x]$ -module (or as an $\mathfrak{R}_M$ -module) under the component-wise addition and the component-wise scalar multiplication, and is called the Ω -multi-twisted (Ω -MT) module. Apart from this, the Ω -MT module $\mathcal{R}$ can also be viewed as an (nt) -dimensional vector space over $\mathbb{F}_q$. Thus there exists an $\mathbb{F}_q$ -linear vector space isomorphism $\psi : \mathbb{F}_{q^t}^n \rightarrow \mathcal{R}$, defined as

$$\psi(a) = (a_1(x), a_2(x), \dots, a_\ell(x)) = a(x) \text{ (say)}$$

for all $a = (a_{1,0}, a_{1,1}, \dots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \dots, a_{2,m_2-1}; \dots; a_{\ell,0}, a_{\ell,1}, \dots, a_{\ell,m_\ell-1}) \in \mathbb{F}_{q^t}^n$, where $a_i(x) = a_{i,0} + a_{i,1}x + \dots + a_{i,m_i-1}x^{m_i-1} \in \mathcal{R}_{m_i, \omega_i}$ for $1 \leq i \leq \ell$. From now on, let $a(x) = \psi(a)$ be the element in $\mathcal{R}$ corresponding to each word $a \in \mathbb{F}_{q^t}^n$, and vice versa. Moreover, it is easy to see that $\psi(T_\Omega(a)) = x\psi(a) = xa(x) \in \mathcal{R}$ for all $a \in \mathbb{F}_{q^t}^n$. From this, it follows that a non-empty subset $\mathcal{C}$ of $\mathbb{F}_{q^t}^n$ is an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ if and only if its image $\psi(\mathcal{C})$ is an $\mathbb{F}_q[x]$ -submodule (or an $\mathfrak{R}_M$ -submodule) of the Ω -MT module $\mathcal{R}$. In view of this, each Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ can be viewed as an $\mathbb{F}_q[x]$ -submodule of the Ω -MT module $\mathcal{R}$, and vice versa.

For example, let $q = 3$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $\omega_1 = 2$ and $\omega_2 = 1$. Let ξ be a root of $x^2 + 2x + 2 \in \mathbb{F}_3[x]$. Let $\mathfrak{C}_1$ be the $(2, 1)$ -MT additive code of length 6 and block lengths $(2, 4)$ considered in Example 3.2.1. One can easily observe that the code $\mathfrak{C}_1$ can also be viewed as an $\mathbb{F}_3[x]$ -submodule (or an $\frac{\mathbb{F}_3[x]}{\langle x^4 - 1 \rangle}$ -submodule) of $\frac{\mathbb{F}_9[x]}{\langle x^2 - 2 \rangle} \times \frac{\mathbb{F}_9[x]}{\langle x^4 - 1 \rangle}$ with a generating set $\{(1 + \xi^7 x, \xi^5 + \xi^7 x + \xi^6 x^2)\}$.

3.3 A canonical decomposition of MT additive codes using the Chinese Remainder Theorem

To provide a canonical decomposition of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, we recall that $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$.

Let $h_1(x), h_2(x), \dots, h_s(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ in $\mathbb{F}_q[x]$. For $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$, let us define

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

Then for $1 \leq i \leq \ell$, we see that $x^{m_i} - \omega_i = h_1(x)^{\epsilon_{1,i}} h_2(x)^{\epsilon_{2,i}} \dots h_s(x)^{\epsilon_{s,i}}$ is the irreducible factorization of the polynomial $x^{m_i} - \omega_i$ over $\mathbb{F}_q$. Now for each i , by applying the Chinese Remainder Theorem [7, Th. 1.2.12], we get

$$\mathcal{R}_{m_i, \omega_i} \simeq \bigoplus_{\nu=1}^s \epsilon_{\nu,i} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle},$$

where the corresponding ring isomorphism from $\mathcal{R}_{m_i, \omega_i}$ onto $\bigoplus_{\nu=1}^s \epsilon_{\nu,i} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}$ is given by

$$a_i(x) \mapsto \left(\epsilon_{1,i}(a_i(x) + \langle h_1(x) \rangle), \epsilon_{2,i}(a_i(x) + \langle h_2(x) \rangle), \dots, \epsilon_{s,i}(a_i(x) + \langle h_s(x) \rangle) \right)$$

for all $a_i(x) \in \mathcal{R}_{m_i, \omega_i}$. This implies that

$$\mathcal{R} = \prod_{i=1}^{\ell} \mathcal{R}_{m_i, \omega_i} \simeq \bigoplus_{\nu=1}^s \underbrace{\left(\epsilon_{\nu,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}, \epsilon_{\nu,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}, \dots, \epsilon_{\nu,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle} \right)}_{\mathbb{G}_\nu} = \bigoplus_{\nu=1}^s \mathbb{G}_\nu = \mathbb{G}, \quad (3.1)$$

and the corresponding ring isomorphism from $\mathcal{R}$ onto $\mathbb{G}$ is given by

$$a(x) \mapsto \left(\epsilon_{1,1}(a_1(x) + \langle h_1(x) \rangle), \epsilon_{1,2}(a_2(x) + \langle h_1(x) \rangle), \dots, \epsilon_{1,\ell}(a_\ell(x) + \langle h_1(x) \rangle), \right. \\ \left. \epsilon_{2,1}(a_1(x) + \langle h_2(x) \rangle), \epsilon_{2,2}(a_2(x) + \langle h_2(x) \rangle), \dots, \epsilon_{2,\ell}(a_\ell(x) + \langle h_2(x) \rangle), \dots, \right. \\ \left. \epsilon_{s,1}(a_1(x) + \langle h_s(x) \rangle), \epsilon_{s,2}(a_2(x) + \langle h_s(x) \rangle), \dots, \epsilon_{s,\ell}(a_\ell(x) + \langle h_s(x) \rangle) \right)$$

for all $a(x) = (a_1(x), a_2(x), \dots, a_\ell(x)) \in \mathcal{R}$. In view of the above isomorphism, from this point on, we shall identify each element $a(x) = (a_1(x), a_2(x), \dots, a_\ell(x)) \in \mathcal{R}$ with the element

$$A(x) = (A_1(x), A_2(x), \dots, A_s(x)) \in \mathbb{G},$$

where $A_\nu(x) = (A_{\nu,1}(x), A_{\nu,2}(x), \dots, A_{\nu,\ell}(x)) \in \mathbb{G}_\nu$ with $A_{\nu,i}(x) = \epsilon_{\nu,i}a_i(x) + \langle h_\nu(x) \rangle \in \epsilon_{\nu,i} \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}$ for $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$. That is, if Ψ denotes the isomorphism from $\mathcal{R}$ onto $\mathbb{G}$, then we shall write $\Psi(a(x)) = A(x)$. We further observe that the set $\mathbb{G}$ can be viewed as an $\mathbb{F}_q[x]$ -module under the component-wise addition and the component-wise scalar multiplication.

Further, for $1 \leq \nu \leq s$, let us define $\mathcal{F}_\nu = \frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle}$. We see that if $d_\nu = \deg h_\nu(x)$, then $\mathcal{F}_\nu$ is the finite field of order q^{d_ν} , which implies that $\mathcal{F}_\nu \simeq \mathbb{F}_{q^{d_\nu}}$ for $1 \leq \nu \leq s$. Furthermore, we observe that the set $\mathbb{G}_\nu$ is an $(\epsilon_\nu t)$ -dimensional vector space over $\mathcal{F}_\nu$ under the component-wise addition and the component-wise scalar multiplication, where $\epsilon_\nu = \sum_{i=1}^{\ell} \epsilon_{\nu,i}$ for each ν . From the above discussion, we have the following canonical form decomposition of each Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Theorem 3.3.1. (a) Let $\mathcal{C}(\subseteq \mathcal{R})$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. For $1 \leq \nu \leq s$, let us define $\mathcal{C}_\nu = \mathcal{C} \cap \mathbb{G}_\nu$. Then for each ν , $\mathcal{C}_\nu$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$. Furthermore, the code $\mathcal{C}$ has a unique direct sum decomposition $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu$. (The subspaces $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_s$ are called constituents of the code $\mathcal{C}$ corresponding to the irreducible polynomials $h_1(x), h_2(x), \dots, h_s(x)$, respectively).

(b) Conversely, if $\mathcal{D}_\nu$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ for $1 \leq \nu \leq s$, then the direct sum $\mathcal{D} = \bigoplus_{\nu=1}^s \mathcal{D}_\nu$ is an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Proof. The proof is straightforward. □

The above theorem shows that the $\mathcal{F}_\nu$ -subspaces of $\mathbb{G}_\nu$ ($1 \leq \nu \leq s$) are building blocks of all Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. In the next theorem, we enumerate all Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Theorem 3.3.2. The total number of distinct Ω -MT additive codes of length n and

block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$N_\Omega = \prod_{\nu=1}^s \left(\sum_{b=0}^{\epsilon_\nu t} \begin{bmatrix} \epsilon_\nu t \\ b \end{bmatrix}_{q^{d_\nu}} \right).$$

Proof. It follows immediately from Theorem 3.3.1 and Lemma 2.2.1. $\square$

Remark 3.3.1. *There are Ω -MT additive codes over $\mathbb{F}_{q^t}$ that can also be viewed as Λ -MT additive codes, where $\Lambda \neq \Omega$. For example, let $q = 5$, $t = 2$, $m_1 = 4$, $m_2 = 2$, and let ξ be a primitive element of $\mathbb{F}_{25}$. Let $\mathcal{C}_2$ be the $\mathbb{F}_5[x]$ -submodule of $\frac{\mathbb{F}_{25}[x]}{\langle x^4-2 \rangle} \times \frac{\mathbb{F}_{25}[x]}{\langle x^2-3 \rangle}$ with the generating set $\{(\xi^5 + \xi^5 x + \xi^{15} x^2 + \xi^6 x^3, 1 + x)\}$. One can easily observe that the code $\mathcal{C}_2$ can also be viewed as an $\mathbb{F}_5[x]$ -submodule of $\frac{\mathbb{F}_{25}[x]}{\langle x^4-2 \rangle} \times \frac{\mathbb{F}_{25}[x]}{\langle x^2-2 \rangle}$, i.e., the code $\mathcal{C}_2$ is a $(2, 3)$ -MT additive code as well as a $(2, 2)$ -MT additive code of length 6 over $\mathbb{F}_{25}$. Thus the total number of distinct MT additive codes of length n over $\mathbb{F}_{q^t}$ is not equal to $(q-1)^\ell N_\Omega$.*

3.4 Trace description of MT additive codes

In this section, we will provide a trace description for all Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. For this, we recall, from Section 2.1, that if $\mathcal{B} = \{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_t\}$ is a basis of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$, then each element $a \in \mathbb{F}_{q^t}$ can be uniquely expressed as $a = a^{(1)}\mathbf{f}_1 + a^{(2)}\mathbf{f}_2 + \dots + a^{(t)}\mathbf{f}_t$, where $a^{(k)} \in \mathbb{F}_q$ for $1 \leq k \leq t$. Further, the map $\Phi_{\mathcal{B}} : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_q^t$, defined as

$$\Phi_{\mathcal{B}}(a) = (a^{(1)}, a^{(2)}, \dots, a^{(t)})$$

for all $a = a^{(1)}\mathbf{f}_1 + a^{(2)}\mathbf{f}_2 + \dots + a^{(t)}\mathbf{f}_t \in \mathbb{F}_{q^t}$ with $a^{(k)} \in \mathbb{F}_q$ for $1 \leq k \leq t$, is an $\mathbb{F}_q$ -linear vector space isomorphism. Furthermore, for any positive integer n , the map $\Phi_{\mathcal{B}}$ can be naturally extended to an $\mathbb{F}_q$ -linear vector space isomorphism from $\mathbb{F}_{q^t}^n$ onto $\mathbb{F}_q^{nt}$ as

$$a \mapsto \left(a_1^{(1)}, a_2^{(1)}, \dots, a_n^{(1)}, a_1^{(2)}, a_2^{(2)}, \dots, a_n^{(2)}, \dots, a_1^{(t)}, a_2^{(t)}, \dots, a_n^{(t)} \right)$$

for all $a = (a_1, a_2, \dots, a_n) \in \mathbb{F}_{q^t}^n$, where $a_i = a_i^{(1)}\mathbf{f}_1 + a_i^{(2)}\mathbf{f}_2 + \dots + a_i^{(t)}\mathbf{f}_t$ with $a_i^{(k)} \in \mathbb{F}_q$ for $1 \leq i \leq n$ and $1 \leq k \leq t$, which we shall denote by $\Phi_{\mathcal{B}}$ itself for the sake of simplicity. On the other hand, for any non-constant polynomial $g(x) \in \mathbb{F}_q[x]$ of degree d , the map $\Phi_{\mathcal{B}}$ can be naturally extended to an $\mathbb{F}_q$ -linear vector space isomorphism from $\frac{\mathbb{F}_{q^t}[x]}{\langle g(x) \rangle}$ onto $\left(\frac{\mathbb{F}_q[x]}{\langle g(x) \rangle} \right)^t$ as

$$a_0 + a_1x + \dots + a_{d-1}x^{d-1} \mapsto \left(a_0^{(1)} + a_1^{(1)}x + \dots + a_{d-1}^{(1)}x^{d-1}, a_0^{(2)} + a_1^{(2)}x + \dots + a_{d-1}^{(2)}x^{d-1}, \dots, a_0^{(t)} + a_1^{(t)}x + \dots + a_{d-1}^{(t)}x^{d-1} \right)$$

for all $a_0 + a_1x + \dots + a_{d-1}x^{d-1} \in \frac{\mathbb{F}_{q^t}[x]}{\langle g(x) \rangle}$, where $a_i = a_i^{(1)}\mathbf{f}_1 + a_i^{(2)}\mathbf{f}_2 + \dots + a_i^{(t)}\mathbf{f}_t \in \mathbb{F}_{q^t}$ with $a_i^{(k)} \in \mathbb{F}_q$ for $0 \leq i \leq d-1$ and $1 \leq k \leq t$, which we shall also denote by $\Phi_{\mathcal{B}}$ for the sake of simplicity.

We will next show that the isomorphism $\Phi_{\mathcal{B}}$ induces a one-to-one correspondence between MT additive codes over $\mathbb{F}_{q^t}$ and MT (linear) codes over $\mathbb{F}_q$, which are introduced and studied in [5, 18, 55, 56]. To establish this connection, let us define $\tilde{\Omega} = (\underbrace{\omega_1, \omega_1, \dots, \omega_1}_{t \text{ times}}, \underbrace{\omega_2, \omega_2, \dots, \omega_2}_{t \text{ times}}, \dots, \underbrace{\omega_\ell, \omega_\ell, \dots, \omega_\ell}_{t \text{ times}})$. Now let us define the map $S_{\tilde{\Omega}} : \mathbb{F}_q^{nt} \rightarrow \mathbb{F}_q^{nt}$ as

$$S_{\tilde{\Omega}}(\mathbf{a}) = \left(\omega_1 a_{1,m_1-1}^{(1)}, a_{1,0}^{(1)}, \dots, a_{1,m_1-2}^{(1)}; \dots; \omega_1 a_{1,m_1-1}^{(t)}, a_{1,0}^{(t)}, \dots, a_{1,m_1-2}^{(t)}; \right. \\ \omega_2 a_{2,m_2-1}^{(1)}, a_{2,0}^{(1)}, \dots, a_{2,m_2-2}^{(1)}; \dots; \omega_2 a_{2,m_2-1}^{(t)}, a_{2,0}^{(t)}, \dots, a_{2,m_2-2}^{(t)}; \dots; \\ \left. \omega_\ell a_{\ell,m_\ell-1}^{(1)}, a_{\ell,0}^{(1)}, \dots, a_{\ell,m_\ell-2}^{(1)}; \dots; \omega_\ell a_{\ell,m_\ell-1}^{(t)}, a_{\ell,0}^{(t)}, \dots, a_{\ell,m_\ell-2}^{(t)} \right)$$

for all

$$\mathbf{a} = \left(a_{1,0}^{(1)}, a_{1,1}^{(1)}, \dots, a_{1,m_1-1}^{(1)}; a_{1,0}^{(2)}, a_{1,1}^{(2)}, \dots, a_{1,m_1-1}^{(2)}; \dots; a_{1,0}^{(t)}, a_{1,1}^{(t)}, \dots, a_{1,m_1-1}^{(t)}; \right. \\ a_{2,0}^{(1)}, a_{2,1}^{(1)}, \dots, a_{2,m_2-1}^{(1)}; a_{2,0}^{(2)}, a_{2,1}^{(2)}, \dots, a_{2,m_2-1}^{(2)}; \dots; a_{2,0}^{(t)}, a_{2,1}^{(t)}, \dots, a_{2,m_2-1}^{(t)}; \dots; \\ \left. a_{\ell,0}^{(1)}, a_{\ell,1}^{(1)}, \dots, a_{\ell,m_\ell-1}^{(1)}; a_{\ell,0}^{(2)}, a_{\ell,1}^{(2)}, \dots, a_{\ell,m_\ell-1}^{(2)}; \dots; a_{\ell,0}^{(t)}, a_{\ell,1}^{(t)}, \dots, a_{\ell,m_\ell-1}^{(t)} \right) \in \mathbb{F}_q^{nt}.$$

It is easy to see that the map $S_{\tilde{\Omega}}$ is an $\mathbb{F}_q$ -linear vector space isomorphism and is called the $\tilde{\Omega}$ -MT shift operator on $\mathbb{F}_q^{nt}$.

Recall that a linear code $\mathcal{C}$ of length nt over $\mathbb{F}_q$ is called an $\tilde{\Omega}$ -MT (linear) code

of length nt and block lengths $(\underbrace{m_1, m_1, \dots, m_1}_{t \text{ times}}, \underbrace{m_2, m_2, \dots, m_2}_{t \text{ times}}, \dots, \underbrace{m_\ell, m_\ell, \dots, m_\ell}_{t \text{ times}})$ over $\mathbb{F}_q$ if it is invariant under the $\tilde{\Omega}$ -MT shift operator $S_{\tilde{\Omega}}$ on $\mathbb{F}_q^{nt}$, i.e., if it satisfies $S_{\tilde{\Omega}}(\mathcal{C}) = \mathcal{C}$. One can easily see that a non-empty subset $\mathcal{C}$ of $\mathbb{F}_q^{nt}$ is an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ if and only if its image $\Phi_{\mathcal{B}}(\mathcal{C}) (\subseteq \mathbb{F}_q^{nt})$ is an $\tilde{\Omega}$ -MT (linear) code of length nt and block lengths $(\underbrace{m_1, m_1, \dots, m_1}_{t \text{ times}}, \underbrace{m_2, m_2, \dots, m_2}_{t \text{ times}}, \dots, \underbrace{m_\ell, m_\ell, \dots, m_\ell}_{t \text{ times}})$ over $\mathbb{F}_q$. Working as in Section 3.2, one can view each $\tilde{\Omega}$ -MT (linear) code of length nt and block lengths $(\underbrace{m_1, m_1, \dots, m_1}_{t \text{ times}}, \underbrace{m_2, m_2, \dots, m_2}_{t \text{ times}}, \dots, \underbrace{m_\ell, m_\ell, \dots, m_\ell}_{t \text{ times}})$ over $\mathbb{F}_q$ as an $\mathbb{F}_q[x]$ -submodule (or an $\mathfrak{R}_M$ -submodule) of the $\tilde{\Omega}$ -MT module $\mathcal{S} = \prod_{i=1}^{\ell} \mathcal{S}_{m_i, \omega_i}^t$, where the quotient ring $\mathcal{S}_{m_i, \omega_i} = \frac{\mathbb{F}_q[x]}{\langle x^{m_i} - \omega_i \rangle}$ is the principal ideal ring for $1 \leq i \leq \ell$. We also recall, from Section 3.3, that $x^{m_i} - \omega_i = h_1(x)^{\epsilon_{1,i}} h_2(x)^{\epsilon_{2,i}} \dots h_s(x)^{\epsilon_{s,i}}$ is the irreducible factorization of the polynomial $x^{m_i} - \omega_i$ over $\mathbb{F}_q$ for $1 \leq i \leq \ell$ and that $\mathcal{F}_\nu = \frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle} \simeq \mathbb{F}_{q^{d_\nu}}$ for $1 \leq \nu \leq s$. By applying the Chinese Remainder Theorem again [7, Th. 1.2.12], we obtain

$$\mathcal{S} \simeq \bigoplus_{\nu=1}^s \underbrace{(\epsilon_{\nu,1} \mathcal{F}_\nu^t, \epsilon_{\nu,2} \mathcal{F}_\nu^t, \dots, \epsilon_{\nu,\ell} \mathcal{F}_\nu^t)}_{\mathbb{J}_\nu} = \bigoplus_{\nu=1}^s \mathbb{J}_\nu = \mathbb{J}.$$

One can easily see that $\Phi_{\mathcal{B}}\left(\frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle}\right) = \left(\frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle}\right)^t = \mathcal{F}_\nu^t$ and $\Phi_{\mathcal{B}}(\mathbb{G}_\nu) = \mathbb{J}_\nu$ for $1 \leq \nu \leq s$, which gives $\Phi_{\mathcal{B}}(\mathbb{G}) = \mathbb{J}$.

Now the following theorem provides a trace description of all Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Theorem 3.4.1. *For $1 \leq \nu \leq s$, let $y_\nu = (y_{\nu,1}, y_{\nu,2}, \dots, y_{\nu,\ell}) \in \mathbb{G}_\nu$ and $\hat{y}_\nu = \Phi_{\mathcal{B}}(y_\nu) = (y_{\nu,1}^{(1)}, y_{\nu,1}^{(2)}, \dots, y_{\nu,1}^{(t)}, y_{\nu,2}^{(1)}, y_{\nu,2}^{(2)}, \dots, y_{\nu,2}^{(t)}, \dots, y_{\nu,\ell}^{(1)}, y_{\nu,\ell}^{(2)}, \dots, y_{\nu,\ell}^{(t)}) \in \mathbb{J}_\nu$, and let us define*

$$c_i(y_1, y_2, \dots, y_s) = \frac{1}{m_i} \left(\sum_{k=1}^t \sum_{\nu=1}^s \text{Tr}_{q^{d_\nu}, q}(y_{\nu,i}^{(k)}) \mathbf{f}_k, \sum_{k=1}^t \sum_{\nu=1}^s \text{Tr}_{q^{d_\nu}, q}(y_{\nu,i}^{(k)} \theta_\nu^{-1}) \mathbf{f}_k, \dots, \sum_{k=1}^t \sum_{\nu=1}^s \text{Tr}_{q^{d_\nu}, q}(y_{\nu,i}^{(k)} \theta_\nu^{-(m_i-1)}) \mathbf{f}_k \right)$$

for $1 \leq i \leq \ell$, where $\theta_\nu \in \mathcal{F}_\nu$ is a root of the irreducible polynomial $h_\nu(x)$ for $1 \leq \nu \leq s$. Let $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with the constituents $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_s$. Then the code $\mathcal{C}$ has a trace description

$$\mathcal{C} = \left\{ (c_1(y_1, y_2, \dots, y_s), c_2(y_1, y_2, \dots, y_s), \dots, c_\ell(y_1, y_2, \dots, y_s)) : y_\nu \in \mathcal{C}_\nu \text{ for } 1 \leq \nu \leq s \right\}.$$

Proof. To prove the result, we see that $\Phi_{\mathcal{B}}(\mathcal{C}) = \bigoplus_{\nu=1}^s \Phi_{\mathcal{B}}(\mathcal{C}_\nu)$ is an $\tilde{\Omega}$ -MT (linear) code of length nt and block lengths $(\underbrace{m_1, m_1, \dots, m_1}_{t \text{ times}}, \underbrace{m_2, m_2, \dots, m_2}_{t \text{ times}}, \dots, \underbrace{m_\ell, m_\ell, \dots, m_\ell}_{t \text{ times}})$ over $\mathbb{F}_q$, where $\Phi_{\mathcal{B}}(\mathcal{C}_\nu)$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{J}_\nu$ for $1 \leq \nu \leq s$. By applying Theorem 6.2 of Sharma *et al.* [56] and using the map $\Phi_{\mathcal{B}}$, the desired result follows. $\square$

In the next section, we will show that MT additive codes over finite fields are asymptotically good.

3.5 MT additive codes over finite fields are asymptotically good

In this section, we will consider a special class of MT additive codes over $\mathbb{F}_{q^t}$ and show that it is asymptotically good by applying probabilistic methods. For this, we assume, throughout this section, that ω is a non-zero element of $\mathbb{F}_q$ with $\text{ord}(\omega) = e$, p is an odd prime coprime to q such that $p \nmid e$, α is a positive integer and $m = p^\alpha$. Further, let us suppose that $m_1 = m_2 = \dots = m_\ell = m = p^\alpha$ and $\omega_1 = \omega_2 = \dots = \omega_\ell = \omega$. In this case, we have $n = m\ell = p^\alpha \ell$ and $M = me = p^\alpha e$. We also note that $\epsilon_{\nu,i} = 1$ for $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$, which implies that $x^m - \omega = h_1(x)h_2(x) \cdots h_s(x)$ is the irreducible factorization of the polynomial $x^m - \omega$ over $\mathbb{F}_q$. Since $p \nmid e$, we see, by Theorem 3.75 of [43], that the polynomial $x^m - \omega$ is reducible over $\mathbb{F}_q$, which implies that $s \geq 2$. Now let ξ be a fixed primitive (me) -th root of unity in an extension field of $\mathbb{F}_q$ satisfying $\xi^m = \omega$. Such an element ξ exists, as $\gcd(me, q) = 1$ and $\text{ord}(\omega) = e$. Since ξ is a root of $x^m - \omega$, the minimal polynomial of ξ over $\mathbb{F}_q$ is a factor of the polynomial $x^m - \omega$ over $\mathbb{F}_q$. One can easily observe that the degree of the minimal polynomial of ξ is equal to the multiplicative order $\text{ord}_{me}(q)$

of q modulo me . Without any loss of generality, let $h_1(x)$ be the minimal polynomial of ξ over $\mathbb{F}_q$. Note that $\deg h_1(x) = d_1 = \text{ord}_{me}(q)$. Now let us suppose, throughout this section, that $v = \text{ord}_p(q)$. So we can write $q^v = 1 + p^\eta c$, where $\eta \geq 1$ and c are integers such that $p \nmid c$. Since $\omega \in \mathbb{F}_q$ and $\text{ord}(\omega) = e$, we see that e divides $q - 1$, which implies that $\text{ord}_e(q) = 1$. Since $p \nmid e$, we note that $\gcd(m, e) = \gcd(p^\alpha, e) = 1$. This implies that $\text{ord}_{me}(q) = \text{lcm}[\text{ord}_m(q), \text{ord}_e(q)] = \text{ord}_m(q)$. Further, one can easily observe that

$$d_1 = \text{ord}_m(q) = \text{ord}_{p^\alpha}(q) = \begin{cases} v & \text{if } \alpha \leq \eta; \\ vp^{\alpha-\eta} & \text{if } \alpha \geq \eta + 1. \end{cases} \quad (3.2)$$

From this point on, let us assume that the integer α satisfies $\alpha \geq \eta + 1$, which implies that

$$\deg h_1(x) = d_1 = vp^{\alpha-\eta} > 1. \quad (3.3)$$

From now on, throughout this section, we will refer to an Ω -MT additive code of length $n = m\ell$ and block lengths $\underbrace{(m, m, \dots, m)}_{\ell \text{ times}}$ over $\mathbb{F}_{q^t}$ simply as an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, where $\Omega = \underbrace{(\omega, \omega, \dots, \omega)}_{\ell \text{ times}}$. We will further restrict our attention to a special class of 1-generator MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ on which our probabilistic methods can work well.

Next, let $d_\nu = \deg h_\nu(x)$ for $1 \leq \nu \leq s$. We recall, from Section [3.3](#), that

$$\mathcal{R} = \mathcal{R}_{m,\omega}^\ell \simeq \bigoplus_{\nu=1}^s \mathbb{W}_\nu^\ell = \bigoplus_{\nu=1}^s \mathbb{G}_\nu = \mathbb{G},$$

where $\mathbb{W}_\nu = \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}$ and $\mathcal{F}_\nu = \frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle} \simeq \mathbb{F}_{q^{d_\nu}}$ for $1 \leq \nu \leq s$. Further, we note that $\mathbb{G}_\nu = \mathbb{W}_\nu^\ell$ is an (ℓt) -dimensional vector space over $\mathcal{F}_\nu$ for $1 \leq \nu \leq s$. By Theorem [3.3.1](#), we see that each $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ is an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$. To show that MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ are asymptotically good, we will study $\mathcal{F}_\nu$ -subspaces of $\mathbb{G}_\nu$.

First of all, we will construct a class of MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ having exactly one non-zero constituent and show that it

is asymptotically good by using probabilistic methods. For this, let $\mathcal{C}_1$ be an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$, and let $\mathcal{C}_\nu = \{\mathbf{0}\}$ for $2 \leq \nu \leq s$. By Theorem 3.3.1, we see that the corresponding code $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu = \mathcal{C}_1$ is an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$. Now we will consider a special class of 1-generator MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ generated by the elements of $\mathbb{G}_1$. To do this, let $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in \mathbb{G}_1$ be fixed. Corresponding to the element $A(x) \in \mathbb{G}_1$, let us define the set

$$\mathcal{C}_A = \{f(x)A(x) = (f(x)A_1(x), f(x)A_2(x), \dots, f(x)A_\ell(x)) : f(x) \in \mathcal{F}_1\}. \quad (3.4)$$

It is easy to observe that the set $\mathcal{C}_A$ is an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$, and hence is an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, generated by the element $A(x) \in \mathbb{G}_1$. Now we have the following lemma.

Lemma 3.5.1. *Let $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in \mathbb{G}_1$ be fixed, and let $\mathcal{C}_A$ be the corresponding MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by (3.4). Then we have $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A \leq \frac{d_1}{t}$. Moreover, we have $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A < \frac{d_1}{t}$ if and only if the polynomial $h_1(x)$ divides $A_i(x)$ for $1 \leq i \leq \ell$.*

Proof. As $\deg h_1(x) = d_1$, we note that $\mathcal{F}_1 = \frac{\mathbb{F}_q[x]}{\langle h_1(x) \rangle} \simeq \mathbb{F}_{q^{d_1}}$. We further note that $\mathcal{C}_A$ is an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ generated by the element $A(x)$, which implies that $|\mathcal{C}_A| \leq q^{\deg h_1(x)} = q^{d_1}$. We further observe that

$$\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \log_{q^t} |\mathcal{C}_A| = \frac{\log_q |\mathcal{C}_A|}{t} \leq \frac{\log_q |q^{\deg h_1(x)}|}{t} = \frac{\deg h_1(x)}{t} = \frac{d_1}{t}.$$

To prove the second part, we observe, for any two distinct elements $f(x), g(x) \in \mathcal{F}_1$, that $f(x)A(x) = g(x)A(x)$ holds if and only if $f(x)A_i(x) = g(x)A_i(x)$ for $1 \leq i \leq \ell$. This holds if and only if $(f(x) - g(x))A_i(x) \equiv \mathbf{0} \pmod{h_1(x)}$ for all i , which further holds if and only if the polynomial $h_1(x)$ divides $A_i(x)$ for $1 \leq i \leq \ell$. From this, the desired result follows. $\square$

To study the asymptotic properties of MT additive codes of length $m\ell$ over $\mathbb{F}_{q^t}$, we will view the set $\mathbb{G}_1$ as a sample space, where each sample of $\mathbb{G}_1$ is chosen with equal probability. In fact, corresponding to each sample $A(x) = (A_1(x), A_2(x), \dots,$

$A_\ell(x)) \in \mathbb{G}_1$, we have a random MT additive code $\mathcal{C}_A$ over the probability space $\mathbb{G}_1$, which is given by the following:

$$\mathcal{C}_A = \{f(x)A(x) = (f(x)A_1(x), f(x)A_2(x), \dots, f(x)A_\ell(x)) : f(x) \in \mathcal{F}_1\} \subseteq \mathbb{G}_1. \quad (3.5)$$

Moreover, the dimension $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A$ and the relative Hamming distance $\Delta(\mathcal{C}_A)$ of the random code $\mathcal{C}_A$ are random variables over the probability space $\mathbb{G}_1$ with uniform probability. In this section, we will study the asymptotic behaviour of the probabilities $\Pr(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \frac{d_1}{t})$ and $\Pr(\Delta(\mathcal{C}_A) > \delta)$, where δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$.

To do this, we assume, throughout this section, that δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$. Further, let $\mathcal{N}_{\mathcal{C}_A}(\delta)$ denote the number of non-zero codewords in $\mathcal{C}_A$ with relative Hamming weight at most δ . Note that $\mathcal{N}_{\mathcal{C}_A}(\delta)$ is a non-negative integral random variable defined over the probability space $\mathbb{G}_1$ and is given by

$$\mathcal{N}_{\mathcal{C}_A}(\delta) = |\{f(x) \in \mathcal{F}_1 : 0 < \widehat{wt}(f(x)A(x)) \leq \delta\}|. \quad (3.6)$$

The random variable $\mathcal{N}_{\mathcal{C}_A}(\delta)$ is called the *cumulative weight enumerator* for the random code $\mathcal{C}_A$ (see Fan *et al.* [25]). Now for each $f(x) \in \mathcal{F}_1$ and samples $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in \mathbb{G}_1$, let us define the *indicator random variable* X_f as

$$X_f = \begin{cases} 1 & \text{if } 0 < \widehat{wt}(f(x)A(x)) \leq \delta; \\ 0 & \text{otherwise.} \end{cases} \quad (3.7)$$

Note that X_f is a Bernoulli random variable defined over the probability space $\mathbb{G}_1$. It is easy to see that $X_0 = 0$ and that

$$\mathcal{N}_{\mathcal{C}_A}(\delta) = \sum_{f(x) \neq 0 \in \mathcal{F}_1} X_f.$$

Now for a given $f(x) \in \mathcal{F}_1$, let I_f be an ideal of $\mathcal{R}_{m,\omega}$ generated by $f(x)$, *i.e.*,

$$I_f = \langle f(x) \rangle_{\mathcal{R}_{m,\omega}} = \{f(x)b(x) : b(x) \in \mathcal{R}_{m,\omega}\} = \{f(x)b_1(x) : b_1(x) \in \mathbb{W}_1\}. \quad (3.8)$$

If $f(x)$ is non-zero, then one can easily see that $|I_f| = q^{td_1} = |\mathbb{W}_1|$, which implies

that $I_f = \mathbb{W}_1$. We also note that $\dim_{\mathbb{F}_{q^t}} I_f = \log_{q^t} |I_f| = d_1$.

Lemma 3.5.2. *For a non-zero $f(x) \in \mathcal{F}_1$, the ideal $I_f = \langle f(x) \rangle_{\mathcal{R}_{m,\omega}}$ is a balanced code of length m and dimension d_1 over $\mathbb{F}_{q^t}$.*

Proof. To prove the result, we first observe that $I_f = \langle f(x) \rangle_{\mathcal{R}_{m,\omega}} = \mathbb{W}_1 \simeq \left\langle \frac{x^m - \omega}{h_1(x)} \right\rangle_{\mathcal{R}_{m,\omega}}$ is an ω -constacyclic code of length m and dimension d_1 over $\mathbb{F}_{q^t}$. Now let us write

$$k(x) = \frac{x^m - \omega}{h_1(x)} = k_0 + k_1x + k_2x^2 + \cdots + k_{m-d_1}x^{m-d_1},$$

where $k_0, k_1, \dots, k_{m-d_1} \in \mathbb{F}_q$. It is easy to see that $k_0 \neq 0$. One can easily observe that the set $G_0 = \{k(x), xk(x), \dots, x^{d_1-1}k(x)\}$ is a basis set of I_f . Since k_0 is non-zero, the set $S_0 = \{0, 1, 2, \dots, d_1 - 1\}$ is the information set of I_f corresponding to the basis set G_0 . Further, one can easily observe, for $1 \leq j \leq m - 1$, that the set $G_j = \{x^j k(x), x^{j+1}k(x), x^{j+2}k(x), \dots, x^{j+d_1-1}k(x)\}$ is also a basis set of I_f and that the set $S_j = \{j, j+1, j+2, \dots, j+d_1-1\}$ (modulo m) is the information set corresponding to the basis set G_j . Furthermore, for each index $i \in \{0, 1, 2, \dots, m-1\}$, we see that $|\{j : 0 \leq j \leq m-1 \text{ and } i \in S_j\}| = d_1$. We next observe that for $0 \leq j \leq m-1$, the projection map $\rho_j : I_f \rightarrow \mathbb{F}_{q^t}^{S_j}$ is a bijection. From this, it follows that the ideal I_f is a balanced code. We further observe that $\dim_{\mathbb{F}_{q^t}} I_f = \log_{q^t} |I_f| = d_1$, which completes the proof. $\square$

Lemma 3.5.3. *Let $f(x) \in \mathcal{F}_1$ be fixed. For $I_f^\ell \subseteq \mathbb{W}_1^\ell = \mathbb{G}_1$, let us define*

$$(I_f^\ell)^{\leq \delta} = \left\{ (\kappa_1(x), \kappa_2(x), \dots, \kappa_\ell(x)) \in I_f^\ell : \widehat{wt}(\kappa_1(x), \kappa_2(x), \dots, \kappa_\ell(x)) \leq \delta \right\}.$$

We have

$$|(I_f^\ell)^{\leq \delta}| \leq q^{\ell t d_1 h_{q^t}(\delta)}.$$

Proof. To prove the result, we see that if $f(x) = 0$, then I_f is a zero code of length m over $\mathbb{F}_{q^t}$. This implies that I_f^ℓ is also a zero code of length $m\ell$ over $\mathbb{F}_{q^t}$, which gives $(I_f^\ell)^{\leq \delta} = I_f^\ell = \{\mathbf{0}\}$. Therefore, we have $|(I_f^\ell)^{\leq \delta}| = 1 \leq q^{\ell t d_1 h_{q^t}(\delta)}$. On the other hand, when $f(x)$ is non-zero, we see, by Lemma 3.5.2, that the ideal I_f is a balanced code of length m and dimension d_1 over $\mathbb{F}_{q^t}$. This, by Theorem 2.1.4, implies that the set I_f^ℓ is a balanced code of length $m\ell$ and dimension ℓd_1 over $\mathbb{F}_{q^t}$. We further observe

that the relative Hamming weight of each non-zero codeword of $(I_f^\ell)^{\leq \delta}$ is at most δ . Now by applying Theorem 2.1.4 again, we get $| (I_f^\ell)^{\leq \delta} | \leq q^{\ell t d_1 h_{q^t}(\delta)}$. $\square$

We further observe the following.

Lemma 3.5.4. *For a given $f(x) \in \mathcal{F}_1$, let $E(X_f)$ denote the expectation of the indicator random variable X_f . We have*

$$E(X_f) \leq q^{-\ell t d_1 (1 - h_{q^t}(\delta))}.$$

Proof. Since X_f is a Bernoulli random variable over the probability space $\mathbb{G}_1$, the expectation of X_f is given by

$$E(X_f) = \Pr(X_f = 1) = \frac{| (I_f^\ell)^{\leq \delta} | - 1}{| I_f^\ell |} < \frac{q^{\ell t d_1 h_{q^t}(\delta)}}{q^{\ell t d_1}} = q^{-\ell t d_1 (1 - h_{q^t}(\delta))}.$$

$\square$

We next make the following observation.

Lemma 3.5.5. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$. For $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in \mathbb{G}_1$, let $\mathcal{C}_A$ be the MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by (3.5). We have*

$$\Pr(\Delta(\mathcal{C}_A) \leq \delta) \leq q^{-\ell t d_1 (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}.$$

Proof. Let us define $X = \sum_{f(x) \in \mathcal{F}_1} X_f$. By (3.6) and (3.7), we see that

$$X = \sum_{f(x) \in \mathcal{F}_1} X_f = \mathcal{N}_{\mathcal{C}_A}(\delta).$$

This implies that X equals the number of elements $f(x) \in \mathcal{F}_1$ such that the corresponding non-zero codeword $f(x)A(x) \in \mathcal{C}_A$ has relative Hamming weight at most δ . From this, it follows that

$$\Pr(\Delta(\mathcal{C}_A) \leq \delta) = \Pr(X > 0).$$

Now by Theorem 2.3.2, we see that $\Pr(X > 0) \leq E(X)$, which implies, by Theorem 2.3.1, that

$$\Pr(\Delta(\mathcal{C}_A) \leq \delta) = \Pr(X > 0) \leq E(X) = E\left(\sum_{f(x) \in \mathcal{F}_1} X_f\right) = \sum_{f(x) \in \mathcal{F}_1} E(X_f).$$

By Lemma 3.5.4, we get

$$E(X) \leq \sum_{f(x) \in \mathcal{F}_1} q^{-\ell t d_1(1-h_{q^t}(\delta))} = q^{d_1} q^{-\ell t d_1(1-h_{q^t}(\delta))} = q^{-\ell t d_1(1-\frac{1}{\ell t}-h_{q^t}(\delta))}.$$

□

For a given prime power q , we see that there exists an odd prime p satisfying $\gcd(p, q) = \gcd(p, e) = 1$. Furthermore, there exists a strictly increasing infinite sequence $\{\alpha_j\}_{j \geq 1}$ of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Note that $\lim_{j \rightarrow \infty} \{\alpha_j\} = \infty$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for each positive integer j . Note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. For $j \geq 1$, let $x^{\mathbf{m}_j} - \omega = h_1^{(j)}(x)h_2^{(j)}(x) \cdots h_{s_j}^{(j)}(x)$ be the irreducible factorization of the polynomial $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$. For $j \geq 1$ and $1 \leq \nu_j \leq s_j$, let $d_{\nu_j}^{(j)} = \deg h_{\nu_j}^{(j)}(x)$. Further, for each positive integer j , let ξ_j be a primitive $(\mathbf{m}_j e)$ -th root of unity in some field extension of $\mathbb{F}_q$ satisfying $\xi_j^{\mathbf{m}_j} = \omega$, and let $h_1^{(j)}(x)$ be the minimal polynomial of ξ_j over $\mathbb{F}_q$. Since $\gcd(\mathbf{m}_j, e) = 1$ and $\text{ord}_e(q) = 1$, we see, by (3.3), that

$$d_1^{(j)} = \deg h_1^{(j)}(x) = \text{ord}_{\mathbf{m}_j e}(q) = \text{lcm}[\text{ord}_{\mathbf{m}_j}(q), \text{ord}_e(q)] = \text{ord}_{\mathbf{m}_j}(q) = v p^{\alpha_j - \eta}$$

for all $j \geq 1$. Next, for each $j \geq 1$, let us define

$$\mathcal{F}_1^{(j)} = \frac{\mathbb{F}_q[x]}{\langle h_1^{(j)}(x) \rangle} \simeq \mathbb{F}_{q^{d_1^{(j)}}} \quad \text{and} \quad \mathbb{G}_1^{(j)} = \left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle} \right)^\ell.$$

For each $j \geq 1$, we shall view the set $\mathbb{G}_1^{(j)}$ as a probability space, where each sample is chosen with equal probability. Now for each positive integer j and each sample $A^{(j)}(x) = (A_1^{(j)}(x), A_2^{(j)}(x), \dots, A_\ell^{(j)}(x)) \in \mathbb{G}_1^{(j)}$, let

$$\mathcal{C}_{A^{(j)}} = \left\{ f^{(j)}(x) A^{(j)}(x) = \left(f^{(j)}(x) A_1^{(j)}(x), \dots, f^{(j)}(x) A_\ell^{(j)}(x) \right) : f^{(j)}(x) \in \mathcal{F}_1^{(j)} \right\} \quad (3.9)$$

be a random MT additive code of length $\mathbf{m}_j \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ defined over the probability space $\mathbb{G}_1^{(j)}$.

Theorem 3.5.1. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. If δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) > \delta \right) \right\} = 1.$$

Proof. As $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, we have $1 - \frac{1}{\ell t} - h_{q^t}(\delta) > 0$. Here we recall that $d_1^{(j)} = \text{ord}_{\mathbf{m}_j}(q) = vp^{\alpha_j - \eta}$. Now by Lemma 3.5.5, we see that

$$\lim_{j \rightarrow \infty} \left\{ \Pr(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta) \right\} \leq \lim_{j \rightarrow \infty} \left\{ q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))} \right\}.$$

Since $\lim_{j \rightarrow \infty} \{\alpha_j\} = \infty$, we have $\lim_{j \rightarrow \infty} \{vp^{\alpha_j - \eta}\} = \infty$, which implies that

$$\lim_{j \rightarrow \infty} \left\{ q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))} \right\} = 0.$$

This gives $\lim_{j \rightarrow \infty} \left\{ \Pr(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta) \right\} = 0$. From this, it follows that

$$\lim_{j \rightarrow \infty} \left\{ \Pr(\Delta(\mathcal{C}_{A^{(j)}}) > \delta) \right\} = 1 - \lim_{j \rightarrow \infty} \left\{ \Pr(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta) \right\} = 1.$$

□

Theorem 3.5.2. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let $\mathbf{m}_j = p^{\alpha_j}$, and let $\mathcal{C}_{A^{(j)}}$ be as defined by (3.9) for each positive integer j . Then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{d_1^{(j)}}{t} = \frac{vp^{\alpha_j - \eta}}{t} \right) \right\} = 1.$$

Proof. Since $x^{\mathbf{m}_j} - \omega = h_1^{(j)}(x)h_2^{(j)}(x) \cdots h_{s_j}^{(j)}(x)$ is the irreducible factorization of the

polynomial $x^{m_j} - \omega$ over $\mathbb{F}_q$, by Lemma 1 of Huffman [34], we see that

$$x^{m_j} - \omega = \prod_{\nu_j=1}^{s_j} h_{\nu_j,0}^{(j)}(x) h_{\nu_j,1}^{(j)}(x) \cdots h_{\nu_j, \kappa_{\nu_j}^{(j)}-1}^{(j)}(x)$$

is the irreducible factorization of the polynomial $x^{m_j} - \omega$ over $\mathbb{F}_{q^t}$, where $\kappa_{\nu_j}^{(j)} = \gcd(t, \deg h_{\nu_j}^{(j)}(x))$ for $1 \leq \nu_j \leq s_j$. Further, for $0 \leq u \leq \kappa_1^{(j)} - 1$, we note that $\deg h_{1,u}^{(j)}(x) = D_1^{(j)} = \frac{d_1^{(j)}}{\kappa_1^{(j)}}$. Now by applying the Chinese Remainder Theorem [7, Th. 1.2.12], we get

$$\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle} \cong \underbrace{\left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_{1,0}^{(j)}(x) \rangle} \oplus \frac{\mathbb{F}_{q^t}[x]}{\langle h_{1,1}^{(j)}(x) \rangle} \oplus \cdots \oplus \frac{\mathbb{F}_{q^t}[x]}{\langle h_{1, \kappa_1^{(j)}-1}^{(j)}(x) \rangle} \right)}_{\mathcal{U}_1^{(j)}},$$

where the corresponding ring isomorphism from $\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle}$ onto $\mathcal{U}_1^{(j)}$ is given by

$$b(x) \mapsto \left(b(x) + \langle h_{1,0}^{(j)}(x) \rangle, b(x) + \langle h_{1,1}^{(j)}(x) \rangle, \dots, b(x) + \langle h_{1, \kappa_1^{(j)}-1}^{(j)}(x) \rangle \right)$$

for all $b(x) \in \frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle}$. Further, by Lemma 3.5.1, we see that $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} < \frac{d_1^{(j)}}{t}$ if and only if the polynomial $h_1^{(j)}(x)$ is a common divisor of $A_1^{(j)}(x), A_2^{(j)}(x), \dots, A_\ell^{(j)}(x)$, which holds if and only if

$$A_1^{(j)}(x) + \langle h_{1,u}^{(j)}(x) \rangle = A_2^{(j)}(x) + \langle h_{1,u}^{(j)}(x) \rangle = \cdots = A_\ell^{(j)}(x) + \langle h_{1,u}^{(j)}(x) \rangle = 0$$

in $\frac{\mathbb{F}_{q^t}[x]}{\langle h_{1,u}^{(j)}(x) \rangle}$ for $0 \leq u \leq \kappa_1^{(j)} - 1$. In other words, we see that $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{d_1^{(j)}}{t}$ if and only if

$$\begin{aligned} & \left(A_1^{(j)}(x) + \langle h_{1,0}^{(j)}(x) \rangle, A_1^{(j)}(x) + \langle h_{1,1}^{(j)}(x) \rangle, \dots, A_1^{(j)}(x) + \langle h_{1, \kappa_1^{(j)}-1}^{(j)}(x) \rangle, \right. \\ & A_2^{(j)}(x) + \langle h_{1,0}^{(j)}(x) \rangle, A_2^{(j)}(x) + \langle h_{1,1}^{(j)}(x) \rangle, \dots, A_2^{(j)}(x) + \langle h_{1, \kappa_1^{(j)}-1}^{(j)}(x) \rangle, \dots, \\ & \left. A_\ell^{(j)}(x) + \langle h_{1,0}^{(j)}(x) \rangle, A_\ell^{(j)}(x) + \langle h_{1,1}^{(j)}(x) \rangle, \dots, A_\ell^{(j)}(x) + \langle h_{1, \kappa_1^{(j)}-1}^{(j)}(x) \rangle \right) \neq \mathbf{0}. \quad (3.10) \end{aligned}$$

Further, since $\deg h_{1,u}^{(j)}(x) = D_1^{(j)} = \frac{d_1^{(j)}}{\kappa_1^{(j)}}$ for $0 \leq u \leq \kappa_1^{(j)} - 1$, one can observe that $\frac{\mathbb{F}_{q^t}[x]}{\langle h_{1,u}^{(j)}(x) \rangle} \cong \mathbb{F}_{q^{tD_1^{(j)}}}$. In view of this, we see that the probability that (3.10) holds is given by

$$\frac{q^{\ell t D_1^{(j)} \kappa_1^{(j)}} - 1}{q^{\ell t D_1^{(j)} \kappa_1^{(j)}}} = \frac{q^{\ell t d_1^{(j)}} - 1}{q^{\ell t d_1^{(j)}}} = 1 - q^{-\ell t d_1^{(j)}},$$

which does not depend on the choice of the sample $A^{(j)}(x) \in \mathbb{G}_1^{(j)}$. From this, it follows that

$$\Pr \left(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{d_1^{(j)}}{t} = \frac{vp^{\alpha_j - \eta}}{t} \right) = 1 - q^{-\ell t v p^{\alpha_j - \eta}}.$$

This further implies that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{vp^{\alpha_j - \eta}}{t} \right) \right\} = \lim_{j \rightarrow \infty} \left\{ 1 - q^{-\ell t v p^{\alpha_j - \eta}} \right\} = 1 - 0 = 1.$$

□

In the following theorem, we establish the existence of an infinite family of MT additive codes over $\mathbb{F}_{q^t}$ with rate $\frac{v}{p^n \ell t}$ and relative Hamming distance at least δ , where δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$.

Theorem 3.5.3. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$. There exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of MT additive codes $\mathcal{C}_j$'s of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$, block length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that*

$$(i) \ R_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{R(\mathcal{C}_j)\} = \frac{v}{p^n \ell t} \text{ and}$$

$$(ii) \ \Delta_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{\Delta(\mathcal{C}_j)\} > \delta.$$

Proof. To prove the result, we see, by Theorem 3.5.2, that there exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of MT additive codes $\mathcal{C}_j$ of length $p^{\alpha_j} \ell$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$. Further, for each positive integer j , the rate of the MT additive code $\mathcal{C}_j$ is given by

$$R(\mathcal{C}_j) = \frac{\dim_{\mathbb{F}_{q^t}} \mathcal{C}_j}{\mathbf{m}_j \ell} = \frac{vp^{\alpha_j - \eta}}{p^{\alpha_j} \ell t} = \frac{v}{p^n \ell t}.$$

From this, it follows that the rate $R_{\mathfrak{F}}$ of the sequence $\mathfrak{F}$ is given by

$$R_{\mathfrak{F}} = \limsup_{j \rightarrow \infty} \{R(\mathcal{C}_j)\} = \limsup_{j \rightarrow \infty} \left\{ \frac{v}{p^n \ell t} \right\} = \frac{v}{p^n \ell t}.$$

Now the desired result follows immediately by applying Theorem [3.5.1](#). $\square$

From the above theorem, it follows that the family of MT additive codes over finite fields is asymptotically good. Now as a consequence of the above theorem, we deduce, in the following corollary, that the family of ω -constacyclic additive codes of prime power length m over $\mathbb{F}_{q^t}$ is asymptotically good when the polynomial $x^m - \omega$ is reducible over $\mathbb{F}_q$, where $\gcd(m, q) = 1$.

Corollary 3.5.1. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{t}$. There exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of constacyclic additive codes $\mathcal{C}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that*

$$(i) \ R_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{R(\mathcal{C}_j)\} = \frac{v}{p^n t} \text{ and}$$

$$(ii) \ \Delta_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{\Delta(\mathcal{C}_j)\} > \delta.$$

Proof. On taking $\ell = 1$ in Theorem [3.5.3](#), we get the desired result. $\square$

In the following corollary, we show that the family of cyclic additive codes over finite fields is asymptotically good without applying Chebyshev's Theorem and without assuming the unresolved Artin's conjecture on primitive roots.

Corollary 3.5.2. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{t}$. There exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of cyclic additive codes $\mathcal{C}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that*

$$(i) \ R_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{R(\mathcal{C}_j)\} = \frac{v}{p^n t} \text{ and}$$

$$(ii) \ \Delta_{\mathfrak{F}} = \lim_{j \rightarrow \infty} \{\Delta(\mathcal{C}_j)\} > \delta.$$

Proof. On taking $\ell = 1$ and $\omega = 1$ in Theorem [3.5.3](#), the desired result follows. $\square$

Example 3.5.1. Let $q = 11$, $p = 13$, $\omega = -1$, $\ell = 1$ and $t = 2$. Here we have $v = \text{ord}_p(q) = \text{ord}_{13}(11) = 12$ and $\eta = 1$. By Theorem [3.5.3](#), we see that there exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of ω -constacyclic additive codes $\mathcal{C}_j$'s of length 13^{α_j} over $\mathbb{F}_{11^2}$ such that $\lim_{j \rightarrow \infty} \{13^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = \frac{v}{p^{\eta}t} = \frac{6}{13}$ and $\Delta_{\mathfrak{F}} > \delta$, where δ is a positive real number satisfying $\delta < 0.364$.

In the next chapter, we will study the dual codes of MT additive codes over finite fields with respect to ordinary, Hermitian and $*$ trace bilinear forms. We will express the constituents of the dual codes of MT additive codes in terms of the constituents of the code. We further apply this result to characterize all MT additive self-orthogonal codes, MT additive self-dual codes, and MT additive codes with complementary duals (MT ACD codes) with respect to the aforementioned trace bilinear forms.

4

Characterization of self-orthogonal, self-dual and ACD multi-twisted additive codes

4.1 Introduction

In this chapter, we study dual codes of Ω -MT additive codes of length $n = m_1 + m_2 + \dots + m_\ell$ and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ by placing ordinary, Hermitian and $*$ trace bilinear forms on $\mathbb{F}_{q^t}^n$, where $m_1, m_2, \dots, m_\ell$ are positive integers coprime to q and $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ with $\omega_1, \omega_2, \dots, \omega_\ell \in \mathbb{F}_q \setminus \{0\}$. We also derive necessary and sufficient conditions under which an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is (i) self-orthogonal, (ii) self-dual and (iii) an additive code with complementary dual (or an ACD code) with respect to the aforementioned trace bilinear forms.

This chapter is structured as follows: In Section 4.2, we study dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with respect to ordinary, Hermitian and $*$ trace bilinear forms. In Section 4.3, we provide a canonical form decomposition of the dual code of each Ω -MT additive code by relating the constituents of the dual code with that of the code (Theorem 4.3.1). In Section 4.4, we further apply this result to derive necessary and sufficient conditions under which an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is (i) self-orthogonal, (ii) self-dual and (iii) additive with complementary dual (ACD code) with respect to the aforementioned trace bilinear forms (Theorem 4.4.1).

4.2 Dual codes of MT additive codes

In this section, we will study dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ by placing three different trace bilinear forms, *viz.* ordinary, Hermitian and $*$ trace bilinear forms on $\mathbb{F}_{q^t}^n$. To define these three trace bilinear forms, let $\text{Tr}_{q^t, q}$ be the trace map from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$, defined as

$$\text{Tr}_{q^t, q}(\beta) = \beta + \beta^q + \dots + \beta^{q^{t-1}} \text{ for all } \beta \in \mathbb{F}_{q^t}.$$

Note that the trace map $\text{Tr}_{q^t, q}$ is non-zero and onto. We next recall, from Section 3.2, that each element $a \in \mathbb{F}_{q^t}^n$ is represented as $a = (a_{1,0}, a_{1,1}, \dots, a_{1,m_1-1}; a_{2,0}, a_{2,1}, \dots, a_{2,m_2-1}; \dots; a_{\ell,0}, a_{\ell,1}, \dots, a_{\ell,m_\ell-1})$ throughout this thesis.

The *ordinary trace bilinear form* on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_0 : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_0 = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} \text{Tr}_{q^t, q}(a_{i,j} b_{i,j})$$

for all $a, b \in \mathbb{F}_{q^t}^n$. By Lemma 5 of Huffman [34], we see that the map $\langle \cdot, \cdot \rangle_0$ is a symmetric and non-degenerate bilinear form on $\mathbb{F}_{q^t}^n$.

The Hermitian trace bilinear form on $\mathbb{F}_{q^t}^n$ is defined only when t is an even integer. Here the integer t can be uniquely written as $t = 2^a z = 2A z$, where $a \geq 1$, z is an odd integer and $A = 2^{a-1}$. One can easily see that there exists a non-zero element $\gamma \in \mathbb{F}_{q^{2A}}$ satisfying $\gamma + \gamma^{q^A} = 0$. Note that the element γ lies in $\mathbb{F}_{q^t}$ and satisfies

$\gamma^{q^{A_g}} = (-1)^g \gamma$ for each integer $g \geq 1$. The *Hermitian trace bilinear form* on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_\gamma : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_\gamma = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} \text{Tr}_{q^t, q}(\gamma a_{i,j} b_{i,j}^{q^{t/2}})$$

for all $a, b \in \mathbb{F}_{q^t}^n$. By Lemma 5 of Huffman [34], we see that the map $\langle \cdot, \cdot \rangle_\gamma$ is an alternating, reflexive and non-degenerate bilinear form on $\mathbb{F}_{q^t}^n$.

To define the $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$, we assume that q is a power of the prime number $\mathfrak{p}$ and that the integer t satisfies $t \not\equiv 1 \pmod{\mathfrak{p}}$. In this case, the map $\phi : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$, defined as

$$\phi(\beta) = \beta^q + \beta^{q^2} + \cdots + \beta^{q^{t-1}} = \text{Tr}_{q^t, q}(\beta) - \beta \text{ for all } \beta \in \mathbb{F}_{q^t},$$

is an $\mathbb{F}_q$ -linear vector space isomorphism. The $*$ trace bilinear form on $\mathbb{F}_{q^t}^n$ is a map $\langle \cdot, \cdot \rangle_* : \mathbb{F}_{q^t}^n \times \mathbb{F}_{q^t}^n \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_* = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} \text{Tr}_{q^t, q}(a_{i,j} \phi(b_{i,j}))$$

for all $a, b \in \mathbb{F}_{q^t}^n$. By Lemma 3.2 of Sharma and Kaur [57], we see that the map $\langle \cdot, \cdot \rangle_*$ is a symmetric and non-degenerate bilinear form on $\mathbb{F}_{q^t}^n$. Moreover, when q is even, the bilinear form $\langle \cdot, \cdot \rangle_*$ is alternating.

Now we shall study the dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ with respect to the aforementioned trace bilinear forms on $\mathbb{F}_{q^t}^n$. For this, we assume, throughout this thesis, that $\sigma \in \{0, \gamma, *\}$. Further, from now on, let $\mathbb{T}_\sigma$ be the set of

- (i) all integers $t \geq 2$ when $\sigma = 0$,
- (ii) all even integers $t \geq 2$ when $\sigma = \gamma$, and
- (iii) all integers $t \geq 2$ satisfying $t \not\equiv 1 \pmod{\mathfrak{p}}$ when $\sigma = *$.

From this point on, let $t \in \mathbb{T}_\sigma$ be fixed for $\sigma \in \{0, \gamma, *\}$. Now if $\mathcal{C}$ is an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, then the

σ -dual code of $\mathcal{C}$ is defined as

$$\mathcal{C}^{\perp\sigma} = \{a \in \mathbb{F}_{q^t}^n : \langle c, a \rangle_\sigma = 0 \text{ for all } c \in \mathcal{C}\}.$$

For $a, b \in \mathbb{F}_{q^t}^n$ and $\sigma \in \{0, *, \gamma\}$, it is easy to observe that $\langle a, b \rangle_\sigma = \langle T_\Omega(a), T_{\hat{\Omega}}(b) \rangle_\sigma$, where $\hat{\Omega} = (\omega_1^{-1}, \omega_2^{-1}, \dots, \omega_\ell^{-1})$. Now let $\mathcal{C}$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. One can easily see that $\mathcal{C} = \{T_\Omega(c) : c \in \mathcal{C}\}$. If $b \in \mathcal{C}^{\perp\sigma}$, then we see that $\langle T_\Omega(c), T_{\hat{\Omega}}(b) \rangle_\sigma = \langle c, b \rangle_\sigma = 0$ for all $c \in \mathcal{C}$, which implies that $T_{\hat{\Omega}}(b) \in \mathcal{C}^{\perp\sigma}$. From this, it follows that the σ -dual code $\mathcal{C}^{\perp\sigma}$ is an $\hat{\Omega}$ -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. We further note that the set $\hat{\mathcal{R}} = \prod_{i=1}^{\ell} \mathcal{R}_{m_i, \omega_i^{-1}}$ can be viewed as an $\mathbb{F}_q[x]$ -module (or as an $\mathfrak{R}_M$ -module) under the component-wise addition and the component-wise scalar multiplication, where $\mathcal{R}_{m_i, \omega_i^{-1}} = \frac{\mathbb{F}_{q^t}[x]}{\langle x^{m_i} - \omega_i^{-1} \rangle}$ for $1 \leq i \leq \ell$. In view of this, we observe that the σ -dual code $\mathcal{C}^{\perp\sigma}$ of an Ω -MT additive code $\mathcal{C}$ of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ can also be viewed as an $\mathbb{F}_q[x]$ -submodule (or as an $\mathfrak{R}_M$ -submodule) of the $\hat{\Omega}$ -MT module $\hat{\mathcal{R}}$.

We now proceed to study the algebraic structures of σ -dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, where $\sigma \in \{0, \gamma, *\}$. For $1 \leq i \leq \ell$ and $0 \leq \theta \leq t-1$, let us define the map $\tau_{q^\theta, 1} : \mathcal{R}_{m_i, \omega_i} \rightarrow \mathcal{R}_{m_i, \omega_i}$ as

$$\tau_{q^\theta, 1}(a_i(x)) = \sum_{j=0}^{m_i-1} a_{i,j}^{q^\theta} x^j \text{ for all } a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j} x^j \in \mathcal{R}_{m_i, \omega_i}.$$

It is easy to see that the map $\tau_{q^\theta, 1}$ is a ring automorphism, whose inverse is the map $\tau_{q^{t-\theta}, 1}$. In addition, the map $\tau_{q^\theta, -1} : \mathcal{R}_{m_i, \omega_i^{-1}} \rightarrow \mathcal{R}_{m_i, \omega_i}$, defined as

$$\tau_{q^\theta, -1}(b_i(x)) = \sum_{j=0}^{m_i-1} b_{i,j}^{q^\theta} x^{-j} \text{ for all } b_i(x) = \sum_{j=0}^{m_i-1} b_{i,j} x^j \in \mathcal{R}_{m_i, \omega_i^{-1}},$$

is a ring isomorphism, where $x^{-1} = \omega_i^{-1} x^{m_i-1} \in \mathcal{R}_{m_i, \omega_i}$. Note that the inverse of $\tau_{q^\theta, -1}$ is the ring isomorphism $\tau_{q^{t-\theta}, -1} : \mathcal{R}_{m_i, \omega_i} \rightarrow \mathcal{R}_{m_i, \omega_i^{-1}}$, defined as

$$\tau_{q^{t-\theta}, -1}(a_i(x)) = \sum_{j=0}^{m_i-1} a_{i,j}^{q^{t-\theta}} x^{-j} \text{ for all } a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j} x^j \in \mathcal{R}_{m_i, \omega_i},$$

where $x^{-1} = \omega_i x^{m_i-1} \in \mathcal{R}_{m_i, \omega_i^{-1}}$. Note that the map $\tau_{q^\theta, -1}$ can be further extended to the map $\tau_{q^\theta, -1} : \widehat{\mathcal{R}} \rightarrow \mathcal{R}$ as

$$\tau_{q^\theta, -1}(b(x)) = (\tau_{q^\theta, -1}(b_1(x)), \tau_{q^\theta, -1}(b_2(x)), \dots, \tau_{q^\theta, -1}(b_\ell(x)))$$

for all $b(x) = (b_1(x), b_2(x), \dots, b_\ell(x)) \in \widehat{\mathcal{R}}$. Moreover, the map $\tau_{1, -1} : \mathfrak{R}_M \rightarrow \mathfrak{R}_M$, defined as

$$\tau_{1, -1}(g(x)) = g(x^{-1}) = \sum_{j=0}^{M-1} g_j x^{-j} \text{ for all } g(x) = \sum_{j=0}^{M-1} g_j x^j \in \mathfrak{R}_M,$$

is a ring isomorphism, where $x^{-1} = x^{M-1}$ in $\mathfrak{R}_M$.

In order to study the algebraic structures of σ -dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$, let us define the map $(\cdot, \cdot)_\sigma : \mathcal{R} \times \widehat{\mathcal{R}} \rightarrow \mathfrak{R}_M$ as

$$(a(x), b(x))_\sigma = \begin{cases} \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \omega_i \left(\frac{x^{M-1}}{x^{m_i} - \omega_i} \right) \tau_{q^\mu, 1} \left(a_i(x) \tau_{1, -1}(b_i(x)) \right) & \text{if } \sigma = 0; \\ \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \omega_i \left(\frac{x^{M-1}}{x^{m_i} - \omega_i} \right) \tau_{q^\mu, 1} \left(\gamma a_i(x) \tau_{q^{t/2}, -1}(b_i(x)) \right) & \text{if } \sigma = \gamma; \\ \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \omega_i \left(\frac{x^{M-1}}{x^{m_i} - \omega_i} \right) \tau_{q^\mu, 1} \left(a_i(x) \left(\sum_{\lambda=1}^{t-1} \tau_{q^\lambda, -1}(b_i(x)) \right) \right) & \text{if } \sigma = * \end{cases}$$

for $a(x) = (a_1(x), a_2(x), \dots, a_\ell(x)) \in \mathcal{R}$ and $b(x) = (b_1(x), b_2(x), \dots, b_\ell(x)) \in \widehat{\mathcal{R}}$.

In the following lemma, we relate the map $(\cdot, \cdot)_\sigma$ with the bilinear form $\langle \cdot, \cdot \rangle_\sigma$ on $\mathbb{F}_{q^t}^n$ and study its basic properties for $\sigma \in \{0, \gamma, *\}$.

Lemma 4.2.1. *Let $a(x) \in \mathcal{R}$ and $b(x) \in \widehat{\mathcal{R}}$. For $\sigma \in \{0, \gamma, *\}$, the following hold.*

(a) $(a(x), b(x))_\sigma = \langle a, b \rangle_\sigma + \langle a, T_{\widehat{\Omega}}(b) \rangle_\sigma x + \dots + \langle a, T_{\widehat{\Omega}}^{M-1}(b) \rangle_\sigma x^{M-1}$ in $\mathfrak{R}_M$, where a and b in $\mathbb{F}_{q^t}^n$ correspond to the elements $a(x) \in \mathcal{R}$ and $b(x) \in \widehat{\mathcal{R}}$, respectively.

(b) The mapping $(\cdot, \cdot)_\sigma$ is a non-degenerate and Hermitian $\tau_{1, -1}$ -sesquilinear form on $\mathcal{R} \times \widehat{\mathcal{R}}$ when $\sigma \in \{0, *\}$, while the map $(\cdot, \cdot)_\gamma$ is a non-degenerate and skew-Hermitian $\tau_{1, -1}$ -sesquilinear form on $\mathcal{R} \times \widehat{\mathcal{R}}$.

Proof. The proof is similar to that of Lemma 2.2 of Kaur and Sharma [41]. $\square$

From the above discussion, we deduce the following:

Theorem 4.2.1. *Let $\mathcal{C}(\subseteq \mathcal{R})$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. For $\sigma \in \{0, \gamma, *\}$, the σ -dual code $\mathcal{C}^{\perp_\sigma}(\subseteq \widehat{\mathcal{R}})$ is an $\mathbb{F}_q[x]$ -submodule (or an $\mathfrak{R}_M$ -submodule) of $\widehat{\mathcal{R}}$ and is given by*

$$\mathcal{C}^{\perp_\sigma} = \left\{ b(x) \in \widehat{\mathcal{R}} : (c(x), b(x))_\sigma = 0 \text{ for all } c(x) \in \mathcal{C} \right\}.$$

4.3 Canonical decomposition of σ -dual codes of MT additive codes

In this section, we study algebraic structures of σ -dual codes of MT additive codes for $\sigma \in \{0, \gamma, *\}$. For this, let $f(x) = f_0 + f_1x + \dots + f_{k-1}x^{k-1} + x^k \in \mathbb{F}_q[x]$ be a monic polynomial with $f_0 \neq 0$. The *reciprocal polynomial* of $f(x)$, denoted by $f^\dagger(x)$, is defined as

$$f^\dagger(x) = f_0^{-1}x^{\deg f(x)}f(x^{-1}) = f_0^{-1}(f_0x^k + f_1x^{k-1} + \dots + f_{k-1}x + 1).$$

A non-zero monic polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be *self-reciprocal* if it satisfies $f(x) = f^\dagger(x)$. On the other hand, if a monic polynomial $f(x) \in \mathbb{F}_q[x]$ satisfies $f(x) \neq f^\dagger(x)$, then we say that the polynomials $f(x)$ and $f^\dagger(x)$ form a *reciprocal pair*. We next recall, from Section 3.3, that

$$x^{m_i} - \omega_i = h_1(x)^{\epsilon_{1,i}} h_2(x)^{\epsilon_{2,i}} \dots h_s(x)^{\epsilon_{s,i}}$$

is the irreducible factorization of the polynomial $x^{m_i} - \omega_i$ over $\mathbb{F}_q$ for $1 \leq i \leq \ell$. This implies that

$$x^{m_i} - \omega_i^{-1} = h_1^\dagger(x)^{\epsilon_{1,i}} h_2^\dagger(x)^{\epsilon_{2,i}} \dots h_s^\dagger(x)^{\epsilon_{s,i}}$$

is the irreducible factorization of the polynomial $x^{m_i} - \omega_i^{-1}$ over $\mathbb{F}_q$ for $1 \leq i \leq \ell$. By applying the Chinese Remainder Theorem again [7, Th. 1.2.12], we obtain

$$\widehat{\mathcal{R}} = \prod_{i=1}^{\ell} \mathcal{R}_{m_i, \omega_i^{-1}} \simeq \bigoplus_{\nu=1}^s \underbrace{\left(\epsilon_{\nu,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_{\nu}^{\dagger}(x) \rangle}, \epsilon_{\nu,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_{\nu}^{\dagger}(x) \rangle}, \dots, \epsilon_{\nu,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_{\nu}^{\dagger}(x) \rangle} \right)}_{\mathbb{G}_{\nu}^{\dagger}} = \bigoplus_{\nu=1}^s \mathbb{G}_{\nu}^{\dagger} = \mathbb{G}^{\dagger}, \quad (4.1)$$

where the corresponding ring isomorphism from $\widehat{\mathcal{R}}$ onto $\mathbb{G}^{\dagger}$ is given by

$$\begin{aligned} b(x) \mapsto & \left(\epsilon_{1,1}(b_1(x) + \langle h_1^{\dagger}(x) \rangle), \epsilon_{1,2}(b_2(x) + \langle h_1^{\dagger}(x) \rangle), \dots, \epsilon_{1,\ell}(b_{\ell}(x) + \langle h_1^{\dagger}(x) \rangle), \right. \\ & \epsilon_{2,1}(b_1(x) + \langle h_2^{\dagger}(x) \rangle), \epsilon_{2,2}(b_2(x) + \langle h_2^{\dagger}(x) \rangle), \dots, \epsilon_{2,\ell}(b_{\ell}(x) + \langle h_2^{\dagger}(x) \rangle), \dots, \\ & \left. \epsilon_{s,1}(b_1(x) + \langle h_s^{\dagger}(x) \rangle), \epsilon_{s,2}(b_2(x) + \langle h_s^{\dagger}(x) \rangle), \dots, \epsilon_{s,\ell}(b_{\ell}(x) + \langle h_s^{\dagger}(x) \rangle) \right) \end{aligned}$$

for all $b(x) = (b_1(x), b_2(x), \dots, b_{\ell}(x)) \in \widehat{\mathcal{R}}$. In view of the above isomorphism, from this point on, we shall identify each element $b(x) = (b_1(x), b_2(x), \dots, b_{\ell}(x)) \in \widehat{\mathcal{R}}$ with the element

$$B(x) = (B_1(x), B_2(x), \dots, B_s(x)) \in \mathbb{G}^{\dagger},$$

where $B_{\nu}(x) = (B_{\nu,1}(x), B_{\nu,2}(x), \dots, B_{\nu,\ell}(x)) \in \mathbb{G}_{\nu}^{\dagger}$ with $B_{\nu,i}(x) = \epsilon_{\nu,i} b_i(x) + \langle h_{\nu}^{\dagger}(x) \rangle \in \epsilon_{\nu,i} \frac{\mathbb{F}_{q^t}[x]}{\langle h_{\nu}^{\dagger}(x) \rangle}$ for $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$. That is, if Υ denotes the isomorphism from $\widehat{\mathcal{R}}$ onto $\mathbb{G}^{\dagger}$, then we shall write $\Upsilon(b(x)) = B(x)$. We further observe that the set $\mathbb{G}^{\dagger}$ can be viewed as an $\mathbb{F}_q[x]$ -module under the component-wise addition and the component-wise scalar multiplication.

Further, for $1 \leq \nu \leq s$, let us define $\mathcal{F}_{\nu}^{\dagger} = \frac{\mathbb{F}_q[x]}{\langle h_{\nu}^{\dagger}(x) \rangle}$. Here it is easy to see that $d_{\nu} = \deg h_{\nu}(x) = \deg h_{\nu}^{\dagger}(x)$ and $\mathcal{F}_{\nu}^{\dagger}$ is the finite field of order $q^{d_{\nu}}$, i.e., $\mathcal{F}_{\nu}^{\dagger} \simeq \mathbb{F}_{q^{d_{\nu}}}$ for $1 \leq \nu \leq s$. Furthermore, we observe that the set $\mathbb{G}_{\nu}$ is an $\epsilon_{\nu}t$ -dimensional vector space over $\mathcal{F}_{\nu}^{\dagger}$ under the component-wise addition and the component-wise scalar multiplication, where $\epsilon_{\nu} = \sum_{i=1}^{\ell} \epsilon_{\nu,i}$ for each ν .

Now for $\sigma \in \{0, \gamma, *\}$, we will further relate the sesquilinear form $(\cdot, \cdot)_{\sigma}$ on $\mathcal{R} \times \widehat{\mathcal{R}}$ with the corresponding map $[\cdot, \cdot]_{\sigma}$ on $\mathbb{G} \times \mathbb{G}^{\dagger}$ and study its properties. Towards this, we see that if $\epsilon_{\nu,i} = 1$ for some ν and i , then $h_{\nu}(x)$ divides $x^{m_i} - \omega_i$ in $\mathbb{F}_q[x]$, which

implies that $x^{m_i} = \omega_i$ in $\mathcal{F}_\nu$. This further implies that

$$\omega_i \left(\frac{x^M - 1}{x^{m_i} - \omega_i} \right) = 1 + \omega_i^{-1} x^{m_i} + \omega_i^{-2} x^{2m_i} + \cdots + \omega_i^{-(\frac{M}{m_i}-1)} x^{(\frac{M}{m_i}-1)m_i} = \frac{M}{m_i} \text{ in } \mathcal{F}_\nu.$$

We also note that the map $\tau_{1,-1} : \mathcal{F}_\nu^\dagger \rightarrow \mathcal{F}_\nu$, defined as

$$\tau_{1,-1} \left(\sum_{k=0}^{d_\nu-1} f_k x^k \right) = \sum_{k=0}^{d_\nu-1} f_k x^{-k} \text{ for all } \sum_{k=0}^{d_\nu-1} f_k x^k \in \mathcal{F}_\nu^\dagger,$$

is a ring isomorphism.

In view of the above discussion, we observe, for $\sigma \in \{0, \gamma, *\}$, that the sesquilinear form $(\cdot, \cdot)_\sigma$ corresponds to the map $[\cdot, \cdot]_\sigma : \mathbb{G} \times \mathbb{G}^\dagger \rightarrow \bigoplus_{\nu=1}^s \mathcal{F}_\nu$, which is defined as follows:

$$[A(x), B(x)]_\sigma = \begin{cases} (R_1(x), R_2(x), \dots, R_s(x)) & \text{if } \sigma = 0; \\ (S_1(x), S_2(x), \dots, S_s(x)) & \text{if } \sigma = \gamma; \\ (T_1(x), T_2(x), \dots, T_s(x)) & \text{if } \sigma = * \end{cases} \quad (4.2)$$

for all $A(x) = (A_1(x), A_2(x), \dots, A_s(x)) \in \mathbb{G}$ and $B(x) = (B_1(x), B_2(x), \dots, B_s(x)) \in \mathbb{G}^\dagger$, where for $1 \leq \nu \leq s$, $R_\nu(x)$, $S_\nu(x)$ and $T_\nu(x)$ are given by

$$\begin{aligned} R_\nu(x) &= \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \epsilon_{\nu,i} \frac{M}{m_i} \tau_{q^\mu,1} \left(A_{\nu,i}(x) \tau_{1,-1}(B_{\nu,i}(x)) \right), \\ S_\nu(x) &= \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \epsilon_{\nu,i} \frac{M}{m_i} \tau_{q^\mu,1} \left(\gamma A_{\nu,i}(x) \tau_{q^{t/2},-1}(B_{\nu,i}(x)) \right) \text{ and} \\ T_\nu(x) &= \sum_{i=1}^{\ell} \sum_{\mu=0}^{t-1} \epsilon_{\nu,i} \frac{M}{m_i} \tau_{q^\mu,1} \left(A_{\nu,i}(x) \left(\sum_{\lambda=1}^{t-1} \tau_{q^\lambda,-1}(B_{\nu,i}(x)) \right) \right). \end{aligned}$$

Further, for $g(x) = (g_1(x), g_2(x), \dots, g_s(x)) \in \bigoplus_{\nu=1}^s \mathcal{F}_\nu^\dagger$, let us define

$$\tau_{1,-1}(g(x)) = \left(\tau_{1,-1}(g_1(x)), \tau_{1,-1}(g_2(x)), \dots, \tau_{1,-1}(g_s(x)) \right) \in \bigoplus_{\nu=1}^s \mathcal{F}_\nu.$$

In the following lemma, we show that the map $[\cdot, \cdot]_\sigma : \mathbb{G} \times \mathbb{G}^\dagger \rightarrow \bigoplus_{\nu=1}^s \mathcal{F}_\nu$ is a reflexive

and non-degenerate $\tau_{1,-1}$ -sesquilinear form for $\sigma \in \{0, \gamma, *\}$.

Lemma 4.3.1. *Let $A(x), A'(x) \in \mathbb{G}$, $B(x), B'(x) \in \mathbb{G}^\dagger$, $f(x) \in \bigoplus_{\nu=1}^s \mathcal{F}_\nu$, and $g(x) \in \bigoplus_{\nu=1}^s \mathcal{F}_\nu^\dagger$. For $\sigma \in \{0, \gamma, *\}$, the following hold.*

- (a) $[A(x) + A'(x), B(x)]_\sigma = [A(x), B(x)]_\sigma + [A'(x), B(x)]_\sigma$ and $[A(x), B(x) + B'(x)]_\sigma = [A(x), B(x)]_\sigma + [A(x), B'(x)]_\sigma$.
- (b) $[f(x)A(x), B(x)]_\sigma = f(x)([A(x), B(x)]_\sigma)$ and $[A(x), g(x)B(x)]_\sigma = \tau_{1,-1}(g(x))([A(x), B(x)]_\sigma)$.
- (c) $[A(x), B(x)]_\sigma = \tau_{1,-1}([B(x), A(x)]_\sigma)$ for $\sigma \in \{0, *\}$, and $[A(x), B(x)]_\gamma = -\tau_{1,-1}([B(x), A(x)]_\gamma)$.
- (d) $[\cdot, \cdot]_\sigma$ is non-degenerate.

Proof. Proofs of parts (a)-(c) are trivial. To prove (d), let $A(x) \in \mathbb{G}$ be such that $[A(x), B(x)]_\sigma = 0$ for all $B(x) \in \mathbb{G}^\dagger$. Here we assert that $A(x) = \mathbf{0}$.

Let us suppose, on the contrary, that $A(x)$ is non-zero. As Ψ is the isomorphism from $\mathcal{R}$ onto $\mathbb{G}$, there exists a unique element $a(x) = (a_1(x), a_2(x), \dots, a_\ell(x)) \in \mathcal{R}$ such that $\Psi(a(x)) = A(x)$, where $a_i(x) = \sum_{j=0}^{m_i-1} a_{i,j}x^j \in \mathcal{R}_{m_i, \omega_i}$ for $1 \leq i \leq \ell$. Let $A(x) = (A_1(x), A_2(x), \dots, A_s(x)) \in \mathbb{G}$, where $A_\nu(x) = (A_{\nu,1}(x), A_{\nu,2}(x), \dots, A_{\nu,\ell}(x)) \in \mathbb{G}_\nu$ with $A_{\nu,i}(x) = \epsilon_{\nu,i}a_i(x) + \langle h_\nu(x) \rangle$ for $1 \leq i \leq \ell$ and $1 \leq \nu \leq s$. Since $A(x)$ is non-zero, we note that $A_\nu(x) \neq 0$ for some ν , $1 \leq \nu \leq s$. From this, we see that $\epsilon_{\nu,z} = 1$ and $a_z(x) \not\equiv 0 \pmod{h_z(x)}$ for some z , $1 \leq z \leq \ell$. Let us write $A_{\nu,z}(x) = \sum_{j=0}^{d_\nu-1} A_{\nu,z}^{(j)}x^j$. As $A_{\nu,z}(x) \neq 0$, we note that $A_{\nu,z}^{(k)}(\neq 0) \in \mathbb{F}_{q^t}$ for some k . Since $\text{Tr}_{q^t, q}$ is a non-zero and an onto map, there exist $c, d, \xi \in \mathbb{F}_{q^t}$ satisfying $\text{Tr}_{q^t, q}(A_{\nu,z}^{(k)}c) \neq 0$, $\text{Tr}_{q^t, q}(\gamma A_{\nu,z}^{(k)}d^{q^{\frac{k}{2}}}) \neq 0$ and $\text{Tr}_{q^t, q}(\xi) \neq 0$. As Υ is the isomorphism from $\widehat{\mathcal{R}}$ onto $\mathbb{G}^\dagger$, there exists a unique element $b(x) = (b_1(x), b_2(x), \dots, b_\ell(x)) \in \widehat{\mathcal{R}}$ satisfying $\Upsilon(b(x)) = B(x)$. Now let us take $b_i(x) = 0$ for $1 \leq i(\neq z) \leq \ell$, and let us take $b_z(x) = c$ when $\sigma = 0$, $b_z(x) = d$ when $\sigma = \gamma$, and $b_z(x) = \phi^{-1}(\xi A_{\nu,z}^{(k)-1})$ when $\sigma = *$. In view of this, we have $B_{\nu,i}(x) = 0$ for all $1 \leq i(\neq z) \leq \ell$ and $B_{\nu,z}(x) = c$ when $\sigma = 0$, $B_{\nu,z}(x) = d$ when $\sigma = \gamma$ and $B_{\nu,z}(x) = \phi^{-1}(\xi A_{\nu,z}^{(k)-1})$ when $\sigma = *$.

Now when $\sigma = 0$, we see that $\tau_{1,-1}(B_{\nu,z}(x)) = c$. This, by (4.2), implies that

$$[A(x), B(x)]_0 = \frac{M}{m_z} \sum_{h=0}^{d_\nu-1} \text{Tr}_{q^t, q}(A_{\nu,z}^{(h)} c) x^h \neq 0,$$

which is a contradiction.

When $\sigma = \gamma$, we see that $\tau_{1,-1}(B_{\nu,z}(x)) = d$. By (4.2) again, we note that

$$[A(x), B(x)]_\gamma = \frac{M}{m_z} \sum_{h=0}^{d_\nu-1} \text{Tr}_{q^t, q}(\gamma A_{\nu,z}^{(h)} d^{q^{\frac{t}{2}}}) x^h \neq 0,$$

which is again a contradiction.

Finally, when $\sigma = *$, we see that $\tau_{1,-1}(B_{\nu,z}(x)) = \phi^{-1}(\xi A_{\nu,z}^{(k)-1})$. By (4.2) again, we see that

$$\begin{aligned} [A(x), B(x)]_* &= \frac{M}{m_z} \sum_{h=0}^{d_\nu-1} \text{Tr}_{q^t, q}(A_{\nu,z}^{(h)} \phi(\phi^{-1}(\xi A_{\nu,z}^{(k)-1}))) x^h \\ &= \frac{M}{m_z} \sum_{h=0}^{d_\nu-1} \text{Tr}_{q^t, q}(\xi A_{\nu,z}^{(h)} A_{\nu,z}^{(k)-1}) x^h \neq 0, \end{aligned}$$

which is again a contradiction.

This proves the assertion. Thus the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ is non-degenerate for all $\sigma \in \{0, \gamma, *\}$. $\square$

Next for $1 \leq \nu \leq s$, let $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger}$ denote the restriction of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ to $\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger$. The following proposition is useful in investigating the algebraic structures of σ -dual codes of Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for each $\sigma \in \{0, \gamma, *\}$.

Proposition 4.3.1. *Let $a(x) \in \mathcal{R}$ and $b(x) \in \widehat{\mathcal{R}}$ be identified with the elements $A(x) = (A_1(x), A_2(x), \dots, A_s(x)) \in \mathbb{G}$ and $B(x) = (B_1(x), B_2(x), \dots, B_s(x)) \in \mathbb{G}^\dagger$, respectively. For $\sigma \in \{0, \gamma, *\}$, we have $[A(x), B(x)]_\sigma = 0$ if and only if $[A_\nu(x), B_\nu(x)]_\sigma = 0$ for $1 \leq \nu \leq s$.*

In the following theorem, we obtain a canonical decomposition of the σ -dual code of each Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$

over $\mathbb{F}_{q^t}$ by relating the constituents of the code with that of its σ -dual code, where $\sigma \in \{0, \gamma, *\}$.

Theorem 4.3.1. *Let $\mathcal{C}$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, and let $\mathcal{C}^{\perp_\sigma}$ be the σ -dual code of $\mathcal{C}$ for $\sigma \in \{0, \gamma, *\}$. Let $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \dots \oplus \mathcal{C}_s$ and $\mathcal{C}^{\perp_\sigma} = \mathcal{C}_1^{(\sigma)} \oplus \mathcal{C}_2^{(\sigma)} \oplus \dots \oplus \mathcal{C}_s^{(\sigma)}$ be the canonical decompositions of $\mathcal{C}$ and $\mathcal{C}^{\perp_\sigma}$, where $\mathcal{C}_\nu = \mathcal{C} \cap \mathbb{G}_\nu$ and $\mathcal{C}_\nu^{(\sigma)} = \mathcal{C}^{\perp_\sigma} \cap \mathbb{G}_\nu^\dagger$ for $1 \leq \nu \leq s$. Then for $1 \leq \nu \leq s$, we have*

$$\mathcal{C}_\nu^{(\sigma)} = \{B_\nu(x) \in \mathbb{G}_\nu^\dagger : [A_\nu(x), B_\nu(x)]_\sigma = 0 \text{ for all } A_\nu(x) \in \mathcal{C}_\nu\} = \mathcal{C}_\nu^{\perp_\sigma},$$

i.e., $\mathcal{C}_\nu^{\perp_\sigma}$ is the orthogonal complement of $\mathcal{C}_\nu$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger}$ for $1 \leq \nu \leq s$. Moreover, we have $\dim_{\mathbb{F}_q^\dagger} \mathcal{C}_\nu^{(\sigma)} = \dim_{\mathbb{F}_q^\dagger} \mathcal{C}_\nu^{\perp_\sigma} = \epsilon_\nu t - \dim_{\mathbb{F}_q} \mathcal{C}_\nu$ for $1 \leq \nu \leq s$.

Proof. The desired result follows from Proposition 4.3.1 and Theorem 2.2.1. $\square$

4.4 Self-orthogonal, self-dual and ACD MT additive codes

Let $\mathcal{C}$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. For $\sigma \in \{0, \gamma, *\}$, the code $\mathcal{C}$ is said to be

- (i) σ -self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_\sigma}$.
- (ii) σ -self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp_\sigma}$.
- (iii) an additive code with σ -complementary-dual (or a σ -ACD code) if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_\sigma} = \{\mathbf{0}\}$.

In this section, we study and characterize σ -self-orthogonal, σ -self-dual and σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. Towards this, we recall that $h_1(x), h_2(x), \dots, h_s(x)$ are all the distinct irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ in $\mathbb{F}_q[x]$. By relabelling $h_\nu(x)$'s (if required), we further assume, without any loss of generality, that

- $h_1(x), h_2(x), \dots, h_{e_1}(x)$ are all the distinct self-reciprocal irreducible factors,

- $h_{e_1+1}(x), h_{e_1+1}^\dagger(x), h_{e_1+2}(x), h_{e_1+2}^\dagger(x), \dots, h_{e_2}(x), h_{e_2}^\dagger(x)$ are the irreducible factors forming reciprocal pairs, and
- $h_{e_2+1}(x), h_{e_2+2}(x), \dots, h_{e_3}(x)$ are the remaining irreducible factors, which are neither self-reciprocal nor do they form reciprocal pairs, of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ over $\mathbb{F}_q$.

Note that $s = e_2 + e_3 - e_1$. Recall that $\deg h_u(x) = d_u$, $\deg h_v(x) = \deg h_v^\dagger(x) = d_v$ and $\deg h_w(x) = d_w$ for $1 \leq u \leq e_1$, $e_1 + 1 \leq v \leq e_2$ and $e_2 + 1 \leq w \leq e_3$. Further, for $1 \leq z \leq e_3$, $e_1 + 1 \leq v \leq e_2$ and $1 \leq i \leq \ell$, let us define

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

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

and $\epsilon_z = \sum_{i=1}^{\ell} \epsilon_{z,i}$. From this, we get

$$x^{m_i} - \omega_i = \prod_{u=1}^{e_1} h_u(x)^{\epsilon_{u,i}} \prod_{v=e_1+1}^{e_2} h_v(x)^{\epsilon_{v,i}} h_v^\dagger(x)^{\epsilon_{v,i}^\dagger} \prod_{w=e_2+1}^{e_3} h_w(x)^{\epsilon_{w,i}}$$

and

$$x^{m_i} - \omega_i^{-1} = \prod_{u=1}^{e_1} h_u(x)^{\epsilon_{u,i}} \prod_{v=e_1+1}^{e_2} h_v^{\epsilon_{v,i}^\dagger}(x) h_v^\dagger(x)^{\epsilon_{v,i}} \prod_{w=e_2+1}^{e_3} h_w^\dagger(x)^{\epsilon_{w,i}}.$$

Now by applying the Chinese Remainder Theorem [7, Th. 1.2.12], we see that

$$\mathcal{R} \simeq \mathbb{G} = \left(\bigoplus_{u=1}^{e_1} \mathbb{G}_u \right) \oplus \left(\bigoplus_{v=e_1+1}^{e_2} (\mathbb{G}_v \oplus \mathbb{G}_v^\dagger) \right) \oplus \left(\bigoplus_{w=e_2+1}^{e_3} \mathbb{G}_w \right) \quad (4.3)$$

and

$$\widehat{\mathcal{R}} \simeq \mathbb{G}^\dagger = \left(\bigoplus_{u=1}^{e_1} \mathbb{G}_u \right) \oplus \left(\bigoplus_{v=e_1+1}^{e_2} (\mathbb{H}_v \oplus \mathbb{H}_v^\dagger) \right) \oplus \left(\bigoplus_{w=e_2+1}^{e_3} \mathbb{G}_w^\dagger \right), \quad (4.4)$$

where

$$\begin{aligned}
\mathbb{G}_u &= \left(\epsilon_{u,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_u(x) \rangle}, \epsilon_{u,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_u(x) \rangle}, \dots, \epsilon_{u,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_u(x) \rangle} \right), \\
\mathbb{G}_v &= \left(\epsilon_{v,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \epsilon_{v,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \dots, \epsilon_{v,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle} \right), \\
\mathbb{G}_v^\dagger &= \left(\epsilon_{v,1}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \epsilon_{v,2}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \dots, \epsilon_{v,\ell}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle} \right), \\
\mathbb{H}_v &= \left(\epsilon_{v,1}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \epsilon_{v,2}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \dots, \epsilon_{v,\ell}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle} \right), \\
\mathbb{H}_v^\dagger &= \left(\epsilon_{v,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \epsilon_{v,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \dots, \epsilon_{v,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle} \right), \\
\mathbb{G}_w &= \left(\epsilon_{w,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w(x) \rangle}, \epsilon_{w,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w(x) \rangle}, \dots, \epsilon_{w,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w(x) \rangle} \right) \text{ and} \\
\mathbb{G}_w^\dagger &= \left(\epsilon_{w,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w^\dagger(x) \rangle}, \epsilon_{w,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w^\dagger(x) \rangle}, \dots, \epsilon_{w,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_w^\dagger(x) \rangle} \right)
\end{aligned}$$

for $1 \leq u \leq e_1$, $e_1 + 1 \leq v \leq e_2$ and $e_2 + 1 \leq w \leq e_3$. For each relevant u, v and w , we note that

$$\begin{aligned}
\mathcal{F}_u &= \frac{\mathbb{F}_q[x]}{\langle h_u(x) \rangle} \simeq \mathbb{F}_{q^{d_u}}, & \mathcal{F}_v &= \frac{\mathbb{F}_q[x]}{\langle h_v(x) \rangle} \simeq \mathbb{F}_{q^{d_v}}, & \mathcal{F}_v^\dagger &= \frac{\mathbb{F}_q[x]}{\langle h_v^\dagger(x) \rangle} \simeq \mathbb{F}_{q^{d_v}}, \\
\mathcal{F}_w &= \frac{\mathbb{F}_q[x]}{\langle h_w(x) \rangle} \simeq \mathbb{F}_{q^{d_w}} \text{ and } \mathcal{F}_w^\dagger &= \frac{\mathbb{F}_q[x]}{\langle h_w^\dagger(x) \rangle} \simeq \mathbb{F}_{q^{d_w}}.
\end{aligned}$$

We also recall, for $1 \leq z \leq e_3$, that $\dim_{\mathcal{F}_z} \mathbb{G}_z = \epsilon_z t$. Further, for $e_1 + 1 \leq v \leq e_2$, we see that if $\epsilon_v^\dagger = \sum_{i=1}^{\ell} \epsilon_{v,i}^\dagger$, then $\dim_{\mathcal{F}_v^\dagger} \mathbb{G}_v^\dagger = \dim_{\mathcal{F}_v} \mathbb{H}_v = \epsilon_v^\dagger t$. Further, from now on, we shall identify each element $a(x) = (a_1(x), a_2(x), \dots, a_\ell(x)) \in \mathcal{R}$ with the element

$$\begin{aligned}
A(x) &= (A_1(x), A_2(x), \dots, A_{e_1}(x), A_{e_1+1}(x), \tilde{A}_{e_1+1}(x), A_{e_1+2}(x), \tilde{A}_{e_1+2}(x), \dots, A_{e_2}(x), \\
&\quad \tilde{A}_{e_2}(x), A_{e_2+1}(x), A_{e_2+2}(x), \dots, A_{e_3}(x)) \in \mathbb{G},
\end{aligned}$$

where

$$\begin{aligned} A_u(x) &= (A_{u,1}(x), A_{u,2}(x), \dots, A_{u,\ell}(x)) \in \mathbb{G}_u, \\ A_v(x) &= (A_{v,1}(x), A_{v,2}(x), \dots, A_{v,\ell}(x)) \in \mathbb{G}_v, \\ \tilde{A}_v(x) &= (\tilde{A}_{v,1}(x), \tilde{A}_{v,2}(x), \dots, \tilde{A}_{v,\ell}(x)) \in \mathbb{G}_v^\dagger \quad \text{and} \\ A_w(x) &= (A_{w,1}(x), A_{w,2}(x), \dots, A_{w,\ell}(x)) \in \mathbb{G}_w \end{aligned}$$

with $A_{u,i}(x) = \epsilon_{u,i}a_i(x) + \langle h_u(x) \rangle$, $A_{v,i}(x) = \epsilon_{v,i}a_i(x) + \langle h_v(x) \rangle$, $\tilde{A}_{v,i}(x) = \epsilon_{v,i}^\dagger a_i(x) + \langle h_v^\dagger(x) \rangle$ and $A_{w,i}(x) = \epsilon_{w,i}a_i(x) + \langle h_w(x) \rangle$ for $1 \leq i \leq \ell$, $1 \leq u \leq e_1$, $e_1 + 1 \leq v \leq e_2$, and $e_2 + 1 \leq w \leq e_3$.

Similarly, each element $b(x) = (b_1(x), b_2(x), \dots, b_\ell(x)) \in \hat{\mathcal{R}}$ can be identified with the element

$$\begin{aligned} B(x) = & (B_1(x), B_2(x), \dots, B_{e_1}(x), B_{e_1+1}(x), \tilde{B}_{e_1+1}(x), B_{e_1+2}(x), \tilde{B}_{e_1+2}(x), \dots, B_{e_2}(x), \\ & \tilde{B}_{e_2}(x), B_{e_2+1}(x), B_{e_2+2}(x), \dots, B_{e_3}(x)) \in \mathbb{G}^\dagger, \end{aligned}$$

where

$$\begin{aligned} B_u(x) &= (B_{u,1}(x), B_{u,2}(x), \dots, B_{u,\ell}(x)) \in \mathbb{G}_u, \\ B_v(x) &= (B_{v,1}(x), B_{v,2}(x), \dots, B_{v,\ell}(x)) \in \mathbb{H}_v, \\ \tilde{B}_v(x) &= (\tilde{B}_{v,1}(x), \tilde{B}_{v,2}(x), \dots, \tilde{B}_{v,\ell}(x)) \in \mathbb{H}_v^\dagger \quad \text{and} \\ B_w(x) &= (B_{w,1}(x), B_{w,2}(x), \dots, B_{w,\ell}(x)) \in \mathbb{G}_w^\dagger \end{aligned}$$

with $B_{u,i}(x) = \epsilon_{u,i}b_i(x) + \langle h_u(x) \rangle$, $B_{v,i}(x) = \epsilon_{v,i}^\dagger b_i(x) + \langle h_v(x) \rangle$, $\tilde{B}_{v,i}(x) = \epsilon_{v,i}b_i(x) + \langle h_v^\dagger(x) \rangle$ and $B_{w,i}(x) = \epsilon_{w,i}b_i(x) + \langle h_w^\dagger(x) \rangle$ for $1 \leq i \leq \ell$, $1 \leq u \leq e_1$, $e_1 + 1 \leq v \leq e_2$ and $e_2 + 1 \leq w \leq e_3$.

Further, by Theorem [3.3.1](#) and by [\(4.3\)](#), we see that each Ω -MT additive code $\mathcal{C}(\subseteq \mathbb{G})$ of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ has a canonical decomposition of the form

$$\mathcal{C} = \left(\bigoplus_{u=1}^{e_1} \mathcal{C}_u \right) \oplus \left(\bigoplus_{v=e_1+1}^{e_2} (\mathcal{C}_v \oplus \mathcal{C}_v^\dagger) \right) \oplus \left(\bigoplus_{w=e_2+1}^{e_3} \mathcal{C}_w \right), \quad (4.5)$$

where $\mathcal{C}_u$ (*resp.* $\mathcal{C}_v$, $\mathcal{C}_v^\dagger$ and $\mathcal{C}_w$) is a subspace of $\mathbb{G}_u$ (*resp.* $\mathbb{G}_v$, $\mathbb{G}_v^\dagger$ and $\mathbb{G}_w$) over $\mathcal{F}_u$ (*resp.* $\mathcal{F}_v$, $\mathcal{F}_v^\dagger$ and $\mathcal{F}_w$) for each u (*resp.* v and w).

Moreover, by equations (4.2) and (4.4) and by applying Theorem 4.3.1, we see that the σ -dual code $\mathcal{C}^{\perp\sigma} (\subseteq \mathbb{G}^\dagger)$ of the code $\mathcal{C}$ has a canonical decomposition of the form

$$\mathcal{C}^{\perp\sigma} = \left(\bigoplus_{u=1}^{e_1} \mathcal{C}_u^{\perp\sigma} \right) \oplus \left(\bigoplus_{v=e_1+1}^{e_2} (\mathcal{C}_v^{\dagger\perp\sigma} \oplus \mathcal{C}_v^{\perp\sigma}) \right) \oplus \left(\bigoplus_{w=e_2+1}^{e_3} \mathcal{C}_w^{\perp\sigma} \right), \quad (4.6)$$

where $\mathcal{C}_u^{\perp\sigma} \subseteq \mathbb{G}_u$ is the orthogonal complement of $\mathcal{C}_u$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ for $1 \leq u \leq e_1$, $\mathcal{C}_v^{\perp\sigma} \subseteq \mathbb{H}_v^\dagger$ is the orthogonal complement of $\mathcal{C}_v$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_v \times \mathbb{H}_v^\dagger}$, $\mathcal{C}_v^{\dagger\perp\sigma} \subseteq \mathbb{H}_v$ is the orthogonal complement of $\mathcal{C}_v^\dagger$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_v^\dagger \times \mathbb{H}_v}$ for $e_1 + 1 \leq v \leq e_2$, and $\mathcal{C}_w^{\perp\sigma} \subseteq \mathbb{G}_w^\dagger$ is the orthogonal complement of $\mathcal{C}_w$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_w \times \mathbb{G}_w^\dagger}$ for $e_2 + 1 \leq w \leq e_3$. Here $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ (*resp.* $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_v \times \mathbb{H}_v^\dagger}$, $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_v^\dagger \times \mathbb{H}_v}$ and $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_w \times \mathbb{G}_w^\dagger}$) denotes the restriction of the sesquilinear form $[\cdot, \cdot]_\sigma$ to $\mathbb{G}_u \times \mathbb{G}_u$ (*resp.* $\mathbb{G}_v \times \mathbb{H}_v^\dagger$, $\mathbb{G}_v^\dagger \times \mathbb{H}_v$ and $\mathbb{G}_w \times \mathbb{G}_w^\dagger$) for $1 \leq u \leq e_1$ (*resp.* for $e_1 + 1 \leq v \leq e_2$ and $e_2 + 1 \leq w \leq e_3$).

For $1 \leq u \leq e_1$, an $\mathcal{F}_u$ -subspace $\mathcal{C}_u$ of $\mathbb{G}_u$ is said to be

- (i) *σ -self-orthogonal* if it satisfies $\mathcal{C}_u \subseteq \mathcal{C}_u^{\perp\sigma}$.
- (ii) *σ -self-dual* if it satisfies $\mathcal{C}_u = \mathcal{C}_u^{\perp\sigma}$.
- (iii) *σ -non-degenerate* if it satisfies $\mathcal{C}_u \cap \mathcal{C}_u^{\perp\sigma} = \{\mathbf{0}\}$.

Now for $e_1 + 1 \leq v \leq e_2$, let η_v denote the number of integers i satisfying $1 \leq i \leq \ell$ and $\epsilon_{v,i} = \epsilon_{v,i}^\dagger = 1$. Further, for each v , let us define

$$\mathbb{K}_v = \mathbb{G}_v \cap \mathbb{H}_v = \left(\epsilon_{v,1} \epsilon_{v,1}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \epsilon_{v,2} \epsilon_{v,2}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \dots, \epsilon_{v,\ell} \epsilon_{v,\ell}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle} \right),$$

and

$$\mathbb{K}_v^\dagger = \mathbb{G}_v^\dagger \cap \mathbb{H}_v^\dagger = \left(\epsilon_{v,1} \epsilon_{v,1}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \epsilon_{v,2} \epsilon_{v,2}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \dots, \epsilon_{v,\ell} \epsilon_{v,\ell}^\dagger \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle} \right).$$

One can easily observe that $\mathbb{K}_v$ (*resp.* $\mathbb{K}_v^\dagger$) is an $(\eta_v t)$ -dimensional vector space over $\mathcal{F}_v$ (*resp.* $\mathcal{F}_v^\dagger$) for $e_1 + 1 \leq v \leq e_2$. It is easy to observe that the restriction $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{K}_v \times \mathbb{K}_v^\dagger}$

of the form $[\cdot, \cdot]_\sigma$ to $\mathbb{K}_v \times \mathbb{K}_v^\dagger$ is a reflexive and a non-degenerate $\tau_{1,-1}$ -sesquilinear form.

Next one can easily see that $x+1$ and $x-1$ are the only irreducible self-reciprocal polynomials of odd degree and that all other irreducible self-reciprocal polynomials over finite fields are of even degrees. More precisely, for $1 \leq u \leq e_1$, if $\deg h_u(x) = d_u$ is odd, then we must have $d_u = 1$ and $h_u(x)$ is either $x+1$ or $x-1$. Moreover, for $1 \leq u \leq e_1$, one can easily observe that the map $\tau_{1,-1} : \mathcal{F}_u \rightarrow \mathcal{F}_u$ is an automorphism of $\mathcal{F}_u (\simeq \mathbb{F}_{q^{d_u}})$ satisfying $\tau_{1,-1}^2 = \tau_{1,1}$, where $\tau_{1,1}$ is the identity automorphism. That is, the map $\tau_{1,-1}$ is either the identity automorphism or the automorphism of $\mathcal{F}_u$ of order 2.

Next for $1 \leq u \leq e_1$, let us define $\mathcal{J}_1 = \{u : 1 \leq u \leq e_1, d_u = 1\}$ and $\mathcal{J}_2 = \{u : 1 \leq u \leq e_1, d_u \text{ is even}\}$. Note that $\{1, 2, \dots, e_1\} = \mathcal{J}_1 \cup \mathcal{J}_2$ (a disjoint union). Since $x+1$ and $x-1$ are the only irreducible self-reciprocal polynomials of degree 1, it is easy to see that $|\mathcal{J}_1| \leq 2$. Now the following lemma is useful in studying and counting all σ -self-orthogonal, σ -self-dual and σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for each $\sigma \in \{0, \gamma, *\}$.

Lemma 4.4.1. *For $1 \leq u \leq e_1$, the following hold.*

- (a) *The map $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_u$ if and only if $u \in \mathcal{J}_1$.*
- (b) *The map $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_u$ of order 2 if and only if $u \in \mathcal{J}_2$.*

Proof. (a) If $u \in \mathcal{J}_1$, then we have $d_u = 1$, from which it follows that $\tau_{1,-1}$ is the identity map on $\mathcal{F}_u \simeq \mathbb{F}_q$.

To prove the forward part, let us suppose that $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_u$. Here we assert that $u \in \mathcal{J}_1$. Since $\tau_{1,-1}$ is the identity map on $\mathcal{F}_u$, we have $x + \langle h_u(x) \rangle = \tau_{1,-1}(x + \langle h_u(x) \rangle) = x^{-1} + \langle h_u(x) \rangle$. This gives $x - x^{-1} \in \langle h_u(x) \rangle$. Note that there exists an integer i ($1 \leq i \leq \ell$) such that $h_u(x)$ divides $x^{m_i} - \omega_i$, which implies that $x^{m_i} \equiv \omega_i \pmod{h_u(x)}$, and hence $x^{-1} + \langle h_u(x) \rangle = \omega_i^{-1} x^{m_i-1} + \langle h_u(x) \rangle$. From this, it follows that $h_u(x)$ divides $\omega_i x^2 - x^{m_i}$. This implies that $h_u(x)$ divides $\omega_i x^2 - x^{m_i} + x^{m_i} - \omega_i = \omega_i(x^2 - 1)$. As $h_u(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$, we see that $h_u(x)$ is either $x+1$ or $x-1$, which gives $d_u = 1$. This shows that $u \in \mathcal{J}_1$.

- (b) It follows immediately from part (a) and using the fact that the map $\tau_{1,-1}$ is either the identity automorphism of $\mathcal{F}_u$ or the automorphism of $\mathcal{F}_u$ having order 2.

□

In the following lemma, we study some basic properties of the restriction map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ for each $\sigma \in \{0, \gamma, *\}$ and $1 \leq u \leq e_1$.

Lemma 4.4.2. *Let $1 \leq u \leq e_1$ be fixed.*

- (a) *For $u \in \mathcal{J}_1$ and $\sigma \in \{0, *\}$, the map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a symmetric and non-degenerate bilinear form on $\mathbb{G}_u$, i.e., $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an orthogonal space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_q$.*
- (b) *For $u \in \mathcal{J}_2$ and $\sigma \in \{0, *\}$, the map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$, i.e., $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_{q^{d_u}}$.*
- (c) *For $u \in \mathcal{J}_1$, the map $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is an alternating, reflexive and non-degenerate bilinear form on $\mathbb{G}_u$, i.e., $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_q$.*
- (d) *For $u \in \mathcal{J}_2$, the map $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a non-degenerate, reflexive and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$.*

Proof. To prove the result, one can easily verify that the map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$ for each u . Now to show that the map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is non-degenerate, let us suppose that $[A_u(x), B_u(x)]_\sigma = 0$ for all $B_u(x) \in \mathbb{G}_u$. Here we assert that $A_u(x) = \mathbf{0}$.

To prove this assertion, let $B(x) = (B_1(x), \dots, B_u(x), \dots, B_{e_3}(x))$ be an arbitrary element of $\mathbb{G}^\dagger$. Let $A(x) = (\mathbf{0}, \dots, \mathbf{0}, \underbrace{A_u(x)}_{u^{\text{th}}}, \mathbf{0}, \dots, \mathbf{0}) \in \mathbb{G}$. Here we see that

$$[A(x), B(x)]_\sigma = [A_u(x), B_u(x)]_\sigma = 0 \text{ for all } B(x) \in \mathbb{G}^\dagger.$$

By Lemma 4.3.1(d), we see that the sesquilinear form $[\cdot, \cdot]_\sigma$ is non-degenerate on $\mathbb{G} \times \mathbb{G}^\dagger$. From this, it follows that $A(x) = \mathbf{0}$, which gives $A_u(x) = \mathbf{0}$.

Further, when $\sigma \in \{0, *\}$, one can easily observe that

$$[A_u(x), B_u(x)]_\sigma = \tau_{1,-1}([B_u(x), A_u(x)]_\sigma) \quad \text{for all } A_u(x), B_u(x) \in \mathbb{G}_u.$$

From this and by applying Lemma 4.4.1, parts (a) and (b) follow immediately.

We next distinguish the following two cases: (i) $u \in \mathcal{J}_1$ and (ii) $u \in \mathcal{J}_2$.

- (i) Let $u \in \mathcal{J}_1$ be fixed. Here we see that $h_u(x)$ is either $x + 1$ or $x - 1$, which gives $d_u = 1$ and $\mathcal{F}_u \simeq \mathbb{F}_q$. In this case, we have $\mathbb{G}_u = (\epsilon_{u,1}\mathbb{F}_{q^t}, \epsilon_{u,2}\mathbb{F}_{q^t}, \dots, \epsilon_{u,\ell}\mathbb{F}_{q^t})$. We further observe that each element $A_u(x) \in \mathbb{G}_u$ is of the form $A_u(x) = A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell})$, where $A_{u,i} \in \epsilon_{u,i}\mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$. We also note, by Lemma 4.4.1(a), that the map $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_u$. We further observe that

$$[A_u, B_u]_\gamma = -[B_u, A_u]_\gamma \quad \text{for all } A_u, B_u \in \mathbb{G}_u.$$

In particular, we have $[A_u, A_u]_\gamma = -[A_u, A_u]_\gamma$, which gives $2[A_u, A_u]_\gamma = 0$ for all $A_u \in \mathbb{G}_u$. From this, it follows that $[A_u, A_u]_\gamma = 0$ when q is odd.

On the other hand, when q is even, we observe that all m_i 's and $\text{ord}(\omega_i)$'s are odd integers. This implies that the integer M is odd, and hence $\frac{M}{m_i} = 1$ in $\mathcal{F}_u \simeq \mathbb{F}_q$. We also observe that $\gamma^{q^{\frac{t}{2}}} = \gamma$, which implies that

$$\begin{aligned} [A_u, A_u]_\gamma &= \sum_{i=1}^{\ell} \epsilon_{u,i} \left(\sum_{\mu=0}^{t-1} \tau_{q^\mu,1}(\gamma A_{u,i} \tau_{q^{t/2},-1}(A_{u,i})) \right) = \sum_{i=1}^{\ell} \epsilon_{u,i} \left(\sum_{\mu=0}^{t-1} (\gamma A_{u,i} A_{u,i}^{q^{t/2}})^{q^\mu} \right) \\ &= \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t,q}(\gamma A_{u,i} A_{u,i}^{q^{t/2}}) = \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^{t/2},q}(\text{Tr}_{q^t,q^{t/2}}(\gamma A_{u,i} A_{u,i}^{q^{t/2}})) \\ &= \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^{t/2},q}(2\gamma A_{u,i} A_{u,i}^{q^{t/2}}) = 0 \quad \text{for all } A_u \in \mathbb{G}_u. \end{aligned}$$

This shows that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is alternating when $u \in \mathcal{J}_1$.

- (ii) Let $u \in \mathcal{J}_2$ be fixed. Here we see that $d_u = \deg h_u(x)$ is even. Further, by Lemma 4.4.1(b), we note that the map $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_u$ of order

2. Further, it is easy to observe that $[A_u(x), B_u(x)]_\gamma = -\tau_{1,-1}([B_u(x), A_u(x)]_\gamma)$ for all $A_u(x), B_u(x) \in \mathbb{G}_u$. This shows that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a skew-Hermitian form on $\mathbb{G}_u$.

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

In the following theorem, we characterize all σ -self-orthogonal, σ -self-dual and σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 4.4.1. *Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed. Let*

$$\mathcal{C} = \left(\bigoplus_{u=1}^{e_1} \mathcal{C}_u \right) \oplus \left(\bigoplus_{v=e_1+1}^{e_2} (\mathcal{C}_v \oplus \mathcal{C}_v^\dagger) \right) \oplus \left(\bigoplus_{w=e_2+1}^{e_3} \mathcal{C}_w \right)$$

be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, where $\mathcal{C}_u$ (resp. $\mathcal{C}_v, \mathcal{C}_v^\dagger$ and $\mathcal{C}_w$) is a subspace of $\mathbb{G}_u$ (resp. $\mathbb{G}_v, \mathbb{G}_v^\dagger$ and $\mathbb{G}_w$) over $\mathcal{F}_u$ (resp. $\mathcal{F}_v, \mathcal{F}_v^\dagger$ and $\mathcal{F}_w$) for each u (resp. v and w). For $\sigma \in \{0, \gamma, *\}$, the following hold.

(a) *The code $\mathcal{C}$ is σ -self-orthogonal if and only if its constituents satisfy the following conditions:*

- $\mathcal{C}_u$ is a σ -self-orthogonal $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$, (i.e., $\mathcal{C}_u \subseteq \mathcal{C}_u^{\perp_\sigma}$) for $1 \leq u \leq e_1$,
- $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$, and
- $\mathcal{C}_w = \{0\}$ for $e_2 + 1 \leq w \leq e_3$.

As a consequence, the total number $\mathfrak{M}$ of distinct σ -self-orthogonal Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{M} = \prod_{u=1}^{e_1} \mathfrak{M}_u \prod_{v=e_1+1}^{e_2} \mathfrak{M}_v, \quad (4.7)$$

where $\mathfrak{M}_u$ denotes the number of distinct σ -self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $1 \leq u \leq e_1$ and $\mathfrak{M}_v$ denotes the number of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$, where $\mathcal{C}_v$ is

an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$.

(b) The code $\mathcal{C}$ is σ -self-dual if and only if its constituents satisfy the following conditions:

- The irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ over $\mathbb{F}_q$ are either self-reciprocal or they form reciprocal pairs.
- $\dim_{\mathcal{F}_u} \mathbb{G}_u = \epsilon_u t$ is even and $\mathcal{C}_u$ is a σ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ (i.e., $\mathcal{C}_u = \mathcal{C}_u^{\perp\sigma}$) for $1 \leq u \leq e_1$, and
- $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger = \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$.

As a consequence, the total number $\mathfrak{N}$ of distinct σ -self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{N} = \prod_{u=1}^{e_1} \mathfrak{N}_u \prod_{v=e_1+1}^{e_2} \mathfrak{N}_v, \quad (4.8)$$

where $\mathfrak{N}_u$ denotes the number of distinct σ -self-dual $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $1 \leq u \leq e_1$ and $\mathfrak{N}_v$ denotes the number of distinct $\mathcal{F}_v$ -subspaces of $\mathbb{K}_v$ for $e_1 + 1 \leq v \leq e_2$.

(c) The code $\mathcal{C}$ is σ -ACD if and only if its constituents satisfy the following conditions:

- $\mathcal{C}_u$ is an $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ satisfying $\mathcal{C}_u \cap \mathcal{C}_u^{\perp\sigma} = \{\mathbf{0}\}$ (i.e., $\mathcal{C}_u$ is a σ -non-degenerate $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$) for $1 \leq u \leq e_1$ and
- $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{G}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{G}_v^\dagger$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ for $e_1 + 1 \leq v \leq e_2$.

As a consequence, the total number $\mathfrak{L}$ of distinct σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{L} = \prod_{u=1}^{e_1} \mathfrak{L}_u \prod_{v=e_1+1}^{e_2} \mathfrak{L}_v \prod_{w=e_2+1}^{e_3} \mathfrak{L}_w,$$

where $\mathfrak{L}_u$ denotes the number of distinct σ -non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $1 \leq u \leq e_1$, $\mathfrak{L}_v$ denotes the number of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$ with $\mathcal{C}_v$ as an $\mathcal{F}_v$ -subspace of $\mathbb{G}_v$ and $\mathcal{C}_v^\dagger$ as an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{G}_v^\dagger$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ for $e_1 + 1 \leq v \leq e_2$, and $\mathfrak{L}_w$ denotes the number of distinct $\mathcal{F}_w$ -subspaces of $\mathbb{G}_w$ for $e_2 + 1 \leq w \leq e_3$.

Proof. (a) By (4.5) and (4.6), we see that $\mathcal{C} \subseteq \mathcal{C}^{\perp\sigma}$ holds if and only if $\mathcal{C}_u \subseteq \mathcal{C}_u^{\perp\sigma}$ for $1 \leq u \leq e_1$, $\mathcal{C}_v$ (resp. $\mathcal{C}_v^\dagger$) is a subspace of $\mathbb{K}_v$ (resp. $\mathbb{K}_v^\dagger$) over $\mathcal{F}_v$ (resp. $\mathcal{F}_v^\dagger$) satisfying $\mathcal{C}_v \subseteq \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v$ and $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$, and $\mathcal{C}_w \subseteq \{\mathbf{0}\}$ and $\{\mathbf{0}\} \subseteq \mathcal{C}_w^{\perp\sigma}$ for $e_2 + 1 \leq w \leq e_3$. Further, for $e_1 + 1 \leq v \leq e_2$, we observe that $\mathcal{C}_v \subseteq \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v$ holds if and only if $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$. Furthermore, for $e_2 + 1 \leq w \leq e_3$, we see that $\mathcal{C}_w \subseteq \{\mathbf{0}\}$ and $\{\mathbf{0}\} \subseteq \mathcal{C}_w^{\perp\sigma}$ hold if and only if $\mathcal{C}_w = \{\mathbf{0}\}$. From this and by applying Theorem 3.3.1, part (a) follows immediately.

(b) By (4.5) and (4.6), we see that $\mathcal{C} = \mathcal{C}^{\perp\sigma}$ holds if and only if all the irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ over $\mathbb{F}_q$ are either self-reciprocal or they form reciprocal pairs, $\mathcal{C}_u = \mathcal{C}_u^{\perp\sigma}$ for $1 \leq u \leq e_1$, $\mathcal{C}_v = \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v$ and $\mathcal{C}_v^\dagger = \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$.

For $1 \leq u \leq e_1$, we further note, by Lemma 4.4.2, that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is non-degenerate. We also recall that $\dim_{\mathcal{F}_u} \mathbb{G}_u = \epsilon_u t$. Now if $\mathcal{C}_u$ is an $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ satisfying $\mathcal{C}_u = \mathcal{C}_u^{\perp\sigma}$, then by Theorem 4.3.1, we see that $\dim_{\mathcal{F}_u} \mathcal{C}_u = \dim_{\mathcal{F}_u} \mathcal{C}_u^{\perp\sigma} = \dim_{\mathcal{F}_u} \mathbb{G}_u - \dim_{\mathcal{F}_u} \mathcal{C}_u = \epsilon_u t - \dim_{\mathcal{F}_u} \mathcal{C}_u$, which implies that $\epsilon_u t = 2 \dim_{\mathcal{F}_u} \mathcal{C}_u$ is an even integer.

For $e_1 + 1 \leq v \leq e_2$, we see that $\mathcal{C}_v = \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v$ holds if and only if $\mathcal{C}_v^\dagger = \mathcal{C}_v^{\perp\sigma} \cap \mathbb{K}_v^\dagger$.

From this and by applying Theorem 3.3.1, part (b) follows immediately.

(c) By (4.5) and (4.6), we see that $\mathcal{C} \cap \mathcal{C}^{\perp\sigma} = \{\mathbf{0}\}$ if and only if $\mathcal{C}_u \cap \mathcal{C}_u^{\perp\sigma} = \{\mathbf{0}\}$, $\mathcal{C}_v$ (resp. $\mathcal{C}_v^\dagger$) is a subspace of $\mathbb{G}_v$ (resp. $\mathbb{G}_v^\dagger$) over $\mathcal{F}_v$ (resp. $\mathcal{F}_v^\dagger$) satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$, and $\mathcal{C}_w \cap \{\mathbf{0}\} = \{\mathbf{0}\}$ and $\{\mathbf{0}\} \cap \mathcal{C}_w^{\perp\sigma} = \{\mathbf{0}\}$ for each u, v and w . From this and by applying Theorem 3.3.1, part (c) follows immediately.

□

In the next chapter, we will apply Theorem 4.4.1 and some basic results on the geometry of symplectic, unitary and orthogonal spaces stated in Chapter 2 to enumerate all σ -self-orthogonal, σ -self-dual and σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for each $\sigma \in \{0, \gamma, *\}$.

5

Enumeration formulae for σ -self-orthogonal, σ -self-dual and σ -ACD multi-twisted additive codes over finite fields

5.1 Introduction

In this chapter, we obtain enumeration formulae for all σ -self-orthogonal, σ -self-dual and σ -ACD Ω -MT additive codes of length $n = m_1 + m_2 + \cdots + m_\ell$ and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$, where $m_1, m_2, \dots, m_\ell$ are positive integers coprime to q and $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ with $\omega_1, \omega_2, \dots, \omega_\ell \in \mathbb{F}_q \setminus \{0\}$. These enumeration formulae are useful in the classification of these three special classes of MT additive codes over finite fields up to monomial equivalence [35, Sec. 9.6 and 9.7].

This chapter is organized as follows: In Section 5.2, we count all σ -self-orthogonal Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$ (Theorem 5.2.1). In Section 5.3, we derive necessary and sufficient conditions for the existence of a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$. We further count all σ -self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ (Theorem 5.3.1). In Section 5.4, we count all σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$ (Theorem 5.3).

5.2 Enumeration of σ -self-orthogonal MT additive codes

In this section, we count all σ -self-orthogonal Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ by applying Theorem 4.4.1(a) and the Witt decomposition theory, where $\sigma \in \{0, \gamma, *\}$. For this, we recall, from Chapter 4, that $\mathcal{J}_1 = \{u : 1 \leq u \leq e_1, d_u = 1\}$ and $\mathcal{J}_2 = \{u : 1 \leq u \leq e_1, d_u \text{ is even}\}$.

In the following theorem, we enumerate all σ -self-orthogonal Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, where $\sigma \in \{0, \gamma, *\}$.

Theorem 5.2.1. *Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed, where $\omega_1, \omega_2, \dots, \omega_\ell$ are non-zero elements of $\mathbb{F}_q$. For $e_1 + 1 \leq v \leq e_2$, let η_v denote the number of integers i satisfying $1 \leq i \leq \ell$ and $\epsilon_{v,i} = \epsilon_{v,i}^\dagger = 1$. For $\sigma \in \{0, \gamma, *\}$, the total number $\mathfrak{M}$ of distinct σ -self-orthogonal Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by*

$$\mathfrak{M} = \prod_{u=1}^{e_1} \mathfrak{M}_u \prod_{v=e_1+1}^{e_2} \left(\sum_{k_1=0}^{\eta_v t} \sum_{k_2=0}^{\eta_v t - k_1} \begin{bmatrix} \eta_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \eta_v t - k_1 \\ k_2 \end{bmatrix}_{q^{d_v}} \right),$$

where for $1 \leq u \leq e_1$, the number $\mathfrak{M}_u$ equals

$$\bullet \sum_{k=0}^{\epsilon_u t/2} \left(\begin{bmatrix} \epsilon_u t/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d}{2}} + 1 \right) \right) \text{ when } u \in \mathcal{J}_1 \text{ with either } \sigma = \gamma \text{ or } \sigma = *$$

and both $\epsilon_u t, q$ being even;

- $\sum_{k=0}^{(\epsilon_u t - 1)/2} \left(\left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 1}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_1$ with either $\sigma = *$ and both $\epsilon_u t, q$ are odd or $\sigma = 0$ and $\epsilon_u t$ is odd;
- $\sum_{k=0}^{\epsilon_u t/2} \left(\left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_1, \sigma \in \{0, *\}$ with either ϵ_u even and $q \equiv 1 \pmod{4}$ or ϵ_u even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\epsilon_u t - 2)/2} \left(\left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_1, \sigma \in \{0, *\}$ with either ϵ_u odd, t even and $q \equiv 1 \pmod{4}$ or ϵ_u odd, $t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or $\epsilon_u \equiv 2 \pmod{4}, t$ odd and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\epsilon_u t - 2)/2} \left(\left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1 \right) \right) + \sum_{k'=1}^{\epsilon_u t/2} \left(q^{\epsilon_u t - 2k'} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k' - 1 \end{matrix} \right]_q \right. \\ \left. \times \prod_{d'=0}^{k'-2} \left(q^{\frac{\epsilon_u t - 2d' - 2}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_1, \sigma = 0$ and both $\epsilon_u t, q$ are even;
- $\sum_{k=0}^{\epsilon_u t/2} \left(\left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right]_{q^{d_u}} \prod_{b=0}^{k-1} \left(q^{\frac{d_u(\epsilon_u t - 2b - 1)}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_2, \sigma \in \{0, \gamma, *\}$ and $\epsilon_u t$ is even;
- $\sum_{k=0}^{(\epsilon_u t - 1)/2} \left(\left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right]_{q^{d_u}} \prod_{b=0}^{k-1} \left(q^{\frac{d_u(\epsilon_u t - 2b)}{2}} + 1 \right) \right)$ when $u \in \mathcal{J}_2, \sigma \in \{0, *\}$ and $\epsilon_u t$ is odd.

To prove the above theorem, we see, by Theorem 4.4.1(a), that it is enough to determine the number $\mathfrak{M}_u$ of distinct σ -self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $1 \leq u \leq e_1$ and the number $\mathfrak{M}_v$ of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$, where $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$ for $e_1 + 1 \leq v \leq e_2$.

In the following lemma, we determine the number $\mathfrak{M}_u$ for $1 \leq u \leq e_1$.

Lemma 5.2.1. *For $\sigma \in \{0, \gamma, *\}$, the following hold.*

(a) *When $u \in \mathcal{J}_1$, the number $\mathfrak{M}_u$ equals*

- $\sum_{k=0}^{\epsilon_u t/2} \left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1 \right)$ if $\sigma \in \{0, *\}$ with either ϵ_u even and $q \equiv 1 \pmod{4}$ or ϵ_u even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\epsilon_u t - 2)/2} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d}{2}} + 1 \right)$ if $\sigma \in \{0, *\}$ with either ϵ_u odd, t even and $q \equiv 1 \pmod{4}$ or ϵ_u odd, $t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or $\epsilon_u \equiv 2 \pmod{4}$, t odd and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\epsilon_u t - 1)/2} \left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 1}{2}} + 1 \right)$ if $\sigma \in \{0, *\}$ and both $\epsilon_u t, q$ are odd;
- $\sum_{k=0}^{(\epsilon_u t - 1)/2} \left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 1}{2}} + 1 \right)$ if $\sigma = 0$, q is even and $\epsilon_u t$ is odd;
- $\sum_{k=0}^{(\epsilon_u t - 2)/2} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1 \right) + \sum_{k'=1}^{\epsilon_u t/2} q^{\epsilon_u t - 2k'} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k' - 1 \end{matrix} \right]_q$
 $\times \prod_{d'=0}^{k'-2} \left(q^{\frac{\epsilon_u t - 2d' - 2}{2}} + 1 \right)$ if $\sigma = 0$ and both $\epsilon_u t, q$ are even;
- $\sum_{k=0}^{\epsilon_u t/2} \left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d}{2}} + 1 \right)$ if $\sigma = *$ and both $\epsilon_u t, q$ are even;
- $\sum_{k=0}^{\epsilon_u t/2} \left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right] \prod_{d=0}^{k-1} \left(q^{\frac{\epsilon_u t - 2d}{2}} + 1 \right)$ if $\sigma = \gamma$ and $\epsilon_u t$ is even.

(b) When $u \in \mathcal{J}_2$, we have

$$\mathfrak{M}_u = \begin{cases} \sum_{k=0}^{\epsilon_u t/2} \left[\begin{matrix} \epsilon_u t/2 \\ k \end{matrix} \right]_{q^{d_u}} \prod_{d=0}^{k-1} \left(q^{\frac{d_u(\epsilon_u t - 2d - 1)}{2}} + 1 \right) & \text{if } \epsilon_u t \text{ is even;} \\ \sum_{k=0}^{(\epsilon_u t - 1)/2} \left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right]_{q^{d_u}} \prod_{d=0}^{k-1} \left(q^{\frac{d_u(\epsilon_u t - 2d)}{2}} + 1 \right) & \text{if } \epsilon_u t \text{ is odd.} \end{cases}$$

Proof. (a) Let $u \in \mathcal{J}_1$. Here we have $d_u = \deg h_u(x) = 1$, and hence $\mathcal{F}_u \simeq \mathbb{F}_q$. In this case, we have $\mathbb{G}_u = (\epsilon_{u,1}\mathbb{F}_{q^t}, \epsilon_{u,2}\mathbb{F}_{q^t}, \dots, \epsilon_{u,\ell}\mathbb{F}_{q^t})$. Therefore each element $A_u(x) \in \mathbb{G}_u$ is of the form $A_u(x) = A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell})$, where $A_{u,i} \in \epsilon_{u,i}\mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$.

When $\sigma = \gamma$, we see, by Lemma 4.4.2(c), that $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_q$. Further, by Theorem 2.2.3(a), we note that the Witt index of $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is $\frac{\epsilon_u t}{2}$. From this and by Theorem 2.2.3(e), we get

$$\mathfrak{M}_u = \sum_{k=0}^{\epsilon_u t/2} \left(\begin{bmatrix} \epsilon_u t/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d}{2}} + 1) \right).$$

From this point on, let $\sigma \in \{0, *\}$. Here by Lemma 4.4.2(a), we see that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an orthogonal space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_q$. Now we shall distinguish the following three cases: **I.** q is odd, **II.** q is even and $\sigma = 0$ and **III.** q is even and $\sigma = *$.

I. Let q be odd. Here, we see that the orthogonal space $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ can also be viewed as a non-degenerate quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ over $\mathcal{F}_u$, where $\mathcal{Q}_u : \mathbb{G}_u \rightarrow \mathcal{F}_u$ is the quadratic map, defined as

$$\mathcal{Q}_u(A_u) = \frac{1}{2}[A_u, A_u]_\sigma \text{ for all } A_u \in \mathbb{G}_u.$$

Further, by Theorem 2.2.6, we note that the Witt index $\mathfrak{m}_u$ of the quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ is given by

$$\mathfrak{m}_u = \begin{cases} \frac{\epsilon_u t - 1}{2} & \text{if } \epsilon_u t \text{ is odd;} \\ \frac{\epsilon_u t}{2} & \text{if either } \epsilon_u \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is even,} \\ & \epsilon_u t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or } \epsilon_u \text{ is odd,} \\ & t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \frac{\epsilon_u t - 2}{2} & \text{if either } \epsilon_u \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is} \\ & \text{odd, } t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or } \epsilon_u \equiv 2 \pmod{4}, \\ & t \text{ is odd and } q \equiv 3 \pmod{4}. \end{cases} \quad (5.1)$$

Now by Theorem 2.2.5(e), we get

$$\mathfrak{M}_u = \sum_{k=0}^{\mathfrak{m}_u} \left(\begin{bmatrix} \mathfrak{m}_u \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\mathfrak{m}_u - 2d} + 1) \right),$$

where $\varrho = 2\mathfrak{m}_u - \epsilon_u t + 1$. Now on substituting the values of $\mathfrak{m}_u$ from (5.1), we get the desired values of $\mathfrak{M}_u$ in the respective cases.

II. Next, let $\sigma = 0$ and q be even. Here all m_i 's and $\text{ord}(\omega_i)$'s are odd integers, which implies that the integer M is odd, and hence $\frac{M}{m_i} = 1$ in $\mathcal{F}_u \simeq \mathbb{F}_q$. Now let us define the set

$$\mathbb{M}_u = \left\{ A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell}) \in \mathbb{G}_u : \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t, q}(A_{u,i}) = 0 \right\}.$$

One can easily observe that $\mathbb{M}_u$ is an $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ having dimension $\epsilon_u t - 1$. Now let us define

$$\Theta_u = (\epsilon_{u,1}, \epsilon_{u,2}, \dots, \epsilon_{u,\ell}) \in \mathbb{G}_u.$$

It is easy to see that $\Theta_u \in \mathbb{M}_u$ if and only if $\sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t, q}(1) = \sum_{i=1}^{\ell} \epsilon_{u,i} t = \epsilon_u t = 0$, which holds if and only if $\epsilon_u t$ is even. Now the following two cases arise: (i) $\epsilon_u t$ is odd and (ii) $\epsilon_u t$ is even.

(i) When $\epsilon_u t$ is odd, we note that $\Theta_u \notin \mathbb{M}_u$ and $\dim_{\mathcal{F}_u} \langle \Theta_u \rangle = 1$. Further, we see that $[A_u, \Theta_u]_0 = 0$ for all $A_u \in \mathbb{M}_u$ and $\mathbb{M}_u \cap \langle \Theta_u \rangle = \{\mathbf{0}\}$. This implies that $\mathbb{G}_u = \mathbb{M}_u \perp \langle \Theta_u \rangle$, i.e., $\mathbb{G}_u$ is an orthogonal direct sum of the $\mathcal{F}_u$ -subspaces $\mathbb{M}_u$ and $\langle \Theta_u \rangle$ of $\mathbb{G}_u$. Further, one can easily observe that any 0-self-orthogonal $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is contained in $\mathbb{M}_u$.

We next assert that the restriction $[\cdot, \cdot]_0 \upharpoonright_{\mathbb{M}_u \times \mathbb{M}_u}$ of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0$ to $\mathbb{M}_u \times \mathbb{M}_u$ is non-degenerate. For this, suppose that there exists $A_u \in \mathbb{M}_u$ satisfying $[A_u, B_u]_0 = 0$ for all $B_u \in \mathbb{M}_u$. Here we will show that $A_u = \mathbf{0}$.

For this, let $\mathcal{Y}_u = B_u + a_u \Theta_u \in \mathbb{G}_u$, where $a_u \in \mathcal{F}_u$. As a_u runs over $\mathcal{F}_u$ and B_u runs over $\mathbb{M}_u$, we see that $\mathcal{Y}_u$ runs over $\mathbb{G}_u$. Now we observe that $[A_u, \mathcal{Y}_u]_0 = [A_u, B_u]_0 + a_u [A_u, \Theta_u]_0 = 0$ for all $\mathcal{Y}_u \in \mathbb{G}_u$. By Lemma 4.4.2(a), we see that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0$ is non-degenerate on $\mathbb{G}_u$, we get $A_u = \mathbf{0}$. This proves the assertion.

Further, for each $A_u \in \mathbb{M}_u$, we observe that $[A_u, A_u]_0 = 0$. This

shows that $(\mathbb{M}_u, [\cdot, \cdot]_0 \upharpoonright_{\mathbb{M}_u \times \mathbb{M}_u})$ is a symplectic space over $\mathcal{F}_u$, whose dimension is $(\epsilon_u t - 1)$ and Witt index is $\frac{\epsilon_u t - 1}{2}$. Now by Theorem 2.2.3(e), for $0 \leq k \leq \frac{\epsilon_u t - 1}{2}$, we see that the total number of distinct k -dimensional 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{M}_u$ (and hence of $\mathbb{G}_u$) is given by

$$\left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d - 1}{2}} + 1).$$

From this and using the fact that the dimension of a maximal 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{M}_u$ is $\frac{\epsilon_u t - 1}{2}$, we obtain

$$\mathfrak{M}_u = \sum_{k=0}^{(\epsilon_u t - 1)/2} \left(\left[\begin{matrix} (\epsilon_u t - 1)/2 \\ k \end{matrix} \right]_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d - 1}{2}} + 1) \right).$$

- (ii) When $\epsilon_u t$ is even, we see that $\Theta_u \in \mathbb{M}_u \cap \mathbb{M}_u^{\perp_0}$. In this case, let $\widehat{\mathbb{M}}_u$ be an $(\epsilon_u t - 2)$ -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{M}_u$ satisfying $\Theta_u \notin \widehat{\mathbb{M}}_u$. One can easily see that $\mathbb{M}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$. Further, it is easy to observe that there exists an element $y_u \in \widehat{\mathbb{M}}_u^{\perp_0} \setminus \mathbb{M}_u$. This implies that $\mathbb{G}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle \oplus \langle y_u \rangle$. We also observe that any 0-self-orthogonal $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is either (i) contained in $\widehat{\mathbb{M}}_u$ or (ii) contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ but not in $\widehat{\mathbb{M}}_u$.

To determine the number $\mathfrak{M}_u$, we shall first count all 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$. Towards this, we note that $[A_u, A_u]_0 = 0$ for all $A_u \in \widehat{\mathbb{M}}_u$. Here we assert that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_u \times \widehat{\mathbb{M}}_u}$ is non-degenerate. For this, suppose that there exists $A_u \in \widehat{\mathbb{M}}_u$ satisfying $[A_u, B_u]_0 = 0$ for all $B_u \in \widehat{\mathbb{M}}_u$. To prove the above assertion, it suffices to show that $A_u = \mathbf{0}$. Let $\mathcal{X}_u = B_u + a_u y_u + b_u \Theta_u \in \mathbb{G}_u$, where $a_u, b_u \in \mathcal{F}_u$. We note that as A_u runs over the set $\widehat{\mathbb{M}}_u$ and elements a_u, b_u run over $\mathcal{F}_u$, the element $\mathcal{X}_u$ runs over $\mathbb{G}_u$. Now it is easy to see that $[A_u, \mathcal{X}_u]_0 = [A_u, B_u]_0 + a_u [A_u, y_u]_0 + b_u [A_u, \Theta_u]_0 = 0$ for all $\mathcal{X}_u \in \mathbb{G}_u$. Since the map $[\cdot, \cdot]_0$ is non-degenerate on $\mathbb{G}_u$, we get $A_u = \mathbf{0}$. From this, it follows that $(\widehat{\mathbb{M}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_u \times \widehat{\mathbb{M}}_u})$ is a symplectic

space of dimension $(\epsilon_u t - 2)$ over $\mathcal{F}_u$. Further, by Theorem 2.2.3(a), we see that the Witt index of $(\widehat{\mathbb{M}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_u \times \widehat{\mathbb{M}}_u})$ is $\frac{\epsilon_u t - 2}{2}$. Now by Theorem 2.2.3(e), we see that there are precisely

$$\mathfrak{T}_u = \sum_{k=0}^{(\epsilon_u t - 2)/2} \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1)$$

distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$, which are contained in $\widehat{\mathbb{M}}_u$.

Now we proceed to count all distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ that are contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ but not in $\widehat{\mathbb{M}}_u$. For this, let U be a k -dimensional 0-self-orthogonal $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$, which is contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$, but not in $\widehat{\mathbb{M}}_u$. One can easily see that $1 \leq k \leq \epsilon_u t/2$ and that any such $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ has a basis set of the form $\{A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u\}$, where $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{\mathbf{0}\}$ for $1 \leq h \leq k-1$ and $A_u^{(k)} \in \widehat{\mathbb{M}}_u$. Now one can easily observe that $U \subseteq U^{\perp_0}$ if and only if $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle \subseteq \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0} (\subseteq \widehat{\mathbb{M}}_u)$ and $A_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$. Since $(\widehat{\mathbb{M}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_u \times \widehat{\mathbb{M}}_u})$ is a symplectic space of dimension $(\epsilon_u t - 2)$ over $\mathcal{F}_u$ and has Witt index $\frac{\epsilon_u t - 2}{2}$. Now by Theorem 2.2.3(e), we see that for $1 \leq k \leq \epsilon_u t/2$, there are precisely

$$\begin{bmatrix} (\epsilon_u t - 2)/2 \\ k - 1 \end{bmatrix}_q \prod_{d=0}^{k-2} (q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1)$$

distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$ having dimension $k-1$. Further, for a given $(k-1)$ -dimensional 0-self-orthogonal $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ of $\widehat{\mathbb{M}}_u$, we observe that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, B_u^{(k)} + \Theta_u \rangle$ holds for some $A_u^{(k)}, B_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$ if and only if $A_u^{(k)} - B_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$. This implies that all $A_u^{(k)}$'s lying in the distinct cosets of the quotient space $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0} / \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ give rise to distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of the form $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$, and vice versa. Further, we see that the $\mathcal{F}_u$ -dimension of the quotient space $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0} /$

$\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ is $\epsilon_u t - 2k$, which implies that the element $A_u^{(k)}$ has $q^{\epsilon_u t - 2k}$ relevant choices. This shows that there are precisely

$$\mathfrak{U}_u = \sum_{k=1}^{\epsilon_u t/2} \left(q^{\epsilon_u t - 2k} \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k-1 \end{bmatrix}_q \prod_{d=0}^{k-2} (q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1) \right)$$

distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$, which are contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ but not in $\widehat{\mathbb{M}}_u$.

On combining both cases, we obtain

$$\begin{aligned} \mathfrak{M}_u = \mathfrak{T}_u + \mathfrak{U}_u &= \sum_{k=0}^{(\epsilon_u t - 2)/2} \left(\begin{bmatrix} (\epsilon_u t - 2)/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1) \right) \\ &\quad + \sum_{k=1}^{\epsilon_u t/2} \left(q^{\epsilon_u t - 2k} \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k-1 \end{bmatrix}_q \prod_{d=0}^{k-2} (q^{\frac{\epsilon_u t - 2d - 2}{2}} + 1) \right). \end{aligned}$$

III. Finally, let $\sigma = *$ and q be even. Here we must have $t \not\equiv 1 \pmod{\mathfrak{p}}$. Since q is even, we have $\mathfrak{p} = 2$, which implies that the integer t is even. As q is even, we also note that all m_i 's and $\text{ord}(\omega_i)$'s are odd integers, which implies that the integer M is odd, and hence $\frac{M}{m_i} = 1$ in $\mathcal{F}_u \simeq \mathbb{F}_q$. Now by (4.2), we see that

$$[A_u, A_u]_* = \sum_{i=1}^{\ell} \epsilon_{u,i} \left((\text{Tr}_{q^t, q}(A_{u,i}))^2 - \text{Tr}_{q^t, q}(A_{u,i}^2) \right) = 0 \text{ for all } A_u \in \mathbb{G}_u.$$

Further, by Lemma 4.4.2(a), we see that $[\cdot, \cdot]_* \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a reflexive and non-degenerate bilinear form. Hence $(\mathbb{G}_u, [\cdot, \cdot]_* \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space over $\mathcal{F}_u$ with dimension $\epsilon_u t$ and Witt index $\frac{\epsilon_u t}{2}$. Now by Theorem 2.2.3(e), we get

$$\mathfrak{M}_u = \sum_{k=0}^{\epsilon_u t/2} \left(\begin{bmatrix} \epsilon_u t/2 \\ k \end{bmatrix}_q \prod_{d=0}^{k-1} (q^{\frac{\epsilon_u t - 2d}{2}} + 1) \right).$$

(b) Next, let $u \in \mathcal{J}_2$. Here we see that the integer $d_u = \deg h_u(x)$ is even and $\mathcal{F}_u \simeq \mathbb{F}_{q^{d_u}}$. To determine the number $\mathfrak{M}_u$, we first note, by Lemma 4.4.2(b), that

$(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ over $\mathcal{F}_u$ when $\sigma \in \{0, *\}$. When $\sigma = \gamma$, by Lemma 4.4.2(d), we see that $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form. Now we will associate an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form with the skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$. For this, we see, by Lemma 4.4.1(b), that $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_u$ of order 2, and hence there exists $\varsigma_u(x) \in \mathcal{F}_u$ satisfying $\tau_{1,-1}(\varsigma_u(x)) \neq \varsigma_u(x)$. Now let us define $\zeta_u(x) = \varsigma_u(x) - \tau_{1,-1}(\varsigma_u(x)) (\neq 0) \in \mathcal{F}_u$, which satisfies $\tau_{1,-1}(\zeta_u(x)) = -\zeta_u(x)$. We further define a map $[\cdot, \cdot]_{\gamma_H} : \mathbb{G}_u \times \mathbb{G}_u \rightarrow \mathcal{F}_u$ as

$$[A_u(x), B_u(x)]_{\gamma_H} = \zeta_u(x)([A_u(x), B_u(x)]_\gamma) \text{ for all } A_u(x), B_u(x) \in \mathbb{G}_u.$$

It is easy to see that the map $[\cdot, \cdot]_{\gamma_H}$ is a non-degenerate, reflexive and Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$. That is, $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an $\epsilon_u t$ -dimensional unitary space over $\mathcal{F}_u \simeq \mathbb{F}_{q^{d_u}}$. Furthermore, one can easily observe that any $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is self-orthogonal with respect to the form $[\cdot, \cdot]_\gamma$ if and only if it is self-orthogonal with respect to the form $[\cdot, \cdot]_{\gamma_H}$. Therefore the number $\mathfrak{M}_u$ equals the number of distinct self-orthogonal $\mathcal{F}_u$ -subspaces of the unitary space $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$. Further, by Theorem 2.2.4(a), we see that the Witt index $\mathfrak{m}_u$ of the unitary space $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is given by

$$\mathfrak{m}_u = \begin{cases} \frac{\epsilon_u t}{2} & \text{if } \epsilon_u t \text{ is even;} \\ \frac{\epsilon_u t - 1}{2} & \text{if } \epsilon_u t \text{ is odd.} \end{cases} \quad (5.2)$$

Now for each $\sigma \in \{0, \gamma_H, *\}$ (and hence for $\sigma \in \{0, \gamma, *\}$), by applying Theorem 2.2.4(f), we get

$$\mathfrak{M}_u = \sum_{k=0}^{\mathfrak{m}_u} \left(\begin{bmatrix} \mathfrak{m}_u \\ k \end{bmatrix}_{q^{d_u}} \prod_{d=0}^{k-1} (q^{d_u(\mathfrak{m}_u - \rho - d)} + 1) \right),$$

where $\rho = \frac{1}{2}$ if $\epsilon_u t$ is even and $\rho = \frac{-1}{2}$ if $\epsilon_u t$ is odd. On substituting the values of the Witt index $\mathfrak{m}_u$ from (5.2) in the respective cases, part (b) follows immediately.

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

In the following lemma, we determine the number $\mathfrak{M}_v$ for $e_1 + 1 \leq v \leq e_2$.

Lemma 5.2.2. *For $\sigma \in \{0, *, \gamma\}$ and $e_1 + 1 \leq v \leq e_2$, we have*

$$\mathfrak{M}_v = \sum_{k_1=0}^{\eta_v t} \sum_{k_2=0}^{\eta_v t - k_1} \begin{bmatrix} \eta_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \eta_v t - k_1 \\ k_2 \end{bmatrix}_{q^{d_v}}.$$

Proof. To prove the result, let $e_1 + 1 \leq v \leq e_2$ be fixed. Here we recall that the number $\mathfrak{M}_v$ equals the number of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$, where $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$. We next observe that the formed space $(\mathbb{K}_v \times \mathbb{K}_v^\dagger, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{K}_v \times \mathbb{K}_v^\dagger})$ is non-degenerate. Now let $\mathcal{C}_v$ be an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ be an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$. Further, if the $\mathcal{F}_v$ -dimension of $\mathcal{C}_v$ is k_1 , then by Theorem 4.3.1, the $\mathcal{F}_v^\dagger$ -dimension of $\mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$ is $\eta_v t - k_1$, where $0 \leq k_1 \leq \eta_v t$. Since $\mathcal{C}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$, we see, by Lemma 2.2.1, that there are precisely $\sum_{k_2=0}^{\eta_v t - k_1} \begin{bmatrix} \eta_v t - k_1 \\ k_2 \end{bmatrix}_{q^{d_v}}$ distinct choices of $\mathcal{C}_v^\dagger$ for a given choice of the k_1 -dimensional $\mathcal{F}_v$ -subspace $\mathcal{C}_v$ of $\mathbb{K}_v$. Further, as $\mathcal{C}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ having dimension k_1 , we see, by Lemma 2.2.1 again, that the number of choices for $\mathcal{C}_v$ is given by $\begin{bmatrix} \eta_v t \\ k_1 \end{bmatrix}_{q^{d_v}}$ for $0 \leq k_1 \leq \eta_v t$. Hence the number $\mathfrak{M}_v$ of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$ with $\mathcal{C}_v$ as an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{C}_v^\dagger$ as an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{C}_v^\dagger \subseteq \mathcal{C}_v^{\perp_\sigma} \cap \mathbb{K}_v^\dagger$ is given by

$$\mathfrak{M}_v = \sum_{k_1=0}^{\eta_v t} \sum_{k_2=0}^{\eta_v t - k_1} \begin{bmatrix} \eta_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \eta_v t - k_1 \\ k_2 \end{bmatrix}_{q^{d_v}}.$$

This proves the lemma. $\square$

Proof of Theorem 5.2.1. On substituting the values of the numbers $\mathfrak{M}_u$ for $1 \leq u \leq e_1$ and the numbers $\mathfrak{M}_v$ for $e_1 + 1 \leq v \leq e_2$ from Lemmas 5.2.1 and 5.2.2 in equation (4.7), the desired result follows immediately. $\square$

The following examples illustrate Theorem 5.2.1.

Example 5.2.1. Let $q = 2$, $t = 2$, $\gamma = 1$, $m_1 = 3$, $m_2 = 5$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 8$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^3 - 1 =$

$(x+1)(x^2+x+1)$ and $x^{m_2}-\omega_2 = x^5-1 = (x+1)(x^4+x^3+x^2+x+1)$ are irreducible factorizations of the polynomials $x^{m_1}-\omega_1$ and $x^{m_2}-\omega_2$ over $\mathbb{F}_2$, respectively. Let us take $h_1(x) = x+1$, $h_2(x) = x^2+x+1$ and $h_3(x) = x^4+x^3+x^2+x+1$, which gives $d_1 = 1$, $d_2 = 2$, $d_3 = 4$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{3,2} = 1$ and $\epsilon_{2,2} = \epsilon_{3,1} = 0$. This implies that $\epsilon_1 = 2$ and $\epsilon_2 = \epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 744 distinct $\ast$ -self-orthogonal and 744 distinct γ -self-orthogonal Ω -MT additive codes of length 8 over $\mathbb{F}_{2^2}$, which agree with Theorem 5.2.1.

Example 5.2.2. Let $q = 5$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $\omega_1 = 1$ and $\omega_2 = 4$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 4)$. Here we see that $x^{m_1}-\omega_1 = x^2-1 = (x+1)(x+4)$ and $x^{m_2}-\omega_2 = x^4-4 = (x^2+2)(x^2+3)$ are irreducible factorizations of the polynomials $x^{m_1}-\omega_1$ and $x^{m_2}-\omega_2$ over $\mathbb{F}_5$, respectively. Let us take $h_1(x) = x+4$, $h_2(x) = x+4$, $h_3(x) = x^2+2$ and $h_3^\dagger(x) = x^2+3$, which gives $d_1 = d_2 = 1$, $d_3 = 2$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = \epsilon_{3,2}^\dagger = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = \epsilon_{3,1}^\dagger = 0$. This implies that $\epsilon_1 = \epsilon_2 = \eta_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 81 distinct 0-self-orthogonal and 81 distinct $\ast$ -self-orthogonal Ω -MT additive codes of length 6 over $\mathbb{F}_{5^2}$, which agree with Theorem 5.2.1.

Example 5.2.3. Let $q = 3$, $t = 2$, $m_1 = 2$, $m_2 = 4$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1}-\omega_1 = x^2-1 = (x+1)(x+2)$ and $x^{m_2}-\omega_2 = x^4-1 = (x+1)(x+2)(x^2+1)$ are irreducible factorizations of the polynomials $x^{m_1}-\omega_1$ and $x^{m_2}-\omega_2$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x+1$, $h_2(x) = x+2$ and $h_3(x) = x^2+1$, which gives $d_1 = d_2 = 1$, $d_3 = 2$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = \epsilon_{3,2} = 1$ and $\epsilon_{3,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = 2$ and $\epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 3125 distinct 0-self-orthogonal and 3125 distinct $\ast$ -self-orthogonal Ω -MT additive codes of length 6 over $\mathbb{F}_{3^2}$, which agree with Theorem 5.2.1.

Example 5.2.4. Let $q = 3$, $t = 3$, $m_1 = m_2 = 2$ and $\omega_1 = 1$ and $\omega_2 = 2$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 2)$. Here we see that $x^{m_1}-\omega_1 = x^2-1 = (x+1)(x+2)$ and $x^{m_2}-\omega_2 = x^2-2 = x^2+1$ are irreducible factorizations of the

polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 2$ and $h_3(x) = x^2 + 1$, which gives $d_1 = d_2 = 1$, $d_3 = 2$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 725 distinct 0-self-orthogonal and 725 distinct *-self-orthogonal Ω -MT additive codes of length 4 over $\mathbb{F}_{3^3}$, which agree with Theorem [5.2.1](#).

Example 5.2.5. Let $q = 5$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 4)$ and $x^{m_2} - \omega_2 = x^4 - 1 = (x + 1)(x + 2)(x + 3)(x + 4)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_5$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 4$, $h_3(x) = x + 2$ and $h_3^\dagger(x) = x + 3$, which gives $d_1 = d_2 = d_3 = 1$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = \epsilon_{3,2} = \epsilon_{3,2}^\dagger = 1$ and $\epsilon_{3,1} = \epsilon_{3,1}^\dagger = 0$. This implies that $\epsilon_1 = \epsilon_2 = 2$ and $\eta_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 50421 distinct 0-self-orthogonal and 50421 distinct *-self-orthogonal Ω -MT additive codes of length 6 over $\mathbb{F}_{5^2}$, which agree with Theorem [5.2.1](#).

Example 5.2.6. Let $q = 7$, $t = 2$, $m_1 = m_2 = 2$, $\omega_1 = 1$ and $\omega_2 = 2$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 2)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 6)$ and $x^{m_2} - \omega_2 = x^2 - 2 = (x + 3)(x + 4)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_7$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 6$, $h_3(x) = x + 3$ and $h_4(x) = x + 4$, which gives $d_1 = d_2 = d_3 = d_4 = 1$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = \epsilon_{4,2} = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = \epsilon_{4,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 9 distinct 0-self-orthogonal and *-self-orthogonal Ω -MT additive codes of length 4 over $\mathbb{F}_{7^2}$, which agree with Theorem [5.2.1](#).

Example 5.2.7. Let $q = 3$, $t = 4$, $m_1 = 4$ and $\omega_1 = 1$, so that $n = m_1 = 4$. Here we see that $x^{m_1} - \omega_1 = x^4 - 1 = (x + 1)(x + 2)(x^2 + 1)$ is irreducible factorization of the polynomial $x^{m_1} - \omega_1$ over $\mathbb{F}_3$. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 2$ and $h_3(x) = x^2 + 1$, which gives $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1$, $d_1 = d_2 = 1$ and $d_3 = 2$. Now by carrying out computations in the Magma Computational Algebra System, we

see that there are precisely 47553 distinct 0-self-orthogonal cyclic additive codes of length 4 over $\mathbb{F}_{3^4}$, which agree with Theorem 5.2.1.

Example 5.2.8. Let $q = 3$, $t = 3$, $m_1 = m_2 = 2$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^{m_2} - \omega_2 = x^2 - 1 = (x+1)(x+2)$ is irreducible factorization of the polynomial $x^{m_1} - \omega_1$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x + 1$ and $h_2(x) = x + 2$, which gives $d_1 = d_2 = 1$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = 1$. This implies that $\epsilon_1 = \epsilon_2 = 2$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 154449 distinct 0-self-orthogonal and 154449 distinct *-self-orthogonal Ω -MT additive codes of length 4 over $\mathbb{F}_{3^3}$, which agree with Theorem 5.2.1.

5.3 Enumeration of σ -self-dual MT additive codes

In the following theorem, we apply Theorem 4.4.1(b) and the Witt decomposition theory to derive a necessary and sufficient condition for the existence of a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, and we also provide enumeration formulae for all σ -self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ for each $\sigma \in \{0, \gamma, *\}$.

Theorem 5.3.1. *Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed. For $\sigma \in \{0, \gamma, *\}$, there exists a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ if and only if the irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ in $\mathbb{F}_q[x]$ are either self-reciprocal or they form reciprocal pairs, $\epsilon_u t$ is an even integer for $1 \leq u \leq e_1$, and the integers ϵ_u , t and q satisfy the following additional conditions:*

- either ϵ_u is even and $q \equiv 1 \pmod{4}$ or
- ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or
- ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$

for each $u \in \mathcal{J}_1$ when $\sigma \in \{0, *\}$ and q is odd. Under these conditions, the total number $\mathfrak{N}$ of distinct σ -self-dual Ω -MT additive codes of length n and block lengths

$(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{N} = \prod_{u \in \mathcal{J}_1} \mathfrak{N}_u \prod_{u \in \mathcal{J}_2} \left(\prod_{b=0}^{(\epsilon_u t/2)-1} (q^{\frac{d_u(\epsilon_u t - 2b - 1)}{2}} + 1) \right) \prod_{v=e_1+1}^{e_2} \left(\sum_{d=0}^{\eta_v t} \begin{bmatrix} \eta_v t \\ d \end{bmatrix}_{q^{d_v}} \right),$$

where for $u \in \mathcal{J}_1$, the number $\mathfrak{N}_u$ equals

- $\prod_{a=0}^{(\epsilon_u t/2)-1} \left(q^{\frac{\epsilon_u t - 2a - 2}{2}} + 1 \right)$ when $\sigma \in \{0, *\}$ with either ϵ_u even and $q \equiv 1 \pmod{4}$ or ϵ_u even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$.
- $\prod_{a=0}^{(\epsilon_u t/2)-2} \left(q^{\frac{\epsilon_u t - 2a - 2}{2}} + 1 \right)$ when $\sigma = 0$ and q is even.
- $\prod_{a=0}^{(\epsilon_u t/2)-1} \left(q^{\frac{\epsilon_u t - 2a}{2}} + 1 \right)$ when either $\sigma = \gamma$ or $\sigma = *$ and q is even.

To derive a necessary and sufficient condition for the existence of a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, we first prove the following lemma.

Lemma 5.3.1. *Let $1 \leq u \leq e_1$ be fixed. For $\sigma \in \{0, \gamma, *\}$, there exists a σ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ if and only if (i) $\epsilon_u t$ is an even integer and (ii) either ϵ_u is even and $q \equiv 1 \pmod{4}$ or ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$ when $\sigma \in \{0, *\}$, q is odd and $u \in \mathcal{J}_1$.*

Proof. To prove the result, let $\mathcal{C}_u$ be a σ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$, i.e., $\mathcal{C}_u = \mathcal{C}_u^{\perp \sigma}$. By Theorem 4.3.1, we get $\dim_{\mathcal{F}_u} \mathcal{C}_u = \dim_{\mathcal{F}_u^\dagger} \mathcal{C}_u^{\perp \sigma} = \dim_{\mathcal{F}_u} \mathbb{G}_u - \dim_{\mathcal{F}_u} \mathcal{C}_u = \epsilon_u t - \dim_{\mathcal{F}_u} \mathcal{C}_u$, which implies that $\epsilon_u t$ is an even integer and that $\dim_{\mathcal{F}_u} \mathcal{C}_u = \frac{\epsilon_u t}{2}$ for each u .

From now on, let $\epsilon_u t$ be an even integer. We also recall that $d_u = 1$ for all $u \in \mathcal{J}_1$ and the integer d_u is even for all $u \in \mathcal{J}_2$.

- (a) First of all, let $u \in \mathcal{J}_1$. In this case, we have $d_u = \deg h_u(x) = 1$, so that $\mathcal{F}_u \simeq \mathbb{F}_q$ and $\mathbb{G}_u = (\epsilon_{u,1} \mathbb{F}_{q^t}, \epsilon_{u,2} \mathbb{F}_{q^t}, \dots, \epsilon_{u,\ell} \mathbb{F}_{q^t})$. When $\sigma = \gamma$, we see, by Lemma 4.4.2(c), that $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ over $\mathcal{F}_u$. Further,

by Theorem 2.2.3(a), we see that the Witt index of $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is $\frac{\epsilon_u t}{2}$, and hence there exists a γ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$.

When q is even and $\sigma = 0$, we see, working as in the proof of Case II(ii) of Lemma 5.2.1(a), that there exists an $\frac{\epsilon_u t}{2}$ -dimensional 0-self-orthogonal (and hence a 0-self-dual) $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$.

Further, when q is even and $\sigma = *$, we see, working as in the proof of Case III of Lemma 5.2.1(a), that $(\mathbb{G}_u, [\cdot, \cdot]_* \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ and Witt index $\frac{\epsilon_u t}{2}$ over $\mathcal{F}_u$, and hence there exists a $*$ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$.

Finally, when q is odd and $\sigma \in \{0, *\}$, we see, by Lemma 4.4.2(a), that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an orthogonal space of dimension $\epsilon_u t$ over $\mathcal{F}_u$, which can be further viewed as a non-degenerate quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ over $\mathcal{F}_u$ with respect to the quadratic map $\mathcal{Q}_u : \mathbb{G}_u \rightarrow \mathcal{F}_u$, defined as $\mathcal{Q}_u(A_u) = \frac{1}{2} [A_u, A_u]_\sigma$ for all $A_u \in \mathbb{G}_u$. Here we observe that there exists a σ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ if and only if the Witt index of the quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ over $\mathcal{F}_u$ is $\frac{\epsilon_u t}{2}$, which, by (5.1), holds if and only if either ϵ_u is even and $q \equiv 1 \pmod{4}$ or ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$.

- (b) Next, let $u \in \mathcal{J}_2$ be fixed. Here $d_u = \deg h_u(x)$ is an even integer and $\mathcal{F}_u \simeq \mathbb{F}_{q^{d_u}}$. When $\sigma \in \{0, *\}$, we see, by Lemma 4.4.2(b), that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ and Witt index $\frac{\epsilon_u t}{2}$ over $\mathcal{F}_u$, and hence there exists a σ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$.

When $\sigma = \gamma$, we see, by Lemma 4.4.2(d), that the map $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$. Working as in the proof of Lemma 5.2.1(b), we place an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ on $\mathbb{G}_u$. Thus it is enough to consider the Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ on $\mathbb{G}_u$ instead of the skew-Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ on $\mathbb{G}_u$. As $\epsilon_u t$ is an even integer, we see, by Lemma 4.4.2(b) and Theorem 2.2.4(a), that $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ and Witt index $\frac{\epsilon_u t}{2}$ over $\mathcal{F}_u$. From this, it follows that there exists a γ -self-dual $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$.

On combining all the above cases, the desired result follows immediately. $\square$

From this point on, we assume, throughout this section, that the irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ in $\mathbb{F}_q[x]$ are either self-reciprocal or they form reciprocal pairs, $\epsilon_u t$ is an even integer for $1 \leq u \leq e_1$, and in the case when $\sigma \in \{0, *\}$ and q is odd, the integers ϵ_u, t and q satisfy the additional conditions:

- either ϵ_u is even and $q \equiv 1 \pmod{4}$ or
- ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or
- ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$

for each $u \in \mathcal{J}_1$. Further, we see, by (4.8), that to count all σ -self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, it is enough to determine the numbers $\mathfrak{N}_u$ for $1 \leq u \leq e_1$ and the numbers $\mathfrak{N}_v$ for $e_1 + 1 \leq v \leq e_2$.

In the following lemma, we determine the number $\mathfrak{N}_u$ for $1 \leq u \leq e_1$.

Lemma 5.3.2. *Suppose that $\epsilon_u t$ is an even integer for $1 \leq u \leq e_1$, and that either*

- ϵ_u is even and $q \equiv 1 \pmod{4}$ or
- ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or
- ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$

for each $u \in \mathcal{J}_1$ when $\sigma \in \{0, *\}$ and q is odd. For $\sigma \in \{0, \gamma, *\}$, the following hold.

(a) When $u \in \mathcal{J}_1$, we have

$$\mathfrak{N}_u = \begin{cases} \prod_{a=0}^{\frac{\epsilon_u t}{2}-1} \left(q^{\frac{\epsilon_u t - 2a - 2}{2}} + 1 \right) & \text{if } \sigma \in \{0, *\} \text{ with either } \epsilon_u \text{ even and } q \equiv 1 \pmod{4} \\ & \text{or } \epsilon_u \text{ even, } \epsilon_u t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \\ & \text{or } \epsilon_u \text{ odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \prod_{a=0}^{\frac{\epsilon_u t}{2}-2} \left(q^{\frac{\epsilon_u t - 2a - 2}{2}} + 1 \right) & \text{if } \sigma = 0 \text{ and } q \text{ is even;} \\ \prod_{a=0}^{\frac{\epsilon_u t}{2}-1} \left(q^{\frac{\epsilon_u t - 2a}{2}} + 1 \right) & \text{if either } \sigma = \gamma \text{ or } \sigma = * \text{ and } q \text{ is even.} \end{cases}$$

(b) When $u \in \mathcal{J}_2$, we have

$$\mathfrak{N}_u = \prod_{b=0}^{\frac{\epsilon_u t}{2}-1} \left(q^{\frac{d_u(\epsilon_u t - 2b - 1)}{2}} + 1 \right).$$

Proof. (a) When $u \in \mathcal{J}_1$, we note that $\deg h_u(x) = d_u = 1$, and hence $\mathcal{F}_u \simeq \mathbb{F}_q$. First of all, let $\sigma = \gamma$. Here by Lemma 4.4.2(c), we see that $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ and Witt index $\frac{\epsilon_u t}{2}$ over $\mathcal{F}_u$. Therefore, in this case, the number $\mathfrak{N}_u$ equals the number of distinct $\frac{\epsilon_u t}{2}$ -dimensional γ -self-orthogonal $\mathcal{F}_u$ -subspaces of $(\mathbb{G}_u, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$. This, by Theorem 2.2.3(e), implies that

$$\mathfrak{N}_u = \prod_{a=0}^{\frac{\epsilon_u t}{2}-1} (q^{\frac{\epsilon_u t - 2a}{2}} + 1).$$

From this point on, let $\sigma \in \{0, *\}$. Here when q is odd, we know that either ϵ_u is even and $q \equiv 1 \pmod{4}$ or ϵ_u is even, $\epsilon_u t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ϵ_u is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$. Further, by Lemma 4.4.2(a), we see that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an orthogonal space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_q$. Now the following three cases arise: **I.** q is odd, **II.** q is even and $\sigma = 0$ and **III.** q is even and $\sigma = *$.

I. Let q be odd. Here working as in Lemma 5.2.1(a), we see that the orthogonal space $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ can also be viewed as a non-degenerate quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ over $\mathcal{F}_u$, where $\mathcal{Q}_u : \mathbb{G}_u \rightarrow \mathcal{F}_u$ is the quadratic map, defined as $\mathcal{Q}_u(A_u) = \frac{1}{2}[A_u, A_u]_\sigma$ for all $A_u \in \mathbb{G}_u$. Further, by (5.1), we note that the corresponding quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ has Witt index $\frac{\epsilon_u t}{2}$. By Lemma 5.3.1, we see that a 0-self-orthogonal $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is 0-self-dual if and only if its $\mathcal{F}_u$ -dimension is $\frac{\epsilon_u t}{2}$. Now by Theorem 2.2.5(e), we see that the number $\mathfrak{N}_u$ of distinct $\frac{\epsilon_u t}{2}$ -dimensional 0-self-orthogonal (and hence 0-self-dual) $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ is given by

$$\mathfrak{N}_u = \prod_{a=0}^{\frac{\epsilon_u t}{2}-1} (q^{\frac{\epsilon_u t - 2a - 2}{2}} + 1).$$

II. Next, let $\sigma = 0$ and q be even. If

$$\mathbb{M}_u = \{A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell}) \in \mathbb{G}_u : \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t, q}(A_{u,i}) = 0\},$$

$\Theta_u = (\epsilon_{u,1}, \epsilon_{u,2}, \dots, \epsilon_{u,\ell}) \in \mathbb{G}_u$ and $\widehat{\mathbb{M}}_u$ is an $(\epsilon_u t - 2)$ -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{M}_u$ satisfying $\Theta_u \notin \widehat{\mathbb{M}}_u$, then we see that there exists an element $y_u \in \widehat{\mathbb{M}}_u^{\perp_0} \setminus \mathbb{M}_u$ such that $\mathbb{G}_u = \mathbb{M}_u \oplus \langle \Theta_u \rangle \oplus \langle y_u \rangle$. Further, we note that any $\frac{\epsilon_u t}{2}$ -dimensional 0-self-orthogonal (and hence a 0-self-dual) $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is contained in $\widehat{\mathbb{M}}_u \oplus \langle y_u \rangle$, but not in $\widehat{\mathbb{M}}_u$. Now working as in the proof of Case **II(ii)** of Lemma 5.2.1(a), we get

$$\mathfrak{N}_u = \prod_{a=0}^{\frac{\epsilon_u t}{2}-2} (q^{\frac{\epsilon_u t-2a-2}{2}} + 1).$$

III. Let $\sigma = *$ and q be even. Working as in the proof of Case **III** of Lemma 5.2.1(a), we see that $(\mathbb{G}_u, [\cdot, \cdot]_{\sigma} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space of dimension $\epsilon_u t$ over $\mathcal{F}_u$, whose Witt index is given by $\frac{\epsilon_u t}{2}$. Now by Theorem 2.2.3(e), we see that the number $\mathfrak{N}_u$ of distinct $\frac{\epsilon_u t}{2}$ -dimensional $*$ -self-orthogonal (and hence $*$ -self-dual) $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ is given by

$$\mathfrak{N}_u = \prod_{a=0}^{\frac{\epsilon_u t}{2}-1} (q^{\frac{\epsilon_u t-2a}{2}} + 1).$$

(b) Let $u \in \mathcal{J}_2$. Here $d_u = \deg h_u(x)$ is an even integer. By Lemma 4.4.2(b), we see that $(\mathbb{G}_u, [\cdot, \cdot]_{\sigma} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ over $\mathcal{F}_u$ when $\sigma \in \{0, *\}$. Further, by Lemma 4.4.2(d), we note that $[\cdot, \cdot]_{\gamma} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a reflexive, non-degenerate and a skew-Hermitian $\tau_{1,-1}$ -sesquilinear form. Here working as in the proof of Lemma 5.2.1(b), we can associate an orthogonality preserving non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ with the form $[\cdot, \cdot]_{\gamma} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$. That is, $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ over $\mathcal{F}_u$. From this, it follows that the number $\mathfrak{N}_u$ equals the number of distinct $\frac{\epsilon_u t}{2}$ -dimensional σ -self-orthogonal $\mathcal{F}_u$ -subspaces of the unitary space

$\mathbb{G}_u$ over $\mathcal{F}_u$. Now by Theorem 2.2.4(f), we get

$$\mathfrak{N}_u = \prod_{b=0}^{\frac{\epsilon_u t}{2}-1} \left(q^{\frac{d_u(\epsilon_u t - 2b - 1)}{2}} + 1 \right).$$

This proves the lemma. $\square$

In the following lemma, we determine the number $\mathfrak{N}_v$ for $e_1 + 1 \leq v \leq e_2$.

Lemma 5.3.3. *For $\sigma \in \{0, \gamma, *\}$ and $e_1 + 1 \leq v \leq e_2$, we have $\mathfrak{N}_v = \sum_{a=0}^{\eta_v t} \left[\begin{smallmatrix} \eta_v t \\ a \end{smallmatrix} \right]_{q^{d_v}}$.*

Proof. By (4.8), we see that the number $\mathfrak{N}_v$ equals the number of distinct $\mathcal{F}_v$ -subspaces of $\mathbb{K}_v$ for all $e_1 + 1 \leq v \leq e_2$. As $\dim_{\mathcal{F}_v} \mathbb{K}_v = \eta_v t$ and $\mathcal{F}_v \simeq \mathbb{F}_{q^{d_v}}$, by Lemma 2.2.1, we obtain

$$\mathfrak{N}_v = \sum_{a=0}^{\eta_v t} \left[\begin{smallmatrix} \eta_v t \\ a \end{smallmatrix} \right]_{q^{d_v}}.$$

$\square$

Proof of Theorem 5.3.1. The first part of the theorem follows immediately from Lemma 5.3.1 and Theorem 4.4.1(b). Further, on substituting the values of the numbers $\mathfrak{N}_u$ for $1 \leq u \leq e_1$ from Lemma 5.3.2 and the values of the numbers $\mathfrak{N}_v$ for $e_1 + 1 \leq v \leq e_2$ from Lemma 5.3.3 in equation (4.8), we get the desired result. $\square$

The following examples illustrate Theorem 5.3.1.

Example 5.3.1. Let $q = 2$, $t = 2$, $\gamma = 1$, $m_1 = 3$, $m_2 = 5$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 8$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^3 - 1 = (x+1)(x^2+x+1)$ and $x^{m_2} - \omega_2 = x^5 - 1 = (x+1)(x^4+x^3+x^2+x+1)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_2$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x^2 + x + 1$ and $h_3(x) = x^4 + x^3 + x^2 + x + 1$, which gives $d_1 = 1$, $d_2 = 2$, $d_3 = 4$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{3,2} = 1$ and $\epsilon_{2,2} = \epsilon_{3,1} = 0$. This implies that $\epsilon_1 = 2$ and $\epsilon_2 = \epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 45 distinct 0-self-dual, 225 distinct *-self-dual and 225 distinct γ -self-dual Ω -MT additive codes of length 8 over $\mathbb{F}_{2^2}$, which agree with Theorem 5.3.1.

Example 5.3.2. Let $q = 3$, $t = 2$, $m_1 = 2$, $m_2 = 4$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 2)$ and $x^{m_2} - \omega_2 = x^4 - 1 = (x + 1)(x + 2)(x^2 + 1)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 2$ and $h_3(x) = x^2 + 1$, which gives $d_1 = d_2 = 1, d_3 = 2$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = \epsilon_{3,2} = 1$ and $\epsilon_{3,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = 2$ and $\epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 256 distinct 0-self-dual and 256 distinct *-self-dual Ω -MT additive codes of length 6 over $\mathbb{F}_{3^2}$, which agree with Theorem [5.3.1](#).

Example 5.3.3. Let $q = 5$, $t = 2$, $m_1 = 2$, $m_2 = 4$, $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 4)$ and $x^{m_2} - \omega_2 = x^4 - 1 = (x + 1)(x + 2)(x + 3)(x + 4)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_5$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 4$, $h_3(x) = x + 2$ and $h_4(x) = x + 3$. Further, we see that $h_u(x) = h_u^\dagger(x)$ for $1 \leq u \leq 2$, $h_3(x) = h_4^\dagger(x)$, which gives $d_1 = d_2 = d_3 = 1$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = \epsilon_{3,2} = \epsilon_{3,2}^\dagger = 1$ and $\epsilon_{3,1} = \epsilon_{3,1}^\dagger = 0$. This implies that $\epsilon_1 = \epsilon_2 = 2$ and $\eta_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 1152 distinct 0-self-dual and 1152 distinct *-self-dual Ω -MT additive codes of length 6 over $\mathbb{F}_{5^2}$, which agree with Theorem [5.3.1](#).

Example 5.3.4. Let $q = 7$, $t = 2$, $m_1 = m_2 = 2$, $\omega_1 = 1$ and $\omega_2 = 6$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 6)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 6)$ and $x^{m_2} - \omega_2 = x^2 - 6 = x^2 + 1$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_7$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 6$ and $h_3(x) = x^2 + 1$, which gives $d_1 = d_2 = 1, d_3 = 2$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = \epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 32 distinct 0-self-dual and 32 distinct *-self-dual Ω -MT additive codes of length 4 over $\mathbb{F}_{7^2}$, which agree with Theorem [5.3.1](#).

5.4 Enumeration of σ -ACD MT additive codes

In this section, we count all σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ by applying Theorem 4.4.1(c) and the Witt decomposition theory, where $\sigma \in \{0, \gamma, *\}$. Towards this, for $e_1 + 1 \leq v \leq e_2$, let us define $\mathcal{I}_v = \{i : 1 \leq i \leq \ell, \epsilon_{v,i} = \epsilon_{v,i}^\dagger\}$ and $\mathcal{I}'_v = \{i : 1 \leq i \leq \ell, \epsilon_{v,i} \neq \epsilon_{v,i}^\dagger\}$. Here we note that $\{1, 2, \dots, \ell\} = \mathcal{I}_v \cup \mathcal{I}'_v$ (a disjoint union). It is easy to see that $\eta_v = \sum_{i \in \mathcal{I}_v} \epsilon_{v,i}$. Further, for each v , let us define the numbers $\varrho_v = \sum_{i \in \mathcal{I}'_v} \epsilon_{v,i}$ and $\tau_v = \sum_{i \in \mathcal{I}'_v} \epsilon_{v,i}^\dagger$. Now in the following theorem, we enumerate all σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, where $\sigma \in \{0, \gamma, *\}$.

Theorem 5.4.1. *Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed, where $\omega_1, \omega_2, \dots, \omega_\ell$ are non-zero elements of $\mathbb{F}_q$. For $\sigma \in \{0, \gamma, *\}$, the total number $\mathfrak{L}$ of distinct σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by*

$$\begin{aligned} \mathfrak{L} = & \prod_{u=1}^{e_1} \mathfrak{L}_u \prod_{v=e_1+1}^{e_2} \left(\sum_{k=0}^{\eta_v t} \sum_{k_1=0}^{\varrho_v t} \sum_{k_2=0}^{\tau_v t} q^{kd_v(\eta_v t - k)} \begin{bmatrix} \eta_v t \\ k \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \varrho_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \tau_v t \\ k_2 \end{bmatrix}_{q^{d_v}} \right) \\ & \times \prod_{w=e_2+1}^{e_3} \left(\sum_{a=0}^{\epsilon_w t} \begin{bmatrix} \epsilon_w t \\ a \end{bmatrix}_{q^{d_w}} \right), \end{aligned}$$

where for $1 \leq u \leq e_1$, the number $\mathfrak{L}_u$ equals

- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k)}{2}} \begin{bmatrix} \epsilon_u t / 2 \\ k / 2 \end{bmatrix}_{q^2}$ when $u \in \mathcal{J}_1$ with either $\sigma = \gamma$ and $\epsilon_u t$ being even
or $\sigma = *$ and both $\epsilon_u t, q$ are even;
- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k + 1)}{2}} \begin{bmatrix} (\epsilon_u t - 1) / 2 \\ k / 2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(\epsilon_u t - k)(k + 1)}{2}} \begin{bmatrix} (\epsilon_u t - 1) / 2 \\ (k - 1) / 2 \end{bmatrix}_{q^2}$ when
 $u \in \mathcal{J}_1$, $\sigma = *$ and both $\epsilon_u t, q$ are odd;
- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k)}{2}} \begin{bmatrix} \epsilon_u t / 2 \\ k / 2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(k\epsilon_u t - k^2 - 1)}{2}} (q^{\frac{\epsilon_u t}{2}} - 1) \begin{bmatrix} (\epsilon_u t - 2) / 2 \\ (k - 1) / 2 \end{bmatrix}_{q^2}$ when
 $u \in \mathcal{J}_1$, $\sigma \in \{0, *\}$ with either ϵ_u even and $q \equiv 1 \pmod{4}$ or $\epsilon_u t \equiv 0 \pmod{4}$,
 ϵ_u even and $q \equiv 3 \pmod{4}$ or ϵ_u odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$;

- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k)}{2}} \left[\frac{\epsilon_u t / 2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(k\epsilon_u t - k^2 - 1)}{2}} (q^{\frac{\epsilon_u t}{2}} + 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2}$ when $u \in \mathcal{J}_1$, $\sigma \in \{0, *\}$ with either ϵ_u odd, t even and $q \equiv 1 \pmod{4}$ or ϵ_u odd, $t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or $\epsilon_u \equiv 2 \pmod{4}$, t odd and $q \equiv 3 \pmod{4}$;
- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k + 1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(\epsilon_u t - k)(k+1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{(k-1)/2} \right]_{q^2}$ when $u \in \mathcal{J}_1$, $\sigma = 0$ and $\epsilon_u t$ is odd;
- $2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{(k\epsilon_u t - k^2 - 2)}{2}} \left\{ (q^k + q - 1) \left[\frac{(\epsilon_u t - 2)/2}{k/2} \right]_{q^2} + (q^{\epsilon_u t - k + 1} - q^{\epsilon_u t - k} + 1) \right. \\ \left. \times \left[\frac{(\epsilon_u t - 2)/2}{(k-2)/2} \right]_{q^2} \right\} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(k+1)\epsilon_u t - (k^2 + 1)}{2}} \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2}$ when $u \in \mathcal{J}_1$, $\sigma = 0$ and both $\epsilon_u t, q$ are even;
- $2 + \sum_{k=1}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k)d_u}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a}}{q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a}} \right)$ when $u \in \mathcal{J}_2$ and $\sigma \in \{0, \gamma, *\}$.

To prove the above theorem, we see, by Theorem 4.4.1(c), that the total number $\mathfrak{L}$ of distinct σ -ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is given by

$$\mathfrak{L} = \prod_{u=1}^{e_1} \mathfrak{L}_u \prod_{v=e_1+1}^{e_2} \mathfrak{L}_v \prod_{w=e_2+1}^{e_3} \mathfrak{L}_w, \quad (5.3)$$

where

- $\mathfrak{L}_u$ equals the number of distinct σ -non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $1 \leq u \leq e_1$;
- $\mathfrak{L}_v$ equals the number of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$ with $\mathcal{C}_v$ as an $\mathcal{F}_v$ -subspace of $\mathbb{G}_v$ and $\mathcal{C}_v^\dagger$ as an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{G}_v^\dagger$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\dagger\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^\perp = \{\mathbf{0}\}$ for $e_1 + 1 \leq v \leq e_2$; and
- $\mathfrak{L}_w$ equals the number of distinct $\mathcal{F}_w$ -subspaces of $\mathbb{G}_w$ for $e_2 + 1 \leq w \leq e_3$.

In view of the above, to prove Theorem 5.4.1, it is enough to determine the numbers $\mathfrak{L}_u$ for $1 \leq u \leq e_1$, $\mathfrak{L}_v$ for $e_1 + 1 \leq v \leq e_2$, and $\mathfrak{L}_w$ for $e_2 + 1 \leq w \leq e_3$. To do

this, we shall first determine the number $\mathfrak{L}_u$ for $u \in \mathcal{J}_1 \cup \mathcal{J}_2 = \{1, 2, \dots, e_1\}$. For this, we first note that if $\mathfrak{L}_{u,k}$ denotes the number of distinct k -dimensional σ -non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ for $0 \leq k \leq \epsilon_u t$, then we have $\mathfrak{L}_u = \sum_{k=0}^{\epsilon_u t} \mathfrak{L}_{u,k}$. Since the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is reflexive and non-degenerate, we see that $\mathfrak{L}_{u,0} = \mathfrak{L}_{u,\epsilon_u t} = 1$, which gives

$$\mathfrak{L}_u = 2 + \sum_{k=1}^{\epsilon_u t-1} \mathfrak{L}_{u,k} \quad \text{for } u \in \mathcal{J}_1 \cup \mathcal{J}_2 = \{1, 2, \dots, e_1\}. \quad (5.4)$$

5.4.1 Determination of the number $\mathfrak{L}_u$ when $u \in \mathcal{J}_1$

In this section, we will consider the case $u \in \mathcal{J}_1$, and we will determine the number $\mathfrak{L}_u$ for $\sigma \in \{0, \gamma, *\}$. Here we have $d_u = 1$, and hence $\mathcal{F}_u \simeq \mathbb{F}_q$. In this case, we have $\mathbb{G}_u = (\epsilon_{u,1}\mathbb{F}_{q^t}, \epsilon_{u,2}\mathbb{F}_{q^t}, \dots, \epsilon_{u,\ell}\mathbb{F}_{q^t})$. Therefore each element $A_u(x) \in \mathbb{G}_u$ is of the form $A_u(x) = A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell})$, where $A_{u,i} \in \epsilon_{u,i}\mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$.

In the following proposition, we determine the number $\mathfrak{L}_u$ when either $\sigma = \gamma$ or $\sigma = *$ and q is even.

Proposition 5.4.1. *Let $u \in \mathcal{J}_1$ be fixed. When either $\sigma = \gamma$ or $\sigma = *$ and q is even, we have*

$$\mathfrak{L}_u = 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t-1} q^{\frac{k(\epsilon_u t-k)}{2}} \left[\frac{\epsilon_u t/2}{k/2} \right]_{q^2}.$$

Proof. To prove the result, we see, by (5.4), that it is enough to determine the number $\mathfrak{L}_{u,k}$ for $1 \leq k \leq \epsilon_u t - 1$. Towards this, we note, by Lemma 4.4.2(c), that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space over $\mathcal{F}_u$ when $\sigma = \gamma$. Moreover, when $\sigma = *$ and q is even, we observe that $[A_u, A_u]_* = 0$ for all $A_u \in \mathbb{G}_u$. This, by Lemma 4.4.2(a), implies that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a symplectic space over $\mathcal{F}_u$. We further see that any k -dimensional σ -non-degenerate $\mathcal{F}_u$ -subspace W of $\mathbb{G}_u$ is also a symplectic space. Further, by Theorem 2.2.3, we see that the dimension k of W must be an even integer. This implies that $\mathfrak{L}_{u,k} = 0$ if k is odd.

Now let us consider the case when k is even, and let W be a k -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$. By Theorem 2.2.3(d), we see that W has a Witt decomposition

$$W = \langle A_u^{(1)}, B_u^{(1)} \rangle \perp \langle A_u^{(2)}, B_u^{(2)} \rangle \perp \dots \perp \langle A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})} \rangle,$$

where $(A_u^{(h)}, B_u^{(h)})$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k}{2}$ and the set $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})}\}$ is called a Witt basis (or a symplectic basis) of W over $\mathcal{F}_u$. By applying Theorems 2.2.2 and 2.2.3(c), we see that there are precisely

$$U_{\frac{k}{2}, \frac{\epsilon_u t}{2}} = H_{\frac{\epsilon_u t}{2}, 0} H_{\frac{\epsilon_u t-2}{2}, 0} \cdots H_{\frac{\epsilon_u t-k+2}{2}, 0} = q^{\frac{k(2\epsilon_u t-k)}{4}} \prod_{a=0}^{(k-2)/2} (q^{\epsilon_u t-2a} - 1)$$

distinct choices for the Witt bases $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})}\}$ of $\mathbb{G}_u$. Further, working as above, we see that a k -dimensional symplectic $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ has precisely

$$U_{\frac{k}{2}, \frac{k}{2}} = H_{\frac{k}{2}, 0} H_{\frac{k-2}{2}, 0} \cdots H_{1, 0} = q^{\frac{k^2}{4}} \prod_{a=0}^{(k-2)/2} (q^{k-2a} - 1)$$

distinct choices for the Witt basis. Therefore the number $\mathfrak{L}_{u,k}$ is given by

$$\mathfrak{L}_{u,k} = \frac{U_{\frac{k}{2}, \frac{\epsilon_u t}{2}}}{U_{\frac{k}{2}, \frac{k}{2}}} = q^{\frac{k(\epsilon_u t-k)}{2}} \left[\frac{\epsilon_u t/2}{k/2} \right]_{q^2}.$$

From this and by (5.4), the desired result follows immediately. $\square$

In the following proposition, we determine the number $\mathfrak{L}_u$ when q is odd and $\sigma \in \{0, *\}$.

Proposition 5.4.2. *Let $u \in \mathcal{J}_1$ be fixed. When $\sigma \in \{0, *\}$ and q is an odd prime power, we have*

$$\mathfrak{L}_u = \begin{cases} 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t-1} q^{\frac{k(\epsilon_u t-k+1)}{2}} \left[\frac{(\epsilon_u t-1)/2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t-1} q^{\frac{(\epsilon_u t-k)(k+1)}{2}} \left[\frac{(\epsilon_u t-1)/2}{(k-1)/2} \right]_{q^2} \\ \text{if } \epsilon_u t \text{ is odd;} \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t-1} q^{\frac{k(\epsilon_u t-k)}{2}} \left[\frac{\epsilon_u t/2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t-1} q^{\frac{(k\epsilon_u t-k^2-1)}{2}} (q^{\frac{\epsilon_u t}{2}} - 1) \left[\frac{(\epsilon_u t-2)/2}{(k-1)/2} \right]_{q^2} \\ \text{if either } \epsilon_u \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is even, } \epsilon_u t \equiv 0 \pmod{4} \text{ and } \\ q \equiv 3 \pmod{4} \text{ or } \epsilon_u \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t-1} q^{\frac{k(\epsilon_u t-k)}{2}} \left[\frac{\epsilon_u t/2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t-1} q^{\frac{(k\epsilon_u t-k^2-1)}{2}} (q^{\frac{\epsilon_u t}{2}} + 1) \left[\frac{(\epsilon_u t-2)/2}{(k-1)/2} \right]_{q^2} \\ \text{if either } \epsilon_u \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is odd, } t \equiv 0 \pmod{4} \\ \text{and } q \equiv 3 \pmod{4} \text{ or } \epsilon_u \equiv 2 \pmod{4}, t \text{ is odd and } q \equiv 3 \pmod{4}. \end{cases}$$

Proof. To prove the result, when $\sigma \in \{0, *\}$, we see, by Lemma 4.4.2(a), that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is an $(\epsilon_u t)$ -dimensional orthogonal space over $\mathcal{F}_u$. Further, as q is odd, the orthogonal space $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ can be viewed as a non-degenerate quadratic space $(\mathbb{G}_u, \mathcal{Q}_u)$ over $\mathcal{F}_u$, where $\mathcal{Q}_u : \mathbb{G}_u \rightarrow \mathcal{F}_u$ is the quadratic map, defined as

$$\mathcal{Q}_u(A_u) = \frac{1}{2}[A_u, A_u]_\sigma \text{ for all } A_u \in \mathbb{G}_u.$$

Further, by Theorem 2.2.6, we note that the Witt index $\mathfrak{m}_u$ of $\mathbb{G}_u$ is given by

$$\mathfrak{m}_u = \begin{cases} \frac{\epsilon_u t - 1}{2} & \text{if } \epsilon_u t \text{ is odd;} \\ \frac{\epsilon_u t}{2} & \text{if either } \epsilon_u \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is even, } \epsilon_u t \equiv 0 \pmod{4}, \\ & \text{and } q \equiv 3 \pmod{4} \text{ or } \epsilon_u \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \frac{\epsilon_u t - 2}{2} & \text{if either } \epsilon_u \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \epsilon_u \text{ is odd,} \\ & t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or } \epsilon_u \equiv 2 \pmod{4}, t \text{ is odd and} \\ & q \equiv 3 \pmod{4}. \end{cases} \quad (5.5)$$

To determine the number $\mathfrak{L}_u$, we see, by (5.4), that it is enough to determine the number $\mathfrak{L}_{u,k}$ for $1 \leq k \leq \epsilon_u t - 1$. So from now on, let $1 \leq k \leq \epsilon_u t - 1$ be fixed. Now let W be a σ -non-degenerate and quadratic $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ such that $\dim_{\mathcal{F}_u} W = k$. By Theorem 2.2.5(d), we see that the Witt decomposition of W is given by

$$W = \langle A_u^{(1)}, B_u^{(1)} \rangle \perp \langle A_u^{(2)}, B_u^{(2)} \rangle \perp \dots \perp \langle A_u^{(\mathfrak{m}_k)}, B_u^{(\mathfrak{m}_k)} \rangle \perp \mathcal{W}_k,$$

where $\mathfrak{m}_k$ is the Witt index of W , $(A_u^{(h)}, B_u^{(h)})$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \mathfrak{m}_k$, and $\mathcal{W}_k$ is an anisotropic $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ satisfying $\dim_{\mathcal{F}_u} \mathcal{W}_k = k - 2\mathfrak{m}_k \leq 2$. Now we shall consider the following two cases separately: (i) k is odd and (ii) k is even.

(i) First let k be odd. Here we observe that $\dim_{\mathcal{F}_u} \mathcal{W}_k = 1$, which, by Theorem 2.2.5(d), implies that $\mathfrak{m}_k = \frac{k-1}{2}$. This further implies that the $\mathcal{F}_u$ -subspace W has a Witt decomposition

$$W = \langle A_u^{(1)}, B_u^{(1)} \rangle \perp \langle A_u^{(2)}, B_u^{(2)} \rangle \perp \dots \perp \langle A_u^{(\frac{k-1}{2})}, B_u^{(\frac{k-1}{2})} \rangle \perp \langle Z_u \rangle,$$

where $(A_u^{(h)}, B_u^{(h)})$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k-1}{2}$ and Z_u is a non-singular vector in $\mathbb{G}_u$. The set $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k-1}{2})}, B_u^{(\frac{k-1}{2})}, Z_u\}$ is

called a Witt basis (or quadratic basis) of W over $\mathcal{F}_u$. By applying Theorems 2.2.2, 2.2.5(b) & (c) and 2.2.7, we see that there are precisely

$$U_{\frac{k-1}{2}, \mathfrak{m}_u} = H_{\mathfrak{m}_u, \epsilon_u t - 2\mathfrak{m}_u} \cdots H_{\mathfrak{m}_u - \frac{(k-3)}{2}, \epsilon_u t - 2\mathfrak{m}_u} (q^{\epsilon_u t - k + 1} - 1 - I_{\mathfrak{m}_u - \frac{(k-1)}{2}, \epsilon_u t - 2\mathfrak{m}_u})$$

$$= \begin{cases} q^{\frac{2\epsilon_u t k - (k+1)^2}{4}} (q^{\frac{\epsilon_u t}{2}} - 1)(q-1) \prod_{a=1}^{(k-1)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ q^{\frac{2\epsilon_u t(k+1) - k(k+4) + 1}{4}} (q-1) \prod_{a=1}^{(k-3)/2} (q^{\epsilon_u t - 2a - 1} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ q^{\frac{2\epsilon_u t k - (k+1)^2}{4}} (q^{\frac{\epsilon_u t}{2}} + 1)(q-1) \prod_{a=1}^{(k-1)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2} \end{cases}$$

distinct choices for the Witt basis $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k-1}{2})}, B_u^{(\frac{k-1}{2})}, Z_u\}$ of $\mathbb{G}_u$. Further, working as above, we see that a k -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ has precisely

$$U_{\frac{k-1}{2}, \frac{k-1}{2}} = H_{\frac{k-1}{2}, 1} H_{\frac{k-3}{2}, 1} \cdots H_{1, 1} (q-1) = q^{\frac{(k-1)^2}{4}} (q-1) \prod_{a=0}^{(k-3)/2} (q^{k-2a-1} - 1)$$

distinct choices of the Witt basis. Therefore, the number $\mathfrak{L}_{u,k}$ is given by

$$\mathfrak{L}_{u,k} = \frac{U_{\frac{k-1}{2}, \mathfrak{m}_u}}{U_{\frac{k-1}{2}, \frac{k-1}{2}}} = \begin{cases} q^{\frac{(k\epsilon_u t - k^2 - 1)}{2}} (q^{\frac{\epsilon_u t}{2}} - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ q^{\frac{(\epsilon_u t - k)(k+1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{(k-1)/2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ q^{\frac{(k\epsilon_u t - k^2 - 1)}{2}} (q^{\frac{\epsilon_u t}{2}} + 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases} \quad (5.6)$$

(ii) Next, let k be even. In this case, by Theorem 2.2.5(d), we note that either $\mathfrak{m}_k = \frac{k}{2}$ or $\mathfrak{m}_k = \frac{k-2}{2}$. Let $R_{u,k}$ and $S_{u,k}$ denote the number of k -dimensional σ -non-degenerate quadratic $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ having Witt indices $\frac{k}{2}$ and $\frac{k-2}{2}$, respectively. Note that $\mathfrak{L}_{u,k} = R_{u,k} + S_{u,k}$.

When $\mathfrak{m}_k = \frac{k}{2}$, we have $\dim_{\mathcal{F}_u} \mathcal{W}_k = 0$. This implies that the $\mathcal{F}_u$ -subspace W has a Witt decomposition

$$W = \langle A_u^{(1)}, B_u^{(1)} \rangle \perp \langle A_u^{(2)}, B_u^{(2)} \rangle \perp \dots \perp \langle A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})} \rangle,$$

where $(A_u^{(h)}, B_u^{(h)})$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k}{2}$ and the set $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})}\}$ is called a Witt basis of W over $\mathcal{F}_u$. By applying Theorems 2.2.2, 2.2.5(c) and 2.2.7, we see that there are precisely

$$U_{\frac{k}{2}, \mathfrak{m}_u} = H_{\mathfrak{m}_u, \epsilon_u t - 2\mathfrak{m}_u} H_{\mathfrak{m}_u - 1, \epsilon_u t - 2\mathfrak{m}_u} \cdots H_{\mathfrak{m}_u - \frac{k-2}{2}, \epsilon_u t - 2\mathfrak{m}_u}$$

$$= \begin{cases} q^{\frac{k(2\epsilon_u t - k - 2)}{4}} (q^{\frac{\epsilon_u t}{2}} - 1)(q^{\frac{\epsilon_u t - k}{2}} + 1) \prod_{a=1}^{(k-2)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ q^{\frac{k(2\epsilon_u t - k - 2)}{4}} \prod_{a=0}^{(k-2)/2} (q^{\epsilon_u t - 2a - 1} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ q^{\frac{k(2\epsilon_u t - k - 2)}{4}} (q^{\frac{\epsilon_u t}{2}} + 1)(q^{\frac{\epsilon_u t - k}{2}} - 1) \prod_{a=1}^{(k-2)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2} \end{cases}$$

distinct choices for the Witt basis $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k}{2})}, B_u^{(\frac{k}{2})}\}$ of $\mathbb{G}_u$. Further, working as above, we see that a k -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ has precisely

$$U_{\frac{k}{2}, \frac{k}{2}} = H_{\frac{k}{2}, 0} H_{\frac{k-2}{2}, 0} \cdots H_{1, 0} = 2q^{\frac{k(k-2)}{4}} (q^{\frac{k}{2}} - 1) \prod_{a=1}^{(k-2)/2} (q^{k-2a} - 1)$$

distinct choices for the Witt basis. Therefore the number $R_{u,k}$ is given by

$$R_{u,k} = \frac{U_{\frac{k}{2}, \mathfrak{m}_u}}{U_{\frac{k}{2}, \frac{k}{2}}} = \begin{cases} \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} + 1)(q^{\frac{\epsilon_u t - k}{2}} + 1) \left[\frac{\epsilon_u t}{2} \right]_{q^2}}{2(q^{\frac{\epsilon_u t}{2}} + 1)} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} + 1) \left[(\epsilon_u t - 1)/2 \right]_{q^2}}{2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} + 1)(q^{\frac{\epsilon_u t - k}{2}} - 1) \left[\frac{\epsilon_u t}{2} \right]_{q^2}}{2(q^{\frac{\epsilon_u t}{2}} - 1)} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases}$$

When $\mathfrak{m}_k = \frac{k-2}{2}$, we see that $\dim_{\mathcal{F}_u} \mathcal{W}_k = 2$. Here working as in Lemmas 3.2 and 3.3 of Sharma and Kaur [58], we observe that $\mathcal{W}_k$ has an orthogonal basis over $\mathcal{F}_u$ and that the number $X_{k, \mathfrak{m}_u}$ of distinct orthogonal bases of $\mathcal{W}_k$ is given

by

$$X_{k, \mathfrak{m}_u} = \begin{cases} \frac{q^{\epsilon_u t - k} (q - 1)^2 (q^{\frac{\epsilon_u t - k}{2}} - 1) (q^{\frac{\epsilon_u t - k + 2}{2}} - 1)}{2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ \frac{q^{\epsilon_u t - k} (q - 1)^2 (q^{\epsilon_u t - k + 1} - 1)}{2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ \frac{q^{\epsilon_u t - k} (q - 1)^2 (q^{\frac{\epsilon_u t - k}{2}} + 1) (q^{\frac{\epsilon_u t - k + 2}{2}} + 1)}{2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases}$$

Thus the k -dimensional $\mathcal{F}_u$ -subspace W of $\mathbb{G}_u$ has a Witt decomposition

$$W = \langle A_u^{(1)}, B_u^{(1)} \rangle \perp \langle A_u^{(2)}, B_u^{(2)} \rangle \perp \dots \perp \langle A_u^{(\frac{k-2}{2})}, B_u^{(\frac{k-2}{2})} \rangle \perp \langle Z_u^{(1)}, Z_u^{(2)} \rangle,$$

where $(A_u^{(h)}, B_u^{(h)})$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k-2}{2}$ and $\{Z_u^{(1)}, Z_u^{(2)}\}$ is an orthogonal basis of the $\mathcal{F}_u$ -subspace $\mathcal{W}_k$ of W . The set $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k-2}{2})}, B_u^{(\frac{k-2}{2})}, Z_u^{(1)}, Z_u^{(2)}\}$ is called a Witt basis of W over $\mathcal{F}_u$. By applying Theorems [2.2.2](#), [2.2.5\(d\)](#) and [2.2.7](#), we see that the number $U_{\frac{k-2}{2}, \mathfrak{m}_u}$ of distinct choices for the Witt basis $\{A_u^{(1)}, B_u^{(1)}, A_u^{(2)}, B_u^{(2)}, \dots, A_u^{(\frac{k-2}{2})}, B_u^{(\frac{k-2}{2})}, Z_u^{(1)}, Z_u^{(2)}\}$ of $\mathbb{G}_u$ is given by

$$\begin{aligned} U_{\frac{k-2}{2}, \mathfrak{m}_u} &= H_{\mathfrak{m}_u, \epsilon_u t - 2\mathfrak{m}_u} H_{\mathfrak{m}_u - 1, \epsilon_u t - 2\mathfrak{m}_u} \cdots H_{\mathfrak{m}_u - \frac{(k-4)}{2}, \epsilon_u t - 2\mathfrak{m}_u} X_{k, \mathfrak{m}_u} \\ &= \begin{cases} q^{\frac{k(2\epsilon_u t - k - 2)}{4}} \frac{(q^{\frac{\epsilon_u t}{2}} - 1)(q^{\frac{\epsilon_u t - k}{2}} - 1)(q - 1)^2}{2} \prod_{a=1}^{(k-2)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ q^{\frac{k(2\epsilon_u t - k - 2)}{4}} \frac{(q - 1)^2}{2} \prod_{a=0}^{(k-2)/2} (q^{\epsilon_u t - 2a - 1} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ q^{\frac{k(2\epsilon_u t - k - 2)}{4}} \frac{(q^{\frac{\epsilon_u t}{2}} + 1)(q^{\frac{\epsilon_u t - k}{2}} + 1)(q - 1)^2}{2} \prod_{a=1}^{(k-2)/2} (q^{\epsilon_u t - 2a} - 1) & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases} \end{aligned}$$

Further, working as above, we see that a k -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ with Witt index $\frac{k-2}{2}$ has precisely

$$\begin{aligned} U_{\frac{k-2}{2}, \frac{k-2}{2}} &= H_{\frac{k-2}{2}, 2} H_{\frac{k-4}{2}, 2} \cdots H_{1, 2} (q^2 - 1)(q - 1) \\ &= q^{\frac{k(k-2)}{2}} (q^{\frac{k}{2}} + 1)(q - 1)^2 \prod_{a=1}^{(k-2)/2} (q^{k-2a} - 1). \end{aligned}$$

distinct choices for the Witt basis. Therefore the number $S_{u,k}$ is given by

$$S_{u,k} = \frac{U_{\frac{k-2}{2}, \mathfrak{m}_u}}{U_{\frac{k-2}{2}, \frac{k-2}{2}}} = \begin{cases} \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} - 1) (q^{\frac{\epsilon_u t - k}{2}} - 1) \left[\frac{\epsilon_u t}{2} \right]_{q^2}}{2(q^{\frac{\epsilon_u t}{2}} + 1)} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} - 1) \left[\frac{(\epsilon_u t - 1)/2}{k/2} \right]_{q^2}}{2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ \frac{q^{\frac{k(\epsilon_u t - k)}{2}} (q^{\frac{k}{2}} - 1) (q^{\frac{\epsilon_u t - k}{2}} + 1) \left[\frac{\epsilon_u t}{2} \right]_{q^2}}{2(q^{\frac{\epsilon_u t}{2}} - 1)} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases}$$

From this, it follows that

$$\mathfrak{L}_{u,k} = R_{u,k} + S_{u,k} = \begin{cases} q^{\frac{k(\epsilon_u t - k)}{2}} \left[\frac{\epsilon_u t}{2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t}{2}; \\ q^{\frac{k(\epsilon_u t - k + 1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{k/2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 1}{2}; \\ q^{\frac{k(\epsilon_u t - k)}{2}} \left[\frac{\epsilon_u t}{2} \right]_{q^2} & \text{if } \mathfrak{m}_u = \frac{\epsilon_u t - 2}{2}. \end{cases} \quad (5.7)$$

Finally, on substituting the values of $\mathfrak{L}_{u,k}$ from (5.6) and (5.7) in equation (5.4), the desired result follows. $\square$

In the following proposition, we determine the number $\mathfrak{L}_u$ when q is even and $\sigma = 0$.

Proposition 5.4.3. *Let $u \in \mathcal{J}_1$ be fixed. When $\sigma = 0$ and q is an even prime power, we have*

$$\mathfrak{L}_u = \begin{cases} 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k + 1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{k/2} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(\epsilon_u t - k)(k + 1)}{2}} \left[\frac{(\epsilon_u t - 1)/2}{(k - 1)/2} \right]_{q^2} & \text{if } \epsilon_u t \text{ is odd;} \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\epsilon_u t - 1} q^{\frac{(k\epsilon_u t - k^2 - 2)}{2}} \left((q^k + q - 1) \left[\frac{(\epsilon_u t - 2)/2}{k/2} \right]_{q^2} + (q^{\epsilon_u t - k + 1} - q^{\epsilon_u t - k} + 1) \right. \\ \quad \times \left. \left[\frac{(\epsilon_u t - 2)/2}{(k - 2)/2} \right]_{q^2} \right) + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\epsilon_u t - 1} q^{\frac{(k + 1)\epsilon_u t - (k^2 + 1)}{2}} \left[\frac{(\epsilon_u t - 2)/2}{(k - 1)/2} \right]_{q^2} & \text{if } \epsilon_u t \text{ is even.} \end{cases}$$

Proof. To determine the number $\mathfrak{L}_u$, we see, by (5.4), that it is enough to determine the number $\mathfrak{L}_{u,k}$ for $1 \leq k \leq \epsilon_u t - 1$. For this, let $1 \leq k \leq \epsilon_u t - 1$ be fixed. As q is even, we note that m_i 's and $\text{ord}(\omega_i)$'s are odd integers. This implies that the integer M is odd, which further implies that $\frac{M}{m_i} = 1$ in $\mathcal{F}_u$. Now let us define the set $\mathbb{M}_u = \left\{ A_u = (A_{u,1}, A_{u,2}, \dots, A_{u,\ell}) \in \mathbb{G}_u : \sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t, q}(A_{u,i}) = 0 \right\}$. One can easily observe that $\mathbb{M}_u$ is an $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ and $\dim_{\mathcal{F}_u} \mathbb{M}_u = (\epsilon_u t - 1)$. Also let $\Theta_u = (\epsilon_{u,1}, \epsilon_{u,2}, \dots, \epsilon_{u,\ell}) \in \mathbb{G}_u$. It is easy to see that $\Theta_u \in \mathbb{M}_u$ if and only if $\sum_{i=1}^{\ell} \epsilon_{u,i} \text{Tr}_{q^t, q}(1) = \sum_{i=1}^{\ell} \epsilon_{u,i} t = \epsilon_u t = 0$, which holds if and only if $\epsilon_u t$ is even. Now the following two cases arise: (i) $\epsilon_u t$ is odd and (ii) $\epsilon_u t$ is even.

(i) First, let $\epsilon_u t$ be odd. In this case, we observe that $\Theta_u \notin \mathbb{M}_u$ and $\dim_{\mathcal{F}_u} \langle \Theta_u \rangle = 1$.

We further see that $[A_u, \Theta_u]_0 = 0$ for all $A_u \in \mathbb{M}_u$ and that $\mathbb{M}_u \cap \langle \Theta_u \rangle = \{\mathbf{0}\}$. This implies that the space $\mathbb{G}_u$ is an orthogonal direct sum of its $\mathcal{F}_u$ -subspaces $\mathbb{M}_u$ and $\langle \Theta_u \rangle$, i.e., $\mathbb{G}_u = \mathbb{M}_u \perp \langle \Theta_u \rangle$. Further, working as in the proof of Case II(i) of Lemma 5.2.1(a), we see that $(\mathbb{M}_u, [\cdot, \cdot]_0 \upharpoonright_{\mathbb{M}_u \times \mathbb{M}_u})$ is a symplectic space over $\mathcal{F}_u$. Moreover, any 0-non-degenerate $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is (i) either contained in $\mathbb{M}_u$ or (ii) contained in $\mathbb{G}_u$ but not in $\mathbb{M}_u$.

To determine the number $\mathfrak{L}_{u,k}$, we will first count all the distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{M}_u$. For this, working as in Proposition 5.4.1, we note that there does not exist any such $\mathcal{F}_u$ -subspace of $\mathbb{M}_u$ when k is odd, while there are exactly

$$\mathfrak{L}_{u,k}^{(\epsilon_1)} = q^{\frac{k(\epsilon_u t - k - 1)}{2}} \begin{bmatrix} (\epsilon_u t - 1)/2 \\ k/2 \end{bmatrix}_{q^2}$$

distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{M}_u$ when k is even.

Next, let W be a k -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$, which is not contained in $\mathbb{M}_u$. One can easily observe that $W = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$, where $A_u^{(h)} \in \mathbb{M}_u \setminus \{\mathbf{0}\}$ for $1 \leq h \leq k-1$ and $A_u^{(k)} \in \mathbb{M}_u$. Now the following two cases arise: k is odd and k is even.

First, suppose that k is odd. Here by applying Theorem 2.2.1, we see that the $\mathcal{F}_u$ -subspace $W = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if the $(k-1)$ -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ of

$\mathbb{M}_u$ is 0-non-degenerate. We further observe that there exists a distinct 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$ corresponding to each element $A_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$ and that the element $A_u^{(k)}$ has $q^{\epsilon_u t - k}$ relevant choices. From this and working as in Proposition 5.4.1, we note that there are exactly

$$\mathfrak{L}_{u,k}^{(0)} = q^{\epsilon_u t - k} q^{\frac{(k-1)(\epsilon_u t - k)}{2}} \begin{bmatrix} (\epsilon_u t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$.

Next, suppose that k is even. If $A_u^{(k)} = \mathbf{0}$, then by Theorem 2.2.1 we see that the $\mathcal{F}_u$ -subspace $W = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, \Theta_u \rangle$ of $\mathbb{G}_u$ is degenerate.

When $A_u^{(k)} \neq \mathbf{0}$, we observe, by applying Theorem 2.2.1 again, that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$ is non-degenerate if and only if the k -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\mathbb{M}_u$ is 0-non-degenerate.

Further, we observe that corresponding to each 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\mathbb{M}_u$, there are precisely $(q^k - 1)$ distinct $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$. From this and working as in Proposition 5.4.1 we see that there are exactly

$$\mathfrak{L}_{u,k}^{(\epsilon_2)} = q^{\frac{k(\epsilon_u t - k - 1)}{2}} (q^k - 1) \begin{bmatrix} (\epsilon_u t - 1)/2 \\ k/2 \end{bmatrix}_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u \rangle$ of $\mathbb{G}_u$ with $A_u^{(h)} \in \mathbb{M}_u \setminus \{\mathbf{0}\}$ and $1 \leq h \leq k$.

On combining all the above cases, we obtain

$$\mathfrak{L}_{u,k} = \mathfrak{L}_{u,k}^{(0)} = q^{\frac{(k+1)(\epsilon_u t - k)}{2}} \begin{bmatrix} (\epsilon_u t - 1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} \text{ when } k \text{ is odd}$$

and

$$\mathfrak{L}_{u,k} = \mathfrak{L}_{u,k}^{(\epsilon_1)} + \mathfrak{L}_{u,k}^{(\epsilon_2)} = q^{\frac{k(\epsilon_u t - k + 1)}{2}} \begin{bmatrix} (\epsilon_u t - 1)/2 \\ k/2 \end{bmatrix}_{q^2} \text{ when } k \text{ is even.}$$

(ii) Let $\epsilon_u t$ be even. Here, we see that $\Theta_u \in \mathbb{M}_u \cap \mathbb{M}_u^{\perp_0}$. Now let $\widehat{\mathbb{M}}_u$ be an $(\epsilon_u t - 2)$ -dimensional $\mathcal{F}_u$ -subspace of $\mathbb{M}_u$ satisfying $\Theta_u \notin \widehat{\mathbb{M}}_u$, so that we have $\mathbb{M}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$. Further, we observe that there exists $y_u \in \widehat{\mathbb{M}}_u^{\perp_0} \setminus \mathbb{M}_u$ such that $\mathbb{G}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle \oplus \langle y_u \rangle$. Moreover, working as in the proof of Case **II(ii)** of Lemma 5.2.1(a), we see that $(\widehat{\mathbb{M}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_u \times \widehat{\mathbb{M}}_u})$ is an $(\epsilon_u t - 2)$ -dimensional symplectic $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$. We also observe that any k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is either contained in $\widehat{\mathbb{M}}_u$, or contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ but not in $\widehat{\mathbb{M}}_u$, or contained in $\widehat{\mathbb{M}}_u \oplus \langle y_u \rangle$ but not in $\widehat{\mathbb{M}}_u$, or contained in $\mathbb{G}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle \oplus \langle y_u \rangle$ but not in any of the subspaces $\widehat{\mathbb{M}}_u$, $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$, and $\widehat{\mathbb{M}}_u \oplus \langle y_u \rangle$. Now we will consider the following four cases separately:

A. We will first count the number of distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$. For this, working as in Proposition 5.4.1, we note that there does not exist such $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$ when k is odd, while there are precisely

$$\mathfrak{R}_{u,k}^{(\epsilon)} = q^{\frac{k(\epsilon_u t - k - 2)}{2}} \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k/2 \end{bmatrix}_{q^2}$$

distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$ when k is even.

B. Now we will count all the distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ that are contained in $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ but not in $\widehat{\mathbb{M}}_u$. For this, working as in case (i), we note that there does not exist any such $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ when k is odd, while $\mathbb{G}_u$ has precisely

$$\mathfrak{S}_{u,k}^{(\epsilon)} = (q^k - 1) q^{\frac{k(\epsilon_u t - k - 2)}{2}} \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k/2 \end{bmatrix}_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces when k is even.

C. Next, we will count all distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u \oplus \langle y_u \rangle$ (and hence of $\mathbb{G}_u$), which are not contained in $\widehat{\mathbb{M}}_u$. To do

this, working as in case (i) again, we see that $\mathbb{G}_u$ has exactly

$$\mathfrak{T}_{u,k}^{(e)} = (q^k - 1)q^{\frac{k(\epsilon_u t - k - 2)}{2}} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k/2 \end{matrix} \right]_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces when k is even, while $\mathbb{G}_u$ has exactly

$$\mathfrak{T}_{u,k}^{(o)} = q^{\frac{(k+1)(\epsilon_u t - k - 1)}{2}} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k - 1)/2 \end{matrix} \right]_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces when k is odd.

D. Finally, we observe that any k -dimensional $\mathcal{F}_u$ -subspace W of $\mathbb{G}_u$ contained in $\mathbb{G}_u = \widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle \oplus \langle y_u \rangle$ but not in any of its subspaces $\widehat{\mathbb{M}}_u$, $\widehat{\mathbb{M}}_u \oplus \langle \Theta_u \rangle$ and $\widehat{\mathbb{M}}_u \oplus \langle y_u \rangle$ is either of the following two types:

- I.** $W = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$, where $\lambda_u \in \mathcal{F}_u \setminus \{0\}$, $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k - 1$ and $A_u^{(k)} \in \widehat{\mathbb{M}}_u$.
- II.** $W = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$, where $k \geq 2$, $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k - 2$ and $A_u^{(k-1)}, A_u^{(k)} \in \widehat{\mathbb{M}}_u$.

I. To determine the number $\mathfrak{L}_{u,k}$, we shall first count all distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$, where $\lambda_u \in \mathcal{F}_u \setminus \{0\}$, $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k - 1$ and $A_u^{(k)} \in \widehat{\mathbb{M}}_u$. Now the following two cases arise: k is even and k is odd.

First let k be even. If $A_u^{(k)} = 0$, then by Theorem [2.2.1](#) we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, \Theta_u + \lambda_u y_u \rangle$ of $\mathbb{G}_u$ is degenerate.

When $A_u^{(k)} \neq 0$, we observe, by applying Theorem [2.2.1](#) again, that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$ of $\mathbb{G}_u$ is non-degenerate if and only if the k -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate. We further observe that corresponding to every non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$, there are precisely $(q - 1)(q^k - 1)$ distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$ of $\mathbb{G}_u$. From this and

working as in Proposition 5.4.1, we see that $\mathbb{G}_u$ has precisely

$$\mathfrak{U}_{u,k}^{(\epsilon)} = q^{\frac{k(\epsilon_u t - k - 2)}{2}} (q - 1)(q^k - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k/2 \end{matrix} \right]_{q^2}$$

such $\mathcal{F}_u$ -subspaces.

Next, suppose that k is odd. Here, by Theorem 2.2.1, we see that the subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if the $(k-1)$ -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate. Further, we see that corresponding to each $\lambda_u \in \mathcal{F}_u \setminus \{0\}$ and each $A_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$, there exists a distinct 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)}, A_u^{(k)} + \Theta_u + \lambda_u y_u \rangle$ of $\mathbb{G}_u$. From this and working as in Proposition 5.4.1, we see that $\mathbb{G}_u$ has precisely

$$\mathfrak{U}_{u,k}^{(\circ)} = q^{\frac{(k+1)(\epsilon_u t - k - 1)}{2}} (q - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces.

II. We will next count all distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$, where $k \geq 2$, $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k-2$ and $A_u^{(k-1)}, A_u^{(k)} \in \widehat{\mathbb{M}}_u$. For this, we shall consider the following two cases separately: k is odd and k is even.

First let k be odd. If $A_u^{(k-1)} = 0$, then by Theorem 2.2.1, we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$ is degenerate.

Now if $A_u^{(k-1)} \neq 0$ and $A_u^{(k)} = 0$, then by Theorem 2.2.1, we observe that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if the $(k-1)$ -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate. Here working as in case (i), we see that $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(\circ_1)} = q^{\frac{(k-1)(\epsilon_u t - k - 1)}{2}} (q^{k-1} - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces.

Now let both $A_u^{(k-1)}$ and $A_u^{(k)}$ be non-zero. Now the following two cases arise: $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent, and $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly independent over $\mathcal{F}_u$.

First of all, suppose that $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent over $\mathcal{F}_u$. In this case, we have $A_u^{(k)} = \alpha_u A_u^{(k-1)}$ for some $\alpha_u \in \mathcal{F}_u \setminus \{0\}$. Here one can easily observe that $\langle A_u^{(1)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle = \langle A_u^{(1)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, \lambda_u y_u + \Theta_u \rangle$, where $\lambda_u \in \mathcal{F}_u \setminus \{0\}$ and $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k-1$. By applying Theorem 2.2.1, it is easy to observe that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, \lambda_u y_u + \Theta_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ is a $(k-1)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. Now working as in case (i) again, we see that if $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent over $\mathcal{F}_u$, then $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(o_2)} = q^{\frac{(k-1)(\epsilon_u t - k-1)}{2}} (q^{k-1} - 1)(q - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$.

Next, suppose that $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly independent over $\mathcal{F}_u$. Here by applying Theorem 2.2.1 again, we see that the subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ is a $(k-1)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. Also we observe that corresponding to every 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle$ of $\widehat{\mathbb{M}}_u$, there are precisely $(q^{k-1} - 1)$ distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u \rangle$. Furthermore, by applying Theorem 2.2.2, we can write $A_u^{(k)} \in \widehat{\mathbb{M}}_u$ as

$$A_u^{(k)} = \alpha_u^{(1)} A_u^{(1)} + \alpha_u^{(2)} A_u^{(2)} + \dots + \alpha_u^{(k-1)} A_u^{(k-1)} + \widetilde{\mathcal{Z}}_u^{(k)},$$

where $\alpha_u^{(h)} \in \mathcal{F}_u$ for $1 \leq h \leq k-1$ and $\widetilde{\mathcal{Z}}_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$. We next observe that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle =$

$\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, \alpha_u^{(k-1)} A_u^{(k-1)} + \tilde{Z}_u^{(k)} + y_u \rangle$. Here one can easily observe that corresponding to every non-zero element $A_u^{(k)} = \alpha_u^{(k-1)} A_u^{(k-1)} + \tilde{Z}_u^{(k)}$, there exists a distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$. From this and working as in Proposition 5.4.1, we see that if $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly independent over $\mathcal{F}_u$, then $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(o_3)} = q^{\frac{(k-1)(\epsilon_u t - k - 1)}{2}} (q^{k-1} - 1) (q^{\epsilon_u t - k} - q) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$.

On combining the above cases, we see that the number of distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ with $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{\mathbf{0}\}$ for $1 \leq h \leq k-2$ and $A_u^{(k-1)}, A_u^{(k)} \in \widehat{\mathbb{M}}_u$, is given by

$$\mathfrak{W}_{u,k}^{(o)} = \mathfrak{W}_{u,k}^{(o_1)} + \mathfrak{W}_{u,k}^{(o_2)} + \mathfrak{W}_{u,k}^{(o_3)} = q^{\frac{k(\epsilon_u t - k) + (\epsilon_u t - 2k + 1)}{2}} (q^{k-1} - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-1)/2} \right]_{q^2}.$$

Next, let k be even. If $A_u^{(k-1)} = A_u^{(k)} = \mathbf{0}$, then by Theorem 2.2.1, we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, \Theta_u, y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if the $(k-2)$ -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate. Now working as in Proposition 5.4.1, we observe that $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(e_1)} = q^{\frac{(k-2)(\epsilon_u t - k)}{2}} \left[\frac{(\epsilon_u t - 2)/2}{(k-2)/2} \right]_{q^2}$$

such distinct $\mathcal{F}_u$ -subspaces.

Now if $A_u^{(k-1)} = \mathbf{0}$ and $A_u^{(k)} \neq \mathbf{0}$, then by applying Theorem 2.2.1 again, we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ is a $(k-2)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. We also note that for

each element $A_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0} \setminus \{0\}$, there exists a distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$, and that the element $A_u^{(k)}$ has exactly $(q^{\epsilon_u t - k} - 1)$ relevant choices. From this and working as in Proposition 5.4.1, we note that $\mathbb{G}_u$ has exactly

$$\mathfrak{W}_{u,k}^{(\epsilon_2)} = q^{\frac{(k-2)(\epsilon_u t - k)}{2}} (q^{\epsilon_u t - k} - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-2)/2} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, \Theta_u, A_u^{(k)} + y_u \rangle$.

Next, if $A_u^{(k)} = 0$ and $A_u^{(k-1)} \neq 0$, then working as above, we see that $\mathbb{G}_u$ has exactly

$$\mathfrak{W}_{u,k}^{(\epsilon_3)} = q^{\frac{(k-2)(\epsilon_u t - k)}{2}} (q^{\epsilon_u t - k} - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k-2)/2} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, y_u \rangle$ of $\mathbb{G}_u$.

Finally, let $A_u^{(k-1)}$ and $A_u^{(k)}$ both be non-zero. Now the following two cases arise: $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent and $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly independent over $\mathcal{F}_u$.

First of all, suppose that $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent over $\mathcal{F}_u$. In this case, we have $A_u^{(k)} = \beta_u A_u^{(k-1)}$ for some $\beta_u \in \mathcal{F}_u \setminus \{0\}$. Here one can easily observe that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} + \Theta_u, \beta_u y_u + \Theta_u \rangle$, where $\beta_u \in \mathcal{F}_u \setminus \{0\}$ and $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{0\}$ for $1 \leq h \leq k-1$. By Theorem 2.2.1, we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} + \Theta_u, \beta_u y_u + \Theta_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if the $(k-2)$ -dimensional $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate. Further, we see that corresponding to every non-zero element $\beta_u \in \mathcal{F}_u$ and every element $A_u^{(k-1)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$, there exists a distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} + \Theta_u, \beta_u y_u + \Theta_u \rangle$ of $\mathbb{G}_u$. From this and working as in Proposition 5.4.1, we note that when $A_u^{(k-1)}$ and $A_u^{(k)}$ are linearly dependent over

$\mathcal{F}_u$, then $\mathbb{G}_u$ has precisely

$$\mathfrak{M}_{u,k}^{(\epsilon_4)} = q^{\frac{(k-2)(\epsilon_u t - k)}{2}} (q^{\epsilon_u t - k} - 1)(q - 1) \left[\frac{(\epsilon_u t - 2)/2}{(k - 2)/2} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$.

Next, let $A_u^{(k-1)}$ and $A_u^{(k)}$ be linearly independent over $\mathcal{F}_u$. Here by applying Theorem 2.2.1 again, we see that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$ is 0-non-degenerate if and only if either

- ($\star$) $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ is a k -dimensional degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$ and $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ is a $(k-2)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$, or
- ($\diamond$) $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ is a k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$ and $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ is a $(k-2)$ -dimensional degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$, or
- ($\dagger$) both $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ and $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ are 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$ of dimensions k and $(k-2)$ respectively, satisfying

$$\det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)}) \neq \det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}),$$

where $\det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)})$ and $\det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)})$ denote the determinants of the Gram matrices of the $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ and $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ of $\widehat{\mathbb{M}}_u$ with respect to the bases $\{A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)}\}$ and $\{A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}\}$, respectively.

We first count all k -dimensional $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying ($\star$). For this, we note that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ is a 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. From this and by Theorem 2.2.2, we can write

$$\widehat{\mathbb{M}}_u = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle \perp \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0},$$

where $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$ is an $(\epsilon_u t - k)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. We further observe that for every pair of linearly independent vectors $A_u^{(k-1)}, A_u^{(k)}$ in $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$, there exists a distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$. It is easy to observe that

$$\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle \perp \langle A_u^{(k-1)}, A_u^{(k)} \rangle,$$

which implies that

$$\det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)}) = \det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}) \det \mathfrak{G}(A_u^{(k-1)}, A_u^{(k)}).$$

Therefore, the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$ is degenerate if and only if $\det \mathfrak{G}(A_u^{(k-1)}, A_u^{(k)}) = 0$, which holds if and only if $A_u^{(k)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-1)} \rangle^{\perp_0}$. Moreover, we note that $A_u^{(k-1)} \in \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0} \setminus \{0\}$, so it has $(q^{\epsilon_u t - k} - 1)$ relevant choices. Further, we note that the pair $(A_u^{(k-1)}, A_u^{(k)})$ has precisely $(q^{\epsilon_u t - k - 1} - q)(q^{\epsilon_u t - k} - 1)$ relevant choices. From this and working as in Proposition [5.4.1](#), we see that $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(\epsilon_5)} = q^{\frac{(k-2)(\epsilon_u t - k)}{2}} (q^{\epsilon_u t - k - 1} - q)(q^{\epsilon_u t - k} - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k - 2)/2 \end{matrix} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying $(\star)$.

We next proceed to count all k -dimensional $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying $(\diamond)$. To do this, working as in Proposition [5.4.1](#), we see that the number of k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces of $\widehat{\mathbb{M}}_u$ is given by

$$q^{\frac{k(\epsilon_u t - k - 2)}{2}} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k/2 \end{matrix} \right]_{q^2}.$$

Let $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ be a k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. Further, we observe that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ has exactly $q^{k-2} \left[\frac{k/2}{(k-2)/2} \right]_{q^2}$ distinct $(k-2)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces. From this and by Lemma 2.2.1, we see that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ has exactly $\left[\frac{k}{k-2} \right]_q - q^{k-2} \left[\frac{k/2}{(k-2)/2} \right]_{q^2}$ distinct $(k-2)$ -dimensional degenerate $\mathcal{F}_u$ -subspaces. Next, let $\langle B_u^{(1)}, B_u^{(2)}, \dots, B_u^{(k-2)} \rangle$ be a fixed $(k-2)$ -dimensional degenerate $\mathcal{F}_u$ -subspace of $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$. We will now choose two linearly independent vectors over $\mathcal{F}_u$, say $B_u^{(k-1)}$ and $B_u^{(k)}$, belonging to the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$. These vectors satisfy the condition $\langle B_u^{(1)}, B_u^{(2)}, \dots, B_u^{(k)} \rangle = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$. Note that the pair $(B_u^{(k-1)}, B_u^{(k)})$ has $(q^2 - 1)(q^2 - q)$ distinct choices. From this and working as in Proposition 5.4.1, we see that $\mathbb{G}_u$ has precisely

$$\begin{aligned} \mathfrak{W}_{u,k}^{(\epsilon_6)} &= q^{\frac{k(\epsilon_u t - k - 2)}{2}} (q^2 - 1)(q^2 - q) \left[\frac{(\epsilon_u t - 2)/2}{k/2} \right]_{q^2} \\ &\quad \times \left(\left[\frac{k}{k-2} \right]_q - q^{k-2} \left[\frac{k/2}{(k-2)/2} \right]_{q^2} \right) \end{aligned}$$

distinct k -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying $(\diamond)$.

Finally, we determine the number of distinct k -dimensional $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying $(\ddagger)$. To do this, working as in Proposition 5.4.1, we see that $\widehat{\mathbb{M}}_u$ has exactly $q^{\frac{(k-2)(\epsilon_u t - k)}{2}} \left[\frac{(\epsilon_u t - 2)/2}{(k-2)/2} \right]_{q^2}$ distinct $(k-2)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspaces. By applying Theorem 2.2.2, we have

$$\widehat{\mathbb{M}}_u = \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle \perp \langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0},$$

where $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$ is an $(\epsilon_u t - k)$ -dimensional 0-non-degenerate $\mathcal{F}_u$ -subspace of $\widehat{\mathbb{M}}_u$. From this, we see that

$$\det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)}) = \det \mathfrak{G}(A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}) \det \mathfrak{G}(A_u^{(k-1)}, A_u^{(k)}),$$

which further implies that the $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$ is 0-non-degenerate if and only if $\det \mathfrak{G}(A_u^{(k-1)}, A_u^{(k)}) \neq 0$, which holds if and only if $A_u^{(k)} \notin \langle A_u^{(k-1)} \rangle^{\perp_0}$ and $(A_u^{(k-1)}, A_u^{(k)})$ is not a hyperbolic pair in $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$. So there are $(q-1)(q^{\epsilon_u t-k} - 1)q^{\epsilon_u t-k-1}$ distinct choices for the pair $(A_u^{(k-1)}, A_u^{(k)})$ such that both $\mathcal{F}_u$ -subspaces $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle$ and $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k)} \rangle$ of $\widehat{\mathbb{M}}_u$ are 0-non-degenerate. Next, by Theorem 2.2.3(a) and (c), we see that $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)} \rangle^{\perp_0}$ has Witt index $\frac{\epsilon_u t-k}{2}$ and exactly $H_{\frac{\epsilon_u t-k}{2}, 0} = q^{\epsilon_u t-k-1}(q^{\epsilon_u t-k} - 1)$ hyperbolic pairs. Thus the pair $(A_u^{(k-1)}, A_u^{(k)})$ has precisely $q^{\epsilon_u t-k-1}(q-1)(q^{\epsilon_u t-k} - 1) - q^{\epsilon_u t-k-1}(q^{\epsilon_u t-k} - 1) = q^{\epsilon_u t-k-1}(q-2)(q^{\epsilon_u t-k} - 1)$ relevant choices. From this, we see that $\mathbb{G}_u$ has precisely

$$\mathfrak{W}_{u,k}^{(\epsilon_7)} = q^{\frac{(k-2)(\epsilon_u t-k)}{2}} q^{\epsilon_u t-k-1} (q-2)(q^{\epsilon_u t-k} - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k-2)/2 \end{matrix} \right]_{q^2}$$

distinct 0-non-degenerate $\mathcal{F}_u$ -subspaces of the type $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ satisfying $(\dagger)$.

Combining the above cases, we see that the number of choices for the 0-non-degenerate $\mathcal{F}_u$ -subspace $\langle A_u^{(1)}, A_u^{(2)}, \dots, A_u^{(k-2)}, A_u^{(k-1)} + \Theta_u, A_u^{(k)} + y_u \rangle$ of $\mathbb{G}_u$ satisfying $A_u^{(h)} \in \widehat{\mathbb{M}}_u \setminus \{\mathbf{0}\}$ for $1 \leq h \leq k-2$ and $A_u^{(k-1)}, A_u^{(k)} \in \widehat{\mathbb{M}}_u$, is given by

$$\begin{aligned} \mathfrak{W}_{u,k}^{(\epsilon)} &= \mathfrak{W}_{u,k}^{(\epsilon_1)} + \mathfrak{W}_{u,k}^{(\epsilon_2)} + \mathfrak{W}_{u,k}^{(\epsilon_3)} + \mathfrak{W}_{u,k}^{(\epsilon_4)} + \mathfrak{W}_{u,k}^{(\epsilon_5)} + \mathfrak{W}_{u,k}^{(\epsilon_6)} + \mathfrak{W}_{u,k}^{(\epsilon_7)} \\ &= q^{\frac{k\epsilon_u t-k^2-2}{2}} (q^{\epsilon_u t-k+1} - q^{\epsilon_u t-k} + 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k-2)/2 \end{matrix} \right]_{q^2} \\ &\quad + q^{\frac{k(\epsilon_u t-k-2)}{2}} (q^{k+1} - q)(q^{k-2} - 1) \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ k/2 \end{matrix} \right]_{q^2}. \end{aligned}$$

Combining the above cases, we obtain

$$\mathfrak{L}_{u,k} = \mathfrak{T}_{u,k}^{(o)} + \mathfrak{U}_{u,k}^{(o)} + \mathfrak{W}_{u,k}^{(o)} = q^{\frac{(k+1)\epsilon_u t-(k^2+1)}{2}} \left[\begin{matrix} (\epsilon_u t - 2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2} \text{ when } k \text{ is odd,}$$

and

$$\mathfrak{L}_{u,k} = \mathfrak{R}_{u,k}^{(\epsilon)} + \mathfrak{S}_{u,k}^{(\epsilon)} + \mathfrak{T}_{u,k}^{(\epsilon)} + \mathfrak{U}_{u,k}^{(\epsilon)} + \mathfrak{W}_{u,k}^{(\epsilon)}$$

$$\begin{aligned}
&= q^{\frac{k\epsilon_u t - k^2 - 2}{2}} \left((q^k + q - 1) \begin{bmatrix} (\epsilon_u t - 2)/2 \\ k/2 \end{bmatrix}_{q^2} \right. \\
&\quad \left. + (q^{\epsilon_u t - k + 1} - q^{\epsilon_u t - k} + 1) \begin{bmatrix} (\epsilon_u t - 2)/2 \\ (k - 2)/2 \end{bmatrix}_{q^2} \right) \text{ when } k \text{ is even.}
\end{aligned}$$

Finally, substituting the above values of $\mathfrak{L}_{u,k}$ in equation (5.4) in the respective cases, the desired result follows. $\square$

5.4.2 Determination of the number $\mathfrak{L}_u$ when $u \in \mathcal{J}_2$

In the following proposition, we determine the number $\mathfrak{L}_u$ when $u \in \mathcal{J}_2$ and $\sigma \in \{0, \gamma, *\}$.

Proposition 5.4.4. *Let $u \in \mathcal{J}_2$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathfrak{L}_u = 2 + \sum_{k=1}^{\epsilon_u t - 1} q^{\frac{k(\epsilon_u t - k)d_u}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a}}{q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a}} \right).$$

Proof. To determine the number $\mathfrak{L}_u$, we see, by (5.4), that it is enough to determine the number $\mathfrak{L}_{u,k}$ for $1 \leq k \leq \epsilon_u t - 1$. Here we shall discuss the following two cases separately: **I.** $\sigma \in \{0, *\}$ and **II.** $\sigma = \gamma$.

I. Let $\sigma \in \{0, *\}$. Here by Lemma 4.4.2(b), we note that $(\mathbb{G}_u, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space over $\mathcal{F}_u$. We further see that any k -dimensional σ -non-degenerate $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is also a unitary space. Now we distinguish the following two cases: (i) k is odd and (ii) k is even.

(i) First, let k be odd. Here by Theorem 2.2.4(e), we see that the k -dimensional $\mathcal{F}_u$ -subspace W of $\mathbb{G}_u$ has a Witt decomposition

$$W = \langle A_u^{(1)}(x), B_u^{(1)}(x) \rangle \perp \dots \perp \langle A_u^{(\frac{k-1}{2})}(x), B_u^{(\frac{k-1}{2})}(x) \rangle \perp \langle Z_u(x) \rangle,$$

where $(A_u^{(h)}(x), B_u^{(h)}(x))$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k-1}{2}$ and $Z_u(x)$ is an anisotropic vector in $\mathbb{G}_u$, and the set $\{A_u^{(1)}(x), B_u^{(1)}(x), A_u^{(2)}(x), B_u^{(2)}(x), \dots, A_u^{(\frac{k-1}{2})}(x), B_u^{(\frac{k-1}{2})}(x), Z_u(x)\}$ is a Witt basis (or a unitary basis) of W over $\mathcal{F}_u$. Let ϑ_h denote the Witt index of $\langle A_u^{(1)}(x), B_u^{(1)}(x), A_u^{(2)}(x),$

$B_u^{(2)}(x), \dots, A_u^{(h-1)}(x), B_u^{(h-1)}(x)\rangle^{\perp\sigma} \subseteq \mathbb{G}_u$ for $1 \leq h \leq \frac{k+1}{2}$. By applying Theorems 2.2.2 and 2.2.4(a)-(d), we see that the number of Witt bases of the type $\{A_u^{(1)}(x), B_u^{(1)}(x), A_u^{(2)}(x), B_u^{(2)}(x), \dots, A_u^{(\frac{k-1}{2})}(x), B_u^{(\frac{k-1}{2})}(x), Z_u(x)\}$ in $\mathbb{G}_u$ is given by

$$\begin{aligned} U_{k, \epsilon_u t} &= H_{\vartheta_1, \epsilon_u t - 2\vartheta_1} H_{\vartheta_2, \epsilon_u t - 2 - 2\vartheta_2} \dots H_{\vartheta_{\frac{k-1}{2}}, \epsilon_u t - k + 3 - 2\vartheta_{\frac{k-1}{2}}} \\ &\quad \times \left(q^{(\epsilon_u t - k + 1)d_u} - 1 - I_{\vartheta_{\frac{k+1}{2}}, \epsilon_u t - k + 1 - 2\vartheta_{\frac{k+1}{2}}} \right) \\ &= q^{\frac{(2\epsilon_u t - k - 1)kd_u}{4}} (q^{\frac{d_u}{2}} - 1) \prod_{a=0}^{k-1} \left(q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a} \right). \end{aligned}$$

Further, working as above and applying Theorem 2.2.4 again, we see that a k -dimensional unitary $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ has precisely

$$U_{k,k} = H_{\frac{k-1}{2}, 1} H_{\frac{k-3}{2}, 1} \dots H_{1,1} (q^{d_u} - 1) = q^{\frac{k(k-1)}{2}} (q^{\frac{d_u}{2}} - 1) \prod_{a=0}^{k-1} \left(q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a} \right)$$

distinct choices for the Witt basis. Therefore, the number of distinct k -dimensional σ -non-degenerate $\mathcal{F}_u$ -subspaces of $\mathbb{G}_u$ is given by

$$\mathfrak{L}_{u,k} = \frac{U_{k, \epsilon_u t}}{U_{k,k}} = q^{\frac{k(\epsilon_u t - k)d_u}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a}}{q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a}} \right) \text{ for } 1 \leq k \leq \epsilon_u t - 1.$$

- (ii) Next, let k be even. Here, we see that each k -dimensional σ -non-degenerate $\mathcal{F}_u$ -subspace W of $\mathbb{G}_u$ has a Witt decomposition of the form

$$W = \langle A_u^{(1)}(x), B_u^{(1)}(x) \rangle \perp \langle A_u^{(2)}(x), B_u^{(2)}(x) \rangle \perp \dots \perp \langle A_u^{(\frac{k}{2})}(x), B_u^{(\frac{k}{2})}(x) \rangle,$$

where $(A_u^{(h)}(x), B_u^{(h)}(x))$ is a hyperbolic pair in $\mathbb{G}_u$ for $1 \leq h \leq \frac{k}{2}$. Now working in a similar manner as in case (i) and by applying Theorem 2.2.4 again, we get

$$\mathfrak{L}_{u,k} = q^{\frac{k(\epsilon_u t - k)d_u}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a}}{q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a}} \right) \text{ for } 1 \leq k \leq \epsilon_u t - 1.$$

II. Let $\sigma = \gamma$. In this case, we see, by Lemma 4.4.2(d), that $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form. Working as in the proof of Lemma 5.2.1(b), we transform the skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$ to an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u}$. We further observe that the map $[\cdot, \cdot]_{\gamma_H}$ is a non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_u$, so $(\mathbb{G}_u, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_u \times \mathbb{G}_u})$ is a unitary space of dimension $\epsilon_u t$ over $\mathcal{F}_u \simeq \mathbb{F}_{q^{d_u}}$. We next observe that any $\mathcal{F}_u$ -subspace of $\mathbb{G}_u$ is non-degenerate with respect to $[\cdot, \cdot]_\gamma$ if and only if it is non-degenerate with respect to $[\cdot, \cdot]_{\gamma_H}$. Now working as in case **I**, we obtain

$$\mathfrak{L}_{u,k} = q^{\frac{k(\epsilon_u t - k)d_u}{2}} \prod_{a=0}^{k-1} \left(\frac{q^{\frac{(\epsilon_u t - a)d_u}{2}} - (-1)^{\epsilon_u t - a}}{q^{\frac{(k-a)d_u}{2}} - (-1)^{k-a}} \right) \text{ for } 1 \leq k \leq \epsilon_u t - 1.$$

From this and by (5.4), the desired result follows immediately. $\square$

5.4.3 Determination of the number $\mathfrak{L}_v$ when $e_1 + 1 \leq v \leq e_2$

In this section, we determine the number $\mathfrak{L}_v$ of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$ with $\mathcal{C}_v$ as an $\mathcal{F}_v$ -subspace of $\mathbb{G}_v$ and $\mathcal{C}_v^\dagger$ as an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{G}_v^\dagger$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\dagger\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ for $e_1 + 1 \leq v \leq e_2$, where $\sigma \in \{0, \gamma, *\}$. To do this, let $e_1 + 1 \leq v \leq e_2$ be fixed. Here we can suppose, without any loss of generality, that there exists an integer j satisfying $1 \leq j \leq \ell$, such that $\epsilon_{v,i} = \epsilon_{v,i}^\dagger$ for $1 \leq i \leq j$ and $\epsilon_{v,i} \neq \epsilon_{v,i}^\dagger$ for $j+1 \leq i \leq \ell$. In other words, we have $\mathcal{I}_v = \{1, 2, \dots, j\}$ and $\mathcal{I}'_v = \{j+1, j+2, \dots, \ell\}$. Consequently, we have $\eta_v = \sum_{i=1}^j \epsilon_{v,i}$, $\varrho_v = \sum_{i=j+1}^{\ell} \epsilon_{v,i}$ and $\tau_v = \sum_{i=j+1}^{\ell} \epsilon_{v,i}^\dagger$. So we can write $\mathbb{G}_v = \mathbb{K}_v \oplus \mathbb{K}'_v$ and $\mathbb{G}_v^\dagger = \mathbb{K}_v^\dagger \oplus \mathbb{K}'_v$, where

$$\begin{aligned} \mathbb{K}_v &= \left(\epsilon_{v,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \epsilon_{v,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \dots, \epsilon_{v,j} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, 0, \dots, 0 \right), \\ \mathbb{K}_v^\dagger &= \left(\epsilon_{v,1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \epsilon_{v,2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, \dots, \epsilon_{v,j} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^\dagger(x) \rangle}, 0, \dots, 0 \right), \\ \mathbb{K}'_v &= \left(0, \dots, 0, \epsilon_{v,j+1} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \epsilon_{v,j+2} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle}, \dots, \epsilon_{v,\ell} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v(x) \rangle} \right) \text{ and} \end{aligned}$$

$$\mathbb{K}_v^{\dagger'} = \left(0, \dots, 0, \epsilon_{v,j+1}^{\dagger} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^{\dagger}(x) \rangle}, \epsilon_{v,j+2}^{\dagger} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^{\dagger}(x) \rangle}, \dots, \epsilon_{v,\ell}^{\dagger} \frac{\mathbb{F}_{q^t}[x]}{\langle h_v^{\dagger}(x) \rangle} \right).$$

In view of this, each $\mathcal{F}_v$ -subspace $\mathcal{C}_v$ of $\mathbb{G}_v$ and each $\mathcal{F}_v^{\dagger}$ -subspace $\mathcal{C}_v^{\dagger}$ of $\mathbb{G}_v^{\dagger}$ can be uniquely expressed as $\mathcal{C}_v = \mathcal{D}_v \oplus \mathcal{D}_v'$ and $\mathcal{C}_v^{\dagger} = \mathcal{D}_v^{\dagger} \oplus \mathcal{D}_v'^{\dagger}$, where $\mathcal{D}_v$ and $\mathcal{D}_v'$ (resp. $\mathcal{D}_v^{\dagger}$ and $\mathcal{D}_v'^{\dagger}$) are subspaces of $\mathbb{K}_v$ and $\mathbb{K}_v'$ (resp. $\mathbb{K}_v^{\dagger}$ and $\mathbb{K}_v'^{\dagger}$) over $\mathcal{F}_v$ (resp. $\mathcal{F}_v^{\dagger}$), respectively. We next observe that $\mathbb{K}_v$ (resp. $\mathbb{K}_v^{\dagger}$) is an $(\eta_v t)$ -dimensional vector space over $\mathcal{F}_v$ (resp. $\mathcal{F}_v^{\dagger}$). Furthermore, we observe that $\mathbb{K}_v'$ and $\mathbb{K}_v'^{\dagger}$ are $(\varrho_v t)$ -dimensional and $(\tau_v t)$ -dimensional spaces over $\mathcal{F}_v$ and $\mathcal{F}_v^{\dagger}$, respectively.

Throughout this section, we will represent elements of the direct sum $\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}$ as $\mathbf{A}_v(x) = A_v(x) + \tilde{A}_v(x)$, where $A_v(x) \in \mathbb{K}_v$ and $\tilde{A}_v(x) \in \mathbb{K}_v^{\dagger}$. Likewise, we will represent elements of the direct sum $\mathcal{F}_v \oplus \mathcal{F}_v^{\dagger}$ as $\mathbf{f}_v(x) = f_v(x) + \tilde{f}_v(x)$, where $f_v(x) \in \mathcal{F}_v$ and $\tilde{f}_v(x) \in \mathcal{F}_v^{\dagger}$. Here we shall view the set $\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}$ as an $(\mathcal{F}_v \oplus \mathcal{F}_v^{\dagger})$ -module under the following addition and scalar multiplication operations:

$$\mathbf{A}_v(x) + \mathbf{B}_v(x) = (A_v(x) + B_v(x)) + (\tilde{A}_v(x) + \tilde{B}_v(x)) \quad (5.8)$$

$$\mathbf{f}_v(x) \mathbf{A}_v(x) = f_v(x) A_v(x) + \tilde{f}_v(x) \tilde{A}_v(x) \quad (5.9)$$

for all $\mathbf{A}_v(x) = A_v(x) + \tilde{A}_v(x)$, $\mathbf{B}_v(x) = B_v(x) + \tilde{B}_v(x) \in \mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}$ and $\mathbf{f}_v(x) = f_v(x) + \tilde{f}_v(x) \in \mathcal{F}_v \oplus \mathcal{F}_v^{\dagger}$. Further, for $\sigma \in \{0, \gamma, *\}$, we observe that

$$[\mathbf{A}_v(x), \mathbf{B}_v(x)]_{\sigma} = [A_v(x), \tilde{B}_v(x)]_{\sigma} + [\tilde{A}_v(x), B_v(x)]_{\sigma} \in \mathcal{F}_v \oplus \mathcal{F}_v^{\dagger}$$

for every $\mathbf{A}_v(x) = A_v(x) + \tilde{A}_v(x)$, $\mathbf{B}_v(x) = B_v(x) + \tilde{B}_v(x) \in \mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}$. Next, for $\sigma \in \{0, \gamma, *\}$, let $[\cdot, \cdot]_{\sigma} \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}) \times (\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger})}$ denote the restriction of the sesquilinear form $[\cdot, \cdot]_{\sigma}$ to $(\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}) \times (\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger})$. Now we observe the following:

Lemma 5.4.1. *Let $e_1 + 1 \leq v \leq e_2$ be fixed. For $\sigma \in \{0, \gamma, *\}$, the following hold.*

- (a) $\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}$ is a free $(\mathcal{F}_v \oplus \mathcal{F}_v^{\dagger})$ -module of rank $\eta_v t$.
- (b) The form $[\cdot, \cdot]_{\sigma} \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}) \times (\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger})}$ is reflexive and non-degenerate.
- (c) The form $[\cdot, \cdot]_{\sigma} \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger}) \times (\mathbb{K}_v \oplus \mathbb{K}_v^{\dagger})}$ is Hermitian when $\sigma \in \{0, *\}$ and is skew-Hermitian when $\sigma = \gamma$.

If $\mathcal{L}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{L}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$, then we observe that their direct sum $\mathcal{L}_v \oplus \mathcal{L}_v^\dagger$ is an $(\mathcal{F}_v \oplus \mathcal{F}_v^\dagger)$ -submodule of $\mathbb{K}_v \oplus \mathbb{K}_v^\dagger$ with respect to the addition and scalar multiplication operations defined by (5.8) and (5.9), respectively. For $\sigma \in \{0, \gamma, *\}$, the orthogonal complement of $\mathcal{L}_v \oplus \mathcal{L}_v^\dagger$ with respect to the form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$ is defined as

$$(\mathcal{L}_v \oplus \mathcal{L}_v^\dagger)^{\perp_\sigma} = \left\{ \mathbf{B}_v(x) \in \mathbb{K}_v \oplus \mathbb{K}_v^\dagger : [\mathbf{A}_v(x), \mathbf{B}_v(x)]_\sigma = 0 \text{ for all } \mathbf{A}_v(x) \in \mathcal{L}_v \oplus \mathcal{L}_v^\dagger \right\}.$$

It is easy to observe that $(\mathcal{L}_v \oplus \mathcal{L}_v^\dagger)^{\perp_\sigma}$ is an $(\mathcal{F}_v \oplus \mathcal{F}_v^\dagger)$ -submodule of $\mathbb{K}_v \oplus \mathbb{K}_v^\dagger$ and that $(\mathcal{L}_v \oplus \mathcal{L}_v^\dagger)^{\perp_\sigma} = \mathcal{L}_v^{\perp_\sigma} \oplus \mathcal{L}_v^{\perp_\sigma}$, where

$$\mathcal{L}_v^{\perp_\sigma} = \left\{ B_v(x) \in \mathbb{K}_v : [\tilde{A}_v(x), B_v(x)]_\sigma = 0 \text{ for all } \tilde{A}_v(x) \in \mathcal{L}_v^\dagger \right\}$$

and

$$\mathcal{L}_v^{\perp_\sigma} = \left\{ \tilde{B}_v(x) \in \mathbb{K}_v^\dagger : [A_v(x), \tilde{B}_v(x)]_\sigma = 0 \text{ for all } A_v(x) \in \mathcal{L}_v \right\}.$$

For $\sigma \in \{0, \gamma, *\}$, we say that an $(\mathcal{F}_v \oplus \mathcal{F}_v^\dagger)$ -submodule $\mathcal{L}_v \oplus \mathcal{L}_v^\dagger$ of $\mathbb{K}_v \oplus \mathbb{K}_v^\dagger$ is σ -non-degenerate if it satisfies

$$(\mathcal{L}_v \oplus \mathcal{L}_v^\dagger) \cap (\mathcal{L}_v \oplus \mathcal{L}_v^\dagger)^{\perp_\sigma} = \{\mathbf{0}\}, \text{ i.e., } (\mathcal{L}_v \oplus \mathcal{L}_v^\dagger) \cap (\mathcal{L}_v^{\perp_\sigma} \oplus \mathcal{L}_v^{\perp_\sigma}) = \{\mathbf{0}\}.$$

By Lemma 5.4.1(c), we see that the form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$ is skew-Hermitian. Here we shall first transform this skew-Hermitian form to an orthogonality preserving Hermitian form as follows: Let us take $\boldsymbol{\lambda}_v(x) = \zeta_v(x) - \tau_{1,-1}(\zeta_v(x)) \in \mathcal{F}_v \oplus \mathcal{F}_v^\dagger$, where $\zeta_v(x)$ is a non-zero element in $\mathcal{F}_v$. Here we note that $\boldsymbol{\lambda}_v(x) \neq 0$ and $\tau_{1,-1}(\boldsymbol{\lambda}_v(x)) = -\boldsymbol{\lambda}_v(x)$. Now let us define a map $[\cdot, \cdot]_{\gamma_H} : (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \rightarrow \mathcal{F}_v \oplus \mathcal{F}_v^\dagger$ as

$$[\mathbf{A}_v(x), \mathbf{B}_v(x)]_{\gamma_H} = \boldsymbol{\lambda}_v(x)[\mathbf{A}_v(x), \mathbf{B}_v(x)]_\gamma \text{ for all } \mathbf{A}_v(x), \mathbf{B}_v(x) \in \mathbb{K}_v \oplus \mathbb{K}_v^\dagger.$$

One can easily observe that the map $[\cdot, \cdot]_{\gamma_H}$ is a non-degenerate and Hermitian form on $(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)$. Further, we observe that an $(\mathcal{F}_v \oplus \mathcal{F}_v^\dagger)$ -submodule of $\mathbb{K}_v \oplus \mathbb{K}_v^\dagger$ is non-degenerate with respect to the form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$ if and only if it is non-degenerate with respect to the form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$. In view of this, from now on, we will consider the Hermitian form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$ in

place of the skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathbb{K}_v \oplus \mathbb{K}_v^\dagger) \times (\mathbb{K}_v \oplus \mathbb{K}_v^\dagger)}$. So without any loss of generality, we assume that $\sigma \in \{0, \gamma_{\mathbf{H}}, *\}$ in this case.

In the following proposition, we determine the number $\mathfrak{L}_v$ for $e_1 + 1 \leq v \leq e_2$ when $\sigma \in \{0, \gamma_{\mathbf{H}}, *\}$, or equivalently, when $\sigma \in \{0, \gamma, *\}$.

Proposition 5.4.5. *Let $e_1 + 1 \leq v \leq e_2$ be fixed. For $\sigma \in \{0, \gamma_{\mathbf{H}}, *\}$ (or equivalently, $\sigma \in \{0, \gamma, *\}$), we have*

$$\mathfrak{L}_v = \sum_{k=0}^{\eta_v t} \sum_{k_1=0}^{\varrho_v t} \sum_{k_2=0}^{\tau_v t} q^{kd_v(\eta_v t - k)} \begin{bmatrix} \eta_v t \\ k \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \varrho_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \tau_v t \\ k_2 \end{bmatrix}_{q^{d_v}}.$$

Proof. To prove the result, we see, by Theorem 4.4.1(c), that the number $\mathfrak{L}_v$ equals the number of distinct pairs $(\mathcal{C}_v, \mathcal{C}_v^\dagger)$ with $\mathcal{C}_v$ as an $\mathcal{F}_v$ -subspace of $\mathbb{G}_v$ and $\mathcal{C}_v^\dagger$ as an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{G}_v^\dagger$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\perp \sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_v^\dagger \cap \mathcal{C}_v^{\perp \sigma} = \{\mathbf{0}\}$. We further note that each $\mathcal{F}_v$ -subspace $\mathcal{C}_v$ of $\mathbb{G}_v$ and each $\mathcal{F}_v^\dagger$ -subspace $\mathcal{C}_v^\dagger$ of $\mathbb{G}_v^\dagger$ can be uniquely expressed as $\mathcal{C}_v = \mathcal{D}_v \oplus \mathcal{D}_v'$ and $\mathcal{C}_v^\dagger = \mathcal{D}_v^\dagger \oplus \mathcal{D}_v^{\dagger'}$, where $\mathcal{D}_v$ and $\mathcal{D}_v'$ (resp. $\mathcal{D}_v^\dagger$ and $\mathcal{D}_v^{\dagger'}$) are subspaces of $\mathbb{K}_v$ and $\mathbb{K}_v'$ (resp. $\mathbb{K}_v^\dagger$ and $\mathbb{K}_v^{\dagger'}$) over $\mathcal{F}_v$ (resp. $\mathcal{F}_v^\dagger$), respectively. Further, for each pair $(\mathcal{D}_v', \mathcal{D}_v^{\dagger'})$, we observe that $(\mathcal{C}_v \oplus \mathcal{C}_v^\dagger) \cap (\mathcal{C}_v^{\perp \sigma} \oplus \mathcal{C}_v^{\perp \sigma}) = \{\mathbf{0}\}$ if and only if $(\mathcal{D}_v \oplus \mathcal{D}_v^\dagger) \cap (\mathcal{D}_v^{\perp \sigma} \oplus \mathcal{D}_v^{\perp \sigma}) = \{\mathbf{0}\}$. We next observe that $(\mathcal{D}_v \oplus \mathcal{D}_v^\dagger) \cap (\mathcal{D}_v^{\perp \sigma} \oplus \mathcal{D}_v^{\perp \sigma}) = \{\mathbf{0}\}$ if and only if $\mathcal{D}_v \cap \mathcal{D}_v^{\perp \sigma} = \{\mathbf{0}\}$ and $\mathcal{D}_v^\dagger \cap \mathcal{D}_v^{\perp \sigma} = \{\mathbf{0}\}$. By Lemma 2.2.1, we see that there are precisely

$$\mathfrak{E}_v = \sum_{k_1=0}^{\varrho_v t} \sum_{k_2=0}^{\tau_v t} \begin{bmatrix} \varrho_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \tau_v t \\ k_2 \end{bmatrix}_{q^{d_v}}$$

distinct choices for the pair $(\mathcal{D}_v', \mathcal{D}_v^{\dagger'})$. So to determine the number $\mathfrak{L}_v$, it is enough to determine the number $\mathfrak{F}_v$ of distinct choices for the pair $(\mathcal{D}_v, \mathcal{D}_v^\dagger)$, where $\mathcal{D}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{D}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$ satisfying $\mathcal{D}_v \cap \mathcal{D}_v^{\perp \sigma} = \{\mathbf{0}\}$ and $\mathcal{D}_v^\dagger \cap \mathcal{D}_v^{\perp \sigma} = \{\mathbf{0}\}$. From the above discussion, we see that the number $\mathfrak{F}_v$ equals the number of distinct σ -non-degenerate $(\mathcal{F}_v \oplus \mathcal{F}_v^\dagger)$ -submodules $\mathcal{D}_v \oplus \mathcal{D}_v^\dagger$ of $\mathbb{K}_v \oplus \mathbb{K}_v^\dagger$, where $\mathcal{D}_v$ is an $\mathcal{F}_v$ -subspace of $\mathbb{K}_v$ and $\mathcal{D}_v^\dagger$ is an $\mathcal{F}_v^\dagger$ -subspace of $\mathbb{K}_v^\dagger$. Further, working as in Proposition 3.5 of Sharma and Kaur [58], we get

$$\mathfrak{F}_v = \sum_{k=0}^{\eta_v t} q^{k(\eta_v t - k)d_v} \begin{bmatrix} \eta_v t \\ k \end{bmatrix}_{q^{d_v}}.$$

From this, we obtain

$$\mathfrak{L}_v = \mathfrak{E}_v \mathfrak{F}_v = \sum_{k=0}^{\eta_v t} \sum_{k_1=0}^{\varrho_v t} \sum_{k_2=0}^{\tau_v t} q^{kd_v(\eta_v t - k)} \begin{bmatrix} \eta_v t \\ k \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \varrho_v t \\ k_1 \end{bmatrix}_{q^{d_v}} \begin{bmatrix} \tau_v t \\ k_2 \end{bmatrix}_{q^{d_v}}.$$

□

5.4.4 Determination of the number $\mathfrak{L}_w$ when $e_2 + 1 \leq w \leq e_3$

In the following proposition, we determine the number $\mathfrak{L}_w$ for $e_2 + 1 \leq w \leq e_3$ when $\sigma \in \{0, \gamma, *\}$.

Proposition 5.4.6. *Let $e_2 + 1 \leq w \leq e_3$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathfrak{L}_w = \sum_{a=0}^{\epsilon_w t} \begin{bmatrix} \epsilon_w t \\ a \end{bmatrix}_{q^{d_w}}.$$

Proof. By Theorem 4.4.1(c), we see that the number $\mathfrak{L}_w$ equals the number of distinct $\mathcal{F}_w$ -subspaces of $\mathbb{G}_w$ for $e_2 + 1 \leq w \leq e_3$. Since $\dim_{\mathcal{F}_w} \mathbb{G}_w = \epsilon_w t$, by applying Lemma 2.2.1, we get

$$\mathfrak{L}_w = \sum_{a=0}^{\epsilon_w t} \begin{bmatrix} \epsilon_w t \\ a \end{bmatrix}_{q^{d_w}}.$$

□

Proof of Theorem 5.4.1. By substituting the values of the numbers $\mathfrak{L}_u$ for $1 \leq u \leq e_1$ from Propositions 5.4.1, 5.4.4, the numbers $\mathfrak{L}_v$ for $e_1 + 1 \leq v \leq e_2$ from Proposition 5.4.5 and the numbers $\mathfrak{L}_w$ for $e_2 + 1 \leq w \leq e_3$ from Proposition 5.4.6 in equation (5.3), we get the desired result. □

The following examples illustrate Theorem 5.4.1.

Example 5.4.1. Let $q = 2$, $t = 2$, $\gamma = 1$, $m_1 = 3$, $m_2 = 5$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 8$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^3 - 1 = (x+1)(x^2+x+1)$ and $x^{m_2} - \omega_2 = x^5 - 1 = (x+1)(x^4+x^3+x^2+x+1)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_2$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x^2 + x + 1$ and $h_3(x) = x^4 + x^3 + x^2 + x + 1$.

Further, we see that $h_u^\dagger(x) = h_u(x)$ for $1 \leq u \leq 3$, which gives $d_1 = 1$, $d_2 = 2$, $d_3 = 4$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{3,2} = 1$ and $\epsilon_{2,2} = \epsilon_{3,1} = 0$. This implies that $\epsilon_1 = 2$ and $\epsilon_2 = \epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 2128 distinct 0-complementary-dual, 1232 distinct $*$ -complementary-dual and 1232 distinct γ -complementary-dual Ω -MT additive codes of length 8 over $\mathbb{F}_{2^2}$, which agree with Theorem 5.4.1.

Example 5.4.2. Let $q = 5$, $t = 2$, $m_1 = m_2 = 3$, $\omega_1 = 1$ and $\omega_2 = 2$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 2)$. Here we see that $x^{m_1} - \omega_1 = x^3 - 1 = (x + 4)(x^2 + x + 1)$ and $x^{m_2} - \omega_2 = x^3 - 2 = (x + 2)(x^2 + 3x + 4)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_5$, respectively. Let us take $h_1(x) = x + 4$, $h_2(x) = x^2 + x + 1$, $h_3(x) = x + 2$ and $h_4(x) = x^2 + 3x + 4$. Further, we see that $h_u^\dagger(x) = h_u(x)$ for $1 \leq u \leq 2$, $h_3^\dagger(x) \neq h_3(x)$, $h_4^\dagger(x) \neq h_4(x)$ and $h_3^\dagger(x) \neq h_4(x)$, which gives $d_1 = d_3 = 1$, $d_2 = d_4 = 2$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = \epsilon_{4,2} = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = \epsilon_{4,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 29568 distinct 0-complementary-dual and 29568 distinct $*$ -complementary-dual Ω -MT additive codes of length 6 over $\mathbb{F}_{5^2}$, which agree with Theorem 5.4.1.

Example 5.4.3. Let $q = 3$, $t = 4$, $m_1 = 2$, and $\omega_1 = 1$, so that $n = m_1 = 2$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 2)$ is irreducible factorization of the polynomials $x^{m_1} - \omega_1$ over $\mathbb{F}_3$. Let us take $h_1(x) = x + 1$ and $h_2(x) = x + 2$. Further, we see that $h_u^\dagger(x) = h_u(x)$ for $1 \leq u \leq 2$, which gives $d_1 = d_2 = 1$ and $\epsilon_1 = \epsilon_2 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 23104 distinct 0-complementary-dual cyclic additive codes of length 2 over $\mathbb{F}_{3^4}$, which agree with Theorem 5.4.1.

Example 5.4.4. Let $q = 3$, $t = 3$, $m_1 = 2$, $m_2 = 4$ and $\omega_1 = 1$ and $\omega_2 = 2$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 2)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 2)$ and $x^{m_2} - \omega_2 = x^4 - 2 = (x^2 + x + 2)(x^2 + 2x + 2)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 2$, $h_3(x) = x^2 + x + 2$ and $h_4(x) = x^2 + 2x + 2$. Further, we see that $h_u(x) = h_u^\dagger(x)$ for $1 \leq u \leq 2$ and

$h_3(x) = h_4^\dagger(x)$, which gives $d_1 = d_2 = 1$, $d_3 = 2$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = \epsilon_{3,2}^\dagger = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = \epsilon_{3,1}^\dagger = 0$. This implies that $\epsilon_1 = \epsilon_2 = \eta_3 = 1$ and $\varrho_3 = \tau_3 = 0$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 36800 distinct 0-complementary-dual and 36800 distinct *-complementary-dual Ω -MT additive codes of length 6 over $\mathbb{F}_{3^3}$, which agree with Theorem [5.4.1](#).

Example 5.4.5. Let $q = 3$, $t = 2$, $m_1 = 2$, $m_2 = 4$ and $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 6$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 2)$ and $x^{m_2} - \omega_2 = x^4 - 1 = (x + 1)(x + 2)(x^2 + 1)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_3$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 2$ and $h_3(x) = x^2 + 1$. Further, we see that $h_u(x) = h_u^\dagger(x)$ for $1 \leq u \leq 3$, which gives $d_1 = d_2 = 1$, $d_3 = 2$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = \epsilon_{3,2} = 1$ and $\epsilon_{3,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = 2$ and $\epsilon_3 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 156800 distinct 0-complementary-dual and 156800 distinct *-complementary-dual Ω -MT additive codes of length 6 over $\mathbb{F}_{3^2}$, which agree with Theorem [5.4.1](#).

Example 5.4.6. Let $q = 5$, $t = 2$, $m_1 = m_2 = 2$, $\omega_1 = \omega_2 = 1$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 1)$. Here we see that $x^{m_1} - \omega_1 = x^{m_1} - \omega_2 = x^2 - 1 = (x + 1)(x + 4)$ is irreducible factorizations of the polynomial $x^{m_1} - \omega_1$ over $\mathbb{F}_5$. Let us take $h_1(x) = x + 1$ and $h_2(x) = x + 4$. Further, we see that $h_u(x) = h_u^\dagger(x)$ for $1 \leq u \leq 2$, which gives $d_1 = d_2 = 1$, $\epsilon_{1,1} = \epsilon_{1,2} = \epsilon_{2,1} = \epsilon_{2,2} = 1$. This implies that $\epsilon_1 = \epsilon_2 = 2$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 795664 distinct 0-complementary-dual and 795664 distinct *-complementary-dual Ω -MT additive codes of length 4 over $\mathbb{F}_{5^2}$, which agree with Theorem [5.4.1](#).

Example 5.4.7. Let $q = 7$, $t = 2$, $m_1 = m_2 = 2$, $\omega_1 = 1$ and $\omega_2 = 2$, so that $n = m_1 + m_2 = 4$ and $\Omega = (\omega_1, \omega_2) = (1, 2)$. Here we see that $x^{m_1} - \omega_1 = x^2 - 1 = (x + 1)(x + 6)$ and $x^{m_2} - \omega_2 = x^2 - 2 = (x + 3)(x + 4)$ are irreducible factorizations of the polynomials $x^{m_1} - \omega_1$ and $x^{m_2} - \omega_2$ over $\mathbb{F}_7$, respectively. Let us take $h_1(x) = x + 1$, $h_2(x) = x + 6$, $h_3(x) = x + 3$ and $h_4(x) = x + 4$. Further, we see that $h_u(x) = h_u^\dagger(x)$

for $1 \leq u \leq 2$, $h_3(x) \neq h_3^\dagger(x)$, $h_4(x) \neq h_4^\dagger(x)$ and $h_3(x) \neq h_4^\dagger(x)$, which gives $d_1 = d_2 = d_3 = d_4 = 1$, $\epsilon_{1,1} = \epsilon_{2,1} = \epsilon_{3,2} = \epsilon_{4,2} = 1$ and $\epsilon_{1,2} = \epsilon_{2,2} = \epsilon_{3,1} = \epsilon_{4,1} = 0$. This implies that $\epsilon_1 = \epsilon_2 = \epsilon_3 = \epsilon_4 = 1$. Now by carrying out computations in the Magma Computational Algebra System, we see that there are precisely 6400 distinct 0-complementary-dual and 6400 distinct $*$ -complementary-dual Ω -MT additive codes of length 4 over $\mathbb{F}_{7^2}$, which agree with Theorem [5.2.1](#).

In the next chapter, we apply probabilistic methods and results from groups and geometry to show that σ -self-orthogonal and σ -ACD MT additive codes over finite fields are asymptotically good for $\sigma \in \{0, \gamma, *\}$. We also deduce, as a special case, that σ -self-orthogonal and σ -ACD constacyclic additive codes over finite fields are asymptotically good for $\sigma \in \{0, \gamma, *\}$.

6

Self-orthogonal and ACD multi-twisted additive codes are asymptotically good

6.1 Introduction

In this chapter, we apply probabilistic methods and results from groups and geometry to study the asymptotic behavior of the rates and relative Hamming distances of self-orthogonal MT additive codes and ACD MT additive codes over finite fields with respect to ordinary, Hermitian and $*$ trace bilinear forms. We show that there exist asymptotically good infinite sequences of self-orthogonal and ACD MT additive codes over finite fields with respect to the aforementioned trace bilinear forms. This shows that self-orthogonal and ACD MT additive codes over finite fields are asymptotically good. We deduce, as special cases, that self-orthogonal

and ACD constacyclic additive codes over finite fields are asymptotically good.

This chapter is organized as follows: In Section 6.2, we study a special class of MT additive codes over finite fields on which our probabilistic methods can work well. In Section 6.3, we apply probabilistic methods and results from groups and geometry to study the asymptotic properties of the rates and relative Hamming distances of self-orthogonal and ACD codes belonging to the special class of MT additive codes studied in Section 6.2 (see Theorems 6.3.1, 6.3.2, 6.3.4, 6.3.5, 6.3.7 and 6.3.8). We also establish the existence of asymptotically good infinite sequences of self-orthogonal and ACD MT additive codes over finite fields (Theorems 6.3.3, 6.3.6 and 6.3.9). As a consequence of these results, we deduce that self-orthogonal and ACD constacyclic additive codes over finite fields are asymptotically good (Corollaries 6.3.1-6.3.3).

6.2 A class of MT additive codes over $\mathbb{F}_{q^t}$

In this section, we study a special class of MT additive codes over $\mathbb{F}_{q^t}$, and we further show that self-orthogonal and ACD codes belonging to this special class of MT additive codes are asymptotically good by applying probabilistic methods and results from groups and geometry stated in Chapter 2. Towards this, we assume, throughout this chapter, that q is a prime power, ω is a non-zero element of $\mathbb{F}_q$ with $\text{ord}(\omega) = e$, and $m = p^\alpha$, where p is an odd prime coprime to q and α is a positive integer. We next assume that $m_1 = m_2 = \cdots = m_\ell = m = p^\alpha$ and $\omega_1 = \omega_2 = \cdots = \omega_\ell = \omega$. We further assume that $p \nmid e$, which, by Theorem 3.75 of [43], implies that the polynomial $x^m - \omega$ is reducible over $\mathbb{F}_q$. Since $m_i = m$ and $\omega_i = \omega$ for $1 \leq i \leq \ell$, we have $n = m_1 + m_2 + \cdots + m_\ell = m\ell$ and $M = me = p^\alpha e$. Here, we also have $\epsilon_{\nu,i} = 1$ for $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$. In view of this, we see that $x^m - \omega = h_1(x)h_2(x) \cdots h_s(x)$ and $x^m - \omega^{-1} = h_1^\dagger(x)h_2^\dagger(x) \cdots h_s^\dagger(x)$ are irreducible factorizations of the polynomials $x^m - \omega$ and $x^m - \omega^{-1}$ over $\mathbb{F}_q$, respectively. Now let ξ be a fixed primitive (me) -th root of unity in an extension field of $\mathbb{F}_q$ satisfying $\xi^m = \omega$. Without any loss of generality, let us assume that $h_1(x)$ is the minimal polynomial of ξ over $\mathbb{F}_q$. We also note that $h_1^\dagger(x)$ is the minimal polynomial of ξ^{-1} over $\mathbb{F}_q$. One can easily observe that the degree of the minimal polynomial of ξ

is equal to the multiplicative order $\text{ord}_{me}(q)$ of q modulo me . From this, we have $d_1 = \deg h_1(x) = \deg h_1^\dagger(x) = \text{ord}_{me}(q)$. Let us suppose, throughout this chapter, that $v = \text{ord}_p(q)$. So we can write $q^v = 1 + p^\eta c$, where $\eta \geq 1$ and c are integers satisfying $p \nmid c$. Further, from (3.2), one can easily observe that

$$d_1 = \text{ord}_m(q) = \text{ord}_{p^\alpha}(q) = \begin{cases} v & \text{if } \alpha \leq \eta; \\ vp^{\alpha-\eta} & \text{if } \alpha \geq \eta + 1. \end{cases}$$

From this point on, we assume that the integer α satisfies $\alpha \geq \eta + 1$, which implies that

$$d_1 = \deg h_1(x) = \deg h_1^\dagger(x) = vp^{\alpha-\eta} > 1. \quad (6.1)$$

From now on, throughout this chapter, we will refer to an Ω -MT additive code of length $n = m\ell$ and block lengths $\underbrace{(m, m, \dots, m)}_{\ell \text{ times}}$ over $\mathbb{F}_{q^t}$ simply as an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, where $\Omega = \underbrace{(\omega, \omega, \dots, \omega)}_{\ell \text{ times}}$. We will further restrict our attention to a special class of 1-generator MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ on which our probabilistic methods can work well.

Next, let $d_\nu = \deg h_\nu(x) = \deg h_\nu^\dagger(x)$ for $1 \leq \nu \leq s$. By (3.1) and (4.1), we recall that

$$\mathcal{R} = \mathcal{R}_{m,\omega}^\ell \simeq \bigoplus_{\nu=1}^s \mathbb{W}_\nu^\ell = \bigoplus_{\nu=1}^s \mathbb{G}_\nu = \mathbb{G}$$

and

$$\widehat{\mathcal{R}} = \mathcal{R}_{m,\omega^{-1}}^\ell \simeq \bigoplus_{\nu=1}^s \mathbb{W}_\nu^{\dagger\ell} = \bigoplus_{\nu=1}^s \mathbb{G}_\nu^\dagger = \mathbb{G}^\dagger,$$

where

$$\mathbb{W}_\nu = \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle}, \quad \mathbb{W}_\nu^\dagger = \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu^\dagger(x) \rangle}, \quad \mathcal{F}_\nu = \frac{\mathbb{F}_q[x]}{\langle h_\nu(x) \rangle} \simeq \mathbb{F}_{q^{d_\nu}} \quad \text{and} \quad \mathcal{F}_\nu^\dagger = \frac{\mathbb{F}_q[x]}{\langle h_\nu^\dagger(x) \rangle} \simeq \mathbb{F}_{q^{d_\nu}}$$

for $1 \leq \nu \leq s$. We further observe, for $1 \leq \nu \leq s$, that the sets $\mathbb{G}_\nu = \mathbb{W}_\nu^\ell$ and $\mathbb{G}_\nu^\dagger = \mathbb{W}_\nu^{\dagger\ell}$ are (ℓt) -dimensional vector spaces over $\mathcal{F}_\nu$ and $\mathcal{F}_\nu^\dagger$, respectively. By Theorem 3.3.1 and by applying the Chinese Remainder Theorem [7, Th. 1.2.12], we see that each $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ is an MT additive code of length $m\ell$ and block

length m over $\mathbb{F}_{q^t}$. In addition, we note, by Theorem 3.3.1 and by applying the Chinese Remainder Theorem [7 Th. 1.2.12] again, that the direct sum of an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ and an $\mathcal{F}_\nu^\dagger$ -subspace of $\mathbb{G}_\nu^\dagger$ is also an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$. Now to study σ -dual codes of these MT additive codes, let $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger}$ denote the restriction of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ to $\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger$ for $\sigma \in \{0, \gamma, *\}$. Here, we recall, by Theorem 4.3.1, that if $\mathcal{C}_\nu$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$, then for $\sigma \in \{0, \gamma, *\}$, the orthogonal complement of $\mathcal{C}_\nu$ with respect to the form $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu^\dagger}$, denoted by $\mathcal{C}_\nu^{\perp\sigma}$, is defined as

$$\mathcal{C}_\nu^{\perp\sigma} = \{B_\nu(x) \in \mathbb{G}_\nu^\dagger : [A_\nu(x), B_\nu(x)]_\sigma = 0 \text{ for all } A_\nu(x) \in \mathcal{C}_\nu\}.$$

Further, we recall that the $\mathcal{F}_\nu$ -subspace $\mathcal{C}_\nu$ of $\mathbb{G}_\nu$ is (i) σ -self-orthogonal (or σ -totally isotropic) if it satisfies $\mathcal{C}_\nu \subseteq \mathcal{C}_\nu^{\perp\sigma}$ and (ii) σ -non-degenerate if it satisfies $\mathcal{C}_\nu \cap \mathcal{C}_\nu^{\perp\sigma} = \{0\}$. Now to show that σ -self-orthogonal and σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ are asymptotically good, we will first study σ -self-orthogonal and σ -non-degenerate $\mathcal{F}_\nu$ -subspaces of $\mathbb{G}_\nu$. Towards this, we first make the following observation.

Lemma 6.2.1. *For $\sigma \in \{0, \gamma, *\}$, if there exists a non-zero σ -self-orthogonal $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$, then $\omega = \omega^{-1}$ and $h_\nu(x) = h_\nu^\dagger(x)$.*

Proof. Its proof is a straightforward exercise. □

6.3 Asymptotically good σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ exist

In this section, we show that for $\sigma \in \{0, \gamma, *\}$, σ -self-orthogonal and σ -ACD MT additive codes over finite fields are asymptotically good. For this, let $\mathbb{Z}_{ep^\eta}^*$ be the unit group of the ring $\mathbb{Z}_{ep^\eta}$ of integers modulo ep^η . Note that $q \in \mathbb{Z}_{ep^\eta}^*$. Let $Q = \langle q \rangle$ be the cyclic subgroup of $\mathbb{Z}_{ep^\eta}^*$ generated by the element $q \in \mathbb{Z}_{ep^\eta}^*$. We next observe the following:

Lemma 6.3.1. (a) *The polynomial $h_1(x)$ is self-reciprocal if and only if $-1 \in Q$.*

(b) Suppose that $-1 \notin Q$. Both polynomials $h_1(x)$ and $h_1^\dagger(x)$ divide $x^m - \omega$ in $\mathbb{F}_q[x]$ if and only if $\omega = \omega^{-1}$.

Proof. (a) Here, we first recall that ξ is a primitive $(p^\alpha e)$ -th root of unity in an extension field of $\mathbb{F}_q$ satisfying $\xi^{p^\alpha} = \omega$. Now since $h_1(x)$ is the minimal polynomial of ξ over $\mathbb{F}_q$ having degree d_1 , we have $\xi \in \mathbb{F}_{q^{d_1}}$. By Theorem 4.4.1 of [35], we see the polynomial $h_1(x)$ corresponds to the q -cyclotomic coset $C_1(q) = \{1, q, q^2, \dots, q^{d_1-1}\}$ modulo ep^α . Furthermore, the q -cyclotomic coset corresponding to the reciprocal polynomial $h_1^\dagger(x)$ is given by $C_{-1}(q) = \{-1, -q, -q^2, \dots, -q^{d_1-1}\}$ modulo ep^α . One can easily see that $h_1(x) = h_1^\dagger(x)$ if and only if $C_1(q) = C_{-1}(q)$, which holds if and only if there exists an integer z satisfying $0 < z < d_1$ and $q^z \equiv -1 \pmod{ep^\alpha}$. This further holds if and only if $q^w \equiv -1 \pmod{ep^\eta}$ for some integer w satisfying $0 < w < v$, which holds if and only if $-1 \in Q$.

(b) Suppose that $-1 \notin Q$. In this case, we see, by part (a), that $h_1(x) \neq h_1^\dagger(x)$. Now both $h_1(x)$ and $h_1^\dagger(x)$ divide $x^m - \omega$ in $\mathbb{F}_q[x]$ if and only if $\xi^m = \omega = \xi^{-m}$, which holds if and only if $\omega = \omega^{-1}$. □

In view of Lemma 6.3.1, we now distinguish the following three cases: **I.** $-1 \in Q$, **II.** $-1 \notin Q$ and $\omega = \omega^{-1}$, and **III.** $-1 \notin Q$ and $\omega \neq \omega^{-1}$.

6.3.1 The case $-1 \in Q$

Throughout this section, let us assume that $-1 \in Q$, *i.e.*, there exists a positive integer z such that $q^z \equiv -1 \pmod{ep^\eta}$. By Lemma 6.3.1(a), we see that $h_1(x) = h_1^\dagger(x)$. In this case, we have $\omega = \omega^{-1}$. This implies that $\mathcal{F}_1 = \mathcal{F}_1^\dagger$ and $\mathbb{G}_1 = \mathbb{G}_1^\dagger$. By (6.1), we see that $d_1 = \deg h_1(x) = vp^{\alpha-\eta} > 1$. As $h_1(x) = h_1^\dagger(x)$, one can easily see that the integer d_1 is even, *i.e.*, the integer $v = \text{ord}_p(q)$ is even in this case. Further, for $\sigma \in \{0, *\}$, we recall, by Lemma 4.4.2(c), that the map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ is a non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form, *i.e.*, $(\mathbb{G}_1, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a unitary space of dimension ℓt over $\mathcal{F}_1 \simeq \mathbb{F}_{q^{d_1}}$. By Lemma 4.4.2(d), we see that the map $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathbb{G}_1$. Here working as in the proof of Lemma 5.2.1(b), one can

transform the skew-Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ to an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$. One can easily see that $(\mathbb{G}_1, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a unitary space of dimension ℓt over $\mathcal{F}_1$. We further observe that an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ is γ -self-orthogonal (*resp.* γ -non-degenerate) if and only if it is self-orthogonal (*resp.* non-degenerate) with respect to the form $[\cdot, \cdot]_{\gamma_H}$. In view of this, from now on, we will consider the Hermitian form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ instead of the skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$. So, without any loss of generality, we assume that $\sigma \in \{0, \gamma_H, *\}$ in this case. That is, $(\mathbb{G}_1, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a unitary space of dimension ℓt over $\mathcal{F}_1$ for each $\sigma \in \{0, \gamma_H, *\}$. From this and by Theorem 2.2.4(b), we see that there exists a σ -self-orthogonal $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$, and hence the converse of Lemma 6.2.1 also holds in this case. Now let us define the sets

$$M_1 = \{A(x) (\neq \mathbf{0}) \in \mathbb{G}_1 : [A(x), A(x)]_\sigma = 0\}$$

and

$$N_1 = \{A(x) (\neq \mathbf{0}) \in \mathbb{G}_1 : [A(x), A(x)]_\sigma \neq 0\}.$$

We see that the set M_1 (*resp.* N_1) consists of all the isotropic (*resp.* non-isotropic) elements of $\mathbb{G}_1$. For $\sigma \in \{0, \gamma_H, *\}$, since $(\mathbb{G}_1, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a unitary space of dimension ℓt over $\mathcal{F}_1 \simeq \mathbb{F}_{q^{d_1}}$, we see, by Theorem 2.2.4(c), that

$$|M_1| = \begin{cases} (q^{\frac{(\ell t - 1)d_1}{2}} - 1)(q^{\frac{\ell t d_1}{2}} + 1) & \text{if } \ell t \text{ is odd;} \\ (q^{\frac{(\ell t - 1)d_1}{2}} + 1)(q^{\frac{\ell t d_1}{2}} - 1) & \text{if } \ell t \text{ is even} \end{cases} \quad (6.2)$$

and

$$|N_1| = \begin{cases} (q^{\frac{\ell t d_1}{2}} - q^{\frac{(\ell t - 1)d_1}{2}})(q^{\frac{\ell t d_1}{2}} + 1) & \text{if } \ell t \text{ is odd;} \\ (q^{\frac{\ell t d_1}{2}} - q^{\frac{(\ell t - 1)d_1}{2}})(q^{\frac{\ell t d_1}{2}} - 1) & \text{if } \ell t \text{ is even.} \end{cases} \quad (6.3)$$

By (6.2) and (6.3), we deduce that $|M_1| \geq (q^{\frac{(\ell t - 1)d_1}{2}} - 1)(q^{\frac{\ell t d_1}{2}} - 1)$ and $|N_1| \geq (q^{\frac{\ell t d_1}{2}} - q^{\frac{(\ell t - 1)d_1}{2}})(q^{\frac{\ell t d_1}{2}} - 1)$. We next make the following observation.

Lemma 6.3.2. *For a non-zero $A(x) \in \mathbb{G}_1$, the set $\mathcal{C}_A = \{f(x)A(x) : f(x) \in \mathcal{F}_1\}$ is a non-zero $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ generated by the element $A(x)$. Further, for $\sigma \in \{0, \gamma, *\}$, the following hold.*

(a) *The subspace $\mathcal{C}_A$ of $\mathbb{G}_1$ is σ -self-orthogonal if and only if $A(x) \in M_1$.*

- (b) The subspace $\mathcal{C}_A$ of $\mathbb{G}_1$ is σ -non-degenerate if and only if $A(x) \in N_1$.
- (c) We have $|\mathcal{C}_A| = q^{d_1}$.

Proof. Parts (a) and (b) are trivial, while part (c) follows from Lemma 3.5.1. $\square$

We now proceed to study asymptotic behaviour of the rates and relative Hamming distances of σ -self-orthogonal and σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$. Towards this, we see, by Theorem 4.4.1, that it is enough to study the asymptotic properties of the rates and relative Hamming distances of σ -self-orthogonal and σ -non-degenerate $\mathcal{F}_1$ -subspaces of $\mathbb{G}_1$. Accordingly, we view the set M_1 (*resp.* N_1) as a probability space, where each sample of M_1 (*resp.* N_1) is chosen with equal probability. Now for each sample $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in M_1$ (*resp.* N_1), we see, by (6.1) and using Lemma 6.3.2, that the set

$$\mathcal{C}_A = \{f(x)A(x) = (f(x)A_1(x), f(x)A_2(x), \dots, f(x)A_\ell(x)) : f(x) \in \mathcal{F}_1\} \quad (6.4)$$

is a random σ -self-orthogonal (*resp.* σ -non-degenerate) $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$, and hence by Theorem 4.4.1, the subspace $\mathcal{C}_A$ is a random σ -self-orthogonal (*resp.* σ -ACD) MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, whose rate is given by

$$R(\mathcal{C}_A) = \frac{\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A}{m\ell} = \frac{\log_{q^t} |\mathcal{C}_A|}{m\ell} = \frac{d_1}{m\ell t} = \frac{vp^{\alpha-\eta}}{p^\alpha \ell t} = \frac{v}{p^\eta \ell t}.$$

Recall that the relative Hamming distance of the random code $\mathcal{C}_A$ is given by $\Delta(\mathcal{C}_A) = \frac{wt(\mathcal{C}_A)}{m\ell}$. In view of this, we see that the relative Hamming distance $\Delta(\mathcal{C}_A)$ and the dimension $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A$ of the random code $\mathcal{C}_A$ are random variables over each of the probability spaces M_1 and N_1 with uniform probability. We will now study the asymptotic behaviour of the probabilities $\Pr(\Delta(\mathcal{C}_A) > \delta)$ and $\Pr(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \frac{d_1}{t})$, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For this, let $f(x) \in \mathcal{F}_1$ be fixed, and let I_f be an ideal of $\mathcal{R}_{m,\omega}$ generated by the element $f(x)$, *i.e.*,

$$I_f = \langle f(x) \rangle_{\mathcal{R}_{m,\omega}} = \{f(x)b(x) : b(x) \in \mathcal{R}_{m,\omega}\} = \{f(x)b_1(x) : b_1(x) \in \mathbb{W}_1\} \subseteq \mathbb{W}_1.$$

We further observe the following:

Lemma 6.3.3. *Let $f(x) \in \mathcal{F}_1$ be fixed, and let $B(x) = (B_1(x), B_2(x), \dots, B_\ell(x)) \in I_f^\ell$. If $f(x) = 0$, then $\Pr(f(x)A(x) = B(x)) = 1$ for all $A(x) \in M_1$ (resp. N_1). Further, if $f(x) \neq 0$, then we have*

$$\Pr(f(x)A(x) = B(x)) \leq \begin{cases} \frac{1}{(q^{\frac{(\ell t-1)d_1}{2}} - 1)(q^{\frac{\ell t d_1}{2}} - 1)} & \text{if } A(x) \text{ runs over the} \\ & \text{probability space } M_1; \\ \frac{1}{(q^{\frac{\ell t d_1}{2}} - q^{\frac{(\ell t-1)d_1}{2}})(q^{\frac{\ell t d_1}{2}} - 1)} & \text{if } A(x) \text{ runs over the} \\ & \text{probability space } N_1. \end{cases}$$

Proof. To prove the result, let $\mathcal{S}_1$ be either M_1 or N_1 . Let T_1 be the number of $A(x) \in \mathcal{S}_1$ satisfying $f(x)A(x) = B(x)$. It is easy to see that $T_1 = |\mathcal{S}_1|$ if $f(x) = 0$, otherwise $T_1 \leq 1$. Therefore, we have $\Pr(f(x)A(x) = B(x)) = \frac{T_1}{|\mathcal{S}_1|}$. From this and on substituting the values of $|M_1|$ and $|N_1|$ from equations (6.2) and (6.3) in the respective cases, we get the desired result. $\square$

Now let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For a sample $A(x)$ in M_1 (resp. N_1), let $\mathcal{N}_{\mathcal{C}_A}(\delta)$ equal the number of non-zero codewords in the random code $\mathcal{C}_A$ whose relative Hamming weight is at most δ . Note that

$$\mathcal{N}_{\mathcal{C}_A}(\delta) = |\{f(x) \in \mathcal{F}_1 : 0 < \widehat{wt}(f(x)A(x)) \leq \delta\}|$$

is a non-negative integral random variable over the probability space M_1 (resp. N_1) and is called the *cumulative weight enumerator* of the random code $\mathcal{C}_A$. Further, for each $f(x) \in \mathcal{F}_1$ and samples $A(x) \in M_1$ (resp. N_1), let us define the *indicator random variable* Y_f as

$$Y_f = \begin{cases} 1 & \text{if } 0 < \widehat{wt}(f(x)A(x)) \leq \delta; \\ 0 & \text{otherwise.} \end{cases}$$

Note that Y_f is a Bernoulli random variable defined over the probability space M_1 (resp. N_1). It is easy to see that $Y_0 = 0$ and that

$$\mathcal{N}_{\mathcal{C}_A}(\delta) = \sum_{f(x) \neq 0 \in \mathcal{F}_1} Y_f.$$

Further, for a non-zero $f(x) \in \mathcal{F}_1$, let $E(Y_f)$ denote the expectation of the corresponding indicator random variable Y_f . We further observe the following:

Lemma 6.3.4. *For a non-zero $f(x) \in \mathcal{F}_1$, we have*

$$E(Y_f) \leq \begin{cases} \frac{q^{-\ell t d_1(1 - \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\frac{(\ell t - 1)d_1}{2}})(1 - q^{-\frac{\ell t d_1}{2}})} & \text{if } A(x) \text{ runs over the probability space } M_1; \\ \frac{q^{-\ell t d_1(1 - h_{q^t}(\delta))}}{(1 - q^{-\frac{d_1}{2}})(1 - q^{-\frac{\ell t d_1}{2}})} & \text{if } A(x) \text{ runs over the probability space } N_1. \end{cases}$$

Proof. To prove the result, let $\mathcal{S}_1$ be either M_1 or N_1 . Here we see that Y_f is a Bernoulli random variable over the probability space $\mathcal{S}_1$ with the uniform probability. This implies that

$$\begin{aligned} E(Y_f) &= \Pr(Y_f = 1) = \frac{|\{A(x) \in \mathcal{S}_1 : 0 < \widehat{wt}(f(x)A(x)) \leq \delta\}|}{|\mathcal{S}_1|} \\ &= \sum_{\substack{B(x) \in I_f^\ell \\ 0 < \widehat{wt}(B(x)) \leq \delta}} \frac{|\{A(x) \in \mathcal{S}_1 : f(x)A(x) = B(x)\}|}{|\mathcal{S}_1|} \\ &= \sum_{B(x) (\neq \mathbf{0}) \in (I_f^\ell)^{\leq \delta}} \Pr(f(x)A(x) = B(x)) \\ &\leq |I_f^\ell|^{\leq \delta} \Pr(f(x)A(x) = B(x)), \end{aligned}$$

where $A(x)$ runs over the probability space $\mathcal{S}_1$. Now by applying Lemmas 3.5.3 and 6.3.3, the desired result follows. $\square$

We next make the following observation.

Lemma 6.3.5. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For $A(x) \in M_1$ (resp. N_1), let $\mathcal{C}_A$ be the corresponding σ -self-orthogonal (resp. σ -ACD) MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by (6.4). We have*

$$\Pr(\Delta(\mathcal{C}_A) \leq \delta) \leq \begin{cases} \frac{q^{-\ell t d_1(1 - \frac{3}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\frac{(\ell t - 1)d_1}{2}})(1 - q^{-\frac{\ell t d_1}{2}})} & \text{if } A(x) \in M_1; \\ \frac{q^{-\ell t d_1(1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\frac{d_1}{2}})(1 - q^{-\frac{\ell t d_1}{2}})} & \text{if } A(x) \in N_1. \end{cases}$$

Proof. Working as in Lemma 3.5.5 and by applying Lemma 6.3.4, the desired result follows. $\square$

Next, let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for all $j \geq 1$. Here we note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. For each integer $j \geq 1$, let $x^{\mathbf{m}_j} - \omega = h_1^{(j)}(x)h_2^{(j)}(x) \cdots h_{s_j}^{(j)}(x)$ be the irreducible factorization of the polynomial $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$. Further, for each positive integer j , let ξ_j be a primitive $(\mathbf{m}_j e)$ -th root of unity in some extension field of $\mathbb{F}_q$ satisfying $\xi_j^{\mathbf{m}_j} = \omega$, and let $h_1^{(j)}(x)$ be the minimal polynomial of ξ_j over $\mathbb{F}_q$. Since $\gcd(\mathbf{m}_j, e) = 1$ and $\text{ord}_e(q) = 1$, we see, by (6.1), that

$$d_1^{(j)} = \deg h_1^{(j)}(x) = \text{ord}_{\mathbf{m}_j e}(q) = \text{lcm}[\text{ord}_{\mathbf{m}_j}(q), \text{ord}_e(q)] = \text{ord}_{\mathbf{m}_j}(q) = vp^{\alpha_j - \eta}$$

for all $j \geq 1$. Next, for each $j \geq 1$, let us recall

$$\mathcal{F}_1^{(j)} = \frac{\mathbb{F}_q[x]}{\langle h_1^{(j)}(x) \rangle} \quad \text{and} \quad \mathbb{G}_1^{(j)} = \left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle} \right)^\ell.$$

Further, since $-1 \in Q$, we see, by Lemma 6.3.1(a), that $h_1^{(j)}(x) = h_1^{(j)\dagger}(x)$ for each j . Now for $\sigma \in \{0, \gamma_H, *\}$, let us define

$$M_1^{(j)} = \left\{ A^{(j)}(x) (\neq \mathbf{0}) \in \mathbb{G}_1^{(j)} : [A^{(j)}(x), A^{(j)}(x)]_\sigma = 0 \right\}$$

and

$$N_1^{(j)} = \left\{ A^{(j)}(x) (\neq \mathbf{0}) \in \mathbb{G}_1^{(j)} : [A^{(j)}(x), A^{(j)}(x)]_\sigma \neq 0 \right\}.$$

Here for each $j \geq 1$, we shall view the set $M_1^{(j)}$ (*resp.* $N_1^{(j)}$) as a probability space, where each sample is chosen with equal probability. Further, for each j and each sample $A^{(j)}(x) = (A_1^{(j)}(x), A_2^{(j)}(x), \dots, A_\ell^{(j)}(x))$ in $M_1^{(j)}$ (*resp.* $N_1^{(j)}$), let

$$\mathcal{C}_{A^{(j)}} = \left\{ f^{(j)}(x)A^{(j)}(x) = \left(f^{(j)}(x)A_1^{(j)}(x), \dots, f^{(j)}(x)A_\ell^{(j)}(x) \right) : f^{(j)}(x) \in \mathcal{F}_1^{(j)} \right\} \quad (6.5)$$

be a random σ -self-orthogonal (*resp.* σ -ACD) MT additive code of length $\mathbf{m}_j \ell$ and

block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ defined over the probability space $M_1^{(j)}$ (resp. $N_1^{(j)}$), where $\sigma \in \{0, \gamma_H, *\}$, (or equivalently, $\sigma \in \{0, \gamma, *\}$).

Theorem 6.3.1. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. If δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) > \delta \right) \right\} = 1.$$

Proof. Since $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, we have $\frac{1}{2} - \frac{1}{2\ell t} - h_{q^t}(\delta) > 0$. Also for $t \geq 2$, we have $\frac{1}{\ell t} \leq \frac{1}{2}$, which implies that $1 - \frac{1}{\ell t} - h_{q^t}(\delta) > 0$ and $1 - \frac{3}{2\ell t} - h_{q^t}(\delta) > 0$. Here we recall that $d_1^{(j)} = vp^{\alpha_j - \eta}$. Now by Lemma 6.3.5, we see that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta \right) \right\} \leq \lim_{j \rightarrow \infty} \left\{ \frac{q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{3}{2\ell t} - h_{q^t}(\delta))}}{\left(1 - q^{\frac{-(\ell t - 1) v p^{\alpha_j - \eta}}{2}}\right) \left(1 - q^{\frac{-\ell t v p^{\alpha_j - \eta}}{2}}\right)} \right\}$$

if $A^{(j)} \in M_1^{(j)}$, while

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta \right) \right\} \leq \lim_{j \rightarrow \infty} \left\{ \frac{q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{\left(1 - q^{\frac{-v p^{\alpha_j - \eta}}{2}}\right) \left(1 - q^{\frac{-\ell t v p^{\alpha_j - \eta}}{2}}\right)} \right\}$$

if $A^{(j)}(x) \in N_1^{(j)}$. Since $\lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, we note that $\lim_{j \rightarrow \infty} \{v p^{\alpha_j - \eta}\} = \infty$, which implies that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta \right) \right\} = 0.$$

From this, it follows that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) > \delta \right) \right\} = 1 - \lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{A^{(j)}}) \leq \delta \right) \right\} = 1.$$

□

Theorem 6.3.2. *Let $\sigma \in \{0, \gamma, *\}$, and let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. For a sample $A^{(j)}(x) \in M_1^{(j)}$ (resp. $N_1^{(j)}$), let $\mathcal{C}_{A^{(j)}}$ be a random σ -self-orthogonal (resp. σ -ACD) MT additive code of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{q^t}$ as defined*

by (6.5). We have

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{d_1^{(j)}}{t} = \frac{vp^{\alpha_j - \eta}}{t} \right) \right\} = 1.$$

Proof. Working as in Theorem 3.5.2, the desired result follows. $\square$

In the following theorem, we consider the case $-1 \in Q$ and $\omega = \omega^{-1}$, and we show that there exist infinite sequences of σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ having rate $\frac{v}{p^n \ell t}$ and relative Hamming distance at least δ for $\sigma \in \{0, \gamma_H, *\}$ (and hence for $\sigma \in \{0, \gamma, *\}$), where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$.

Theorem 6.3.3. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. Suppose that $-1 \in Q$ and $\omega = \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, there exist infinite sequences $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -self-orthogonal MT additive codes $\mathcal{C}_j$'s and σ -ACD MT additive codes $\mathcal{D}_j$'s of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{q^t}$ respectively, such that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$,*

$$(i) \ R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{v}{p^n \ell t},$$

$$(ii) \ \Delta_{\mathfrak{F}} > \delta \text{ and } \Delta_{\mathfrak{G}} > \delta.$$

Proof. It follows immediately from Theorems 6.3.1 and 6.3.2. $\square$

As a consequence of the above theorem, we see that σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ are asymptotically good for each $\sigma \in \{0, \gamma, *\}$. Furthermore, in the following corollary, we deduce that σ -self-orthogonal and σ -ACD ω -constacyclic additive codes over $\mathbb{F}_{q^t}$ are asymptotically good when $-1 \in Q$ and $\omega = \omega^{-1}$.

Corollary 6.3.1. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2t}$. Suppose that $-1 \in Q$ and $\omega = \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, there exist infinite sequences $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -self-orthogonal ω -constacyclic additive codes $\mathcal{C}_j$'s and σ -ACD ω -constacyclic additive codes $\mathcal{D}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$ respectively, such that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{v}{p^n t}$, $\Delta_{\mathfrak{F}} > \delta$ and $\Delta_{\mathfrak{G}} > \delta$.*

Proof. It follows immediately by taking $\ell = 1$ in Theorem [6.3.3](#). $\square$

Example 6.3.1. Let $q = 11$, $p = 17$, $\omega = -1$, $\ell = 1$ and $t = 2$. Here we have $v = \text{ord}_p(q) = \text{ord}_{17}(11) = 16$, $\eta = 1$, $e = \text{ord}(\omega) = 2$, and $Q = \langle 11 \rangle = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33\}$. Note that $-1 = 33 \in Q$ and $\omega = \omega^{-1}$ in this case. By Corollary [6.3.1](#), we see that there exist infinite sequences $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -self-orthogonal ω -constacyclic additive codes $\mathcal{C}_j$'s and σ -ACD ω -constacyclic additive codes $\mathcal{D}_j$'s of length 17^{α_j} over $\mathbb{F}_{11^2}$ respectively, such that $\lim_{j \rightarrow \infty} \{17^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{v}{p^{\eta}t} = \frac{8}{13}$, $\Delta_{\mathfrak{F}} > \delta$ and $\Delta_{\mathfrak{G}} > \delta$, where δ is a positive real number satisfying $\delta < 0.159$.

Remark 6.3.1. Taking $\omega = 1$ in Corollary [6.3.1](#), we see that σ -self-orthogonal and σ -ACD cyclic additive codes over finite fields are asymptotically good.

6.3.2 The case $-1 \notin Q$ and $\omega = \omega^{-1}$

Throughout this section, let us assume that $-1 \notin Q$ and $\omega = \omega^{-1}$. Here by Lemma [6.3.1](#)(b), we see that $h_1(x) \neq h_1^\dagger(x)$ and that $h_1^\dagger(x)$ divides $x^m - \omega$ in $\mathbb{F}_q[x]$. This implies that the polynomials $h_1(x)$ and $h_1^\dagger(x)$ form a reciprocal pair. From now on, throughout this section, we will represent elements of the direct sum $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ as $\mathbf{A}(x) = A(x) + \tilde{A}(x)$, where $A(x) \in \mathbb{G}_1$ and $\tilde{A}(x) \in \mathbb{G}_1^\dagger$. Similarly, we will represent elements of the direct sum $\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ as $\mathbf{f}(x) = f(x) + \tilde{f}(x)$, where $f(x) \in \mathcal{F}_1$ and $\tilde{f}(x) \in \mathcal{F}_1^\dagger$. One can easily observe that the set $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ can be viewed as an $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -module under the following operations:

$$\mathbf{A}(x) + \mathbf{B}(x) = (A(x) + B(x)) + (\tilde{A}(x) + \tilde{B}(x)) \quad (\text{addition}) \quad (6.6)$$

$$\mathbf{f}(x) \odot \mathbf{A}(x) = f(x)A(x) + \tilde{f}(x)\tilde{A}(x) \quad (\text{scalar multiplication}) \quad (6.7)$$

for all $\mathbf{A}(x) = A(x) + \tilde{A}(x)$, $\mathbf{B}(x) = B(x) + \tilde{B}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ and $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$. Further, for $\sigma \in \{0, \gamma, *\}$, we observe that

$$[\mathbf{A}(x), \mathbf{B}(x)]_\sigma = [A(x), \tilde{B}(x)]_\sigma + [\tilde{A}(x), B(x)]_\sigma \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$$

for all $\mathbf{A}(x) = A(x) + \tilde{A}(x)$, $\mathbf{B}(x) = B(x) + \tilde{B}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$.

Next, let $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$ be the restriction of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ to $(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)$. In the following lemma, we derive some basic properties of this restriction map.

Lemma 6.3.6. *For $\sigma \in \{0, \gamma, *\}$ the following hold.*

- (a) $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is a free $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -module of rank $4t$.
- (b) $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$ is a reflexive and non-degenerate $\tau_{1,-1}$ -sesquilinear form.
- (c) The form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$ is Hermitian when $\sigma \in \{0, *\}$ and is skew-Hermitian when $\sigma = \gamma$.

Proof. The proof of part (a) is a straightforward exercise, while parts (b) and (c) follow from Lemma 4.4.2 $\square$

Now if $\mathcal{C}_1$ is an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ and $\mathcal{C}_1^\dagger$ is an $\mathcal{F}_1^\dagger$ -subspace of $\mathbb{G}_1^\dagger$, then the direct sum $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ is an $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ with respect to the addition and scalar multiplication defined by (6.6) and (6.7), respectively. Conversely, every $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule $\mathcal{D}$ of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ can be uniquely expressed as a direct sum $\mathcal{D} = \mathcal{D}_1 \oplus \mathcal{D}_1^\dagger$, where $\mathcal{D}_1$ is an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ and $\mathcal{D}_1^\dagger$ is an $\mathcal{F}_1^\dagger$ -subspace of $\mathbb{G}_1^\dagger$.

Let $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ be an $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$, where $\mathcal{C}_1$ is an $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ and $\mathcal{C}_1^\dagger$ is an $\mathcal{F}_1^\dagger$ -subspace of $\mathbb{G}_1^\dagger$. For $\sigma \in \{0, \gamma, *\}$, the orthogonal complement of $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ with respect to the form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$ is defined as

$$(\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger)^{\perp_\sigma} = \{\mathbf{B}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger : [\mathbf{A}(x), \mathbf{B}(x)]_\sigma = 0 \text{ for all } \mathbf{A}(x) \in \mathcal{C}_1 \oplus \mathcal{C}_1^\dagger\}.$$

We observe that $(\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger)^{\perp_\sigma}$ is an $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ and that $(\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger)^{\perp_\sigma} = \mathcal{C}_1^{\perp_\sigma} \oplus \mathcal{C}_1^{\perp_\sigma \dagger}$, where $\mathcal{C}_1^{\perp_\sigma} \subseteq \mathbb{G}_1$ is the orthogonal complement of $\mathcal{C}_1$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ and $\mathcal{C}_1^{\perp_\sigma \dagger} \subseteq \mathbb{G}_1^\dagger$ is the orthogonal complement of $\mathcal{C}_1^\dagger$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1^\dagger \times \mathbb{G}_1^\dagger}$. We say that the $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is σ -self-orthogonal (or σ -totally isotropic) if it satisfies $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger \subseteq (\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger)^{\perp_\sigma}$. One can easily see that the module $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ is σ -self-orthogonal if and only if $\mathcal{C}_1 \subseteq \mathcal{C}_1^{\perp_\sigma}$. Furthermore, we say that the module $\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger$ is σ -non-degenerate if it satisfies $(\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger) \cap (\mathcal{C}_1 \oplus \mathcal{C}_1^\dagger)^{\perp_\sigma} = \{0\}$.

By Lemma 6.3.6(c), we see that the form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$ is skew-Hermitian. Here we shall first transform this skew-Hermitian form to an orthogonality preserving Hermitian form as follows: Let us take $\zeta(x) = \varsigma(x) - \tau_{1,-1}(\varsigma(x)) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$, where $\varsigma(x)$ is a non-zero element in $\mathcal{F}_1$. Note that $\zeta(x) \neq 0$ and $\tau_{1,-1}(\zeta(x)) = -\zeta(x)$. Now let us define a map $[\cdot, \cdot]_{\gamma_H} : (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \rightarrow \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ as

$$[\mathbf{A}(x), \mathbf{B}(x)]_{\gamma_H} = \zeta(x)([\mathbf{A}(x), \mathbf{B}(x)]_\gamma) \text{ for all } \mathbf{A}(x), \mathbf{B}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger.$$

It is easy to observe that the map $[\cdot, \cdot]_{\gamma_H}$ is a non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form. We next observe that an $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is γ -self-orthogonal (*resp.* γ -non-degenerate) if and only if it is self-orthogonal (*resp.* non-degenerate) with respect to the form $[\cdot, \cdot]_{\gamma_H}$. In view of this, from now on, we will consider the Hermitian form $[\cdot, \cdot]_{\gamma_H}$ on $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ instead of the skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)}$. So without any loss of generality, we assume that $\sigma \in \{0, \gamma_H, *\}$ in this case.

Next, a non-zero element $\mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is called an *isotropic* element if it satisfies $[\mathbf{A}(x), \mathbf{A}(x)]_\sigma = [A(x) + \tilde{A}(x), A(x) + \tilde{A}(x)]_\sigma = 0$, *i.e.*, if $[A(x), \tilde{A}(x)]_\sigma = [\tilde{A}(x), A(x)]_\sigma = 0$. It is easy to see that each non-zero element of $\mathbb{G}_1 \cup \mathbb{G}_1^\dagger$ is trivially an isotropic element. The isotropic element $\mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is said to be *non-trivial* if both $A(x)$ and $\tilde{A}(x)$ are non-zero. A non-zero element $\mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is said to be *non-isotropic* if it satisfies $[\mathbf{A}(x), \mathbf{A}(x)]_\sigma \neq 0$, *i.e.*, if $[A(x), \tilde{A}(x)]_\sigma \neq 0$ and $[\tilde{A}(x), A(x)]_\sigma \neq 0$.

Now for $\sigma \in \{0, \gamma_H, *\}$, let us define the sets

$$M_2 = \{ \mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger : A(x) (\neq \mathbf{0}) \in \mathbb{G}_1, \tilde{A}(x) (\neq \mathbf{0}) \in \mathbb{G}_1^\dagger \\ \text{and } [A(x), \tilde{A}(x)]_\sigma = 0 \}$$

and

$$N_2 = \{ \mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger : A(x) (\neq \mathbf{0}) \in \mathbb{G}_1, \tilde{A}(x) (\neq \mathbf{0}) \in \mathbb{G}_1^\dagger \\ \text{and } [A(x), \tilde{A}(x)]_\sigma \neq 0 \}$$

Note that the set M_2 (*resp.* N_2) consists of all non-trivial isotropic elements (*resp.* non-isotropic elements) of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$. For $\sigma \in \{0, \gamma_H, *\}$, we see, by Lemma 6.3.6, that $\left(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger, [\cdot, \cdot]_\sigma \upharpoonright_{(\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger) \times (\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger)} \right)$ is a free σ -non-degenerate $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -module of rank ℓt . Here, working as in Lemma 3.18(a) of Sharma and Kaur [58], we obtain

$$|M_2| = (q^{\ell t d_1} - 1)(q^{(\ell t - 1)d_1} - 1). \quad (6.8)$$

We further note that there are $2(q^{\ell t d_1} - 1)$ trivial isotropic elements in $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$. From this and by (6.8), we get

$$|N_2| = (q^{\ell t d_1} - 1)(q^{\ell t d_1} - q^{(\ell t - 1)d_1}). \quad (6.9)$$

Now to show that σ -self-orthogonal and σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ are asymptotically good, in view of Theorem 4.4.1, we will study σ -self-orthogonal and σ -non-degenerate $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodules of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$.

Lemma 6.3.7. *Let $\mathbf{A}(x) = A(x) + \tilde{A}(x) \in \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ be such that $A(x)(\neq \mathbf{0}) \in \mathbb{G}_1$ and $\tilde{A}(x)(\neq \mathbf{0}) \in \mathbb{G}_1^\dagger$. Then the set*

$$\mathfrak{C}_{\mathbf{A}} = \left\{ \mathbf{f}(x) \odot \mathbf{A}(x) = f(x)A(x) + \tilde{f}(x)\tilde{A}(x) : \mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger \right\}$$

is a non-zero $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ generated by the element $\mathbf{A}(x)$. Further, for $\sigma \in \{0, \gamma, *\}$, the following hold.

- (a) *The submodule $\mathfrak{C}_{\mathbf{A}}$ of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is σ -self-orthogonal if and only if $\mathbf{A}(x) \in M_2$.*
- (b) *The submodule $\mathfrak{C}_{\mathbf{A}}$ of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$ is σ -non-degenerate if and only if $\mathbf{A}(x) \in N_2$.*
- (c) *We have $|\mathfrak{C}_{\mathbf{A}}| = q^{2d_1}$.*

Proof. Parts (a) and (b) are trivial, while part (c) follows from Lemma 3.5.1. $\square$

Now to study the asymptotic properties of the rates and relative Hamming distances of σ -self-orthogonal and σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, in view of Theorem 4.4.1, we will study $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$. For this, we view the set M_2 (*resp.* N_2) as a probability space, where

each sample of M_2 (*resp.* N_2) is chosen with equal probability. Now for each sample $\mathbf{A}(x) = A(x) + \tilde{A}(x) \in M_2$ (*resp.* N_2), we see, by Lemma 6.3.7, that the set

$$\mathfrak{C}_{\mathbf{A}} = \{\mathbf{f}(x) \odot \mathbf{A}(x) = f(x)A(x) + \tilde{f}(x)\tilde{A}(x) : \mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger\} \quad (6.10)$$

is a random σ -self-orthogonal (*resp.* σ -non-degenerate) $(\mathcal{F}_1 \oplus \mathcal{F}_1^\dagger)$ -submodule of $\mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$, and hence by Theorem 4.4.1, the submodule $\mathfrak{C}_{\mathbf{A}}$ is a random σ -self-orthogonal (*resp.* σ -ACD) MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, whose rate is given by

$$R(\mathfrak{C}_{\mathbf{A}}) = \frac{\dim_{\mathbb{F}_{q^t}} \mathfrak{C}_{\mathbf{A}}}{m\ell} = \frac{\log_{q^t} |\mathfrak{C}_{\mathbf{A}}|}{m\ell} = \frac{2d_1}{m\ell t} = \frac{2vp^{\alpha-\eta}}{p^{\alpha}\ell t} = \frac{2v}{p^{\eta}\ell t}.$$

Moreover, the relative Hamming distance of the random code $\mathfrak{C}_{\mathbf{A}}$ is given by $\Delta(\mathfrak{C}_{\mathbf{A}}) = \frac{wt(\mathfrak{C}_{\mathbf{A}})}{m\ell}$. In view of this, we see that the relative Hamming distance $\Delta(\mathfrak{C}_{\mathbf{A}})$ and the dimension $\dim_{\mathbb{F}_{q^t}} \mathfrak{C}_{\mathbf{A}}$ of the random code $\mathfrak{C}_{\mathbf{A}}$ are random variables over the probability spaces M_2 and N_2 with uniform probability. We now study the asymptotic behaviour of the probabilities $\Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) > \delta)$ and $\Pr(\dim_{\mathbb{F}_{q^t}} \mathfrak{C}_{\mathbf{A}} = \frac{2d_1}{t})$, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For this, let $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ be fixed, and let $I_{\mathbf{f}}$ be an ideal of $\mathcal{R}_{m,\omega}$ generated by the element $\mathbf{f}(x)$, *i.e.*,

$$\begin{aligned} I_{\mathbf{f}} &= \langle \mathbf{f}(x) \rangle_{\mathcal{R}_{m,\omega}} = \{\mathbf{f}(x) \odot \mathbf{b}(x) : \mathbf{b}(x) \in \mathcal{R}_{m,\omega}\} \\ &= \{f(x)b_1(x) + \tilde{f}(x)\tilde{b}_1(x) : b_1(x) + \tilde{b}_1(x) \in \mathbb{W}_1 \oplus \mathbb{W}_1^\dagger\} \\ &= \langle f(x) \rangle_{\mathcal{R}_{m,\omega}} \oplus \langle \tilde{f}(x) \rangle_{\mathcal{R}_{m,\omega}} = I_f \oplus I_{\tilde{f}}, \end{aligned}$$

where $I_f (\subseteq \mathbb{W}_1)$ and $I_{\tilde{f}} (\subseteq \mathbb{W}_1^\dagger)$ are ideals of $\mathcal{R}_{m,\omega}$ generated by the elements $f(x) \in \mathcal{F}_1$ and $\tilde{f}(x) \in \mathcal{F}_1^\dagger$, respectively. We further note that $I_{\mathbf{f}}^\ell = I_f^\ell \oplus I_{\tilde{f}}^\ell \subseteq \mathbb{G}_1 \oplus \mathbb{G}_1^\dagger$. Now let us define

$$(I_{\mathbf{f}}^\ell)^{\leq \delta} = \left\{ (\mathbf{u}_1(x), \mathbf{u}_2(x), \dots, \mathbf{u}_\ell(x)) \in I_{\mathbf{f}}^\ell : \widehat{wt}(\mathbf{u}_1(x), \mathbf{u}_2(x), \dots, \mathbf{u}_\ell(x)) \leq \delta \right\}.$$

Lemma 6.3.8. *For a non-zero $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$, we have*

$$|(I_{\mathbf{f}}^\ell)^{\leq \delta}| \leq \begin{cases} q^{\ell t d_1 h_{q^t}(\delta)} & \text{if either } f(x) = 0 \text{ or } \tilde{f}(x) = 0; \\ q^{2\ell t d_1 h_{q^t}(\delta)} & \text{if both } f(x) \text{ and } \tilde{f}(x) \text{ are non-zero.} \end{cases}$$

Proof. Working as in Lemma 3.5.3, the desired result follows. $\square$

Lemma 6.3.9. *Let $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ be fixed, and let $\mathbf{B}(x) = B(x) + \tilde{B}(x) \in I_{\mathbf{f}}^\ell$. We have*

$$\Pr \left(\mathbf{f}(x) \odot \mathbf{A}(x) = \mathbf{B}(x) \right) \leq \begin{cases} 1 & \text{if } f(x) = \tilde{f}(x) = 0; \\ \frac{1}{(q^{\ell t d_1} - 1)} & \text{if either } f(x) \text{ or } \tilde{f}(x) \\ & \text{is non-zero, but not both;} \\ \frac{1}{(q^{\ell t d_1} - 1)(q^{(\ell t - 1)d_1} - 1)} & \text{if both } f(x) \text{ and } \tilde{f}(x) \\ & \text{are non-zero and } \mathbf{A}(x) \\ & \text{runs over the probability} \\ & \text{space } M_2; \\ \frac{1}{(q^{\ell t d_1} - 1)(q^{\ell t d_1} - q^{(\ell t - 1)d_1})} & \text{if both } f(x) \text{ and } \tilde{f}(x) \\ & \text{are non-zero and } \mathbf{A}(x) \\ & \text{runs over the probability} \\ & \text{space } N_2. \end{cases}$$

Proof. To prove the result, let $\mathcal{S}_2$ be either M_2 or N_2 . Now let T_2 be the number of elements $\mathbf{A}(x) \in \mathcal{S}_2$ satisfying $\mathbf{f}(x) \odot \mathbf{A}(x) = \mathbf{B}(x)$. It is easy to see that $T_2 \leq 1$ if both $f(x)$ and $\tilde{f}(x)$ are non-zero. Otherwise, we observe that

$$T_2 = \begin{cases} |\mathcal{S}_2| & \text{if } \mathbf{f}(x) = 0; \\ (q^{(\ell t - 1)d_1} - 1) & \text{if either } f(x) \text{ or } \tilde{f}(x) \text{ is zero (but not both) and} \\ & \mathbf{A}(x) \text{ runs over the probability space } M_2; \\ (q^{\ell t d_1} - q^{(\ell t - 1)d_1}) & \text{if either } f(x) \text{ or } \tilde{f}(x) \text{ is zero (but not both) and} \\ & \mathbf{A}(x) \text{ runs over the probability space } N_2. \end{cases}$$

Therefore, we have $\Pr(\mathbf{f}(x) \odot \mathbf{A}(x) = \mathbf{B}(x)) = \frac{T_2}{|\mathcal{S}_2|}$. From this and by substituting

the values of $|M_2|$ and $|N_2|$ from equations (6.8) and (6.9) in the respective cases, the desired result follows. $\square$

Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For a sample $\mathbf{A}(x) \in M_2$ (*resp.* N_2), let $\mathfrak{N}_{\mathfrak{C}_{\mathbf{A}}}(\delta)$ equals the number of non-zero codewords in the random code $\mathfrak{C}_{\mathbf{A}}$ whose relative Hamming weight is at most δ . Note that

$$\mathfrak{N}_{\mathfrak{C}_{\mathbf{A}}}(\delta) = |\{\mathbf{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger : 0 < \widehat{wt}(\mathbf{f}(x) \odot \mathbf{A}(x)) \leq \delta\}|$$

is a non-negative integral random variable defined over the probability space M_2 (*resp.* N_2) with uniform probability and is called the *cumulative weight enumerator* of the random code $\mathfrak{C}_{\mathbf{A}}$. Corresponding to each $\mathbf{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ and samples $\mathbf{A}(x) \in M_2$ (*resp.* N_2), let us define the *indicator random variable* $\mathbf{Y}_{\mathbf{f}}$ as

$$\mathbf{Y}_{\mathbf{f}} = \begin{cases} 1 & \text{if } 0 < \widehat{wt}(\mathbf{f}(x) \odot \mathbf{A}(x)) \leq \delta; \\ 0 & \text{otherwise.} \end{cases}$$

Here we observe that $\mathbf{Y}_{\mathbf{f}}$ is a Bernoulli random variable defined over the probability space M_2 (*resp.* N_2). It is easy to see that $\mathbf{Y}_{\mathbf{0}} = 0$ and

$$\mathfrak{N}_{\mathfrak{C}_{\mathbf{A}}}(\delta) = \sum_{\mathbf{f}(x) (\neq 0) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} \mathbf{Y}_{\mathbf{f}}.$$

For a non-zero $\mathbf{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$, let $E(\mathbf{Y}_{\mathbf{f}})$ be the expectation of the corresponding indicator random variable $\mathbf{Y}_{\mathbf{f}}$.

Lemma 6.3.10. *For a given non-zero $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$, we have*

$$E(\mathbf{Y}_{\mathbf{f}}) \leq \begin{cases} \frac{q^{-\ell t d_1(1-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})} & \text{if either } f(x) \text{ or } \tilde{f}(x) \text{ is non-zero, but} \\ & \text{not both;} \\ \frac{q^{-2\ell t d_1(1-\frac{1}{2\ell t}-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})(1-q^{-(\ell t-1)d_1})} & \text{if both } f(x) \text{ and } \tilde{f}(x) \text{ are non-zero and} \\ & \mathbf{A}(x) \text{ runs over the probability space } M_2; \\ \frac{q^{-2\ell t d_1(1-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})(1-q^{-d_1})} & \text{if both } f(x) \text{ and } \tilde{f}(x) \text{ are non-zero and} \\ & \mathbf{A}(x) \text{ runs over the probability space } N_2. \end{cases}$$

Proof. Working as in Lemma 6.3.4 and applying Lemmas 6.3.8 and 6.3.9, the desired result follows. $\square$

Lemma 6.3.11. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For $\mathbf{A}(x) \in M_2$ (resp. N_2), let $\mathfrak{C}_{\mathbf{A}}$ be the corresponding σ -self-orthogonal (resp. σ -ACD) MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by (6.10). We have*

$$\Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) \leq \delta) \leq \begin{cases} \frac{2q^{-\ell t d_1(1-\frac{1}{\ell t}-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})} + \frac{q^{-2\ell t d_1(1-\frac{3}{2\ell t}-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})(1-q^{-(\ell t-1)d_1})} & \text{if } \mathbf{A}(x) \in M_2; \\ \frac{2q^{-\ell t d_1(1-\frac{1}{\ell t}-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})} + \frac{q^{-2\ell t d_1(1-\frac{1}{\ell t}-h_{q^t}(\delta))}}{(1-q^{-\ell t d_1})(1-q^{-d_1})} & \text{if } \mathbf{A}(x) \in N_2. \end{cases}$$

Proof. Let us define $\mathbf{Y} = \sum_{\mathbf{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} \mathbf{Y}_{\mathbf{f}}$. Since $\mathbf{Y}_0 = 0$, we note that

$$\mathbf{Y} = \sum_{\mathbf{f}(x) (\neq 0) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} \mathbf{Y}_{\mathbf{f}} = \mathfrak{N}_{\mathfrak{C}_{\mathbf{A}}}(\delta)$$

equals the number of non-zero elements $\mathbf{f}(x) = f(x) + \tilde{f}(x) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger$ such that the corresponding codeword $\mathbf{f}(x) \odot \mathbf{A}(x) \in \mathfrak{C}_{\mathbf{A}}$ has relative Hamming weight at most δ . This implies that $\Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) \leq \delta) = \Pr(\mathbf{Y} > 0)$. By Theorem 2.3.2, we get $\Pr(\mathbf{Y} > 0) \leq E(\mathbf{Y})$. Further, by Theorem 2.3.1, we get

$$\Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) \leq \delta) = \Pr(\mathbf{Y} > 0) \leq E(\mathbf{Y}) = E\left(\sum_{\mathbf{f}(x) (\neq 0) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} \mathbf{Y}_{\mathbf{f}}\right) = \sum_{\mathbf{f}(x) (\neq 0) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} E(\mathbf{Y}_{\mathbf{f}}).$$

Now if $\mathbf{A}(x) \in M_2$, we see, by Lemma 6.3.10, that

$$\begin{aligned} \Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) \leq \delta) &\leq \sum_{\mathbf{f}(x) (\neq 0) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} E(\mathbf{Y}_{\mathbf{f}}) \\ &= \sum_{\substack{\text{either } f(x) \text{ or } \tilde{f}(x) \\ \text{is zero, but not both}}} E(\mathbf{Y}_{\mathbf{f}}) + \sum_{\substack{\text{both } f(x) \text{ and } \tilde{f}(x) \\ \text{are non-zero}}} E(\mathbf{Y}_{\mathbf{f}}) \end{aligned}$$

$$\begin{aligned}
 &\leq \sum_{\substack{\text{either } f(x) \text{ or } \tilde{f}(x) \\ \text{is zero, but not both}}} \frac{q^{-\ell t d_1 (1 - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})} \\
 &+ \sum_{\substack{\text{both } f(x) \text{ and } \tilde{f}(x) \\ \text{are non-zero}}} \frac{q^{-2\ell t d_1 (1 - \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})(1 - q^{-(\ell t - 1)d_1})} \\
 &= \frac{2(q^{d_1} - 1)q^{-\ell t d_1 (1 - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})} + \frac{(q^{d_1} - 1)^2 q^{-2\ell t d_1 (1 - \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})(1 - q^{-(\ell t - 1)d_1})} \\
 &\leq \frac{2q^{d_1} q^{-\ell t d_1 (1 - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})} + \frac{q^{2d_1} q^{-2\ell t d_1 (1 - \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})(1 - q^{-(\ell t - 1)d_1})} \\
 &= \frac{2q^{-\ell t d_1 (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})} + \frac{q^{-2\ell t d_1 (1 - \frac{3}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})(1 - q^{-(\ell t - 1)d_1})}.
 \end{aligned}$$

On the other hand, when $\mathbf{A}(x) \in N_2$, working as above and by applying Lemma [6.3.10](#), we obtain

$$\Pr(\Delta(\mathfrak{C}_{\mathbf{A}}) \leq \delta) \leq \sum_{\mathbf{f}(x) (\neq \mathbf{0}) \in \mathcal{F}_1 \oplus \mathcal{F}_1^\dagger} E(\mathbf{Y}_{\mathbf{f}}) \leq \frac{2q^{-\ell t d_1 (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})} + \frac{q^{-2\ell t d_1 (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t d_1})(1 - q^{-d_1})}.$$

This proves the lemma. □

Next, let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for all $j \geq 1$. Here we note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. For each j , let ξ_j be a primitive $(\mathbf{m}_j e)$ -th root of unity in some extension field of $\mathbb{F}_q$ satisfying $\xi_j^{\mathbf{m}_j} = \omega$, and let $h_1^{(j)}(x)$ be the minimal polynomial of ξ_j over $\mathbb{F}_q$. Since $-1 \notin Q$ and $\omega = \omega^{-1}$, we see, by Lemma [6.3.1\(b\)](#), that $h_1^{(j)}(x) \neq h_1^{(j)\dagger}(x)$ and that both $h_1^{(j)}(x)$ and $h_1^{(j)\dagger}(x)$ are factors of the polynomial $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$ for all j . That is, both $h_1^{(j)}(x)$ and $h_1^{(j)\dagger}(x)$ form a reciprocal pair. Next, for each $j \geq 1$, let us recall

$$\mathcal{F}_1^{(j)} = \frac{\mathbb{F}_q[x]}{\langle h_1^{(j)}(x) \rangle}, \quad \mathcal{F}_1^{(j)\dagger} = \frac{\mathbb{F}_q[x]}{\langle h_1^{(j)\dagger}(x) \rangle}, \quad \mathbb{G}_1^{(j)} = \left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)}(x) \rangle} \right)^\ell \text{ and } \mathbb{G}_1^{(j)\dagger} = \left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_1^{(j)\dagger}(x) \rangle} \right)^\ell.$$

Further, let us define the sets

$$M_2^{(j)} = \left\{ \mathbf{A}^{(j)}(x) = A^{(j)}(x) + \tilde{A}^{(j)}(x) \in \mathbb{G}_1^{(j)} \oplus \mathbb{G}_1^{(j)\dagger} : A^{(j)}(x) (\neq \mathbf{0}) \in \mathbb{G}_1^{(j)}, \right.$$

$$\tilde{A}^{(j)}(x)(\neq \mathbf{0}) \in \mathbb{G}_1^{(j)\dagger} \text{ and } [A^{(j)}(x), \tilde{A}^{(j)}(x)]_\sigma = 0 \Big\}$$

and

$$N_2^{(j)} = \left\{ \mathbf{A}^{(j)}(x) = A^{(j)}(x) + \tilde{A}^{(j)}(x) \in \mathbb{G}_1^{(j)} \oplus \mathbb{G}_1^{(j)\dagger} : A^{(j)}(x)(\neq \mathbf{0}) \in \mathbb{G}_1^{(j)}, \right. \\ \left. \tilde{A}^{(j)}(x)(\neq \mathbf{0}) \in \mathbb{G}_1^{(j)\dagger} \text{ and } [A^{(j)}(x), \tilde{A}^{(j)}(x)]_\sigma \neq 0 \right\}.$$

Note that $M_2^{(j)}$ is the set of all non-trivial isotropic elements of $\mathbb{G}_1^{(j)} \oplus \mathbb{G}_1^{(j)\dagger}$, while the set $N_2^{(j)}$ consists of all non-isotropic elements of $\mathbb{G}_1^{(j)} \oplus \mathbb{G}_1^{(j)\dagger}$. For each $j \geq 1$, we shall view the set $M_2^{(j)}$ (*resp.* $N_2^{(j)}$) as a probability space, where each sample is chosen with equal probability. Further, for each j and each sample $\mathbf{A}^{(j)}(x) = A^{(j)}(x) + \tilde{A}^{(j)}(x) \in M_2^{(j)}$ (*resp.* $N_2^{(j)}$), let

$$\mathfrak{C}_{\mathbf{A}^{(j)}} = \{\mathbf{f}^{(j)}(x) \odot \mathbf{A}^{(j)}(x) : \mathbf{f}^{(j)}(x) \in \mathcal{F}_1^{(j)} \oplus \mathcal{F}_1^{(j)\dagger}\} \subseteq \mathbb{G}_1^{(j)} \oplus \mathbb{G}_1^{(j)\dagger} \quad (6.11)$$

be a random σ -self-orthogonal (*resp.* σ -ACD) MT additive code of length $\mathbf{m}_j \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ defined over the probability space $M_2^{(j)}$ (*resp.* $N_2^{(j)}$) for each $\sigma \in \{0, \gamma_{\mathbf{H}}, *\}$ (and hence for each $\sigma \in \{0, \gamma, *\}$).

Theorem 6.3.4. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. If δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) > \delta \right) \right\} = 1.$$

Proof. Since $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, we have $\frac{1}{2} - \frac{1}{2\ell t} - h_{q^t}(\delta) > 0$. Further, as $t \geq 2$, we see that $\frac{1}{\ell t} \leq \frac{1}{2}$, which implies that $1 - \frac{1}{\ell t} - h_{q^t}(\delta) > 0$ and $1 - \frac{3}{2\ell t} - h_{q^t}(\delta) > 0$. Now if $\mathbf{A}^{(j)}(x) \in M_2^{(j)}$, then we see, by Lemma 6.3.11, that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} \leq 2 \lim_{j \rightarrow \infty} \left\{ \frac{q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t v p^{\alpha_j - \eta}})} \right\} \\ + \lim_{j \rightarrow \infty} \left\{ \frac{q^{-2\ell t v p^{\alpha_j - \eta} (1 - \frac{3}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t v p^{\alpha_j - \eta}})(1 - q^{-(\ell t - 1) v p^{\alpha_j - \eta}})} \right\}.$$

On the other hand, when $\mathbf{A}^{(j)}(x) \in N_2^{(j)}$, we see, by Lemma 6.3.11 again, that

$$\begin{aligned} \lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} &\leq 2 \lim_{j \rightarrow \infty} \left\{ \frac{q^{-\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t v p^{\alpha_j - \eta}})} \right\} \\ &\quad + \lim_{j \rightarrow \infty} \left\{ \frac{q^{-2\ell t v p^{\alpha_j - \eta} (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{(1 - q^{-\ell t v p^{\alpha_j - \eta}})(1 - q^{-v p^{\alpha_j - \eta}})} \right\}. \end{aligned}$$

Now since $\lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, we note that $\lim_{j \rightarrow \infty} \{v p^{\alpha_j - \eta}\} = \infty$, which implies that $\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} = 0$. From this, it follows that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) > \delta \right) \right\} = 1 - \lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathfrak{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} = 1.$$

□

Theorem 6.3.5. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers such that $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let $\sigma \in \{0, \gamma, *\}$. For $\mathbf{A}^{(j)}(x) \in M_2^{(j)}$ (resp. $N_2^{(j)}$), let $\mathfrak{C}_{\mathbf{A}^{(j)}}$ be a random σ -self-orthogonal (resp. σ -ACD) MT additive code of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ as defined by (6.11). We have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\dim_{\mathbb{F}_{q^t}} \mathfrak{C}_{\mathbf{A}^{(j)}} = \frac{2d_1^{(j)}}{t} = \frac{2v p^{\alpha_j - \eta}}{t} \right) \right\} = 1.$$

Proof. Working in a similar manner as in Theorem 3.5.2, the desired result follows. □

In the following theorem, we consider the case $-1 \notin Q$ and $\omega = \omega^{-1}$, and we show that there exist infinite sequences of σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ with rate $\frac{2v}{p^n \ell t}$ and relative Hamming distance at least δ for $\sigma \in \{0, \gamma_{\mathbf{H}}, *\}$ (and hence for $\sigma \in \{0, \gamma, *\}$), where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$.

Theorem 6.3.6. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. Suppose that $-1 \notin Q$ and $\omega = \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, there exist infinite sequences $\mathfrak{F} = \{\mathfrak{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathfrak{D}_j\}_{j \geq 1}$ of σ -self-orthogonal MT additive codes $\mathfrak{C}_j$'s and σ -ACD*

MT additive codes $\mathfrak{D}_j$'s of length $\mathfrak{m}_j \ell = p^{\alpha_j} \ell$, block length $\mathfrak{m}_j = p^{\alpha_j}$ and dimension $\frac{2vp^{\alpha_j-\eta}}{t}$ over $\mathbb{F}_{q^t}$ respectively, such that $\lim_{j \rightarrow \infty} \{\mathfrak{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$,

$$(i) \ R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{2v}{p^{\eta} \ell t},$$

$$(ii) \ \Delta_{\mathfrak{F}} > \delta \text{ and } \Delta_{\mathfrak{G}} > \delta.$$

Proof. It follows immediately from Theorems [6.3.4](#) and [6.3.5](#). $\square$

As a consequence of Theorem [6.3.6](#), we see that σ -self-orthogonal and σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ are asymptotically good for each $\sigma \in \{0, \gamma, *\}$. Furthermore, in the following corollary, we deduce that σ -self-orthogonal and σ -ACD ω -constacyclic additive codes over $\mathbb{F}_{q^t}$ are asymptotically good when $\omega = \omega^{-1}$ and $-1 \notin Q$.

Corollary 6.3.2. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2t}$. Suppose that $-1 \notin Q$ and $\omega = \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, there exist infinite sequences $\mathfrak{F} = \{\mathfrak{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathfrak{D}_j\}_{j \geq 1}$ of σ -self-orthogonal ω -constacyclic additive codes $\mathfrak{C}_j$'s and σ -ACD ω -constacyclic additive codes $\mathfrak{D}_j$'s of length $\mathfrak{m}_j = p^{\alpha_j}$ and dimension $\frac{2vp^{\alpha_j-\eta}}{t}$ over $\mathbb{F}_{q^t}$ respectively, such that $\lim_{j \rightarrow \infty} \{\mathfrak{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{2v}{p^{\eta} t}$, $\Delta_{\mathfrak{F}} > \delta$ and $\Delta_{\mathfrak{G}} > \delta$.*

Proof. It follows immediately by taking $\ell = 1$ in Theorem [6.3.6](#). $\square$

Remark 6.3.2. *Taking $\omega = 1$ in the above corollary, we see that σ -self-orthogonal and σ -ACD cyclic additive codes over finite fields are asymptotically good.*

Example 6.3.2. Let $q = 17$, $p = 19$, $\omega = 1$, $\ell = 1$ and $t = 2$. Here we have $v = \text{ord}_p(q) = \text{ord}_{19}(17) = 9$, $\eta = 1$, $e = \text{ord}(\omega) = 1$, and $Q = \langle 17 \rangle = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$. Note that $-1 = 18 \notin Q$ in this case. By Corollary [6.3.2](#), we see that there exist infinite sequences $\mathfrak{F} = \{\mathfrak{C}_j\}_{j \geq 1}$ and $\mathfrak{G} = \{\mathfrak{D}_j\}_{j \geq 1}$ of σ -self-orthogonal cyclic additive codes $\mathfrak{C}_j$'s and σ -ACD cyclic additive codes $\mathfrak{D}_j$'s of length 19^{α_j} over $\mathbb{F}_{17^2}$ respectively, such that $\lim_{j \rightarrow \infty} \{19^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = R_{\mathfrak{G}} = \frac{2v}{p^{\eta} t} = \frac{9}{19}$, $\Delta_{\mathfrak{F}} > \delta$ and $\Delta_{\mathfrak{G}} > \delta$, where δ is a positive real number satisfying $\delta < 0.170$.

6.3.3 The case $-1 \notin Q$ and $\omega \neq \omega^{-1}$

Throughout this section, let us suppose that $-1 \notin Q$ and $\omega \neq \omega^{-1}$. Here by 6.3.1(b), we see that $h_1(x) \neq h_1^\dagger(x)$ and that $h_1^\dagger(x)$ does not divide $x^m - \omega$ in $\mathbb{F}_q[x]$. Further, we see, by Theorem 4.4.1(a), that there does not exist any non-zero σ -self-orthogonal $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ for each $\sigma \in \{0, \gamma, *\}$. In this case, we will show that σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ are asymptotically good. For this, we will study σ -non-degenerate $\mathcal{F}_1$ -subspaces of $\mathbb{G}_1$. Let us define the set

$$N_3 = \mathbb{G}_1 \setminus \{0\}.$$

It is easy to see that

$$|N_3| = q^{\ell t d_1} - 1.$$

Here we first make the following observation.

Lemma 6.3.12. *Let $A(x) \in N_3$ be fixed. For $\sigma \in \{0, \gamma, *\}$, the set*

$$\mathcal{C}_A = \{f(x)A(x) : f(x) \in \mathcal{F}_1\}$$

is a σ -non-degenerate $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ with $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \frac{d_1}{t}$.

Proof. One can easily see that the set $\mathcal{C}_A$ is a σ -non-degenerate $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$. Further, by applying Lemma 3.5.1, we obtain $\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \frac{d_1}{t}$. $\square$

Now to study the asymptotic properties of the rates and relative Hamming distances of σ -ACD MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, by Theorem 4.4.1(c), we view the set N_3 as a probability space, where each sample of N_3 is chosen with equal probability. Now for each sample $A(x) = (A_1(x), A_2(x), \dots, A_\ell(x)) \in N_3$, by Lemma 6.3.12, we see that the set

$$\mathcal{C}_A = \{f(x)A(x) = (f(x)A_1(x), f(x)A_2(x), \dots, f(x)A_\ell(x)) : f(x) \in \mathcal{F}_1\} \quad (6.12)$$

is a random σ -non-degenerate $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$, and hence by Theorem 4.4.1(c), the subspace $\mathcal{C}_A$ is a random σ -ACD MT additive code of length $m\ell$ and block

length m over $\mathbb{F}_{q^t}$, whose rate is given by

$$R(\mathcal{C}_A) = \frac{\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A}{m\ell} = \frac{\log_{q^t} |\mathcal{C}_A|}{m\ell} = \frac{d_1}{m\ell t} = \frac{vp^{\alpha-\eta}}{p^\alpha \ell t} = \frac{v}{p^\alpha \ell t}.$$

Recall that the relative Hamming distance of the random code $\mathcal{C}_A$ is given by $\Delta(\mathcal{C}_A) = \frac{wt(\mathcal{C}_A)}{m\ell}$. In view of this, we see that the relative Hamming distance $\Delta(\mathcal{C}_A)$ and the dimension $\dim_{\mathbb{F}_{q^t}}(\mathcal{C}_A)$ of the random code $\mathcal{C}_A$ are random variables over the probability space N_3 with uniform probability. We now study the asymptotic behavior of the probabilities $\Pr(\Delta(\mathcal{C}_A) > \delta)$ and $\Pr(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_A = \frac{d_1}{t})$, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. Following the same notations and working as in Section [6.3.1](#), we observe the following:

Lemma 6.3.13. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For $A(x) \in N_3$, let $\mathcal{C}_A$ be the corresponding σ -ACD MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by [\(6.12\)](#). We have*

$$\Pr(\Delta(\mathcal{C}_A) \leq \delta) \leq \frac{q^{-\ell t d_1 (1 - \frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-\ell t d_1}}.$$

Proof. Working as in Lemma [6.3.5](#), the desired result follows. $\square$

Next, let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for all $j \geq 1$. Here we note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. Since $-1 \notin Q$ and $\omega \neq \omega^{-1}$, we see, by Lemma [6.2.1\(b\)](#), that $h_1^{(j)}(x) \neq h_1^{(j)\dagger}(x)$ and that $h_1^{(j)\dagger}(x)$ does not divide $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$. Further, let us define the set

$$N_3^{(j)} = \mathbb{G}_1^{(j)} \setminus \{\mathbf{0}\}.$$

Here we shall view the set $N_3^{(j)}$ as a probability space, where each sample is chosen with equal probability. For each $j \geq 1$, and each sample $A^{(j)}(x) = (A_1^{(j)}(x), A_2^{(j)}(x), \dots, A_\ell^{(j)}(x)) \in N_3^{(j)}$, let

$$\mathcal{C}_{A^{(j)}} = \left\{ f^{(j)}(x)A^{(j)}(x) = \left(f^{(j)}(x)A_1^{(j)}(x), \dots, f^{(j)}(x)A_\ell^{(j)}(x) \right) : f^{(j)}(x) \in \mathcal{F}_1^{(j)} \right\} \quad (6.13)$$

be a random σ -ACD MT additive code of length $\mathbf{m}_j \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ defined over the probability space $N_3^{(j)}$ for each $\sigma \in \{0, \gamma, *\}$.

Theorem 6.3.7. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$. If δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta \left(\mathcal{C}_{A^{(j)}} \right) > \delta \right) \right\} = 1.$$

Proof. Working as in Theorem 6.3.1 and by applying Lemma 6.3.13, the desired result follows. $\square$

Theorem 6.3.8. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Suppose that $-1 \notin Q$ and $\omega \neq \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, let $\mathcal{C}_{A^{(j)}}$ be a random σ -ACD MT additive code of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{q^t}$ as defined by (6.13). We have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\dim_{\mathbb{F}_{q^t}} \mathcal{C}_{A^{(j)}} = \frac{d_1^{(j)}}{t} = \frac{vp^{\alpha_j - \eta}}{t} \right) \right\} = 1.$$

Proof. Working as in Theorem 3.5.2, the desired result follows. $\square$

In the following theorem, for $\sigma \in \{0, \gamma, *\}$, we show that there exists an infinite sequence of σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ having rate $\frac{v}{p^{\eta} \ell t}$ and relative Hamming distance at least δ , where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. From this, it follows that σ -ACD MT additive codes over $\mathbb{F}_{q^t}$ are asymptotically good.

Theorem 6.3.9. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$. For $\sigma \in \{0, \gamma, *\}$, there exists an infinite sequence $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -ACD MT additive codes $\mathcal{D}_j$'s of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$, block length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$, such that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$,*

$$(i) \ R_{\mathfrak{G}} = \frac{v}{p^{\eta} \ell t} \text{ and}$$

$$(ii) \ \Delta_{\mathfrak{G}} > \delta.$$

Proof. It follows immediately from Theorems 6.3.7 and 6.3.8. $\square$

As a consequence of Theorem [6.3.9](#), we deduce, in the following corollary, that σ -ACD ω -constacyclic additive codes over finite fields are asymptotically good when $-1 \notin Q$ and $\omega \neq \omega^{-1}$.

Corollary 6.3.3. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2t}$. Suppose that $\omega \neq \omega^{-1}$. For $\sigma \in \{0, \gamma, *\}$, there exists an infinite sequence $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -ACD ω -constacyclic additive codes $\mathcal{D}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ and dimension $\frac{vp^{\alpha_j - \eta}}{t}$ over $\mathbb{F}_{q^t}$ such that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, $R_{\mathfrak{G}} = \frac{v}{p^{\eta}t}$ and $\Delta_{\mathfrak{G}} > \delta$.*

Proof. On taking $\ell = 1$ in Theorem [6.3.9](#), we get the desired result. $\square$

Example 6.3.3. Let $q = 7$, $p = 13$, $\omega = 2$ and $\ell = t = 2$. Here we have $v = \text{ord}_p(q) = \text{ord}_{13}(7) = 12$, $\eta = 1$, $e = \text{ord}(\omega) = 3$, and $Q = \langle 7 \rangle = \{1, 4, 7, 10, 16, 19, 22, 25, 28, 31, 34, 37\}$. Note that $-1 = 38 \notin Q$ and $\omega \neq \omega^{-1}$ in this case. By Theorem [6.3.9](#), we see that there exists an infinite sequence $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of σ -ACD MT additive codes $\mathcal{D}_j$'s of length $2 \cdot (13)^{\alpha_j}$ and block lengths 13^{α_j} over $\mathbb{F}_{7^2}$ respectively, such that $\lim_{j \rightarrow \infty} \{13^{\alpha_j}\} = \infty$, $R_{\mathfrak{G}} = \frac{v}{2p^{\eta}t} = \frac{3}{13}$ and $\Delta_{\mathfrak{G}} > \delta$, where δ is a positive real number satisfying $\delta < 0.236$.

In the next chapter, we will show that σ -self-dual MT additive codes over finite fields are asymptotically good for each $\sigma \in \{0, \gamma, *\}$ by applying probabilistic methods and results from groups and geometry. We will also study a special class of 0-self-dual MT additive codes over $\mathbb{F}_{q^t}$, viz. doubly-even self-dual MT additive codes and characterize a special class of these codes in terms of their constituents, where q is an even prime power. Further, by applying the probabilistic methods and results from groups and geometry, we will show that the doubly-even 0-self-dual MT additive codes over $\mathbb{F}_{2^t}$ are also asymptotically good.

7

Self-dual multi-twisted additive codes are asymptotically good

7.1 Introduction

In this chapter, we study self-dual MT additive codes over finite fields with respect to ordinary, Hermitian and $*$ trace bilinear forms. We will apply probabilistic methods and results from groups and geometry to study the asymptotic behaviour of their relative Hamming distances. Further, we show that there exist asymptotically good infinite sequences of self-dual MT additive codes over finite fields with respect to the aforementioned trace bilinear forms. This shows that self-dual MT additive codes over finite fields are asymptotically good. In addition, we define and study a special class of self-dual MT additive codes over $\mathbb{F}_{q^t}$ with respect to the ordinary trace bilinear form, *viz.* doubly-even self-dual MT additive codes and characterize a special class of these codes in terms of their constituents with the help of their trace

description, where q is an even prime power. With the help of this characterization and using probabilistic methods and results from groups and geometry, we further study the asymptotic behaviour of their relative Hamming distances and show that doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ are also asymptotically good.

This chapter is structured as follows: In Section [7.2](#), we consider three special classes of self-dual MT additive codes over finite fields with respect to ordinary, Hermitian and $*$ trace bilinear forms and study the asymptotic behaviour of their relative Hamming distances using probabilistic methods and results from groups and geometry (Theorem [7.2.2](#)). We further establish the existence of asymptotically good infinite sequences of self-dual MT additive codes over finite fields with respect to the above-mentioned trace bilinear forms (Theorem [7.2.3](#)). As a consequence, we deduce that self-dual cyclic and negacyclic additive codes over finite fields are asymptotically good (Corollary [7.2.1](#)). In Section [7.3](#), we define and study a special class of self-dual MT additive codes over finite fields of even characteristic with respect to the ordinary trace bilinear form, *viz.* doubly-even self-dual MT additive codes and provide a characterization of a special class of these codes in terms of their constituents with the help of their trace description (Theorem [7.3.1](#)). In Section [7.4](#), we derive a necessary and sufficient condition for the existence of a doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ (Theorem [7.4.1](#)). Finally, we consider a special class of doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ on which our probabilistic methods work well and show that there exists an asymptotically good infinite sequence of doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ (Theorem [7.4.4](#)). As a consequence, we deduce that doubly-even self-dual cyclic additive codes over $\mathbb{F}_{2^t}$ are asymptotically good (Corollary [7.4.1](#)).

7.2 Asymptotically good σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ exist

In this section, we consider a special class of σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ and show that it is asymptotically good by applying probabilistic methods and results from groups and geometry stated in Chapter [2](#). Towards this, we first make the following observation.

Lemma 7.2.1. *For each odd prime p , there are infinitely many prime powers q such that $\text{ord}_p(q)$ is an even integer. Furthermore, if q is an odd power of 2, then there are several odd primes p such that $\text{ord}_p(q)$ is an even integer.*

Proof. To prove the first part, let p be an odd prime, and let g be an odd primitive root modulo p , (such a primitive root g always exists). For any integer k , we see that the integer $g + kp$ is also a primitive root modulo p . Now consider the following arithmetic progression (A.P.):

$$\dots\dots\dots, g - 2p, g - p, g, g + p, g + 2p, \dots\dots\dots$$

Since $\gcd(g, p) = 1$, we see, by Dirichlet's Theorem on primes in A.P. [63, Th. 1.2.7], that there are infinitely many primes $\mathfrak{P}$ such that $\mathfrak{P} \equiv g \pmod{p}$, i.e., $\mathfrak{P}$ is a primitive root modulo p . Now let us take $q = \mathfrak{P}^\theta$, where θ is an odd positive integer. Here we observe that

$$\text{ord}_p(q) = \text{ord}_p(\mathfrak{P}^\theta) = \frac{\text{ord}_p(\mathfrak{P})}{\gcd(\theta, \text{ord}_p(\mathfrak{P}))} = \frac{p-1}{\gcd(\theta, p-1)},$$

which is an even integer.

On the other hand, if q is an odd power of 2, i.e., $q = 2^\theta$ with θ an odd positive integer, we choose an odd prime p such that 2 is a primitive root modulo p , i.e., $\text{ord}_p(2) = p-1$. Note that there are several such odd primes p (see OEIS Entry A001122 [49]). In this case, we see that

$$\text{ord}_p(q) = \text{ord}_p(2^\theta) = \frac{\text{ord}_p(2)}{\gcd(\theta, \text{ord}_p(2))} = \frac{p-1}{\gcd(\theta, p-1)},$$

which is an even integer. This proves the lemma. $\square$

By Lemma 7.2.1, we see that there are infinitely many pairs (p, q) of odd primes p and prime powers q such that $\gcd(p, q) = 1$ and $\text{ord}_p(q)$ is an even integer.

By Theorem 5.3.1, we see, for $\sigma \in \{0, \gamma, *\}$, that if there exists a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, then all the irreducible factors of the polynomials $x^{m_1} - \omega_1, x^{m_2} - \omega_2, \dots, x^{m_\ell} - \omega_\ell$ over $\mathbb{F}_q$ are either self-reciprocal or they form reciprocal pairs. From this, we deduce the following:

Lemma 7.2.2. *For $\sigma \in \{0, \gamma, *\}$, if there exists a σ -self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, then $\omega_i = \omega_i^{-1}$ for $1 \leq i \leq \ell$.*

From this point on, throughout this chapter, we assume that $\omega_i = \omega_i^{-1}$ for $1 \leq i \leq \ell$. Now to show that σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ are asymptotically good, let us assume, throughout this section, that m is a positive integer coprime to q , and ω is a non-zero element of $\mathbb{F}_q$ with $\text{ord}(\omega) = e$. Further, from now on, let us suppose that $m_1 = m_2 = \dots = m_\ell = m$ and $\omega_1 = \omega_2 = \dots = \omega_\ell = \omega$, so that $n = m\ell$ and $M = me$. Therefore we have $\epsilon_{\nu,i} = 1$ for $1 \leq \nu \leq s$ and $1 \leq i \leq \ell$. In view of this, we see that $x^m - \omega = h_1(x)h_2(x) \cdots h_s(x)$ and $x^m - \omega^{-1} = h_1^\dagger(x)h_2^\dagger(x) \cdots h_s^\dagger(x)$ are the irreducible factorizations of the polynomials $x^m - \omega$ and $x^m - \omega^{-1}$ over $\mathbb{F}_q$, respectively. Now let ξ be a fixed primitive (me) -th root of unity in an extension field of $\mathbb{F}_q$ satisfying $\xi^m = \omega$.

From this point on, let us fix an odd prime p and a prime power q such that $\gcd(p, q) = 1$ and $v = \text{ord}_p(q)$ is an even integer, (there are infinitely many such pairs (p, q) by Lemma 7.2.1). Let us take $m = p^\alpha$, where $\alpha \geq 1$ is an integer. We also assume, in view of Lemma 7.2.2, that the element $\omega \in \mathbb{F}_q$ satisfies $\omega = \omega^{-1}$. We shall refer to an Ω -MT additive code of length $n = m\ell$ and block lengths $(\underbrace{m, m, \dots, m}_{\ell \text{ times}})$ over $\mathbb{F}_{q^t}$ simply as an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, where $\Omega = (\underbrace{\omega, \omega, \dots, \omega}_{\ell \text{ times}})$ with $\omega = \omega^{-1}$.

Since $\omega = \omega^{-1}$, we see that $\omega \in \{1, -1\}$, which implies that $e = \text{ord}(\omega) \in \{1, 2\}$. Now as $x + 1$ is a factor of $x^m + 1$ and $x - 1$ is a factor of $x^m - 1$ over $\mathbb{F}_q$, we assume that $h_1(x)$ is either $x + 1$ or $x - 1$ according as ω is either -1 or 1 . Recall that the minimal polynomial of ξ over $\mathbb{F}_q$ is a factor of $x^m - \omega$. Without any loss of generality, let $h_2(x)$ be the minimal polynomial of ξ over $\mathbb{F}_q$. Note that $d_2 = \deg h_2(x) = \deg h_2^\dagger(x) = \text{ord}_{me}(q)$. As $v = \text{ord}_p(q)$, we can write $q^v = 1 + p^\eta c$, where $\eta \geq 1$ and c are integers such that $p \nmid c$. From (3.2), one can easily observe that

$$d_2 = \text{ord}_{me}(q) = \text{ord}_m(q) = \text{ord}_{p^\alpha}(q) = \begin{cases} v & \text{if } \alpha \leq \eta; \\ vp^{\alpha-\eta} & \text{if } \alpha \geq \eta + 1. \end{cases} \quad (7.1)$$

Since $v = \text{ord}_p(q)$ is even, we note, by (7.1), that the integer d_2 is even and $q^{d_2} \equiv$

1 (mod m). This implies that $q^{\frac{d_2}{2}} \equiv -1 \pmod{m}$, as $m = p^\alpha$ is a power of the odd prime p . Since $e \in \{1, 2\}$, we see that $q^{\frac{d_2}{2}} \equiv -1 \pmod{me}$. From this, we observe that all the irreducible factors $h_1(x), h_2(x), \dots, h_s(x)$ of $x^m - \omega$ over $\mathbb{F}_q$ are self-reciprocal. This implies that $\mathcal{F}_\nu = \mathcal{F}_\nu^\dagger$, $\mathbb{G}_\nu = \mathbb{G}_\nu^\dagger$ and $\dim_{\mathcal{F}_\nu} \mathbb{G}_\nu = \ell t$ for $1 \leq \nu \leq s$. We recall that $h_1(x)$ is either $x + 1$ or $x - 1$ according as ω is either -1 or 1 . One can easily see that the integer $d_\nu = \deg h_\nu(x)$ is even for $2 \leq \nu \leq s$.

In view of Theorem [5.3.1](#), we assume, throughout this section, that ℓt is an even integer. In the case when q is odd and $\sigma \in \{0, *\}$, we also assume that either ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$. We also assume that ω is either 1 or -1 . These assumptions are necessary and sufficient for the existence of a σ -self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Now let $1 \leq \nu \leq s$ be fixed. From now on, we will represent each element $\mathbf{f}_\nu(x) \in \mathcal{F}_\nu^{\frac{\ell t}{2}}$ as $\mathbf{f}_\nu(x) = (f_\nu^{(1)}(x), f_\nu^{(2)}(x), \dots, f_\nu^{(\frac{\ell t}{2})}(x))$ and each element $\mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}}$ as $\mathbf{A}_\nu(x) = (A_\nu^{(1)}(x), A_\nu^{(2)}(x), \dots, A_\nu^{(\frac{\ell t}{2})}(x))$, where $f_\nu^{(h)}(x) \in \mathcal{F}_\nu$ and $A_\nu^{(h)}(x) \in \mathbb{G}_\nu$ for $1 \leq h \leq \frac{\ell t}{2}$. For $\mathbf{f}_\nu(x) \in \mathcal{F}_\nu^{\frac{\ell t}{2}}$ and $\mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}}$, let us define

$$\mathbf{f}_\nu(x) \odot \mathbf{A}_\nu(x) = f_\nu^{(1)}(x)A_\nu^{(1)}(x) + f_\nu^{(2)}(x)A_\nu^{(2)}(x) + \dots + f_\nu^{(\frac{\ell t}{2})}(x)A_\nu^{(\frac{\ell t}{2})}(x) \in \mathbb{G}_\nu.$$

Further, for a fixed $\mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}}$, let us define

$$\mathcal{C}_{\mathbf{A}_\nu} = \left\{ \mathbf{f}_\nu(x) \odot \mathbf{A}_\nu(x) : \mathbf{f}_\nu(x) \in \mathcal{F}_\nu^{\frac{\ell t}{2}} \right\}.$$

It is easy to observe that the set $\mathcal{C}_{\mathbf{A}_\nu}$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ with the ordered basis $\mathbf{A}_\nu(x)$. Now let us define the set

$$T_\nu = \left\{ \mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}} : \mathcal{C}_{\mathbf{A}_\nu} = \mathcal{C}_{\mathbf{A}_\nu}^{\perp_\sigma} \right\}. \quad (7.2)$$

When $\mathbf{A}_\nu(x) \in T_\nu$, it is easy to see that $\dim_{\mathcal{F}_\nu} \mathcal{C}_{\mathbf{A}_\nu} = \frac{\ell t}{2}$. Further, let us define the sets

$$T = T_1 \oplus T_2 \oplus \dots \oplus T_s = \left\{ (\mathbf{A}_1(x), \mathbf{A}_2(x), \dots, \mathbf{A}_s(x)) : \mathbf{A}_\nu(x) \in T_\nu \text{ for } 1 \leq \nu \leq s \right\}$$

and

$$\mathcal{F} = \mathcal{F}_1^{\frac{\ell t}{2}} \oplus \mathcal{F}_2^{\frac{\ell t}{2}} \oplus \cdots \oplus \mathcal{F}_s^{\frac{\ell t}{2}} = \left\{ (\mathbf{f}_1(x), \mathbf{f}_2(x), \dots, \mathbf{f}_s(x)) : \mathbf{f}_\nu(x) \in \mathcal{F}_\nu^{\frac{\ell t}{2}} \text{ for } 1 \leq \nu \leq s \right\}.$$

Furthermore, for

$$\mathbf{A}(x) = (\mathbf{A}_1(x), \mathbf{A}_2(x), \dots, \mathbf{A}_s(x)) \in T$$

and

$$\mathbf{f}(x) = (\mathbf{f}_1(x), \mathbf{f}_2(x), \dots, \mathbf{f}_s(x)) \in \mathcal{F},$$

let us define

$$\mathbf{f}(x) \diamond \mathbf{A}(x) = (\mathbf{f}_1(x) \odot \mathbf{A}_1(x), \mathbf{f}_2(x) \odot \mathbf{A}_2(x), \dots, \mathbf{f}_s(x) \odot \mathbf{A}_s(x)) \in \mathbb{G}.$$

Theorem 7.2.1. *For $\mathbf{A}(x) \in T$, the set*

$$\mathcal{C}_{\mathbf{A}} = \{\mathbf{f}(x) \diamond \mathbf{A}(x) : \mathbf{f}(x) \in \mathcal{F}\} \tag{7.3}$$

is a σ -self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ with rate $R(\mathcal{C}_{\mathbf{A}}) = \frac{1}{2}$.

Proof. To prove the result, let us write $\mathbf{A}(x) = (\mathbf{A}_1(x), \mathbf{A}_2(x), \dots, \mathbf{A}_s(x)) \in T$, where $\mathbf{A}_\nu(x) \in T_\nu$ for $1 \leq \nu \leq s$. Here we first observe that $\mathcal{C}_{\mathbf{A}} = \bigoplus_{\nu=1}^s \mathcal{C}_{\mathbf{A}_\nu}$. As $\mathcal{C}_{\mathbf{A}_\nu}$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ for $1 \leq \nu \leq s$, we see, by Theorem 3.3.1, that the code $\mathcal{C}_{\mathbf{A}}$ is an MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ with the constituents as $\mathcal{C}_{\mathbf{A}_1}, \mathcal{C}_{\mathbf{A}_2}, \dots, \mathcal{C}_{\mathbf{A}_s}$. Since $\mathbf{A}_\nu(x) \in T_\nu$, we note that $\mathcal{C}_{\mathbf{A}_\nu} = \mathcal{C}_{\mathbf{A}_\nu}^{\perp_\sigma}$ for $1 \leq \nu \leq s$, which, by Theorem 4.4.1(b), implies that the code $\mathcal{C}_{\mathbf{A}}$ is a σ -self-dual code over $\mathbb{F}_{q^t}$. Furthermore, we note that $\sum_{\nu=1}^s d_\nu = m$ and $|\mathcal{C}_{\mathbf{A}_\nu}| = q^{\frac{d_\nu \ell t}{2}}$ for each ν . From this, it follows that

$$|\mathcal{C}_{\mathbf{A}}| = \prod_{\nu=1}^s |\mathcal{C}_{\mathbf{A}_\nu}| = \prod_{\nu=1}^s q^{\frac{d_\nu \ell t}{2}} = q^{\frac{\ell t}{2} \sum_{\nu=1}^s d_\nu} = q^{\frac{m \ell t}{2}},$$

which implies that

$$R(\mathcal{C}_{\mathbf{A}}) = \frac{\log_{q^t} |\mathcal{C}_{\mathbf{A}}|}{m\ell} = \frac{m\ell}{2m\ell} = \frac{1}{2}.$$

□

Now to study the asymptotic behaviour of relative Hamming distances of σ -self-dual MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$, we shall view the set T as a probability space, where each sample of T is chosen with equal probability. We note that $|T| = \prod_{\nu=1}^s |T_\nu|$. In the following lemma, we explicitly determine the cardinalities of the sets $T_1, T_2, \dots, T_s$, which are needed to determine the size of the probability space T .

Lemma 7.2.3. *For $1 \leq \nu \leq s$, we have*

$$|T_\nu| = \begin{cases} \prod_{h=0}^{\frac{\ell t}{2}-1} q^h (q^{\ell t-2h} - 1) & \text{if } \nu = 1 \text{ and either } \sigma = \gamma \text{ or } \sigma = * \text{ and } q \text{ is even;} \\ \prod_{h=0}^{\frac{\ell t}{2}-2} q^{h+1} (q^{\ell t-2h-2} - 1)(q - 1) q^{\frac{\ell t-2}{2}} & \text{if } \nu = 1, \sigma = 0 \text{ and both } \ell t, q \text{ are even;} \\ \prod_{h=0}^{\frac{\ell t}{2}-1} q^h (q^{\frac{\ell t-2h}{2}} - 1)(q^{\frac{\ell t-2h-2}{2}} + 1) & \text{if } \nu = 1, \sigma \in \{0, *\} \text{ with either } \ell \text{ being} \\ & \text{even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ being even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \\ & \text{or } \ell \text{ being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \prod_{h=0}^{\frac{\ell t}{2}-1} q^{d_\nu h} (q^{\frac{d_\nu(\ell t-2h-1)}{2}} + 1)(q^{\frac{d_\nu(\ell t-2h)}{2}} - 1) & \text{if } 2 \leq \nu \leq s; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. To prove the result, we observe that for each ν , the number $|T_\nu|$ is equal to the number of all possible ordered bases of σ -self-dual $\mathcal{F}_\nu$ -subspaces of $\mathbb{G}_\nu$. Here we shall distinguish the following two cases: **I.** $\nu = 1$ and **II.** $2 \leq \nu \leq s$.

- I. First let $\nu = 1$. Here we have $d_1 = 1$, $\mathcal{F}_1 \simeq \mathbb{F}_q$ and $\mathbb{G}_1 \simeq \mathbb{F}_{q^t}^\ell$. Therefore each element $A_1(x) \in \mathbb{G}_1$ is of the type $A_1(x) = A_1 = (A_{1,1}, A_{1,2}, \dots, A_{1,\ell})$, where $A_{1,i} \in \mathbb{F}_{q^t}$ for $1 \leq i \leq \ell$.

When $\sigma = \gamma$, we see, by Lemma 4.4.2(c), that $(\mathbb{G}_1, [\cdot, \cdot]_\gamma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a symplectic space of dimension ℓt and Witt index $\frac{\ell t}{2}$ over $\mathcal{F}_1$. Now by applying Theorems 2.2.2 and 2.2.3(b) & (d), we get

$$|T_1| = \prod_{h=0}^{\frac{\ell t}{2}-1} q^h (q^{\ell t-2h} - 1).$$

When q is odd and $\sigma \in \{0, *\}$, we have either ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$. In this case, we shall view the orthogonal space $(\mathbb{G}_1, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ as a non-degenerate quadratic space $(\mathbb{G}_1, \mathcal{Q}_1)$ over $\mathcal{F}_1$ with respect to the quadratic map $\mathcal{Q}_1 : \mathbb{G}_1 \rightarrow \mathcal{F}_1$, defined as

$$\mathcal{Q}_1(A_1) = \frac{1}{2} [A_1, A_1]_\sigma \text{ for all } A_1 \in \mathbb{G}_1.$$

We see, by Theorem 2.2.6, that the quadratic space $(\mathbb{G}_1, \mathcal{Q}_1)$ of dimension ℓt has Witt index $\frac{\ell t}{2}$ over $\mathcal{F}_1$. Now by applying Theorems 2.2.2, 2.2.5(b) & (d) and 2.2.7, we see that

$$|T_1| = \prod_{h=0}^{\frac{\ell t}{2}-1} q^h (q^{\frac{\ell t-2h}{2}} - 1) (q^{\frac{\ell t-2h-2}{2}} + 1).$$

When q is even and $\sigma = *$, we see, working as in the proof of Case **III** of Lemma 5.2.1(a), that $(\mathbb{G}_1, (\cdot, \cdot)_* \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1})$ is a symplectic space of dimension ℓt and Witt index $\frac{\ell t}{2}$ over $\mathcal{F}_1$. Now by applying Theorems 2.2.2 and 2.2.3(b) & (d), we get

$$|T_1| = \prod_{h=0}^{\frac{\ell t}{2}-1} q^h (q^{\ell t-2h} - 1).$$

Finally, let q be even and $\sigma = 0$. Here, we see, working as in the proof of Case **I(ii)** of Lemma 5.2.1(a), that the set

$$\mathbb{M}_1 = \{A_1 = (A_{1,1}, A_{1,2}, \dots, A_{1,\ell}) \in \mathbb{G}_1 : \sum_{i=1}^{\ell} \text{Tr}_{q^t, q}(A_{1,i}) = 0\}$$

is an $(\ell t - 1)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ containing the element $\Theta_1 = (\underbrace{1, 1, \dots, 1}_{\ell \text{ times}}) \in \mathbb{G}_1$. One can easily observe that $\Theta_1 \in \mathbb{M}_1 \cap \mathbb{M}_1^{\perp_0}$. Now let $\widehat{\mathbb{M}}_1$ be an $(\ell t - 2)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ satisfying $\Theta_1 \notin \widehat{\mathbb{M}}_1$, so that

$\mathbb{M}_1 = \widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$. Further, it is easy to observe that there exists an element $y_1 \in \widehat{\mathbb{M}}_1^{\perp_0} \setminus \mathbb{M}_1$ such that $\mathbb{G}_1 = \widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle \oplus \langle y_1 \rangle$. Here we see that any element of $\mathbb{G}_1$ is of the form $A_1 + a\Theta_1 + by_1$, where $A_1 \in \widehat{\mathbb{M}}_1$ and $a, b \in \mathcal{F}_1$. Further, the element $A_1 + a\Theta_1 + by_1 \in \mathbb{G}_1$ is isotropic if and only if $b = 0$. This implies that each 0-self-orthogonal $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ must be contained in $\widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$. Furthermore, one can easily observe that $(\widehat{\mathbb{M}}_1, [\cdot, \cdot]_0 \upharpoonright \widehat{\mathbb{M}}_1 \times \widehat{\mathbb{M}}_1)$ is a symplectic space of dimension $(\ell t - 2)$ and Witt index $\frac{\ell t - 2}{2}$ over $\mathcal{F}_1$. From this, it follows that any 0-self-dual $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ must be contained in $\widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$, but not in $\widehat{\mathbb{M}}_1$. Now to determine the number $|T_1|$, we proceed to count the number of distinct ordered bases of all 0-self-dual $\mathcal{F}_1$ -subspaces of $\mathbb{G}_1$ that are contained in $\widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$ but not in $\widehat{\mathbb{M}}_1$. For this, we see, by applying Theorems 2.2.2 and 2.2.3(a), (b) & (d), that there are precisely $\prod_{h=0}^{\frac{\ell t}{2}-2} q^{h+1}(q^{\ell t-2h-2} - 1)$ distinct mutually orthogonal isotropic elements $A_1^{(1)} + a_1\Theta_1, A_1^{(2)} + a_2\Theta_1, \dots, A_1^{(\frac{\ell t-2}{2})} + a_{\frac{\ell t-2}{2}}\Theta_1$ in $\widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$, where $A_1^{(h)} \in \widehat{\mathbb{M}}_1$ and $a_h \in \mathcal{F}_1$ for $1 \leq h \leq \frac{\ell t-2}{2}$. Next, for $A_1^{(\frac{\ell t}{2})} \in \widehat{\mathbb{M}}_1$ and $a_{\frac{\ell t}{2}} \in \mathcal{F}_1$, we see that the element $A_1^{(\frac{\ell t}{2})} + a_{\frac{\ell t}{2}}\Theta_1$ is orthogonal to the element $A_1^{(h)} + a_h\Theta_1$ for $1 \leq h \leq \frac{\ell t-2}{2}$ with respect to the form $[\cdot, \cdot]_0 \upharpoonright_{\mathbb{G}_1 \times \mathbb{G}_1}$ if and only if $A_1^{(\frac{\ell t}{2})} \in \langle A_1^{(1)}, A_1^{(2)}, \dots, A_1^{(\frac{\ell t-2}{2})} \rangle$. In view of this, let us write $A_1^{(\frac{\ell t}{2})}$ as $A_1^{(\frac{\ell t}{2})} = b_1 A_1^{(1)} + b_2 A_1^{(2)} + \dots + b_{\frac{\ell t-2}{2}} A_1^{(\frac{\ell t-2}{2})}$, where $b_1, b_2, \dots, b_{\frac{\ell t-2}{2}} \in \mathcal{F}_1$. Further, we observe that the set $\{A_1^{(1)} + a_1\Theta_1, A_1^{(2)} + a_2\Theta_1, \dots, A_1^{(\frac{\ell t}{2})} + a_{\frac{\ell t}{2}}\Theta_1\}$ is linearly independent over $\mathcal{F}_1$ if and only if $a_{\frac{\ell t}{2}} \neq a_1 b_1 + a_2 b_2 + \dots + a_{\frac{\ell t-2}{2}} b_{\frac{\ell t-2}{2}}$. Thus there are precisely $q^{\frac{\ell t-2}{2}}(q-1)$ distinct choices for the desired element $A_1^{(\frac{\ell t}{2})} + a_{\frac{\ell t}{2}}\Theta_1$ in $\widehat{\mathbb{M}}_1 \oplus \langle \Theta_1 \rangle$. From this, it follows that

$$|T_1| = \prod_{h=0}^{\frac{\ell t}{2}-2} q^{h+1}(q^{\ell t-2h-2} - 1)(q-1)q^{\frac{\ell t-2}{2}}.$$

- II. Next, let $2 \leq \nu \leq s$. Here we note that the integer $d_\nu = \deg h_\nu(x)$ is even and $\mathcal{F}_\nu \simeq \mathbb{F}_{q^{d_\nu}}$. When $\sigma \in \{0, *\}$, we see, by Lemma 4.4.2(b), that $(\mathbb{G}_\nu, [\cdot, \cdot]_\sigma \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu})$ is a unitary space of dimension ℓt and Witt index $\frac{\ell t}{2}$ over $\mathcal{F}_\nu$. Further, working as in the proof of Lemma 5.2.1(b), we can define an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H}$ on $\mathbb{G}_\nu \times \mathbb{G}_\nu$. We further observe that $(\mathbb{G}_\nu, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu})$ is a unitary space of dimension ℓt and Witt index $\frac{\ell t}{2}$ over

$\mathcal{F}_\nu$. From this and by applying Theorems [2.2.2](#) and [2.2.4](#)(a), (c) & (e), we obtain

$$|T_\nu| = \prod_{h=0}^{\frac{\ell t}{2}-1} q^{d_\nu h} (q^{\frac{d_\nu(\ell t-2h-1)}{2}} + 1) (q^{\frac{d_\nu(\ell t-2h)}{2}} - 1).$$

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

For each sample $\mathbf{A}(x)$ in the probability space T , we see, by Theorem [7.2.1](#), that the code $\mathcal{C}_\mathbf{A}$ (as defined by [\(7.3\)](#)) is a random σ -self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ with rate $R(\mathcal{C}_\mathbf{A}) = \frac{1}{2}$. The relative Hamming distance $\Delta(\mathcal{C}_\mathbf{A}) = \frac{wt(\mathcal{C}_\mathbf{A})}{m\ell}$ of the random code $\mathcal{C}_\mathbf{A}$ is a random variable over the probability space T , where each sample is chosen with equal probability.

We now study the asymptotic behaviour of the probability $\Pr(\Delta(\mathcal{C}_\mathbf{A}) > \delta)$, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$. Towards this, for $\mathbf{f}(x) \in \mathcal{F}$, let us define

$$I_\mathbf{f} = \left\{ \mathbf{f}(x) \diamond \mathbf{A}(x) : \mathbf{A}(x) \in \bigoplus_{\nu=1}^s \mathbb{G}_\nu^{\frac{\ell t}{2}} \right\} \subseteq \mathbb{G}. \quad (7.4)$$

Further, for $1 \leq \nu \leq s$ and $\mathbf{f}_\nu(x) \in \mathcal{F}_\nu^{\frac{\ell t}{2}}$, let us define

$$I_{\mathbf{f}_\nu} = \left\{ \mathbf{f}_\nu(x) \odot \mathbf{A}_\nu(x) : \mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}} \right\} \subseteq \mathbb{G}_\nu.$$

Note that $I_\mathbf{f} = \bigoplus_{\nu=1}^s I_{\mathbf{f}_\nu}$. Further, one can easily observe that $I_{\mathbf{f}_\nu} = \{\mathbf{0}\}$ if $\mathbf{f}_\nu(x) = 0$, while $I_{\mathbf{f}_\nu} = \mathbb{G}_\nu$ if $\mathbf{f}_\nu(x) \neq 0$.

Lemma 7.2.4. *Let $\mathbf{f}(x) \in \mathcal{F}$ be fixed. For $I_\mathbf{f} \subseteq \mathbb{G}$, let us define*

$$(I_\mathbf{f})^{\leq \delta} = \left\{ \mathbf{F}(x) \in I_\mathbf{f} : \widehat{wt}(\mathbf{F}(x)) \leq \delta \right\}.$$

We have

$$|(I_\mathbf{f})^{\leq \delta}| \leq \prod_{\nu=1}^s q^{\ell t d_\nu h_{q^t}(\delta)}.$$

Proof. To prove the result, we note that if $\mathbf{f}(x) = \mathbf{0}$, then $\mathbf{f}_\nu(x) = 0$, and hence $I_{\mathbf{f}_\nu} = \{\mathbf{0}\}$ for $1 \leq \nu \leq s$. This gives $I_\mathbf{f} = \{\mathbf{0}\}$ and $|(I_\mathbf{f})^{\leq \delta}| = 1 \leq \prod_{\nu=1}^s q^{\ell t d_\nu h_{q^t}(\delta)}$. Now suppose that $\mathbf{f}(x) (\neq \mathbf{0}) \in \mathcal{F}$. Here $\mathbf{f}_\nu(x) \neq 0$, and hence $I_{\mathbf{f}_\nu} = \mathbb{G}_\nu$ for some ν satisfying $1 \leq \nu \leq s$. We next observe that $\mathbb{W}_\nu = \frac{\mathbb{F}_{q^t}[x]}{\langle h_\nu(x) \rangle} \simeq \left\langle \frac{x^m - \omega}{h_\nu(x)} \right\rangle_{\mathcal{R}_{m,\omega}}$, and

hence $\mathbb{W}_\nu$ is a minimal ideal of $\frac{\mathbb{F}_{q^t}[x]}{\langle x^m - \omega \rangle}$, i.e., $\mathbb{W}_\nu$ is an ω -constacyclic code of length m and dimension d_ν over $\mathbb{F}_{q^t}$. Now working as in Lemma 3.5.2, we see that $\mathbb{W}_\nu$ is a balanced code of length m and dimension d_ν over $\mathbb{F}_{q^t}$. Further, by Theorem 2.1.4, we see that $I_{\mathbf{f}_\nu} = \mathbb{G}_\nu = \mathbb{W}_\nu^\ell$ is a balanced code of length $m\ell$ and dimension $d_\nu\ell$ over $\mathbb{F}_{q^t}$. Let $S_{\mathbf{f}} = \{\nu : 1 \leq \nu \leq s \text{ and } \mathbf{f}_\nu(x) \neq 0\}$. By applying Theorem 2.1.4 again, we see that $I_{\mathbf{f}} = \bigoplus_{\nu \in S_{\mathbf{f}}} I_{\mathbf{f}_\nu}$ is a balanced code of length $m\ell$ and dimension $\sum_{\nu \in S_{\mathbf{f}}} d_\nu\ell$ over $\mathbb{F}_{q^t}$ and that

$$|(I_{\mathbf{f}})^{\leq \delta}| \leq q^{\sum_{\nu \in S_{\mathbf{f}}} \ell d_\nu h_{q^t}(\delta)} = \prod_{\nu \in S_{\mathbf{f}}} q^{\ell d_\nu h_{q^t}(\delta)} \leq \prod_{\nu=1}^s q^{\ell d_\nu h_{q^t}(\delta)}.$$

□

Lemma 7.2.5. *For a non-zero $\mathbf{f}(x) \in \mathcal{F}$, let $B(x) \in I_{\mathbf{f}}$ be fixed. We have*

$$\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)) \leq \begin{cases} \left(\frac{q^{-\frac{(\ell t+2)}{2}}}{1-q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{-\frac{d_\nu(\ell t+1)}{2}}}{(1-q^{-d_\nu})(1+q^{-\frac{d_\nu}{2}})} \right) & \text{if either } \sigma = \gamma \text{ or} \\ & \sigma = * \text{ and } q \text{ is even;} \\ \left(\frac{q^{-\frac{\ell t}{2}}}{2(1-q^{-1})} \right) \prod_{\nu=2}^s \left(\frac{q^{-\frac{d_\nu(\ell t+1)}{2}}}{(1-q^{-d_\nu})(1+q^{-\frac{d_\nu}{2}})} \right) & \text{if } \sigma \in \{0, *\} \text{ with} \\ & \text{either } \ell \text{ being even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ being even,} \\ & \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or } \ell \text{ being odd,} \\ & t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \left(\frac{q^{-\frac{\ell t}{2}}}{1-q^{-1}} \right) \prod_{\nu=2}^s \left(\frac{q^{-\frac{d_\nu(\ell t+1)}{2}}}{(1-q^{-d_\nu})(1+q^{-\frac{d_\nu}{2}})} \right) & \text{if } \sigma = 0 \text{ and both } \ell t, q \\ & \text{are even,} \end{cases}$$

where the element $\mathbf{A}(x)$ runs over the probability space T in the probability $\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x))$.

Proof. To prove the result, let us write $B(x) = (B_1(x), B_2(x), \dots, B_s(x))$. Let $\mathbf{N}$ be the number of elements $\mathbf{A}(x) \in T$ satisfying $\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)$. It is easy to see that $\mathbf{N} = \prod_{\nu=1}^s \mathbf{N}_\nu$, where $\mathbf{N}_\nu$ is the number of elements $\mathbf{A}_\nu(x) \in T_\nu$ satisfying $\mathbf{f}_\nu(x) \odot \mathbf{A}_\nu(x) = B_\nu(x)$ for $1 \leq \nu \leq s$. Further, for each ν , we observe that $\mathbf{N}_\nu = |T_\nu|$ if $\mathbf{f}_\nu(x) = 0$, while $\mathbf{N}_\nu = 0$ if $\mathbf{f}_\nu(x) \neq 0$ and $[B_\nu(x), B_\nu(x)]_\sigma \neq 0$. On the other hand, if $\mathbf{f}_\nu(x) \neq 0$ and $[B_\nu(x), B_\nu(x)]_\sigma = 0$, one can easily observe that

$$N_\nu = \begin{cases} \prod_{h=0}^{\frac{\ell t}{2}-2} q^h (q^{\ell t-2h} - 1) & \text{if } \nu = 1 \text{ and either } \sigma = \gamma \text{ or } \sigma = * \text{ and } q \text{ is even;} \\ \prod_{h=0}^{\frac{\ell t}{2}-2} q^h (q^{\frac{\ell t-2h}{2}} - 1) (q^{\frac{\ell t-2h-2}{2}} + 1) & \text{if } \nu = 1, \sigma \in \{0, *\} \text{ with either } \ell \text{ being} \\ & \text{even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ being even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \\ & \text{or } \ell \text{ being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \prod_{h=0}^{\frac{\ell t}{2}-2} q^{h+1} (q^{\ell t-2h-2} - 1) & \text{if } \nu = 1, \sigma = 0 \text{ and both } \ell t, q \text{ are even;} \\ \prod_{h=0}^{\frac{\ell t}{2}-2} q^{d_\nu h} (q^{\frac{d_\nu(\ell t-2h-1)}{2}} + 1) (q^{\frac{d_\nu(\ell t-2h)}{2}} - 1) & \text{if } 2 \leq \nu \leq s. \end{cases}$$

We further observe that $\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)) = \prod_{\nu=1}^s \frac{N_\nu}{|T_\nu|}$. From this and by substituting the values of the numbers $|T_1|, |T_2|, \dots, |T_s|$ from Lemma 7.2.3 in the respective cases, the desired result follows. $\square$

From now on, let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$. For each sample $\mathbf{A}(x) \in T$, let $\mathbf{N}_{\mathcal{C}_\mathbf{A}}(\delta)$ be the number of non-zero codewords of the random code $\mathcal{C}_\mathbf{A}$ having relative Hamming weight at most δ . We note that

$$\mathbf{N}_{\mathcal{C}_\mathbf{A}}(\delta) = \left| \left\{ \mathbf{f}(x) \in \mathcal{F} : 0 < \widehat{wt}(\mathbf{f}(x) \diamond \mathbf{A}(x)) \leq \delta \right\} \right|$$

is a non-negative integral random variable defined on the probability space T and is called the *cumulative weight enumerator* for the random code $\mathcal{C}_\mathbf{A}$. Further, corresponding to a given $\mathbf{f}(x) \in \mathcal{F}$ and samples $\mathbf{A}(x) \in T$, let us define the *indicator random variable* $\mathbf{Z}_\mathbf{f}$ as

$$\mathbf{Z}_\mathbf{f} = \begin{cases} 1 & \text{if } 0 < \widehat{wt}(\mathbf{f}(x) \diamond \mathbf{A}(x)) \leq \delta; \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\mathbf{Z}_\mathbf{f}$ is a Bernoulli random variable defined on the probability space T . It is easy to see that $\mathbf{Z}_\mathbf{0} = 0$ and $\mathbf{N}_{\mathcal{C}_\mathbf{A}}(\delta) = \sum_{\mathbf{f}(x) \neq \mathbf{0} \in \mathcal{F}} \mathbf{Z}_\mathbf{f}$.

Lemma 7.2.6. *For a non-zero element $\mathbf{f}(x) \in \mathcal{F}$, let $E(\mathbf{Z}_{\mathbf{f}})$ denote the expectation of the indicator random variable $\mathbf{Z}_{\mathbf{f}}$ defined on the probability space T . We have*

$$E(\mathbf{Z}_{\mathbf{f}}) \leq \begin{cases} \left(\frac{q^{-\ell t(\frac{1}{2} + \frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if either } \sigma = \gamma \text{ or } \sigma = * \\ & \text{and } q \text{ is even;} \\ \left(\frac{q^{-\ell t(\frac{1}{2} - h_{q^t}(\delta))}}{2(1 - q^{-1})} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if } \sigma \in \{0, *\} \text{ with either } \ell \text{ being} \\ & \text{even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ being even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \\ & \text{or } \ell \text{ being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \left(\frac{q^{-\ell t(\frac{1}{2} - h_{q^t}(\delta))}}{1 - q^{-1}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if } \sigma = 0 \text{ and both } \ell t, q \text{ are even.} \end{cases}$$

Proof. Since $\mathbf{Z}_{\mathbf{f}}$ is a Bernoulli random variable defined on the probability space T , we have

$$\begin{aligned} E(\mathbf{Z}_{\mathbf{f}}) &= \Pr(\mathbf{Z}_{\mathbf{f}} = 1) = \frac{\left| \left\{ \mathbf{A}(x) \in T : 0 < \widehat{wt}(\mathbf{f}(x) \diamond \mathbf{A}(x)) \leq \delta \right\} \right|}{|T|} \\ &= \sum_{\substack{B(x) \in I_{\mathbf{f}} \\ 0 < \widehat{wt}(B(x)) \leq \delta}} \frac{\left| \left\{ \mathbf{A}(x) \in T : \mathbf{f}(x) \diamond \mathbf{A}(x) = B(x) \right\} \right|}{|T|} \\ &= \sum_{B(x) (\neq \mathbf{0}) \in (I_{\mathbf{f}})^{\leq \delta}} \Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)) \\ &\leq |(I_{\mathbf{f}})^{\leq \delta}| \times \Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)), \end{aligned}$$

where $\mathbf{A}(x)$ runs over the probability space T in the probability $\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x))$. Now by Lemmas 7.2.4 and 7.2.5, the desired result follows. $\square$

Lemma 7.2.7. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$. For $\mathbf{A}(x) \in T$, let $\mathcal{C}_{\mathbf{A}}$ be the corresponding σ -self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{q^t}$ as defined by (7.3). We have*

$$\Pr(\Delta(\mathcal{C}_{\mathbf{A}}) \leq \delta) \leq \begin{cases} \left(\frac{q^{-\ell t(\frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if either } \sigma = \gamma \text{ or } \sigma = * \\ & \text{and } q \text{ is even;} \\ \left(\frac{q^{\frac{\ell t h_{q^t}(\delta)}{2(1 - q^{-1})}}}{1 - q^{-1}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if } \sigma \in \{0, *\} \text{ with either } \ell \text{ being} \\ & \text{even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ being even, } \ell t \equiv 0 \pmod{4} \text{ and} \\ & q \equiv 3 \pmod{4} \text{ or } \ell \text{ being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \left(\frac{q^{\frac{\ell t h_{q^t}(\delta)}{1 - q^{-1}}}}{1 - q^{-1}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) & \text{if } \sigma = 0 \text{ and both } \ell t, q \text{ are even.} \end{cases}$$

Proof. Let us define $\mathbf{Z} = \sum_{\mathbf{f}(x) \in \mathcal{F}} \mathbf{Z}_{\mathbf{f}}$. As $\mathbf{Z}_0 = 0$, we see that

$$\mathbf{Z} = \sum_{\mathbf{f}(x) \neq 0} \mathbf{Z}_{\mathbf{f}} = \mathbf{N}_{\mathcal{C}_{\mathbf{A}}}(\delta),$$

which equals the number of non-zero elements $\mathbf{f}(x) \in \mathcal{F}$ such that the corresponding codeword $\mathbf{f}(x) \diamond \mathbf{A}(x) \in \mathcal{C}_{\mathbf{A}}$ has relative Hamming weight at most δ . From this, it follows that $\Pr(\Delta(\mathcal{C}_{\mathbf{A}}) \leq \delta) = \Pr(\mathbf{Z} > 0)$. Further, by Theorem 2.3.2, we see that $\Pr(\mathbf{Z} > 0) \leq E(\mathbf{Z})$. Furthermore, by Theorem 2.3.1, we get

$$\Pr(\Delta(\mathcal{C}_{\mathbf{A}}) \leq \delta) = \Pr(\mathbf{Z} > 0) \leq E(\mathbf{Z}) = E\left(\sum_{\mathbf{f}(x) \neq 0} \mathbf{Z}_{\mathbf{f}}\right) = \sum_{\mathbf{f}(x) \neq 0} E(\mathbf{Z}_{\mathbf{f}}).$$

Now if either $\sigma = \gamma$ or $\sigma = *$ and q is even, we see, by Lemma 7.2.6, that

$$\begin{aligned} E(\mathbf{Z}) &\leq \sum_{\mathbf{f}(x) \neq 0} \left(\frac{q^{-\ell t(\frac{1}{2} + \frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) \\ &\leq \left(\frac{q^{\frac{\ell t}{2}} q^{-\ell t(\frac{1}{2} + \frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{\frac{d_{\nu} \ell t}{2}} q^{-d_{\nu} \ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right) \\ &= \left(\frac{q^{-\ell t(\frac{1}{\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu=2}^s \left(\frac{q^{-d_{\nu} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu}})(1 + q^{-\frac{d_{\nu}}{2}})} \right). \end{aligned}$$

Working as above and by applying Lemma 7.2.6 again, we get the desired result in

the remaining cases. $\square$

Now let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for $j \geq 1$. Note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. For each $j \geq 1$, let $x^{\mathbf{m}_j} - \omega = h_1^{(j)}(x)h_2^{(j)}(x) \cdots h_{s_j}^{(j)}(x)$ be the irreducible factorization of the polynomial $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$ such that $h_1^{(j)}(x) = x - 1$ if $\omega = 1$, while $h_1^{(j)}(x) = x + 1$ if $\omega = -1$. For $j \geq 1$ and $1 \leq \nu_j \leq s_j$, let $d_{\nu_j}^{(j)} = \deg h_{\nu_j}^{(j)}(x)$. Further, for each positive integer j , let ξ_j be a primitive $(\mathbf{m}_j e)$ -th root of unity in some field extension of $\mathbb{F}_q$ satisfying $\xi_j^{\mathbf{m}_j} = \omega$, and let $h_2^{(j)}(x)$ be the minimal polynomial of ξ_j over $\mathbb{F}_q$. Further, we see, by (7.1), that $d_2^{(j)} = \deg h_2^{(j)}(x) = v p^{\alpha_j - \eta} > 1$ for each j . As $v = \text{ord}_p(q)$ is even, we see, for each j , that all the irreducible factors $h_1^{(j)}(x), h_2^{(j)}(x), \dots, h_{s_j}^{(j)}(x)$ of $x^{\mathbf{m}_j} - \omega$ over $\mathbb{F}_q$ are self-reciprocal. We also note that $d_1^{(j)} = \deg h_1^{(j)}(x) = 1$ and $d_{\nu_j}^{(j)} = \deg h_{\nu_j}^{(j)}(x)$ is an even integer for $2 \leq \nu_j \leq s_j$.

Next, for each $j \geq 1$, let us recall

$$\mathcal{F}_{\nu_j}^{(j)} = \frac{\mathbb{F}_q[x]}{\langle h_{\nu_j}^{(j)}(x) \rangle}, \quad \mathbb{G}_{\nu_j}^{(j)} = \left(\frac{\mathbb{F}_{q^t}[x]}{\langle h_{\nu_j}^{(j)}(x) \rangle} \right)^\ell \quad \text{for } 1 \leq \nu_j \leq s_j, \quad \text{and let } \mathbb{G}^{(j)} = \bigoplus_{\nu_j=1}^{s_j} \mathbb{G}_{\nu_j}^{(j)}.$$

Let $j \geq 1$ and $1 \leq \nu_j \leq s_j$ be fixed. For

$$\mathbf{f}_{\nu_j}^{(j)}(x) = (f_{\nu_j}^{(j,1)}(x), f_{\nu_j}^{(j,2)}(x), \dots, f_{\nu_j}^{(j, \frac{\ell t}{2})}(x)) \in \left(\mathcal{F}_{\nu_j}^{(j)} \right)^{\frac{\ell t}{2}}$$

and

$$\mathbf{A}_{\nu_j}^{(j)}(x) = (A_{\nu_j}^{(j,1)}(x), A_{\nu_j}^{(j,2)}(x), \dots, A_{\nu_j}^{(j, \frac{\ell t}{2})}(x)) \in \left(\mathbb{G}_{\nu_j}^{(j)} \right)^{\frac{\ell t}{2}},$$

let us define

$$\mathbf{f}_{\nu_j}^{(j)}(x) \odot \mathbf{A}_{\nu_j}^{(j)}(x) = f_{\nu_j}^{(j,1)}(x)A_{\nu_j}^{(j,1)}(x) + f_{\nu_j}^{(j,2)}(x)A_{\nu_j}^{(j,2)}(x) + \cdots + f_{\nu_j}^{(j, \frac{\ell t}{2})}(x)A_{\nu_j}^{(j, \frac{\ell t}{2})}(x) \in \mathbb{G}_{\nu_j}^{(j)}.$$

Corresponding to the element $\mathbf{A}_{\nu_j}^{(j)}(x) \in \left(\mathbb{G}_{\nu_j}^{(j)} \right)^{\frac{\ell t}{2}}$, let us define

$$\mathcal{C}_{\mathbf{A}_{\nu_j}^{(j)}} = \left\{ \mathbf{f}_{\nu_j}^{(j)}(x) \odot \mathbf{A}_{\nu_j}^{(j)}(x) : \mathbf{f}_{\nu_j}^{(j)}(x) \in \left(\mathcal{F}_{\nu_j}^{(j)} \right)^{\frac{\ell t}{2}} \right\}.$$

It is easy to observe that the set $\mathcal{C}_{\mathbf{A}_{\nu_j}^{(j)}}$ is an $\mathcal{F}_{\nu_j}^{(j)}$ -subspace of $\mathbb{G}_{\nu_j}^{(j)}$ generated by the

ordered basis $\mathbf{A}_{\nu_j}^{(j)}(x)$. Now let us define the set

$$T_{\nu_j}^{(j)} = \left\{ \mathbf{A}_{\nu_j}^{(j)}(x) \in (\mathbb{G}_{\nu_j}^{(j)})^{\frac{\ell t}{2}} : \mathcal{C}_{\mathbf{A}_{\nu_j}^{(j)}} = \mathcal{C}_{\mathbf{A}_{\nu_j}^{(j)}}^{\perp_{\sigma}} \right\}. \quad (7.5)$$

When $\mathbf{A}_{\nu_j}^{(j)}(x) \in T_{\nu_j}^{(j)}$, we see that $\dim_{\mathcal{F}_{\nu_j}^{(j)}} \mathcal{C}_{\mathbf{A}_{\nu_j}^{(j)}} = \frac{\ell t}{2}$. Further, let us define the sets

$$\begin{aligned} T^{(j)} &= T_1^{(j)} \oplus T_2^{(j)} \oplus \dots \oplus T_{s_j}^{(j)} \\ &= \left\{ (\mathbf{A}_1^{(j)}(x), \mathbf{A}_2^{(j)}(x), \dots, \mathbf{A}_{s_j}^{(j)}(x)) : \mathbf{A}_{\nu_j}^{(j)}(x) \in T_{\nu_j}^{(j)} \text{ for } 1 \leq \nu_j \leq s_j \right\} \end{aligned}$$

and

$$\begin{aligned} \mathcal{F}^{(j)} &= (\mathcal{F}_1^{(j)})^{\frac{\ell t}{2}} \oplus (\mathcal{F}_2^{(j)})^{\frac{\ell t}{2}} \oplus \dots \oplus (\mathcal{F}_{s_j}^{(j)})^{\frac{\ell t}{2}} \\ &= \left\{ (\mathbf{f}_1^{(j)}(x), \mathbf{f}_2^{(j)}(x), \dots, \mathbf{f}_{s_j}^{(j)}(x)) : \mathbf{f}_{\nu_j}^{(j)}(x) \in (\mathcal{F}_{\nu_j}^{(j)})^{\frac{\ell t}{2}} \text{ for } 1 \leq \nu_j \leq s_j \right\}. \end{aligned}$$

Furthermore, for

$$\mathbf{A}^{(j)}(x) = (\mathbf{A}_1^{(j)}(x), \mathbf{A}_2^{(j)}(x), \dots, \mathbf{A}_{s_j}^{(j)}(x)) \in T^{(j)}$$

and

$$\mathbf{f}^{(j)}(x) = (\mathbf{f}_1^{(j)}(x), \mathbf{f}_2^{(j)}(x), \dots, \mathbf{f}_{s_j}^{(j)}(x)) \in \mathcal{F}^{(j)},$$

let us define

$$\mathbf{f}^{(j)}(x) \diamond \mathbf{A}^{(j)}(x) = (\mathbf{f}_1^{(j)}(x) \odot \mathbf{A}_1^{(j)}(x), \mathbf{f}_2^{(j)}(x) \odot \mathbf{A}_2^{(j)}(x), \dots, \mathbf{f}_{s_j}^{(j)}(x) \odot \mathbf{A}_{s_j}^{(j)}(x)) \in \mathbb{G}^{(j)}.$$

For each $j \geq 1$, we shall view the set $T^{(j)}$ as a probability space, where each sample of $T^{(j)}$ is chosen with equal probability. Further, for each sample $\mathbf{A}^{(j)}(x)$ in the probability space $T^{(j)}$, we see, by Theorem 7.2.1, that the code

$$\mathcal{C}_{\mathbf{A}^{(j)}} = \left\{ \mathbf{f}^{(j)}(x) \diamond \mathbf{A}^{(j)}(x) : \mathbf{f}^{(j)}(x) \in \mathcal{F}^{(j)} \right\}$$

is a random σ -self-dual MT additive code of length $\mathbf{m}_j \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{q^t}$ with rate $R(\mathcal{C}_{\mathbf{A}^{(j)}}) = \frac{1}{2}$.

Theorem 7.2.2. *Let $\{\alpha_j\}_{j \geq i}$ be a strictly increasing infinite sequence of positive*

integers satisfying $\alpha_j \geq \eta + 1$. If δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$, then we have

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) > \delta \right) \right\} = 1.$$

Proof. As $h_{q^t}(\delta) < \frac{1}{2\ell t}$, we have $\frac{1}{2\ell t} - h_{q^t}(\delta) > 0$. By Lemma 7.2.7, we see that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} \leq \begin{cases} \left(\frac{q^{-\ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{1 - q^{-2}} \right) \prod_{\nu_j=2}^{s_j} \left(\frac{q^{-d_{\nu_j}^{(j)} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu_j}^{(j)}})(1 + q^{-\frac{d_{\nu_j}^{(j)}}{2}})} \right) \\ \text{if either } \sigma = \gamma \text{ or } \sigma = * \text{ and } q \text{ is even;} \\ \left(\frac{q^{\ell t h_{q^t}(\delta)}}{2(1 - q^{-1})} \right) \prod_{\nu_j=2}^{s_j} \left(\frac{q^{-d_{\nu_j}^{(j)} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu_j}^{(j)}})(1 + q^{-\frac{d_{\nu_j}^{(j)}}{2}})} \right) \text{ if } \sigma \in \{0, *\} \\ \text{with either } \ell \text{ being even and } q \equiv 1 \pmod{4} \text{ or } \ell \\ \text{being even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or} \\ \ell \text{ being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \left(\frac{q^{\ell t h_{q^t}(\delta)}}{1 - q^{-1}} \right) \prod_{\nu_j=2}^{s_j} \left(\frac{q^{-d_{\nu_j}^{(j)} \ell t(\frac{1}{2\ell t} - h_{q^t}(\delta))}}{(1 - q^{-d_{\nu_j}^{(j)}})(1 + q^{-\frac{d_{\nu_j}^{(j)}}{2}})} \right) \\ \text{if } \sigma = 0 \text{ and both } \ell t, q \text{ are even.} \end{cases}$$

Since $\lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, we see that $\lim_{j \rightarrow \infty} \{d_2^{(j)}\} = \lim_{j \rightarrow \infty} \{vp^{\alpha_j - \eta}\} = \infty$. This implies that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} = 0,$$

which further implies that

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) > \delta \right) \right\} = 1 - \lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) \leq \delta \right) \right\} = 1.$$

□

In the following theorem, we show that for each $\sigma \in \{0, \gamma, *\}$, there exists an infinite sequence of σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ with rate $\frac{1}{2}$ and relative Hamming distance at least δ , where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$.

Theorem 7.2.3. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$. For $\sigma \in \{0, \gamma, *\}$, there exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of σ -self-dual MT additive*

codes $\mathcal{C}_j$'s of length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{q^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that $R_{\mathfrak{F}} = \frac{1}{2}$ and $\Delta_{\mathfrak{F}} > \delta$.

Proof. It follows immediately from Theorem [7.2.2](#). □

From the above theorem, it follows that σ -self-dual MT additive codes over $\mathbb{F}_{q^t}$ are asymptotically good for each $\sigma \in \{0, \gamma, *\}$. Further, as a consequence of the above theorem, we deduce that σ -self-dual cyclic and negacyclic additive codes over $\mathbb{F}_{q^t}$ are asymptotically good.

Corollary 7.2.1. *Let δ be a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2t}$. For $\sigma \in \{0, \gamma, *\}$, there exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of σ -self-dual cyclic (resp. negacyclic) additive codes $\mathcal{C}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{q^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that $R_{\mathfrak{F}} = \frac{1}{2}$ and $\Delta_{\mathfrak{F}} > \delta$.*

Proof. Taking $\ell = 1$ in Theorem [7.2.3](#), we get the desired result. □

Example 7.2.1. Let $q = 2$, $p = 13$, $\omega = 1$, $\ell = 1$ and $t = 2$. Here we have $v = \text{ord}_p(q) = \text{ord}_{13}(2) = 12$ and $\eta = 1$. By Corollary [7.2.1](#), we see that there exists an infinite sequence $\mathfrak{F} = \{\mathcal{C}_j\}_{j \geq 1}$ of σ -self-dual cyclic additive codes $\mathcal{C}_j$'s of length 13^{α_j} over $\mathbb{F}_4$ such that $\lim_{j \rightarrow \infty} \{13^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = \frac{1}{2}$ and $\Delta_{\mathfrak{F}} > \delta$, where δ is a positive real number satisfying $\delta < 0.0744$.

Doubly-even self-dual (linear) codes over finite fields of even characteristic (also called Type II codes) form an interesting class of self-dual (linear) codes and are useful in constructing unimodular lattices and determining modular forms [\[11, 26, 35, 48\]](#). Our next goal is to define and study doubly-even self-dual additive codes over finite fields of even characteristic, which form a special subclass of 0-self-dual additive codes and an extension of doubly-even self-dual linear codes. We will also characterize a class of doubly-even self-dual MT additive codes in terms of their constituents and show that this special class of doubly-even self-dual MT additive codes is asymptotically good using probabilistic methods and results from groups and geometry. Towards this, we study doubly-even self-dual MT additive codes over finite fields in the following section.

7.3 Doubly-even self-dual multi-twisted additive codes

To define doubly-even self-dual additive codes, we assume, throughout this section, that q is an even prime power, say $q = 2^r$, where $r \geq 1$. Here we must have $\omega_1 = \omega_2 = \dots = \omega_\ell = 1$. As $\gcd(m_i, q) = 1$ for $1 \leq i \leq \ell$, we see that $m_1, m_2, \dots, m_\ell$ are odd positive integers. We also assume, throughout this section, that $m_1 \equiv m_2 \equiv \dots \equiv m_\ell \pmod{4}$. Let us take $h_1(x) = x + 1$.

By Theorem 4 of Seroussi and Lempel [53], we see that there exists a self-dual basis (or a trace orthogonal basis) of $\mathbb{F}_{q^t}$ over $\mathbb{F}_2$, *i.e.*, there exists a basis $\mathcal{B} = \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{rt}\}$ of $\mathbb{F}_{q^t}$ over $\mathbb{F}_2$ satisfying

$$\text{Tr}_{q^t, 2}(\mathbf{e}_j \mathbf{e}_k) = \begin{cases} 1 & \text{if } j = k; \\ 0 & \text{otherwise.} \end{cases}$$

Further, each element $y \in \mathbb{F}_{q^t}$ can be uniquely expressed as $y = \sum_{j=1}^{rt} y_j \mathbf{e}_j$, where $y_j \in \mathbb{F}_2$ for $1 \leq j \leq rt$. For any element $y \in \mathbb{F}_{q^t}$, the Lee weight $wt_L^{\mathcal{B}}(y)$ associated with the basis $\mathcal{B}$ is defined as the integer sum $wt_L^{\mathcal{B}}(y) = \sum_{j=1}^{rt} y_j \in \mathbb{Z}$ (see [12]). Further, for a vector $a = (a_1, a_2, \dots, a_n) \in \mathbb{F}_{q^t}^n$, the Lee weight $wt_L^{\mathcal{B}}(a)$ associated with the basis $\mathcal{B}$ is defined as the sum

$$wt_L^{\mathcal{B}}(a) = \sum_{i=1}^n wt_L^{\mathcal{B}}(a_i).$$

Now a 0-self-dual additive code of length n over $\mathbb{F}_{q^t}$ is called a *doubly-even self-dual additive code* if the Lee weight of its every codeword is divisible by 4. We next make the following observation.

Lemma 7.3.1. *Let $\mathcal{B} = \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_{rt}\}$ be a self-dual basis of $\mathbb{F}_{q^t}$ over $\mathbb{F}_2$, and let $wt_L^{\mathcal{B}}$ denote the Lee weight function corresponding to the basis $\mathcal{B}$. Let $a = (a_1, a_2, \dots, a_n)$, $b = (b_1, b_2, \dots, b_n) \in \mathbb{F}_{q^t}^n$ be fixed, and let us define $a * b = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$. Then we have*

$$wt_L^{\mathcal{B}}(a + b) \equiv wt_L^{\mathcal{B}}(a) + wt_L^{\mathcal{B}}(b) - 2wt_L^{\mathcal{B}}(a * b) \pmod{4}.$$

Moreover, if $\langle a, b \rangle_0 = \sum_{i=1}^n \text{Tr}_{q^t, q}(a_i b_i) = 0$, then we have $wt_L^{\mathcal{B}}(a * b) \equiv 0 \pmod{2}$. As a

consequence, we have

$$wt_L^{\mathcal{B}}(a + b) \equiv wt_L^{\mathcal{B}}(a) + wt_L^{\mathcal{B}}(b) \pmod{4}.$$

Proof. To prove the result, we see, by Lemma 7.1 of Ling *et al.* [44], that

$$wt_L^{\mathcal{B}}(a + b) \equiv wt_L^{\mathcal{B}}(a) + wt_L^{\mathcal{B}}(b) - 2wt_L^{\mathcal{B}}(a * b) \pmod{4}.$$

Now for $1 \leq i \leq n$, let us write $a_i = \sum_{j=1}^{rt} a_{i,j} \mathbf{e}_j$ and $b_i = \sum_{j=1}^{rt} b_{i,j} \mathbf{e}_j$, where $a_{i,j}, b_{i,j} \in \mathbb{F}_2$ for $1 \leq j \leq rt$. For each i , we further note that

$$a_i b_i = \sum_{j=1}^{rt} \sum_{k=1}^{rt} a_{i,j} b_{i,k} \mathbf{e}_j \mathbf{e}_k = \sum_{j=1}^{rt} \sum_{k=1}^{rt} \sum_{u=1}^{rt} a_{i,j} b_{i,k} z_u^{(j,k)} \mathbf{e}_u,$$

where $\mathbf{e}_j \mathbf{e}_k = \sum_{u=1}^{rt} z_u^{(j,k)} \mathbf{e}_u$ with $z_u^{(j,k)} \in \mathbb{F}_2$ for $1 \leq u, j, k \leq rt$. Since $\text{Tr}_{q^t,2}(\mathbf{e}_u) = \text{Tr}_{q^t,2}(\mathbf{e}_u \mathbf{e}_u) = 1$, we obtain

$$\sum_{u=1}^{rt} z_u^{(j,k)} = \sum_{u=1}^{rt} z_u^{(j,k)} \text{Tr}_{q^t,2}(\mathbf{e}_u) = \text{Tr}_{q^t,2} \left(\sum_{u=1}^{rt} z_u^{(j,k)} \mathbf{e}_u \right) = \text{Tr}_{q^t,2}(\mathbf{e}_j \mathbf{e}_k) = \begin{cases} 1 & \text{if } j = k; \\ 0 & \text{otherwise.} \end{cases}$$

From this, we get $wt_L^{\mathcal{B}}(a * b) = \sum_{i=1}^n wt_L^{\mathcal{B}}(a_i b_i) = \sum_{i=1}^n \sum_{j=1}^{rt} a_{i,j} b_{i,j}$.

Now if $\langle a, b \rangle_0 = 0$, then we have $\text{Tr}_{q,2}(\langle a, b \rangle_0) = 0$, which implies that

$$\begin{aligned} \text{Tr}_{q,2}(\langle a, b \rangle_0) &= \text{Tr}_{q,2} \left(\sum_{i=1}^n \text{Tr}_{q^t,q}(a_i b_i) \right) = \sum_{i=1}^n \text{Tr}_{q^t,2}(a_i b_i) \\ &= \sum_{i=1}^n \sum_{j=1}^{rt} \sum_{k=1}^{rt} a_{i,j} b_{i,k} \text{Tr}_{q^t,2}(\mathbf{e}_j \mathbf{e}_k) = \sum_{i=1}^n \sum_{j=1}^{rt} a_{i,j} b_{i,j} = 0. \end{aligned}$$

From this, it follows that if $\langle a, b \rangle_0 = 0$, then $wt_L^{\mathcal{B}}(a * b) \equiv 0 \pmod{2}$. Consequently, we have $wt_L^{\mathcal{B}}(a + b) \equiv wt_L^{\mathcal{B}}(a) + wt_L^{\mathcal{B}}(b) \pmod{4}$. □

The following two lemmas are needed to characterize doubly-even self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$.

Lemma 7.3.2. *Let $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu$ be an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$. Suppose that the constituent $\mathcal{C}_1$ of $\mathcal{C}$ corresponds to the irreducible factor $h_1(x) = x+1$ of $x^{m_1}+1$ over $\mathbb{F}_q$. If every codeword in $\mathcal{C}$ has Lee weight divisible by 4, then the Lee weight of every codeword in $\mathcal{C}_1$ is also divisible by 4. Conversely, if each codeword in $\mathcal{C}_1$ has Lee weight divisible by 4, then the Lee weight of each codeword in $\mathcal{C}$ corresponding to the subcode $\mathcal{C}_1 \oplus \{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\}$ of $\mathcal{C}$ is also divisible by 4.*

Proof. To prove this, we first note that $\mathcal{F}_1 \simeq \mathbb{F}_q$ and $\mathbb{G}_1 \simeq (\epsilon_{1,1}\mathbb{F}_{q^t}, \epsilon_{1,2}\mathbb{F}_{q^t}, \dots, \epsilon_{1,\ell}\mathbb{F}_{q^t})$. Now let $y_1 = (y_{1,1}, y_{1,2}, \dots, y_{1,\ell}) \in \mathcal{C}_1$ be fixed. By Theorem 3.4.1, we see that the codeword $c \in \mathcal{C}$ corresponding to the element $(y_1, \mathbf{0}, \dots, \mathbf{0}) \in \mathcal{C}_1 \oplus \{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\}$ is given by $c = (c_{1,0}, c_{1,1}, \dots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \dots, c_{2,m_2-1}; \dots; c_{\ell,0}, c_{\ell,1}, \dots, c_{\ell,m_\ell-1})$, where $c_{i,j} = y_{1,i}$ for $1 \leq i \leq \ell$ and $0 \leq j \leq m_i - 1$. This implies that

$$\begin{aligned} wt_L^{\mathcal{B}}(c) &= \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(c_{i,j}) = \sum_{i=1}^{\ell} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(y_{1,i}) = \sum_{i=1}^{\ell} m_i wt_L^{\mathcal{B}}(y_{1,i}) \\ &\equiv m_1 \sum_{i=1}^{\ell} wt_L^{\mathcal{B}}(y_{1,i}) \equiv m_1 wt_L^{\mathcal{B}}(y_1) \pmod{4}. \end{aligned}$$

This shows that $wt_L^{\mathcal{B}}(c) \equiv 0 \pmod{4}$ if and only if $wt_L^{\mathcal{B}}(y_1) \equiv 0 \pmod{4}$. From this, the desired result follows. $\square$

Lemma 7.3.3. *Let $h_1(x), h_2(x), \dots, h_s(x)$ be all the distinct irreducible factors of the polynomials $x^{m_1}+1, x^{m_2}+1, \dots, x^{m_\ell}+1$ over $\mathbb{F}_q$. Let $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu$ be a 0-self-orthogonal Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$, where the constituent $\mathcal{C}_\nu$ corresponds to the polynomial $h_\nu(x)$ for $1 \leq \nu \leq s$. Suppose that there exists an integer w satisfying $1 \leq w \leq s$ and $h_w(x) \neq x+1$. Then the Lee weight of each codeword of $\mathcal{C}$ corresponding to the subcode $\{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\} \oplus \mathcal{C}_w \oplus \{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\}$ of $\mathcal{C}$ is a multiple of 4.*

Proof. To prove the result, let $y_w = (y_{w,1}, y_{w,2}, \dots, y_{w,\ell}) \in \mathcal{C}_w$ be fixed. Let

$$\hat{y}_w = \Phi_{\mathcal{B}}(y_w) = (y_{w,1}^{(1)}, y_{w,1}^{(2)}, \dots, y_{w,1}^{(t)}, y_{w,2}^{(1)}, y_{w,2}^{(2)}, \dots, y_{w,2}^{(t)}, \dots, y_{w,\ell}^{(1)}, y_{w,\ell}^{(2)}, \dots, y_{w,\ell}^{(t)}) \in \Phi_{\mathcal{B}}(\mathcal{C}_w),$$

where the map $\Phi_{\mathcal{B}}$ is as defined in Section 3.4. Further, let us define $\mathcal{T}_w = \{i : 1 \leq$

$i \leq \ell$ and $\epsilon_{w,i} = 1\}$. Then by Theorem [3.4.1](#), we see that the codeword $c \in \mathcal{C}$ corresponding to the element $(\mathbf{0}, \dots, \mathbf{0}, y_w, \mathbf{0}, \dots, \mathbf{0}) \in \{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\} \oplus \mathcal{C}_w \oplus \{\mathbf{0}\} \oplus \dots \oplus \{\mathbf{0}\}$ is given by $c = (c_{1,0}, c_{1,1}, \dots, c_{1,m_1-1}; c_{2,0}, c_{2,1}, \dots, c_{2,m_2-1}; \dots; c_{\ell,0}, c_{\ell,1}, \dots, c_{\ell,m_\ell-1})$, where for $1 \leq i \leq \ell$ and $0 \leq j \leq m_i - 1$,

$$c_{i,j} = \begin{cases} \sum_{k=1}^t \text{Tr}_{q^{d_w}, q}(y_{w,i}^{(k)} \theta_w^{-j}) \mathbf{f}_k & \text{if } i \in \mathcal{T}_w; \\ 0 & \text{otherwise.} \end{cases} \quad (7.6)$$

Now let $P(x)$ be the minimal polynomial of θ_w^{-1} over $\mathbb{F}_2$. Since $h_w(x) \neq x+1$, we have $\theta_w^{-1} \neq 1$. As a result, the number of non-zero monomials in $P(x)$ must be odd, *i.e.*, the polynomial $P(x)$ must be of the form $P(x) = 1 + x^{\kappa_1} + x^{\kappa_2} + \dots + x^{\kappa_{d-1}} \in \mathbb{F}_2[x]$, where d is an odd integer. Note that

$$1 + \theta_w^{-\kappa_1} + \theta_w^{-\kappa_2} + \dots + \theta_w^{-\kappa_{d-1}} = 0. \quad (7.7)$$

Now for $i \in \mathcal{T}_w$ and $0 \leq j \leq m_i - 1$, we see, by [\(7.6\)](#) and [\(7.7\)](#), that

$$c_{i,j} + c_{i,j+\kappa_1} + c_{i,j+\kappa_2} + \dots + c_{i,j+\kappa_{d-1}} = 0.$$

Further, for $i \in \mathcal{T}_w$ and $0 \leq j \leq m_i - 1$, let us define $f_{i,j}^{(0)} = c_{i,j}$ and $f_{i,j}^{(\mathfrak{z})} = f_{i,j}^{(\mathfrak{z}-1)} + c_{i,j+\kappa_{\mathfrak{z}}}$ for $1 \leq \mathfrak{z} \leq d-1$. We next observe that

$$\begin{aligned} d \, wt_L^{\mathcal{B}}(c) &= \sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} d \, wt_L^{\mathcal{B}}(c_{i,j}) = \sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(c_{i,j}, c_{i,j+\kappa_1}, c_{i,j+\kappa_2}, \dots, c_{i,j+\kappa_{d-1}}) \\ &= \sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(f_{i,j}^{(0)}, f_{i,j}^{(0)} + f_{i,j}^{(1)}, \dots, f_{i,j}^{(d-3)} + f_{i,j}^{(d-2)}, f_{i,j}^{(d-2)}). \end{aligned}$$

By applying Lemma [7.3.1](#), we get

$$\begin{aligned} d \, wt_L^{\mathcal{B}}(c) &\equiv 2 \sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} \left(\sum_{b_1=0}^{d-2} wt_L^{\mathcal{B}}(f_{i,j}^{(b_1)}) \right) - 2 \sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} \left(\sum_{b_2=0}^{d-3} wt_L^{\mathcal{B}}(f_{i,j}^{(b_2)} * f_{i,j}^{(b_2+1)}) \right) \pmod{4} \\ &\equiv 2 \sum_{b_1=0}^{d-2} \left(\sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(f_{i,j}^{(b_1)}) \right) - 2 \sum_{b_2=0}^{d-3} \left(\sum_{i \in \mathcal{T}_w} \sum_{j=0}^{m_i-1} wt_L^{\mathcal{B}}(f_{i,j}^{(b_2)} * f_{i,j}^{(b_2+1)}) \right) \pmod{4} \end{aligned}$$

$$\begin{aligned}
&\equiv 2 \left(wt_L^{\mathcal{B}}(c) + wt_L^{\mathcal{B}}(c + T_{\Omega}^{-\kappa_1}(c)) + \cdots + wt_L^{\mathcal{B}}(c + T_{\Omega}^{-\kappa_1}(c) + \cdots + T_{\Omega}^{-\kappa_{d-2}}(c)) \right) \\
&- 2 \left(wt_L^{\mathcal{B}}(c * (c + T_{\Omega}^{-\kappa_1}(c))) + wt_L^{\mathcal{B}}((c + T_{\Omega}^{-\kappa_1}(c)) * (c + T_{\Omega}^{-\kappa_1}(c) + T_{\Omega}^{-\kappa_2}(c))) \right. \\
&\quad + \cdots + wt_L^{\mathcal{B}}((c + T_{\Omega}^{-\kappa_1}(c) + \cdots + T_{\Omega}^{-\kappa_{d-3}}(c)) * (c + T_{\Omega}^{-\kappa_1}(c) + T_{\Omega}^{-\kappa_2}(c) \\
&\quad \left. + \cdots + T_{\Omega}^{-\kappa_{d-2}}(c))) \right) \pmod{4}. \tag{7.8}
\end{aligned}$$

Since $\mathcal{C}$ is a 0-self-orthogonal Ω -MT additive code, by Lemma 7.3.1, we note that $2wt_L^{\mathcal{B}}(z) \equiv 0 \pmod{4}$ and $2wt_L^{\mathcal{B}}(z * z') \equiv 0 \pmod{4}$ for all $z, z' \in \mathcal{C}$. From this and by (7.8), it follows that $d wt_L^{\mathcal{B}}(c) \equiv 0 \pmod{4}$. Since d is odd, we obtain $wt_L^{\mathcal{B}}(c) \equiv 0 \pmod{4}$ for all $c \in \mathcal{C}$. This proves the lemma. $\square$

In the following theorem, we identify a class of doubly-even self-dual Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_{\ell})$ over $\mathbb{F}_{q^t}$.

Theorem 7.3.1. *Let $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_{\nu}$ be a 0-self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_{\ell})$ over $\mathbb{F}_{q^t}$, where the constituent $\mathcal{C}_1(\subseteq \mathbb{G}_1)$ corresponds to the irreducible factor $h_1(x) = x + 1$ of $x^{m_i} + 1$ over $\mathbb{F}_q$ for $1 \leq i \leq \ell$. Then the code $\mathcal{C}$ is a doubly-even self-dual code over $\mathbb{F}_{q^t}$ if and only if every codeword of the constituent $\mathcal{C}_1$ has Lee weight divisible by 4.*

Proof. To prove the result, it is enough to show that the Lee weight of each codeword $c \in \mathcal{C}$ is divisible by 4 if and only if the Lee weight of each codeword $y_1 \in \mathcal{C}_1$ is divisible by 4. To do this, consider an arbitrary codeword $c \in \mathcal{C}$. As $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_{\nu}$, there exists $y_{\nu} \in \mathcal{C}_{\nu}$ for $1 \leq \nu \leq s$ such that the codeword $c \in \mathcal{C}$ corresponds to the element $y = (y_1, y_2, \dots, y_s) \in \bigoplus_{\nu=1}^s \mathcal{C}_{\nu}$. We next observe that $(y_1, y_2, \dots, y_s) = (y_1, \mathbf{0}, \dots, \mathbf{0}) + (\mathbf{0}, y_2, \mathbf{0}, \dots, \mathbf{0}) + \cdots + (\mathbf{0}, \dots, \mathbf{0}, y_s)$. Now for $1 \leq \nu \leq s$, let $x_{\nu} \in \mathcal{C}$ be the codeword corresponding to the element $(\mathbf{0}, \dots, \mathbf{0}, y_{\nu}, \mathbf{0}, \dots, \mathbf{0}) \in \{\mathbf{0}\} \oplus \cdots \oplus \{\mathbf{0}\} \oplus \mathcal{C}_{\nu} \oplus \{\mathbf{0}\} \oplus \cdots \oplus \{\mathbf{0}\}$, where x_{ν} is given by Theorem 3.4.1. Since $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_{\nu}$, we must have $c = x_1 + x_2 + \cdots + x_s$. Since $\mathcal{C}$ is a 0-self-dual Ω -MT additive code, by Lemma 7.3.1, we note that $wt_L^{\mathcal{B}}(c) \equiv \sum_{\nu=1}^s wt_L^{\mathcal{B}}(x_{\nu}) \pmod{4}$. Now by applying Lemmas 7.3.2 and 7.3.3, the desired result follows immediately. $\square$

In the next section, we will apply the above theorem to show that doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ are asymptotically good.

7.4 Doubly-even self-dual multi-twisted additive codes are asymptotically good

In this section, we study a special class of doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ and show that it is asymptotically good by applying probabilistic methods and results from groups and geometry. For this, we assume, throughout this section, that $q = 2$. Here we have $\Omega = (1, 1, \dots, 1) \in \mathbb{F}_2^\ell$. Let us fix an odd prime p such that $v = \text{ord}_p(2)$ is even, (there are several such odd primes p by Lemma 7.2.1). Let us take $m = p^\alpha$, where α is a positive integer. Let us assume that $m_1 = m_2 = \dots = m_\ell = m$ so that $n = m\ell$. As $v = \text{ord}_p(2)$, one can write $2^v = 1 + p^\eta c$, where $\eta \geq 1$ and c are integers with $\gcd(p, c) = 1$. We note, by (7.1), that $\text{ord}_{p^\alpha}(2) = vp^{\alpha-\eta}$ for all $\alpha \geq \eta + 1$. Let $x^m + 1 = x^{p^\alpha} + 1 = h_1(x)h_2(x) \cdots h_s(x)$ be the irreducible factorization of the polynomial $x^m + 1$ over $\mathbb{F}_2$, where $h_1(x) = x + 1$. Let $d_\nu = \deg h_\nu(x)$ for $1 \leq \nu \leq s$. We recall, from Section 3.3, that $\mathcal{R} \simeq \bigoplus_{\nu=1}^s \mathbb{W}_\nu^\ell = \bigoplus_{\nu=1}^s \mathbb{G}_\nu = \mathbb{G}$, where $\mathbb{W}_\nu = \frac{\mathbb{F}_{2^t}[x]}{\langle h_\nu(x) \rangle}$ and $\mathcal{F}_\nu = \frac{\mathbb{F}_2[x]}{\langle h_\nu(x) \rangle} \simeq \mathbb{F}_{2^{d_\nu}}$ for $1 \leq \nu \leq s$. Let ξ be a primitive m -th root of unity in some extension of $\mathbb{F}_2$, and let $h_2(x)$ be the minimal polynomial of ξ over $\mathbb{F}_2$. Here we note that $d_2 = \deg h_2(x) = \text{ord}_m(2) = \text{ord}_{p^\alpha}(2) = vp^{\alpha-\eta}$ is an even integer. From this, we see that all the irreducible factors $h_1(x), h_2(x), \dots, h_s(x)$ of $x^m + 1$ over $\mathbb{F}_2$ are self-reciprocal, $d_1 = \deg h_1(x) = 1$ and that the integer $d_\nu = \deg h_\nu(x)$ is even for $2 \leq \nu \leq s$.

We next see, by (4.5) and (4.6), that every MT additive code $\mathcal{C}$ of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ and its 0-dual code $\mathcal{C}^{\perp_0}$ can be uniquely expressed as

$$\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu \quad \text{and} \quad \mathcal{C}^{\perp_0} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu^{\perp_0},$$

where $\mathcal{C}_\nu$ is an $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ and $\mathcal{C}_\nu^{\perp_0}$ is the orthogonal complement of $\mathcal{C}_\nu$ with respect to the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0 \upharpoonright_{\mathbb{G}_\nu \times \mathbb{G}_\nu}$ for $1 \leq \nu \leq s$. Further, by Theorem 4.4.1(b), we see that $\mathcal{C}$ is a 0-self-dual code if and only if $\mathcal{C}_\nu = \mathcal{C}_\nu^{\perp_0}$, i.e., $\mathcal{C}_\nu$ is a 0-self-dual $\mathcal{F}_\nu$ -subspace of $\mathbb{G}_\nu$ for $1 \leq \nu \leq s$ and $\dim_{\mathcal{F}_\nu} \mathbb{G}_\nu = \ell t$ is an even integer. In view of this, we assume, throughout this section, that ℓt is an even integer. In the following theorem, we derive a necessary and sufficient condition for

the existence of a doubly-even self-dual MT additive code over $\mathbb{F}_{2^t}$.

Theorem 7.4.1. *There exists a doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ if and only if $\ell t \equiv 0 \pmod{8}$.*

Proof. Since the integer ℓt is even, we see, by Theorem 5.3.1, that there exists a 0-self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$. Now let $\mathcal{C} = \bigoplus_{\nu=1}^s \mathcal{C}_\nu$ be a 0-self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$, where the constituent $\mathcal{C}_1 (\subseteq \mathbb{G}_1)$ corresponds to the irreducible factor $h_1(x) = x + 1$ of $x^m + 1$ over $\mathbb{F}_2$. As $d_1 = \deg h_1(x) = 1$, we see that $\mathcal{F}_1 \simeq \mathbb{F}_2$ and $\mathbb{G}_1 \simeq \mathbb{F}_{2^\ell}^\ell$. Now for all $A_1 \in \mathbb{G}_1$, one can easily see that $[A_1, A_1]_0 \equiv wt_L^{\mathcal{B}}(A_1) \pmod{2}$. Further, by Theorem 7.3.1, we observe that $\mathcal{C}$ is a doubly-even self-dual code if and only if the Lee weight of each codeword of $\mathcal{C}_1$ is a multiple of 4.

Now let us define the set

$$\mathbb{M}_1 = \{A_1 \in \mathbb{G}_1 : [A_1, A_1]_0 = 0\} = \{A_1 \in \mathbb{G}_1 : wt_L^{\mathcal{B}}(A_1) \text{ is even}\}.$$

It is easy to observe that the set $\mathbb{M}_1$ is an $(\ell t - 1)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ containing the element $\mathbf{1} = \underbrace{(1, 1, \dots, 1)}_{\ell \text{ times}} \in \mathbb{G}_1$. Further, the space $(\mathbb{M}_1, [\cdot, \cdot]_0 \upharpoonright_{\mathbb{M}_1 \times \mathbb{M}_1})$ can be viewed as a quadratic space $(\mathbb{M}_1, \mathcal{Q}_1)$ with respect to the quadratic map $\mathcal{Q}_1 : \mathbb{M}_1 \rightarrow \mathcal{F}_1$, defined as

$$\mathcal{Q}_1(A_1) = \frac{1}{2} wt_L^{\mathcal{B}}(A_1) \pmod{2} \text{ for all } A_1 \in \mathbb{M}_1.$$

Here one can easily observe that $\mathbf{1} \in \mathbb{M}_1 \cap \mathbb{M}_1^{\perp_0}$. Now let $\widehat{\mathbb{M}}_1$ be an $(\ell t - 2)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ satisfying $\mathbf{1} \notin \widehat{\mathbb{M}}_1$, which gives $\mathbb{M}_1 = \widehat{\mathbb{M}}_1 \oplus \langle \mathbf{1} \rangle$. Further, it is easy to observe that there exists an element $z_1 \in \widehat{\mathbb{M}}_1^{\perp_0} \setminus \mathbb{M}_1$ satisfying $\mathbb{G}_1 = \widehat{\mathbb{M}}_1 \oplus \langle \mathbf{1} \rangle \oplus \langle z_1 \rangle$. From this, we note that any element of $\mathbb{G}_1$ is of the form $A_1 + a\mathbf{1} + bz_1$, where $A_1 \in \widehat{\mathbb{M}}_1$ and $a, b \in \mathcal{F}_1$. Further, we see that $[A_1 + a\mathbf{1} + bz_1, A_1 + a\mathbf{1} + bz_1]_0 = 0$ if and only if $b = 0$. This implies that each 0-self-orthogonal $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ must be contained in $\widehat{\mathbb{M}}_1 \oplus \langle \mathbf{1} \rangle$. Let $\mathcal{Q}'_1$ be the restriction of $\mathcal{Q}_1$ to $\widehat{\mathbb{M}}_1$. We next observe that $(\widehat{\mathbb{M}}_1, \mathcal{Q}'_1)$ is a non-defective quadratic space over $\mathcal{F}_1$. Since $\dim_{\mathcal{F}_1} \widehat{\mathbb{M}}_1 = (\ell t - 2)$ is even, we further see, by Theorem 2.2.8, that the quadratic space $(\widehat{\mathbb{M}}_1, \mathcal{Q}'_1)$ has Witt index at most $\frac{\ell t - 2}{2}$. From this, it follows that any 0-self-dual $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ must be

contained in $\widehat{\mathbb{M}}_1 \oplus \langle \mathbf{1} \rangle$ but not in $\widehat{\mathbb{M}}_1$. One can easily observe that there exists a basis $\{A_1^{(1)} + a_1 \mathbf{1}, A_1^{(2)} + a_2 \mathbf{1}, \dots, A_1^{(\frac{\ell t}{2})} + a_{\frac{\ell t}{2}} \mathbf{1}\}$ of a 0-self-dual $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ satisfying $wt_L^{\mathcal{B}}(A_1^{(h)} + a_h \mathbf{1}) \equiv 0 \pmod{4}$ for $1 \leq h \leq \frac{\ell t}{2}$ if and only if the Witt index of the quadratic space $(\widehat{\mathbb{M}}_1, \mathcal{Q}'_1)$ is $\frac{\ell t - 2}{2}$. Now working as in Proposition 3 of Wood [69], we see that the quadratic space $(\widehat{\mathbb{M}}_1, \mathcal{Q}'_1)$ has Witt index $\frac{\ell t - 2}{2}$ if and only if $\ell t \equiv 0 \pmod{8}$. From this, the desired result follows. $\square$

In view of the above theorem, we assume, throughout this section, that $\ell t \equiv 0 \pmod{8}$. So there always exists a doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$. We next recall, from Section 7.2, that

$$T_\nu = \left\{ \mathbf{A}_\nu(x) \in \mathbb{G}_\nu^{\frac{\ell t}{2}} : \mathcal{C}_{\mathbf{A}_\nu} = \mathcal{C}_{\mathbf{A}_\nu}^{\perp_\sigma} \right\} \text{ for } 2 \leq \nu \leq s.$$

Now let us define the sets

$$\mathfrak{T}_1 = \left\{ \mathbf{A}_1(x) \in \mathbb{G}_1^{\frac{\ell t}{2}} : \mathcal{C}_{\mathbf{A}_1} = \mathcal{C}_{\mathbf{A}_1}^{\perp_0} \text{ and } wt_L^{\mathcal{B}}(A_1^{(h)}) \equiv 0 \pmod{4} \text{ for } 1 \leq h \leq \frac{\ell t}{2} \right\}$$

and

$$\mathfrak{T} = \mathfrak{T}_1 \oplus T_2 \oplus \dots \oplus T_s.$$

Furthermore, for

$$\mathbf{A}(x) = (\mathbf{A}_1(x), \mathbf{A}_2(x), \dots, \mathbf{A}_s(x)) \in \mathfrak{T}$$

and

$$\mathbf{f}(x) = (\mathbf{f}_1(x), \mathbf{f}_2(x), \dots, \mathbf{f}_s(x)) \in \mathcal{F},$$

let us define

$$\mathbf{f}(x) \diamond \mathbf{A}(x) = (\mathbf{f}_1(x) \odot \mathbf{A}_1(x), \mathbf{f}_2(x) \odot \mathbf{A}_2(x), \dots, \mathbf{f}_s(x) \odot \mathbf{A}_s(x)) \in \mathbb{G}.$$

Theorem 7.4.2. *For $\mathbf{A}(x) \in \mathfrak{T}$, the set*

$$\mathcal{C}_{\mathbf{A}} = \{\mathbf{f}(x) \diamond \mathbf{A}(x) : \mathbf{f}(x) \in \mathcal{F}\} \tag{7.9}$$

is doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ with rate $R(\mathcal{C}_{\mathbf{A}}) = \frac{1}{2}$.

Proof. Working as in Theorem 7.2.1, we see that the code $\mathcal{C}_{\mathbf{A}}$ is a 0-self-dual MT-additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ with rate $\frac{1}{2}$. Since $\mathbf{A}_1(x) \in \mathfrak{T}_1$, we note that $wt_L^{\mathcal{B}}(c_1) \equiv 0 \pmod{4}$ for all $c_1 \in \mathcal{C}_{\mathbf{A}_1}$, which, by Theorem 7.3.1, implies that the code $\mathcal{C}_{\mathbf{A}}$ is a doubly-even self-dual code over $\mathbb{F}_{2^t}$. From this, the desired result follows. $\square$

Now to study the asymptotic behaviour of relative Hamming distances of doubly-even self-dual MT additive codes of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$, we shall view the set $\mathfrak{T}$ as a probability space, where each sample of $\mathfrak{T}$ is chosen with equal probability. Here it is easy to note that $|\mathfrak{T}| = |\mathfrak{T}_1| \prod_{\nu=2}^s |T_{\nu}|$. In the following lemma, we explicitly determine the size of the probability space $\mathfrak{T}$.

Lemma 7.4.1. *We have*

$$|\mathfrak{T}| = 2^{\frac{\ell t - 2}{2}} \prod_{h=1}^{\frac{\ell t}{2} - 1} 2^h (2^{\frac{\ell t - 2h}{2}} - 1) (2^{\frac{\ell t - 2h - 2}{2}} + 1) \prod_{\nu=2}^s \left(\prod_{h=0}^{\frac{\ell t}{2} - 1} 2^{d_{\nu} h} (2^{\frac{d_{\nu}(\ell t - 2h - 1)}{2}} + 1) (2^{\frac{d_{\nu}(\ell t - 2h)}{2}} - 1) \right).$$

Proof. To prove the result, we observe that the number $|\mathfrak{T}_1|$ is equal to the number of all possible ordered bases of 0-self-dual $\mathcal{F}_1$ -subspaces of $\mathbb{G}_1$ whose each codeword has Lee weight a multiple of 4. Moreover, for $2 \leq \nu \leq s$, the number $|T_{\nu}|$ is equal to the number of all ordered bases of 0-self-dual $\mathcal{F}_{\nu}$ -subspaces of $\mathbb{G}_{\nu}$. Now we shall distinguish the following two cases: **I.** $\nu = 1$ and **II.** $2 \leq \nu \leq s$.

I. First let $\nu = 1$. Here we have $d_1 = 1$, $\mathcal{F}_1 \simeq \mathbb{F}_2$ and $\mathbb{G}_1 \simeq \mathbb{F}_{2^{\ell}}$. From the proof of Theorem 7.4.1, we recall that the set

$$\mathbb{M}_1 = \{A_1 \in \mathbb{G}_1 : [A_1, A_1]_0 = 0\} = \{A_1 \in \mathbb{G}_1 : wt_L^{\mathcal{B}}(A_1) \text{ is even}\}$$

is an $(\ell t - 1)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ containing the element $\mathbf{1} = \underbrace{(1, 1, \dots, 1)}_{\ell \text{ times}} \in \mathbb{G}_1$ and satisfying $\mathbf{1} \in \mathbb{M}_1 \cap \mathbb{M}_1^{\perp_0}$. We also recall that the set $\widehat{\mathbb{M}}_1$

is an $(\ell t - 2)$ -dimensional $\mathcal{F}_1$ -subspace of $\mathbb{G}_1$ satisfying $\mathbf{1} \notin \widehat{\mathbb{M}}_1$ and that there exists an element $z_1 \in \widehat{\mathbb{M}}_1^{\perp_0} \setminus \mathbb{M}_1$ satisfying $\mathbb{G}_1 = \widehat{\mathbb{M}}_1 \oplus \langle \mathbf{1} \rangle \oplus \langle z_1 \rangle$. Working as in the proof of Theorem 7.4.1, we see that the space $(\widehat{\mathbb{M}}_1, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathbb{M}}_1 \times \widehat{\mathbb{M}}_1})$ can be viewed as a non-defective quadratic space $(\widehat{\mathbb{M}}_1, \mathcal{Q})$ over $\mathbb{F}_2$ with respect to the

quadratic map $\mathcal{Q} : \widehat{\mathbb{M}}_1 \rightarrow \mathbb{F}_2$, defined as

$$\mathcal{Q}(A_1) = \frac{1}{2} wt_L^{\mathcal{B}}(A_1) \pmod{2} \text{ for all } A_1 \in \widehat{\mathbb{M}}_1.$$

We next see, by Theorem 2.2.8, that the quadratic space $(\widehat{\mathbb{M}}_1, \mathcal{Q})$ has dimension $(\ell t - 2)$ and Witt index $\frac{\ell t - 2}{2}$ over $\mathbb{F}_2$. Now working as in the proof of Case I of Lemma 7.2.3 and applying Theorems 2.2.9(c) and 2.2.10, we obtain

$$|\mathfrak{T}_1| = 2^{\frac{\ell t - 2}{2}} \prod_{h=1}^{\frac{\ell t}{2} - 1} 2^h (2^{\frac{\ell t - 2h}{2}} - 1) (2^{\frac{\ell t - 2h - 2}{2}} + 1).$$

II. For $2 \leq \nu \leq s$, we see, by Lemma 7.2.3, that

$$|T_\nu| = \prod_{h=0}^{\frac{\ell t}{2} - 1} 2^{d_\nu h} (2^{\frac{d_\nu(\ell t - 2h - 1)}{2}} + 1) (2^{\frac{d_\nu(\ell t - 2h)}{2}} - 1).$$

This completes the proof of the lemma. □

For each sample $\mathbf{A}(x)$ in the probability space $\mathfrak{T}$, we see, by Theorem 7.4.2, that the code $\mathcal{C}_{\mathbf{A}}$ (as defined by (7.9)) is a random doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ with rate $R(\mathcal{C}_{\mathbf{A}}) = \frac{1}{2}$. The relative Hamming distance $\Delta(\mathcal{C}_{\mathbf{A}}) = \frac{wt(\mathcal{C}_{\mathbf{A}})}{m\ell}$ of the random code $\mathcal{C}_{\mathbf{A}}$ is a random variable over the probability space $\mathfrak{T}$, where each sample is chosen with equal probability. We will now study the asymptotic behaviour of the probability $\Pr(\Delta(\mathcal{C}_{\mathbf{A}}) > \delta)$, where δ is a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$.

Lemma 7.4.2. *For a non-zero $\mathbf{f}(x) \in \mathcal{F}$, let $B(x) \in I_{\mathbf{f}}$ be fixed, (here $I_{\mathbf{f}}$ is as defined by (7.4)). We have*

$$\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x)) \leq 2^{\frac{-(\ell t - 2)}{2}} \prod_{\nu=2}^s \left(\frac{2^{\frac{-d_\nu(\ell t + 1)}{2}}}{(1 - 2^{-d_\nu})(1 + 2^{\frac{-d_\nu}{2}})} \right),$$

where the element $\mathbf{A}(x)$ runs over the probability space $\mathfrak{T}$ in the probability $\Pr(\mathbf{f}(x) \diamond \mathbf{A}(x) = B(x))$.

Proof. Working as in Lemma 7.2.5 and applying Lemma 7.4.1, the result follows immediately. $\square$

From now on, let δ be a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$. Corresponding to a given $\mathbf{f}(x) \in \mathcal{F}$ and samples $\mathbf{A}(x) \in \mathfrak{T}$, let us define the *indicator random variable* $\mathcal{Z}_{\mathbf{f}}$ as

$$\mathcal{Z}_{\mathbf{f}} = \begin{cases} 1 & \text{if } 0 < \widehat{wt}(\mathbf{f}(x) \diamond \mathbf{A}(x)) \leq \delta; \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\mathcal{Z}_{\mathbf{f}}$ is a Bernoulli random variable defined on the probability space $\mathfrak{T}$ and $\mathcal{Z}_{\mathbf{0}} = 0$.

Lemma 7.4.3. *For a non-zero element $\mathbf{f}(x) \in \mathcal{F}$, let $E(\mathcal{Z}_{\mathbf{f}})$ denote the expectation of the indicator random variable $\mathcal{Z}_{\mathbf{f}}$ defined on the probability space $\mathfrak{T}$. We have*

$$E(\mathcal{Z}_{\mathbf{f}}) \leq 2^{-\ell t(\frac{1}{2} - \frac{1}{\ell t} - h_{2^t}(\delta))} \prod_{\nu=2}^s \left(\frac{2^{-d_{\nu}\ell t(\frac{1}{2} + \frac{1}{2\ell t} - h_{2^t}(\delta))}}{(1 - 2^{-d_{\nu}})(1 + 2^{-\frac{d_{\nu}}{2}})} \right).$$

Proof. Working as in Lemma 7.2.6 and applying Lemmas 7.2.4 and 7.4.2, the result follows immediately. $\square$

Lemma 7.4.4. *Let δ be a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$. For $\mathbf{A}(x) \in \mathfrak{T}$, let $\mathcal{C}_{\mathbf{A}}$ be the corresponding doubly-even self-dual MT additive code of length $m\ell$ and block length m over $\mathbb{F}_{2^t}$ as defined by (7.9). We have*

$$\Pr(\Delta(\mathcal{C}_{\mathbf{A}}) \leq \delta) \leq 2^{(1+\ell t h_{2^t}(\delta))} \prod_{\nu=2}^s \left(\frac{2^{-d_{\nu}\ell t(\frac{1}{2\ell t} - h_{2^t}(\delta))}}{(1 - 2^{-d_{\nu}})(1 + 2^{-\frac{d_{\nu}}{2}})} \right).$$

Proof. Working as in Lemma 7.2.7 and applying Lemma 7.4.3, we get the desired result. $\square$

Now let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$ for all $j \geq 1$. Let us define $\mathbf{m}_j = p^{\alpha_j}$ for $j \geq 1$. Note that $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$. Now let us define the sets

$$\mathfrak{T}_1^{(j)} = \left\{ \mathbf{A}_1^{(j)}(x) \in (\mathbb{G}_1^{(j)})^{\frac{\ell t}{2}} : \mathcal{C}_{\mathbf{A}_1^{(j)}} = \mathcal{C}_{\mathbf{A}_1^{(j)}}^{\perp_0} \text{ \& } wt_L^{\mathcal{B}}(A_1^{(j,h)}(x)) \equiv 0 \pmod{4} \text{ for } 1 \leq h \leq \frac{\ell t}{2} \right\}$$

and

$$\mathfrak{T}^{(j)} = \mathfrak{T}_1^{(j)} \oplus T_2^{(j)} \oplus \cdots \oplus T_{s_j}^{(j)},$$

where the set $T_{\nu_j}^{(j)}$ is as defined by (7.5) for $2 \leq \nu_j \leq s_j$. Furthermore, for

$$\mathbf{A}^{(j)}(x) = \left(\mathbf{A}_1^{(j)}(x), \mathbf{A}_2^{(j)}(x), \dots, \mathbf{A}_{s_j}^{(j)}(x) \right) \in \mathfrak{T}^{(j)}$$

and

$$\mathbf{f}^{(j)}(x) = \left(\mathbf{f}_1^{(j)}(x), \mathbf{f}_2^{(j)}(x), \dots, \mathbf{f}_{s_j}^{(j)}(x) \right) \in \mathcal{F}^{(j)},$$

let us define

$$\mathbf{f}^{(j)}(x) \diamond \mathbf{A}^{(j)}(x) = \left(\mathbf{f}_1^{(j)}(x) \odot \mathbf{A}_1^{(j)}(x), \mathbf{f}_2^{(j)}(x) \odot \mathbf{A}_2^{(j)}(x), \dots, \mathbf{f}_{s_j}^{(j)}(x) \odot \mathbf{A}_{s_j}^{(j)}(x) \right) \in \mathbb{G}^{(j)}.$$

For each $j \geq 1$, we shall view the set $\mathfrak{T}^{(j)}$ as a probability space, where each sample of $\mathfrak{T}^{(j)}$ is chosen with equal probability. Further, for each sample $\mathbf{A}^{(j)}(x)$ in the probability space $\mathfrak{T}^{(j)}$, we see, by Theorem 7.4.2, that the code

$$\mathcal{C}_{\mathbf{A}^{(j)}} = \left\{ \mathbf{f}^{(j)}(x) \diamond \mathbf{A}^{(j)}(x) : \mathbf{f}^{(j)}(x) \in \mathcal{F}^{(j)} \right\}$$

is a random doubly-even self-dual MT additive code of length $\mathbf{m}_j \ell$ and block length $\mathbf{m}_j$ over $\mathbb{F}_{2^t}$ with rate $R(\mathcal{C}_{\mathbf{A}^{(j)}}) = \frac{1}{2}$.

Theorem 7.4.3. *Let $\{\alpha_j\}_{j \geq 1}$ be a strictly increasing infinite sequence of positive integers satisfying $\alpha_j \geq \eta + 1$. If δ is a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$, then we have*

$$\lim_{j \rightarrow \infty} \left\{ \Pr \left(\Delta(\mathcal{C}_{\mathbf{A}^{(j)}}) > \delta \right) \right\} = 1.$$

Proof. Working as in Theorem 7.2.2 and applying Lemma 7.4.4 and using the fact that $\lim_{j \rightarrow \infty} \{d_2^{(j)}\} = \lim_{j \rightarrow \infty} \{vp^{\alpha_j - \eta}\} = \infty$, the desired result follows immediately. $\square$

In the following theorem, we show that there exists an infinite sequence of doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ with rate $\frac{1}{2}$ and relative Hamming distance at least δ , where δ is a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$.

Theorem 7.4.4. *Let δ be a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2\ell t}$. There exists an infinite sequence $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of doubly-even self-dual MT additive codes $\mathcal{D}_j$'s of*

length $\mathbf{m}_j \ell = p^{\alpha_j} \ell$ and block length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{2^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that $R_{\mathfrak{G}} = \frac{1}{2}$ and $\Delta_{\mathfrak{G}} > \delta$.

Proof. It follows immediately from Theorem [7.4.3](#) □

The above theorem shows that doubly-even self-dual MT additive codes over $\mathbb{F}_{2^t}$ are asymptotically good. Further, as a consequence of the above theorem, we deduce that doubly-even self-dual cyclic additive codes over $\mathbb{F}_{2^t}$ are asymptotically good.

Corollary 7.4.1. *Let δ be a positive real number satisfying $h_{2^t}(\delta) < \frac{1}{2^t}$. There exists an infinite sequence $\mathfrak{G} = \{\mathcal{D}_j\}_{j \geq 1}$ of doubly-even self-dual cyclic additive codes $\mathcal{D}_j$'s of length $\mathbf{m}_j = p^{\alpha_j}$ over $\mathbb{F}_{2^t}$ with $\lim_{j \rightarrow \infty} \{\mathbf{m}_j\} = \lim_{j \rightarrow \infty} \{p^{\alpha_j}\} = \infty$, such that $R_{\mathfrak{G}} = \frac{1}{2}$ and $\Delta_{\mathfrak{G}} > \delta$.*

Proof. The desired result follows on taking $\ell = 1$ in Theorem [7.4.4](#) □

Example 7.4.1. Let $q = 2$, $p = 11$, $\omega = 1$, $\ell = 2$ and $t = 4$. Here we have $v = \text{ord}_p(q) = \text{ord}_{11}(2) = 10$ and $\eta = 1$. By Theorem [7.4.4](#), we see that there exists an infinite sequence $\mathfrak{F} = \{\mathcal{D}_j\}_{j \geq 1}$ of doubly-even self-dual MT additive codes $\mathcal{D}_j$'s of length $2 \cdot (11)^{\alpha_j}$ and block lengths 11^{α_j} over $\mathbb{F}_{2^4}$ respectively, such that $\lim_{j \rightarrow \infty} \{11^{\alpha_j}\} = \infty$, $R_{\mathfrak{F}} = \frac{1}{2}$ and $\Delta_{\mathfrak{F}} > \delta$, where δ is a positive real number satisfying $\delta < 0.0232$.

In the next chapter, we will define a new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, which is a generalization of a special class of MT additive codes over finite fields and an extension of linear quasi-Abelian codes over finite fields introduced and studied by Wasan [\[67\]](#). We will provide a canonical form decomposition of these codes and study their dual codes with respect to ordinary, Hermitian and $*$ trace bilinear forms. We will apply the results on the geometry of symplectic, unitary and orthogonal spaces to enumerate all self-orthogonal, self-dual and additive codes with complementary duals (or ACD codes) belonging to the family of additive quasi-abelian codes over finite fields.

8

Additive quasi-Abelian codes over finite fields and their dual codes

8.1 Introduction

In this chapter, we define and study a new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, which is a generalization of a special class of MT additive codes over finite fields and an extension of linear QA codes over finite fields introduced by Wasan [67]. We study the algebraic structures of these codes and their dual codes with respect to ordinary, Hermitian, and $*$ trace bilinear forms. We further derive necessary and sufficient conditions under which an additive QA code is (i) self-orthogonal (ii) self-dual and (iii) additive code with complementary dual (or an ACD code). We also derive necessary and sufficient conditions for the existence of a self-dual additive QA code. Besides this, we provide enumeration formulae for all self-orthogonal, self-dual and ACD additive QA codes over finite

fields. We also list several MDS and almost MDS codes belonging to the family of additive QA codes.

Throughout this chapter, let q be a prime power, $t \geq 2$ be an integer, $\mathbb{F}_{q^t}$ be the finite field of order q^t , and let H be an additive Abelian group of order m , where $\gcd(m, q) = 1$. This chapter is structured as follows: In Section 8.2, we present some basic results on group algebras and group codes over finite fields. In Section 8.3, we define and study additive H -quasi-Abelian (H -QA) codes over $\mathbb{F}_{q^t}$ and their dual codes by placing ordinary, Hermitian and $*$ trace bilinear forms. In Section 8.4, we provide canonical decompositions of additive H -QA codes $\mathbb{F}_{q^t}$ and their dual codes with respect to the aforementioned trace bilinear forms (Theorems 8.4.1 and 8.4.2). In Section 8.5, we provide necessary and sufficient conditions under which an additive H -QA code over $\mathbb{F}_{q^t}$ is (i) self-orthogonal, (ii) self-dual and (iii) ACD code (Theorem 8.5.1). We also derive necessary and sufficient conditions for the existence of a self-dual additive H -QA code over $\mathbb{F}_{q^t}$ (Theorem 8.5.2). In Section 8.6, we obtain explicit enumeration formulae for all self-orthogonal, self-dual and ACD additive H -QA codes over $\mathbb{F}_{q^t}$ in terms of the parameters r_1 , r_2 and r_3 whose values depend on q and the structure of the group H (Theorems 8.6.1, 8.6.2 and 8.6.3). We also derive formulae to determine the parameters r_1 , r_2 and r_3 when H is an arbitrary finite Abelian group (Theorems 8.7.2 and 8.7.3). In Section 8.8, we list several MDS and almost MDS codes belonging to the class of 1-generator additive H -QA codes over $\mathbb{F}_{q^t}$ (Table 8.1).

8.2 Some preliminaries

Throughout this chapter, let $\mathbb{F}_q$ denote the finite field of order q , and let G denote a finite additive group of order n . Let us consider the set

$$\mathbb{F}_q[G] = \left\{ \sum_{g \in G} a_g y^g : a_g \in \mathbb{F}_q \right\},$$

where y is an indeterminate. Note that any two elements $\sum_{g \in G} a_g y^g$ and $\sum_{g \in G} b_g y^g$ in $\mathbb{F}_q[G]$ are equal if and only if $a_g = b_g$ for all $g \in G$. Let us define addition and

multiplication operations on $\mathbb{F}_q[G]$ as

$$\sum_{g \in G} a_g y^g + \sum_{g \in G} b_g y^g = \sum_{g \in G} (a_g + b_g) y^g$$

and

$$\left(\sum_{g \in G} a_g y^g \right) \left(\sum_{h \in G} b_h y^h \right) = \sum_{g, h \in G} a_g b_h y^{g+h}$$

for all $\sum_{g \in G} a_g y^g, \sum_{g \in G} b_g y^g \in \mathbb{F}_q[G]$. Under these operations, the set $\mathbb{F}_q[G]$ forms a ring with unity as well as an n -dimensional vector space over $\mathbb{F}_q$ with the set $\{y^g : g \in G\}$ as a basis. In fact, the set $\mathbb{F}_q[G]$ forms an algebra over $\mathbb{F}_q$ and is called the group algebra of G over $\mathbb{F}_q$. This gives rise to an $\mathbb{F}_q$ -linear vector space isomorphism from $\mathbb{F}_q[G]$ onto $\mathbb{F}_q^n$, defined as

$$\sum_{g \in G} a_g y^g \mapsto (a_g)_{g \in G} \quad \text{for all} \quad \sum_{g \in G} a_g y^g \in \mathbb{F}_q[G].$$

Further, the group algebra $\mathbb{F}_q[G]$ is Abelian if and only if the group G is Abelian.

Now a *group code* of G over $\mathbb{F}_q$ is defined as a left (*resp.* right) ideal of $\mathbb{F}_q[G]$. Next, let H be a subgroup of G of order m and index ℓ in G , which gives $n = m\ell$. Let $\mathbb{F}_q[H]$ denote the group algebra of H over $\mathbb{F}_q$. The group algebra $\mathbb{F}_q[G]$ can also be viewed as a left (*resp.* right) $\mathbb{F}_q[H]$ -module. An *H-quasi-group (H-QG) code* of length $m\ell$ and index ℓ over $\mathbb{F}_q$ is defined as a left (*resp.* right) $\mathbb{F}_q[H]$ -submodule of $\mathbb{F}_q[G]$. It is easy to see that the left (*resp.* right) $\mathbb{F}_q[H]$ -modules $\mathbb{F}_q[G]$ and $(\mathbb{F}_q[H])^\ell$ are isomorphic, and hence each *H-QG* code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ can also be viewed as a left (*resp.* right) $\mathbb{F}_q[H]$ -submodule of $(\mathbb{F}_q[H])^\ell$. Note that when $H = G$, *H-QG* codes coincide with group codes of G over $\mathbb{F}_q$. When G is an Abelian group, *H-QG* codes are called *H-quasi-Abelian (H-QA) codes* over $\mathbb{F}_q$ [14, 38, 50]. In particular, when H is a cyclic group, *H-QG* codes over $\mathbb{F}_q$ coincide with quasi-cyclic codes of length $m\ell$ and index ℓ over $\mathbb{F}_q$ [38, 45], which is an important and a well-studied family of error-correcting codes with nice algebraic structures and containing many record-breaker codes.

8.3 Additive quasi-Abelian codes over finite fields and their dual codes

In this chapter, we extend the family of QG codes to additive quasi-group codes. Note that the group algebra $\mathbb{F}_{q^t}[G]$ of G over $\mathbb{F}_{q^t}$ can be viewed as a left (*resp.* right) $\mathbb{F}_q[G]$ -module.

Definition 8.3.1. *An additive group code of G over $\mathbb{F}_{q^t}$ is defined as a left (*resp.* right) $\mathbb{F}_q[G]$ -submodule of $\mathbb{F}_{q^t}[G]$.*

When G is an Abelian group, additive group codes of G over $\mathbb{F}_{q^t}$ are called *additive Abelian codes*. In particular, when G is a cyclic group of order n , additive group codes of G over $\mathbb{F}_{q^t}$ coincide with cyclic additive codes of length n over $\mathbb{F}_{q^t}$ [32-34, 57, 58]. We further note that the group algebra $\mathbb{F}_{q^t}[G]$ can be viewed as a left (*resp.* right) $\mathbb{F}_q[H]$ -module.

Definition 8.3.2. *Let H be a subgroup of G of order m and index ℓ . An additive H -quasi-group (H -QG) code $\mathcal{C}$ of length $n = m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is defined as a left (*resp.* right) $\mathbb{F}_q[H]$ -submodule of $\mathbb{F}_{q^t}[G]$. Elements of the additive H -QG code $\mathcal{C}$ are called codewords.*

In particular, when $H = G$, additive H -QG codes coincide with additive group codes of G over $\mathbb{F}_{q^t}$. When G is an Abelian group, additive H -QG codes over $\mathbb{F}_{q^t}$ are called *additive H -quasi-Abelian (H -QA) codes* over $\mathbb{F}_{q^t}$.

The *Hamming distance* between two elements $a = \sum_{g \in G} a_g y^g$, $b = \sum_{g \in G} b_g y^g \in \mathbb{F}_{q^t}[G]$, denoted by $d(a, b)$, is defined as $d(a, b) = |\{g \in G : a_g \neq b_g\}|$. Further, the *Hamming weight* of an element $a = \sum_{g \in G} a_g y^g \in \mathbb{F}_{q^t}[G]$, denoted by $wt(a)$, is defined as $wt(a) = d(a, \mathbf{0}) = |\{g \in G : a_g \neq 0\}|$. If $\mathcal{C}$ is an additive H -QG code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$, then the *Hamming distance* of the code $\mathcal{C}$, denoted by $d(\mathcal{C})$, is defined as

$$d(\mathcal{C}) = \min\{d(a, b) : a, b \in \mathcal{C} \text{ and } a \neq b\},$$

while the *Hamming weight* of the code $\mathcal{C}$, denoted by $wt(\mathcal{C})$, is defined as

$$wt(\mathcal{C}) = \min\{wt(c) : \mathbf{0} \neq c \in \mathcal{C}\}.$$

It is easy to observe that $d(\mathcal{C}) = wt(\mathcal{C})$.

From now on, we assume, throughout this chapter, that the group G is Abelian. We will study dual codes of additive H -QA codes over $\mathbb{F}_{q^t}$ by placing three different trace bilinear forms on $\mathbb{F}_{q^t}[G]$, *viz.* ordinary, Hermitian and $*$ trace bilinear forms.

The *ordinary trace bilinear form* on $\mathbb{F}_{q^t}[G]$ is a map $\langle \cdot, \cdot \rangle_0 : \mathbb{F}_{q^t}[G] \times \mathbb{F}_{q^t}[G] \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_0 = \left\langle \sum_{g \in G} a_g y^g, \sum_{g \in G} b_g y^g \right\rangle_0 = \sum_{g \in G} \text{Tr}_{q^t, q}(a_g b_g)$$

for all $a = \sum_{g \in G} a_g y^g$, $b = \sum_{g \in G} b_g y^g \in \mathbb{F}_{q^t}[G]$. By Lemma 5 of Huffman [34], we see that the ordinary trace bilinear form $\langle \cdot, \cdot \rangle_0$ is a symmetric and non-degenerate bilinear form on $\mathbb{F}_{q^t}[G]$.

Next, to define the Hermitian trace bilinear form on $\mathbb{F}_{q^t}[G]$, we assume that $t \geq 2$ is an even integer. Let us write $t = 2^a z$ where $a \geq 1$ and z is an odd integer. Further, let us write $t = 2Az$, where $A = 2^{a-1}$. Note that $\mathbb{F}_{q^{2A}}$ is a subfield of $\mathbb{F}_{q^t}$. It is easy to observe that there exists a non-zero element $\gamma \in \mathbb{F}_{q^{2A}} (\subseteq \mathbb{F}_{q^t})$ such that $\gamma + \gamma^{q^A} = 0$. The *Hermitian trace bilinear form* on $\mathbb{F}_{q^t}[G]$ is a map $\langle \cdot, \cdot \rangle_\gamma : \mathbb{F}_{q^t}[G] \times \mathbb{F}_{q^t}[G] \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_\gamma = \left\langle \sum_{g \in G} a_g y^g, \sum_{g \in G} b_g y^g \right\rangle_\gamma = \sum_{g \in G} \text{Tr}_{q^t, q}(\gamma a_g b_g^{q^{t/2}})$$

for all $a = \sum_{g \in G} a_g y^g$, $b = \sum_{g \in G} b_g y^g \in \mathbb{F}_{q^t}[G]$. By Lemma 5 of Huffman [34], we see that the Hermitian trace bilinear form $\langle \cdot, \cdot \rangle_\gamma$ is an alternating, reflexive and non-degenerate bilinear form on $\mathbb{F}_{q^t}[G]$.

The $*$ trace bilinear form on $\mathbb{F}_{q^t}[G]$, is defined only when the integer t satisfies $t \not\equiv 1 \pmod{\mathfrak{p}}$, where $\mathfrak{p}$ is the characteristic of the finite field $\mathbb{F}_{q^t}$. In this case, the linear operator $\phi : \mathbb{F}_{q^t} \rightarrow \mathbb{F}_{q^t}$, defined as

$$\phi(\beta) = \beta^q + \beta^{q^2} + \cdots + \beta^{q^{t-1}} = \text{Tr}_{q^t, q}(\beta) - \beta \text{ for all } \beta \in \mathbb{F}_{q^t},$$

is an $\mathbb{F}_q$ -linear vector space isomorphism. The $*$ trace bilinear form on $\mathbb{F}_{q^t}[G]$ is a map $\langle \cdot, \cdot \rangle_* : \mathbb{F}_{q^t}[G] \times \mathbb{F}_{q^t}[G] \rightarrow \mathbb{F}_q$, defined as

$$\langle a, b \rangle_* = \left\langle \sum_{g \in G} a_g y^g, \sum_{g \in G} b_g y^g \right\rangle_* = \sum_{g \in G} \text{Tr}_{q^t, q}(a_g \phi(b_g))$$

for all $a = \sum_{g \in G} a_g y^g$, $b = \sum_{g \in G} b_g y^g \in \mathbb{F}_{q^t}[G]$. By Lemma 3.2 of Sharma and Kaur [57], we see that the $*$ trace bilinear form $\langle \cdot, \cdot \rangle_*$ is a symmetric and non-degenerate bilinear form on $\mathbb{F}_{q^t}[G]$. Moreover, when q is even, the bilinear form $\langle \cdot, \cdot \rangle_*$ is alternating.

Now we shall study dual codes of additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ with respect to these three trace bilinear forms on $\mathbb{F}_{q^t}[G]$. For this, let $\sigma \in \{0, \gamma, *\}$, and let $\mathbb{T}_\sigma$ be the set of

- (i) all integers $t \geq 2$ when $\sigma = 0$,
- (ii) all even integers $t \geq 2$ when $\sigma = \gamma$, and
- (iii) all integers $t \geq 2$ satisfying $t \not\equiv 1 \pmod{\mathfrak{p}}$ when $\sigma = *$.

Now for $\sigma \in \{0, \gamma, *\}$, let $t \in \mathbb{T}_\sigma$ be fixed from now on. Now if $\mathcal{C}$ is an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$, then its σ -dual code $\mathcal{C}^{\perp_\sigma}$ is defined as

$$\mathcal{C}^{\perp_\sigma} = \{a \in \mathbb{F}_{q^t}[G] : \langle c, a \rangle_\sigma = 0 \text{ for all } c \in \mathcal{C}\}.$$

It is easy to observe that the σ -dual code $\mathcal{C}^{\perp_\sigma}$ is also an $\mathbb{F}_q[H]$ -submodule of $\mathbb{F}_{q^t}[G]$, i.e., $\mathcal{C}^{\perp_\sigma}$ is an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. Further, the additive H -QA code $\mathcal{C}$ is said to be

- (i) σ -self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^{\perp_\sigma}$.
- (ii) σ -self-dual if it satisfies $\mathcal{C} = \mathcal{C}^{\perp_\sigma}$.
- (iii) an additive code with σ -complementary-dual (or a σ -ACD code) if it satisfies $\mathcal{C} \cap \mathcal{C}^{\perp_\sigma} = \{\mathbf{0}\}$.

To study algebraic structures of additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ and their σ -dual codes, let $\{g_1, g_2, \dots, g_\ell\}$ be a complete set of representatives of all the distinct cosets of H in G . Note that

$$G = (H + g_1) \cup (H + g_2) \cup \dots \cup (H + g_\ell) \text{ (a disjoint union),}$$

i.e., each $g \in G$ can be uniquely expressed as $g = h + g_i$ for some $h \in H$ and for some integer i satisfying $1 \leq i \leq \ell$. Thus each element $a \in \mathbb{F}_{q^t}[G]$ can be uniquely expressed as

$$a = \sum_{i=1}^{\ell} \sum_{h \in H} a_{h+g_i} y^{h+g_i} = \sum_{i=1}^{\ell} a_i(y) y^{g_i},$$

where $a_i(y) = \sum_{h \in H} a_{h+g_i} y^h \in \mathbb{F}_{q^t}[H]$ for $1 \leq i \leq \ell$.

Next, let us define $\mathcal{R} := \mathbb{F}_{q^t}[H]$ and $\mathcal{S} := \mathbb{F}_q[H]$. We note that $\mathcal{S} \subseteq \mathcal{R}$ and that $\mathcal{R}$ and $\mathcal{S}$ are group algebras of H over $\mathbb{F}_{q^t}$ and $\mathbb{F}_q$, respectively. Further, we observe that the group algebra $\mathbb{F}_{q^t}[G]$ and the set $\mathcal{R}^\ell$ of all ℓ -tuples over the group algebra $\mathcal{R}$ can be viewed as $\mathcal{S}$ -modules. Now let us define a map $\Phi : \mathbb{F}_{q^t}[G] \rightarrow \mathcal{R}^\ell$ as

$$\Phi(a) = (a_1(y), a_2(y), \dots, a_\ell(y)) = a(y) \text{ (say) for all } a = \sum_{i=1}^{\ell} \sum_{h \in H} a_{h+g_i} y^{h+g_i} \in \mathbb{F}_{q^t}[G],$$

where $a_i(y) = \sum_{h \in H} a_{h+g_i} y^h \in \mathcal{R}$ for $1 \leq i \leq \ell$. It is easy to observe that the map Φ is an $\mathcal{S}$ -module isomorphism.

Lemma 8.3.1. *The map Φ induces a one-to-one correspondence between additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ and $\mathcal{S}$ -submodules of $\mathcal{R}^\ell$.*

It is evident from the above lemma that the structure of an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ depends on the group H and the index ℓ and does not depend on the structure of the group G .

To study algebraic structures of σ -dual codes of additive H -QA codes, let us define a map $\tau_{q^w, \pi} : \mathcal{R} \rightarrow \mathcal{R}$ as

$$\tau_{q^w, \pi} \left(\sum_{h \in H} a_h y^h \right) = \sum_{h \in H} a_h^{q^w} y^{\pi h} \quad \text{for all } \sum_{h \in H} a_h y^h \in \mathcal{R},$$

where w, π are integers satisfying $0 \leq w \leq t-1$, $1 \leq \pi \leq m-1$ and $\gcd(\pi, m) = 1$. Note that the map $\tau_{q^w, \pi}$ is a ring automorphism, whose inverse is the ring automorphism $\tau_{q^{t-w}, \pi^{-1}}$, where π^{-1} is the multiplicative inverse of π modulo m . The map $\tau_{q^w, \pi}$ can be extended to the $\mathcal{S}$ -module $\mathcal{R}^\ell$ component-wise. Further, for $\sigma \in \{0, \gamma, *\}$ and $t \in \mathbb{T}_\sigma$, let us define a map $(\cdot, \cdot)_\sigma : \mathcal{R}^\ell \times \mathcal{R}^\ell \rightarrow \mathcal{S}$ as

$$(a(y), b(y))_\sigma = \begin{cases} \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} (a_i(y) \tau_{1, -1} (b_i(y))) & \text{if } \sigma = 0; \\ \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} (\gamma a_i(y) \tau_{q^{t/2}, -1} (b_i(y))) & \text{if } \sigma = \gamma; \\ \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(a_i(y) \left(\sum_{\lambda=1}^{t-1} \tau_{q^\lambda, -1} (b_i(y)) \right) \right) & \text{if } \sigma = * \end{cases} \quad (8.1)$$

for all $a(y) = (a_1(y), a_2(y), \dots, a_\ell(y))$, $b(y) = (b_1(y), b_2(y), \dots, b_\ell(y)) \in \mathcal{R}^\ell$. Note that the map $(\cdot, \cdot)_\sigma$ is a $\tau_{1,-1}$ -sesquilinear form on $\mathcal{R}^\ell$ for $\sigma \in \{0, \gamma, *\}$. We state some of its basic properties in the following lemma.

Lemma 8.3.2. *Let $a(y), b(y), c(y) \in \mathcal{R}^\ell$ and $\alpha(y), \beta(y) \in \mathcal{S}$. For $\sigma \in \{0, \gamma, *\}$, we have*

$$(a) \quad (a(y) + b(y), c(y))_\sigma = (a(y), c(y))_\sigma + (b(y), c(y))_\sigma \text{ and}$$

$$(a(y), b(y) + c(y))_\sigma = (a(y), b(y))_\sigma + (a(y), c(y))_\sigma.$$

$$(b) \quad (\alpha(y)a(y), b(y))_\sigma = \alpha(y)(a(y), b(y))_\sigma \text{ and}$$

$$(a(y), \beta(y)b(y))_\sigma = \tau_{1,-1}(\beta(y))(a(y), b(y))_\sigma.$$

$$(c) \quad (b(y), a(y))_\sigma = \tau_{1,-1}((a(y), b(y))_\sigma) \text{ for } \sigma \in \{0, *\}.$$

$$(d) \quad (b(y), a(y))_\gamma = -\tau_{1,-1}((a(y), b(y))_\gamma) \text{ and } (a(y), \tau_{1,-1}(a(y)))_\gamma = 0.$$

$$(e) \quad (\cdot, \cdot)_\sigma \text{ is non-degenerate.}$$

Proof. Working as in Lemma 6 of Huffman [34] when $\sigma \in \{0, \gamma\}$ and as in Lemma 3.3 of Sharma and Kaur *et al.* [57] when $\sigma = *$, the desired result follows. $\square$

Now if $\mathfrak{C}$ is an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$, then for $\sigma \in \{0, \gamma, *\}$, the σ -dual code $\mathfrak{C}^{\perp_\sigma}$ of $\mathfrak{C}$ is defined as

$$\mathfrak{C}^{\perp_\sigma} = \{a(y) \in \mathcal{R}^\ell : (c(y), a(y))_\sigma = 0 \text{ for all } c(y) \in \mathfrak{C}\}.$$

Note that $\mathfrak{C}^{\perp_\sigma}$ is also an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$. The following lemma relates the trace bilinear form $\langle \cdot, \cdot \rangle_\sigma$ on $\mathbb{F}_{q^t}[G]$ with the $\tau_{1,-1}$ -sesquilinear form $(\cdot, \cdot)_\sigma$ on $\mathcal{R}^\ell$ for $\sigma \in \{0, \gamma, *\}$.

Lemma 8.3.3. *For $\sigma \in \{0, \gamma, *\}$, we have*

$$(a(y), b(y))_\sigma = \sum_{u \in H} \langle y^{-u}a, b \rangle_\sigma y^u \text{ for all } a, b \in \mathbb{F}_{q^t}[G].$$

Proof. To prove the result, let $a, b \in \mathbb{F}_{q^t}[G]$ be fixed. Let us write $a = \sum_{g \in G} a_g y^g$ and $b = \sum_{g \in G} b_g y^g$, which implies that $a(y) = \Phi(a) = (a_1(y), a_2(y), \dots, a_\ell(y))$ and

$b(y) = \Phi(b) = (b_1(y), b_2(y), \dots, b_\ell(y))$, where $a_i(y) = \sum_{h \in H} a_{h+g_i} y^h \in \mathcal{R}$ and $b_i(y) = \sum_{h \in H} b_{h+g_i} y^h \in \mathcal{R}$ for $1 \leq i \leq \ell$. Further, let us take $\mathcal{Q} = 1$ and $\theta = 1$ when $\sigma = 0$, while $\mathcal{Q} = q^{t/2}$ and $\theta = \gamma$ when $\sigma = \gamma$. Now for $\sigma \in \{0, \gamma\}$, we see, by (8.1), that

$$\begin{aligned}
 (a(y), b(y))_\sigma &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1}(\theta a_i(y) \tau_{\mathcal{Q}, -1}(b_i(y))) \\
 &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(\sum_{h \in H} \sum_{k \in H} \theta a_{h+g_i} b_{k+g_i}^{\mathcal{Q}} y^{h-k} \right) \\
 &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(\sum_{u \in H} \sum_{k \in H} \theta a_{k+u+g_i} b_{k+g_i}^{\mathcal{Q}} y^u \right) \\
 &= \sum_{u \in H} \left(\sum_{i=1}^{\ell} \sum_{k \in H} \sum_{w=0}^{t-1} (\theta a_{k+u+g_i} b_{k+g_i}^{\mathcal{Q}})^{q^w} \right) y^u \\
 &= \sum_{u \in H} \sum_{g \in G} \sum_{w=0}^{t-1} (\theta a_{g+u} b_g^{\mathcal{Q}})^{q^w} y^u = \sum_{u \in H} \sum_{g \in G} \text{Tr}_{q^t, q}(\theta a_{g+u} b_g^{\mathcal{Q}}) y^u \\
 &= \sum_{u \in H} \left\langle \sum_{g \in G} a_{g+u} y^g, \sum_{g \in G} b_g y^g \right\rangle_\sigma y^u = \sum_{u \in H} \langle y^{-u} a, b \rangle_\sigma y^u.
 \end{aligned}$$

Next, for $\sigma = *$, we see, by (8.1) again, that

$$\begin{aligned}
 (a(y), b(y))_* &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(a_i(y) \left(\sum_{\lambda=1}^{t-1} \tau_{q^\lambda, -1}(b_i(y)) \right) \right) \\
 &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(\sum_{h \in H} \sum_{k \in H} \sum_{\lambda=1}^{t-1} a_{h+g_i} b_{k+g_i}^{q^\lambda} y^{h-k} \right) \\
 &= \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w, 1} \left(\sum_{u \in H} \sum_{k \in H} a_{k+u+g_i} \phi(b_{k+g_i}) y^u \right) \\
 &= \sum_{u \in H} \left(\sum_{i=1}^{\ell} \sum_{k \in H} \sum_{w=0}^{t-1} (a_{k+u+g_i} \phi(b_{k+g_i}))^{q^w} \right) y^u \\
 &= \sum_{u \in H} \sum_{g \in G} \sum_{w=0}^{t-1} (a_{g+u} \phi(b_g))^{q^w} y^u = \sum_{u \in H} \sum_{g \in G} \text{Tr}_{q^t, q}(a_{g+u} \phi(b_g)) y^u \\
 &= \sum_{u \in H} \left\langle \sum_{g \in G} a_{g+u} y^g, \sum_{g \in G} b_g y^g \right\rangle_* y^u = \sum_{u \in H} \langle y^{-u} a, b \rangle_* y^u.
 \end{aligned}$$

This proves the lemma. □

From the above discussion, we deduce the following:

Lemma 8.3.4. *Let $\mathcal{C}(\subseteq \mathbb{F}_{q^t}[G])$ be an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. Then $\Phi(\mathcal{C})$ is an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$. Further, for $\sigma \in \{0, \gamma, *\}$, we have $\Phi(\mathcal{C}^{\perp_\sigma}) = (\Phi(\mathcal{C}))^{\perp_\sigma}$, where*

$$(\Phi(\mathcal{C}))^{\perp_\sigma} = \{a(y) \in \mathcal{R}^\ell : (c(y), a(y))_\sigma = 0 \text{ for all } c(y) \in \Phi(\mathcal{C})\}.$$

Henceforth, by Lemmas [8.3.1](#) and [8.3.4](#), we view each additive H -QA code $\mathcal{C}$ of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ as an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$, and its σ -dual code $\mathcal{C}^{\perp_\sigma}$ is given by

$$\mathcal{C}^{\perp_\sigma} = \{a(y) \in \mathcal{R}^\ell : (c(y), a(y))_\sigma = 0 \text{ for all } c(y) \in \mathcal{C}\}.$$

In particular, when H is a cyclic group, additive H -QG codes over $\mathbb{F}_{q^t}$ form a special subclass of multi-twisted additive codes over $\mathbb{F}_{q^t}$, which are studied and shown to be asymptotically good in the Chapters [3](#)[7](#).

8.4 Canonical decompositions of additive H -QA codes over $\mathbb{F}_{q^t}$ and their σ -dual codes

Recall that H is a subgroup of G of order m and index ℓ in G . We assume that $\gcd(m, q) = 1$ from now on. Let M be the exponent of H . Note that M divides m , which implies that $\gcd(M, q) = 1$. Let $\mathbb{K}$ be a field extension of $\mathbb{F}_{q^t}$ containing a primitive M -th root of unity, say ζ . A *character* of H is defined as a group homomorphism from H into the multiplicative group of $\mathbb{K}$. Let $\hat{H}$ denote the set of all characters of H . For $\chi_1, \chi_2 \in \hat{H}$, define $\chi_1\chi_2 \in \hat{H}$ as $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for all $a \in H$. Note that $\hat{H}$ is an Abelian group under this multiplication operation and is called the *character group* of H . By Exercise 5.5 of [\[43\]](#), we see that the groups $\hat{H}$ and H are isomorphic. Let χ_h be the character of H corresponding to the element $h \in H$. For $h, k \in H$, we have $\chi_{h+k} = \chi_h\chi_k$. Note that the character χ_0 (corresponding to the identity element 0 of H) is the identity element of the

character group $\widehat{H}$, *i.e.*, we have $\chi_0(a) = 1$ for all $a \in H$. The character χ_0 is called the trivial character of H .

Since $\gcd(m, q) = 1$, we see, by applying Maschke's Theorem, that both group algebras $\mathcal{S}$ and $\mathcal{R}$ are semisimple, *i.e.*, both $\mathcal{S}$ and $\mathcal{R}$ can be expressed as direct sums of minimal ideals by partitioning H into q -cyclotomic classes and q^t -cyclotomic classes, respectively (see [2] pp.116-117). To recall the definition of cyclotomic classes, let Q be either q or q^t . For $h_1, h_2 \in H$, we define $h_1 \sim h_2$ if and only if $h_2 = Q^u h_1$ for some integer $u \geq 0$, where $Q^u h_1 = \underbrace{h_1 + h_1 + \cdots + h_1}_{Q^u \text{ times}}$. Note that $\sim$ is an equivalence relation on H , and hence partitions the group H into a disjoint union of distinct equivalence classes. For $h \in H$, the equivalence class $S_Q(h)$ of $h \in H$ must be finite and is given by

$$S_Q(h) = \{k \in H : k \sim h\} = \{h, Qh, Q^2h, \dots, Q^{z_h-1}h\},$$

where z_h is the smallest positive integer satisfying $Q^{z_h}h = h$ in H . The equivalence class $S_Q(h)$ is called the Q -cyclotomic class of h for each $h \in H$. Note that z_h is the multiplicative order of Q modulo $\text{ord}(h)$, where $\text{ord}(h)$ denotes the (additive) order of the element h in H , *i.e.*, $z_h = \text{ord}_{\text{ord}(h)}(Q)$. The element $h \in H$ is called a *representative* of the Q -cyclotomic class $S_Q(h)$. Note that any two Q -cyclotomic classes in H are either identical or disjoint. The Q -cyclotomic class $S_Q(h)$ of $h \in H$ is said to be of the

- (i) Type I if $h = -h$,
- (i) Type II if $h \neq -h$ and $S_Q(h) = S_Q(-h)$, and
- (i) Type III if $S_Q(h) \neq S_Q(-h)$.

Now the following three lemmas state some basic properties of the Q -cyclotomic class $S_Q(h)$ for $h \in H$.

Lemma 8.4.1. *Let Q be either q or q^t . The following hold.*

- (a) *If 0 denotes the identity element of H , then $S_Q(0)$ is of Type I.*
- (b) *If $h \in H$ is such that the Q -cyclotomic class $S_Q(h)$ is of Type I, then $\text{ord}(h)$ is either 1 or 2 and $|S_Q(h)| = 1$.*

- (c) For $h \in H$, the Q -cyclotomic class $S_Q(h)$ is of Type II if and only if there exists a positive integer w such that $Q^w \equiv -1 \pmod{\text{ord}(h)}$.
- (d) If $h \in H$ is such that the Q -cyclotomic class $S_Q(h)$ is of Type II, then $|S_Q(h)|$ must be even.

Proof. It follows from Remark 3.1 of Jitman and Ling [38]. □

Lemma 8.4.2. For any $h \in H$, we have $S_q(h) = S_{q^t}(h) \cup S_{q^t}(hq) \cup \dots \cup S_{q^t}(hq^{\kappa_h-1})$, where $\kappa_h = \gcd(t, |S_q(h)|)$. Furthermore, for $0 \leq j \leq \kappa_h - 1$, we have

$$|S_{q^t}(hq^j)| = \frac{|S_q(h)|}{\gcd(t, |S_q(h)|)}.$$

Proof. Working as in Lemma 1 of Huffman [34], the desired result follows. □

Lemma 8.4.3. Let $h \in H$ be fixed, and let $\kappa_h = \gcd(t, |S_q(h)|)$. Then the following hold.

- (a) $S_q(h)$ is of Type I if and only if $S_{q^t}(h)$ is of Type I and $S_q(h) = S_{q^t}(h) = \{h\}$.
- (b) If $S_{q^t}(h)$ is of Type II, then $S_q(h)$ is of Type II. The converse does not hold in general.
- (c) If $S_q(h)$ is of Type II, then $S_{q^t}(h) = S_{q^t}(-hq^j)$ for some integer j satisfying $0 \leq j \leq \kappa_h - 1$.

Proof. (a) Proof is trivial.

- (b) Let $h \in H$ be such that $S_{q^t}(h)$ is of Type II. That is, we have $S_{q^t}(h) = S_{q^t}(-h)$ and $h \neq -h$, which implies that $S_{q^t}(hq^j) = S_{q^t}(-hq^j)$ for $0 \leq j \leq \kappa_h - 1$. Now by Lemma [8.4.2], we get $S_q(h) = S_q(-h)$, and hence $S_q(h)$ is of Type II. To prove the second part, let $q = 3$, $t = 2$ and $H = \mathbb{Z}_4 = \{0, 1, 2, 3\}$. Note that $S_3(1) = \{1, 3\} = S_3(-1)$ and $S_{3^2}(1) = \{1\} \neq \{-1\} = S_{3^2}(-1)$. This shows that $S_3(1)$ is of Type II, but $S_{3^2}(1)$ is not of Type II.

- (c) Let $S_q(h)$ be of Type II, which implies that $S_q(h) = S_q(-h)$ and $h \neq -h$. Since $|S_q(h)| = |S_q(-h)|$, by Lemma [8.4.2], we have $S_q(h) = \bigcup_{i=0}^{\kappa_h-1} S_{q^t}(hq^i)$ and

$S_q(-h) = \bigcup_{i=0}^{\kappa_h-1} S_{q^t}(-hq^i)$. Since any two q^t -cyclotomic classes are either identical or disjoint, we must have $S_{q^t}(h) = S_{q^t}(-hq^j)$ for some integer j satisfying $0 \leq j \leq \kappa_h - 1$.

□

Now let R be a finite commutative ring with unity. An element $e \in R$ is called an *idempotent* of R if it satisfies $e^2 = e$ in R . Further, a non-zero idempotent e of R is called a *primitive idempotent* if it can not be expressed as a sum of two non-zero orthogonal idempotents of R . By Corollary II.2 of Ding *et al.* [22], we see that all the primitive idempotents of $\mathbb{K}[H]$ are given by

$$E_x = \frac{1}{m} \sum_{h \in H} \chi_x(-h) y^h \in \mathbb{K}[H], \quad (8.2)$$

where x runs over H . Further, by Proposition II.4 of Ding *et al.* [22], we have

$$\mathbb{K}[H] = \bigoplus_{x \in H} \mathbb{K}[H] E_x.$$

We now proceed to determine all the primitive idempotents of $\mathcal{S}$ and $\mathcal{R}$. For this, let $S_H = \{h_1, h_2, \dots, h_s\}$ be a complete set of representatives of distinct q -cyclotomic classes of H . One can easily see that $H = \bigcup_{\nu=1}^s S_q(h_\nu)$ (a disjoint union). Now by Proposition III.6 of Ding *et al.* [22], we see that there is a one-to-one correspondence between q -cyclotomic classes of H and primitive idempotents of $\mathcal{S}$ and that the primitive idempotent of $\mathcal{S}$ corresponding to the q -cyclotomic class $S_q(h_\nu)$ of H is given by

$$e_{h_\nu} = \sum_{x \in S_q(h_\nu)} E_x = \frac{1}{m} \sum_{x \in S_q(h_\nu)} \sum_{h \in H} \chi_x(-h) y^h \quad (8.3)$$

for $1 \leq \nu \leq s$. By Proposition III.6 of Ding *et al.* [22], we see that the group algebra $\mathcal{S}$ can be decomposed as

$$\mathcal{S} \simeq \bigoplus_{\nu=1}^s \mathcal{S} e_{h_\nu} = \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu}, \quad (8.4)$$

where $\mathcal{F}_{h_\nu} = \mathcal{S} e_{h_\nu}$ is the minimal ideal of $\mathcal{S}$ generated by the primitive idempotent

e_{h_ν} for $1 \leq \nu \leq s$. Further, let $d_\nu = |S_q(h_\nu)|$ for $1 \leq \nu \leq s$. By Proposition III.6 of Ding *et al.* [22], we see that $\mathcal{F}_{h_\nu}$ is the finite field of order q^{d_ν} for $1 \leq \nu \leq s$, and that $\mathcal{F}_{h_\nu} \cap \mathcal{F}_{h_{\nu'}} = \{0\}$ if $\nu \neq \nu'$.

Next, by Lemma 8.4.2, we see that

$$T_H = \{h_1, h_1q, \dots, h_1q^{\kappa_{h_1}-1}, h_2, h_2q, \dots, h_2q^{\kappa_{h_2}-1}, \dots, h_s, h_sq, \dots, h_sq^{\kappa_{h_s}-1}\}$$

is a complete set of representatives of distinct q^t -cyclotomic classes of H , where $\kappa_{h_\nu} = \gcd(t, |S_q(h_\nu)|)$ for $1 \leq \nu \leq s$. We note that

$$H = \bigcup_{\nu=1}^s \bigcup_{j=0}^{\kappa_{h_\nu}-1} S_{q^t}(h_\nu q^j) \text{ (a disjoint union).}$$

By Proposition III.6 of Ding *et al.* [22], we see that there is a one-to-one correspondence between q^t -cyclotomic classes of H and primitive idempotents of $\mathcal{R}$ and that the primitive idempotent of $\mathcal{R}$ corresponding to the q^t -cyclotomic class $S_{q^t}(h_\nu q^j)$ of H is given by

$$e_{h_\nu, j} = \sum_{x \in S_{q^t}(h_\nu q^j)} E_x = \frac{1}{m} \sum_{x \in S_{q^t}(h_\nu q^j)} \sum_{h \in H} \chi_x(-h) y^h \quad (8.5)$$

for $0 \leq j \leq \kappa_{h_\nu} - 1$ and $1 \leq \nu \leq s$. From this, it follows that

$$e_{h_\nu} = e_{h_\nu, 0} + e_{h_\nu, 1} + \dots + e_{h_\nu, \kappa_{h_\nu}-1} \quad \text{for } 1 \leq \nu \leq s.$$

By Proposition III.6 of Ding *et al.* [22] again, we see that the group algebra $\mathcal{R}$ can be decomposed as

$$\mathcal{R} \simeq \bigoplus_{\nu=1}^s \bigoplus_{j=0}^{\kappa_{h_\nu}-1} \mathcal{R}e_{h_\nu, j} = \bigoplus_{\nu=1}^s \bigoplus_{j=0}^{\kappa_{h_\nu}-1} \mathcal{F}_{h_\nu, j} = \bigoplus_{\nu=1}^s \mathcal{G}_{h_\nu}, \quad (8.6)$$

where $\mathcal{F}_{h_\nu, j} = \mathcal{R}e_{h_\nu, j}$ is the minimal ideal of $\mathcal{R}$ generated by the primitive idempotent $e_{h_\nu, j}$ for $0 \leq j \leq \kappa_{h_\nu} - 1$ and $\mathcal{G}_{h_\nu} = \bigoplus_{j=0}^{\kappa_{h_\nu}-1} \mathcal{F}_{h_\nu, j}$ for $1 \leq \nu \leq s$. Further, by Lemma 8.4.2, we see that $D_\nu = |S_{q^t}(h_\nu q^j)| = \frac{d_\nu}{\kappa_{h_\nu}}$ for $1 \leq \nu \leq s$ and $0 \leq j \leq \kappa_{h_\nu} - 1$. For

each ν and j , we note, by Proposition III.6 of Ding *et al.* [22] again, that $\mathcal{F}_{h_\nu, j}$ is the finite field of order q^{tD_ν} . We also observe that $\mathcal{F}_{h_\nu, j} \cap \mathcal{F}_{h_{\nu'}, j'} = \{0\}$ if $(\nu, j) \neq (\nu', j')$. More precisely, the algebra isomorphism from $\mathcal{R}$ onto $\bigoplus_{\nu=1}^s \mathcal{G}_{h_\nu}$ is given by

$$a(y) \mapsto \sum_{\nu=1}^s \sum_{j=0}^{\kappa_{h_\nu}-1} a(y) e_{h_\nu, j} = \sum_{\nu=1}^s a(y) e_{h_\nu} = \sum_{\nu=1}^s A_\nu(y) \text{ for each } a(y) \in \mathcal{R},$$

where $A_\nu(y) = a(y) e_{h_\nu}$ for each ν . Therefore, we have

$$\mathcal{R}^\ell \simeq \mathcal{G} = \bigoplus_{\nu=1}^s \mathcal{G}_{h_\nu}^\ell. \quad (8.7)$$

In view of the above isomorphism, from now on, we shall identify each element $a(y) = (a_1(y), a_2(y), \dots, a_\ell(y)) \in \mathcal{R}^\ell$ with the element $A(y) = \sum_{\nu=1}^s A_\nu(y) \in \mathcal{G}$, where $A_\nu(y) = (A_{\nu,1}(y), A_{\nu,2}(y), \dots, A_{\nu,\ell}(y)) \in \mathcal{G}_{h_\nu}^\ell$ with $A_{\nu,i}(y) = a_i(y) e_{h_\nu} \in \mathcal{G}_{h_\nu}$ for $1 \leq i \leq \ell$ and $1 \leq \nu \leq s$. More precisely, if Ψ denotes the isomorphism from $\mathcal{R}^\ell$ onto $\mathcal{G}$, then we shall write $\Psi(a(y)) = A(y)$. Further, it is easy to note that the set $\mathcal{G}_{h_\nu}$ is a vector space over $\mathcal{F}_{h_\nu}$ under the component-wise addition and the component-wise scalar multiplication. We next make the following observation.

Lemma 8.4.4. *For $1 \leq \nu \leq s$, $\mathcal{G}_{h_\nu}^\ell = \mathcal{F}_{h_\nu,0}^\ell \oplus \mathcal{F}_{h_\nu,1}^\ell \oplus \dots \oplus \mathcal{F}_{h_\nu,\kappa_{h_\nu}-1}^\ell$ is an ℓt -dimensional vector space over $\mathcal{F}_{h_\nu}$.*

From the above discussion, we deduce the following:

Theorem 8.4.1. (a) *Let $\mathcal{C}$ be an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. For $1 \leq \nu \leq s$, let us define $\mathcal{C}_\nu = \mathcal{C} \cap \mathcal{G}_{h_\nu}^\ell$. For each ν , $\mathcal{C}_\nu$ is an $\mathcal{F}_{h_\nu}$ -subspace of $\mathcal{G}_{h_\nu}^\ell$. Furthermore, we have $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \dots \oplus \mathcal{C}_s$, and this direct sum decomposition is unique. (The subspaces $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_s$ are called constituents of the code $\mathcal{C}$.)*

(b) *Conversely, let $\mathcal{D} = \mathcal{D}_1 + \mathcal{D}_2 + \dots + \mathcal{D}_s$, where $\mathcal{D}_\nu$ is an $\mathcal{F}_{h_\nu}$ -subspace of $\mathcal{G}_{h_\nu}^\ell$ for $1 \leq \nu \leq s$. Then we have $\mathcal{D} = \mathcal{D}_1 \oplus \mathcal{D}_2 \oplus \dots \oplus \mathcal{D}_s$. Further, $\mathcal{D}$ is an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$.*

Proof. Its proof is a straightforward exercise. □

From the above theorem, it follows that the $\mathcal{F}_{h_\nu}$ -subspaces of $\mathcal{G}_{h_\nu}^\ell$ ($1 \leq \nu \leq s$) are building blocks of all additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. In the following theorem, we count all additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$.

Lemma 8.4.5. *For $1 \leq \nu \leq s$, let $d_\nu = |S_q(h_\nu)|$. The total number of distinct additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by*

$$\mathfrak{N}(\ell, H) = \prod_{\nu=1}^s \left(\sum_{k=0}^{\ell t} \left[\begin{matrix} \ell t \\ k \end{matrix} \right]_{q^{d_\nu}} \right).$$

Proof. It follows immediately by applying Theorem [8.4.1](#) and Lemmas [2.2.1](#) and [8.4.4](#). □

For each $h \in H$, there exists a unique integer ν satisfying $1 \leq \nu \leq s$ and $S_q(h) = S_q(h_\nu)$, and we define $e_h = e_{h_\nu}$. Similarly, for $h \in H$ and integer k satisfying $0 \leq k \leq \kappa_{h_\nu} - 1$, there exist unique integers ν and j satisfying $1 \leq \nu \leq s$, $0 \leq j \leq \kappa_{h_\nu} - 1$ and $S_{q^t}(hq^k) = S_{q^t}(h_\nu q^{j+k})$, and we define $e_{h,k} = e_{h_\nu, j+k}$.

Lemma 8.4.6. *Let $k \in H$ be such that $S_q(k)$ is of Type I. Then either $k = 0$ or $\text{ord}(k) = 2$, (there exists an element $k \in H$ with $\text{ord}(k) = 2$ if and only if M is even).*

(a) When $k = 0$, we have

$$e_0 = e_{0,0} = \frac{1}{m} \sum_{h \in H} y^h.$$

Furthermore, we have $\mathcal{F}_0 = \{\theta e_0 : \theta \in \mathbb{F}_q\}$ and $\mathcal{F}_{0,0} = \{\alpha e_0 : \alpha \in \mathbb{F}_{q^t}\}$.

(b) Let $\text{ord}(k) = 2$. Let us define $X = \{a \in H : \chi_k(a) = 1\}$. Then X is a proper subgroup of H and there exists $b \in H \setminus X$ such that $H = X \cup (b + X)$. Further, we have

$$e_k = e_{k,0} = \frac{1}{m} (1 - y^b) \sum_{h \in X} y^h.$$

Furthermore, we have $\mathcal{F}_k = \{\theta e_k : \theta \in \mathbb{F}_q\}$ and $\mathcal{F}_{k,0} = \{\alpha e_k : \alpha \in \mathbb{F}_{q^t}\}$.

Proof. Since $S_q(k)$ is of Type I, we see, by (8.3) and (8.5), that $S_q(k) = \{k\} = S_{q^t}(k)$, which implies that

$$e_k = e_{k,0} = \frac{1}{m} \sum_{h \in H} \chi_k(-h) y^h.$$

(a) Let $k = 0$. Since $\chi_0(a) = 1$ for all $a \in H$, we obtain

$$e_0 = e_{0,0} = \frac{1}{m} \sum_{h \in H} \chi_0(-h) y^h = \frac{1}{m} \sum_{h \in H} y^h.$$

Further, one can easily see that

$$\left(\sum_{z \in H} \theta_z y^z \right) e_0 = \left(\sum_{z \in H} \theta_z y^z \right) \frac{1}{m} \left(\sum_{h \in H} y^h \right) = \left(\sum_{z \in H} \theta_z \right) e_0 \text{ for all } \sum_{z \in H} \theta_z y^z \in \mathcal{S}.$$

Similarly, we see that

$$\left(\sum_{z \in H} \alpha_z y^z \right) e_0 = \left(\sum_{z \in H} \alpha_z \right) e_0 \text{ for all } \sum_{z \in H} \alpha_z y^z \in \mathcal{R}.$$

This shows that $\mathcal{F}_0 = \{\theta e_0 : \theta \in \mathbb{F}_q\}$ and $\mathcal{F}_{0,0} = \{\alpha e_0 : \alpha \in \mathbb{F}_{q^t}\}$.

(b) Let $\text{ord}(k) = 2$, i.e., $k \neq 0$ and $2k = 0$. Here we first note that $\chi_k(a) \in \{1, -1\}$ for all $a \in H$. Note that X is a subgroup of H . Since $k \neq 0$, we see that $X \neq H$. So there exists $b \in H \setminus X$, which implies that $\chi_k(b) = -1$. One can easily observe that $H \setminus X = b + X$. From this, it follows that $H = X \cup (b + X)$. Further, one can easily see that

$$e_k = e_{k,0} = \frac{1}{m} \sum_{h \in H} \chi_k(-h) y^h = \frac{1}{m} (1 - y^b) \sum_{h \in X} y^h.$$

We next observe that

$$\left(\sum_{z \in H} \theta_z y^z \right) e_k = \left(\sum_{z \in H} \theta_z y^z \right) \left(\frac{1}{m} (1 - y^b) \sum_{h \in X} y^h \right) = \left(\sum_{z \in X} \theta_z - \sum_{z \in X} \theta_{b+z} \right) e_k$$

for all $\sum_{z \in X} \theta_z y^z \in \mathcal{S}$. Similarly, one can see that

$$\left(\sum_{z \in H} \alpha_z y^z \right) e_k = \left(\sum_{z \in H} \alpha_z y^z \right) \left(\frac{1}{m} (1 - y^b) \sum_{h \in X} y^h \right) = \left(\sum_{z \in X} \alpha_z - \sum_{z \in X} \alpha_{b+z} \right) e_k$$

for all $\sum_{z \in H} \alpha_z y^z \in \mathcal{R}$. From this, it follows that $\mathcal{F}_k = \{\theta e_k : \theta \in \mathbb{F}_q\}$ and $\mathcal{F}_{k,0} = \{\alpha e_k : \alpha \in \mathbb{F}_{q^t}\}$.

□

To study σ -dual codes of additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$, we will study the action of the automorphisms $\tau_{1,-1}$ and $\tau_{q^{t/2},-1}$ of $\mathcal{R}$ on its minimal ideals. For this, we prove the following two lemmas:

Lemma 8.4.7. *Let ν and j be fixed integers satisfying $1 \leq \nu \leq s$ and $0 \leq j \leq \kappa_{h_\nu} - 1$. For $0 \leq w \leq t - 1$, we have $\tau_{q^w,1}(e_{h_\nu,j}) = e_{h_\nu,j+w}$ and $\tau_{q^w,-1}(e_{h_\nu,j}) = e_{-h_\nu,j+w}$.*

Proof. To prove the result, let $\pi \in \{1, -1\}$, and let us consider

$$\begin{aligned} \tau_{q^w,\pi}(e_{h_\nu,j}) &= \frac{1}{m} \sum_{x \in S_{q^t}(h_\nu q^j)} \sum_{h \in H} \chi_x(-h)^{q^w} y^{\pi h} = \frac{1}{m} \sum_{x \in S_{q^t}(h_\nu q^j)} \sum_{h \in H} \chi_x(-h q^w) y^{\pi h} \\ &= \frac{1}{m} \sum_{x \in S_{q^t}(h_\nu q^j)} \sum_{k \in H} \chi_x(-\pi^{-1} k q^w) y^k = \frac{1}{m} \sum_{x \in S_{q^t}(h_\nu q^j)} \sum_{k \in H} \chi_{x\pi^{-1}q^w}(-k) y^k \\ &= \frac{1}{m} \sum_{x \in S_{q^t}(\pi^{-1}h_\nu q^{j+w})} \sum_{k \in H} \chi_x(-k) y^k = e_{\pi^{-1}h_\nu,j+w}. \end{aligned}$$

From this, the desired result follows. □

Recall that $S_H = \{h_1, h_2, \dots, h_s\}$ is a complete set of representatives of distinct q -cyclotomic classes of H . For $1 \leq \nu \leq s$, there exists a unique integer ν' satisfying $1 \leq \nu' \leq s$ and $S_q(-h_\nu) = S_q(h_{\nu'})$. This gives rise to a permutation μ of the set $\{1, 2, \dots, s\}$ satisfying $S_q(-h_\nu) = S_q(h_{\mu(\nu)})$ for $1 \leq \nu \leq s$. This, by Lemma 8.4.7, implies that $\tau_{q^w,-1}(e_{h_\nu,j}) = e_{h_{\mu(\nu)},j+w}$ for $0 \leq w \leq t - 1, 0 \leq j \leq \kappa_{h_\nu} - 1$ and $1 \leq \nu \leq s$.

It is easy to see that μ^2 is the identity map, which implies that μ is either the identity permutation or a product of transpositions. Further, for $1 \leq \nu \leq s$, we note that $\mu(\nu) = \nu$ if and only if the q -cyclotomic class $S_q(h_\nu)$ of H is either of the Type I or II. Also, one can easily see that $\kappa_{h_\nu} = \kappa_{h_{\mu(\nu)}}$ for each ν . From this, we deduce the following:

Corollary 8.4.1. *For $1 \leq \nu \leq s$, we have $\tau_{1,-1}(e_{h_\nu}) = \tau_{q^{t/2},-1}(e_{h_\nu}) = e_{h_{\mu(\nu)}}$.*

Lemma 8.4.8. *For $1 \leq \nu \leq s$, we have $\tau_{1,-1}(\mathcal{G}_{h_\nu}) = \tau_{q^{t/2},-1}(\mathcal{G}_{h_\nu}) = \mathcal{G}_{h_{\mu(\nu)}}$. In particular, if $S_q(h_\nu)$ is of Type I or II, then we have $\tau_{1,-1}(\mathcal{G}_{h_\nu}) = \tau_{q^{t/2},-1}(\mathcal{G}_{h_\nu}) = \mathcal{G}_{h_\nu}$.*

Proof. It follows immediately from Corollary [8.4.1](#). $\square$

Under the above identification of $\mathcal{R}^\ell$ with $\mathcal{G}$, we observe that for $\sigma \in \{0, \gamma, *\}$, the sesquilinear form $(\cdot, \cdot)_\sigma$ on $\mathcal{R}^\ell$ corresponds to the map $[\cdot, \cdot]_\sigma : \mathcal{G} \times \mathcal{G} \rightarrow \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu}$, defined as

$$[A(y), B(y)]_\sigma = \begin{cases} \sum_{\nu=1}^s \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w,1} (A_{\nu,i}(y) \tau_{1,-1}(B_{\mu(\nu),i}(y))) & \text{if } \sigma = 0; \\ \sum_{\nu=1}^s \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w,1} (\gamma A_{\nu,i}(y) \tau_{q^{t/2},-1}(B_{\mu(\nu),i}(y))) & \text{if } \sigma = \gamma; \\ \sum_{\nu=1}^s \sum_{i=1}^{\ell} \left(\sum_{w=0}^{t-1} \tau_{q^w,1} \left(A_{\nu,i}(y) \left(\sum_{\lambda=1}^{t-1} \tau_{q^\lambda,-1}(B_{\mu(\nu),i}(y)) \right) \right) \right) & \text{if } \sigma = * \end{cases} \quad (8.8)$$

for all $A(y) = \sum_{\nu=1}^s (A_{\nu,1}(y), A_{\nu,2}(y), \dots, A_{\nu,\ell}(y)) \in \mathcal{G}$ and $B(y) = \sum_{\nu=1}^s (B_{\nu,1}(y), B_{\nu,2}(y), \dots, B_{\nu,\ell}(y)) \in \mathcal{G}$. Next, for all $f(y) = \sum_{\nu=1}^s f_\nu(y) \in \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu} (\simeq \mathcal{S})$, let us define $\tau_{1,-1}(f(y)) = \sum_{\nu=1}^s \tau_{1,-1}(f_{\mu(\nu)}(y)) \in \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu}$. In the following lemma, we show that the map $[\cdot, \cdot]_\sigma : \mathcal{G} \times \mathcal{G} \rightarrow \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu}$ is a reflexive and non-degenerate $\tau_{1,-1}$ -sesquilinear form for $\sigma \in \{0, \gamma, *\}$.

Lemma 8.4.9. *Let $A(y), B(y), C(y) \in \mathcal{G}$ and $f(y) \in \bigoplus_{\nu=1}^s \mathcal{F}_{h_\nu}$. For $\sigma \in \{0, \gamma, *\}$, the following hold.*

(a) $[A(y) + B(y), C(y)]_\sigma = [A(y), C(y)]_\sigma + [B(y), C(y)]_\sigma$ and

$$[A(y), B(y) + C(y)]_\sigma = [A(y), B(y)]_\sigma + [A(y), C(y)]_\sigma.$$

(b) $[f(y)A(y), B(y)]_\sigma = f(y)[A(y), B(y)]_\sigma$ and

$$[A(y), f(y)B(y)]_\sigma = \tau_{1,-1}(f(y))[A(y), B(y)]_\sigma.$$

(c) $[A(y), B(y)]_\sigma = \tau_{1,-1}([B(y), A(y)]_\sigma)$ for $\sigma \in \{0, *\}$, and

$$[A(y), B(y)]_\gamma = -\tau_{1,-1}([B(y), A(y)]_\gamma).$$

(d) $[\cdot, \cdot]_\sigma$ is non-degenerate.

Proof. Proofs of parts (a)-(c) are trivial.

To prove (d), let $A(y) \in \mathcal{G}$ be such that $[A(y), C(y)]_\sigma = 0$ for all $C(y) \in \mathcal{G}$. Here, we assert that $A(y) = \mathbf{0}$. Let us suppose, on the contrary, that $A(y) \neq \mathbf{0}$. There exists non-zero $a(y) = (a_1(y), a_2(y), \dots, a_\ell(y)) \in \mathcal{R}^\ell$ such that $\Psi(a(y)) = A(y)$, where $a_i(y) = \sum_{h \in H} a_{h+g_i} y^h \in \mathcal{R}$ for $1 \leq i \leq \ell$. Let us write $A(y) = \sum_{\nu=1}^s A_\nu(y)$, where $A_\nu(y) = (A_{\nu,1}(y), A_{\nu,2}(y), \dots, A_{\nu,\ell}(y))$ with $A_{\nu,i}(y) = a_i(y) e_{h_\nu}$ for $1 \leq i \leq \ell$ and $1 \leq \nu \leq s$. Since $a(y)$ is non-zero, we note that $a_i(y) = \sum_{h \in H} a_{h+g_i} y^h$ is non-zero for some i , which implies that $A_{\nu,i}(y) = a_i(y) e_{h_\nu} \neq 0$ for some ν and i and that $a_{k+g_i} \neq 0$ for some i and $k \in H$. Since the trace map $\text{Tr}_{q^t, q}$ is onto, there exist $c, d, \xi \in \mathbb{F}_{q^t}$ such that $\text{Tr}_{q^t, q}(a_{k+g_i} c) \neq 0$, $\text{Tr}_{q^t, q}(\gamma a_{k+g_i} d^{q^{t/2}}) \neq 0$ and $\text{Tr}_{q^t, q}(\xi) \neq 0$. Now let us define $b_j(y) = 0$ for $1 \leq j(\neq i) \leq \ell$ and

$$b_i(y) = \begin{cases} c & \text{when } \sigma = 0; \\ d & \text{when } \sigma = \gamma; \\ \phi^{-1}(\xi a_{k+g_i}^{-1}) & \text{when } \sigma = *. \end{cases}$$

Let us define $b(y) = (b_1(y), b_2(y), \dots, b_\ell(y)) \in \mathcal{R}^\ell$, and let us take $B(y) = \Psi(b(y)) \in \mathcal{G}$. Now by (8.8), we see that

$$[A(y), B(y)]_0 = \sum_{h \in H} \text{Tr}_{q^t, q}(a_{h+g_i} c) y^h e_{h_\nu} \neq 0,$$

which is a contradiction. By (8.8) again, we note that

$$[A(y), B(y)]_\gamma = \sum_{h \in H} \text{Tr}_{q^t, q}(\gamma a_{h+g_i} d^{q^{t/2}}) y^h e_{h_\nu} \neq 0,$$

which is again a contradiction.

Finally, when $\sigma = *$, by (8.8) again, we see that

$$[A(y), B(y)]_* = \sum_{h \in H} \text{Tr}_{q^t, q}(\xi a_{h+g_i} a_{k+g_i}^{-1}) y^h e_{h_\nu} \neq 0,$$

which is again a contradiction.

This proves the assertion. Thus the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ is non-degenerate. $\square$

Next, for $1 \leq \nu \leq s$, let $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_\nu}^\ell \times \mathcal{G}_{h_{\mu(\nu)}}^\ell}$ denote the restriction of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ to $\mathcal{G}_{h_\nu}^\ell \times \mathcal{G}_{h_{\mu(\nu)}}^\ell$, $1 \leq \nu \leq s$. We further deduce the following:

Corollary 8.4.2. *For $a(y), b(y) \in \mathcal{R}^\ell$, let $\Psi(a(y)) = A(y) = \sum_{\nu=1}^s A_\nu(y) \in \mathcal{G}$ and $\Psi(b(y)) = B(y) = \sum_{\nu=1}^s B_\nu(y) \in \mathcal{G}$. For $\sigma \in \{0, \gamma, *\}$, we have*

$$[A(y), B(y)]_\sigma = 0 \text{ if and only if } [A_\nu(y), B_{\mu(\nu)}(y)]_\sigma = 0 \text{ for } 1 \leq \nu \leq s.$$

In the following theorem, we obtain a canonical decomposition of the σ -dual code of each additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ by relating the constituents of a code with that of its σ -dual code for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.4.2. *Let $\mathcal{C}$ be an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. Let $\mathcal{C} = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_s$ and $\mathcal{C}^{\perp_\sigma} = \mathcal{C}_1^{(\sigma)} \oplus \mathcal{C}_2^{(\sigma)} \oplus \cdots \oplus \mathcal{C}_s^{(\sigma)}$ be the canonical decompositions of $\mathcal{C}$ and $\mathcal{C}^{\perp_\sigma}$, where $\mathcal{C}_\nu = \mathcal{C} \cap \mathcal{G}_{h_\nu}^\ell$ and $\mathcal{C}_\nu^{(\sigma)} = \mathcal{C}^{\perp_\sigma} \cap \mathcal{G}_{h_{\mu(\nu)}}^\ell$ for $1 \leq \nu \leq s$ and $\sigma \in \{0, \gamma, *\}$. Then for $1 \leq \nu \leq s$, we have*

$$\mathcal{C}_\nu^{(\sigma)} = \{B_{\mu(\nu)}(y) \in \mathcal{G}_{h_{\mu(\nu)}}^\ell : [A_\nu(y), B_{\mu(\nu)}(y)]_\sigma = 0 \text{ for all } A_\nu(y) \in \mathcal{C}_\nu\} = \mathcal{C}_\nu^{\perp_\sigma},$$

i.e., $\mathcal{C}_\nu^{\perp_\sigma}$ is the orthogonal complement of $\mathcal{C}_\nu$ with respect to $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_\nu}^\ell \times \mathcal{G}_{h_{\mu(\nu)}}^\ell}$ for $1 \leq \nu \leq s$. Moreover, we have $\dim_{\mathcal{F}_{h_\nu}}(\mathcal{C}_\nu) + \dim_{\mathcal{F}_{h_{\mu(\nu)}}}(\mathcal{C}_\nu^{\perp_\sigma}) = \ell t$ for $1 \leq \nu \leq s$.

Proof. It follows immediately by applying Lemma [8.4.9](#), Corollary [8.4.2](#), and Theorem [2.2.2](#). $\square$

8.5 σ -Self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes over $\mathbb{F}_{q^t}$

In this section, we will characterize all σ -self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$. To do this, we first recall that $S_H = \{h_1, h_2, \dots, h_s\}$ is a complete set of representatives

of distinct q -cyclotomic classes of H and that μ is a permutation of $\{1, 2, \dots, s\}$ satisfying $S_q(-h_\nu) = S_q(h_{\mu(\nu)})$ for $1 \leq \nu \leq s$. We further assume, without any loss of generality, that

- $h_1, h_2, \dots, h_{r_1}$ are representatives of all Type I q -cyclotomic classes of H ,
- $h_{r_1+1}, h_{r_1+2}, \dots, h_{r_2}$ are representatives of all Type II q -cyclotomic classes of H and
- $h_{r_2+1}, h_{\mu(r_2+1)}, h_{r_2+2}, h_{\mu(r_2+2)}, \dots, h_{r_3}, h_{\mu(r_3)}$ are representatives of all Type III q -cyclotomic classes of H .

Thus the set S_H can be partitioned as $S_H = S_H(\text{I}) \cup S_H(\text{II}) \cup S_H(\text{III})$, where

$$\begin{aligned} S_H(\text{I}) &= \{h_1, h_2, \dots, h_{r_1}\}, \\ S_H(\text{II}) &= \{h_{r_1+1}, h_{r_1+2}, \dots, h_{r_2}\} \text{ and} \\ S_H(\text{III}) &= \{h_{r_2+1}, h_{\mu(r_2+1)}, h_{r_2+2}, h_{\mu(r_2+2)}, \dots, h_{r_3}, h_{\mu(r_3)}\}. \end{aligned}$$

Note that $s = 2r_3 - r_2$ and the parameters r_1, r_2, r_3 depend upon the structure of the finite Abelian group H and prime power q . By (8.7) and applying Lemma 8.4.8, we see that

$$\mathcal{R}^\ell \simeq \mathcal{G} = \left(\bigoplus_{u=1}^{r_1} \mathcal{G}_{h_u}^\ell \right) \oplus \left(\bigoplus_{v=r_1+1}^{r_2} \mathcal{G}_{h_v}^\ell \right) \oplus \left(\bigoplus_{w=r_2+1}^{r_3} (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \right), \quad (8.9)$$

where $\mathcal{G}_{h_u}$ (*resp.* $\mathcal{G}_{h_v}$, $\mathcal{G}_{h_w}$ and $\mathcal{G}_{h_{\mu(w)}}$) is a vector space over $\mathcal{F}_{h_u}$ (*resp.* $\mathcal{F}_{h_v}$, $\mathcal{F}_{h_w}$ and $\mathcal{F}_{h_{\mu(w)}}$) for each u (*resp.* v and w). From now on, we shall identify each element $a(y) = (a_1(y), a_2(y), \dots, a_\ell(y)) \in \mathcal{R}^\ell$ with the element

$$A(y) = \sum_{u=1}^{r_1} A_u(y) + \sum_{v=r_1+1}^{r_2} A_v(y) + \sum_{w=r_2+1}^{r_3} (A_w(y) + A_{\mu(w)}(y)) \in \mathcal{G},$$

where

$$\begin{aligned} A_u(y) &= (A_{u,1}(y), A_{u,2}(y), \dots, A_{u,\ell}(y)) \in \mathcal{G}_{h_u}^\ell, \\ A_v(y) &= (A_{v,1}(y), A_{v,2}(y), \dots, A_{v,\ell}(y)) \in \mathcal{G}_{h_v}^\ell, \end{aligned}$$

$$\begin{aligned} A_w(y) &= (A_{w,1}(y), A_{w,2}(y), \dots, A_{w,\ell}(y)) \in \mathcal{G}_{h_w}^\ell \quad \text{and} \\ A_{\mu(w)}(y) &= (A_{\mu(w),1}(y), A_{\mu(w),2}(y), \dots, A_{\mu(w),\ell}(y)) \in \mathcal{G}_{h_{\mu(w)}}^\ell \end{aligned}$$

with $A_{u,i}(y) = a_i(y)e_{h_u} \in \mathcal{G}_{h_u}$, $A_{v,i}(y) = a_i(y)e_{h_v} \in \mathcal{G}_{h_v}$, $A_{w,i}(y) = a_i(y)e_{h_w} \in \mathcal{G}_{h_w}$ and $A_{\mu(w),i}(y) = a_i(y)e_{h_{\mu(w)}} \in \mathcal{G}_{h_{\mu(w)}}$ for $1 \leq u \leq r_1$, $r_1 + 1 \leq v \leq r_2$, $r_2 + 1 \leq w \leq r_3$ and $1 \leq i \leq \ell$. Further, by [8.9] and Theorem [8.4.1], we see that every additive H -QA code $\mathcal{C}$ of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ has a canonical decomposition of the form

$$\mathcal{C} = \left(\bigoplus_{u=1}^{r_1} \mathcal{C}_u \right) \oplus \left(\bigoplus_{v=r_1+1}^{r_2} \mathcal{C}_v \right) \oplus \left(\bigoplus_{w=r_2+1}^{r_3} (\mathcal{C}_w \oplus \mathcal{C}_{\mu(w)}) \right), \quad (8.10)$$

where $\mathcal{C}_u$ (resp. $\mathcal{C}_v$, $\mathcal{C}_w$ and $\mathcal{C}_{\mu(w)}$) is a subspace of $\mathcal{G}_{h_u}^\ell$ (resp. $\mathcal{G}_{h_v}^\ell$, $\mathcal{G}_{h_w}^\ell$ and $\mathcal{G}_{h_{\mu(w)}}^\ell$) over $\mathcal{F}_{h_u}$ (resp. $\mathcal{F}_{h_v}$, $\mathcal{F}_{h_w}$ and $\mathcal{F}_{h_{\mu(w)}}$) for each u (resp. v and w). Moreover, by [8.9] and Theorem [8.4.2], we observe that the σ -dual code $\mathcal{C}^{\perp_\sigma} (\subseteq \mathcal{G})$ of the code $\mathcal{C}$ has a canonical decomposition of the form

$$\mathcal{C}^{\perp_\sigma} = \left(\bigoplus_{u=1}^{r_1} \mathcal{C}_u^{\perp_\sigma} \right) \oplus \left(\bigoplus_{v=r_1+1}^{r_2} \mathcal{C}_v^{\perp_\sigma} \right) \oplus \left(\bigoplus_{w=r_2+1}^{r_3} (\mathcal{C}_{\mu(w)}^{\perp_\sigma} \oplus \mathcal{C}_w^{\perp_\sigma}) \right), \quad (8.11)$$

where $\mathcal{C}_u^{\perp_\sigma} \subseteq \mathcal{G}_{h_u}^\ell$ is the orthogonal complement of $\mathcal{C}_u$ with respect to $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ for $1 \leq u \leq r_1$, $\mathcal{C}_v^{\perp_\sigma} \subseteq \mathcal{G}_{h_v}^\ell$ is the orthogonal complement of $\mathcal{C}_v$ with respect to $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ for $r_1 + 1 \leq v \leq r_2$, $\mathcal{C}_w^{\perp_\sigma} \subseteq \mathcal{G}_{h_{\mu(w)}}^\ell$ is the orthogonal complement of $\mathcal{C}_w$ with respect to $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_w}^\ell \times \mathcal{G}_{h_{\mu(w)}}^\ell}$ and $\mathcal{C}_{\mu(w)}^{\perp_\sigma} \subseteq \mathcal{G}_{h_w}^\ell$ is the orthogonal complement of $\mathcal{C}_{\mu(w)}$ with respect to $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_{\mu(w)}}^\ell \times \mathcal{G}_{h_w}^\ell}$ for $r_2 + 1 \leq w \leq r_3$.

For $1 \leq \nu \leq r_2$, an $\mathcal{F}_{h_\nu}$ -subspace $\mathcal{C}_\nu$ of $\mathcal{G}_{h_\nu}^\ell$ is said to be

- (i) σ -self-orthogonal if it satisfies $\mathcal{C}_\nu \subseteq \mathcal{C}_\nu^{\perp_\sigma}$.
- (ii) σ -self-dual if it satisfies $\mathcal{C}_\nu = \mathcal{C}_\nu^{\perp_\sigma}$.
- (iii) σ -non-degenerate if it satisfies $\mathcal{C}_\nu \cap \mathcal{C}_\nu^{\perp_\sigma} = \{\mathbf{0}\}$.

We next observe the following:

Lemma 8.5.1. (a) For $1 \leq u \leq r_1$, the map $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_{h_u,0}$ and $\mathcal{F}_{h_u}$.

(b) For $r_1 + 1 \leq v \leq r_2$ and $0 \leq j \leq \kappa_{h_v} - 1$, the map $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_{h_v,j}$ of order 2.

(c) For $r_1 + 1 \leq v \leq r_2$, the map $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_{h_v}$ of order 2.

Proof. (a) Here we note that $d_u = |S_q(h_u)| = 1$, which gives $\kappa_{h_u} = \gcd(d_u, t) = 1$ and $D_u = \frac{d_u}{\kappa_{h_u}} = 1$. We also note that $e_{h_u} = e_{h_u,0}$. Further, by Corollary 8.4.1, we see that $\tau_{1,-1}(e_{h_u}) = e_{h_u}$. Now by Lemma 8.4.6, we see that $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_{h_u,0}$ and $\mathcal{F}_{h_u}$.

(b) Let $r_1 + 1 \leq v \leq r_2$ and $0 \leq j \leq \kappa_{h_v} - 1$ be fixed. Since $\tau_{1,-1}^2$ is the identity automorphism of $\mathcal{F}_{h_v,j}$, we note that $\tau_{1,-1}$ is either the identity automorphism or the automorphism of $\mathcal{F}_{h_v,j}$ of order 2. We assert that $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_{h_v,j}$ of order 2.

Suppose, on the contrary, that $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_{h_v,j}$. Now let $\theta = \sum_{k \in H} \theta_k y^k$ be a non-zero element of $\mathcal{F}_{h_v,j}$. Since $\tau_{1,-1}$ is the identity automorphism of $\mathcal{F}_{h_v,j}$, we have $\tau_{1,-1}(y^h \theta) = y^h \theta$ for all $h \in H$, which implies that $\sum_{k \in H} \theta_k y^{-(h+k)} = \sum_{k \in H} \theta_k y^{h+k}$ for all $h \in H$. This further implies that $\sum_{f \in H} \theta_{-(f+h)} y^f = \sum_{f \in H} \theta_{f-h} y^f$ for all $h \in H$. From this, it follows that

$$\theta_g = \theta_{-(g+2h)} \text{ holds for all } g, h \in H. \quad (8.12)$$

Now when m is odd, we see that $\{-2h : h \in H\} = H$. This, by (8.12), implies that $\theta_h = \theta_0$ for all $h \in H$. From this and by Lemma 8.4.6(a), we get

$$\theta = \theta_0 \sum_{k \in H} y^k = m\theta_0 \left(\frac{1}{m} \sum_{k \in H} y^k \right) = m\theta_0 e_0 \in \mathcal{F}_{0,0}.$$

This implies that $\theta \in \mathcal{F}_{0,0} \cap \mathcal{F}_{h_v,j} = \{0\}$, i.e., $\theta = 0$, which is a contradiction.

On the other hand, when m is even, we see that q is odd and that there exists an element $k \in H$ such that $\text{ord}(k) = 2$. Here working as in Lemma 8.4.6(b), we

see that $H = X \cup (b + X)$, where $X = \{a \in H : \chi_k(a) = 1\}$ is a proper subgroup of H and the element $b \in H$ satisfies $\chi_k(b) = -1$. Since $\{-2h : h \in H\} = X$, we see, by (8.12), that $\theta_0 = \theta_x$ for all $x \in X$. We also note that $\{-(b + 2h) : h \in H\} = b + X$, which, by (8.12) again, gives $\theta_b = \theta_{b+x}$ for all $x \in X$. We also see, by Lemma 8.4.6, that

$$me_0 = \sum_{x \in X} y^x + \sum_{x \in X} y^{b+x}$$

and

$$me_k = \sum_{x \in X} y^x - \sum_{x \in X} y^{b+x}.$$

From this, it follows that

$$\theta = \sum_{k \in H} \theta_k y^k = \theta_0 \sum_{x \in X} y^x + \theta_b \sum_{x \in X} y^{b+x} = \frac{m}{2} (\theta_0(e_0 + e_k) + \theta_b(e_0 - e_k)) \in \mathcal{F}_{0,0} \oplus \mathcal{F}_{k,0}.$$

This shows that $\theta \in \mathcal{F}_{h_v,j} \cap (\mathcal{F}_{0,0} \oplus \mathcal{F}_{k,0}) = \{0\}$, i.e., $\theta = 0$, which is a contradiction.

This shows that $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_{h_v,j}$ of order 2.

(c) Working as in part (b), the desired result follows. □

In the following lemma, we study some basic properties of the restriction maps $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ and $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ for $1 \leq u \leq r_1$ and $r_1 + 1 \leq v \leq r_2$, where $\sigma \in \{0, \gamma, *\}$.

Lemma 8.5.2. *Let $1 \leq u \leq r_1$ and $r_1 + 1 \leq v \leq r_2$ be fixed. The following hold.*

- (a) *For $\sigma \in \{0, \gamma, *\}$, the restriction map $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ (resp. $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$) is reflexive and non-degenerate $\tau_{1,-1}$ -sesquilinear form on $\mathcal{G}_{h_u}^\ell$ (resp. $\mathcal{G}_{h_v}^\ell$).*
- (b) *For $\sigma \in \{0, *\}$, the form $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ is symmetric, while the form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ is alternating.*
- (c) *For $\sigma \in \{0, *\}$, the form $[\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ is Hermitian, while the form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ is skew-Hermitian.*

Proof. Working as in Lemma 8.4.9 and using Lemma 8.5.1, the desired result follows. $\square$

In the following theorem, we characterize all σ -self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.5.1. *Let $\mathcal{C} = \left(\bigoplus_{u=1}^{r_1} \mathcal{C}_u \right) \oplus \left(\bigoplus_{v=r_1+1}^{r_2} \mathcal{C}_v \right) \oplus \left(\bigoplus_{w=r_2+1}^{r_3} (\mathcal{C}_w \oplus \mathcal{C}_{\mu(w)}) \right)$ be an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. Then for $\sigma \in \{0, \gamma, *\}$, the following hold.*

(a) *The code $\mathcal{C}$ is σ -self-orthogonal if and only if*

- $\mathcal{C}_u$ is a σ -self-orthogonal $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ (i.e., $\mathcal{C}_u \subseteq \mathcal{C}_u^{\perp_\sigma}$) for $1 \leq u \leq r_1$,
- $\mathcal{C}_v$ is a σ -self-orthogonal $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ (i.e., $\mathcal{C}_v \subseteq \mathcal{C}_v^{\perp_\sigma}$) for $r_1 + 1 \leq v \leq r_2$, and
- $\mathcal{C}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_{\mu(w)} \subseteq \mathcal{C}_w^{\perp_\sigma}$ for $r_2 + 1 \leq w \leq r_3$.

As a consequence, the total number $\mathcal{M}$ of distinct σ -self-orthogonal additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by

$$\mathcal{M} = \prod_{u=1}^{r_1} \mathcal{M}_u \prod_{v=r_1+1}^{r_2} \mathcal{M}_v \prod_{w=r_2+1}^{r_3} \mathcal{M}_w, \quad (8.13)$$

where $\mathcal{M}_u$ denotes the number of distinct σ -self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ for $1 \leq u \leq r_1$, $\mathcal{M}_v$ denotes the number of distinct σ -self-orthogonal $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ for $r_1 + 1 \leq v \leq r_2$, and $\mathcal{M}_w$ denotes the number of distinct pairs $(\mathcal{C}_w, \mathcal{C}_{\mu(w)})$, where $\mathcal{C}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_{\mu(w)} \subseteq \mathcal{C}_w^{\perp_\sigma}$ for $r_2 + 1 \leq w \leq r_3$.

(b) *The code $\mathcal{C}$ is σ -self-dual if and only if*

- the integer lt is even,
- either q is even or ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $lt \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$ in the case when $\sigma \in \{0, *\}$,

- $\mathcal{C}_u$ is a σ -self-dual $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ (i.e., $\mathcal{C}_u = \mathcal{C}_u^{\perp\sigma}$) for $1 \leq u \leq r_1$,
- $\mathcal{C}_v$ is a σ -self-dual $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ (i.e., $\mathcal{C}_v = \mathcal{C}_v^{\perp\sigma}$) for $r_1+1 \leq v \leq r_2$,
and
- $\mathcal{C}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_{\mu(w)} = \mathcal{C}_w^{\perp\sigma}$ for $r_2+1 \leq w \leq r_3$.

As a consequence, the total number $\mathcal{N}$ of distinct σ -self-dual additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by

$$\mathcal{N} = \prod_{u=1}^{r_1} \mathcal{N}_u \prod_{v=r_1+1}^{r_2} \mathcal{N}_v \prod_{w=r_2+1}^{r_3} \mathcal{N}_w,$$

where $\mathcal{N}_u$ denotes the number of distinct σ -self-dual $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ for $1 \leq u \leq r_1$, $\mathcal{N}_v$ denotes the number of distinct σ -self-dual $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ for $r_1+1 \leq v \leq r_2$, and $\mathcal{N}_w$ denotes the number of distinct $\mathcal{F}_{h_w}$ -subspaces of $\mathcal{G}_{h_w}^\ell$ for $r_2+1 \leq w \leq r_3$.

(c) The code $\mathcal{C}$ is σ -ACD if and only if

- $\mathcal{C}_u$ is an $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ satisfying $\mathcal{C}_u \cap \mathcal{C}_u^{\perp\sigma} = \{\mathbf{0}\}$ (i.e., $\mathcal{C}_u$ is a σ -non-degenerate $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$) for $1 \leq u \leq r_1$,
- $\mathcal{C}_v$ is an $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ satisfying $\mathcal{C}_v \cap \mathcal{C}_v^{\perp\sigma} = \{\mathbf{0}\}$ (i.e., $\mathcal{C}_v$ is a σ -non-degenerate $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$) for $r_1+1 \leq v \leq r_2$, and
- $\mathcal{C}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_w \cap \mathcal{C}_{\mu(w)}^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_{\mu(w)} \cap \mathcal{C}_w^{\perp\sigma} = \{\mathbf{0}\}$ for $r_2+1 \leq w \leq r_3$.

As a consequence, the total number $\mathcal{L}$ of distinct σ -ACD H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by

$$\mathcal{L} = \prod_{u=1}^{r_1} \mathcal{L}_u \prod_{v=r_1+1}^{r_2} \mathcal{L}_v \prod_{w=r_2+1}^{r_3} \mathcal{L}_w, \quad (8.14)$$

where $\mathcal{L}_u$ denotes the number of distinct σ -non-degenerate $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ for $1 \leq u \leq r_1$, $\mathcal{L}_v$ denotes the number of distinct σ -non-degenerate $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ for $r_1+1 \leq v \leq r_2$, and $\mathcal{L}_w$ denotes the number of distinct pairs

$(\mathcal{C}_w, \mathcal{C}_{\mu(w)})$ with $\mathcal{C}_w$ as an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ as an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_w \cap \mathcal{C}_{\mu(w)}^{\perp_\sigma} = \{0\}$ and $\mathcal{C}_{\mu(w)} \cap \mathcal{C}_w^{\perp_\sigma} = \{0\}$ for $r_2 + 1 \leq w \leq r_3$.

Proof. To prove the result, we first see, by Theorem 8.4.2, that if there exists a σ -self-dual $\mathcal{F}_{h_u}$ -subspace $\mathcal{C}_u$ of $\mathcal{G}_{h_u}^\ell$, then the integer ℓt must be even and $\dim_{\mathcal{F}_{h_u}} \mathcal{C}_u = \frac{\ell t}{2}$. When $\sigma \in \{0, *\}$, we see that there exists a σ -self-dual $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ if and only if the Witt index of $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is $\frac{\ell t}{2}$, which, by Theorems 2.2.6 and 2.2.8, holds if and only if either both $\ell t, q$ are even or ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$. On the other hand, when $\sigma = \gamma$, we see, by Theorem 2.2.3, that the Witt index of $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is $\frac{\ell t}{2}$, so there exists a γ -self-dual $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$. Now the desired result follows by (8.10) and (8.11) and applying Theorem 8.4.2. $\square$

In the following theorem, we provide necessary and sufficient conditions for the existence of a σ -self-dual additive H -QA code over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.5.2. (a) For $\sigma \in \{0, *\}$, there exists a σ -self-dual additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ if and only if either both $\ell t, q$ are even or ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$.

(b) There exists a γ -self-dual additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ if and only if the integer ℓt is even.

Proof. It follows immediately from Theorem 8.5.1. $\square$

8.6 Enumeration of σ -self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes over finite fields

In this section, we provide enumeration formulae for all σ -self-orthogonal, σ -self-dual and σ -ACD additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ by applying Theorem 8.5.1 and the Witt decomposition theory, where $\sigma \in \{0, \gamma, *\}$.

8.6.1 Enumeration formula for σ -self-orthogonal additive H -QA codes

In the following theorem, we enumerate all distinct σ -self-orthogonal additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.6.1. *For $\sigma \in \{0, \gamma, *\}$, the total number $\mathcal{M}$ of distinct σ -self-orthogonal additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by*

$$\mathcal{M} = \prod_{u=1}^{r_1} \mathcal{M}_u \prod_{v=r_1+1}^{r_2} \mathcal{M}_v \prod_{w=r_2+1}^{r_3} \left(\sum_{k_1=0}^{\ell t} \sum_{k_2=0}^{\ell t-k_1} \begin{bmatrix} \ell t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \ell t - k_1 \\ k_2 \end{bmatrix}_{q^{d_w}} \right),$$

where for $1 \leq u \leq r_1$, the number $\mathcal{M}_u$ equals

- $\sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-2}{2}} + 1)$ when $\sigma \in \{0, *\}$ with either ℓ being even and $q \equiv 1 \pmod{4}$ or ℓ being even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ being odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\ell t-2)/2} \begin{bmatrix} (\ell t-2)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i}{2}} + 1)$ when $\sigma \in \{0, *\}$ with either ℓ being odd, t even and $q \equiv 1 \pmod{4}$ or ℓ being odd, $t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or $\ell \equiv 2 \pmod{4}$, t being odd and $q \equiv 3 \pmod{4}$;
- $\sum_{k=0}^{(\ell t-1)/2} \begin{bmatrix} (\ell t-1)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-1}{2}} + 1)$ when $\sigma \in \{0, *\}$ and both $\ell t, q$ are odd;
- $\sum_{k=0}^{(\ell t-1)/2} \begin{bmatrix} (\ell t-1)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-1}{2}} + 1)$ when $\sigma = 0$, q is even and ℓt is odd;
- $\sum_{k=0}^{(\ell t-2)/2} \begin{bmatrix} (\ell t-2)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-2}{2}} + 1) + \sum_{k=1}^{\ell t/2} q^{\ell t-2k} \begin{bmatrix} (\ell t-2)/2 \\ k-1 \end{bmatrix}_q \prod_{j=0}^{k-2} (q^{\frac{\ell t-2j-2}{2}} + 1)$ when $\sigma = 0$ and both $q, \ell t$ are even;
- $\sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i}{2}} + 1)$ when either $\sigma = \gamma$ or $\sigma = *$ and both $\ell t, q$ are even,

while for $r_1 + 1 \leq v \leq r_2$, the number $\mathcal{M}_v$ equals

$$\begin{aligned} & \bullet \sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_{q^{dv}} \prod_{i=0}^{k-1} (q^{\frac{dv(\ell t-2i-1)}{2}} + 1) \text{ when } \sigma \in \{0, \gamma, *\} \text{ and } \ell t \text{ is even;} \\ & \bullet \sum_{k=0}^{(\ell t-1)/2} \begin{bmatrix} (\ell t-1)/2 \\ k \end{bmatrix}_{q^{dv}} \prod_{i=0}^{k-1} (q^{\frac{dv(\ell t-2i)}{2}} + 1) \text{ when } \sigma \in \{0, *\} \text{ and } \ell t \text{ is odd.} \end{aligned}$$

To prove the above theorem, we see, by Theorem 8.5.1, that it is enough to determine the numbers $\mathcal{M}_u$, $\mathcal{M}_v$ and $\mathcal{M}_w$ for $1 \leq u \leq r_1$, $r_1 + 1 \leq v \leq r_2$ and $r_2 + 1 \leq w \leq r_3$.

In the following lemma, we determine the number $\mathcal{M}_u$ for $1 \leq u \leq r_1$ when $\sigma \in \{0, *\}$ and q is odd.

Lemma 8.6.1. *Let $1 \leq u \leq r_1$ be fixed. When $\sigma \in \{0, *\}$ and q is an odd prime power, we have*

$$\mathcal{M}_u = \begin{cases} \sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-2}{2}} + 1) & \text{if either } \ell \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ is} \\ & \text{even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or} \\ & \ell \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \sum_{k=0}^{(\ell t-2)/2} \begin{bmatrix} (\ell t-2)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i}{2}} + 1) & \text{if either } \ell \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \\ & \text{or } \ell \text{ is odd, } t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \\ & \text{or } \ell \equiv 2 \pmod{4}, t \text{ is odd and } q \equiv 3 \pmod{4}; \\ \sum_{k=0}^{(\ell t-1)/2} \begin{bmatrix} (\ell t-1)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i-1}{2}} + 1) & \text{if } \ell t \text{ is odd.} \end{cases}$$

Proof. To prove the result, we see, by Lemma 8.5.2(a) and (b), that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is an (ℓt) -dimensional orthogonal space over $\mathcal{F}_{h_u} \simeq \mathbb{F}_q$. Since q is odd, we see that the space $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ can also be viewed as a non-degenerate quadratic space $(\mathcal{G}_{h_u}^\ell, \mathcal{Q}_u)$ over $\mathcal{F}_{h_u}$, where $\mathcal{Q}_u : \mathcal{G}_{h_u}^\ell \rightarrow \mathcal{F}_{h_u}$ is the quadratic map, defined as

$$\mathcal{Q}_u(A_u(y)) = \frac{1}{2}[A_u(y), A_u(y)]_\sigma \text{ for all } A_u(y) \in \mathcal{G}_{h_u}^\ell.$$

Further, by Theorem 2.2.6, we note that the Witt index $\mathfrak{m}_u$ of the quadratic space

$(\mathcal{G}_{h_u}^\ell, \mathcal{Q}_u)$ is given by

$$\mathfrak{m}_u = \begin{cases} \frac{\ell t - 1}{2} & \text{if } \ell t \text{ is odd;} \\ \frac{\ell t}{2} & \text{if either } \ell \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ is even, } \ell t \equiv 0 \pmod{4} \text{ and} \\ & q \equiv 3 \pmod{4} \text{ or } \ell \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \frac{\ell t - 2}{2} & \text{if either } \ell \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ is odd, } t \equiv 0 \pmod{4} \\ & \text{and } q \equiv 3 \pmod{4} \text{ or } \ell \equiv 2 \pmod{4}, t \text{ is odd and } q \equiv 3 \pmod{4}. \end{cases} \quad (8.15)$$

Now by Theorem 2.2.5(e), we get

$$\mathcal{M}_u = \sum_{k=0}^{\mathfrak{m}_u} \left(\begin{bmatrix} \mathfrak{m}_u \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\mathfrak{m}_u - \varsigma_u - i} + 1) \right),$$

where $\varsigma_u = 2\mathfrak{m}_u - \ell t + 1$. Now, substituting the values of $\mathfrak{m}_u$ from (8.15) in the respective cases, the desired result follows. $\square$

In the following lemma, we determine the number $\mathcal{M}_u$ for $1 \leq u \leq r_1$ when $\sigma = 0$ and q is even.

Lemma 8.6.2. *Let $1 \leq u \leq r_1$ be fixed. When $\sigma = 0$ and q is an even prime power, we have*

$$\mathcal{M}_u = \begin{cases} \sum_{k=0}^{(\ell t - 1)/2} \begin{bmatrix} (\ell t - 1)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 1}{2}} + 1) & \text{if } \ell t \text{ is odd;} \\ \sum_{k=0}^{(\ell t - 2)/2} \begin{bmatrix} (\ell t - 2)/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 2}{2}} + 1) \\ + \sum_{k=1}^{\ell t/2} q^{\ell t - 2k} \begin{bmatrix} (\ell t - 2)/2 \\ k - 1 \end{bmatrix}_q \prod_{j=0}^{k-2} (q^{\frac{\ell t - 2j - 2}{2}} + 1) & \text{if } \ell t \text{ is even.} \end{cases}$$

Proof. To prove the result, we see, by Lemma 8.4.3, that $d_u = |S_q(h_u)| = 1$ and $\kappa_{h_u} = \gcd(t, d_u) = 1$. This implies that $e_{h_u,0} = e_{h_u}$, which gives $\mathcal{G}_{h_u} = \mathcal{F}_{h_u,0}$. We further note, by Lemma 8.4.6, that each $A_u(y) \in \mathcal{G}_{h_u}^\ell$ is of the form

$$A_u(y) = (A_{u,1}(y), A_{u,2}(y), \dots, A_{u,\ell}(y)) \in \mathcal{G}_{h_u}^\ell,$$

where $A_{u,i}(y) = \theta_i e_{h_u} \in \mathcal{F}_{h_u,0}$ with $\theta_i \in \mathbb{F}_{q^t}$ for each i . We further note that

$$\sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \tau_{q^w,1}(A_{u,i}(y)) = \sum_{i=1}^{\ell} \sum_{w=0}^{t-1} \theta_i^{q^w} e_{h_u} = \sum_{i=1}^{\ell} \text{Tr}_{q^t,q}(\theta_i) e_{h_u}.$$

Now let us define the set

$$\mathcal{W}_u = \left\{ A_u(y) = (\theta_1 e_{h_u}, \theta_2 e_{h_u}, \dots, \theta_{\ell} e_{h_u}) \in \mathcal{G}_{h_u}^{\ell} : \sum_{i=1}^{\ell} \text{Tr}_{q^t,q}(\theta_i) e_{h_u} = 0 \right\}. \quad (8.16)$$

It is easy to observe that $\mathcal{W}_u$ is an $(\ell t - 1)$ -dimensional $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^{\ell}$. Let us denote $\mathbf{1}_u = (\underbrace{e_{h_u}, e_{h_u}, \dots, e_{h_u}}_{\ell \text{ times}}) \in \mathcal{G}_{h_u}^{\ell}$. It is easy to see that $\mathbf{1}_u \in \mathcal{W}_u$ if and only if ℓt is an even integer. Now the following two cases arise: (i) ℓt is odd and (ii) ℓt is even.

- (i) Let ℓt be odd. In this case, we observe that $\mathbf{1}_u \notin \mathcal{W}_u$ and $\dim_{\mathcal{F}_{h_u}} \langle \mathbf{1}_u \rangle = 1$. Next, we see that $[A_u(y), \mathbf{1}_u]_0 = 0$ for all $A_u(y) \in \mathcal{W}_u$ and $\mathcal{W}_u \cap \langle \mathbf{1}_u \rangle = \{\mathbf{0}\}$. This implies that $\mathcal{G}_{h_u}^{\ell} = \mathcal{W}_u \perp \langle \mathbf{1}_u \rangle$, i.e., $\mathcal{G}_{h_u}^{\ell}$ is the orthogonal direct sum of $\mathcal{W}_u$ and $\langle \mathbf{1}_u \rangle$. We further note that any 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^{\ell}$ is contained in $\mathcal{W}_u$.

Next, we assert that the restriction $[\cdot, \cdot]_0 \upharpoonright_{\mathcal{W}_u \times \mathcal{W}_u}$ of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0$ to $\mathcal{W}_u \times \mathcal{W}_u$ is non-degenerate. For this, suppose that there exists $A_u(y) \in \mathcal{W}_u$ satisfying $[A_u(y), B_u(y)]_0 = 0$ for all $B_u(y) \in \mathcal{W}_u$. We will now prove that $A_u(y) = \mathbf{0}$.

For this, let $C_u(y) = B_u(y) + \alpha_u(y) \mathbf{1}_u$, where $\alpha_u(y) \in \mathcal{F}_{h_u}$. As $\alpha_u(y)$ runs over $\mathcal{F}_{h_u}$ and $B_u(y)$ runs over $\mathcal{W}_u$, we see that $C_u(y)$ runs over $\mathcal{W}_u$. We observe that $[A_u(y), C_u(y)]_0 = [A_u(y), B_u(y)]_0 + \alpha_u(y) [A_u(y), \mathbf{1}_u]_0 = 0$ for all $C_u(y) \in \mathcal{W}_u$. By Lemma 8.5.2, we see that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0$ is non-degenerate on $\mathcal{G}_{h_u}^{\ell}$, which gives $A_u(y) = \mathbf{0}$. This proves the assertion.

Next, for each $A_u(y) \in \mathcal{W}_u$, we observe that $[A_u(y), A_u(y)]_0 = 0$. This shows that $(\mathcal{W}_u, [\cdot, \cdot]_0 \upharpoonright_{\mathcal{W}_u \times \mathcal{W}_u})$ is an $(\ell t - 1)$ -dimensional symplectic space over $\mathcal{F}_{h_u}$. By Theorem 2.2.3(a), we see that $\mathcal{W}_u$ has Witt index $\frac{\ell t - 1}{2}$. Now by Theorem 2.2.3(e), we see, for $0 \leq k \leq \frac{\ell t - 1}{2}$, that $\mathcal{W}_u$ (and hence $\mathcal{G}_{h_u}^{\ell}$) has precisely

$$\left[\begin{matrix} (\ell t - 1)/2 \\ k \end{matrix} \right]_q \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 1}{2}} + 1)$$

distinct k -dimensional 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces. From this, the number $\mathcal{M}_u$ is given by

$$\mathcal{M}_u = \sum_{k=0}^{(\ell t - 1)/2} \left(\left[\begin{matrix} (\ell t - 1)/2 \\ k \end{matrix} \right]_q \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 1}{2}} + 1) \right).$$

(ii) Next, let ℓt be even. In this case, we see that $\mathbf{1}_u \in \mathcal{W}_u \cap \mathcal{W}_u^{\perp_0}$. Let $\widehat{\mathcal{W}}_u$ be an $(\ell t - 2)$ -dimensional $\mathcal{F}_{h_u}$ -subspace of $\mathcal{W}_u$ such that $\mathbf{1}_u \notin \widehat{\mathcal{W}}_u$. Here, we note that $\mathcal{W}_u = \widehat{\mathcal{W}}_u \oplus \langle \mathbf{1}_u \rangle$. Further, there exists $z_u(y) \in \widehat{\mathcal{W}}_u^{\perp_0} \setminus \mathcal{W}_u$. One can easily see that $\mathcal{G}_{h_u}^\ell = \widehat{\mathcal{W}}_u \oplus \langle \mathbf{1}_u \rangle \oplus \langle z_u(y) \rangle$. We next observe that any 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ is either contained in $\widehat{\mathcal{W}}_u$ or contained in $\widehat{\mathcal{W}}_u \oplus \langle \mathbf{1}_u \rangle$ but not in $\widehat{\mathcal{W}}_u$.

- First of all, we count all distinct 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of $\widehat{\mathcal{W}}_u$. Toward this, we note that $[A_u(y), A_u(y)]_0 = 0$ for all $A_u(y) \in \widehat{\mathcal{W}}_u$. Now we assert that the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathcal{W}}_u \times \widehat{\mathcal{W}}_u}$ is non-degenerate. For this, suppose that there exists $A_u(y) \in \widehat{\mathcal{W}}_u$ satisfying $[A_u(y), B_u(y)]_0 = 0$ for all $B_u(y) \in \widehat{\mathcal{W}}_u$. Here, it is enough to show that $A_u(y) = \mathbf{0}$. Let $C_u(y) = B_u(y) + \alpha_u(y)z_u(y) + \beta_u(y)\mathbf{1}_u \in \mathcal{G}_{h_u}^\ell$, where $\alpha_u(y), \beta_u(y) \in \mathcal{F}_{h_u}$. We note that as $A_u(y)$ runs over the set $\widehat{\mathcal{W}}_u$ and the elements $\alpha_u(y), \beta_u(y)$ run over the set $\mathcal{F}_{h_u}$, the element $C_u(y)$ runs over $\mathcal{G}_{h_u}^\ell$. We next see that

$$[A_u(y), C_u(y)]_0 = [A_u(y), B_u(y)]_0 + \alpha_u(y)[A_u(y), z_u(y)]_0 + \beta_u(y)[A_u(y), \mathbf{1}_u]_0 = 0$$

for all $C_u(y) \in \mathcal{G}_{h_u}^\ell$. Since the map $[\cdot, \cdot]_0$ is non-degenerate on $\mathcal{G}_{h_u}^\ell$, we have $A_u(y) = \mathbf{0}$. From this, it follows that $(\widehat{\mathcal{W}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathcal{W}}_u \times \widehat{\mathcal{W}}_u})$ is an $(\ell t - 2)$ -dimensional symplectic $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ with the Witt index $\frac{\ell t - 2}{2}$. Now by Theorem 2.2.3(e), we see, for $0 \leq k \leq \frac{\ell t - 2}{2}$, that $\mathcal{G}_{h_u}^\ell$ has precisely $\left[\begin{matrix} (\ell t - 2)/2 \\ k \end{matrix} \right]_q \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 2}{2}} + 1)$ distinct k -dimensional 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces, which are contained in $\widehat{\mathcal{W}}_u$. This implies that the number $\mathcal{T}_u$

of distinct 0-self-orthogonal $\mathcal{F}_u$ -subspaces of $\widehat{\mathcal{W}}_u$ is given by

$$\mathcal{T}_u = \sum_{k=0}^{(\ell t - 2)/2} \begin{bmatrix} (\ell t - 2)/2 \\ k \end{bmatrix} \prod_{i=0}^{k-1} (q^{\frac{\ell t - 2i - 2}{2}} + 1).$$

- Now we shall count all distinct 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ that are contained in $\widehat{\mathcal{W}}_u \oplus \langle \mathbf{1}_u \rangle$ but not in $\widehat{\mathcal{W}}_u$. For this, let U be such a k -dimensional 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$, where $1 \leq k \leq \frac{\ell t}{2}$. One can easily see that U has a basis of the form $\{A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y), A_u^{(k)}(y) + \mathbf{1}_u\}$, where $A_u^{(j)}(y) \in \widehat{\mathcal{W}}_u \setminus \{\mathbf{0}\}$ for $1 \leq j \leq k-1$ and $A_u^{(k)}(y) \in \widehat{\mathcal{W}}_u$. Further, we note that $U \subseteq U^{\perp_0}$ if and only if

$$\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle \subseteq \langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0}$$

and $A_u^{(k)}(y) \in \langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0}$.

Since $(\widehat{\mathcal{W}}_u, [\cdot, \cdot]_0 \upharpoonright_{\widehat{\mathcal{W}}_u \times \widehat{\mathcal{W}}_u})$ is a symplectic space of dimension $(\ell t - 2)$ and Witt index $\frac{\ell t - 2}{2}$, we see, by Theorem 2.2.3(e), that for $1 \leq k \leq \ell t/2$, $\widehat{\mathcal{W}}_u$ has precisely

$$\begin{bmatrix} (\ell t - 2)/2 \\ k - 1 \end{bmatrix} \prod_{j=0}^{k-2} (q^{\frac{\ell t - 2j - 2}{2}} + 1)$$

distinct $(k - 1)$ -dimensional 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of the type $\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle$.

Further, for a given $(k - 1)$ -dimensional 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspace $\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle$ of $\widehat{\mathcal{W}}_u$ and $A_u^{(k)}(y), B_u^{(k)}(y) \in \langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0}$, we observe that

$$\langle A_u^{(1)}(y), \dots, A_u^{(k-1)}(y), A_u^{(k)}(y) + \mathbf{1}_u \rangle = \langle A_u^{(1)}(y), \dots, A_u^{(k-1)}(y), B_u^{(k)}(y) + \mathbf{1}_u \rangle$$

if and only if $A_u^{(k)}(y) - B_u^{(k)}(y) \in \langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0}$, which holds if and only if both $A_u^{(k)}(y), B_u^{(k)}(y)$ belong to the same coset of $\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle$ in $\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0}$. Since the $\mathcal{F}_{h_u}$ -dimension of $\langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle^{\perp_0} / \langle A_u^{(1)}(y), A_u^{(2)}(y), \dots, A_u^{(k-1)}(y) \rangle$ is $\ell t - 2k$, there are precisely $q^{\ell t - 2k}$ relevant choices for

$A_u^{(k)}(y)$. This shows that there are precisely

$$\mathcal{U}_u = \sum_{k=1}^{\ell t/2} \left(q^{\ell t-2k} \begin{bmatrix} (\ell t-2)/2 \\ k-1 \end{bmatrix}_q \prod_{j=0}^{k-2} (q^{\frac{\ell t-2j-2}{2}} + 1) \right)$$

distinct 0-self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$, which are contained in $\widehat{\mathcal{W}}_u \oplus \langle \mathbf{1}_u \rangle$ but not in $\widehat{\mathcal{W}}_u$.

Combining both cases, we obtain

$$\begin{aligned} \mathcal{M}_u = \mathcal{T}_u + \mathcal{U}_u &= \sum_{k=0}^{(\ell t-2)/2} \left(\begin{bmatrix} (\ell t-2)/2 \\ k \end{bmatrix}_q \prod_{j=0}^{k-1} (q^{\frac{\ell t-2j-2}{2}} + 1) \right) \\ &\quad + \sum_{k=1}^{\ell t/2} \left(q^{\ell t-2k} \begin{bmatrix} (\ell t-2)/2 \\ k-1 \end{bmatrix}_q \prod_{j=0}^{k-2} (q^{\frac{\ell t-2j-2}{2}} + 1) \right). \end{aligned}$$

From this, the desired result follows. $\square$

In the following lemma, we determine the number $\mathcal{M}_u$ for $1 \leq u \leq r_1$ when either $\sigma = \gamma$ or $\sigma = *$ and q is even.

Lemma 8.6.3. *Let $1 \leq u \leq r_1$ be fixed. When either $\sigma = \gamma$ or $\sigma = *$ and q is even, we have*

$$\mathcal{M}_u = \sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i}{2}} + 1).$$

Proof. To prove the result, we see, by Lemma 8.5.2(a) and (b), that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is a symplectic space of dimension ℓt over $\mathcal{F}_{h_u} \simeq \mathbb{F}_q$. Moreover, when $\sigma = *$ and q is even, by (8.8), we observe that $[A_u(y), A_u(y)]_* = 0$ for all $A_u(y) \in \mathcal{G}_{h_u}^\ell$. This, by Lemma 8.5.2(a) and (b), implies that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is a symplectic space of dimension ℓt over $\mathcal{F}_{h_u}$. We further note, by Theorem 2.2.3(a), that the Witt index of $\mathcal{G}_{h_u}^\ell$ is $\frac{\ell t}{2}$. Using this and by Theorem 2.2.3(e), we see that the number $\mathcal{M}_u$ of distinct σ -self-orthogonal $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ is given by

$$\mathcal{M}_u = \sum_{k=0}^{\ell t/2} \left(\begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_q \prod_{i=0}^{k-1} (q^{\frac{\ell t-2i}{2}} + 1) \right).$$

$\square$

In the following lemma, we determine the number $\mathcal{M}_v$ for $r_1 + 1 \leq v \leq r_2$, where $\sigma \in \{0, \gamma, *\}$.

Lemma 8.6.4. *Let $r_1 + 1 \leq v \leq r_2$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathcal{M}_v = \begin{cases} \sum_{k=0}^{\ell t/2} \begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_{q^{d_v}} \prod_{i=0}^{k-1} (q^{\frac{d_v(\ell t - 2i - 1)}{2}} + 1) & \text{when } \sigma \in \{0, \gamma, *\} \text{ and } \ell t \text{ is even;} \\ \sum_{k=0}^{(\ell t - 1)/2} \begin{bmatrix} (\ell t - 1)/2 \\ k \end{bmatrix}_{q^{d_v}} \prod_{i=0}^{k-1} (q^{\frac{d_v(\ell t - 2i)}{2}} + 1) & \text{when } \sigma \in \{0, *\} \text{ and } \ell t \text{ is odd.} \end{cases}$$

Proof. To prove the result, we recall that $\mathcal{F}_{h_v} \simeq \mathbb{F}_{q^{d_v}}$. Further, by Lemma 8.4.1(d), we see that $d_v = |S_q(h_v)|$ is an even integer. Here we shall consider the following two cases separately: (i) $\sigma \in \{0, *\}$ and (ii) $\sigma = \gamma$.

- (i) Let $\sigma \in \{0, *\}$. Here we note, by Lemma 8.5.2(a) and (c), that $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is a unitary space of dimension ℓt over $\mathcal{F}_{h_v}$. Further, by Theorem 2.2.4(a), we see that the Witt index ϑ_v of the unitary space $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is given by

$$\vartheta_v = \begin{cases} \frac{\ell t}{2} & \text{if } \ell t \text{ is even;} \\ \frac{\ell t - 1}{2} & \text{if } \ell t \text{ is odd.} \end{cases} \quad (8.17)$$

Now by applying Theorem 2.2.4(f), we see that the number $\mathcal{M}_v$ of distinct σ -self-orthogonal $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ is given by

$$\mathcal{M}_v = \sum_{k=0}^{\vartheta_v} \left(\begin{bmatrix} \vartheta_v \\ k \end{bmatrix}_{q^{d_v}} \prod_{i=0}^{k-1} (q^{d_v(\vartheta_v - \rho - i)} + 1) \right),$$

where $\rho = \frac{1}{2}$ if ℓt is even and $\rho = \frac{-1}{2}$ if ℓt is odd. Further, by substituting the values of ϑ_v from (8.17) in the respective cases, the desired result follows immediately.

- (ii) Next, let $\sigma = \gamma$. Here we first note that t (and hence ℓt) is an even integer. In this case, by Lemma 8.5.2(a) and (c), we note that $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form. We will first transform the form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ to an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$. To do this, we see, by Lemma 8.5.1(c),

that $\tau_{1,-1}$ is the automorphism of $\mathcal{F}_{h_v}$ of order 2. So there exists a non-zero element $\xi_v(y) \in \mathcal{F}_{h_v}$ such that $\tau_{1,-1}(\xi_v(y)) \neq \xi_v(y)$. Let $\theta_v(y) = \xi_v(y) - \tau_{1,-1}(\xi_v(y)) (\neq 0) \in \mathcal{F}_{h_v}$. Note that $\tau_{1,-1}(\theta_v(y)) = -\theta_v(y)$. Now it is easy to observe that the map $[\cdot, \cdot]_{\gamma_H} : \mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell \rightarrow \mathcal{F}_{h_v}$, defined as

$$[A_v(y), B_v(y)]_{\gamma_H} = \theta_v(y)[A_v(y), B_v(y)]_\gamma$$

for all $A_v(y), B_v(y) \in \mathcal{G}_{h_v}^\ell$, is a non-degenerate Hermitian $\tau_{1,-1}$ -sesquilinear form on $\mathcal{G}_{h_v}^\ell$. Thus $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is a unitary space of dimension ℓt over $\mathcal{F}_{h_v}$. Further, as $\theta_v(y) \in \mathcal{F}_{h_v} \setminus \{0\}$, we see that an $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ is γ -self-orthogonal if and only if it is self-orthogonal with respect to the form $[\cdot, \cdot]_{\gamma_H}$. Thus the total number of distinct γ -self-orthogonal $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ is equal to the number of self-orthogonal $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ with respect to $[\cdot, \cdot]_{\gamma_H}$. Now working as in case (i), we obtain

$$\mathcal{N}_v = \sum_{k=0}^{\ell t/2} \left(\begin{bmatrix} \ell t/2 \\ k \end{bmatrix}_{q^{d_v}} \prod_{i=0}^{k-1} (q^{\frac{d_v(\ell t - 2i - 1)}{2}} + 1) \right).$$

□

In the following lemma, we determine $\mathcal{M}_w$ for $r_2 + 1 \leq w \leq r_3$, where $\sigma \in \{0, \gamma, *\}$.

Lemma 8.6.5. *Let $r_2 + 1 \leq w \leq r_3$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathcal{M}_w = \sum_{k_1=0}^{\ell t} \sum_{k_2=0}^{\ell t - k_1} \begin{bmatrix} \ell t \\ k_1 \end{bmatrix}_{q^{d_w}} \begin{bmatrix} \ell t - k_1 \\ k_2 \end{bmatrix}_{q^{d_w}}.$$

Proof. It follows immediately by applying Theorem 8.4.2 and Lemma 2.2.1. □

Proof of Theorem 8.6.1. Substituting the value of the number $\mathcal{M}_u$ for $1 \leq u \leq r_1$ from Lemmas 8.6.1-8.6.3, the number $\mathcal{M}_v$ for $r_1 + 1 \leq v \leq r_2$ from Lemma 8.6.4, and the number $\mathcal{M}_w$ for $r_2 + 1 \leq w \leq r_3$ from Lemma 8.6.5 in equation (8.13), we get the desired result. □

8.6.2 Enumeration formula for σ -self-dual additive H -QA codes

In the following theorem, we enumerate all σ -self-dual additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.6.2. *For $\sigma \in \{0, \gamma, *\}$, the number $\mathcal{N}$ of distinct σ -self-dual additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by*

$$\mathcal{N} = \prod_{u=1}^{r_1} \mathcal{N}_u \prod_{v=r_1+1}^{r_2} \mathcal{N}_v \prod_{w=r_2+1}^{r_3} \left(\sum_{k=0}^{\ell t} \begin{bmatrix} \ell t \\ k \end{bmatrix}_{q^{d_w}} \right),$$

where for $1 \leq u \leq r_1$, the number $\mathcal{N}_u$ is given by

$$\mathcal{N}_u = \begin{cases} \prod_{i=0}^{\frac{\ell t}{2}-1} (q^{\frac{\ell t-2i-2}{2}} + 1) & \text{if } \sigma \in \{0, *\} \text{ with either } \ell \text{ being even and } q \equiv 1 \pmod{4} \\ & \text{or } \ell \text{ being even, } \ell t \equiv 0 \pmod{4} \text{ and } q \equiv 3 \pmod{4} \text{ or } \ell \\ & \text{being odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}; \\ \prod_{i=0}^{\frac{\ell t}{2}-2} (q^{\frac{\ell t-2i-2}{2}} + 1) & \text{when } \sigma = 0 \text{ and both } q, \ell t \text{ are even;} \\ \prod_{i=0}^{\frac{\ell t}{2}-1} (q^{\frac{\ell t-2i}{2}} + 1) & \text{when either } \sigma = \gamma \text{ or } \sigma = * \text{ and } q \text{ is even;} \\ 0 & \text{otherwise} \end{cases}$$

and for $r_1 + 1 \leq v \leq r_2$, the number $\mathcal{N}_v$ is given by

$$\mathcal{N}_v = \begin{cases} \prod_{i=0}^{\frac{\ell t}{2}-1} (q^{\frac{d_v(\ell t-2i-1)}{2}} + 1) & \text{if } \ell t \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. To prove the result, we note that $\mathcal{N} = 0$ when ℓt is odd. So we assume, from now on, that ℓt is an even integer. Here, we see, by Theorem [8.5.2](#), that for $\sigma \in \{0, *\}$, there exists a σ -self-dual additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ if and only if either both ℓt and q are even or ℓ is even and $q \equiv 1 \pmod{4}$ or ℓ is even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ is odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$ and that there always exists a γ -self-dual additive H -QA code of

length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$. Further, by Theorem 8.5.1(b), we see that the number $\mathcal{N}$ of distinct σ -self-dual additive H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by

$$\mathcal{N} = \prod_{u=1}^{r_1} \mathcal{N}_u \prod_{v=r_1+1}^{r_2} \mathcal{N}_v \prod_{w=r_2+1}^{r_3} \mathcal{N}_w, \quad (8.18)$$

where $\mathcal{N}_u$ is equal to the number of distinct σ -self-dual $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ for $1 \leq u \leq r_1$, $\mathcal{N}_v$ is equal to the number of distinct σ -self-dual $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ for $r_1 + 1 \leq v \leq r_2$, and $\mathcal{N}_w$ is equal to the number of distinct $\mathcal{F}_{h_w}$ -subspaces of $\mathcal{G}_{h_w}^\ell$ for $r_2 + 1 \leq w \leq r_3$. When $1 \leq u \leq r_1$, working as in the proofs of Lemmas 8.6.1-8.6.3 and taking $k = \frac{\ell t}{2}$, we get the desired value of $\mathcal{N}_u$. On the other hand, when $r_1 + 1 \leq v \leq r_2$, we get the desired values of $\mathcal{N}_v$ on taking $k = \frac{\ell t}{2}$ in the proof of Lemma 8.6.4. For $r_2 + 1 \leq w \leq r_3$, we see, by applying Lemma 2.2.1, that

$$\mathcal{N}_w = \sum_{k=0}^{\ell t} \left[\begin{matrix} \ell t \\ k \end{matrix} \right]_{q^{d_w}}.$$

From this, the desired result follows. $\square$

8.6.3 Enumeration formula for σ -ACD H -QA codes

In the following theorem, we enumerate all σ -ACD H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ for $\sigma \in \{0, \gamma, *\}$.

Theorem 8.6.3. *For $\sigma \in \{0, \gamma, *\}$, the number $\mathcal{L}$ of distinct σ -ACD H -QA codes of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by*

$$\mathcal{L} = \prod_{u=1}^{r_1} \mathcal{L}_u \prod_{v=r_1+1}^{r_2} \mathcal{L}_v \prod_{w=r_2+1}^{r_3} \left(\sum_{k=0}^{\ell t} q^{kd_w(\ell t-k)} \left[\begin{matrix} \ell t \\ k \end{matrix} \right]_{q^{d_w}} \right),$$

where for $1 \leq u \leq r_1$, the number $\mathcal{L}_u$ equals

$$\bullet \ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \left[\begin{matrix} \ell t/2 \\ k/2 \end{matrix} \right]_{q^2} \text{ when either } \sigma = \gamma \text{ and } \ell t \text{ being even or } \sigma = * \text{ and both } \ell t, q \text{ are even;}$$

$$\bullet 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k+1)}{2}} \left[\begin{matrix} (\ell t-1)/2 \\ k/2 \end{matrix} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)(\ell t-k)}{2}} \left[\begin{matrix} (\ell t-1)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

when $\sigma \in \{0, *\}$ and both $q, \ell t$ are odd;

$$\bullet 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \left[\begin{matrix} \ell t/2 \\ k/2 \end{matrix} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-1)}{2}} (q^{\frac{\ell t}{2}} - 1) \left[\begin{matrix} (\ell t-2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

when $\sigma \in \{0, *\}$ with either ℓ being even and $q \equiv 1 \pmod{4}$ or ℓ being even, $\ell t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or ℓ being odd, $t \equiv 2 \pmod{4}$ and $q \equiv 3 \pmod{4}$;

$$\bullet 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \left[\begin{matrix} \ell t/2 \\ k/2 \end{matrix} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-1)}{2}} (q^{\frac{\ell t}{2}} + 1) \left[\begin{matrix} (\ell t-2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

when $\sigma \in \{0, *\}$ with either ℓ being odd, t even and $q \equiv 1 \pmod{4}$ or ℓ being odd, $t \equiv 0 \pmod{4}$ and $q \equiv 3 \pmod{4}$ or $\ell \equiv 2 \pmod{4}$, t being odd and $q \equiv 3 \pmod{4}$;

$$\bullet 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k+1)}{2}} \left[\begin{matrix} (\ell t-1)/2 \\ k/2 \end{matrix} \right]_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)(\ell t-k)}{2}} \left[\begin{matrix} (\ell t-1)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

when $\sigma = 0$, q is even and ℓt is odd;

$$\bullet 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-2)}{2}} \left((q^k + q - 1) \left[\begin{matrix} (\ell t-2)/2 \\ k/2 \end{matrix} \right]_{q^2} + (q^{\ell t-k+1} - q^{\ell t-k} + 1) \right. \\ \left. \times \left[\begin{matrix} (\ell t-2)/2 \\ (k-2)/2 \end{matrix} \right]_{q^2} \right) + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)\ell t-(k^2+1)}{2}} \left[\begin{matrix} (\ell t-2)/2 \\ (k-1)/2 \end{matrix} \right]_{q^2}$$

when $\sigma = 0$ and both $q, \ell t$ are even,

while for $r_1 + 1 \leq v \leq r_2$ and $\sigma \in \{0, \gamma, *\}$, we have

$$\mathcal{L}_v = 2 + \sum_{k=1}^{\ell t-1} q^{\frac{k(\ell t-k)d_v}{2}} \prod_{i=0}^{k-1} \left(\frac{q^{\frac{(\ell t-i)d_v}{2}} - (-1)^{\ell t-i}}{q^{\frac{(k-i)d_v}{2}} - (-1)^{k-i}} \right).$$

To prove the above theorem, we see, by Theorem 8.5.1(c), that it is enough to

determine the number $\mathcal{L}_u$ for $1 \leq u \leq r_1$, the number $\mathcal{L}_v$ for $r_1 + 1 \leq v \leq r_2$, and the number $\mathcal{L}_w$ for $r_2 + 1 \leq w \leq r_3$, where

- $\mathcal{L}_u$ equals the number of distinct σ -non-degenerate $\mathcal{F}_{h_u}$ -subspaces of $\mathcal{G}_{h_u}^\ell$ for $1 \leq u \leq r_1$,
- $\mathcal{L}_v$ equals the number of distinct σ -non-degenerate $\mathcal{F}_{h_v}$ -subspaces of $\mathcal{G}_{h_v}^\ell$ for $r_1 + 1 \leq v \leq r_2$, and
- $\mathcal{L}_w$ equals the number of distinct pairs $(\mathcal{C}_w, \mathcal{C}_{\mu(w)})$ with $\mathcal{C}_w$ as an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ as an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_w \cap \mathcal{C}_{\mu(w)}^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_{\mu(w)} \cap \mathcal{C}_w^{\perp\sigma} = \{\mathbf{0}\}$ for $r_2 + 1 \leq w \leq r_3$.

To determine the numbers $\mathcal{L}_u$'s and $\mathcal{L}_v$'s, let $\mathcal{L}_{u,k}$ (*resp.* $\mathcal{L}_{v,k}$) denote the number of distinct k -dimensional σ -non-degenerate $\mathcal{F}_{h_u}$ -subspaces (*resp.* $\mathcal{F}_{h_v}$ -subspaces) of $\mathcal{G}_{h_u}^\ell$ (*resp.* $\mathcal{G}_{h_v}^\ell$) for $0 \leq k \leq \ell t$ and $1 \leq u \leq r_1$ (*resp.* $r_1 + 1 \leq v \leq r_2$). Further, by Lemma 8.5.2, we note that the $\tau_{1,-1}$ -sesquilinear forms $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell}$ and $[\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ are reflexive and non-degenerate. So we have $\mathcal{L}_{u,0} = \mathcal{L}_{u,\ell t} = 1$ and $\mathcal{L}_{v,0} = \mathcal{L}_{v,\ell t} = 1$ for each u and v . This implies that

$$\mathcal{L}_u = \sum_{k=0}^{\ell t} \mathcal{L}_{u,k} = 2 + \sum_{k=1}^{\ell t-1} \mathcal{L}_{u,k} \quad \text{for } 1 \leq u \leq r_1 \text{ and} \quad (8.19)$$

$$\mathcal{L}_v = \sum_{k=0}^{\ell t} \mathcal{L}_{v,k} = 2 + \sum_{k=1}^{\ell t-1} \mathcal{L}_{v,k} \quad \text{for } r_1 + 1 \leq v \leq r_2. \quad (8.20)$$

In the following lemma, we determine the number $\mathcal{L}_u$ for $1 \leq u \leq r_1$ when either $\sigma = \gamma$ or $\sigma = *$ and q is even.

Lemma 8.6.6. *Let $1 \leq u \leq r_1$ be fixed. When either $\sigma = \gamma$ or $\sigma = *$ and q is even, we have*

$$\mathcal{L}_u = 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \begin{bmatrix} \ell t/2 \\ k/2 \end{bmatrix}_{q^2}.$$

Proof. To prove the result, we note, by (8.19), that it is enough to determine the number $\mathcal{L}_{u,k}$ for $1 \leq k \leq \ell t - 1$. For this, we see, by Lemma 8.5.2(a) and (b), that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma|_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is a symplectic space of dimension ℓt over $\mathcal{F}_{h_u} \simeq \mathbb{F}_q$ when $\sigma = \gamma$.

Moreover, when $\sigma = *$ and q is even, we observe that $[A_u(y), A_u(y)]_* = 0$ for all $A_u(y) \in \mathcal{G}_{h_u}^\ell$. This, by Lemma 8.5.2(a) and (b), implies that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is a symplectic space over $\mathcal{F}_{h_u}$. We further note that any k -dimensional σ -non-degenerate $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ is also a symplectic space, and hence by Theorem 2.2.3(a), its dimension k must be an even integer. This implies that $\mathcal{L}_{u,k} = 0$ when k is odd. Now working as in Proposition 5.4.1, we get the desired result. $\square$

In the following lemma, we determine the number $\mathcal{L}_u$ for $1 \leq u \leq r_1$ when $\sigma \in \{0, *\}$ and q is odd.

Lemma 8.6.7. *Let $1 \leq u \leq r_1$ be fixed. When $\sigma \in \{0, *\}$ and q is an odd prime power, we have*

$$\mathcal{L}_u = \begin{cases} 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k+1)}{2}} \begin{bmatrix} (\ell t-1)/2 \\ k/2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)(\ell t-k)}{2}} \begin{bmatrix} (\ell t-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if} \\ \ell t \text{ is odd;} \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \begin{bmatrix} \ell t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-1)}{2}} (q^{\frac{\ell t}{2}} + 1) \begin{bmatrix} (\ell t-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if} \\ \text{either } \ell \text{ is odd, } t \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ is odd, } t \equiv 0 \pmod{4} \\ \text{and } q \equiv 3 \pmod{4} \text{ or } \ell \equiv 2 \pmod{4}, t \text{ is odd and } q \equiv 3 \pmod{4}; \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k)}{2}} \begin{bmatrix} \ell t/2 \\ k/2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-1)}{2}} (q^{\frac{\ell t}{2}} - 1) \begin{bmatrix} (\ell t-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if} \\ \text{either } \ell \text{ is even and } q \equiv 1 \pmod{4} \text{ or } \ell \text{ is even, } \ell t \equiv 0 \pmod{4} \text{ and} \\ q \equiv 3 \pmod{4} \text{ or } \ell \text{ is odd, } t \equiv 2 \pmod{4} \text{ and } q \equiv 3 \pmod{4}. \end{cases}$$

Proof. To prove the result, we see, by Lemma 8.5.2(a) and (b), that $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ is an orthogonal space of dimension ℓt over $\mathcal{F}_{h_u} \simeq \mathbb{F}_q$. Since q is odd, we see that the orthogonal space $(\mathcal{G}_{h_u}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_u}^\ell \times \mathcal{G}_{h_u}^\ell})$ can be viewed as a non-degenerate quadratic space $(\mathcal{G}_{h_u}^\ell, \mathcal{Q}_u)$ over $\mathcal{F}_{h_u}$, where $\mathcal{Q}_u : \mathcal{G}_{h_u}^\ell \rightarrow \mathcal{F}_{h_u}$ is the quadratic map, defined as

$$\mathcal{Q}_u(A_u(y)) = \frac{1}{2}[A_u(y), A_u(y)]_\sigma \text{ for all } A_u(y) \in \mathcal{G}_{h_u}^\ell.$$

Further, the Witt index $\mathfrak{m}_u$ of the quadratic space $(\mathcal{G}_{h_u}^\ell, \mathcal{Q}_u)$ is given by (8.15). Now

working as in Proposition [5.4.2](#), the desired result follows. $\square$

In the following lemma, we determine the number $\mathcal{L}_u$ when $\sigma = 0$ and q is even.

Lemma 8.6.8. *Let $1 \leq u \leq r_1$ be fixed. When $\delta = 0$ and q is an even prime power, we have*

$$\mathcal{L}_u = \begin{cases} 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{k(\ell t-k+1)}{2}} \begin{bmatrix} (\ell t-1)/2 \\ k/2 \end{bmatrix}_{q^2} + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)(\ell t-k)}{2}} \begin{bmatrix} (\ell t-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} \\ \text{if } \ell t \text{ is odd;} \\ 2 + \sum_{\substack{k=1 \\ k \text{ is even}}}^{\ell t-1} q^{\frac{(k\ell t-k^2-2)}{2}} \left((q^k + q - 1) \begin{bmatrix} (\ell t-2)/2 \\ k/2 \end{bmatrix}_{q^2} + (q^{\ell t-k+1} - q^{\ell t-k} + 1) \right. \\ \left. \times \begin{bmatrix} (\ell t-2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2} \right) + \sum_{\substack{k=1 \\ k \text{ is odd}}}^{\ell t-1} q^{\frac{(k+1)\ell t-(k^2+1)}{2}} \begin{bmatrix} (\ell t-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} \\ \text{if } \ell t \text{ is even.} \end{cases}$$

Proof. By Lemma [8.4.3](#), we see that $d_u = 1$ and $\kappa_{h_u} = \gcd(t, d_u) = 1$. This implies that $e_{h_u,0} = e_{h_u}$, which gives $\mathcal{G}_{h_u} = \mathcal{F}_{h_u,0}$. Further, by Lemma [8.4.6](#), we note that each $A_u(y) \in \mathcal{G}_{h_u}^\ell$ is of the form $A_u(y) = (A_{u,1}(y), A_{u,2}(y), \dots, A_{u,\ell}(y)) \in \mathcal{G}_{h_u}^\ell$, where $A_{u,i}(y) = \theta_i e_{h_u} \in \mathcal{F}_{h_u,0}$ with $\theta_i \in \mathbb{F}_{q^t}$. Now let $\mathcal{W}_u$ be the $(\ell t - 1)$ -dimensional $\mathcal{F}_{h_u}$ -subspace of $\mathcal{G}_{h_u}^\ell$ as defined by [\(8.16\)](#), and let $\mathbf{1}_u = (\underbrace{e_{h_u}, e_{h_u}, \dots, e_{h_u}}_{\ell \text{ times}}) \in \mathcal{G}_{h_u}^\ell$. Here it is easy to observe that $\mathbf{1}_u \in \mathcal{W}_u$ if and only if ℓt is an even integer. Now working as in Proposition [5.4.3](#), the desired result follows. $\square$

In the following lemma, we determine the number $\mathcal{L}_v$ for $r_1 + 1 \leq v \leq r_2$ when $\sigma \in \{0, \gamma, *\}$.

Lemma 8.6.9. *Let $r_1 + 1 \leq v \leq r_2$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathcal{L}_v = 2 + \sum_{k=1}^{\ell t-1} q^{\frac{k(\ell t-k)d_v}{2}} \prod_{i=0}^{k-1} \left(\frac{q^{\frac{(\ell t-i)d_v}{2}} - (-1)^{\ell t-i}}{q^{\frac{(k-i)d_v}{2}} - (-1)^{k-i}} \right).$$

Proof. To prove the result, we note, by [\(8.20\)](#), that it is enough to determine the number $\mathcal{L}_{v,k}$ for $1 \leq k \leq \ell t - 1$. For this, we see, by Lemma [8.4.1](#)(d), that the

integer $d_v = |S_q(h_v)|$ must be even and $\mathcal{F}_{h_v} \simeq \mathbb{F}_{q^{d_v}}$. Now we shall distinguish the following two cases: (i) $\sigma \in \{0, *\}$ and (ii) $\sigma = \gamma$.

- (i) Let $\sigma \in \{0, *\}$. Here we note, by Lemma 8.5.2(a) and (c), that $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_\sigma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is an (ℓt) -dimensional unitary space over $\mathcal{F}_{h_v}$. We further observe that any k -dimensional σ -non-degenerate $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ is also a unitary space. Now working as in Case I of Proposition 5.4.4, the desired result follows.
- (ii) Let $\sigma = \gamma$. In this case, we note, by Lemma 8.5.2(a) and (c) again, that $[\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ is a reflexive, non-degenerate and skew-Hermitian $\tau_{1,-1}$ -sesquilinear form. Now working as in the proof of part (ii) of Lemma 8.6.4, the skew-Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\gamma \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$ can be transformed to an orthogonality preserving Hermitian $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell}$. Thus $(\mathcal{G}_{h_v}^\ell, [\cdot, \cdot]_{\gamma_H} \upharpoonright_{\mathcal{G}_{h_v}^\ell \times \mathcal{G}_{h_v}^\ell})$ is an (ℓt) -dimensional unitary space over $\mathcal{F}_{h_v}$. We further note that any $\mathcal{F}_{h_v}$ -subspace of $\mathcal{G}_{h_v}^\ell$ is non-degenerate with respect to $[\cdot, \cdot]_\gamma$ if and only if it is non-degenerate with respect to $[\cdot, \cdot]_{\gamma_H}$. Now working as in Case I of Proposition 5.4.4, the desired result follows.

□

We now proceed to determine the number $\mathcal{L}_w$ of distinct pairs $(\mathcal{C}_w, \mathcal{C}_{\mu(w)})$ with $\mathcal{C}_w$ as an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{C}_{\mu(w)}$ as an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$ satisfying $\mathcal{C}_w \cap \mathcal{C}_{\mu(w)}^{\perp_\sigma} = \{\mathbf{0}\}$ and $\mathcal{C}_{\mu(w)} \cap \mathcal{C}_w^{\perp_\sigma} = \{\mathbf{0}\}$ for $r_2 + 1 \leq w \leq r_3$, where $\sigma \in \{0, \gamma, *\}$. To do this, we represent elements of the direct sum $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ as $\mathbf{A}_w(y) = A_w(y) + A_{\mu(w)}(y)$, where $A_w(y) \in \mathcal{G}_{h_w}^\ell$ and $A_{\mu(w)}(y) \in \mathcal{G}_{h_{\mu(w)}}^\ell$. Analogously, we represent elements of the direct sum $\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}}$ as $\boldsymbol{\alpha}_w(y) = \alpha_w(y) + \alpha_{\mu(w)}(y)$, where $\alpha_w(y) \in \mathcal{F}_{h_w}$ and $\alpha_{\mu(w)}(y) \in \mathcal{F}_{h_{\mu(w)}}$. We further view the direct sum $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ as an $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -module with respect to the following operations:

$$\mathbf{A}_w(y) + \mathbf{B}_w(y) = (A_w(y) + B_w(y)) + (A_{\mu(w)}(y) + B_{\mu(w)}(y)) \quad (\text{addition}) \quad (8.21)$$

$$\boldsymbol{\alpha}_w(y) \odot \mathbf{A}_w(y) = \alpha_w(y)A_w(y) + \alpha_{\mu(w)}(y)A_{\mu(w)}(y) \quad (\text{scalar multiplication}) \quad (8.22)$$

for all $\mathbf{A}_w(y) = A_w(y) + A_{\mu(w)}(y)$, $\mathbf{B}_w(y) = B_w(y) + B_{\mu(w)}(y) \in \mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ and $\boldsymbol{\alpha}_w(y) = \alpha_w(y) + \alpha_{\mu(w)}(y) \in \mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}}$. Furthermore, for $\sigma \in \{0, \gamma, *\}$, we see

that

$$[\mathbf{A}_w(y), \mathbf{B}_w(y)]_\sigma = [A_w(y), B_{\mu(w)}(y)]_\sigma + [A_{\mu(w)}(y), B_w(y)]_\sigma \in \mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}}$$

for all $\mathbf{A}_w(y) = A_w(y) + A_{\mu(w)}(y)$, $\mathbf{B}_w(y) = B_w(y) + B_{\mu(w)}(y) \in \mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$. Next for $\sigma \in \{0, \gamma, *\}$, let $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ denote the restriction of the $\tau_{1,-1}$ -sesquilinear form $[\cdot, \cdot]_\sigma$ to $(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)$. We next observe the following:

Lemma 8.6.10. *Let $r_2 + 1 \leq w \leq r_3$ be fixed. For $\sigma \in \{0, \gamma, *\}$, the following hold.*

- (a) $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ is a free $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -module of rank ℓt .
- (b) The form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ is reflexive and non-degenerate.
- (c) The form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ is Hermitian when $\sigma \in \{0, *\}$, while the form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ is skew-Hermitian.

One can easily observe that any $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodule of $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ is of the form $\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}$, where $\mathcal{D}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{D}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$. On the other hand, if $\mathcal{D}_w$ is an $\mathcal{F}_{h_w}$ -subspace of $\mathcal{G}_{h_w}^\ell$ and $\mathcal{D}_{\mu(w)}$ is an $\mathcal{F}_{h_{\mu(w)}}$ -subspace of $\mathcal{G}_{h_{\mu(w)}}^\ell$, then $\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}$ is an $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodule of $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ with respect to the addition and scalar multiplication operations defined by (8.21) and (8.22). Further, the orthogonal complement of $\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}$ with respect to the form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ is defined as

$$(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)})^{\perp_\sigma} = \left\{ \mathbf{B}_w(y) \in \mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell : [\mathbf{A}_w(y), \mathbf{B}_w(y)]_\sigma = 0 \text{ for all } \mathbf{A}_w(y) \in \mathcal{D}_w \oplus \mathcal{D}_{\mu(w)} \right\}.$$

Note that $(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)})^{\perp_\sigma}$ is an $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodule of $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$. We next observe that $(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)})^{\perp_\sigma} = \mathcal{D}_w^{\perp_\sigma} \oplus \mathcal{D}_{\mu(w)}^{\perp_\sigma}$, where

$$\mathcal{D}_{\mu(w)}^{\perp_\sigma} = \left\{ B_w(y) \in \mathcal{G}_{h_w}^\ell : [A_{\mu(w)}(y), B_w(y)]_\sigma = 0 \text{ for all } A_{\mu(w)}(y) \in \mathcal{D}_{\mu(w)} \right\}$$

and

$$\mathcal{D}_w^{\perp\sigma} = \left\{ B_{\mu(w)}(y) \in \mathcal{G}_{h_{\mu(w)}}^\ell : [A_w(y), B_{\mu(w)}(y)]_\sigma = 0 \text{ for all } A_w(y) \in \mathcal{D}_w \right\}.$$

Further, for $\sigma \in \{0, \gamma, *\}$, we say that the $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodule $\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}$ is σ -non-degenerate if it satisfies $(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}) \cap (\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)})^{\perp\sigma} = \{\mathbf{0}\}$, i.e., if it satisfies $(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}) \cap (\mathcal{D}_w^{\perp\sigma} \oplus \mathcal{D}_{\mu(w)}^{\perp\sigma}) = \{\mathbf{0}\}$. From this, we observe that $(\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)}) \cap (\mathcal{D}_w \oplus \mathcal{D}_{\mu(w)})^{\perp\sigma} = \{\mathbf{0}\}$ if and only if $\mathcal{D}_w \cap \mathcal{D}_{\mu(w)}^{\perp\sigma} = \{\mathbf{0}\}$ and $\mathcal{D}_{\mu(w)} \cap \mathcal{D}_w^{\perp\sigma} = \{\mathbf{0}\}$. Thus the number $\mathcal{L}_w$ is equal to the number of distinct σ -non-degenerate $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodules of $\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ with respect to the form $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$, where $\sigma \in \{0, \gamma, *\}$.

Next, by Lemma 8.6.10(c), we see that $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ is a skew-Hermitian form, which can be transformed to an orthogonality preserving Hermitian form as follows: Let us take $\boldsymbol{\theta}_w(y) = \beta_w(y) - \tau_{1,-1}(\beta_w(y)) \in \mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}}$, where $\beta_w(y)$ is a non-zero element in $\mathcal{F}_{h_w}$. Note that $\boldsymbol{\theta}_w(y) \neq 0$ and $\tau_{1,-1}(\boldsymbol{\theta}_w(y)) = -\boldsymbol{\theta}_w(y)$. Now let us define a map $[\cdot, \cdot]_{\gamma_H} : (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \rightarrow \mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}}$ as

$$[\mathbf{A}_w(y), \mathbf{B}_w(y)]_{\gamma_H} = \boldsymbol{\theta}_w(y)[\mathbf{A}_w(y), \mathbf{B}_w(y)]_\gamma \text{ for all } \mathbf{A}_w(y), \mathbf{B}_w(y) \in \mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell.$$

It is easy to observe that the map $[\cdot, \cdot]_{\gamma_H}$ is a non-degenerate and Hermitian $\tau_{1,-1}$ -sesquilinear form. We further observe that an $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodule of $(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)$ is non-degenerate with respect to the form $[\cdot, \cdot]_\gamma$ if and only if it is non-degenerate with respect to the form $[\cdot, \cdot]_{\gamma_H}$. Therefore, it suffices to consider the non-degenerate and Hermitian form $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ instead of the non-degenerate and skew-Hermitian form $[\cdot, \cdot]_\gamma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$. In the following lemma, we determine the number $\mathcal{L}_w$ for $r_2 + 1 \leq w \leq r_3$ when $\sigma \in \{0, \gamma, *\}$.

Lemma 8.6.11. *Let $r_2 + 1 \leq w \leq r_3$ be fixed. For $\sigma \in \{0, \gamma, *\}$, we have*

$$\mathcal{L}_w = 2 + \sum_{k=1}^{\ell t - 1} q^{kd_w(\ell t - k)} \begin{bmatrix} \ell t \\ k \end{bmatrix}_{q^{d_w}}.$$

Proof. Here we see, by Theorem 8.5.1 and the above discussion, that the number $\mathcal{L}_w$ is equal to the number of distinct non-degenerate $(\mathcal{F}_{h_w} \oplus \mathcal{F}_{h_{\mu(w)}})$ -submodules of

$\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell$ with the respect to the Hermitian forms $[\cdot, \cdot]_\sigma \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ and $[\cdot, \cdot]_{\gamma_H} \upharpoonright_{(\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell) \times (\mathcal{G}_{h_w}^\ell \oplus \mathcal{G}_{h_{\mu(w)}}^\ell)}$ according as $\sigma \in \{0, *\}$ or $\sigma = \gamma$. Now working as in Proposition 3.5 of Sharma and Kaur [58], the desired result follows. $\square$

Proof of Theorem 8.6.3. Substituting the values of the number $\mathcal{L}_u$ for $1 \leq u \leq r_1$ from Lemmas 8.6.6-8.6.8, the number $\mathcal{L}_v$ for $r_1 + 1 \leq v \leq r_2$ from Lemma 8.6.9, and the number $\mathcal{L}_w$ for $r_2 + 1 \leq w \leq r_3$ from Lemma 8.6.11 in the equation (8.14), we get the desired result. $\square$

Now to explicitly determine the numbers $\mathcal{M}$, $\mathcal{N}$ and $\mathcal{L}$, one needs to compute the parameters r_1, r_2 and r_3 , which depend upon the structure of the finite Abelian group H . Jitman and Ling [38] determined these parameters when H is an elementary p -group (*i.e.*, when $H \simeq (\mathbb{Z}_p)^s$) and Palines *et al.* [50] determined these parameters when $H \simeq (\mathbb{Z}_{p^k})^s$, where p is a prime number and k, s are positive integers. In the next section, we determine these parameters when H is an arbitrary finite Abelian group.

8.7 Determination of the parameters r_1, r_2 and r_3 when H is an arbitrary finite Abelian group

Recall that H is a finite Abelian group of order $m > 1$. Let us write $m = p_1^{m_1} p_2^{m_2} \cdots p_z^{m_z}$, where $p_1, p_2, \dots, p_z$ are distinct primes and $m_1, m_2, \dots, m_z$ are positive integers. By the fundamental theorem of finite Abelian groups, we see that

$$H \simeq H_1 \oplus H_2 \oplus \cdots \oplus H_z, \quad (8.23)$$

where H_i is a p_i -group of order $p_i^{m_i}$ such that $H_i \simeq \mathbb{Z}_{p_i}^{m_{i,1}} \oplus \mathbb{Z}_{p_i}^{m_{i,2}} \oplus \cdots \oplus \mathbb{Z}_{p_i}^{m_{i,t_i}}$ with $m_i = m_{i,1} + m_{i,2} + \cdots + m_{i,t_i}$ and $m_{i,1} \geq m_{i,2} \geq \cdots \geq m_{i,t_i} \geq 1$ for $1 \leq i \leq z$. The following theorem provides the number of elements of a given order in a finite Abelian group.

Theorem 8.7.1. [8] *Let H be a finite Abelian group of order $m = p_1^{m_1} p_2^{m_2} \cdots p_z^{m_z}$ as defined by (8.23), where $p_1, p_2, \dots, p_z$ are distinct primes and $m_1, m_2, \dots, m_z$ are positive integers. Then the order of any element of H is of the form $\mathbf{n} = p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_s}^{k_s}$, where $1 \leq s \leq z$, $1 \leq i_1 < i_2 < \cdots < i_s \leq z$ and $1 \leq k_j \leq m_{i_j,1}$*

for $1 \leq j \leq s$. Furthermore, for $1 \leq j \leq s$, let us define $\mathbf{s}_j = \sum_{\ell_1=1}^{t_{i_j}} \min\{m_{i_j, \ell_1}, k_j\}$ and $\mathbf{t}_j = \sum_{\ell_1=1}^{t_{i_j}} \min\{m_{i_j, \ell_1}, k_j - 1\}$. The number $\mathcal{N}_H(\mathbf{n})$ of elements of order $\mathbf{n}$ in H is given by

$$\mathcal{N}_H(\mathbf{n}) = \prod_{j=1}^s p_{i_j}^{\mathbf{t}_j} (p_{i_j}^{\mathbf{s}_j - \mathbf{t}_j} - 1),$$

where the difference $\mathbf{s}_j - \mathbf{t}_j$ equals the number of integers ℓ_1 satisfying $1 \leq \ell_1 \leq t_{i_j}$ and $m_{i_j, \ell_1} \geq k_j$ for each j .

Proof. It follows from Theorem 1 of Benson [8]. □

From now on, let $\text{ord}_\beta(q)$ denote the multiplicative order of q modulo β , where β is a positive integer coprime to q . If p is an odd prime coprime to q such that $f = \text{ord}_p(q)$, then we can write $q^f = 1 + p^d c$, where c, d are integers satisfying $d \geq 1$ and $p \nmid c$. Further, one can easily observe, for any integer $\alpha \geq 1$, that

$$\text{ord}_{p^\alpha}(q) = \begin{cases} f & \text{if } \alpha \leq d; \\ fp^{\alpha-d} & \text{if } \alpha \geq d+1. \end{cases} \quad (8.24)$$

Similarly, if q is an odd prime power, then we can write $q = \pm 1 + 2^d c$, where $d \geq 2$ and c is odd. In this case, one can easily observe, for all $\alpha \geq 1$, that

$$\text{ord}_{2^\alpha}(q) = \begin{cases} 1 & \text{if } \alpha \leq d \text{ and } q = 1 + 2^d c; \\ 2 & \text{if } \alpha \leq d \text{ and } q = -1 + 2^d c; \\ 2^{\alpha-d} & \text{if } \alpha \geq d+1. \end{cases} \quad (8.25)$$

For $1 \leq s \leq z$, let us define

$$\mathcal{I}_s = \{(i_1, i_2, \dots, i_s) \in \mathbb{N}^s : 1 \leq i_1 < i_2 < \dots < i_s \leq z\}$$

and for $1 \leq s \leq z-1$, let us define

$$\mathcal{J}_s = \{(i_1, i_2, \dots, i_s) \in \mathbb{N}^s : 2 \leq i_1 < i_2 < \dots < i_s \leq z\}.$$

Note that $\mathcal{J}_s \subset \mathcal{I}_s$. For $\mathbf{i} = (i_1, i_2, \dots, i_s) \in \mathcal{I}_s$, let us define

$$\mathbf{z}_{\mathbf{i}} = p_{i_1}^{m_{i_1,1}} p_{i_2}^{m_{i_2,1}} \cdots p_{i_s}^{m_{i_s,1}} \text{ and } \mathbf{z}_{\mathbf{i}}^* = p_{i_1} p_{i_2} \cdots p_{i_s}.$$

For $\mathbf{i} \in \mathcal{I}_s$, let $\alpha_{\mathbf{i}}$ be a positive integer satisfying $\alpha_{\mathbf{i}} | \mathbf{z}_{\mathbf{i}}$ and $\mathbf{z}_{\mathbf{i}}^* | \alpha_{\mathbf{i}}$. One can easily see that $\alpha_{\mathbf{i}} = p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_s}^{k_s}$, where $1 \leq k_j \leq m_{i_j,1}$ for $1 \leq j \leq s$. Let $h \in H$ be a non-zero element with $\text{ord}(h) = \alpha_{\mathbf{i}}$. Here we observe that

$$|S_q(h)| = d_h = \text{ord}_{\alpha_{\mathbf{i}}}(q) = \text{lcm}[\text{ord}_{p_{i_1}^{k_1}}(q), \text{ord}_{p_{i_2}^{k_2}}(q), \dots, \text{ord}_{p_{i_s}^{k_s}}(q)], \quad (8.26)$$

where $\text{ord}_{p_{i_j}^{k_j}}(q)$'s can be determined using equations (8.24) and (8.25). Thus, using equations (8.24)-(8.26), one can determine the size d_h of the q -cyclotomic class $S_q(h)$ of H for each $h \in H$. In the following theorem, we explicitly determine the parameters r_1, r_2 and r_3 when H is a finite Abelian group of odd order.

Theorem 8.7.2. *Let H be a finite Abelian group of odd order $m = p_1^{m_1} p_2^{m_2} \cdots p_z^{m_z}$, where $p_1, p_2, \dots, p_z$ are distinct odd primes and $m_1, m_2, \dots, m_z$ are positive integers. We have*

$$\begin{aligned} r_1 &= 1, \\ r_2 &= \sum_{s=1}^z \sum_{\mathbf{i} \in \mathcal{I}_s} \lambda^{\dagger}(\mathbf{i}) \sum_{\substack{\alpha_{\mathbf{i}} | \mathbf{z}_{\mathbf{i}} \\ \mathbf{z}_{\mathbf{i}}^* | \alpha_{\mathbf{i}}}} \frac{\mathcal{N}_H(\alpha_{\mathbf{i}})}{\text{ord}_{\alpha_{\mathbf{i}}}(q)} \quad \text{and} \\ r_3 &= \sum_{s=1}^z \sum_{\mathbf{i} \in \mathcal{I}_s} (1 - \lambda^{\dagger}(\mathbf{i})) \sum_{\substack{\alpha_{\mathbf{i}} | \mathbf{z}_{\mathbf{i}} \\ \mathbf{z}_{\mathbf{i}}^* | \alpha_{\mathbf{i}}}} \frac{\mathcal{N}_H(\alpha_{\mathbf{i}})}{2 \text{ord}_{\alpha_{\mathbf{i}}}(q)}, \end{aligned}$$

where for $1 \leq s \leq z$ and $\mathbf{i} = (i_1, i_2, \dots, i_s) \in \mathcal{I}_s$, the number $\lambda^{\dagger}(\mathbf{i})$ is defined as

$$\lambda^{\dagger}(\mathbf{i}) = \begin{cases} 1 & \text{if } \nu_2(\text{ord}_{p_{i_1}}(q)) = \nu_2(\text{ord}_{p_{i_2}}(q)) = \cdots = \nu_2(\text{ord}_{p_{i_s}}(q)) \geq 1; \\ 0 & \text{otherwise,} \end{cases} \quad (8.27)$$

(here the numbers $\mathcal{N}_H(\alpha_{\mathbf{i}})$'s are as determined in Theorem 8.7.1 and the numbers $\text{ord}_{\alpha_{\mathbf{i}}}(q)$'s can be determined using equations (8.24)-(8.26)).

Proof. To prove the result, we see, by Lemma 8.4.1(a) and (b), that for $h \in H$, the

q -cyclotomic class $S_q(h)$ of H is of Type I if and only if $h = 0$. From this, it follows that $r_1 = 1$.

Next, to determine the parameters r_2 and r_3 , let $h = (h_1, h_2, \dots, h_z) (\neq 0)$ be an arbitrary element of H . By Theorem 8.7.1, we see that the order of the element h is of the form $p_{i_1}^{k_1} p_{i_2}^{k_2} \cdots p_{i_s}^{k_s}$, where $1 \leq s \leq z$, $1 \leq i_1 < i_2 < \cdots < i_s \leq z$ and $k_1, k_2, \dots, k_s$ are positive integers satisfying $1 \leq k_j \leq m_{i_j,1}$ for $1 \leq j \leq s$. This implies that $\text{ord}(h_{i_j}) = p_{i_j}^{k_j}$ for $1 \leq j \leq s$ and $h_\ell = 0$ for all $\ell \in \{1, 2, \dots, z\} \setminus \{i_1, i_2, \dots, i_s\}$. Let us assume that $\text{ord}_{p_{i_j}}(q) = b_j$ for $1 \leq j \leq s$. We next assert that $S_q(h)$ is of Type II if and only if $\nu_2(b_1) = \nu_2(b_2) = \cdots = \nu_2(b_s) \geq 1$.

To prove this assertion, let us first assume that $S_q(h)$ is of Type II. We will show that $\nu_2(b_1) = \nu_2(b_2) = \cdots = \nu_2(b_s) \geq 1$. For this, we see, by Lemma 8.4.1(c), that there exists a least positive integer w such that $q^w \equiv -1 \pmod{\text{ord}(h)}$, which implies that $q^w \equiv -1 \pmod{p_{i_j}}$ for $1 \leq j \leq s$. This implies that b_j divides $2w$ for $1 \leq j \leq s$. Since $q^w \equiv -1 \pmod{p_{i_j}}$, one can easily observe that $\nu_2(2w) = 1 + \nu_2(w) = \nu_2(b_j)$ for $1 \leq j \leq s$. This implies that $\nu_2(b_1) = \nu_2(b_2) = \cdots = \nu_2(b_s) \geq 1$.

Conversely, let us assume that $\nu_2(b_1) = \nu_2(b_2) = \cdots = \nu_2(b_s) = \theta \geq 1$. We will show that $S_q(h)$ is of Type II. To prove this, we see, by Lemma 8.4.1(c), that it suffices to show that there exists a positive integer w' such that $q^{w'} \equiv -1 \pmod{\text{ord}(h)}$. Since $q^{b_j} \equiv 1 \pmod{p_{i_j}}$, we can write $q^{b_j} = 1 + p_{i_j}^{\beta_j} c_j$, where p_{i_j} does not divide c_j for $1 \leq j \leq s$. From this, one can easily see that

$$\text{ord}_{p_{i_j}}^{k_j}(q) = \begin{cases} b_j & \text{if } k_j \leq \beta_j; \\ b_j p_{i_j}^{k_j - \beta_j} & \text{if } k_j > \beta_j. \end{cases} \quad (8.28)$$

So we can write $\text{ord}_{p_{i_j}}^{k_j}(q) = 2^\theta w_j$, where w_j is odd for $1 \leq j \leq s$. Note that $\nu_2(b_j) = \nu_2(\text{ord}_{p_{i_j}}^{k_j}(q)) = \nu_2(2^\theta w_j) = \theta$ for each j . This implies that $q^{2^{\theta-1} w_j} \equiv -1 \pmod{p_{i_j}^{k_j}}$ for $1 \leq j \leq s$. Let us take $w' = 2^{\theta-1} w_1 w_2 \cdots w_s$. Now, by applying the Chinese Remainder Theorem [63, Th. 2.2.2], it is easy to see that $q^{w'} \equiv -1 \pmod{\text{ord}(h)}$, which, by Lemma 8.4.1(c), implies that $S_q(h)$ is of Type II and $|S_q(h)| = 2^\theta w_1 w_2 \cdots w_s$. This proves the assertion.

From this, the desired result follows immediately. $\square$

We now illustrate the above theorem in the following example.

Example 8.7.1. Let $q = 2$, and let $H = \mathbb{Z}_{3^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ be an Abelian group of order 405. Here we have $z = 2$, $p_1 = 3$, $p_2 = 5$, $m_{1,1} = 3$ and $m_{2,1} = 1$. By Theorem 8.7.2, we see that $r_1 = 1$. Now to determine the parameters r_2 and r_3 , we note that $\mathcal{I}_1 = \{1, 2\}$, $\mathcal{I}_2 = \{(1, 2)\}$, $\mathbf{z}_1 = 3^3$, $\mathbf{z}_1^* = 3$, $\mathbf{z}_2 = \mathbf{z}_2^* = 5$, $\mathbf{z}_{(1,2)} = 135$ and $\mathbf{z}_{(1,2)}^* = 15$. Since $\text{ord}_3(2) = 2$ and $\text{ord}_5(2) = 4$, by (8.27), we have $\lambda^\dagger(1) = \lambda^\dagger(2) = 1$ and $\lambda^\dagger(1, 2) = 0$. As $\text{ord}_3(2) = 2$, we see, by (8.28), that $\text{ord}_9(2) = 6$ and $\text{ord}_{27}(2) = 18$. From this and using the fact that $\text{ord}_5(2) = 4$, one can easily see that $\text{ord}_{15}(2) = \text{lcm}[\text{ord}_3(2), \text{ord}_5(2)] = 4$, $\text{ord}_{45}(2) = \text{lcm}[\text{ord}_9(2), \text{ord}_5(2)] = 12$ and $\text{ord}_{135}(2) = \text{lcm}[\text{ord}_{27}(2), \text{ord}_5(2)] = 36$. Further, by applying Theorem 8.7.1, we get $\mathcal{N}_H(3) = 8$, $\mathcal{N}_H(9) = 18$, $\mathcal{N}_H(27) = 54$, $\mathcal{N}_H(5) = 4$, $\mathcal{N}_H(15) = 32$, $\mathcal{N}_H(45) = 72$ and $\mathcal{N}_H(135) = 216$. From this and by applying Theorem 8.7.2 again, we get

$$r_2 = \frac{\mathcal{N}_H(3)}{\text{ord}_3(2)} + \frac{\mathcal{N}_H(9)}{\text{ord}_9(2)} + \frac{\mathcal{N}_H(27)}{\text{ord}_{27}(2)} + \frac{\mathcal{N}_H(5)}{\text{ord}_5(2)} = \frac{8}{2} + \frac{18}{6} + \frac{54}{18} + \frac{4}{4} = 11$$

and

$$r_3 = \frac{\mathcal{N}_H(15)}{2 \text{ord}_{15}(2)} + \frac{\mathcal{N}_H(45)}{2 \text{ord}_{45}(2)} + \frac{\mathcal{N}_H(135)}{2 \text{ord}_{135}(2)} = \frac{32}{8} + \frac{72}{24} + \frac{216}{72} = 10.$$

In the following theorem, we explicitly determine the parameters r_1, r_2 and r_3 when H is a finite Abelian group of even order.

Theorem 8.7.3. Let H be a finite Abelian group of order $m = p_1^{m_1} p_2^{m_2} \cdots p_z^{m_z}$ as defined by (8.23), where $p_1 = 2$, $p_2, p_3, \dots, p_z$ are distinct odd primes and $m_1, m_2, \dots, m_z$ are positive integers. Let us define $\omega = \min\{\nu_2(q+1), m_{1,1}\}$. Here q must be odd, and we have

$$\begin{aligned} r_1 &= 2^{t_1}, \\ r_2 &= \sum_{j=2}^{\omega} \frac{\mathcal{N}_H(2^j)}{\text{ord}_{2^j}(q)} + \sum_{s=2}^z \sum_{\mathbf{i} \in \mathcal{J}_{s-1}} \sum_{k_1=0}^{\omega} \lambda_{k_1}(\mathbf{i}) \sum_{\substack{\alpha_i | \mathbf{z}_i \\ \mathbf{z}_i^* | \alpha_i}} \frac{\mathcal{N}_H(2^{k_1} \alpha_i)}{\text{ord}_{2^{k_1} \alpha_i}(q)} \quad \text{and} \\ r_3 &= \sum_{j=\omega+1}^{m_{1,1}} \frac{\mathcal{N}_H(2^j)}{2 \text{ord}_{2^j}(q)} + \sum_{s=2}^z \sum_{\mathbf{i} \in \mathcal{J}_{s-1}} \sum_{k_1=0}^{m_{1,1}} (1 - \lambda_{k_1}(\mathbf{i})) \sum_{\substack{\alpha_i | \mathbf{z}_i \\ \mathbf{z}_i^* | \alpha_i}} \frac{\mathcal{N}_H(2^{k_1} \alpha_i)}{2 \text{ord}_{2^{k_1} \alpha_i}(q)}, \end{aligned}$$

where for $0 \leq k_1 \leq m_{1,1}$, $2 \leq s \leq z$ and $\mathbf{i} = (i_2, i_3, \dots, i_s) \in \mathcal{J}_{s-1}$, the number $\lambda_{k_1}(\mathbf{i})$

is defined as

$$\lambda_{k_1}(\mathbf{i}) = \begin{cases} 1 & \text{if either } k_1 \in \{0, 1\} \text{ and } \nu_2(\text{ord}_{p_{i_2}}(q)) = \cdots = \nu_2(\text{ord}_{p_{i_s}}(q)) \geq 1 \text{ or} \\ & k_1 \geq 2, q \equiv -1 \pmod{2^{k_1}} \text{ and } \nu_2(\text{ord}_{p_{i_2}}(q)) = \cdots = \nu_2(\text{ord}_{p_{i_s}}(q)) = 1; \\ 0 & \text{otherwise,} \end{cases} \quad (8.29)$$

(here the numbers $\mathcal{N}_H(2^{k_1}\alpha_i)$'s are as determined in Theorem 8.7.1 and the numbers $\text{ord}_{2^{k_1}\alpha_i}(q)$'s can be determined using equations (8.24)-(8.26)).

Proof. To prove the result, let h be an arbitrary element of H . By Lemma 8.4.1(a) and (b), we see that $S_q(h)$ is of Type I if and only if $\text{ord}(h) = 1$ or 2 . Further, by Theorem 8.7.1, we see that there is exactly one element of order 1 and $2^{t_1} - 1$ elements of order 2 in H . As each q -cyclotomic class of H of Type I is a singleton set, we obtain $r_1 = 2^{t_1}$.

Next, to determine the parameters r_2 and r_3 , we distinguish the following two cases: **I.** $\text{ord}(h) = 2^{k_1}$, where $2 \leq k_1 \leq m_{1,1}$, and **II.** $\text{ord}(h) = 2^{k_1}p_{i_2}^{k_2}p_{i_3}^{k_3} \cdots p_{i_s}^{k_s}$, where $2 \leq i_2 < i_3 < \cdots < i_s \leq z$ and $k_1, k_2, \dots, k_s$ are integers satisfying $0 \leq k_1 \leq m_{1,1}$ and $1 \leq k_j \leq m_{i_j,1}$ for $2 \leq j \leq s$.

I. Let $\text{ord}(h) = 2^{k_1}$, where $2 \leq k_1 \leq m_{1,1}$. Here we assert that $S_q(h)$ is of Type II if and only if $q \equiv -1 \pmod{2^{k_1}}$. To prove this assertion, we first assume that $S_q(h)$ is of Type II. We will show that $q \equiv -1 \pmod{2^{k_1}}$. For this, we see, by Lemma 8.4.1(c), that there exists a least positive integer w such that $q^w \equiv -1 \pmod{2^{k_1}}$. Since $k_1 \geq 2$, it is easy to observe that w is odd. Further, since $\gcd(q, 2) = 1$, we see that q belongs to the unit group $U(2^{k_1})$ of $\mathbb{Z}_{2^{k_1}}$. We know that $U(2^{k_1}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{k_1-2}} \simeq \langle -1 \rangle \times \langle 5 \rangle$. So we can write $q \equiv (-1)^a 5^b \pmod{2^{k_1}}$ for some positive integers a and b . Since $q^w \equiv -1 \pmod{2^{k_1}}$, we get $(-1)^{aw} 5^{bw} \equiv -1 \pmod{2^{k_1}}$. From this and using the fact that $k_1 \geq 2$, it follows that the integer a must be odd and $5^{bw} \equiv 1 \pmod{2^{k_1}}$. This implies that $bw \equiv 0 \pmod{2^{k_1-2}}$. As w is odd, we must have $b \equiv 0 \pmod{2^{k_1-2}}$, which implies that $5^b \equiv 1 \pmod{2^{k_1}}$. From this, it follows that $q \equiv -1 \pmod{2^{k_1}}$.

Conversely, let us assume that $q \equiv -1 \pmod{2^{k_1}}$. Here we see that $h \neq -h$ and $hq = -h$ in H , which implies that $S_q(h)$ is of Type II.

II. Next, let $\text{ord}(h) = 2^{k_1} p_{i_2}^{k_2} p_{i_3}^{k_3} \cdots p_{i_s}^{k_s}$, where $2 \leq i_2 < i_3 < \cdots < i_s \leq z$ and $k_1, k_2, \dots, k_s$ are integers satisfying $0 \leq k_1 \leq m_{1,1}$ and $1 \leq k_j \leq m_{i_j,1}$ for $2 \leq j \leq s$. Further, let us assume that $\text{ord}_{p_{i_j}}(q) = b_j$ for $2 \leq j \leq s$. Here, we distinguish the following two cases: (i) $\text{ord}(h)$ is odd and (ii) $\text{ord}(h)$ is even.

(i) Let $\text{ord}(h)$ be odd, *i.e.*, $k_1 = 0$. Here working as in Theorem 8.7.2 and by applying Lemma 8.4.1(c), we observe that $S_q(h)$ is of Type II if and only if $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) \geq 1$.

(ii) Let $\text{ord}(h)$ be even, *i.e.*, $k_1 \geq 1$.

If $k_1 = 1$, *i.e.*, $\text{ord}(h) = 2p_{i_2}^{k_2} p_{i_3}^{k_3} \cdots p_{i_s}^{k_s}$, working as in Theorem 8.7.2 again, we see that $S_q(h)$ is of Type II if and only if $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) \geq 1$.

From now on, let us assume, throughout the proof, that $k_1 \geq 2$. Here we assert that $S_q(h)$ is of Type II if and only if $q \equiv -1 \pmod{2^{k_1}}$ and $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) = 1$.

To prove this assertion, let us first assume that $S_q(h)$ is of Type II. We will show that $q \equiv -1 \pmod{2^{k_1}}$ and $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) = 1$. For this, we see, by Lemma 8.4.1(c), that there exists a least positive integer w such that $q^w \equiv -1 \pmod{\text{ord}(h)}$, which implies that $q^w \equiv -1 \pmod{p_{i_j}}$ for $1 \leq j \leq s$. This further implies that b_j divides $2w$ for $2 \leq j \leq s$. From this, we see that $\nu_2(2w) = 1 + \nu_2(w) = \nu_2(b_j)$ for $2 \leq j \leq s$. Since $q^w \equiv -1 \pmod{2^{k_1}}$ and $k_1 \geq 2$, we note that w is odd. This implies that $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) = 1$. Further, working as in case I, we see that $q \equiv -1 \pmod{2^{k_1}}$.

Conversely, let us assume that $q \equiv -1 \pmod{2^{k_1}}$ and $\nu_2(b_2) = \nu_2(b_3) = \cdots = \nu_2(b_s) = 1$. Here we will show that $S_q(h)$ is of Type II. For this, we note, by Lemma 8.4.1(c), that it is enough to show that there exists a positive integer w' such that $q^{w'} \equiv -1 \pmod{\text{ord}(h)}$. Here working as in Theorem 8.7.2 again, it is easy to see that $\nu_2(\text{ord}_{p_{i_j}}^{k_j}(q)) = \nu_2(b_j) = 1$ for $2 \leq j \leq s$. So we can write $\text{ord}_{p_{i_j}}^{k_j}(q) = 2w_j$, where w_j is odd for $2 \leq j \leq s$. We next observe that $q^{w_j} \equiv -1 \pmod{p_{i_j}^{k_j}}$ for $2 \leq j \leq s$. Let us take $w' = w_2 w_3 \cdots w_s$. Now by applying the Chinese Remainder

Theorem [63, Th. 2.2.2], one can easily see that $q^{w'} \equiv -1 \pmod{\text{ord}(h)}$, which implies that $S_q(h)$ is of type II and $|S_q(h)| = 2w_2w_3 \cdots w_s$.

From this, the desired result follows immediately. $\square$

Now the following example illustrates the above theorem.

Example 8.7.2. Let $q = 7$, and let $H = \mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^2} \oplus \mathbb{Z}_5$ be an Abelian group of order 720. Here we have $z = 3$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $m_{1,1} = 3$, $m_{2,1} = 2$, $m_{3,1} = 1$, $t_1 = 2$, and $\omega = \min\{\nu_2(q+1), m_{1,1}\} = 3$. By Theorem 8.7.2, we see that $r_1 = 2^{t_1} = 4$. Now to determine the parameters r_2 and r_3 , we note that $\mathcal{J}_1 = \{2, 3\}$, $\mathcal{J}_2 = \{(2, 3)\}$, $\mathbf{z}_2 = 9$, $\mathbf{z}_2^* = 3$, $\mathbf{z}_3 = \mathbf{z}_3^* = 5$, $\mathbf{z}_{(2,3)} = 45$ and $\mathbf{z}_{(2,3)}^* = 15$. Since $\text{ord}_3(7) = 1$ and $\text{ord}_5(7) = 4$, by (8.29), we have $\lambda_{k_1}(2) = 0$ for $0 \leq k_1 \leq 3$, $\lambda_0(3) = \lambda_1(3) = 1$, $\lambda_2(3) = 0$ and $\lambda_{k_1}(2, 3) = 0$ for $0 \leq k_1 \leq 3$. Further, as $\text{ord}_2(7) = \text{ord}_3(7) = 1$, we see, by (8.28), that $\text{ord}_4(7) = \text{ord}_8(7) = 2$, and $\text{ord}_9(7) = 3$. We also note that $\text{ord}_6(7) = 1$. From this and using the fact that $\text{ord}_5(7) = 4$, one can easily see that

$$\begin{aligned} \text{ord}_{10}(7) &= 4, & \text{ord}_{12}(7) &= 2, & \text{ord}_{15}(7) &= 4, & \text{ord}_{18}(7) &= 3, \\ \text{ord}_{20}(7) &= 4, & \text{ord}_{24}(7) &= 2, & \text{ord}_{30}(7) &= 4, & \text{ord}_{36}(7) &= 6, \\ \text{ord}_{40}(7) &= 4, & \text{ord}_{45}(7) &= 12, & \text{ord}_{60}(7) &= 4, & \text{ord}_{72}(7) &= 6, \\ \text{ord}_{90}(7) &= 12, & \text{ord}_{120}(7) &= 4, & \text{ord}_{180}(7) &= 12, & \text{ord}_{360}(7) &= 12. \end{aligned}$$

Further, by applying Theorem 8.7.1, we get

$$\begin{aligned} \mathcal{N}_H(2) &= 3, & \mathcal{N}_H(3) &= 2, & \mathcal{N}_H(4) &= 4, & \mathcal{N}_H(5) &= 4, & \mathcal{N}_H(6) &= 6, \\ \mathcal{N}_H(8) &= 8, & \mathcal{N}_H(9) &= 6, & \mathcal{N}_H(10) &= 12, & \mathcal{N}_H(12) &= 8, & \mathcal{N}_H(15) &= 8, \\ \mathcal{N}_H(18) &= 18, & \mathcal{N}_H(20) &= 16, & \mathcal{N}_H(24) &= 16, & \mathcal{N}_H(30) &= 24, & \mathcal{N}_H(36) &= 24, \\ \mathcal{N}_H(40) &= 32, & \mathcal{N}_H(45) &= 24, & \mathcal{N}_H(60) &= 32, & \mathcal{N}_H(72) &= 48, & \mathcal{N}_H(90) &= 72, \\ \mathcal{N}_H(120) &= 64, & \mathcal{N}_H(180) &= 96 & \text{ and } & \mathcal{N}_H(360) &= 192. \end{aligned}$$

From this and by applying Theorem 8.7.2 again, we get

$$r_2 = \frac{\mathcal{N}_H(4)}{\text{ord}_4(7)} + \frac{\mathcal{N}_H(8)}{\text{ord}_8(7)} + \frac{\mathcal{N}_H(5)}{\text{ord}_5(7)} + \frac{\mathcal{N}_H(10)}{\text{ord}_{10}(7)} = \frac{4}{2} + \frac{8}{2} + \frac{4}{4} + \frac{12}{4} = 10$$

and

$$r_3 = \frac{\mathcal{N}_H(3)}{2 \text{ord}_3(7)} + \frac{\mathcal{N}_H(6)}{2 \text{ord}_6(7)} + \frac{\mathcal{N}_H(12)}{2 \text{ord}_{12}(7)} + \frac{\mathcal{N}_H(24)}{2 \text{ord}_{24}(7)} + \frac{\mathcal{N}_H(9)}{2 \text{ord}_9(7)} + \frac{\mathcal{N}_H(18)}{2 \text{ord}_{18}(7)}$$

$$\begin{aligned}
& + \frac{\mathcal{N}_H(36)}{2 \operatorname{ord}_{36}(7)} + \frac{\mathcal{N}_H(72)}{2 \operatorname{ord}_{72}(7)} + \frac{\mathcal{N}_H(20)}{2 \operatorname{ord}_{20}(7)} + \frac{\mathcal{N}_H(40)}{2 \operatorname{ord}_{40}(7)} + \frac{\mathcal{N}_H(15)}{2 \operatorname{ord}_{15}(7)} + \frac{\mathcal{N}_H(30)}{2 \operatorname{ord}_{30}(7)} \\
& + \frac{\mathcal{N}_H(60)}{2 \operatorname{ord}_{60}(7)} + \frac{\mathcal{N}_H(120)}{2 \operatorname{ord}_{40}(7)} + \frac{\mathcal{N}_H(45)}{2 \operatorname{ord}_{45}(7)} + \frac{\mathcal{N}_H(90)}{2 \operatorname{ord}_{90}(7)} + \frac{\mathcal{N}_H(180)}{2 \operatorname{ord}_{180}(7)} + \frac{\mathcal{N}_H(360)}{2 \operatorname{ord}_{360}(7)} \\
& = \frac{2}{2} + \frac{6}{2} + \frac{8}{4} + \frac{16}{4} + \frac{6}{6} + \frac{18}{6} + \frac{24}{12} + \frac{48}{12} + \frac{16}{8} + \frac{32}{8} + \frac{8}{8} + \frac{24}{8} + \frac{32}{8} + \frac{64}{8} + \frac{24}{24} \\
& + \frac{72}{24} + \frac{96}{24} + \frac{192}{24} = 58.
\end{aligned}$$

8.8 MDS and almost MDS additive H -QA codes

Recall that $\mathcal{S} = \mathbb{F}_q[H]$ and $\mathcal{R} = \mathbb{F}_{q^t}[H]$, and that an additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$, and hence is an $\mathbb{F}_q$ -linear subspace of $\mathcal{R}^\ell$. We also recall, from Chapter 2, that the dimension k of an additive H -QA code $\mathcal{C}$ of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ is given by $k = \dim_{\mathbb{F}_{q^t}} \mathcal{C} = \log_{q^t} |\mathcal{C}|$, which need not be an integer in general. We will refer to an additive H -QA code of length $m\ell$, dimension k and Hamming distance d over $\mathbb{F}_{q^t}$ as an additive $[m\ell, k, d]$ H -QA code over $\mathbb{F}_{q^t}$. The additive $[m\ell, k, d]$ H -QA code $\mathcal{C}$ over $\mathbb{F}_{q^t}$ is said to be *maximum distance separable* (MDS) if its parameters satisfy $d = m\ell - \lceil k \rceil + 1$, whereas the code $\mathcal{C}$ is said to be *almost MDS* if its parameters satisfy $d = m\ell - \lceil k \rceil$.

For each $a(y) = (a_1(y), a_2(y), \dots, a_\ell(y)) \in \mathcal{R}^\ell$, let us define

$$\mathcal{C}_a = \{v(y)a(y) = (v(y)a_1(y), v(y)a_2(y), \dots, v(y)a_\ell(y)) \mid v(y) \in \mathcal{S}\}.$$

Note that $\mathcal{C}_a$ is an $\mathcal{S}$ -submodule of $\mathcal{R}^\ell$ generated by $a(y)$, and hence is a 1-generator additive H -QA code of length $m\ell$ and index ℓ over $\mathbb{F}_{q^t}$ generated by $a(y)$. Now in Table 8.1, we list some MDS and almost MDS additive codes belonging to the class of 1-generator additive H -QA codes $\mathcal{C}_a$'s over $\mathbb{F}_{q^t}$ by carrying out computations in Magma. Here ξ denotes a primitive element of $\mathbb{F}_{q^t}$, $[m\ell, k, d]$ are the parameters of the code $\mathcal{C}_a$ generated by the element $a(y) \in \mathcal{R}^\ell$, and the elements of H are ordered as $h_1, h_2, \dots, h_m$. When $H = \mathbb{Z}_2 \oplus \mathbb{Z}_2$, we have $m = 4$, and we assume that $h_1 = (0, 0)$, $h_2 = (0, 1)$, $h_3 = (1, 0)$ and $h_4 = (1, 1)$. When $H = \mathbb{Z}_2 \oplus \mathbb{Z}_6$, we have $m = 6$, and we assume that $h_1 = (0, 0)$, $h_2 = (0, 1)$, $h_3 = (0, 2)$, $h_4 = (1, 0)$, $h_5 = (1, 1)$ and $h_6 = (1, 2)$. When $H = \mathbb{Z}_2 \oplus \mathbb{Z}_4$, we have $m = 8$, and we assume that $h_1 = (0, 0)$, $h_2 = (0, 1)$, $h_3 = (0, 2)$, $h_4 = (0, 3)$, $h_5 = (1, 0)$, $h_6 = (1, 1)$, $h_7 = (1, 2)$

and $h_8 = (1, 3)$. The codes $\mathcal{C}_a$ whose parameters $[m\ell, k, d]$ are labelled as * are MDS codes, while the remaining codes listed in Table 8.1 are almost MDS codes.

(q, t, ℓ, m)	H	$a(y)$	$[m\ell, k, d]$
$(3, 2, 2, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(y^{h_2} + \xi^6 y^{h_3} + \xi^5 y^{h_4},$ $y^{h_1} + \xi^7 y^{h_2} + \xi^5 y^{h_3} + y^{h_4})$	$[8, \frac{3}{2}, 6]$
$(3, 2, 2, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(y^{h_1} + \xi y^{h_2} + \xi^7 y^{h_3} + \xi^6 y^{h_4},$ $\xi y^{h_1} + \xi^5 y^{h_2} + 2y^{h_3} + \xi^5 y^{h_4})$	$[8, 2, 6]$
$(3, 2, 2, 8)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$(\xi^5 y^{h_1} + y^{h_2} + y^{h_3} + \xi^5 y^{h_5} + \xi^7 y^{h_6} + y^{h_8},$ $2y^{h_1} + \xi y^{h_2} + \xi^2 y^{h_3} + \xi^5 y^{h_4} + 2y^{h_5}$ $+ \xi^5 y^{h_6} + \xi^7 y^{h_7} + y^{h_8})$	$[16, \frac{7}{2}, 12]$
$(3, 2, 3, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(\xi^5 y^{h_1} + \xi^2 y^{h_2} + \xi y^{h_3} + \xi^7 y^{h_4},$ $\xi^5 y^{h_1} + \xi y^{h_2} + \xi^3 y^{h_3} + \xi^6 y^{h_4},$ $\xi^3 y^{h_2} + \xi^3 y^{h_3} + \xi^6 y^{h_4})$	$[12, 2, 10]$
$(5, 2, 2, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(\xi^9 y^{h_1} + \xi^{23} y^{h_2} + 3y^{h_3} + \xi^4 y^{h_4},$ $\xi^{11} y^{h_1} + 3y^{h_2} + 3y^{h_3} + \xi^{22} y^{h_4})$	$[8, 2, 6]$
$(5, 2, 2, 6)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	$(\xi^{14} y^{h_1} + \xi y^{h_2} + \xi^{19} y^{h_3} + \xi^{10} y^{h_4}$ $+ \xi^{19} y^{h_5} + \xi y^{h_6}, 2y^{h_1} + 4y^{h_2} + \xi^{13} y^{h_3}$ $+ \xi^{17} y^{h_4} + \xi^9 y^{h_5} + \xi^{19} y^{h_6})$	$[12, 3, 9]$
$(5, 2, 2, 6)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	$(\xi^{13} y^{h_1} + \xi^4 y^{h_2} + 3y^{h_3} + \xi^9 y^{h_4} + \xi^8 y^{h_5} + \xi^3 y^{h_6},$ $\xi^{20} y^{h_1} + \xi^{22} y^{h_2} + y^{h_3} + \xi^{19} y^{h_4} + \xi^3 y^{h_5} + \xi^5 y^{h_6})$	* $[12, \frac{5}{2}, 10]$
$(5, 2, 3, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(2y^{h_1} + \xi^7 y^{h_2} + \xi^{22} y^{h_3} + \xi^4 y^{h_4},$ $\xi^{14} y^{h_1} + \xi y^{h_2} + \xi^{20} y^{h_3} + \xi^{21} y^{h_4},$ $y^{h_1} + \xi^{20} y^{h_2} + \xi^9 y^{h_3} + \xi^{10} y^{h_4})$	$[12, \frac{3}{2}, 10]$
$(5, 2, 3, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(3y^{h_1} + \xi^2 y^{h_2} + 4y^{h_3} + \xi^7 y^{h_4},$ $\xi^{22} y^{h_1} + 2y^{h_2} + \xi^8 y^{h_3} + \xi^9 y^{h_4},$ $\xi^{23} y^{h_1} + \xi^{19} y^{h_2} + \xi^{10} y^{h_3} + 2y^{h_4})$	* $[12, 2, 11]$
$(5, 2, 3, 6)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	$(\xi y^{h_1} + \xi^{23} y^{h_2} + \xi^4 y^{h_3} + \xi^{19} y^{h_5} + \xi^{15} y^{h_6},$ $\xi^7 y^{h_1} + y^{h_2} + \xi^{23} y^{h_3} + \xi^5 y^{h_4} + 2y^{h_5} + \xi^5 y^{h_6},$ $\xi^{11} y^{h_1} + \xi^8 y^{h_2} + \xi^{11} y^{h_3} + \xi^8 y^{h_4} + y^{h_5} + \xi^{21} y^{h_6})$	$[18, 3, 15]$
$(7, 2, 2, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(\xi^{15} y^{h_1} + \xi^7 y^{h_2} + \xi^{22} y^{h_3} + \xi^{10} y^{h_4},$ $\xi^{13} y^{h_1} + \xi^{43} y^{h_2} + \xi^4 y^{h_3} + y^{h_4})$	* $[8, 2, 7]$
$(7, 2, 2, 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	$(5y^{h_1} + \xi^{21} y^{h_2} + \xi^{46} y^{h_3} + \xi^{25} y^{h_4},$ $\xi^{15} y^{h_1} + \xi^{29} y^{h_2} + \xi^{42} y^{h_3} + 6y^{h_4})$	$[8, 2, 6]$

$(7, 2, 3, 6)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	$(\xi^{11}y^{h_1} + 4y^{h_2} + \xi^{12}y^{h_3} + 2y^{h_4} + \xi y^{h_5} + \xi^{30}y^{h_6},$ $\xi^{29}y^{h_1} + \xi^{41}y^{h_3} + \xi^{41}y^{h_4} + 2y^{h_5} + \xi^{31}y^{h_6},$ $6y^{h_1} + \xi^{19}y^{h_2} + \xi^{29}y^{h_3} + \xi^{46}y^{h_4} + \xi^{47}y^{h_5} + \xi^{35}y^{h_6})$	$[18, 3, 15]$
----------------	------------------------------------	---	---------------

Table 8.1: Some MDS and almost MDS additive H -QA codes over $\mathbb{F}_{q^t}$

In the next chapter, we mention a brief conclusion and state some interesting open research questions in this direction.

Conclusion and future work

Let q be a prime power and $t \geq 2$ be an integer. Let $\mathbb{F}_q$ and $\mathbb{F}_{q^t}$ denote the finite fields of orders q and q^t , respectively. Let n, ℓ be positive integers, and let $m_1, m_2, \dots, m_\ell$ be positive integers coprime to q satisfying $n = m_1 + m_2 + \dots + m_\ell$. Let $\Omega = (\omega_1, \omega_2, \dots, \omega_\ell)$ be fixed, where $\omega_1, \omega_2, \dots, \omega_\ell$ are non-zero elements of $\mathbb{F}_q$. In this thesis, a new class of additive codes over finite fields, *viz.* Ω -multi-twisted (Ω -MT) additive codes, is defined and studied, which is a generalization of cyclic and constacyclic additive codes and an extension of MT (linear) codes introduced by Aydin and Halilović [5]. By applying the Chinese Remainder Theorem, a canonical form decomposition for Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is provided. A trace description for all Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is provided through their canonical form decomposition. Further, the asymptotic properties of the rates and relative Hamming distances of a special class of MT additive codes are studied by applying probabilistic methods. It is shown that there exists an asymptotically

good infinite sequence of MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with rate $\frac{v}{p^\eta \ell t}$ and relative Hamming distance at least δ , where δ is a positive real number satisfying $h_{q^t}(\delta) < 1 - \frac{1}{\ell t}$, p is an odd prime coprime to q , $v = \text{ord}_p(q)$ and η is the largest positive integer satisfying $p^\eta | (q^v - 1)$. This shows that the family of MT additive codes over finite fields is asymptotically good. As a consequence, special classes of MT additive codes such as cyclic and constacyclic additive codes over finite fields are shown to be asymptotically good.

By placing ordinary, Hermitian and $*$ trace bilinear forms, the dual codes of all MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ are studied. More precisely, necessary and sufficient conditions for an Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ to be (i) self-orthogonal, (ii) self-dual and (iii) an additive code with complementary dual (or an ACD code) with respect to the aforementioned trace bilinear forms are derived. Besides this, a necessary and sufficient condition for the existence of a self-dual Ω -MT additive code of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ is also derived. Further, by applying these results and Witt decomposition theory, explicit enumeration formulae for all self-orthogonal, self-dual and ACD Ω -MT additive codes of length n and block lengths $(m_1, m_2, \dots, m_\ell)$ over $\mathbb{F}_{q^t}$ are also obtained with respect to the aforementioned trace bilinear forms. These enumeration formulae are useful in classifying these special classes of MT additive codes over finite fields up to monomial equivalence. Furthermore, probabilistic methods and results from groups and geometry are employed to establish the existence of asymptotically good infinite sequences of self-orthogonal and ACD MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with relative Hamming distance at least δ and rates $\frac{v}{p^\eta \ell t}$ and $\frac{2v}{p^\eta \ell t}$ with respect to the aforementioned trace bilinear forms, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2} - \frac{1}{2\ell t}$, p is an odd prime coprime to q , $v = \text{ord}_p(q)$ and η is the largest positive integer satisfying $p^\eta | (q^v - 1)$. This shows that self-orthogonal and ACD MT additive codes over finite fields are asymptotically good. As a consequence, their special classes such as self-orthogonal and ACD constacyclic additive codes over finite fields are shown to be asymptotically good. It is also shown that there exists an asymptotically good infinite sequence of self-dual MT additive codes of length $p^\alpha \ell$ and block length $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{q^t}$ with relative Hamming distance

at least δ and rate $\frac{1}{2}$ with respect to the aforementioned trace bilinear forms, where δ is a positive real number satisfying $h_{q^t}(\delta) < \frac{1}{2\ell t}$ and p is an odd prime coprime to q such that $\text{ord}_p(q)$ is even. This shows that self-dual MT additive codes over finite fields are asymptotically good. As a special case, it is deduced that self-dual cyclic and negacyclic additive codes over finite fields are asymptotically good. Besides this, a special class of self-dual MT additive codes over $\mathbb{F}_{q^t}$ with respect to the ordinary trace bilinear form, *viz.* doubly-even self-dual MT additive codes, is studied, where q is an even prime power. With the help of the trace description of MT additive codes, a characterization of a special class of doubly-even self-dual MT additive codes is provided in terms of their constituents. Using this characterization and by applying probabilistic methods and results from groups and geometry, it is shown that the doubly-even self-dual MT additive codes of length $p^\alpha \ell$ and block lengths $p^\alpha \rightarrow \infty$ over $\mathbb{F}_{2^t}$ are asymptotically good, where p is an odd prime such that $\text{ord}_p(2)$ is even. Consequently, it is deduced that doubly-even self-dual cyclic additive codes over $\mathbb{F}_{2^t}$ are asymptotically good.

Finally, a new class of additive codes over finite fields, *viz.* additive quasi-Abelian (QA) codes, is defined and studied, which is a generalization of a special class of MT additive codes over finite fields and an extension of linear QA codes over finite fields introduced by Wasan [67]. By placing ordinary, Hermitian and $*$ trace bilinear forms, algebraic structures of these codes and their dual codes are thoroughly investigated by expressing these codes as direct sums of additive codes over finite fields. Necessary and sufficient conditions are derived for an additive QA code to be (i) self-orthogonal, (ii) self-dual and (iii) ACD. A necessary and sufficient condition for the existence of a self-dual additive QA code is derived. Explicit enumeration formulae for all self-orthogonal, self-dual and ACD additive QA codes are also obtained. Besides this, several MDS and almost MDS codes belonging to the class of 1-generator additive QA codes are also listed. It would be interesting

- to classify all self-dual, self-orthogonal and ACD MT additive codes over finite fields.
- to determine Hamming weight distributions of MT additive codes over finite fields with the help of their trace description.

- to further study MT additive codes over finite commutative chain rings and their dual codes.
- to explore if additive QA codes over finite fields in general, and their three special classes such as self-orthogonal, self-dual and ACD additive QA codes over finite fields in particular, are asymptotically good.

Bibliography

- [1] Alahmadi, A., Güneri, C., Shoaib, H. and Solé, P.: Long quasi-polycyclic t -CIS codes, *Adv. Math. Commun.* 12(1), pp. 189-198, 2018.
- [2] Alperin, J. L. and Bell, R. B.: *Groups and representations*, Graduate Texts in Mathematics, Vol. 162, Springer, New York, 1995.
- [3] Ambrose, C. D.: On Artin's primitive root conjecture, Doctoral thesis, Göttingen Univ., 2014.
- [4] Aydin, N., Siap, I., and Ray-Chaudhuri, D. K.: The structure of 1-generator quasi-twisted codes and new linear codes, *Des. Codes Cryptogr.* 24(3), pp. 313-326, 2001.
- [5] Aydin, N. and Halilović, A.: A generalization of quasi-twisted codes: Multi-twisted codes, *Finite Fields Appl.* 45, pp. 96-106, 2017.
- [6] Ball, S., Gamboa, G. and Lavrauw, M.: On additive MDS codes over small fields, *Adv. Math. Commun.* 17(4), 2023.
- [7] Beachy, J. A.: *Introductory lectures on rings and modules*, Cambridge Univ. Press, Cambridge, 1999.
- [8] Benson, S.: Students ask the darnedest things: A result in elementary group theory, *Math. Magazine* 70(3), pp. 207-211, 1997.
- [9] Berman, S. D.: Semisimple cyclic and Abelian codes II, *Cybernetics* 3(3), pp. 17-23, 1967.

- [10] Berlekamp, E. R.: *Algebraic Coding Theory*, McGraw-Hill Book Company, New York, 1968.
- [11] Betsumiya, K., Harada, M. and Munemasa, A.: A complete classification of doubly even self-dual codes of length 40, *Electron. J. Comb.* 19(3), 2012.
- [12] Betsumiya, K., Harada, M. and Munemasa, A., Type II Codes over $\mathbb{F}_{2^r}$, *14th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, Lecture Notes in Computer Science, Vol. 2227, pp. 102-111, Springer Berlin Heidelberg (2001).
- [13] Bierbrauer, J. and Edel, Y.: Quantum twisted codes, *J. Combin. Des.* 8(3), pp. 174–188, 2000.
- [14] Borello, M., Güneri, C., Saçıkara, E. and Solé, P.: The concatenated structure of quasi-abelian codes, *Des. Codes Cryptogr.* 90, pp. 2647-2661, 2022.
- [15] Brualdi, R. A.: *Introductory combinatorics*, Prentice Hall, New Jersey, 2009.
- [16] Calderbank, A. R., Rains, E. M., Shor, P. M. and Sloane, N. J. A.: Quantum error correction via codes over GF(4), *IEEE Trans. Inform. Theory* 44(4), pp. 1369-1387, 1998.
- [17] Cao, Y., Chang, X. and Cao, Y.: Constacyclic $\mathbb{F}_q$ -linear codes over $\mathbb{F}_{q^t}$, *Appl. Algebra Engrg. Comm. Comput.* 26(4), pp. 369–388, 2015.
- [18] Chauhan, V. and Sharma, A.: A generalization of multi-twisted codes over finite fields, their Galois duals and Type II codes, *J. Appl. Math. Comput.* 68(2), pp. 1413-1447, 2022.
- [19] Chauhan, V. and Sharma, A.: Hamming weight enumerators of multi-twisted codes with at most two non-zero constituents, *Finite Fields Appl.* 76, Article No. 101910, 2021.
- [20] Chen, C. L., Peterson, W. W. and Weldon Jr., E. J.: Some results on quasi-cyclic codes, *Inform. and Control.* 15(4), pp. 407-423, 1969.

- [21] Chepyzhov, V. V.: New lower bounds for minimum distance of linear quasi-cyclic and almost linear cyclic codes, *Probl. Peredachi Inf.* 28(1), pp. 39-51, 1992.
- [22] Ding, C., Kohel, D. R. and Ling, S.: Split group codes, *IEEE Trans. Inform. Theory* 46(2), pp. 485-495, 2000.
- [23] Dummit, D. S. and Foote, R. M.: *Abstract Algebra*, 3rd ed., Wiley Hoboken, New Jersey, 2004.
- [24] Fan, Y. and Lin, L. R.: Thresholds of random quasi-abelian codes, *IEEE Trans. Inform. Theory* 61(1), pp. 82-90, 2014.
- [25] Fan, Y., Ling, S., Liu, H., Shen, J. and Xing, C.: Cumulative distance enumerators of random codes and their thresholds, <http://arxiv.org/abs/1212.5679>, 2012.
- [26] Gaborit, P., Pless, V., Solé, P. and Atkin, O.: Type II codes over $\mathbb{F}_4$, *Finite Fields Appl.* 8(2), pp. 171-183, 2002.
- [27] Grove, L. C.: *Classical groups and geometric algebra*, American Mathematical Society, Providence, Rhode Island, 2008.
- [28] Guruswami, V., Rudra, A. and Sudan, M.: *Essential coding theory*, Draft available at: <http://www.cse.buffalo.edu/faculty/atri/courses/coding-theory/book>, 2022.
- [29] Heath-Brown, D. R.: Artin's conjecture for primitive roots, *The Quarterly J. Math.* 37 (1), pp. 27-38, 1986.
- [30] Hill, R. and Greenough, P. P.: Optimal quasi-twisted codes, *In Proc. Int. Workshop Algebraic and Comb. Coding Theory, Voneshta Voda, Bulgaria* pp. 92-97 (1992).
- [31] Hooley, C.: On Artin's conjecture, *J. Reine Angew. Math.* 225, pp. 209-220 (1967).

- [32] Huffman, W. C.: Additive cyclic codes over $\mathbb{F}_4$, *Adv. Math. Commun.* 1(4), pp. 427–459, 2007.
- [33] Huffman, W. C.: Additive cyclic codes over $\mathbb{F}_4$, *Adv. Math. Commun.* 2(3), pp. 309–343, 2008.
- [34] Huffman, W. C.: Cyclic $\mathbb{F}_q$ -linear $\mathbb{F}_{q^t}$ -codes, *Int. J. Inform. Coding Theory* 1(3), pp. 249–284, 2010.
- [35] Huffman, W. C. and Pless, V.: *Fundamentals of error-correcting codes*, Cambridge Univ. Press, Cambridge, 2010.
- [36] Huffman, W. C.: On the theory of $\mathbb{F}_q$ -linear $\mathbb{F}_{q^t}$ -codes, *Adv. Math. Commun.* 7(3), pp. 349–378, 2013.
- [37] Jia, Y.: On quasi-twisted codes over finite fields, *Finite Fields Appl.* 18, pp. 237–257, 2012.
- [38] Jitman, S. and Ling, S.: Quasi-abelian codes, *Des. Codes Cryptogr.* 74, pp. 511–531, 2015.
- [39] Jitman, S., Palines, H. S. and Dela Cruz, R. B.: On quasi-abelian complementary dual codes, *In Coding Theory and Applications: ICMCTA*, pp. 192–206, 2017.
- [40] Kabatiansky, G. A.: On existence of good cyclic almost linear codes over non prime fields, *Probl. Peredachi Inf.* 13(3), pp. 18–21, 1977.
- [41] Kaur, T. and Sharma, A.: Constacyclic additive codes over finite fields, *Discrete Math. Algorithms Appl.* 9(3), Article no. 1750037, pp. 1–35, 2017.
- [42] Lang, S. and Tate, J. (eds.): *The collected papers of Emil Artin*, Addison–Wesley Publishing Co., Inc., Reading, Mass. London, 1965.
- [43] Lidl, R. and Niederreiter, H.: *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1994.
- [44] 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.

- [45] Ling, S. and Solé, P.: On the algebraic structure of quasi-cyclic codes I. Finite fields, *IEEE Trans. Inform. Theory* 47(7), pp. 2751-2760, 2001.
- [46] Ling, S. and Xing, C.: *Coding theory: A first course*, Cambridge University Press, 2004.
- [47] Moree, P.: Artin's primitive root conjecture - a survey, *Integers* 12(6), pp. 1305–1416 (2012).
- [48] Nebe, G., Quebbemann, H. G., Rains, E. M. and Sloane, N. J.: Complete weight enumerators of generalized doubly-even self-dual codes, *Finite Fields Appl.* 10(4), pp. 540-550, 2004.
- [49] OEIS Foundation Inc.: Primes with primitive root 2, Entry A001122 in *The On-Line Encyclopedia of Integer Sequences*, <https://oeis.org/A001122>, 2022.
- [50] Palines, H. S., Jitman, S. and Cruz, R. B. D.: Hermitian self-dual quasi-abelian codes, *J. Algebra Comb. Discrete Appl.* 5(1), pp. 5-18, 2018.
- [51] Prange, E.: Cyclic error-correcting codes in two symbols, *Air force Cambridge research center*, pp. 103, 1957.
- [52] Rains, E. M.: Nonbinary quantum codes, *IEEE Trans. Inform. Theory* 45(6), pp. 1827–1832, 1999.
- [53] Seroussi, G. and Lempel, A.: Factorization of symmetric matrices and trace-orthogonal bases in finite fields, *SIAM J. Comput.* 9(4), pp. 758-767, 1980.
- [54] Shannon, C. E.: A mathematical theory of communication, *Bell Syst. Tech. J.* 27, pp. 379-423 and 623-656, 1948.
- [55] Sharma, A. and Chauhan, V.: Skew multi-twisted codes over finite fields and their Galois duals, *Finite Fields Appl.* 59, pp. 297-334, 2019.
- [56] 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.
- [57] Sharma, A. and Kaur, T.: On cyclic $\mathbb{F}_q$ -linear $\mathbb{F}_{q^t}$ -codes, *Int. J. Inf. Coding Theory* 4(1), pp. 19-46, 2017.

- [58] Sharma, A. and Kaur, T.: Enumeration of complementary-dual cyclic $\mathbb{F}_q$ -linear $\mathbb{F}_{q^t}$ -codes, *Discrete Math.* 341(4), pp. 965-980, 2018.
- [59] Shi, M., Wu, R. and Solé, P.: Asymptotically good additive cyclic codes exist, *IEEE Communications Letters* 22(10), pp. 1980-1983, 2018.
- [60] Shi, M., Liu, N., Özbudak, F. and Solé, P.: Additive cyclic complementary dual codes over $\mathbb{F}_4$, *Finite Fields Appl.* 83, Article No. 102087, pp. 1-22, 2022.
- [61] Shi, M., Liu, N., Kim, J. L. and Solé, P.: Additive complementary dual codes over $\mathbb{F}_4$, *Des. Codes Cryptogr.* 91(1), pp. 273-284, 2023.
- [62] Siap, I. and Kulhan, N.: The structure of generalized quasi-cyclic codes, *Appl. Math. E-Notes* 5, pp. 24-30, 2005.
- [63] Stein, W.: *Elementary number theory: primes, congruences, and secrets*, Undergrad. Texts Math., Springer, New York, 2009.
- [64] Szymiczek, K.: *Bilinear algebra: An introduction to the algebraic theory of quadratic forms*, Gordon and Breach Science Publishers, Amsterdam, 1997.
- [65] Taylor, D. E.: *The geometry of the classical groups*, Sigma Series in Pure Mathematics, Heldermann Verlag, 1992.
- [66] Upfal, E. and Mitzenmacher, M.: *Probability and computing: randomized algorithms and probabilistic analysis*, Cambridge Univ. Press, Cambridge, 2005.
- [67] Wasan, S. K.: Quasi abelian codes, *Publ. Inst. Math.* 21(35), pp. 201-206, 1977.
- [68] Townsend, R. L. and Weldon, E. J., Jr.: Self-orthogonal quasi-cyclic codes, *IEEE Trans. Inform. Theory* 13(2), pp. 183-195, 1967.
- [69] Wood, J. A.: Witt's extension theorem for mod four valued quadratic forms, *Trans. Amer. Math. Soc.* 336(1), pp. 445-461, 1993.
- [70] Zhang, G. and Chen, B.: Self-orthogonal quasi-abelian codes are asymptotically good, *Finite Fields Appl.* 78, 101958, 2022.