On some special classes of linear and additive codes over finite commutative chain rings

A Ph.D. Thesis

by

Monika Yadav
(PhD18302)

Under the Supervision of Prof. Anuradha Sharma

Indraprastha Institute of Information Technology, Delhi

May 2024

On some special classes of linear and additive codes over finite commutative chain rings

A Thesis

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

by

Monika Yadav

(PhD18302)

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 linear and additive codes over finite commutative chain rings"** being submitted by **"Ms. Monika Yadav"** to the **Indraprastha Institute of Information Technology Delhi**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by her under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

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

New Delhi
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 linear and additive codes over finite commutative chain rings"**, 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.

Monika.

Signature of the candidate
Monika Yadav
Date: May 7, 2024

Acknowledgements

I am profoundly grateful to all those who have supported me throughout this challenging yet rewarding journey of completing my doctoral dissertation.

First and foremost, I extend my heartfelt gratitude to my Ph.D. advisor, Prof. Anuradha Sharma, for her invaluable guidance, unwavering support, and insightful feedback. Her mentorship has not only shaped my research but also enriched my growth as a scholar.

I would also like to acknowledge the Council of Scientific & Industrial Research (CSIR) for its financial support, which allowed me to focus on my research without financial constraints.

I am also grateful to Dr. Donghoon Chang and Dr. Subhabrata Samajder, members of my Ph.D. committee for their generous support and encouragement. I sincerely thank Dr. Shanta Laishram (ISI, New Delhi, India), the external examiner during my comprehensive exam and fellowship enhancement seminar.

I extend my sincere gratitude to IIIT-Delhi for the support and facilities provided throughout my Ph.D. journey. The state-of-the-art infrastructure, well-equipped labs, and comprehensive resources have been instrumental in the success of my research. I would also like to thank all my friends and research fellows at IIIT-Delhi for the discussion and for sharing their valuable ideas, which helped me to understand the concepts well.

I am extremely grateful to my thesis evaluation committee members, Prof. Steven T. Dougherty (University of Scranton, Scranton, PA, USA), Prof. Kiyoshi Nagata (Daito Bunka University, Itabashi-ku, Tokyo, Japan), and Prof. Santanu Sarkar (Indian Institute of Technology Madras, Chennai, India), for their valuable

time and consideration.

My gratitude extends to my family for their boundless love and unwavering faith in my abilities. To my parents, whose sacrifices and constant motivation have been the pillars of my journey, I owe an immeasurable debt of gratitude.

I would also like to express my deepest gratitude to my husband for his unwavering support and understanding throughout the challenging journey of pursuing a Ph.D. His selfless support allowed me to focus on my research and reach the culmination of this academic endeavor.

Above all, I am grateful to the Almighty for blessing me with strength and wisdom.

New Delhi Monika Yadav
May 2024

Abstract

Self-orthogonal codes, self-dual codes, and linear codes with complementary duals (LCD codes) constitute the three most important and well-studied classes of linear codes. These codes have nice algebraic structures and are of great significance both from the practical and theoretical points of view. Self-orthogonal and self-dual codes have nice connections with the theory of designs and are useful in constructing secret-sharing schemes with nice access structures. LCD codes are useful in designing orthogonal direct-sum masking schemes, which protect sensitive information against side-channel attacks (SCA) and fault injection attacks (FIA). In the 1990s, it was shown that many binary non-linear codes can be viewed as Gray images of linear codes over the ring $\mathbb{Z}_4$ of integers modulo 4. Since then, much research has been devoted to studying self-orthogonal, self-dual, and LCD codes over finite commutative chain rings. In fact, the problem of the determination of enumeration formulae for self-orthogonal, self-dual, and LCD codes has attracted a great deal of attention, as these enumeration formulae are useful in classifying such codes up to equivalence.

In this thesis, we obtain enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings of odd characteristic. As special cases, one can obtain enumeration formulae for self-orthogonal and self-dual codes over quasi-Galois rings and Galois rings of odd characteristic. However, we observe that this enumeration technique can not be extended to count all self-orthogonal and self-dual codes over quasi-Galois rings and Galois rings of even characteristic. We modify this enumeration technique and provide explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over quasi-Galois and Galois rings of even characteristic. We also obtain explicit enumeration formulae for all σ-LCD codes of an arbitrary length over finite commutative chain rings. Besides this, we show that the class of σ-LCD codes over finite commutative chain rings is asymptotically good. We also show that every free linear code over a finite commutative chain ring is equivalent to a σ-LCD code when the residue field of the chain ring is of order at least 5. We also explicitly determine all inequivalent σ-LCD codes of length n, rank k and Hamming distance d over a finite commutative chain ring when $k \in \{1, n-1\}$ and $1 \leq d \leq n$.

We further study additive codes over finite commutative chain rings and their dual codes with respect to the ordinary trace bilinear form in the Galois additivity case. We derive necessary and sufficient conditions under which an additive code over a finite commutative chain ring is (i) self-orthogonal, (ii) self-dual, and (iii) an additive code with complementary dual (or an ACD code). We further provide enumeration formulae for all additive self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings in certain special cases. We also count all ACD codes of an arbitrary length over finite commutative chain rings. We further show that a free additive code over a finite commutative chain ring is a maximum distance separable code (or an MDS code) if and only if its Torsion code is an additive MDS code. This motivates us to introduce and study two new classes of additive codes over finite fields, *viz.* additive generalized Reed-Solomon (additive GRS) codes and additive generalized twisted Reed-Solomon (additive GTRS) codes, which are extensions of linear GRS codes and linear GTRS codes, respectively. Unlike linear GRS codes, we note that additive GRS codes are not MDS codes in general. We also identify several new classes of additive MDS and almost MDS codes within the families of additive GRS and GTRS codes. We also note that, unlike linear codes, the dual code of an additive MDS code need not be an additive MDS code. We identify several classes of additive MDS codes whose dual codes are also MDS within the families of additive GRS and GTRS codes. We provide constructions of additive MDS self-orthogonal, self-dual and ACD codes over finite fields through additive GRS and GTRS codes. We also obtain several classes of additive TRS codes that are not monomially equivalent to additive RS codes. Based on additive MDS codes whose dual codes are also MDS, we provide a perfect

threshold secret-sharing scheme that can detect cheating, identify a certain number of cheaters among the participants, and correctly recover the secret.

List of Publications

1. **Yadav, M.** and Sharma, A.: Mass formulae for Euclidean self-orthogonal and self-dual codes over finite commutative chain rings, *Discrete Math.* 344(1), 112152 (2021).

2. 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).

3. **Yadav, M.** and Sharma, A.: On the enumeration and classification of σ-LCD codes over finite commutative chain rings, *Discrete Math.* 345(8), 112915 (2022).

4. **Yadav, M.** and Sharma, A.: A recursive method for the construction and enumeration of self-orthogonal and self-dual codes over the quasi-Galois ring $\mathbb{F}_{2^r}[u]/ < u^e >$, *Des. Codes Cryptogr.* 91(5), pp. 1973-2003 (2023).

5. **Yadav, M.** and Sharma, A.: Construction and enumeration of self-orthogonal and self-dual codes over Galois rings of even characteristic, *Des. Codes Cryptogr.* 92, pp. 303-339 (2024).

6. **Yadav, M.** and Sharma, A.: Some new classes of additive MDS and almost MDS codes over finite fields, *Finite Fields Appl.* 95, p. 102394 (2024).

7. Sharma, S., **Yadav, M.** and Sharma, A.: On additive quasi-Abelian codes over finite fields and their duality properties, *Under review.*

Contents

List of Symbols

Symbol	**Meaning**
$\lvert Y \rvert$	Cardinality of the set Y
$\mathbb{F}_q$	The finite field of order q
$GR(p^e, r)$	The Galois ring of characteristic p^e and cardinality p^{er}
$\lfloor \cdot \rfloor$	The floor function
$\lceil \cdot \rceil$	The ceiling function
$\begin{bmatrix} \cdot \\ \cdot \end{bmatrix}_q$	The Gaussian binomial coefficient
Ker Φ	The kernel of the linear transformation Φ
A^t	The transpose of the matrix A
$\det A$	The determinant of the matrix A
$\mathcal{D}iag(A)$	The diagonal matrix whose principal diagonal is the same as that of the square matrix A
$\mathcal{M}_{\kappa \times n}(\mathcal{R})$	The set of all $\kappa \times n$ matrices over the ring $\mathcal{R}$
$Sym_\kappa(\mathcal{R})$	The set of all $\kappa \times \kappa$ symmetric matrices over the ring $\mathcal{R}$
$Alt_\kappa(\mathcal{R})$	The set of all $\kappa \times \kappa$ alternating matrices over the ring $\mathcal{R}$
$\mathcal{R}^*$	The unit group of the ring $\mathcal{R}$
d_H	The Hamming distance
w_H	The Hamming weight
$\dim_F(V)$	The dimension of a finite-dimensional vector space V

	over the finite field F
$[\cdot,\cdot]\restriction_{V\times V}$	The restriction of the map $[\cdot,\cdot]$ to $V\times V$
$\mathbb{N}$	The set of natural numbers
$\binom{m}{i}$	The binomial coefficient "m choose i"
$a\equiv b \pmod{\ell}$	The integers a and b are congruent modulo a positive integer ℓ
$\deg(f(x))$	The degree of a non-zero polynomial $f(x)$
$\min\{a,b\}$	The minimum of a and b
$\max\{a,b\}$	The maximum of a and b
$\gcd(a,b)$	The greatest common divisor of a and b
ϕ	The Euler phi function

1 Introduction

The object of this thesis is

- to enumerate all self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings of odd characteristic.
- to obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over quasi-Galois rings of even characteristic.
- to count all self-orthogonal and self-dual codes of an arbitrary length over Galois rings of even characteristic.
- to study and enumerate linear codes with complementary σ-duals (*i.e.,* σ-LCD codes) over finite commutative chain rings.
- to study and enumerate additive self-orthogonal, additive self-dual, and additive codes with complementary duals (ACD codes) over finite commutative chain rings.

- to introduce and study some new classes of additive MDS and almost MDS codes over finite fields.

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

1.1 Self-orthogonal and self-dual codes over finite commutative chain rings

Self-orthogonal and self-dual codes form the two most important and extensively studied classes of linear codes. These codes have nice connections with the theory of designs [5, 60] and the theory of modular forms and unimodular lattices [8, 37, 44, 84]. These codes are also useful in constructing quantum error-correcting codes [4, 57, 93] and designing secret-sharing schemes with nice access structures [17, 39]. This motivated several coding theorists to study these codes and provide methods to construct these codes [42, 45, 57, 83].

In the 1990s, it was shown that many binary non-linear codes (*e.g.* Kerdock, Preparata, Goethals and Delsarte-Goethals codes) can be viewed as Gray images of linear codes over the ring $\mathbb{Z}_4$ of integers modulo 4 [20, 21]. Since then, there has been much interest in studying self-orthogonal and self-dual codes over finite commutative chain rings [13, 37, 38, 45, 47, 75–77, 93]. In particular, the problem of determination of explicit enumeration formulae for self-orthogonal and self-dual codes over various finite commutative chain rings has also attracted a lot of attention, as these enumeration formulae are useful in the classification of these two classes of codes up to equivalence [12, 13, 31, 77, 100]. Below, we summarize the results known in this direction.

Pless [83] obtained explicit enumeration formulae for self-orthogonal and self-dual codes over finite fields. Gaborit [45] obtained explicit enumeration formulae for self-dual codes over the ring $\mathbb{Z}_4$ and the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^2\rangle$. Betty *et al.* [13] provided enumeration formula for self-dual codes over the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^3\rangle$. Further, with the help of this enumeration formula, they classified all self-dual codes of lengths 2 and 4 over $\mathbb{F}_q[u]/\langle u^3\rangle$, where $q \in \{2, 3, 4, 5, 7, 8, 9\}$. Galvez *et al.* [47] obtained the enumeration formula for self-orthogonal codes over the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^2\rangle$. As a special case of this result, they deduced the enumeration formula for self-dual codes over $\mathbb{F}_q[u]/\langle u^2\rangle$, as derived earlier by Gaborit [45]. In the same work, they also counted all self-orthogonal codes over the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^3\rangle$, where q is an odd prime power. With the help of these enumeration formulae, they also classified all self-orthogonal and self-dual codes of lengths $2, 3, 4, 5, 6$ and 7 over the ring $\mathbb{F}_2[u]/\langle u^2\rangle$ and all self-orthogonal and self-dual codes of lengths $2, 3, 4, 5$ and 6 over the ring $\mathbb{F}_3[u]/\langle u^2\rangle$. Betty and Munemasa [12] obtained the enumeration formula for all self-orthogonal codes over the ring $\mathbb{Z}_{p^2}$ of integers modulo p^2, where p is a prime. They also established the enumeration formula for all even quaternary codes (*i.e.*, self-dual codes over $\mathbb{Z}_4$ with the Hamming weight of each codeword divisible by 8). Using this enumeration formula, they derived the enumeration formula for all Type II quaternary codes (*i.e.*, even quaternary codes containing the all-one vector $\mathbf{1} = (1, 1, \ldots, 1)$) as a special case. In a related work, Nagata *et al.* [76] gave a characterization of all self-dual codes over the ring $\mathbb{Z}_{p^3}$ of integers modulo p^3, where p is a prime. They also provided the explicit enumeration formula for all self-dual codes over $\mathbb{Z}_{p^3}$. In a subsequent work, Nagata *et al.* [77] obtained the enumeration formula for all self-dual codes over the ring $\mathbb{Z}_{p^e}$ of integers modulo p^e, where p is an odd prime and $e \geq 4$ is an integer. In another related work, Nagata *et al.* [75] explained the sequential structure of self-dual codes over the ring $\mathbb{Z}_{2^e}$ of integers modulo 2^e, where $e \geq 3$ is an integer. They also provided the enumeration formula for all self-dual codes over the ring $\mathbb{Z}_{2^e}$.

In Chapter 2, we first recall some basic properties of finite commutative chain rings and their special classes such as Galois rings and quasi-Galois rings. We further discuss algebraic structures and some basic properties of linear codes over finite commutative chain rings and their special classes such as self-orthogonal, self-dual and linear codes with complementary duals (LCD codes). We next state some basic results on the geometry of symplectic, unitary, orthogonal and quadratic spaces over finite fields. We also present enumeration formulae for all self-orthogonal and self-dual codes over finite fields obtained by Pless [83]. These results are needed to count all self-orthogonal, self-dual and LCD codes over finite commutative chain rings.

Now let e and r be positive integers, and let p be a prime number. Let $\mathcal{R}_{e,r}$

denote a finite commutative chain ring with the maximal ideal $\langle u\rangle$ of nilpotency index e. Then the quotient ring $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u\rangle$ is a finite field and is called the residue field of $\mathcal{R}_{e,r}$. Suppose that the residue field $\overline{\mathcal{R}}_{e,r}$ is of order p^r. One can see that the characteristic of the chain ring $\mathcal{R}_{e,r}$ is a power of p. When $e = 1$, we note that $\mathcal{R}_{1,r} \simeq \mathbb{F}_{p^r}$ and that the enumeration formulae for self-orthogonal and self-dual codes over $\mathcal{R}_{1,r}$ are obtained by Pless [83]. So we assume, throughout this thesis, that $e \geq 2$.

In Chapter 3, we assume that the characteristic of the chain ring $\mathcal{R}_{e,r}$ is odd, *i.e.,* p is an odd prime. We first provide a recursive method to construct a self-orthogonal (*resp.* self-dual) code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over the chain ring $\mathcal{R}_{e,r}$ from a self-orthogonal (*resp.* self-dual) code of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and length n over the finite commutative chain ring $\mathcal{R}_{e-2,r} = \mathcal{R}_{e,r}/\langle u^{e-2}\rangle$, and vice versa, where $e \geq 4$ is an integer and $k_1, k_2, \ldots, k_e$ are non-negative integers satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. This recursive method gives rise to a recurrence relation between the number of self-orthogonal (*resp.* self-dual) codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ and the number of self-orthogonal (*resp.* self-dual) codes of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and length n over the chain ring $\mathcal{R}_{e-2,r} = \mathcal{R}_{e,r}/\langle u^{e-2}\rangle$. By repeatedly applying this recurrence relation, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of a given length and a given type over $\mathcal{R}_{e,r}$. From this, we obtain enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathcal{R}_{e,r}$. As special cases, one can obtain enumeration formulae for all self-orthogonal and self-dual codes over quasi-Galois and Galois rings of odd characteristic. With the help of these enumeration formulae and by carrying out computations in the Magma Computational Algebra System, we classify all self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over the quasi-Galois ring $\mathbb{F}_5[u]/\langle u^2\rangle$ and of lengths $2, 3$ and 4 over the quasi-Galois ring $\mathbb{F}_7[u]/\langle u^2\rangle$.

In Chapter 4, we observe that when $p = 2$ and $\mathcal{R}_{e,r} = \mathbb{F}_{2^r}[u]/\langle u^e\rangle$ (a quasi-Galois ring of characteristic 2), each self-orthogonal (*resp.* self-dual) code over $\mathcal{R}_{e,r}/\langle u^{e-2}\rangle \simeq \mathbb{F}_{2^r}[u]/\langle u^{e-2}\rangle$ can not be lifted to a self-orthogonal (*resp.* self-dual) code over $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ through the construction method employed in Chapter 3. Thus the enumeration technique employed in Chapter 3 to count all self-orthogonal (*resp.* self-dual) codes over finite commutative chain rings of odd characteristic can not be extended as it is to enumerate self-orthogonal (*resp.* self-dual) codes over the quasi-Galois ring $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$. In fact, the enumeration formula for self-orthogonal codes over the quasi-Galois ring $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ is known only when $e=2$, while the enumeration formula for self-dual codes over the ring $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ is known only when $e\in\{2,3\}$. In this chapter, we provide a modified recursive method to construct self-orthogonal and self-dual codes of the type $\{k_1,k_2,\ldots,k_e\}$ and length n over $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ from a self-orthogonal code of the same length n and dimension $k_1+k_2+\cdots+k_{\lceil\frac{e}{2}\rceil}$ over $\mathbb{F}_{2^r}$, and vice versa, where n is a positive integer and $k_1,k_2,\ldots,k_e$ are non-negative integers satisfying $2k_1+2k_2+\cdots+2k_{e-i+1}+k_{e-i+2}+k_{e-i+3}+\cdots+k_i\leq n$ for $\lceil\frac{e+1}{2}\rceil\leq i\leq e$. Further, by using this modified recursive method, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ for each integer $e\geq 2$. We also obtain complete lists of inequivalent self-orthogonal and self-dual codes of lengths $2,3,4$ and 5 over the ring $\mathbb{F}_2[u]/\langle u^3\rangle$ and of lengths $2,3$ and 4 over the ring $\mathbb{F}_4[u]/\langle u^2\rangle$.

Next, let $\mathscr{R}_{e,r}$ denote the Galois ring of characteristic 2^e and cardinality 2^{er}. The Teichm*ü*ller set $\mathcal{T}_r$ of the Galois ring $\mathscr{R}_{e,r}$ can be viewed as the finite field of order 2^r under the addition operation $\oplus$ and the multiplication operation of $\mathscr{R}_{e,r}$, where for $a,b\in\mathcal{T}_r$, $a\oplus b$ is the unique element in $\mathcal{T}_r$ satisfying $a\oplus b=(a+b) \pmod 2$. When $r=1$, Nagata *et al.* [75] counted all self-dual codes over the ring $\mathscr{R}_{e,1}=\mathbb{Z}_{2^e}$ using the enumeration formula for doubly even codes over $\mathcal{T}_1=\{0,1\}$ obtained by Gaborit [45, Th. 7]. When $r\geq 2$, we observe that the enumeration technique employed by Nagata *et al.* [75] can not be extended as it is to count self-orthogonal and self-dual codes over $\mathscr{R}_{e,r}$. This is because, when $r\geq 2$, one needs to count solutions of the system (5.4.2) consisting of linear as well as non-linear equations over $\mathcal{T}_r$. When $r=1$, the system (5.4.2) reduces to the system of linear equations over $\mathcal{T}_1$ and one can write down its matrix form representation and count its solutions. However, the same technique can not be employed to count solutions of the system (5.4.2) over $\mathcal{T}_r$ when $r\geq 2$. Besides this, one needs to count certain special linear codes of length n over $\mathcal{T}_r$, which we shall call doubly even codes over $\mathcal{T}_r$ (see Definition 5.2.1 and Section 5.3). When $r=1$, Gaborit [45, Th. 7] provided the explicit enumeration formula for doubly even codes of length n over $\mathcal{T}_1(\simeq\mathbb{F}_2)$ by noting that $c\cdot c\equiv w_H(c) \pmod 4$ for all $c \in \mathcal{T}_1^n$ and further applying the well-known MacWilliams identity for Hamming weight enumerators of binary linear codes. Nagata *et al.* [75] applied Theorem 7 of Gaborit [45] to count self-dual codes over $\mathscr{R}_{e,1} = \mathbb{Z}_{2^e}$. However, when $r \geq 2$, we note that $c \cdot c \equiv w_H(c) \pmod 4$ does not hold for all $c \in \mathcal{T}_r^n$, and hence the enumeration technique for counting doubly even codes over $\mathcal{T}_1 (\simeq \mathbb{F}_2)$, employed in [45], can not be extended to count doubly even codes over $\mathcal{T}_r$ when $r \geq 2$. In this chapter, we first count all doubly even codes over $\mathcal{T}_r$ and their two special classes, *viz.* the codes containing the all-one vector and the codes that do not contain the all-one vector, by studying the geometry of a certain special quadratic space over $\mathcal{T}_r$. One can deduce the enumeration formula for binary doubly even codes obtained in [45, Th. 7] from the enumeration formula for doubly even codes over $\mathcal{T}_r$ as a special case, which gives rise to another proof of Theorem 7 of Gaborit [45]. We further provide a modified recursive method to construct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ from a $(k_1 + k_2 + \cdots + k_{\lfloor \frac{e}{2} \rfloor})$-doubly even self-orthogonal code of the same length n and dimension $k_1 + k_2 + \cdots + k_{\lceil \frac{e}{2} \rceil}$ over $\mathcal{T}_r$, where n is a positive integer and $k_1, k_2, \ldots, k_e$ are non-negative integers satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. With the help of this recursive construction method and the enumeration formulae for doubly even codes over $\mathcal{T}_r$ and their two special classes, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathscr{R}_{e,r}$. Using these enumeration formulae, we classify all self-orthogonal and self-dual codes of lengths $2, 3$ and 4 over $\mathscr{R}_{2,2}$ up to monomial equivalence.

1.2 σ-LCD codes over finite commutative chain rings

Linear codes with complementary duals (or LCD codes) are linear codes, which intersect with their respective dual codes trivially. These codes constitute one of the most important and well-studied classes of linear codes and play a significant role in counter-measures to passive and active side-channel analyses on embedded cryptosystems [18, 25, 26, 90]. Besides applications in cryptography, these codes have several applications in communication systems, consumer electronics, and data storage [24, 72]. This motivated many researchers to further study these codes and to provide several methods to construct these codes [28, 29, 55, 64, 66, 68, 89]. Besides this, the problem of determination of the explicit enumeration formula for LCD codes has recently attracted a lot of attention [27, 69, 91], as these enumeration formula are useful in classifying such codes up to equivalence [3]. Below, we summarize some of the significant results known in this direction.

Massey [72] gave an algebraic characterization of LCD codes over finite fields and showed that asymptotically good LCD codes over finite fields exist. He also showed that LCD codes provide an optimum linear coding solution for the two-user binary adder channel. Later, Sendrier [89] showed that LCD codes over finite fields meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes. Carlet *et al.* [29] showed that any linear code over the finite field $\mathbb{F}_q$ of order q is equivalent to a Euclidean LCD code over $\mathbb{F}_q$ when $q > 3$ and that any linear code over the finite field $\mathbb{F}_{q^2}$ of order q^2 is equivalent to a Hermitian LCD code over $\mathbb{F}_{q^2}$ when $q > 2$. Liu *et al.* [67] characterized and studied LCD codes over finite commutative chain rings in particular and over finite principal ideal rings in general. In another work [66], they investigated σ-LCD codes of length n over the finite commutative chain ring R, where σ is a mapping from R^n into itself satisfying certain conditions. They also constructed new entanglement-assisted quantum error-correcting codes with maximal entanglement by using Gray images of σ-LCD codes over the chain ring $\mathbb{F}_q[u]/\langle u^2\rangle$. In a recent work, Bhowmick *et al.* [14] showed that an LCD code over a finite commutative local Frobenius ring is free. They also derived a necessary and sufficient condition for the existence of an LCD code over a finite commutative local Frobenius ring. They also identified some new optimal cyclic LCD codes over the ring $\mathbb{Z}_4$ of different lengths. In a related work, Araya and Harada [3] gave a complete classification of LCD codes of lengths up to 13 over $\mathbb{F}_2$ and LCD codes of lengths up to 10 over $\mathbb{F}_3$. They also explicitly determined all inequivalent LCD $[n, 1, d]$-codes and $[n, n-1, d]$-codes over $\mathbb{F}_2$ and $\mathbb{F}_3$.

Now let σ_0 be an automorphism of $\mathcal{R}_{e,r}$, and let $\overline{\sigma}_0$ be the corresponding automorphism of the residue field $\overline{\mathcal{R}}_{e,r}$ of $\mathcal{R}_{e,r}$, defined as $\overline{\sigma}_0(a + \langle u\rangle) = \sigma_0(a) + \langle u\rangle$ for all $a + \langle u\rangle \in \overline{\mathcal{R}}_{e,r}$. Let σ be an automorphism of $\mathcal{R}_{e,r}^n$ corresponding to the automorphism σ_0 of $\mathcal{R}_{e,r}$, defined as $\sigma(v_1, v_2, \ldots, v_n) = (\sigma_0(v_1), \sigma_0(v_2), \ldots, \sigma_0(v_n))$ for all

$(v_1, v_2, \ldots, v_n) \in \mathcal{R}_{e,r}^n$.

In Chapter 6, we obtain explicit enumeration formulae for all σ-LCD codes of an arbitrary length over the chain ring $\mathcal{R}_{e,r}$ when $\overline{\sigma}_0^2$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$. With the help of these enumeration formulae and by applying the classification algorithm, we classify all Euclidean LCD codes of lengths 2, 3, 4 and 5 over the quasi-Galois ring $\mathbb{F}_2[u]/\langle u^2\rangle$ and of lengths 2, 3 and 4 over the quasi-Galois ring $\mathbb{F}_3[u]/\langle u^2\rangle$, and all σ-LCD codes of lengths 2, 3 and 4 over the quasi-Galois ring $\mathbb{F}_4[u]/\langle u^2\rangle$, where σ_0 is an automorphism of $\mathbb{F}_4[u]/\langle u^2\rangle$ such that the corresponding automorphism $\overline{\sigma}_0$ of the residue field $\mathbb{F}_4$ has order 2. Besides this, we show that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good, and that every free linear $[n, k, d]$-code over $\mathcal{R}_{e,r}$ is equivalent to a σ-LCD $[n, k, d]$-code over $\mathcal{R}_{e,r}$ when $|\overline{\mathcal{R}}_{e,r}| > 4$. We also explicitly determine all inequivalent σ-LCD $[n, 1, d]$-codes and $[n, n-1, d]$-codes over $\mathcal{R}_{e,r}$ for $1 \leq d \leq n$.

1.3 Additive codes over finite commutative chain rings

Linear codes are further extended to additive codes, which have nice algebraic structures and are useful in constructing quantum stabilizer codes [15, 22, 93]. Calderbank *et al.* [22] first introduced and studied additive codes over the finite field $\mathbb{F}_4$ and their dual codes with respect to the ordinary trace bilinear form. They also constructed quantum error-correcting codes from additive self-orthogonal codes over $\mathbb{F}_4$. Later, Bierbrauer and Edel [15] developed the theory of additive codes over arbitrary finite fields. In a related work, Huffman [52] studied additive codes over finite fields and their dual codes with respect to the ordinary and Hermitian trace bilinear forms. He also derived the MacWilliams identity and a Singleton type bound for additive codes over finite fields. Mahmoudi and Samei [71] studied additive codes over Galois rings. They studied algebraic structures of these codes by establishing a one-to-one correspondence between linear codes over $\mathbb{Z}_{p^e}$ and additive codes over the Galois ring $GR(p^e, r)$, where p is a prime and e, r are positive integers. Cao *et al.* [23] studied cyclic additive codes over Galois rings and provided a canonical form decomposition for these codes. With the help of this decomposition, they further enumerated all cyclic additive codes of an arbitrary length over Galois rings. Moro *et al.* [74] studied cyclic additive codes over finite commutative chain rings with respect to two different notions of additivity, *viz.* Galois-additivity and Eisenstein-additivity. Recently, Sidana and Kashyap [93] constructed entanglement-assisted quantum error-correcting codes (EAQECCs) from additive codes over finite commutative local Frobenius rings. They also provided a formula for the minimum number of entanglement qudits required to construct an EAQECC from an additive code over a Galois ring.

Now let $r \geq 1$, $m \geq 2$ and $e \geq 2$ be integers. Let

$$\mathcal{R}_{e,r} = \frac{GR(p^{\mathfrak{s}}, r)[x]}{\langle g(x), p^{\mathfrak{s}-1}x^t \rangle}$$

and

$$\mathcal{R}_{e,rm} = \frac{GR(p^{\mathfrak{s}}, rm)[x]}{\langle g(x), p^{\mathfrak{s}-1}x^t \rangle}$$

be two finite commutative chain rings, where $g(x) = x^{\kappa} + p(a_{\kappa-1}x^{\kappa-1} + \cdots + a_1 x + a_0) \in GR(p^{\mathfrak{s}}, r)[x]$ is an Eisenstein polynomial with a_0 as a unit in $GR(p^{\mathfrak{s}}, r)$, $e = \kappa(\mathfrak{s}-1) + t$, and $1 \leq t \leq \kappa$ when $\mathfrak{s} \geq 2$, while $t = \kappa$ when $\mathfrak{s} = 1$. Note that $\mathcal{R}_{e,r}$ is a subring of $\mathcal{R}_{e,rm}$. By Theorem 4.3.1 of [16], we see that $\mathcal{R}_{e,rm}$ is the Galois extension of $\mathcal{R}_{e,r}$ of degree m. If $u := x + \langle g(x), p^{\mathfrak{s}-1}x^t \rangle$, then one can easily see that e is the least positive integer satisfying $u^e = 0$ in $\mathcal{R}_{e,r}$ (and in $\mathcal{R}_{e,rm}$) and that $\langle u \rangle$ is the unique maximal ideal of both $\mathcal{R}_{e,r}$ and $\mathcal{R}_{e,rm}$. Note that the residue field $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u \rangle$ of $\mathcal{R}_{e,r}$ is of order p^r and the residue field $\overline{\mathcal{R}}_{e,rm} = \mathcal{R}_{e,rm}/\langle u \rangle$ of $\mathcal{R}_{e,rm}$ is of order p^{rm}. One can easily see that the set $\mathcal{R}_{e,rm}^n$ of all n-tuples over $\mathcal{R}_{e,rm}$ can be viewed as an $\mathcal{R}_{e,r}$-module under the component-wise addition and the component-wise scalar multiplication. Now an additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ is defined as an $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$.

In Chapter 7, we study additive codes over $\mathcal{R}_{e,rm}$ and their dual codes with respect to the ordinary trace bilinear form. We also study their three special classes, *viz.* additive self-orthogonal codes, additive self-dual codes and additive codes with complementary duals (ACD codes) with respect to the ordinary trace bilinear form. We also derive necessary and sufficient conditions under which an additive code over $\mathcal{R}_{e,rm}$ is (i) self-orthogonal, (ii) self-dual, and (iii) ACD. Besides this, we derive necessary and sufficient conditions for the existence of an additive self-dual code over $\mathcal{R}_{e,rm}$. As an application of these results, we obtain explicit enumeration formulae for all additive self-orthogonal and self-dual codes of an arbitrary length over $\mathcal{R}_{e,rm}$ in the following three cases: (i) both p and m are odd (ii) $p = 2$ and $\mathfrak{s} = 1$, and (iii) $p = 2$, $\kappa = 1$ and m is odd. We will also count all ACD codes of an arbitrary length over $\mathcal{R}_{e,rm}$, where $e \geq 2$, $r \geq 1$ and $m \geq 2$ are arbitrary integers. We also note that a free additive code $\mathcal{C}$ over $\mathcal{R}_{e,rm}$ is a maximum distance separable (MDS) code if and only if its Torsion code $Tor_1(\mathcal{C})$ is an additive MDS code over $\overline{\mathcal{R}}_{e,rm}$, where an additive code of length n over $\overline{\mathcal{R}}_{e,rm}$ is defined as an $\overline{\mathcal{R}}_{e,r}$-subspace of $\overline{\mathcal{R}}_{e,rm}^{n}$.

MDS codes are optimal codes that attain the well-known Singleton bound. These codes achieve the highest possible Hamming distance for given code length and size. As the Hamming distance of a code measures its error-detecting and error-correcting capabilities, these codes exhibit the maximum error-detecting and error-correcting capabilities for given code length and size. Singleton [94] first introduced and studied MDS codes, because of their usefulness in constructing constant-weight binary codes with large sizes and large Hamming distances. Reed and Solomon [86] introduced and studied generalized Reed-Solomon (GRS) codes, constituting the most important and well-studied class of linear MDS codes. These codes are useful in improving the reliability of compact discs and digital audio tapes due to their burst error-correction capabilities. These codes are also useful in designing DNA error-correcting codes [97, 98] and locally recoverable codes for distributive storage systems [50, 96]. Besides GRS codes, there are other well-known constructions of linear MDS codes with the help of n-arcs in projective geometry [48, 70] and circulant Cauchy matrices [87]. In general, MDS codes have found applications in network coding, cryptography, data storage, and quantum mechanics [9, 35, 43, 50]. Besides this, these codes have nice connections with geometric objects such as n-arcs and combinatorial objects such as orthogonal arrays [48, 53]. This motivated several coding theorists to study these codes and provide construction methods for these codes [10, 35, 55, 65, 86].

In a recent and related work, Beelen *et al.* [11] introduced and studied twisted Reed-Solomon (TRS) codes with one twist as a natural generalization of RS codes and showed that these codes are not MDS in general. They also identified two classes of TRS codes, which are MDS. In another work, Beelen *et al.* [9] observed that the dual codes of TRS codes are not TRS codes in general. They further identified a class of TRS codes whose dual codes are also TRS. Besides this, they identified a class of TRS codes that resist Sidelnikov-Shestakov and Wieschebrink attacks on the McEliece cryptosystem. Beelen *et al.* [10] further studied TRS codes with ℓ twists and identified several classes of TRS codes, which are MDS. They also identified several classes of TRS codes that are not monomially equivalent to RS codes. Fang and Fu [43] constructed six new classes of MDS self-dual codes over finite fields through GRS and extended GRS codes. Jin [55] constructed several classes of MDS LCD codes over finite fields through GRS codes. Liu and Liu [65] provided methods to construct MDS LCD codes over finite fields through generalized twisted Reed-Solomon (GTRS) codes with ℓ twists.

Additive MDS codes over finite fields have nice connections with geometric objects such as pseudo-arcs [7] and are also useful in constructing quantum stabilizer codes [61]. Recently, Shi *et al.* [92] remarked that only the additivity and complementarity properties (and not the linearity property) of a code are needed to design orthogonal direct-sum masking schemes, which are useful in protecting sensitive information against side-channel attacks (SCA) and fault injection attacks (FIA). Hence additive codes with complementary duals (ACD codes) can also be used in counter-measures to passive and active side-channel analyses on embedded cryptosystems. One can easily see that the security parameter of such schemes is equal to the Hamming distance of the code. In another recent work, Choi *et al.* [32] provided methods to construct ACD codes over finite fields. They also listed some ACD codes with good parameters over $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_9$, and identified some MDS ACD codes among these codes.

In Chapter 8, we introduce and study two new classes of additive codes over finite fields, *viz.* additive generalized Reed-Solomon (additive GRS) codes and additive generalized twisted Reed-Solomon (additive GTRS) codes, which are extensions of linear generalized Reed-Solomon (GRS) codes and generalized twisted Reed-Solomon (GTRS) codes, respectively. Unlike linear GRS codes, we note that additive GRS codes are not MDS codes and the dual code of an additive GRS code need not be an additive GRS code in general. We derive necessary and sufficient conditions under which an additive GRS code is MDS. We further apply this result to identify several new classes of additive MDS codes and a class of additive MDS codes whose dual codes are also MDS within the family of additive GRS codes. We also identify several new classes of additive codes that are either MDS or almost MDS within the family of additive GTRS codes. We also obtain several classes of additive TRS codes that are not monomially equivalent to additive RS codes. Besides this, we identify classes of monomially inequivalent additive MDS TRS codes and additive MDS RS codes, whose dual codes are also MDS. We also provide methods to construct additive MDS self-orthogonal, self-dual, and ACD codes through additive GRS and GTRS codes. Based on additive MDS codes whose dual codes are also MDS, we present a perfect threshold secret-sharing scheme that can detect cheating, identify a certain number of cheaters among the participants, and correctly recover the secret.

1.4 Conclusion and future work

In Chapter 9, we mention a brief conclusion and state some interesting open problems.

2

Some preliminaries

In this chapter, we will first state some basic properties of finite commutative chain rings. We will also discuss algebraic structures and some basic properties of linear codes over finite commutative chain rings and their special subclasses such as self-orthogonal, self-dual and linear codes with complementary duals (LCD codes). We will next state some basic results on the geometry of symplectic, unitary, orthogonal and quadratic spaces over finite fields. We will also present enumeration formulae for all self-orthogonal and self-dual codes over finite fields obtained by Pless [83]. These results are needed to count all self-orthogonal, self-dual and LCD codes over finite commutative chain rings.

2.1 Finite commutative chain rings

A finite commutative ring R with unity is called (i) a local ring if it has a unique maximal ideal and (ii) a chain ring if all its ideals form a chain under the set-theoretic inclusion relation. One can easily see that a finite commutative chain ring has a unique maximal ideal, and hence is a local ring. However, a local ring need not be a chain ring. For example, one can easily see that the quotient ring $\mathbb{F}_2[u,v]/\langle u^2, v^2, uv - vu\rangle$ is a local ring, but not a chain ring. Now the following theorem provides a characterization of finite commutative chain rings.

Theorem 2.1.1. *[36, Prop. 2.1] For a finite commutative ring R with unity, the following statements are equivalent:*

(a) R is a local ring and the maximal ideal of R is principal.

(b) R is a local principal ideal ring.

(c) R is a chain ring.

If R is a finite commutative chain ring and M is the maximal ideal of R, then the quotient ring $\overline{R} = R/M$ is a finite field and is called the residue field of R. Some examples of finite commutative chain rings are finite fields, quasi-Galois rings and Galois rings [73].

A quasi-Galois ring is defined as a quotient ring of the form $\mathbb{F}_q[u]/\langle u^e\rangle$, where $\mathbb{F}_q$ is the finite field of order q and e is a positive integer. In particular, when $e = 1$, we note that $\mathbb{F}_q[u]/\langle u\rangle$ is the finite field $\mathbb{F}_q$. One can easily see that all the ideals of $\mathbb{F}_q[u]/\langle u^e\rangle$ form a chain $\{0\} \subset \langle u^{e-1}\rangle \subset \langle u^{e-2}\rangle \subset \cdots \langle u\rangle \subset \langle 1\rangle = \mathbb{F}_q[u]/\langle u^e\rangle$. Thus by Theorem 2.1.1, the quotient ring $\mathbb{F}_q[u]/\langle u^e\rangle$ is a finite commutative chain ring with the maximal ideal $\langle u\rangle$.

We will next define Galois rings and state their basic properties. A finite commutative ring R with unity is called a Galois ring if all its zero-divisors (including 0) form an ideal of R generated by a prime number. Some examples of Galois rings are finite fields and rings of integers modulo prime powers. If R is a Galois ring whose zero-divisors (including 0) form an ideal of R generated by a prime number p, then by Lemmas 14.2 and 14.4 of [101], we see that the ring R has characteristic $p^{\mathfrak{s}}$ and cardinality $p^{\mathfrak{s}r}$, where $\mathfrak{s}$ and r are positive integers. Further, for a prime number p and positive integers $\mathfrak{s}$ and r, the following theorem provides a method to construct a Galois ring of characteristic $p^{\mathfrak{s}}$ and cardinality $p^{\mathfrak{s}r}$ and shows that such a Galois ring is unique up to isomorphism.

Theorem 2.1.2. *[101] Let p be a prime number and $\mathfrak{s}, r$ be positive integers. Let $\mathbb{Z}_{p^{\mathfrak{s}}}$ be the ring of integers modulo $p^{\mathfrak{s}}$, and let $\mathbb{Z}_{p^{\mathfrak{s}}}[x]$ be the ring of all polynomials in the indeterminate x over $\mathbb{Z}_{p^{\mathfrak{s}}}$. Let $h(x) \in \mathbb{Z}_{p^{\mathfrak{s}}}[x]$ be a monic basic irreducible polynomial of degree r, (such a polynomial $h(x)$ always exists in $\mathbb{Z}_{p^{\mathfrak{s}}}[x]$ by Theorem 13.9 of [101]). Then the quotient ring $\mathbb{Z}_{p^{\mathfrak{s}}}[x]/\langle h(x)\rangle$ is a Galois ring of characteristic $p^{\mathfrak{s}}$ and cardinality $p^{\mathfrak{s}r}$. Furthermore, any Galois ring of characteristic $p^{\mathfrak{s}}$ and cardinality $p^{\mathfrak{s}r}$ is isomorphic to the quotient ring $\mathbb{Z}_{p^{\mathfrak{s}}}[x]/\langle h(x)\rangle$.*

By the above theorem, we see that for every prime number p and positive integers $\mathfrak{s}$ and r, there exists a unique (up to isomorphism) Galois ring of characteristic $p^{\mathfrak{s}}$ and cardinality $p^{\mathfrak{s}r}$, which we will denote by $GR(p^{\mathfrak{s}}, r)$. By Lemma 14.4 of [101], we see that all the ideals of the Galois ring $GR(p^{\mathfrak{s}}, r)$ form the chain $\{0\} \subset \langle p^{\mathfrak{s}-1}\rangle \subset \langle p^{\mathfrak{s}-2}\rangle \subset \cdots \subset \langle p\rangle \subset \langle 1\rangle = GR(p^{\mathfrak{s}}, r)$. Thus by Theorem 2.1.1, the Galois ring $GR(p^{\mathfrak{s}}, r)$ is a chain ring. From this, it follows that the ideal $\langle p\rangle$ is the maximal ideal of $GR(p^{\mathfrak{s}}, r)$ and that the quotient ring $\overline{GR(p^{\mathfrak{s}}, r)} = GR(p^{\mathfrak{s}}, r)/\langle p\rangle$ is the finite field of order p^r and is called the residue field of $GR(p^{\mathfrak{s}}, r)$. Further, by Theorem 14.8 of [101], we see that there exists an element $\xi \in GR(p^{\mathfrak{s}}, r)$, which is a root of a monic basic primitive polynomial of degree r over $\mathbb{Z}_{p^{\mathfrak{s}}}$ and has multiplicative order $p^r - 1$. One can easily see that $GR(p^{\mathfrak{s}}, r) = \mathbb{Z}_{p^{\mathfrak{s}}}[\xi] = \{a_0 + a_1\xi + \cdots + a_{r-1}\xi^{r-1} : a_i \in \mathbb{Z}_{p^{\mathfrak{s}}} \text{ for } 0 \leq i \leq r-1\}$. Furthermore, the cyclic group generated by ξ is the only subgroup of the unit group of $GR(p^{\mathfrak{s}}, r)$, which is isomorphic to the multiplicative group of the residue field $\overline{GR(p^{\mathfrak{s}}, r)}$. The set $\{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is called the Teichm*ü*ller set of the Galois ring $GR(p^{\mathfrak{s}}, r)$. By Theorem 14.8 of [101], we see that each element in the Galois ring $GR(p^{\mathfrak{s}}, r)$ can be uniquely expressed as $a_0 + a_1 p + a_2 p^2 + \cdots + a_{\mathfrak{s}-1}p^{\mathfrak{s}-1}$, where $a_0, a_1, a_2, \ldots, a_{\mathfrak{s}-1} \in \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$.

Now the following theorem provides a method to construct all finite commutative chain rings as extensions of Galois rings.

Theorem 2.1.3. *[73, Th. XVII.5] For a prime number p and positive integers $\mathfrak{s}$ and r, the quotient ring*

$$\mathfrak{R} = \frac{GR(p^{\mathfrak{s}}, r)[x]}{\langle g(x), p^{\mathfrak{s}-1}x^t\rangle}$$

is a finite commutative chain ring, where $g(x) = x^\kappa + p(a_{\kappa-1}x^{\kappa-1} + \cdots + a_1 x + a_0) \in GR(p^{\mathfrak{s}}, r)[x]$ is an Eisenstein polynomial with a_0 as a unit in $GR(p^{\mathfrak{s}}, r)$ and $1 \leq t \leq \kappa$

when $\mathfrak{s} \geq 2$, while $t = \kappa$ when $\mathfrak{s} = 1$. If $u := x + \langle g(x), p^{\mathfrak{s}-1}x^t \rangle$, then the ideal $\langle u \rangle$ is the unique maximal ideal of $\mathfrak{R}$ and has nilpotency index $e = \kappa(\mathfrak{s}-1)+t$, and the residue field $\overline{\mathfrak{R}} = \mathfrak{R}/\langle u \rangle$ is of order p^r. Furthermore, all the ideals of the chain ring $\mathfrak{R}$ are given by

$$\{0\} \subset \langle u^{e-1} \rangle \subset \langle u^{e-2} \rangle \subset \cdots \langle u \rangle \subset \langle 1 \rangle = \mathfrak{R}.$$

Conversely, any finite commutative chain ring is isomorphic to a quotient ring of the form $\mathfrak{R}$ for some prime number p, positive integers $\mathfrak{s}$, r, κ and t, and the Eisentein polynomial $g(x) \in GR(p^{\mathfrak{s}}, r)[x]$.
(The integers $p, \mathfrak{s}, r, \kappa$ and t are called invariants of the chain ring $\mathfrak{R}$ with the maximal ideal of nilpotency index $e = \kappa(\mathfrak{s}-1)+t$.)

From this point on, we assume, throughout this thesis, that p is a prime number and e, r are positive integers. Let $\mathcal{R}_{e,r}$ denote a finite commutative chain ring with the invariants $p, \mathfrak{s}, r, \kappa$ and t, the maximal ideal $\langle u \rangle$ of nilpotency index $e = \kappa(\mathfrak{s}-1)+t$ and the residue field $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u \rangle$ as the finite field of order p^r. By Theorem 2.1.3, we see that all the ideals of $\mathcal{R}_{e,r}$ are given by $\{0\} \subset \langle u^{e-1} \rangle \subset \langle u^{e-2} \rangle \subset \cdots \subset \langle u \rangle \subset \langle 1 \rangle = \mathcal{R}_{e,r}$. Further, we note that $|\langle u^i \rangle| = p^{r(e-i)}$ for $0 \leq i \leq e$.

Theorem 2.1.4. *[73] The following hold.*

(a) The characteristic of $\mathcal{R}_{e,r}$ is $p^{\mathfrak{s}}$ for some positive integer $\mathfrak{s}$.

(b) We have $|\mathcal{R}_{e,r}| = |\overline{\mathcal{R}}_{e,r}|^e = p^{re}$.

(c) The Galois ring $GR(p^{\mathfrak{s}}, r)$ is the largest Galois ring contained in $\mathcal{R}_{e,r}$ and is called the coefficient ring of $\mathcal{R}_{e,r}$. Furthermore, the Teichmüller set $\mathcal{T}_{e,r} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ of the coefficient ring $GR(p^{\mathfrak{s}}, r)$ is also considered as the Teichmüller set of the chain ring $\mathcal{R}_{e,r}$.

(d) Each element $a \in \mathcal{R}_{e,r}$ can be uniquely expressed as

$$a = a_0 + ua_1 + \cdots + u^{e-1}a_{e-1}, \quad \textit{where} \quad a_i \in \mathcal{T}_{e,r} \textit{ for } 0 \leq i \leq e-1,$$

(such a representation of elements of $\mathcal{R}_{e,r}$ is called the Teichmüller representation). Moreover, a is a unit in $\mathcal{R}_{e,r}$ if and only if $a_0 \neq 0$.

(e) If ξ is a root of a monic basic primitive polynomial of degree r over $\mathbb{Z}_{p^{\mathfrak{s}}}$, then $GR(p^{\mathfrak{s}}, r) = \mathbb{Z}_{p^{\mathfrak{s}}}[\xi]$. Each element $a \in \mathcal{R}_{e,r}$ can also be uniquely expressed as

$$a = \sum_{i=0}^{\kappa-1} \big(\sum_{j=0}^{r-1} a_{ij}\xi^j\big)u^i,$$

where $a_{ij} \in \mathbb{Z}_{p^{\mathfrak{s}}}$ for $0 \leq i \leq t-1$ and $0 \leq j \leq r-1$, while $a_{ij} \in \mathbb{Z}_{p^{\mathfrak{s}-1}}$ for $t \leq i \leq \kappa - 1$ and $0 \leq j \leq r-1$.

One can define a canonical epimorphism $^- : \mathcal{R}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ as $a \mapsto \bar{a} = a + \langle u \rangle$ for all $a \in \mathcal{R}_{e,r}$. Note that the function $^-\restriction_{\mathcal{T}_{e,r}} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection.

Next, let σ_0 be an automorphism of $\mathcal{R}_{e,r}$, and let $\overline{\sigma}_0$ be the corresponding automorphism of the residue field $\overline{\mathcal{R}}_{e,r}$ of $\mathcal{R}_{e,r}$, defined as

$$\overline{\sigma}_0(\overline{a}) = \sigma_0(a) + \langle u \rangle = \overline{\sigma_0(a)}$$

for all $\overline{a} = a + \langle u \rangle \in \overline{\mathcal{R}}_{e,r}$. Let $Aut(\mathcal{R}_{e,r})$ denote the automorphism group of $\mathcal{R}_{e,r}$. Let $Aut_1(\mathcal{R}_{e,r})$ denote the set consisting of all automorphisms σ_0 of $\mathcal{R}_{e,r}$ such that the corresponding automorphism $\overline{\sigma}_0$ of $\overline{\mathcal{R}}_{e,r}$ is the identity automorphism, and let $Aut_2(\mathcal{R}_{e,r})$ denote the set consisting of all automorphisms σ_0 of $\mathcal{R}_{e,r}$ such that the corresponding automorphism $\overline{\sigma}_0$ of $\overline{\mathcal{R}}_{e,r}$ has order 2. Note that $Aut_1(\mathcal{R}_{e,r})$ is a subgroup of $Aut(\mathcal{R}_{e,r})$. Moreover, when $\mathfrak{s} \geq 2$, we see that $e = \kappa(\mathfrak{s}-1) + t > \kappa$. Further, by Theorem 2.1.4(d), we can write $u^\kappa = p\beta h$ in $\mathcal{R}_{e,r}$, where $\beta \in \mathcal{T}_{e,r} \setminus \{0\}$ and $h = 1 + h_1 u + h_2 u^2 + \cdots + h_{e-1}u^{e-1} \in 1 + \langle u \rangle$ with $h_1, h_2, \ldots, h_{e-1} \in \mathcal{T}_{e,r}$. Now the following theorem provides the automorphism group $Aut(\mathcal{R}_{e,r})$ of $\mathcal{R}_{e,r}$.

Theorem 2.1.5. *Let $\mathcal{R}_{e,r}$ be a finite commutative chain ring with invariants $p, \mathfrak{s}, r, \kappa$ and t, where $e = \kappa(\mathfrak{s}-1) + t$ is the nilpotency index of the unique maximal ideal $\langle u \rangle$ of $\mathcal{R}_{e,r}$. For $0 \leq b \leq r-1$, $\alpha \in \mathcal{T}_{e,r}$ and $\omega \in 1 + \langle u \rangle$, let us define a map $\sigma_{\alpha,\omega}^{(b)} : \mathcal{R}_{e,r} \to \mathcal{R}_{e,r}$ as*

$$\sigma_{\alpha,\omega}^{(b)}(a) = \sum_{i=0}^{\kappa-1} \big(\sum_{j=0}^{r-1} a_{ij}\xi^{jp^b}\big)\alpha^i\omega^i u^i \ \text{ for all } \ a = \sum_{i=0}^{\kappa-1} \big(\sum_{j=0}^{r-1} a_{ij}\xi^j\big)u^i \in \mathcal{R}_{e,r},$$

where $a_{ij} \in \mathbb{Z}_{p^{\mathfrak{s}}}$ for $0 \leq i \leq \kappa - 1$ and $0 \leq j \leq r-1$, while $0 \leq a_{ij} < p^{\mathfrak{s}-1}$ when

$t \le i \le \kappa - 1$.

(a) [2, *Prop. 1]* *When* $\mathfrak{s} = 1$, *the automorphism group* $Aut(\mathcal{R}_{e,r})$ *of* $\mathcal{R}_{e,r}$ *is given by*

$$Aut(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,\omega}^{(b)} : 0 \le b \le r-1, \alpha \in \mathcal{T}_{e,r} \setminus \{0\} \text{ and } \omega \in 1 + \langle u \rangle\}.$$

(b) [1, *Prop. 5]* *When* $\mathfrak{s} \ge 2$, *we can write* $u^\kappa = p\beta h$ *in* $\mathcal{R}_{e,r}$, *where* $\beta \in \mathcal{T}_{e,r} \setminus \{0\}$ *and* $h = 1 + h_1 u + h_2 u^2 + \cdots + h_{e-1}u^{e-1} \in 1 + \langle u \rangle$ *with* $h_1, h_2, \ldots, h_{e-1} \in \mathcal{T}_{e,r}$. *For* $0 \le b \le r-1$, *let* $\mathcal{J}_b$ *denote the set of all pairs* (α, ω) *with* $\alpha \in \mathcal{T}_{e,r} \setminus \{0\}$ *and* $\omega \in 1 + \langle u \rangle$ *satisfying* $\alpha^\kappa = \beta^{p^b - 1}$ *and* $p\omega^\kappa = p(1 + h_1^{p^b}\alpha\omega u + h_2^{p^b}\alpha^2\omega^2u^2 + \cdots + h_{e-1}^{p^b}\alpha^{e-1}\omega^{e-1}u^{e-1})h^{-1}$. *Then the automorphism group* $Aut(\mathcal{R}_{e,r})$ *of* $\mathcal{R}_{e,r}$ *is given by*

$$Aut(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,\omega}^{(b)} : 0 \le b \le r-1 \text{ and } (\alpha,\omega) \in \mathcal{J}_b\}.$$

By the above theorem, we see that for each automorphism σ_0 of $\mathcal{R}_{e,r}$, the corresponding automorphism $\overline{\sigma}_0$ of $\overline{\mathcal{R}}_{e,r}$ is given by $\overline{\sigma}_0(\overline{\xi}) = \overline{\xi}^{p^b}$ if $\sigma_0(\xi) = \xi^{p^b}$ for some integer b satisfying $0 \le b \le r-1$. In the following corollary, we explicitly determine the subgroup $Aut_1(\mathcal{R}_{e,r})$ of the automorphism group $Aut(\mathcal{R}_{e,r})$.

Corollary 2.1.1. *Let* $\mathcal{R}_{e,r}$ *be a finite commutative chain ring with invariants* $p, \mathfrak{s}, r, \kappa$ *and* t, *where* $e = \kappa(\mathfrak{s}-1) + t$.

(a) When $\mathfrak{s} = 1$, *we have*

$$Aut_1(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,\omega}^{(0)} : \alpha \in \mathcal{T}_{e,r} \setminus \{0\} \text{ and } \omega \in 1 + \langle u \rangle\}.$$

(b) When $\mathfrak{s} \ge 2$, *we have*

$$Aut_1(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,w}^{(0)} : (\alpha,\omega) \in \mathcal{J}_0\},$$

where $\mathcal{J}_0$ *is the set of all pairs* (α,ω) *with* $\alpha \in \mathcal{T}_{e,r} \setminus \{0\}$ *and* $\omega \in 1 + \langle u \rangle$ *satisfying* $\alpha^\kappa = 1$ *and* $p\omega^\kappa = p(1 + h_1\alpha\omega u + h_2\alpha^2\omega^2u^2 + \cdots + h_{e-1}\alpha^{e-1}\omega^{e-1}u^{e-1})h^{-1}$.

In the following corollary, we explicitly determine the subset $Aut_2(\mathcal{R}_{e,r})$ of the automorphism group $Aut(\mathcal{R}_{e,r})$.

Corollary 2.1.2. *Let $\mathcal{R}_{e,r}$ be a finite commutative chain ring with invariants $p, \mathfrak{s}, r, \kappa$ and t, where $e = \kappa(\mathfrak{s} - 1) + t$. When r is odd, we have $Aut_2(\mathcal{R}_{e,r}) = \emptyset$.*

(a) When r is even and $\mathfrak{s} = 1$, we have

$$Aut_2(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,\omega}^{(r/2)} : \alpha \in \mathcal{T}_{e,r} \setminus \{0\} \text{ and } \omega \in 1 + \langle u \rangle\}.$$

(b) When r is even and $\mathfrak{s} \geq 2$, we have

$$Aut_2(\mathcal{R}_{e,r}) = \{\sigma_{\alpha,w}^{(r/2)} : (\alpha, \omega) \in \mathcal{J}_{r/2}\},$$

where $\mathcal{J}_{r/2}$ is the set of all pairs (α, ω) with $\alpha \in \mathcal{T}_{e,r} \setminus \{0\}$ and $\omega \in 1 + \langle u \rangle$ satisfying $\alpha^{\kappa} = \beta^{p^{r/2}-1}$ and $p\omega^{\kappa} = p(1 + h_1^{p^{r/2}}\alpha\omega u + h_2^{p^{r/2}}\alpha^2\omega^2u^2 + \cdots + h_{e-1}^{p^{r/2}}\alpha^{e-1}\omega^{e-1}u^{e-1})h^{-1}$.

The following lemma is quite useful in counting all self-orthogonal and self-dual codes over finite commutative chain rings.

Lemma 2.1.1. *[12] Let $A \in \mathcal{M}_{k\times n}(\overline{\mathcal{R}}_{e,r})$ be a matrix of rank k. Let us define a map $\Phi_A : \mathcal{M}_{k\times n}(\overline{\mathcal{R}}_{e,r}) \to \mathcal{M}_{k\times k}(\overline{\mathcal{R}}_{e,r})$ as*

$$\Phi_A(N) = AN^t + NA^t \text{ for all } N \in \mathcal{M}_{k\times n}(\overline{\mathcal{R}}_{e,r}).$$

The map Φ_A is an $\overline{\mathcal{R}}_{e,r}$-linear transformation with image

$$\Phi_A(\mathcal{M}_{k\times n}(\overline{\mathcal{R}}_{e,r})) = \begin{cases} Alt_k(\overline{\mathcal{R}}_{e,r}) & \text{if } p = 2; \\ Sym_k(\overline{\mathcal{R}}_{e,r}) & \text{if } p \text{ is odd.} \end{cases}$$

Proof. It follows from Lemma 3.1 of Betty *et al.* [12]. □

Now in the following section, we will discuss algebraic structures of linear codes over the chain ring $\mathcal{R}_{e,r}$ and their dual codes.

2.2 Linear codes over finite commutative chain rings

Let n be a positive integer, and let $\mathcal{R}_{e,r}^n$ be the set of all n-tuples over $\mathcal{R}_{e,r}$. The set $\mathcal{R}_{e,r}^n$ can be viewed as an $\mathcal{R}_{e,r}$-module under the component-wise addition and the component-wise scalar multiplication. A linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$ is defined as an $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,r}^n$. The code $\mathcal{C}$ is called a free code if it is a free $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,r}^n$. Elements of the code $\mathcal{C}$ are called codewords. The number of codewords in the code $\mathcal{C}$ is called the size of the code $\mathcal{C}$.

Now let us define a map $d_H : \mathcal{R}_{e,r}^n \times \mathcal{R}_{e,r}^n \to \mathbb{N} \cup \{0\}$ as

$$d_H(a, b) = |\{i : 1 \leq i \leq n, a_i \neq b_i\}|$$

for all $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in \mathcal{R}_{e,r}^n$. For all $a, b \in \mathcal{R}_{e,r}^n$, it is easy to see that $d_H(a, b) \geq 0$, and that $d_H(a, b) = 0$ if and only if $a = b$. Further, $d_H(a, b) = d_H(b, a)$ and $d_H(a, b) \leq d_H(a, c) + d_H(c, b)$ for all $a, b, c \in \mathcal{R}_{e,r}^n$. Thus the map d_H is a metric on $\mathcal{R}_{e,r}^n$ and is called the Hamming distance on $\mathcal{R}_{e,r}^n$.

Next, let $\mathcal{C}$ be a linear code of length n over $\mathcal{R}_{e,r}$. The Hamming distance of the code $\mathcal{C}$, denoted by $d_H(\mathcal{C})$, is defined as the smallest of the Hamming distances between pairs of its distinct codewords. The following theorem states the well-known Singleton bound for linear codes over $\mathcal{R}_{e,r}$.

Theorem 2.2.1. *(Singleton bound) If $\mathcal{C}$ is a linear code of length n over $\mathcal{R}_{e,r}$, then we have*

$$|\mathcal{C}| \leq |\mathcal{R}_{e,r}|^{n-d_H(\mathcal{C})+1}.$$

A linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$ is said to be maximum distance separable (MDS) if it satisfies $|\mathcal{C}| = |\mathcal{R}_{e,r}|^{n-d_H(\mathcal{C})+1}$.

A generator matrix for a linear code $\mathcal{C}$ is defined as a matrix over $\mathcal{R}_{e,r}$ whose rows form a minimal generating set of the code $\mathcal{C}$. Further, two linear codes of length n over $\mathcal{R}_{e,r}$ are said to be permutation equivalent if one code can be obtained from the other by permuting the coordinate positions only. Now the following theorem states Proposition 3.2 of Norton and Sălăgean [80].

Theorem 2.2.2. *[80, Prop. 3.2] Every linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$ is permutation equivalent to a code with a generator matrix in the standard form*

$$G = \begin{bmatrix} I_{k_1} & A_{1,1} & \cdots & A_{1,e-2} & A_{1,e-1} & A_{1,e} \\ 0 & uI_{k_2} & \cdots & uA_{2,e-2} & uA_{2,e-1} & uA_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & u^{e-2}I_{k_{e-1}} & u^{e-2}A_{e-1,e-1} & u^{e-2}A_{e-1,e} \\ 0 & 0 & \cdots & 0 & u^{e-1}I_{k_e} & u^{e-1}A_{e,e} \end{bmatrix} = \begin{bmatrix} T_1 \\ uT_2 \\ \vdots \\ u^{e-2}T_{e-1} \\ u^{e-1}T_e \end{bmatrix}, \quad (2.2.1)$$

where the columns are grouped into blocks of sizes $k_1,\ k_2,\ \ldots,\ k_{e-1},\ k_e,\ k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$, the matrix I_{k_i} is the $k_i \times\ k_i$ identity matrix over $\mathcal{R}_{e,r}$ and the matrix $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{R}_{e,r})$ is considered modulo u^{j-i+1} for $1 \leq i \leq j \leq e$, i.e., the matrix $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{R}_{e,r})$ is of the form $A_{i,j} = A_{i,j}^{(0)} + A_{i,j}^{(1)}u + \cdots + A_{i,j}^{(j-i)}u^{j-i}$ with the matrices $A_{i,j}^{(0)},\ A_{i,j}^{(1)}, \ldots, A_{i,j}^{(j-i)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_{e,r})$ for $1 \leq i \leq j \leq e$.

A linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$ is said to be of the type $\{k_1, k_2, k_3, \ldots, k_e\}$ if it is permutation equivalent to a code whose generator matrix in standard form is of the type (2.2.1). By Theorem 3.5 of Norton and Sălăgean [80], we observe that the code $\mathcal{C}$ of the type $\{k_1, k_2, k_3, \ldots, k_e\}$ contains $(p^r)^{\sum\limits_{i=1}^{e}(e-i+1)k_i}$ codewords. Throughout this thesis, we will denote a linear code $\mathcal{C}$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ with a generator matrix G by $\mathcal{C} = \mathcal{R}_{e,r}^{k_1+k_2+\cdots+k_e}G$ for our convenience. The integer $k = k_1 + k_2 + \cdots + k_e$ is called the rank of the code $\mathcal{C}$. Samei and Mahmoudi [88] derived an upper bound on the Hamming distance of a linear code over $\mathcal{R}_{e,r}$ in terms of its rank, which we state in the following theorem.

Theorem 2.2.3. *[88, Th. 3.7] If $\mathcal{C}$ is a linear code of length n and rank k over $\mathcal{R}_{e,r}$, then we have*

$$d_H(\mathcal{C}) \leq n - k + 1.$$

A linear code $\mathcal{C}$ of length n and rank k over $\mathcal{R}_{e,r}$ is said to be maximum distance with respect to rank (MDR) if it satisfies $d_H(\mathcal{C}) = n - k + 1$.

Now two linear codes $\mathcal{C}$ and $\mathcal{D}$ of length n over $\mathcal{R}_{e,r}$ are said to be monomially equivalent if one code can be obtained from the other by a combination of operations of the following two types:

A. Permutation of the n coordinate positions of the code.

B. Multiplication of the code symbols appearing in a given coordinate position by the units in the ring $\mathcal{R}_{e,r}$.

Otherwise, the codes $\mathcal{C}$ and $\mathcal{D}$ are said to be monomially inequivalent. One can easily see that all monomially equivalent linear codes over $\mathcal{R}_{e,r}$ have the same size, rank and Hamming distance.

For $a = (a_1, a_2, \ldots, a_n) \in \mathcal{R}_{e,r}^n$, let us define $\bar{a} \in \overline{\mathcal{R}}_{e,r}^n$ as $\bar{a} = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n)$. Now given a linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$, the *i-th* Torsion code of $\mathcal{C}$ is defined as

$$Tor_i(\mathcal{C}) = \{\bar{a} \in \overline{\mathcal{R}}_{e,r}^n : u^{i-1}a' \in \mathcal{C} \text{ for some } a' \in \mathcal{R}_{e,r}^n \text{ satisfying } \overline{a'} = \bar{a}\}$$

for $1 \leq i \leq e$. It is easy to see that the *i-th* Torsion code $Tor_i(\mathcal{C})$ is a linear code of length n over $\overline{\mathcal{R}}_{e,r}$ for each i. By Lemma 3.4 of Norton and Sălăgean [80], we note that if the code $\mathcal{C}$ has a generator matrix G in the standard form (2.2.1), then the *i-th* Torsion code $Tor_i(\mathcal{C})$ of the code $\mathcal{C}$ has dimension $k_1 + k_2 + \cdots + k_i$ over $\overline{\mathcal{R}}_{e,r}$ and has a generator matrix

$$\begin{bmatrix} I_{k_1} & \overline{A}_{1,1} & \overline{A}_{1,2} & \cdots & \overline{A}_{1,i-1} & \cdots & \overline{A}_{1,e-1} & \overline{A}_{1,e} \\ 0 & I_{k_2} & \overline{A}_{2,2} & \cdots & \overline{A}_{2,i-1} & \cdots & \overline{A}_{2,e-1} & \overline{A}_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_i} & \cdots & \overline{A}_{i,e-1} & \overline{A}_{i,e} \end{bmatrix}, \tag{2.2.2}$$

(throughout this thesis, if $\mathcal{A}$ is a $g \times h$ matrix over $\mathcal{R}_{e,r}$ with the (i,j)-th entry as $a_{i,j}$, then $\overline{\mathcal{A}}$ is a $g \times h$ matrix over $\overline{\mathcal{R}}_{e,r}$ whose (i,j)-th entry is $\bar{a}_{i,j}$ for each i and j). It is easy to see that

$$Tor_i(\mathcal{C}) \subseteq Tor_{i+1}(\mathcal{C})$$

for $1 \leq i \leq e-1$ and that

$$|\mathcal{C}| = \prod_{i=1}^{e} |Tor_i(\mathcal{C})|.$$

Next, the Euclidean bilinear form on $\mathcal{R}_{e,r}^n$ is a mapping $\cdot : \mathcal{R}_{e,r}^n \times \mathcal{R}_{e,r}^n \to \mathcal{R}_{e,r}$, defined as

$$a \cdot b = a_1b_1 + a_2b_2 + \cdots + a_nb_n$$

for all $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ in $\mathcal{R}_{e,r}^n$. It is easy to observe that the map $\cdot$ is a non-degenerate and symmetric bilinear form on $\mathcal{R}_{e,r}^n$. Now the (Euclidean) dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$ is defined as

$$\mathcal{C}^\perp = \{y \in \mathcal{R}_{e,r}^n \ : \ z \cdot y = 0 \text{ for all } z \in \mathcal{C}\}.$$

Note that the dual code $\mathcal{C}^\perp$ is also a linear code of length n over $\mathcal{R}_{e,r}$. By Theorem 3.10 of Norton and Sălăgean [80], we see that if the code $\mathcal{C}$ is of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$, then its dual code $\mathcal{C}^\perp$ is of the type $\{n - (k_1 + k_2 + \cdots + k_e), k_e, k_{e-1}, \ldots, k_2\}$. Further, the code $\mathcal{C}$ is said to be (i) self-orthogonal if it satisfies $\mathcal{C} \subseteq \mathcal{C}^\perp$, (ii) self-dual if it satisfies $\mathcal{C} = \mathcal{C}^\perp$ and (iii) linear code with complementary dual (or an LCD code) if it satisfies $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$.

Next, one can easily observe that the Euclidean bilinear form $\cdot$ on $\mathcal{R}_{e,r}^n$ induces the map $\cdot : \overline{\mathcal{R}}_{e,r}^n \times \overline{\mathcal{R}}_{e,r}^n \to \overline{\mathcal{R}}_{e,r}$, defined as

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n$$

for all $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ in $\overline{\mathcal{R}}_{e,r}^n$. Note that the map $\cdot$ is a non-degenerate and symmetric bilinear form on $\overline{\mathcal{R}}_{e,r}^n$. Further, if $\mathcal{D}$ is a linear code of length n over $\overline{\mathcal{R}}_{e,r}$, then its dual code $\mathcal{D}^\perp$ is defined as

$$\mathcal{D}^\perp = \{\beta \in \overline{\mathcal{R}}_{e,r}^n : \alpha \cdot \beta = 0 \text{ for all } \alpha \in \mathcal{D}\}.$$

Note that $\mathcal{D}^\perp$ is also a linear code of length n over $\overline{\mathcal{R}}_{e,r}$. Now the following theorem provides a necessary and sufficient condition under which a linear code of length n over $\mathcal{R}_{e,r}$ is self-orthogonal or self-dual.

Theorem 2.2.4. *Let $n \geq 1, e \geq 2$ be integers, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$. Let $\mathcal{C}$ be a linear code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ with a generator matrix G as defined by (2.2.1). The following hold.*

(a) The code $\mathcal{C}$ is self-orthogonal if and only if

$$T_iT_j^t \equiv 0 \pmod{u^{e-i-j+2}} \quad \text{for } 1 \leq i \leq j \leq e \text{ and } i + j \leq e + 1. \tag{2.2.3}$$

(b) A self-orthogonal code $\mathcal{C}$ is self-dual if and only if $k_j = k_{e-j+2}$ for $1 \leq j \leq e$.

Proof. Its proof is a straightforward exercise. □

Now the following lemma relates the Torsion codes of a self-orthogonal code over $\mathcal{R}_{e,r}$.

Lemma 2.2.1. *[38] Let $\mathcal{C}$ be a self-orthogonal code of length n over $\mathcal{R}_{e,r}$. The following hold.*

(a) $Tor_i(\mathcal{C}) \subseteq Tor_i(\mathcal{C})^{\perp}$ for $1 \leq i \leq \lfloor \frac{e+1}{2} \rfloor$.

(b) $Tor_i(\mathcal{C}) \subseteq Tor_{e-i+1}(\mathcal{C})^{\perp}$ for $\lfloor \frac{e+1}{2} \rfloor + 1 \leq i \leq e$.

In particular, if $\mathcal{C}$ is a self-dual code of length n over $\mathcal{R}_{e,r}$, then

$$Tor_i(\mathcal{C}) = Tor_{e-i+1}(\mathcal{C})^{\perp}$$

for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$.

Proof. (a) Part (a) follows from Lemma 5.1 of Dougherty *et al.* [38].

(b) Next, let $\lfloor \frac{e+1}{2} \rfloor + 1 \leq i \leq e$ be fixed, and let $c' \in Tor_i(\mathcal{C})$ and $y' \in Tor_{e-i+1}(\mathcal{C})$. Then there exist $c, y \in \mathcal{R}_{e,r}^n$ such that $\bar{c} = c'$, $\bar{y} = y'$ and $u^{i-1}c, u^{e-i}y \in \mathcal{C}$. Since $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, we have $u^{e-i}y \cdot u^{i-1}c = 0$ for all $y \in \mathcal{R}_{e,r}^n$ satisfying $\bar{y} = y' \in Tor_{e-i+1}(\mathcal{C})$. This implies that $\bar{y} \cdot \bar{c} = 0$ for all $\bar{y} \in Tor_{e-i+1}(\mathcal{C})$, which further implies that $c' = \bar{c} \in Tor_{e-i+1}(\mathcal{C})^{\perp}$. This shows that $Tor_i(\mathcal{C}) \subseteq Tor_{e-i+1}(\mathcal{C})^{\perp}$.

In particular, if $\mathcal{C}$ is a self-dual code of length n over $\mathcal{R}_{e,r}$, then one can easily observe that $|Tor_i(\mathcal{C})| = |Tor_{e-i+1}(\mathcal{C})^{\perp}|$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. From this and by part (b), we get $Tor_i(\mathcal{C}) = Tor_{e-i+1}(\mathcal{C})^{\perp}$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. □

From the above discussion, we deduce the following:

Remark 2.2.1. *If $\mathcal{C}$ is a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$, then we have $2k_1+2k_2+\cdots+2k_{e-i+1}+k_{e-i+2}+k_{e-i+3}+\cdots+k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. From this, it follows that $n \geq 2(k_1 + k_2 + \cdots + k_{\frac{e}{2}}) + k_{\frac{e}{2}+1}$ if e is even, while $n \geq 2(k_1 + k_2 + \cdots + k_{\frac{e+1}{2}})$ if e is odd.*

In particular, if $\mathcal{C}$ is a self-dual code of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$, then we have $k_i = k_{e-i+2}$ for $1 \leq i \leq e$. From this, it follows that $n = 2(k_1 + k_2 + \cdots + k_{\frac{e}{2}}) + k_{\frac{e}{2}+1}$ if e is even, while $n = 2(k_1 + k_2 + \cdots + k_{\frac{e+1}{2}})$ if e is odd.

In the following section, we will present some basic definitions and results from groups and geometry, which are needed to count all self-orthogonal, self-dual, and LCD codes over $\mathcal{R}_{e,r}$.

2.3 Some basic results from groups and geometry

Let V be a finite-dimensional vector space over the finite field $\mathbb{F}_q$, and let π be an automorphism of $\mathbb{F}_q$. A map $\mathcal{B} : V \times V \to \mathbb{F}_q$ is called a π-sesquilinear form on V if it satisfies the following four properties:

(i) $\mathcal{B}(a + b, c) = \mathcal{B}(a, c) + \mathcal{B}(b, c)$ for all $a, b, c \in V$.

(ii) $\mathcal{B}(\alpha a, b) = \alpha\mathcal{B}(a, b)$ for all $\alpha \in \mathbb{F}_q$ and $a, b \in V$.

(iii) $\mathcal{B}(a, b + c) = \mathcal{B}(a, b) + \mathcal{B}(a, c)$ for all $a, b, c \in V$.

(iv) $\mathcal{B}(a, \alpha b) = \pi(\alpha)\mathcal{B}(a, b)$ for all $\alpha \in \mathbb{F}_q$ and $a, b \in V$.

In particular, when π is the identity automorphism of $\mathbb{F}_q$, the π-sesquilinear form $\mathcal{B}$ is called a bilinear form on V. The π-sesquilinear form $\mathcal{B}$ on V is said to be

- left non-degenerate if there exists $a \in V$ such that $\mathcal{B}(a, b) = 0$ for all $b \in V$, then $a = 0$.
- right non-degenerate if there exists $b \in V$ such that $\mathcal{B}(a, b) = 0$ for all $a \in V$, then $b = 0$.
- reflexive if there exist $a, b \in V$ such that $\mathcal{B}(a, b) = 0$, then $\mathcal{B}(b, a) = 0$.
- alternating if π is the identity automorphism of $\mathbb{F}_q$ and $\mathcal{B}(a, a) = 0$ for all $a \in V$.

- Hermitian if π is the automorphism of $\mathbb{F}_q$ of order 2 and $\mathcal{B}(a,b) = \pi(\mathcal{B}(b,a))$ for all $a, b \in V$.
- symmetric if π is the identity automorphism of $\mathbb{F}_q$ and $\mathcal{B}(a,b) = \mathcal{B}(b,a)$ for all $a, b \in V$.

Note that a symmetric or a Hermitian π-sesquilinear form on V is also reflexive. If $\mathcal{B}$ is a reflexive π-sesquilinear form on V, then $\mathcal{B}$ is left non-degenerate on V if and only if $\mathcal{B}$ is right non-degenerate on V, which we will simply refer to as a non-degenerate π-sesquilinear form on V.

Now a formed space over $\mathbb{F}_q$ is defined as a pair $(V, \mathcal{B})$, where V is a finite-dimensional vector space over $\mathbb{F}_q$ and $\mathcal{B}$ is a π-sesquilinear form on V. The formed space $(V, \mathcal{B})$ is said to be left (*resp.* right) non-degenerate if $\mathcal{B}$ is a left (*resp.* right) non-degenerate π-sesquilinear form on V. The formed space $(V, \mathcal{B})$ is said to be reflexive if $\mathcal{B}$ is a reflexive π-sesquilinear form on V. The dimension of the formed space $(V, \mathcal{B})$ is defined as the dimension of V as a vector space over $\mathbb{F}_q$, which is denoted by $\dim_{\mathbb{F}_q}(V)$. Further, the Gram matrix of an n-dimensional formed space $(V, \mathcal{B})$ with respect to the ordered basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of V, denoted by $\mathfrak{G}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, is defined as an $n \times n$ matrix over $\mathbb{F}_q$, whose (i,j)-th entry is the element $\mathcal{B}(\alpha_i, \alpha_j)$ for $1 \leq i, j \leq n$. By Theorem 24 of [40, Ch. 11], we see that the determinant of the Gram matrix $\mathfrak{G}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ can be expressed as

$$\det(\mathfrak{G}(\alpha_1, \alpha_2, \ldots, \alpha_n)) = \sum_{\pi' \in \mathscr{S}_n} sgn(\pi')\mathcal{B}(\alpha_1, \alpha_{\pi'(1)})\mathcal{B}(\alpha_2, \alpha_{\pi'(2)}) \cdots \mathcal{B}(\alpha_n, \alpha_{\pi'(n)}),$$

where $\mathscr{S}_n$ is the symmetric group of $\{1, 2, \ldots, n\}$ and the function $sgn : \mathscr{S}_n \to \{1, -1\}$ is called the signum function and is defined as

$$sgn(\pi') = \begin{cases} 1 & \text{if } \pi' \text{ is an even permutation in } \mathscr{S}_n; \\ -1 & \text{if } \pi' \text{ is an odd permutation in } \mathscr{S}_n. \end{cases}$$

Now the following theorem provides a characterization of a non-degenerate formed space in terms of its Gram matrix.

Theorem 2.3.1. *[95, Th. 5.1.1] Let $(V, \mathcal{B})$ be an n-dimensional formed space over $\mathbb{F}_q$ with an ordered basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. The formed space $(V, \mathcal{B})$ is left (resp.*

right) non-degenerate if and only if the Gram matrix $\mathfrak{G}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *of* $(V, \mathcal{B})$ *is non-singular.*

Next, the formed space $(V, \mathcal{B})$ is called

- a symplectic space if π is the identity automorphism of $\mathbb{F}_q$ and $\mathcal{B}$ is an alternating, reflexive and non-degenerate bilinear form on V.
- a unitary space if π is the automorphism of $\mathbb{F}_q$ of order 2 and $\mathcal{B}$ is a Hermitian (and hence reflexive) and non-degenerate π-sesquilinear form on V.
- an orthogonal space (or a finite geometry) if π is the identity automorphism of $\mathbb{F}_q$ and $\mathcal{B}$ is a symmetric (and hence reflexive) and non-degenerate bilinear form on V.

A formed space $(U, \mathcal{B}_U)$ is said to be a subspace of the formed space $(V, \mathcal{B})$ if U is a subspace of V and $\mathcal{B}_U = \mathcal{B} \restriction_{U \times U}$. A subspace $(U, \mathcal{B}_U)$ of the formed space $(V, \mathcal{B})$ is said to be non-degenerate if the π-sesquilinear form $\mathcal{B}_U$ is non-degenerate, (or equivalently, if the π-sesquilinear form $\mathcal{B}$ is non-degenerate on U). A direct sum $V = U_1 \oplus U_2$ of two subspaces U_1 and U_2 of $(V, \mathcal{B})$ is said to be an orthogonal direct sum of U_1 and U_2, written as $V = U_1 \perp U_2$, if $\mathcal{B}(v_1, v_2) = 0$ for all $v_1 \in U_1$ and $v_2 \in U_2$. If U is a subspace of the formed space $(V, \mathcal{B})$, then its orthogonal complement

$$U^\perp = \{a \in V : \mathcal{B}(a, b) = 0 \text{ for all } b \in U\}$$

is also a subspace of the formed space $(V, \mathcal{B})$. In fact, the following hold.

Theorem 2.3.2. *[49, Prop. 2.4] Let* $(V, \mathcal{B})$ *be a finite-dimensional reflexive and non-degenerate formed space over* $\mathbb{F}_q$. *If* U *is a subspace of the formed space* $(V, \mathcal{B})$, *then its orthogonal complement*

$$U^\perp = \{v_2 \in V : \mathcal{B}(v_2, v_1) = 0 \textit{ for all } v_1 \in U\}$$

is also a subspace of the formed space $(V, \mathcal{B})$ *and*

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

Furthermore, if the formed space $(U, \mathcal{B} \restriction_{U \times U})$ is non-degenerate, then we have

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

Let $(V, \mathcal{B})$ be a reflexive and non-degenerate formed space over $\mathbb{F}_q$. A non-zero vector $v \in V$ is said to be isotropic if it satisfies $\mathcal{B}(v, v) = 0$, while a vector $v \in V$ is said to be anisotropic if it satisfies $\mathcal{B}(v, v) \neq 0$. A subspace W of $(V, \mathcal{B})$ is said to be totally isotropic if it satisfies $W \subseteq W^{\perp}$. By Theorem 2.3.2, we see that the dimension of a totally isotropic subspace of $(V, \mathcal{B})$ is at most $\frac{1}{2} \dim_{\mathbb{F}_q}(V)$. Further, by Theorem 7.4 of [99], we note that all maximal totally isotropic subspaces of $(V, \mathcal{B})$ have the same dimension. The dimension ν of a maximal totally isotropic subspace of V is called the Witt index of V. A subspace U of V is said to be anisotropic if it has no isotropic vector. A pair (w_1, w_2) of isotropic vectors in the formed space $(V, \mathcal{B})$ is called a hyperbolic pair if it satisfies $\mathcal{B}(w_1, w_2) = 1$. If (w_1, w_2) is a hyperbolic pair in the formed space $(V, \mathcal{B})$, then the vectors w_1 and w_2 are linearly independent over $\mathbb{F}_q$ and the subspace $\langle w_1, w_2 \rangle$ of $(V, \mathcal{B})$ with the basis set $\{w_1, w_2\}$ over $\mathbb{F}_q$ is called a hyperbolic line.

The following theorem states some basic properties of finite-dimensional symplectic spaces over finite fields.

Theorem 2.3.3. *[99, pp. 69-70] Let $(V, \mathcal{B})$ be an n-dimensional symplectic space over $\mathbb{F}_q$. Then the dimension n of V is even and the following hold.*

(a) The Witt index of the space $(V, \mathcal{B})$ is $\frac{n}{2}$.

(b) The space $(V, \mathcal{B})$ admits a Witt decomposition of the form

$$V = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\frac{n}{2}}, b_{\frac{n}{2}} \rangle,$$

where $(a_1, b_1), (a_2, b_2), \ldots, (a_{\frac{n}{2}}, b_{\frac{n}{2}})$ are hyperbolic pairs in V.

(c) The number $\mathcal{I}_{\frac{n}{2},0}$ of isotropic vectors in V is given by $\mathcal{I}_{\frac{n}{2},0} = q^n - 1$.

(d) The number $\mathcal{H}_{\frac{n}{2},0}$ of hyperbolic pairs in V is given by $\mathcal{H}_{\frac{n}{2},0} = q^{n-1}(q^n - 1)$.

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

$$\prod_{i=0}^{k-1}\left(\frac{q^{n-2i}-1}{q^{i+1}-1}\right).$$

The following theorem states some basic properties of finite-dimensional unitary spaces over finite fields.

Theorem 2.3.4. *[99, pp. 116-117] Let $(V, \mathcal{B})$ be an n-dimensional unitary space over $\mathbb{F}_{q^2}$. Let ν be the Witt index of $(V, \mathcal{B})$. Then the following hold.*

(a) The Witt index ν of the space $(V, \mathcal{B})$ is given by

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

(b) The space $(V, \mathcal{B})$ admits a Witt decomposition of the form

$$V = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_\nu, b_\nu\rangle \perp W,$$

where $(a_1, b_1), (a_2, b_2), \ldots, (a_\nu, b_\nu)$ are hyperbolic pairs in V and W is an anisotropic subspace of V having dimension $n - 2\nu \leq 1$.

(c) When $n \geq 2$, the unitary space $(V, \mathcal{B})$ contains an isotropic vector, and the total number $\mathcal{I}_{\nu,n-2\nu}$ of isotropic vectors in V is given by

$$\mathcal{I}_{\nu,n-2\nu} = (q^{n-1} - (-1)^{n-1})(q^n - (-1)^n).$$

(d) When $n \geq 2$, the number $\mathcal{H}_{\nu,n-2\nu}$ of hyperbolic pairs in V is given by

$$\mathcal{H}_{\nu,n-2\nu} = q^{2n-3}(q^{n-1} - (-1)^{n-1})(q^n - (-1)^n).$$

We next proceed to recall some basic results on the geometry of quadratic spaces over finite fields. A quadratic form on V is defined as a mapping $\mathrm{Q} : V \to \mathbb{F}_q$ satisfying the following two properties:

(i) $\mathrm{Q}(\alpha v) = \alpha^2 \mathrm{Q}(v)$ for all $\alpha \in \mathbb{F}_q$ and $v \in V$.

(ii) The map $B_{\mathrm{Q}} : V \times V \to \mathbb{F}_q$, defined as

$$B_{\mathrm{Q}}(v_1, v_2) = \mathrm{Q}(v_1 + v_2) - \mathrm{Q}(v_1) - \mathrm{Q}(v_2) \quad \text{for all} \quad v_1, v_2 \in V,$$

is a symmetric bilinear form on V.

The pair (V, Q) is called a quadratic space over $\mathbb{F}_q$ with the associated symmetric bilinear form B_{Q}. The quadratic space (V, Q) over $\mathbb{F}_q$ is said to be non-degenerate if it satisfies $\mathrm{Q}^{-1}(0) \cap V^{\perp_{B_{\mathrm{Q}}}} = \{0\}$, where $Q^{-1}(0) = \{v \in V : Q(v) = 0\}$ and $V^{\perp_{B_{\mathrm{Q}}}} = \{w \in V : B_{\mathrm{Q}}(v, w) = 0 \text{ for all } v \in V\}$. Further, a non-zero vector v in the quadratic space (V, Q) is said to be singular if it satisfies $\mathrm{Q}(v) = 0$. A subspace of (V, Q) is defined as a pair (W, Q_W), where W is a subspace of V and $\mathrm{Q}_W = \mathrm{Q} \restriction_W$.

Next, two quadratic spaces $(V_1, \mathcal{Q}_1)$ and $(V_2, \mathcal{Q}_2)$ are said to be isometric if there exists a vector space isomorphism $\tau : V_1 \to V_2$ satisfying $\mathcal{Q}_2(\tau(v)) = \mathcal{Q}_1(v)$ for all $v \in V_1$. We next state the Witt's Cancellation Theorem for quadratic spaces over finite fields of odd characteristic.

Theorem 2.3.5. *[49, Th. 5.1](Witt's Cancellation Theorem). Let q be an odd prime power. If U and W are two non-degenerate isometric subspaces of a quadratic space (V, Q) over $\mathbb{F}_q$, then the subspaces $U^{\perp_{B_{\mathrm{Q}}}}$ and $W^{\perp_{B_{\mathrm{Q}}}}$ are also isometric.*

A subspace W of (V, Q) is said to be totally singular if $\mathrm{Q}(w) = 0$ for all $w \in W$. By Corollaries 5.3 and 12.11 of [49], we note that all maximal totally singular subspaces of (V, Q) have the same dimension. The dimension of a maximal totally singular subspace of V is called the Witt index of (V, Q). Further, a subspace U of (V, Q) is said to be non-singular if it has no singular vector. A hyperbolic pair in (V, Q) is defined as a pair (v_1, v_2) of singular vectors $v_1, v_2 \in V$ satisfying $B_{\mathrm{Q}}(v_1, v_2) = 1$. One can easily see that if (v_1, v_2) is a hyperbolic pair in (V, Q), then the vectors v_1 and v_2 are linearly independent over $\mathbb{F}_q$ and the subspace $\langle v_1, v_2 \rangle$ of (V, Q) with the basis set $\{v_1, v_2\}$ is called a hyperbolic line in (V, Q). Further, we have the following:

Proposition 2.3.1. *[49, Prop. 12.1] If there exists a singular vector in a non-degenerate quadratic space (V, Q) of dimension at least 2, then there exists a hyperbolic pair in (V, Q).*

Now let q be an odd prime power. Here with every symmetric bilinear form $\mathfrak{B} : V \times V \to \mathbb{F}_q$, one can associate the quadratic map $\mathfrak{Q}_{\mathfrak{B}} : V \to \mathbb{F}_q$, defined as

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

It is easy to see that the quadratic space $(V, \mathfrak{Q}_{\mathfrak{B}})$ is non-degenerate if and only if the bilinear form $\mathfrak{B}$ is non-degenerate. Therefore when q is an odd prime power, one can associate a non-degenerate quadratic space over $\mathbb{F}_q$ with every orthogonal space over $\mathbb{F}_q$, and vice versa. Now the following theorem states some basic properties of finite-dimensional non-degenerate quadratic spaces over a finite field of odd characteristic.

Theorem 2.3.6. *[99, pp. 138-141] Let q be an odd prime power, and let (V, Q) be an n-dimensional non-degenerate quadratic space over $\mathbb{F}_q$. Let ν be the Witt index of (V, Q). Then the following hold.*

(a) The Witt index ν of the quadratic space (V, Q) is given by

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

(b) The space (V, Q) admits a Witt decomposition of the form

$$V = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_\nu, b_\nu \rangle \perp W,$$

where $(a_1, b_1), (a_2, b_2), \ldots, (a_\nu, b_\nu)$ are hyperbolic pairs in V and W is an anisotropic subspace of V having dimension $n-2\nu \leq 2$. (The corresponding basis $\{a_1, b_1, a_2, b_2, \ldots, a_\nu, b_\nu\} \cup \mathfrak{A}_W$ with $\mathfrak{A}_W$ as a basis of W is called a quadratic basis of V.)

(c) When $n \geq 3$, the quadratic space (V, Q) contains a singular vector and the total number $\mathcal{I}_{\nu,n-2\nu}$ of singular vectors in V is given by

$$\mathcal{I}_{\nu,n-2\nu} = (q^\nu - 1)(q^{n-\nu-1} + 1).$$

(d) The number $\mathcal{H}_{\nu,n-2\nu}$ *of hyperbolic pairs in* V *is given by*

$$\mathcal{H}_{\nu,n-2\nu} = q^{n-2}(q^{\nu}-1)(q^{n-\nu-1}+1).$$

Next, let q be an even prime power. Here if Q is a quadratic form on V, then the associated symmetric bilinear form B_{Q} on V satisfies $B_{\mathrm{Q}}(v,v)=0$ for all $v \in V$, *i.e.*, B_{Q} is an alternating form on V. Here the quadratic form Q can not be uniquely determined in terms of B_{Q}. Further, the quadratic space (V, Q) over $\mathbb{F}_q$ is said to be non-defective if it satisfies $V \cap V^{\perp_{B_{\mathrm{Q}}}} = \{0\}$. Otherwise, the quadratic space (V,Q) over $\mathbb{F}_q$ is said to be defective. Now the following theorem states some basic properties of finite-dimensional non-degenerate quadratic spaces over a finite field of even characteristic.

Theorem 2.3.7. *[49, Prop. 14.47] Let* q *be an even prime power, and let* (V,Q) *be an* n*-dimensional non-degenerate quadratic space over* $\mathbb{F}_q$*. Let* ν *be the Witt index of* (V,Q)*. Then the following hold.*

(a) The Witt index ν *of the quadratic space* (V,Q) *is given by*

- $\nu = \frac{n-1}{2}$ *if* n *is odd.*
- *either* $\nu = \frac{n}{2}$ *or* $\nu = \frac{n-2}{2}$ *if* n *is even.*

(b) The space (V,Q) *admits a Witt decomposition of the form*

$$V = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_\nu, b_\nu\rangle \perp W,$$

where $(a_1,b_1),(a_2,b_2),\ldots,(a_\nu,b_\nu)$ *are hyperbolic pairs in* V *and* W *is a non-singular subspace of* V *having dimension* $n-2\nu \leq 2$.

(c) The number $\mathcal{I}_{\nu,n-2\nu}$ *of singular vectors in* V *is given by*

$$\mathcal{I}_{\nu,n-2\nu} = \begin{cases} q^{n-1}-1 & \textit{if } \nu = \frac{n-1}{2}; \\ (q^{\frac{n}{2}-1}+1)(q^{\frac{n}{2}}-1) & \textit{if } \nu = \frac{n}{2}; \\ (q^{\frac{n}{2}-1}-1)(q^{\frac{n}{2}}+1) & \textit{if } \nu = \frac{n-2}{2}. \end{cases}$$

(d) The number $\mathcal{H}_{\nu,n-2\nu}$ of hyperbolic pairs in V is given by

$$\mathcal{H}_{\nu,n-2\nu} = \begin{cases} q^{n-2}(q^{n-1}-1) & \text{if } \nu = \frac{n-1}{2}; \\ q^{n-2}(q^{\frac{n}{2}}-1)(q^{\frac{n}{2}-1}+1) & \text{if } \nu = \frac{n}{2}; \\ q^{n-2}(q^{\frac{n}{2}}+1)(q^{\frac{n}{2}-1}-1) & \text{if } \nu = \frac{n-2}{2}. \end{cases}$$

We next state the Witt's Cancellation Theorem for quadratic spaces over finite fields of even characteristic.

Theorem 2.3.8. *[49, Cor. 12.12](Witt's Cancellation Theorem). Let q be an even prime power. Let (V, Q) be a non-defective quadratic space over $\mathbb{F}_q$, and let U and W be two isometric subspaces of V. Then $U^{\perp_{B_{\mathrm{Q}}}}$ and $W^{\perp_{B_{\mathrm{Q}}}}$ are also isometric.*

For more details, one may refer to [49, 99]. We next recall the following well-known result:

Theorem 2.3.9. *For an integer k satisfying $1 \leq k \leq n$ and a prime power q, the number of distinct k-dimensional subspaces of an n-dimensional vector space over the finite field $\mathbb{F}_q$ of order q is given by the Gaussian binomial coefficient*

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

(Recall that the Gaussian binomial coefficient $\begin{bmatrix} n \\ 0 \end{bmatrix}_q$ is assigned the value 1.)

We also need the following well-known result to discuss the solvability of polynomial equations of the form $x^q - x - \alpha = 0$ over $\mathbb{F}_{q^m}$.

Theorem 2.3.10. *[62, Th. 2.25] For $\alpha \in \mathbb{F}_{q^m}$ we have $Tr_{q,m}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^m}$, where $Tr_{q,m} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ denotes the trace map.*

By applying Theorems 2.3.3 and 2.3.6, Pless [83] obtained enumeration formulae for all self-orthogonal and self-dual codes over finite fields, which we present in the following section.

Enumeration formulae for self-orthogonal and self-dual codes over finite fields

Let $\mathbb{F}_q^n$ denote the n-dimensional vector space consisting of all n-tuples over $\mathbb{F}_q$. A linear code $\mathfrak{D}$ of length n and dimension k over $\mathbb{F}_q$ is defined as a k-dimensional subspace of $\mathbb{F}_q^n$. Further, the mapping $\cdot : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$, defined as

$$\alpha \cdot \beta = \alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n$$

for all $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ in $\mathbb{F}_q^n$, is a non-degenerate and symmetric bilinear form on $\mathbb{F}_q^n$ and is called the Euclidean bilinear form on $\mathbb{F}_q^n$. Thus the pair $(\mathbb{F}_q^n, \cdot)$ is an n-dimensional orthogonal space over $\mathbb{F}_q$.

Next, if $\mathfrak{D}$ is a linear code of length n over $\mathbb{F}_q$, then its dual code $\mathfrak{D}^\perp$ is defined as

$$\mathfrak{D}^\perp = \{z \in \mathbb{F}_q^n : v \cdot z = 0 \text{ for all } v \in \mathfrak{D}\},$$

i.e., the dual code $\mathfrak{D}^\perp$ is defined as the orthogonal complement of $\mathfrak{D}$ with respect to the Euclidean bilinear form $\cdot$. It is easy to see that the dual code $\mathfrak{D}^\perp$ is also a linear code of length n over $\mathbb{F}_q$. Further, the code $\mathfrak{D}$ is said to be (i) self-orthogonal if it satisfies $\mathfrak{D} \subseteq \mathfrak{D}^\perp$, (ii) self-dual if it satisfies $\mathfrak{D} = \mathfrak{D}^\perp$, and (iii) a linear code with complementary dual (or an LCD code) if it satisfies $\mathfrak{D} \cap \mathfrak{D}^\perp = \{0\}$. Next, by Theorem 2.3.2, we see that $\dim_{\mathbb{F}_q}(\mathfrak{D}) + \dim_{\mathbb{F}_q}(\mathfrak{D}^\perp) = n$. From this, it follows that if the code $\mathfrak{D}$ is self-orthogonal, then $\dim_{\mathbb{F}_q}(\mathfrak{D}) \leq \frac{n}{2}$. Further, if the code $\mathfrak{D}$ is self-dual, then n must be an even integer and $\dim_{\mathbb{F}_q}(\mathfrak{D}) = \frac{n}{2}$.

Since $(\mathbb{F}_q^n, \cdot)$ is an orthogonal space, each self-orthogonal code of length n and dimension k over $\mathbb{F}_q$ can be viewed as a k-dimensional totally isotropic $\mathbb{F}_q$-linear subspace of the orthogonal space $(\mathbb{F}_q^n, \cdot)$. When n is even, each self-dual code of length n over $\mathbb{F}_q$ (if it exists) can be viewed as an $\frac{n}{2}$-dimensional totally isotropic $\mathbb{F}_q$-linear subspace of the orthogonal space $(\mathbb{F}_q^n, \cdot)$. Therefore when n is even, there exists a self-dual code of length n over $\mathbb{F}_q$ if and only if the Witt index of the orthogonal space $(\mathbb{F}_q^n, \cdot)$ is $\frac{n}{2}$. Further, we observe that each LCD code of length n and dimension k over $\mathbb{F}_q$ can be viewed as a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of the orthogonal space $(\mathbb{F}_q^n, \cdot)$.

In particular, when q is an odd prime power, we observe that the orthogonal space $(\mathbb{F}_q^n, \cdot)$ can also be viewed as a non-degenerate quadratic space with respect to the quadratic map $\mathfrak{Q} : \mathbb{F}_q^n \to \mathbb{F}_q$, defined as

$$\mathfrak{Q}(v) = \frac{1}{2} v \cdot v \quad \text{for all} \quad v \in \mathbb{F}_q^n.$$

By making these observations and by applying Theorems 2.3.3 and 2.3.6, Pless [83] obtained explicit enumeration formulae for all self-orthogonal and self-dual codes over finite fields. To state these enumeration formulae, let $\sigma_q(n,k)$ denote the number of distinct self-orthogonal codes of length n and dimension k over $\mathbb{F}_q$, where k, n are integers satisfying $0 \leq k \leq n$. It is clear that $\sigma_q(n,0) = 1$ and $\sigma_q(n,k) = 0$ for all integers $k > \frac{n}{2}$. Now the following theorem provides the explicit value of the number $\sigma_q(n,k)$ for $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$.

Theorem 2.3.11. *[83, Th. 2] For an integer k satisfying $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ and a prime power q, we have*

$$\sigma_q(n,k) = \begin{cases} \dfrac{\prod\limits_{i=0}^{k-1} (q^{n-1-2i} - 1)}{\prod\limits_{j=1}^{k} (q^j - 1)} & \textit{if } n \textit{ is odd;} \\[3ex] \dfrac{(q^{n-k} - q^{\frac{n}{2}-k} + q^{\frac{n}{2}} - 1) \prod\limits_{i=1}^{k-1} (q^{n-2i} - 1)}{\prod\limits_{j=1}^{k} (q^j - 1)} & \textit{if } n \textit{ is even, } q \textit{ is odd and} \\ & (-1)^{\frac{n}{2}} \textit{ is a square in } \mathbb{F}_q; \\[3ex] \dfrac{(q^{n-k} + q^{\frac{n}{2}-k} - q^{\frac{n}{2}} - 1) \prod\limits_{i=1}^{k-1} (q^{n-2i} - 1)}{\prod\limits_{j=1}^{k} (q^j - 1)} & \textit{if } n \textit{ is even, } q \textit{ is odd and} \\ & (-1)^{\frac{n}{2}} \textit{ is not a square in } \mathbb{F}_q; \\[3ex] \dfrac{(q^{n-k} - 1) \prod\limits_{i=1}^{k-1} (q^{n-2i} - 1)}{\prod\limits_{j=1}^{k} (q^j - 1)} & \textit{if both } n \textit{ and } q \textit{ are even.} \end{cases}$$

On considering the case when n is even and on taking $k = \frac{n}{2}$ in the above theorem, Pless [83] obtained the enumeration formula $\sigma_q(n, \frac{n}{2})$ for all self-dual codes of length n over $\mathbb{F}_q$, which we present in the following theorem.

Theorem 2.3.12. *If there exists a self-dual code of length n over $\mathbb{F}_q$, then the integer n must be even. Further, for an even integer n, the number of self-dual codes of length n over $\mathbb{F}_q$ is given by*

$$\sigma_q\left(n, \frac{n}{2}\right) = \begin{cases} \prod\limits_{i=1}^{\frac{n}{2}-1} (q^i + 1) & \text{if } q \text{ is even;} \\ 2\prod\limits_{i=1}^{\frac{n}{2}-1} (q^i + 1) & \text{if } q \text{ is odd and } (-1)^{\frac{n}{2}} \text{ is a square in } \mathbb{F}_q; \\ 0 & \text{otherwise.} \end{cases}$$

As a consequence, there exists a self-dual code of length n over $\mathbb{F}_q$ if and only if either q is even or q is odd and $(-1)^{\frac{n}{2}}$ is a square in $\mathbb{F}_q$.

In Chapters 3 and 4, we will apply Theorems 2.3.11 and 2.3.12 to count all self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,r}$. From now on, throughout this thesis, we will follow the same notations as in Chapter 2.

3

Enumeration formulae for self-orthogonal and self-dual codes over finite commutative chain rings of odd characteristic

3.1 Introduction

In this chapter, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings of odd characteristic. With the help of these enumeration formulae, we classify all self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over the chain ring $\mathbb{F}_5[u]/\langle u^2\rangle$ and of lengths $2, 3$ and 4 over the chain ring $\mathbb{F}_7[u]/\langle u^2\rangle$. For this, we recall, from Chapter 2, that $\mathcal{R}_{e,r}$ is a finite commutative chain ring with the maximal ideal $\langle u\rangle$ of nilpotency index $e \geq 2$ and the residue field $\overline{\mathcal{R}}_{e,r}$ of order p^r, where p is a prime and r is a positive integer. The set $\mathcal{T}_{e,r} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is the Teichm$\ddot{u}$ller set of the chain ring $\mathcal{R}_{e,r}$. We assume, throughout this chapter, that the characteristic of the chain ring $\mathcal{R}_{e,r}$ is odd, which, by Theorem 2.1.4, holds if and only if p is an odd prime.

This chapter is organized as follows: In Section 3.2, we consider the case $e = 2$ and count all self-orthogonal and self-dual codes of an arbitrary length n over the chain ring $\mathcal{R}_{2,r}$ (Theorems 3.2.3 and 3.2.5). In Section 3.3, we consider the case $e = 3$ and obtain enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length n over the chain ring $\mathcal{R}_{3,r}$ (Theorems 3.3.3 and 3.3.5). In Section 3.4, we first derive a recurrence relation between the enumeration formula for self-orthogonal (*resp.* self-dual) codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ and the enumeration formula for self-orthogonal (*resp.* self-dual) codes of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and of the same length n over $\mathcal{R}_{e-2,r}$ by providing a recursive method to construct a self-orthogonal (*resp.* self-dual) code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ from a self-orthogonal (*resp.* self-dual) code of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and of the same length n over $\mathcal{R}_{e-2,r}$ and vice versa, where $e \geq 4$ is an integer and $k_1, k_2, \ldots, k_e$ are non-negative integers satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$ (Theorems 3.4.1 and 3.4.3). By repeatedly applying this recurrence relation and enumeration formulae for self-orthogonal and self-dual codes over $\mathcal{R}_{2,r}$ and $\mathcal{R}_{3,r}$ (as obtained in Theorems 3.2.3, 3.2.5, 3.3.3 and 3.3.5), we obtain an enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length n over the chain ring $\mathcal{R}_{e,r}$ for all integers $e \geq 4$ (Theorems 3.4.5 and 3.4.6). In Section 3.5, we classify all self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over the chain ring $\mathbb{F}_5[u]/\langle u^2 \rangle$ and of lengths $2, 3$ and 4 over the chain ring $\mathbb{F}_7[u]/\langle u^2 \rangle$ by applying the classification algorithm and using the enumeration formulae obtained in Section 3.2.

Throughout this chapter, let $\mathcal{N}_e(n; k_1, k_2, \ldots, k_e)$ and $\mathcal{M}_e(n; k_1, k_2, \ldots, k_e)$ be the number of distinct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$, respectively. Let $\mathcal{N}_e(n)$ and $\mathcal{M}_e(n)$ denote the number of distinct self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,r}$, respectively. In the following section, we will consider the case $e = 2$ and count all self-orthogonal and self-dual codes of length n over $\mathcal{R}_{2,r}$.

3.2 Enumeration of self-orthogonal and self-dual codes over the chain ring $\mathcal{R}_{2,r}$

We assume, throughout this section, that $e = 2$. Here we see, by Theorem 2.2.2, that every linear code $\mathcal{C}$ of length n over $\mathcal{R}_{2,r}$ is permutation equivalent to a code with a generator matrix in the standard form

$$\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} + uB_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix},$$

where the columns are grouped into blocks of sizes k_1, k_2, $k_3 = n - k_1 - k_2$, and $B_{1,2} \in \mathcal{M}_{k_1 \times k_3}(\mathcal{T}_{2,r})$, $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_{2,r})$ for $1 \leq i \leq j \leq 2$. Further, if $\mathcal{C}$ is a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$, then by Remark 2.2.1 and Lemma 2.2.1, we have $k_1 \leq k_3$, $n \geq 2k_1 + k_2$ and $Tor_1(\mathcal{C}) \subseteq Tor_2(\mathcal{C}) \subseteq Tor_1(\mathcal{C})^{\perp}$. In particular, if $\mathcal{C}$ is a self-dual code, then by Remark 2.2.1 and Lemma 2.2.1 again, we have $k_1 = k_3$, $n = 2k_1 + k_2$ and $Tor_1(\mathcal{C}) \subseteq Tor_2(\mathcal{C}) = Tor_1(\mathcal{C})^{\perp}$.

First of all, we will count all self-orthogonal codes of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ with prescribed Torsion codes. To do this, we assume, throughout this section, that $\mathcal{C}_1$ is a k_1-dimensional linear code of length n over $\overline{\mathcal{R}}_{2,r}$ with a generator matrix

$$\begin{bmatrix} I_{k_1} & A'_{1,1} & A'_{1,2} \end{bmatrix}$$

and that $\mathcal{C}_2$ is a $(k_1 + k_2)$-dimensional linear code of length n over $\overline{\mathcal{R}}_{2,r}$ with a generator matrix

$$\begin{bmatrix} I_{k_1} & A'_{1,1} & A'_{1,2} \\ 0 & I_{k_2} & A'_{2,2} \end{bmatrix},$$

where $A'_{1,1} \in \mathcal{M}_{k_1 \times k_2}(\overline{\mathcal{R}}_{2,r})$, $A'_{1,2} \in \mathcal{M}_{k_1 \times k_3}(\overline{\mathcal{R}}_{2,r})$ and $A'_{2,2} \in \mathcal{M}_{k_2 \times k_3}(\overline{\mathcal{R}}_{2,r})$. It is clear that $\mathcal{C}_1 \subseteq \mathcal{C}_2$. Further, since the map $^{-}\restriction_{\mathcal{T}_{2,r}} : \mathcal{T}_{2,r} \to \overline{\mathcal{R}}_{2,r}$ is a bijection, there exist unique matrices $A_{1,1} \in \mathcal{M}_{k_1 \times k_2}(\mathcal{T}_{2,r})$, $A_{1,2} \in \mathcal{M}_{k_1 \times k_3}(\mathcal{T}_{2,r})$ and $A_{2,2} \in \mathcal{M}_{k_2 \times k_3}(\mathcal{T}_{2,r})$ such that $\overline{A}_{1,1} = A'_{1,1}$, $\overline{A}_{1,2} = A'_{1,2}$ and $\overline{A}_{2,2} = A'_{2,2}$. Then we have the following:

Lemma 3.2.1. *If $\mathcal{C}$ is a linear code of length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$, then there exists a matrix $B_{1,2} \in \mathcal{M}_{k_1\times k_3}(\mathcal{T}_{2,r})$ such that the matrix*

$$\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} + uB_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix} \tag{3.2.1}$$

is a generator matrix of the code $\mathcal{C}$.

Proof. As $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$, there exist matrices $M_{1,0} \in \mathcal{M}_{k_1\times k_1}(\mathcal{T}_{2,r})$, $M_{1,1} \in \mathcal{M}_{k_1\times k_2}(\mathcal{T}_{2,r})$ and $M_{1,2} \in \mathcal{M}_{k_1\times k_3}(\mathcal{T}_{2,r})$ such that

$$\mathcal{R}_{2,r}^{k_1+k_2} \begin{bmatrix} I_{k_1} + uM_{1,0} & A_{1,1} + uM_{1,1} & A_{1,2} + uM_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix} \subseteq \mathcal{C}.$$

Now by applying elementary row operations, we obtain

$$\mathcal{R}_{2,r}^{k_1+k_2} \begin{bmatrix} I_{k_1} - uM_{1,0} & 0 \\ 0 & I_{k_2} \end{bmatrix} \begin{bmatrix} I_{k_1} + uM_{1,0} & A_{1,1} + uM_{1,1} & A_{1,2} + uM_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix}$$

$$= \mathcal{R}_{2,r}^{k_1+k_2} \begin{bmatrix} I_{k_1} & A_{1,1} + u(M_{1,1} - M_{1,0}A_{1,1}) & A_{1,2} + u(M_{1,2} - M_{1,0}A_{1,2}) \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix} \subseteq \mathcal{C}.$$

We further apply elementary row operations and note that

$$\mathcal{R}_{2,r}^{k_1+k_2} \begin{bmatrix} I_{k_1} & -(M_{1,1} - M_{1,0}A_{1,1}) \\ 0 & I_{k_2} \end{bmatrix}$$
$$\times \begin{bmatrix} I_{k_1} & A_{1,1} + u(M_{1,1} - M_{1,0}A_{1,1}) & A_{1,2} + u(M_{1,2} - M_{1,0}A_{1,2}) \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix}$$

$$= \mathcal{R}_{2,r}^{k_1+k_2} \begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} + u(M_{1,2} - M_{1,0}A_{1,2} - M_{1,1}A_{2,2} + M_{1,0}A_{1,1}A_{2,2}) \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix} \subseteq \mathcal{C}.$$

We further observe that there exists a unique matrix $B_{1,2} \in \mathcal{M}_{k_1\times k_3}(\mathcal{T}_{2,r})$ satisfying

$$B_{1,2} \equiv M_{1,2} - M_{1,0}A_{1,2} - M_{1,1}A_{2,2} + M_{1,0}A_{1,1}A_{2,2} \pmod{u}.$$

This gives

$$\mathcal{R}_{2,r}^{k_1+k_2}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix} \subseteq \mathcal{C}.$$

Furthermore, we have

$$|\mathcal{C}| = |Tor_1(\mathcal{C})||Tor_2(\mathcal{C})| = (p^r)^{2k_1+k_2} = \left|\mathcal{R}_{2,r}^{k_1+k_2}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} \\ 0 & uI_{k_2} & uA_{2,2} \end{bmatrix}\right| \leq |\mathcal{C}|.$$

From this, it follows that the code $\mathcal{C}$ has a generator matrix of the form (3.2.1). □

For the remainder of this section, we assume that $\mathcal{C}_1 \subseteq \mathcal{C}_1^{\perp}$ and $\mathcal{C}_2 \subseteq \mathcal{C}_1^{\perp}$. This implies that $2k_1 + k_2 \leq n$ and that

$$\begin{aligned} I_{k_1} + A'_{1,1}A'^t_{1,1} + A'_{1,2}A'^t_{1,2} &= 0, & (3.2.2) \\ A'_{1,1} + A'_{1,2}A'^t_{2,2} &= 0. & (3.2.3) \end{aligned}$$

By equations (3.2.2) and (3.2.3), we get $A'_{1,2}\big(-A'^t_{2,2}A'_{2,2}A'^t_{1,2} - A'^t_{1,2}\big) = I_{k_1}$, from which it follows that the matrix $A'_{1,2}$ is of full row-rank.

In the following theorem, we enumerate all self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$.

Theorem 3.2.1. *There are precisely*

$$(p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}}$$

distinct self-orthogonal codes $\mathcal{C}$ of length n $(\geq 2k_1+k_2)$ over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$.

Proof. Let $\mathcal{C}$ be a self-orthogonal code of length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$. Here we see, by Lemma 3.2.1, that the code $\mathcal{C}$ has a generator matrix of the form (3.2.1). We further observe that the code $\mathcal{C}$ is self-orthogonal code if and only if

$$I_{k_1} + A_{1,1}A^t_{1,1} + A_{1,2}A^t_{1,2} + u(A_{1,2}B^t_{1,2} + B_{1,2}A^t_{1,2}) \equiv 0 \pmod{u^2}, \quad (3.2.4)$$

$$A_{1,1} + A_{1,2}A_{2,2}^t \equiv 0 \pmod{u}. \quad (3.2.5)$$

We further note that (3.2.5) is equivalent to (3.2.3). In view of this, we need to count the choices of the matrix $B_{1,2}$ over $\mathcal{T}_{2,r}$ satisfying (3.2.4). By (3.2.2), we have

$$I_{k_1} + A_{1,1}A_{1,1}^t + A_{1,2}A_{1,2}^t \equiv uP \pmod{u^2},$$

where P is a symmetric matrix over $\mathcal{T}_{2,r}$. On substituting this in equation (3.2.4), we get

$$A_{1,2}B_{1,2}^t + B_{1,2}A_{1,2}^t + P \equiv 0 \pmod{u}. \quad (3.2.6)$$

Since the map $^{-} \restriction_{\mathcal{T}_{2,r}} : \mathcal{T}_{2,r} \to \overline{\mathcal{R}}_{2,r}$ is a bijection, the number of choices for the matrix $B_{1,2}$ over $\mathcal{T}_{2,r}$ satisfying (3.2.6) is equal to the number of choices for the matrix $\overline{B}_{1,2}$ over $\overline{\mathcal{R}}_{2,r}$ satisfying

$$\overline{A}_{1,2}\overline{B}_{1,2}^t + \overline{B}_{1,2}\overline{A}_{1,2}^t = -\overline{P}. \quad (3.2.7)$$

Since the matrix $\overline{A}_{1,2}$ is of full row-rank, we see, by Lemma 2.1.1, that the number of choices for the matrix $\overline{B}_{1,2}$ satisfying (3.2.7) is equal to $|\text{Ker } \Phi_{\overline{A}_{1,2}}| = (p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}}$. From this, it follows that the number of distinct self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$ and $Tor_2(\mathcal{C}) = \mathcal{C}_2$ is given by $(p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}}$. □

In the following theorem, we count all self-orthogonal codes of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$.

Theorem 3.2.2. *The number $\mathcal{N}_2(n; k_1, k_2)$ of distinct self-orthogonal codes of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ is given by*

$$\mathcal{N}_2(n;k_1,k_2) = \begin{cases} \sigma_{p^r}(n,k_1) \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{p^r} (p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}} & \text{if } n \geq 2k_1 + k_2; \\ 0 & \text{otherwise,} \end{cases}$$

where $\sigma_{p^r}(n, k_1)$ is as determined in Theorem 2.3.11.

Proof. Let $\mathcal{D}$ be a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{D}) = \mathcal{D}_1$ and $Tor_2(\mathcal{D}) = \mathcal{D}_2$. Here we have $\dim_{\overline{\mathcal{R}}_{2,r}}(\mathcal{D}_1) = k_1$, $\dim_{\overline{\mathcal{R}}_{2,r}}(\mathcal{D}_2) = k_1 + k_2$ and $\mathcal{D}_1 \subseteq \mathcal{D}_2$. By Lemma 2.2.1, we see that the Torsion codes $\mathcal{D}_1$ and $\mathcal{D}_2$ satisfy $\mathcal{D}_1 \subseteq \mathcal{D}_2^\perp$ and $\mathcal{D}_2 \subseteq \mathcal{D}_1^\perp$. Further, by Remark 2.2.1, we must have $n \geq 2k_1 + k_2$. We next note, by Theorem 2.3.11, that there are precisely $\sigma_{p^r}(n, k_1)$ distinct self-orthogonal codes $\mathcal{D}_1$ of dimension k_1 and length n over $\overline{\mathcal{R}}_{2,r}$. Further, for a given k_1-dimensional self-orthogonal code $\mathcal{D}_1$ of length n over $\overline{\mathcal{R}}_{2,r}$, we observe that the number of choices for the $(k_1 + k_2)$-dimensional code $\mathcal{D}_2$ of length n over $\overline{\mathcal{R}}_{2,r}$ satisfying $\mathcal{D}_1 \subseteq \mathcal{D}_2 \subseteq \mathcal{D}_1^{\perp}$ is equal to the number of distinct k_2-dimensional subspaces $\mathcal{D}_2/\mathcal{D}_1$ of the quotient space $\mathcal{D}_1^{\perp}/\mathcal{D}_1$, which has dimension $n - 2k_1$ over $\overline{\mathcal{R}}_{2,r}$. From this and by applying Theorem 2.3.9, we see that the code $\mathcal{D}_2$ has precisely $\begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{p^r}$ distinct choices for a given choice of the self-orthogonal code $\mathcal{D}_1$. Furthermore, for given codes $\mathcal{D}_1$ and $\mathcal{D}_2$, we see, by Theorem 3.2.1, that there are precisely $(p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}}$ distinct self-orthogonal codes $\mathcal{D}$ of length n over $\mathcal{R}_{2,r}$ with $Tor_1(\mathcal{D}) = \mathcal{D}_1$ and $Tor_2(\mathcal{D}) = \mathcal{D}_2$. From this, the desired result follows immediately. □

Now in the following theorem, we obtain an enumeration formula for all self-orthogonal codes of length n over $\mathcal{R}_{2,r}$.

Theorem 3.2.3. *The number $\mathcal{N}_2(n)$ of distinct self-orthogonal codes of length n over $\mathcal{R}_{2,r}$ is given by*

$$\mathcal{N}_2(n) = \sum_{k_1=0}^{\lfloor \frac{n}{2} \rfloor} \sigma_{p^r}(n, k_1) \sum_{k_2=0}^{n-2k_1} \begin{bmatrix} n - 2k_1 \\ k_2 \end{bmatrix}_{p^r} (p^r)^{\frac{k_1(2n-3k_1-2k_2-1)}{2}},$$

where $\sigma_{p^r}(n, k_1)$, $0 \leq k_1 \leq \lfloor \frac{n}{2} \rfloor$, is as determined in Theorem 2.3.11.

Proof. It follows immediately from Theorem 3.2.2. □

In the following theorem, we first derive a necessary and sufficient condition for a linear code of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ to be a self-dual code. We also count all self-dual codes of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$.

Theorem 3.2.4. *(a) Let $\mathcal{C}$ be a linear code of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ whose generator matrix G is given by (3.2.1). The code $\mathcal{C}$ is self-dual if and only if $n = 2k_1 + k_2$ and the code $\mathcal{C}$ is self-orthogonal (i.e., the block matrices $A_{1,1}$, $A_{1,2}$, $A_{2,2}$ and $B_{1,2}$ in the generator matrix G satisfy the matrix equations (3.2.4) and (3.2.5)).*

(b) *The number $\mathcal{M}_2(n; k_1, k_2)$ of distinct self-dual codes of the type $\{k_1, k_2\}$ and length n over $\mathcal{R}_{2,r}$ is given by*

$$\mathcal{M}_2(n; k_1, k_2) = \begin{cases} \sigma_{p^r}(n, k_1)(p^r)^{\frac{k_1(k_1-1)}{2}} & \text{if } n = 2k_1 + k_2; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (a) It follows immediately by Remark 2.2.1 and Theorem 2.2.4.

(b) By part (a), we note that $\mathcal{M}_2(n; k_1, k_2) = 0$ if $n \neq 2k_1 + k_2$. When $n = 2k_1 + k_2$, we see, by part (a) and Theorem 3.2.2, that $\mathcal{M}_2(n; k_1, k_2) = \mathcal{N}_2(n; k_1, n - 2k_1) = \sigma_{p^r}(n, k_1)(p^r)^{\frac{k_1(k_1-1)}{2}}$. □

In the following theorem, we obtain an enumeration formula for all self-dual codes of length n over $\mathcal{R}_{2,r}$.

Theorem 3.2.5. *The number $\mathcal{M}_2(n)$ of distinct self-dual codes of length n over $\mathcal{R}_{2,r}$ is given by*

$$\mathcal{M}_2(n) = \sum_{k_1=0}^{\lfloor \frac{n}{2} \rfloor} \sigma_{p^r}(n, k_1)(p^r)^{\frac{k_1(k_1-1)}{2}}.$$

Proof. It follows immediately from Theorem 3.2.4. □

Remark 3.2.1. *Theorem 2 and Corollary 1 of Galvez et al. [47] follow, as special cases, from Theorems 3.2.2 and 3.2.5, respectively. Corollary 1 of Betty and Munemasa [12] follows from Theorem 3.2.2 as a special case.*

In the next section, we will consider the case $e = 3$ and count all self-orthogonal and self-dual codes of length n over the chain ring $\mathcal{R}_{3,r}$.

3.3 Enumeration of self-orthogonal and self-dual codes over the chain ring $\mathcal{R}_{3,r}$

Throughout this section, we assume that $e = 3$. Here we see, by Theorem 2.2.2, that every linear code $\mathcal{C}$ of length n over $\mathcal{R}_{3,r}$ is permutation equivalent to a code with a generator matrix in the standard form

$$\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} & A_{1,3}+uB_{1,3}+u^2C_{1,3} \\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uB_{2,3}) \\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3} \end{bmatrix}, \tag{3.3.1}$$

where the columns are grouped into blocks of sizes k_1, k_2, k_3, $k_4 = n-k_1-k_2-k_3$, and $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_{3,r})$ for $1 \leq i \leq j \leq 3$, $B_{1,2} \in \mathcal{M}_{k_1 \times k_3}(\mathcal{T}_{3,r})$, $B_{1,3} \in \mathcal{M}_{k_1 \times k_4}(\mathcal{T}_{3,r})$, $C_{1,3} \in \mathcal{M}_{k_1 \times k_4}(\mathcal{T}_{3,r})$, $B_{2,3} \in \mathcal{M}_{k_2 \times k_4}(\mathcal{T}_{3,r})$. Now if $\mathcal{C}$ is a self-orthogonal code of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$, then by Remark 2.2.1 and Lemma 2.2.1, we must have $k_1 \leq k_4$, $k_1 + k_2 \leq k_3 + k_4$, $Tor_1(\mathcal{C}) \subseteq Tor_1(\mathcal{C})^{\perp}$, $Tor_2(\mathcal{C}) \subseteq Tor_2(\mathcal{C})^{\perp}$ and $Tor_3(\mathcal{C}) \subseteq Tor_1(\mathcal{C})^{\perp}$. In particular, if the code $\mathcal{C}$ is self-dual, then by Remark 2.2.1 and Lemma 2.2.1 again, we must have $k_1 = k_4$, $k_2 = k_3$, $n = 2k_1 + 2k_2$, $Tor_1(\mathcal{C}) \subseteq Tor_2(\mathcal{C}) = Tor_2(\mathcal{C})^{\perp} \subseteq Tor_1(\mathcal{C})^{\perp}$ and $Tor_3(\mathcal{C}) = Tor_1(\mathcal{C})^{\perp}$. Furthermore, when $Tor_2(\mathcal{C}) = Tor_2(\mathcal{C})^{\perp}$, we see, by Theorem 2.3.2, that $2\dim_{\overline{\mathcal{R}}_{3,r}}(Tor_2(\mathcal{C})) = n$, which implies that the length n must be an even integer and that the Torsion code $Tor_2(\mathcal{C})$ is a self-dual code of length n and dimension $\frac{n}{2}$ over $\overline{\mathcal{R}}_{3,r}$. On the other hand, when n is even, we see, by Theorem 2.3.12, that there exists a self-dual code of length n and dimension $\frac{n}{2}$ over $\overline{\mathcal{R}}_{3,r}$ if and only if $(-1)^{\frac{n}{2}}$ is a square in $\overline{\mathcal{R}}_{3,r} \simeq \mathbb{F}_{p^r}$. In view of this, we see that if there exists a self-dual code of length n over $\mathcal{R}_{3,r}$, then the length n must be an even integer and the element $(-1)^{\frac{n}{2}}$ must be a square in $\overline{\mathcal{R}}_{3,r}$.

To begin with, we will first count all self-orthogonal codes of length n over $\mathcal{R}_{3,r}$ with prescribed Torsion codes. To do this, we assume, throughout this section, that $\mathcal{C}_1$ is a k_1-dimensional linear code of length n over $\overline{\mathcal{R}}_{3,r}$ with a generator matrix

$$\begin{bmatrix} I_{k_1} & A'_{1,1} & A'_{1,2} & A'_{1,3} \end{bmatrix},$$

$\mathcal{C}_2$ is a (k_1+k_2)-dimensional linear code of length n over $\overline{\mathcal{R}}_{3,r}$ with a generator matrix

$$\begin{bmatrix} I_{k_1} & A'_{1,1} & A'_{1,2} & A'_{1,3} \\ 0 & I_{k_2} & A'_{2,2} & A'_{2,3} \end{bmatrix},$$

and that $\mathcal{C}_3$ is a $(k_1 + k_2 + k_3)$-dimensional linear code of length n over $\overline{\mathcal{R}}_{3,r}$ with a generator matrix

$$\begin{bmatrix} I_{k_1} & A'_{1,1} & A'_{1,2} & A'_{1,3} \\ 0 & I_{k_2} & A'_{2,2} & A'_{2,3} \\ 0 & 0 & I_{k_3} & A'_{3,3} \end{bmatrix},$$

where $A'_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\overline{\mathcal{R}}_{3,r})$ for $1 \leq i \leq j \leq 3$. Since the map $^{-}\restriction_{\mathcal{T}_{3,r}} : \mathcal{T}_{3,r} \to \overline{\mathcal{R}}_{3,r}$ is a bijection, there exist unique matrices $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_{3,r})$ satisfying $\overline{A}_{i,j} = A'_{i,j}$ for $1 \leq i \leq j \leq 3$. Further, it is clear that $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \mathcal{C}_3$. Then we have the following:

Lemma 3.3.1. *If $\mathcal{C}$ is a linear code of length n over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$, $Tor_2(\mathcal{C}) = \mathcal{C}_2$ and $Tor_3(\mathcal{C}) = \mathcal{C}_3$, then there exist matrices $B_{1,2} \in \mathcal{M}_{k_1 \times k_3}(\mathcal{T}_{3,r})$, $B_{1,3} \in \mathcal{M}_{k_1 \times k_4}(\mathcal{T}_{3,r})$, $B_{2,3} \in \mathcal{M}_{k_2 \times k_4}(\mathcal{T}_{3,r})$ and $C_{1,3} \in \mathcal{M}_{k_1 \times k_4}(\mathcal{T}_{3,r})$ such that the matrix*

$$\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} + uB_{1,2} & A_{1,3} + uB_{1,3} + u^2C_{1,3} \\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3} + uB_{2,3}) \\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3} \end{bmatrix} \tag{3.3.2}$$

is a generator matrix of the code $\mathcal{C}$.

Proof. As $Tor_1(\mathcal{C}) = \mathcal{C}_1$, $Tor_2(\mathcal{C}) = \mathcal{C}_2$ and $Tor_3(\mathcal{C}) = \mathcal{C}_3$, there exist matrices $M_{1,j}$, $N_{1,j} \in \mathcal{M}_{k_1 \times k_{j+1}}(\mathcal{T}_{3,r})$ for $0 \leq j \leq 3$, and $M_{2,\ell} \in \mathcal{M}_{k_2 \times k_{\ell+1}}(\mathcal{T}_{3,r})$ for $1 \leq \ell \leq 3$ such that

$$\mathcal{R}_{3,r}^{k_1+k_2+k_3} H \subseteq \mathcal{C},$$

where the matrix H equals

$$\begin{bmatrix} I_{k_1} + uM_{1,0} + u^2N_{1,0} & A_{1,1} + uM_{1,1} + u^2N_{1,1} & A_{1,2} + uM_{1,2} + u^2N_{1,2} & A_{1,3} + uM_{1,3} + u^2N_{1,3} \\ 0 & u(I_{k_2} + uM_{2,1}) & u(A_{2,2} + uM_{2,2}) & u(A_{2,3} + uM_{2,3}) \\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3} \end{bmatrix}.$$

By applying elementary row operations, we obtain

$$\mathcal{R}_{3,r}^{k_1+k_2+k_3} \begin{bmatrix} I_{k_1} - uM_{1,0} - u^2N_{1,0} + u^2M_{1,0}^2 & Q_1 + uQ_2 & Q_3 \\ 0 & I_{k_2} - uM_{2,1} & Q_4 \\ 0 & 0 & I_{k_3} \end{bmatrix} H \subseteq \mathcal{C},$$

where

$$\begin{aligned}
Q_1 &= -M_{1,1} + M_{1,0}A_{1,1},\\
Q_2 &= -N_{1,1} + M_{1,0}M_{1,1} + N_{1,0}A_{1,1} - M_{1,0}^2A_{1,1} + M_{1,1}M_{2,1} - M_{1,0}A_{1,1}M_{2,1},\\
Q_3 &= -N_{1,2} + M_{1,0}M_{1,2} + N_{1,0}A_{1,2} - (M_{1,0})^2A_{1,2} - Q_1M_{2,2} - Q_2A_{2,2},\\
Q_4 &= -M_{2,2} + M_{2,1}A_{2,2}.
\end{aligned}$$

From this, we get

$$\mathcal{R}_{3,r}^{k_1+k_2+k_3}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uM''_{1,2} & A_{1,3}+uM''_{1,3}+u^2N''_{1,3}\\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uM''_{2,3})\\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3}\end{bmatrix} \subseteq \mathcal{C},$$

where

$$\begin{aligned}
M''_{1,2} &= M_{1,2} - M_{1,0}A_{1,2} + Q_1A_{2,2},\\
M''_{1,3} &= M_{1,3} - M_{1,0}A_{1,3} + Q_1A_{2,3},\\
N''_{1,3} &= N_{1,3} - M_{1,0}M_{1,3} - N_{1,0}A_{1,3} + M_{1,0}^2A_{1,3} + Q_1M_{2,3} + Q_2A_{2,3} + Q_3A_{3,3},\\
M''_{2,3} &= M_{2,3} - M_{2,1}A_{2,3} + Q_4A_{3,3}.
\end{aligned}$$

We further observe that there exist unique matrices $B_{1,2}$, $C_{1,2}$ and $B_{2,3}$ over $\mathcal{T}_{3,r}$ satisfying $M''_{1,2} \equiv B_{1,2}+uC_{1,2} \pmod{u^2}$ and $M''_{2,3} \equiv B_{2,3} \pmod{u}$. On further applying the elementary row operations, we see that

$$\mathcal{R}_{3,r}^{k_1+k_2+k_3}\begin{bmatrix} I_{k_1} & 0 & -C_{1,2}\\ 0 & I_{k_2} & 0\\ 0 & 0 & I_{k_3}\end{bmatrix}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2}+u^2C_{1,2} & A_{1,3}+uM''_{1,3}+u^2N''_{1,3}\\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uB_{2,3})\\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3}\end{bmatrix}$$

$$= \mathcal{R}_{3,r}^{k_1+k_2+k_3}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} & A_{1,3}+uM''_{1,3}+u^2(N''_{1,3}-C_{1,2}A_{3,3})\\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uB_{2,3})\\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3}\end{bmatrix} \subseteq \mathcal{C}.$$

Next, we observe that there exist unique matrices $B_{1,3}$ and $C_{1,3}$ over $\mathcal{T}_{3,r}$ satisfying

$M''_{1,3}+u(N''_{1,3}-C_{1,2}A_{3,3})\equiv B_{1,3}+uC_{1,3} \pmod{u^2}$. This gives

$$\mathcal{R}_{3,r}^{k_1+k_2+k_3}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} & A_{1,3}+uB_{1,3}+u^2C_{1,3}\\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uB_{2,3})\\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3}\end{bmatrix}\subseteq \mathcal{C}.$$

Furthermore, we note that

$$\begin{aligned}|\mathcal{C}| &= \prod_{i=1}^{3}|Tor_i(\mathcal{C})| = (p^r)^{3k_1+2k_2+k_3}\\ &= \left|\mathcal{R}_{3,r}^{k_1+k_2+k_3}\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2}+uB_{1,2} & A_{1,3}+uB_{1,3}+u^2C_{1,3}\\ 0 & uI_{k_2} & uA_{2,2} & u(A_{2,3}+uB_{2,3})\\ 0 & 0 & u^2I_{k_3} & u^2A_{3,3}\end{bmatrix}\right|\leq|\mathcal{C}|.\end{aligned}$$

From this, it follows that the code $\mathcal{C}$ has a generator matrix of the form (3.3.2). □

For the remainder of this section, we assume that the codes $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ satisfy $\mathcal{C}_1\subseteq\mathcal{C}_1^{\perp}$, $\mathcal{C}_2\subseteq\mathcal{C}_2^{\perp}$ and $\mathcal{C}_3\subseteq\mathcal{C}_1^{\perp}$. This implies that

$$I_{k_1}+A'_{1,1}A'^{t}_{1,1}+A'_{1,2}A'^{t}_{1,2}+A'_{1,3}A'^{t}_{1,3} = 0, \qquad (3.3.3)$$

$$A'_{1,1}+A'_{1,2}A'^{t}_{2,2}+A'_{1,3}A'^{t}_{2,3} = 0, \qquad (3.3.4)$$

$$A'_{1,2}+A'_{1,3}A'^{t}_{3,3} = 0, \qquad (3.3.5)$$

$$I_{k_2}+A'_{2,2}A'^{t}_{2,2}+A'_{2,3}A'^{t}_{2,3} = 0. \qquad (3.3.6)$$

By (3.3.3)-(3.3.5), we see that the matrix $A'_{1,3}$ is of full row-rank. In the following theorem, we enumerate all self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{C})=\mathcal{C}_1$, $Tor_2(\mathcal{C})=\mathcal{C}_2$ and $Tor_3(\mathcal{C})=\mathcal{C}_3$.

Theorem 3.3.1. *The number of distinct self-orthogonal codes $\mathcal{C}$ of length n $(\geq 2k_1+2k_2)$ over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{C})=\mathcal{C}_1$, $Tor_2(\mathcal{C})=\mathcal{C}_2$ and $Tor_3(\mathcal{C})=\mathcal{C}_3$ is given by*

$$(p^r)^{k_1(2n-3k_1-k_3-1)+k_2(n-4k_1-k_2-k_3)}.$$

Proof. Let $\mathcal{C}$ be a self-orthogonal code of length n over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{C})=\mathcal{C}_1$, $Tor_2(\mathcal{C})=\mathcal{C}_2$ and $Tor_3(\mathcal{C})=\mathcal{C}_3$. Here by Lemma 3.3.1, we see that the code $\mathcal{C}$

has a generator matrix of the form (3.3.2). We further observe that the code $\mathcal{C}$ is self-orthogonal if and only if

$$\begin{aligned} I_{k_1}+A_{1,1}A_{1,1}^t+A_{1,2}A_{1,2}^t+A_{1,3}A_{1,3}^t & \\ +u\big(A_{1,2}B_{1,2}^t+B_{1,2}A_{1,2}^t+A_{1,3}B_{1,3}^t+B_{1,3}A_{1,3}^t\big) & \\ +u^2\big(B_{1,2}B_{1,2}^t+B_{1,3}B_{1,3}^t+A_{1,3}C_{1,3}^t+C_{1,3}A_{1,3}^t\big) &\equiv 0 \pmod{u^3}, \qquad (3.3.7)\\ A_{1,1}+A_{1,2}A_{2,2}^t+A_{1,3}A_{2,3}^t & \\ +u\big(B_{1,2}A_{2,2}^t+B_{1,3}A_{2,3}^t+A_{1,3}B_{2,3}^t\big) &\equiv 0 \pmod{u^2}, \qquad (3.3.8)\\ A_{1,2}+A_{1,3}A_{3,3}^t &\equiv 0 \pmod{u}, \qquad (3.3.9)\\ I_{k_2}+A_{2,2}A_{2,2}^t+A_{2,3}A_{2,3}^t &\equiv 0 \pmod{u}. \qquad (3.3.10)\end{aligned}$$

It is easy to observe that (3.3.9) is equivalent to (3.3.5) and that (3.3.10) is equivalent to (3.3.6). In view of this, we need to determine the number of possible choices for the matrices $B_{1,2}$, $B_{1,3}$, $C_{1,3}$ and $B_{2,3}$ over $\mathcal{T}_{3,r}$ satisfying (3.3.7) and (3.3.8). For this, we note that (3.3.3) implies that

$$I_{k_1}+A_{1,1}A_{1,1}^t+A_{1,2}A_{1,2}^t+A_{1,3}A_{1,3}^t\equiv uP_1+u^2P_2 \pmod{u^3},$$

where $P_1,P_2\in Sym_{k_1}(\mathcal{T}_{3,r})$. On substituting this in (3.3.7), we get

$$\begin{aligned} P_1+A_{1,2}B_{1,2}^t+B_{1,2}A_{1,2}^t+A_{1,3}B_{1,3}^t+B_{1,3}A_{1,3}^t+u\big(B_{1,2}B_{1,2}^t & \\ +B_{1,3}B_{1,3}^t+A_{1,3}C_{1,3}^t+C_{1,3}A_{1,3}^t+P_2\big) &\equiv 0 \pmod{u^2}. \quad (3.3.11)\end{aligned}$$

As $B_{1,2}\in\mathcal{M}_{k_1\times k_3}(\mathcal{T}_{3,r})$ can be chosen arbitrarily, there are precisely $(p^r)^{k_1k_3}$ distinct choices for the matrix $B_{1,2}$. Now for a given choice of the matrix $B_{1,2}$, we will determine the number of possible choices for the matrix $\overline{B}_{1,3}$ satisfying

$$\overline{A}_{1,3}\overline{B}_{1,3}^t+\overline{B}_{1,3}\overline{A}_{1,3}^t=-\big(\overline{P}_1+\overline{A}_{1,2}\overline{B}_{1,2}^t+\overline{B}_{1,2}\overline{A}_{1,2}^t\big). \qquad (3.3.12)$$

Since $\overline{P}_1\in Sym_{k_1}(\overline{\mathcal{R}}_{3,r})$, the matrix $\overline{A}_{1,3}$ is of full row-rank and the map $^{-}\restriction_{\mathcal{T}_{3,r}}$: $\mathcal{T}_{3,r}\to\overline{\mathcal{R}}_{3,r}$ is a bijection, by Lemma 2.1.1, we see that the number of relevant choices for the matrix $B_{1,3}$ satisfying (3.3.12) is equal to $|\text{Ker }\Phi_{\overline{A}_{1,3}}|=(p^r)^{\frac{k_1(2n-3k_1-2k_2-2k_3-1)}{2}}$.

Further, for given matrices $B_{1,2}$ and $B_{1,3}$ satisfying (3.3.12), we get

$$P_1 + A_{1,2}B_{1,2}^t + B_{1,2}A_{1,2}^t + A_{1,3}B_{1,3}^t + B_{1,3}A_{1,3}^t \equiv uP_3 \pmod{u^2}, \tag{3.3.13}$$

where $P_3 \in Sym_{k_1}(\mathcal{T}_{3,r})$. Now on substituting this in (3.3.11), we obtain

$$A_{1,3}C_{1,3}^t + C_{1,3}A_{1,3}^t \equiv -\big(P_2 + P_3 + B_{1,2}B_{1,2}^t + B_{1,3}B_{1,3}^t\big) \pmod{u}. \tag{3.3.14}$$

Further, we note that the number of choices for the matrix $C_{1,3}$ over $\mathcal{T}_{3,r}$ satisfying (3.3.14) is equal to the number of choices for the matrix $\overline{C}_{1,3}$ over $\overline{\mathcal{R}}_{3,r}$ satisfying

$$\overline{A}_{1,3}\overline{C}_{1,3}^t + \overline{C}_{1,3}\overline{A}_{1,3}^t = -(\overline{P}_2 + \overline{P}_3 + \overline{B}_{1,2}\overline{B}_{1,2}^t + \overline{B}_{1,3}\overline{B}_{1,3}^t). \tag{3.3.15}$$

Since $\overline{P}_2, \overline{P}_3 \in Sym_{k_1}(\overline{\mathcal{R}}_{3,r})$, by applying Lemma 2.1.1 again, we see that the matrix $\overline{C}_{1,3}$ satisfying (3.3.15) has precisely $|\text{Ker } \Phi_{\overline{A}_{1,3}}| = (p^r)^{\frac{k_1(2n-3k_1-2k_2-2k_3-1)}{2}}$ distinct choices. Next we will count all possible choices for the matrix $B_{2,3}$ over $\mathcal{T}_{3,r}$ satisfying (3.3.8). To do this, we see, by (3.3.4), that

$$A_{1,1} + A_{1,2}A_{2,2}^t + A_{1,3}A_{2,3}^t \equiv uP_4 \pmod{u^2}$$

for some $P_4 \in \mathcal{M}_{k_1\times k_2}(\mathcal{T}_{3,r})$. On substituting this in (3.3.8), we get

$$P_4 + B_{1,2}A_{2,2}^t + B_{1,3}A_{2,3}^t + A_{1,3}B_{2,3}^t \equiv 0 \pmod{u}. \tag{3.3.16}$$

Now the number of choices for the matrix $B_{2,3}$ over $\mathcal{T}_{3,r}$ satisfying (3.3.16) is equal to the number of choices for the matrix $\overline{B}_{2,3}$ over $\overline{\mathcal{R}}_{3,r}$ satisfying

$$\overline{A}_{1,3}\overline{B}_{2,3}^t = -\big(\overline{P}_4 + \overline{B}_{1,2}\overline{A}_{2,2}^t + \overline{B}_{1,3}\overline{A}_{2,3}^t\big). \tag{3.3.17}$$

To count the choices for the matrix $\overline{B}_{2,3}$, let $\overline{A}_{1,3} = (\mathbf{a}_i)$ and $\overline{B}_{2,3} = (\mathbf{x}_j)$, where $\mathbf{a}_i$'s and $\mathbf{x}_j$'s are the rows of the matrices $\overline{A}_{1,3}$ and $\overline{B}_{2,3}$, respectively. Moreover, let us suppose that $-\big(\overline{P}_4 + \overline{B}_{1,2}\overline{A}_{2,2}^t + \overline{B}_{1,3}\overline{A}_{2,3}^t\big) = (m_{ij})$, where m_{ij} denotes the (i,j)-th entry of the matrix $-\big(\overline{P}_4 + \overline{B}_{1,2}\overline{A}_{2,2}^t + \overline{B}_{1,3}\overline{A}_{2,3}^t\big)$ for $1 \le i \le k_1$ and $1 \le j \le k_2$. In view of this, the matrix equation (3.3.17) is equivalent to the following system of equations over $\overline{\mathcal{R}}_{3,r}$:

$$\mathbf{a}_i \cdot \mathbf{x}_j = m_{ij} \text{ for } 1 \leq i \leq k_1 \text{ and } 1 \leq j \leq k_2,$$

which can be represented by the following matrix equation:

$$\mathcal{A}\begin{bmatrix} \mathbf{x}_1^t \\ \mathbf{x}_2^t \\ \mathbf{x}_3^t \\ \vdots \\ \mathbf{x}_{k_2}^t \end{bmatrix} = \begin{bmatrix} m_{11} \\ m_{12} \\ m_{13} \\ \vdots \\ m_{k_1k_2} \end{bmatrix}, \text{ where } \mathcal{A} = \begin{bmatrix} \mathbf{a}_1 & & \\ & \ddots & \\ & & \mathbf{a}_1 \\ \vdots & \vdots & \vdots \\ \mathbf{a}_{k_1} & & \\ & \ddots & \\ & & \mathbf{a}_{k_1} \end{bmatrix}.$$

Note that the matrix $\mathcal{A}$ is of order $k_1k_2 \times k_2(n-k_1-k_2-k_3)$. Since the matrix $\overline{A}_{1,3} = (\mathbf{a}_i)$ is of full row-rank, the rows of the matrix $\mathcal{A}$ are linearly independent over $\overline{\mathcal{R}}_{3,r}$. Thus the number of choices for the matrix $\overline{B}_{2,3}$ satisfying (3.3.17) is given by $(p^r)^{k_2(n-2k_1-k_2-k_3)}$.

Now from the above discussion, it follows that the number of distinct self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_1$, $Tor_2(\mathcal{C}) = \mathcal{C}_2$ and $Tor_3(\mathcal{C}) = \mathcal{C}_3$ is given by $(p^r)^{k_1(2n-3k_1-k_3-1)+k_2(n-4k_1-k_2-k_3)}$. □

In the following theorem, we count all self-orthogonal codes of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$.

Theorem 3.3.2. *(a) Let $\mathcal{C}$ be a linear code of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$ whose generator matrix G is given by (3.3.1). Then the code $\mathcal{C}$ is self-orthogonal if and only if $k_1 \leq k_4 = n-k_1-k_2-k_3$, $2(k_1+k_2) \leq n$, and the block matrices $A_{i,j}$ for $1 \leq i \leq j \leq 3$, $B_{1,2}$, $B_{1,3}$, $C_{1,3}$ and $B_{2,3}$ of the generator matrix G satisfy the matrix equations (3.3.7)-(3.3.10).*

(b) The number $\mathcal{N}_3(n; k_1, k_2, k_3)$ of distinct self-orthogonal codes of the type $\{k_1, k_2,$

$k_3\}$ and length n over $\mathcal{R}_{3,r}$ is given by

$$\mathcal{N}_3(n;k_1,k_2,k_3)=\begin{cases}\sigma_{p^r}(n,k_1+k_2)\begin{bmatrix}k_1+k_2\\ k_1\end{bmatrix}_{p^r}\begin{bmatrix}n-2k_1-k_2\\ k_3\end{bmatrix}_{p^r}\\ \times(p^r)^{k_1(2n-3k_1-k_3-1)+k_2(n-4k_1-k_2-k_3)}\\ \textit{if } 2k_1+k_2+k_3\leq n \textit{ and } 2(k_1+k_2)\leq n;\\ 0 \quad \textit{otherwise,}\end{cases}$$

where the number $\sigma_{p^r}(n,k_1+k_2)$ is as determined in Theorem 2.3.11.

Proof. (a) It follows immediately by Remark 2.2.1 and Theorem 2.2.4.

(b) Here we first note, by part (a), that $\mathcal{N}_3(n;k_1,k_2,k_3)=0$ when either $2k_1+k_2+k_3>n$ or $2k_1+2k_2>n$.

Next, let k_1,k_2,k_3 be non-negative integers satisfying $2k_1+k_2+k_3\leq n$ and $2k_1+2k_2\leq n$, and let $\mathcal{D}$ be a self-orthogonal code of the type $\{k_1,k_2,k_3\}$ and length n over $\mathcal{R}_{3,r}$ with $Tor_1(\mathcal{D})=\mathcal{D}_1$, $Tor_2(\mathcal{D})=\mathcal{D}_2$ and $Tor_3(\mathcal{D})=\mathcal{D}_3$. Here we have $\dim_{\overline{\mathcal{R}}_{3,r}}(\mathcal{D}_1)=k_1$, $\dim_{\overline{\mathcal{R}}_{3,r}}(\mathcal{D}_2)=k_1+k_2$ and $\dim_{\overline{\mathcal{R}}_{3,r}}(\mathcal{D}_3)=k_1+k_2+k_3$. Further, by Lemma 2.2.1, we see that the Torsion codes $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$ satisfy $\mathcal{D}_1\subseteq\mathcal{D}_2\subseteq\mathcal{D}_3\subseteq\mathcal{D}_1^{\perp}$ and $\mathcal{D}_2\subseteq\mathcal{D}_2^{\perp}$. Now by Theorem 2.3.11, we note that there are precisely $\sigma_{p^r}(n,k_1+k_2)$ distinct self-orthogonal codes $\mathcal{D}_2$ of length n and dimension k_1+k_2 over $\overline{\mathcal{R}}_{3,r}$. Further, for a given (k_1+k_2)-dimensional self-orthogonal code $\mathcal{D}_2$ of length n over $\overline{\mathcal{R}}_{3,r}$, we see, by Theorem 2.3.9, that there are precisely $\begin{bmatrix}k_1+k_2\\ k_1\end{bmatrix}_{p^r}$ distinct k_1-dimensional linear subcodes $\mathcal{D}_1$ of the code $\mathcal{D}_2$. Furthermore, for a given (k_1+k_2)-dimensional self-orthogonal code $\mathcal{D}_2$ of length n over $\overline{\mathcal{R}}_{3,r}$ and a given k_1-dimensional linear subcode $\mathcal{D}_1$ of the code $\mathcal{D}_2$, we observe that there is a one-to-one correspondence between $(k_1+k_2+k_3)$-dimensional linear codes $\mathcal{D}_3$ of length n over $\overline{\mathcal{R}}_{3,r}$ satisfying $\mathcal{D}_2\subseteq\mathcal{D}_3\subseteq\mathcal{D}_1^{\perp}$ and k_3-dimensional subspaces $\mathcal{D}_3/\mathcal{D}_2$ of the quotient space $\mathcal{D}_1^{\perp}/\mathcal{D}_2$, which has dimension $n-2k_1-k_2$ over $\overline{\mathcal{R}}_{3,r}$. Now by applying Theorem 2.3.9 again, we see that the code $\mathcal{D}_3$ has precisely $\begin{bmatrix}n-2k_1-k_2\\ k_3\end{bmatrix}_{p^r}$ distinct choices for given codes $\mathcal{D}_1$ and $\mathcal{D}_2$. Finally, for given codes $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{D}_3$, we note, by Theorem 3.3.1, that there are precisely $(p^r)^{k_1(2n-3k_1-k_3-1)+k_2(n-4k_1-k_2-k_3)}$ distinct self-orthogonal codes $\mathcal{D}$ of the type $\{k_1,k_2,k_3\}$ and length n over $\mathcal{R}_{3,r}$ satisfying

$Tor_1(\mathcal{D}) = \mathcal{D}_1$, $Tor_2(\mathcal{D}) = \mathcal{D}_2$ and $Tor_3(\mathcal{D}) = \mathcal{D}_3$. From this, part (b) follows immediately.

□

In the following theorem, we provide an enumeration formula for all self-orthogonal codes of length n over $\mathcal{R}_{3,r}$.

Theorem 3.3.3. *The number $\mathcal{N}_3(n)$ of distinct self-orthogonal codes of length n over $\mathcal{R}_{3,r}$ is given by*

$$\mathcal{N}_3(n) = \sum_{k_1=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{k_2=0}^{\lfloor \frac{n}{2} \rfloor - k_1} \sum_{k_3=0}^{n-2k_1-k_2} \sigma_{p^r}(n, k_1+k_2)(p^r)^{k_1(2n-3k_1-k_3-1)+k_2(n-4k_1-k_2-k_3)} \times \begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} n-2k_1-k_2 \\ k_3 \end{bmatrix}_{p^r}.$$

Proof. It follows immediately from Theorem 3.3.2. □

In the following theorem, we derive a necessary and sufficient condition under which a linear code of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$ is a self-dual code. Using this, we also count all self-dual codes of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$.

Theorem 3.3.4. *(a) Let $\mathcal{C}$ be a linear code of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$ whose generator matrix G is given by (3.3.1). Then the code $\mathcal{C}$ is self-dual if and only if $k_2 = k_3$, $n = 2(k_1+k_2)$, $(-1)^{\frac{n}{2}}$ is a square in $\overline{\mathcal{R}}_{3,r} \simeq \mathbb{F}_{p^r}$, and the block matrices $A_{i,j}$ for $1 \leq i \leq j \leq 3$, $B_{1,2}$, $B_{1,3}$, $C_{1,3}$ and $B_{2,3}$ in the generator matrix G satisfy the matrix equations (3.3.7)-(3.3.10).*

(b) The number $\mathcal{M}_3(n; k_1, k_2, k_3)$ of distinct self-dual codes of the type $\{k_1, k_2, k_3\}$ and length n over $\mathcal{R}_{3,r}$ is given by

$$\mathcal{M}_3(n; k_1, k_2, k_3) = \begin{cases} 2\prod_{i=1}^{\frac{n}{2}-1}(p^{ri}+1)\begin{bmatrix} \frac{n}{2} \\ k_1 \end{bmatrix}_{p^r} p^{\frac{rk_1(n-2)}{2}} & \textit{if } n \textit{ is even, } (-1)^{\frac{n}{2}} \textit{ is a} \\ \textit{square in } \overline{\mathcal{R}}_{3,r}, k_2 = k_3 \textit{ and } n = 2k_1 + 2k_2; & \\ 0 \quad \textit{otherwise.} & \end{cases}$$

Proof. (a) It follows immediately by Remark 2.2.1, Lemma 2.2.1 and Theorem 2.3.12.

(b) Here we first suppose that n is even, $(-1)^{\frac{n}{2}}$ is a square in $\overline{\mathcal{R}}_{3,r}$, $k_2 = k_3$ and $n = 2k_1 + 2k_2$. In this case, we see, by Theorems 2.3.12 and 3.3.2, that

$$\begin{aligned}\mathcal{M}_3(n; k_1, k_2, k_3) &= \mathcal{N}_3\left(n; k_1, \frac{n-2k_1}{2}, \frac{n-2k_1}{2}\right)\\ &= \sigma_{p^r}\left(n, \frac{n}{2}\right)\begin{bmatrix}\frac{n}{2}\\ k_1\end{bmatrix}_{p^r} p^{\frac{rk_1(n-2)}{2}} = 2\prod_{i=1}^{\frac{n}{2}-1}(p^{ri}+1)\begin{bmatrix}\frac{n}{2}\\ k_1\end{bmatrix}_{p^r} p^{\frac{rk_1(n-2)}{2}}.\end{aligned}$$

Otherwise, by part (a), we have $\mathcal{M}_3(n; k_1, k_2, k_3) = 0$.

□

From the above theorem, we see that if there exists a self-dual code of length n over $\mathcal{R}_{3,r}$, then the length n must be an even integer and $(-1)^{\frac{n}{2}}$ must be a square in $\overline{\mathcal{R}}_{3,r} \simeq \mathbb{F}_{p^r}$. Now in the following theorem, we provide an enumeration formula for all self-dual codes of length n over $\mathcal{R}_{3,r}$.

Theorem 3.3.5. *The number $\mathcal{M}_3(n)$ of distinct self-dual codes of length n over $\mathcal{R}_{3,r}$ is given by*

$$\mathcal{M}_3(n) = \begin{cases} 2\prod\limits_{i=1}^{\frac{n}{2}-1}(p^{ri}+1)\left(\sum\limits_{k_1=0}^{\frac{n}{2}}\begin{bmatrix}\frac{n}{2}\\ k_1\end{bmatrix}_{p^r} p^{\frac{rk_1(n-2)}{2}}\right) & \text{if } n \text{ is even and } (-1)^{\frac{n}{2}} \text{ is a square in } \overline{\mathcal{R}}_{3,r};\\ 0 & \text{otherwise.}\end{cases}$$

Proof. It follows immediately from Theorem 3.3.4. □

Remark 3.3.1. *Theorem 1 of Betty et al. [13] and Theorem 4.1 of Nagata et al. [76] follow from Theorem 3.3.5 as special cases.*

In the following section, we will consider the case $e \geq 4$ and count all self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,r}$. Towards this, we will first provide a recursive method to construct a self-orthogonal (*resp.* self-dual) code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ from a self-orthogonal (*resp.* self-dual) code of the type $\{k_1+k_2, k_3, \ldots, k_{e-1}\}$ and of the same length n over $\mathcal{R}_{e-2,r}$, and vice versa. With the help of this recursive method, we will derive a recurrence relation between the number $\mathcal{N}_e(n;k_1,k_2,\ldots,k_e)$ (*resp.* $\mathcal{M}_e(n;k_1,k_2,\ldots,k_e)$) and the number $\mathcal{N}_{e-2}(n;k_1+k_2,k_3,\ldots,k_{e-1})$ (*resp.* $\mathcal{M}_{e-2}(n;k_1+k_2,k_3,\ldots,k_{e-1})$). By repeatedly applying this recurrence relation, we will express the number $\mathcal{N}_e(n;k_1,k_2,\ldots,k_e)$ (*resp.* $\mathcal{M}_e(n;k_1,k_2,\ldots,k_e)$) in terms of the number $\mathcal{N}_2(n;k_1+k_2+\cdots+k_{\frac{e}{2}},k_{\frac{e}{2}+1})$ (*resp.* $\mathcal{M}_2(n;k_1+k_2+\cdots+k_{\frac{e}{2}},k_{\frac{e}{2}+1})$) when e is even and in terms of the number $\mathcal{N}_3(n;k_1+k_2+\cdots+k_{\frac{e-1}{2}},k_{\frac{e+1}{2}},k_{\frac{e+3}{2}})$ (*resp.* $\mathcal{M}_3(n;k_1+k_2+\cdots+k_{\frac{e-1}{2}},k_{\frac{e+1}{2}},k_{\frac{e+3}{2}})$) when e is odd. We will further apply Theorems 3.2.2 and 3.3.2(b) to explicitly determine the numbers $\mathcal{N}_e(n)$ and $\mathcal{M}_e(n)$.

3.4 Enumeration of self-orthogonal and self-dual codes over the chain ring $\mathcal{R}_{e,r}$, where $e \geq 4$

Throughout this section, we assume that $e \geq 4$. Here we first observe that the quotient ring $\mathcal{R}_{e,r}/\langle u^{e-2}\rangle$ is a finite commutative chain ring with the unique maximal ideal $\langle u+\langle u^{e-2}\rangle\rangle$, whose nilpotency index is $e-2$. From this point on, we will denote the quotient ring $\mathcal{R}_{e,r}/\langle u^{e-2}\rangle$ by $\mathcal{R}_{e-2,r}$ for our convenience. Further, for each element $a \in \mathcal{R}_{e,r}$, we will denote the corresponding element $a+\langle u^{e-2}\rangle \in \mathcal{R}_{e-2,r}$ by a itself for the sake of simplicity, and we will perform addition and multiplication in $\mathcal{R}_{e-2,r}$ modulo u^{e-2}. In view of this, we can assume, without any loss of generality, that the chain ring $\mathcal{R}_{e-2,r}$ has maximal ideal $\langle u\rangle$, where the element u has nilpotency index $e-2$ in $\mathcal{R}_{e-2,r}$. In particular, we can view the Teichm*ü*ller set $\mathcal{T}_{e,r}=\{0,1,\xi,\xi^2,\ldots,\xi^{p^r-2}\}$ of $\mathcal{R}_{e,r}$ as the Teichmüller set of $\mathcal{R}_{e-2,r}$. From this and by Theorem 2.1.4(d), we can assume that each element $a \in \mathcal{R}_{e-2,r}$ can be uniquely expressed as $a=a_0+a_1u+a_2u^2+\cdots+a_{e-3}u^{e-3}$, where $a_0,a_1,a_2,\ldots,a_{e-3} \in \mathcal{T}_{e,r}$. Under this assumption, it is easy to see that $\overline{\mathcal{R}}_{e,r}=\overline{\mathcal{R}}_{e-2,r}=\{0,1,\overline{\xi},\overline{\xi}^2,\ldots,\overline{\xi}^{p^r-2}\}$.

Next, we make the following observation:

Remark 3.4.1. *Assume that $\mathcal{C}$ is a self-orthogonal code of length n over $\mathcal{R}_{e,r}$ with a generator matrix G in the standard form (2.2.1). Here by Lemma 2.2.1(b), we note that $Tor_e(\mathcal{C}) \subseteq Tor_1(\mathcal{C})^{\perp}$. Further, by (2.2.2), we obtain the following system* *of matrix equations over $\overline{\mathcal{R}}_{e,r}$:*

$$I_{k_1} + \sum_{i=1}^{e} \overline{A}_{1,i}\overline{A}_{1,i}^{t} = 0 \quad \textit{and} \quad \overline{A}_{1,\ell} + \sum_{j=\ell+1}^{e} \overline{A}_{1,j}\overline{A}_{\ell+1,j}^{t} = 0 \ \textit{for } 1 \leq \ell \leq e-1.$$

Now using the above matrix equations, one can easily observe that there exists a matrix $\overline{C}_e \in \mathcal{M}_{k_{e+1}\times k_1}(\overline{\mathcal{R}}_{e,r})$ satisfying $\overline{A}_{1,e}\overline{C}_e = I_{k_1}$, which implies that the matrix $\overline{A}_{1,e}$ is of full-row rank.

By Theorem 2.2.2, we see that every linear code $\mathcal{C}$ of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$ is permutation equivalent to a code with a generator matrix in the standard form (2.2.1). On combining the last two blocks of the columns of the matrix (2.2.1), we may assume that the code $\mathcal{C}$ is permutation equivalent to a code whose generator matrix is in the following standard form

$$G = \begin{bmatrix} T_1 \\ uT_2 \\ u^2T_3 \\ \vdots \\ u^{e-2}T_{e-1} \\ u^{e-1}T_e \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} & \cdots & A_{1,e-2} & A'_{1,e} \\ 0 & uI_{k_2} & uA_{2,2} & \cdots & uA_{2,e-2} & uA'_{2,e} \\ 0 & 0 & u^2I_{k_3} & \cdots & u^2A_{3,e-2} & u^2A'_{3,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u^{e-2}I_{k_{e-1}} & u^{e-2}A'_{e-1,e} \\ 0 & 0 & 0 & \cdots & 0 & u^{e-1}A'_{e,e} \end{bmatrix}, \qquad (3.4.1)$$

where the columns of the matrix G are grouped into blocks of sizes k_1, k_2, $\ldots$, k_{e-1}, $k_e + k_{e+1}$, the matrix I_{k_i} is the $k_i \times \ k_i$ identity matrix over $\mathcal{R}_{e,r}$, the matrix $A_{i,j} \in \mathcal{M}_{k_i\times k_{j+1}}(\mathcal{R}_{e,r})$ is considered modulo u^{j-i+1} for $1 \leq i \leq j \leq e-2$, $A'_{\ell,e} \in \mathcal{M}_{k_\ell\times(k_e+k_{e+1})}(\mathcal{R}_{e,r})$ for $1 \leq \ell \leq e$ and the matrix $\overline{A}'_{e,e} \in \mathcal{M}_{k_e\times(k_e+k_{e+1})}(\overline{\mathcal{R}}_{e,r})$ is of full row-rank.

In the following theorem, we derive a recurrence relation between the numbers $\mathcal{N}_e(n; k_1, k_2, \ldots, k_{e-1}, k_e)$ and $\mathcal{N}_{e-2}(n; k_1+k_2, k_3, \ldots, k_{e-1})$. The proof of this theorem also provides a recursive method to construct a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ from a self-orthogonal code of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and of the same length n over $\mathcal{R}_{e-2,r}$, and vice versa.

Theorem 3.4.1. *Let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} +$*

$k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. The following hold.

(a) There exists a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$ if and only if there exists a self-orthogonal code of the type $\{k_1 + k_2, k_3, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$.

(b) Moreover, each self-orthogonal code of the type $\{k_1 + k_2, k_3, k_4, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$ gives rise to precisely

$$\begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)}$$

distinct self-orthogonal codes of the type $\{k_1, k_2, k_3, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$.

(c) We have

$$\mathcal{N}_e(n; k_1, k_2, \ldots, k_e) = \mathcal{N}_{e-2}(n; k_1 + k_2, k_3, \ldots, k_{e-1})(p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)} \times \begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r}.$$

Proof. To prove the result, let $\mathcal{C}$ be a self-orthogonal code of the type $\{k_1, k_2, k_3, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$. Without any loss of generality, suppose that the matrix G, as defined by (3.4.1), is a generator matrix of the code $\mathcal{C}$. Now consider a linear code $\widehat{\mathcal{C}}$ of length n over $\mathcal{R}_{e-2,r}$ with a generator matrix

$$\begin{bmatrix} L_1 \\ L_2 \\ uL_3 \\ \vdots \\ u^{e-3}L_{e-1} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} & A_{1,3} & \cdots & A_{1,e-2} & A'_{1,e} \\ 0 & I_{k_2} & A_{2,2} & A_{2,3} & \cdots & A_{2,e-2} & A'_{2,e} \\ 0 & 0 & uI_{k_3} & uA_{3,3} & \cdots & uA_{3,e-2} & uA''_{3,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^{e-3}I_{k_{e-1}} & u^{e-3}A''_{e-1,e} \end{bmatrix},$$

where I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathcal{R}_{e-2,r}$ and $A''_{j,e} \equiv A'_{j,e} \pmod{u^{e-j}}$ for $3 \leq j \leq e-1$. Since $\mathcal{C}$ is a self-orthogonal code over $\mathcal{R}_{e,r}$, we see, by Theorem 2.2.4, that $T_i T_j^t \equiv 0 \pmod{u^{e-i-j+2}}$ for all integers i and j satisfying $1 \leq i \leq j \leq e$ and $i + j \leq e + 1$. This implies that $L_1 L_1^t \equiv 0 \pmod{u^{e-2}}$, $L_1 L_\ell^t \equiv 0 \pmod{u^{e-\ell}}$ for

$2 \leq \ell \leq e-1$ and $L_i L_j^t \equiv 0 \pmod{u^{e-i-j+2}}$ for $2 \leq i \leq j \leq e-1$ and $i+j \leq e+1$. Now by applying Theorem 2.2.4 again and noting that the dimension of the Torsion code $Tor_1(\widehat{\mathcal{C}})$ over $\overline{\mathcal{R}}_{e-2,r}$ is k_1+k_2, we see that the code $\widehat{\mathcal{C}}$ is a self-orthogonal code of the type $\{k_1+k_2, k_3, k_4, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$.

On the other hand, let $\widehat{\mathcal{D}}$ be a self-orthogonal code of the type $\{k_1+k_2, k_3, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$. We first note that $Tor_1(\widehat{\mathcal{D}})$ has dimension k_1+k_2 over $\overline{\mathcal{R}}_{e-2,r}$, and we choose a k_1-dimensional subspace $\mathcal{D}_1$ of $Tor_1(\widehat{\mathcal{D}})$, which can be chosen in precisely

$$\begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r}$$

distinct ways, by Theorem 2.3.9. Now we will construct a self-orthogonal code $\mathcal{D}$ of the type $\{k_1, k_2, k_3, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ such that $Tor_1(\mathcal{D}) = \mathcal{D}_1$ and $Tor_{i+1}(\mathcal{D}) = Tor_i(\widehat{\mathcal{D}})$ for $1 \leq i \leq e-2$.

For this, we suppose, without any loss of generality, that the code $\widehat{\mathcal{D}}$ has a generator matrix of the form

$$\mathcal{H}_1 = \begin{bmatrix} \mathcal{S}_1'' \\ \mathcal{S}_2 \\ u\mathcal{S}_3 \\ \vdots \\ u^{e-3}\mathcal{S}_{e-1} \end{bmatrix} = \begin{bmatrix} I_{k_1} & Y_{1,1} & Y_{1,2}'' & Y_{1,3}'' & \cdots & Y_{1,e-2}'' & Y_{1,e}'' \\ 0 & I_{k_2} & Y_{2,2} & Y_{2,3} & \cdots & Y_{2,e-2} & Y_{2,e} \\ 0 & 0 & uI_{k_3} & uY_{3,3} & \cdots & uY_{3,e-2} & uY_{3,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^{e-3}I_{k_{e-1}} & u^{e-3}Y_{e-1,e} \end{bmatrix},$$

where the columns of the matrix $\mathcal{H}_1$ are grouped into blocks of sizes k_1, k_2, $\ldots$, k_{e-1}, $k_e+k_{e+1} = n-(k_1+k_2+\cdots+k_{e-1})$, the matrix I_{k_i} is the $k_i \times\ k_i$ identity matrix over $\mathcal{R}_{e-2,r}$, the matrix $Y_{1,1} \in \mathcal{M}_{k_1\times k_2}(\mathcal{R}_{e-2,r})$ is considered modulo u, the matrix $Y_{1,\ell}'' \in \mathcal{M}_{k_1\times k_{\ell+1}}(\mathcal{R}_{e-2,r})$ is considered modulo $u^{\ell-1}$ for $2 \leq \ell \leq e-2$, the matrix $Y_{1,e}'' \in \mathcal{M}_{k_1\times(k_e+k_{e+1})}(\mathcal{R}_{e-2,r})$ is considered modulo u^{e-2}, the matrix $Y_{a,e} \in \mathcal{M}_{k_a\times(k_e+k_{e+1})}(\mathcal{R}_{e-2,r})$ is considered modulo u^{e-a} for $2 \leq a \leq e-1$ and the matrix $Y_{i,j} \in \mathcal{M}_{k_i\times k_{j+1}}(\mathcal{R}_{e-2,r})$ is considered modulo u^{j-i+1} for $2 \leq i \leq j \leq e-2$.

Next, we choose the matrices $B_{1,j} \in \mathcal{M}_{k_1\times k_{j+1}}(\mathcal{T}_{e,r})$ for $2 \leq j \leq e-2$, arbitrarily. Now for given choices of matrices $B_{1,2}, B_{1,3}, \ldots, B_{1,e-2}$, we apply elementary row operations and observe that the code $\widehat{\mathcal{D}}$ can also be generated by the matrix of the form

$$\mathcal{H}_2 = \begin{bmatrix} \mathcal{S}_1' \\ \mathcal{S}_2 \\ u\mathcal{S}_3 \\ \vdots \\ u^{e-3}\mathcal{S}_{e-1} \end{bmatrix} = \begin{bmatrix} I_{k_1} & Y_{1,1} & Y_{1,2} & Y_{1,3}' & \cdots & Y_{1,e-2}' & Y_{1,e}' \\ 0 & I_{k_2} & Y_{2,2} & Y_{2,3} & \cdots & Y_{2,e-2} & Y_{2,e} \\ 0 & 0 & uI_{k_3} & uY_{3,3} & \cdots & uY_{3,e-2} & \gamma Y_{3,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^{e-3}I_{k_{e-1}} & u^{e-3}Y_{e-1,e} \end{bmatrix},$$

where $Y_{1,2} = Y_{1,2}'' + uB_{1,2}$, the matrix $Y_{1,\ell}' = Y_{1,\ell}'' + \sum\limits_{k=2}^{\ell-1} u^{k-1}B_{1,k}Y_{k+1,\ell} + u^{\ell-1}B_{1,\ell}$ for $3 \leq \ell \leq e-2$ and $Y_{1,e}' = Y_{1,e}'' + \sum\limits_{k=2}^{e-2} u^{k-1}B_{1,k}Y_{k+1,e}$. We further apply elementary row operations and observe that the code $\widehat{\mathcal{D}}$ can also be generated by the matrix

$$\mathcal{H} = \begin{bmatrix} \mathcal{S}_1 \\ \mathcal{S}_2 \\ u\mathcal{S}_3 \\ \vdots \\ u^{e-3}\mathcal{S}_{e-1} \end{bmatrix} = \begin{bmatrix} I_{k_1} & Y_{1,1} & Y_{1,2} & Y_{1,3} & \cdots & Y_{1,e-2} & Y_{1,e} \\ 0 & I_{k_2} & Y_{2,2} & Y_{2,3} & \cdots & Y_{2,e-2} & Y_{2,e} \\ 0 & 0 & uI_{k_3} & uY_{3,3} & \cdots & uY_{3,e-2} & uY_{3,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^{e-3}I_{k_{e-1}} & u^{e-3}Y_{e-1,e} \end{bmatrix},$$

where the matrix $Y_{1,j} \in \mathcal{M}_{k_1 \times k_{j+1}}(\mathcal{R}_{e-2,r})$ is considered modulo u^j for $3 \leq j \leq e-2$. We next view the matrix $\mathcal{H}$ over $\mathcal{R}_{e,r}$, and we will now construct a generator matrix for a self-orthogonal code over $\mathcal{R}_{e,r}$ from the matrix $\mathcal{H}$. For this, let us define

$$\begin{aligned} T_1 &\equiv \mathcal{S}_1 + u^{e-2}[0\ 0\ \cdots 0\ C_{1,e}] + u^{e-1}[0\ 0\ \cdots\ 0\ B_{1,e}] \pmod{u^e}, \\ T_j &\equiv \mathcal{S}_j + u^{e-j}[0\ 0\ \cdots\ 0\ B_{j,e}] \pmod{u^{e-j+1}} \text{ for } 2 \leq j \leq e-1, \\ T_e &\equiv [0\ 0\ \cdots\ 0\ Y_{e,e}] \pmod{u}, \end{aligned}$$

where the matrices $C_{1,e} \in \mathcal{M}_{k_1 \times (k_e+k_{e+1})}(\mathcal{T}_{e,r})$, $Y_{e,e} \in \mathcal{M}_{k_e \times (k_e+k_{e+1})}(\mathcal{T}_{e,r})$ and $B_{j,e} \in \mathcal{M}_{k_j \times (k_e+k_{e+1})}(\mathcal{T}_{e,r})$ for $1 \leq j \leq e-1$ are to be chosen suitably. Now let $\mathcal{D}$ be a linear code of length n over $\mathcal{R}_{e,r}$ generated by the following matrix over $\mathcal{R}_{e,r}$:

$$G' = \begin{bmatrix} T_1 \\ uT_2 \\ \vdots \\ u^{e-2}T_{e-1} \\ u^{e-1}T_e \end{bmatrix} = \begin{bmatrix} I_{k_1} & Y_{1,1} & Y_{1,2} & \cdots & Y_{1,e-2} & Y_{1,e} + u^{e-2}C_{1,e} + u^{e-1}B_{1,e} \\ 0 & uI_{k_2} & uY_{2,2} & \cdots & uY_{2,e-2} & u(Y_{2,e} + u^{e-2}B_{2,e}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & u^{e-2}I_{k_{e-1}} & u^{e-2}(Y_{e-1,e} + uB_{e-1,e}) \\ 0 & 0 & 0 & \cdots & 0 & u^{e-1}Y_{e,e} \end{bmatrix}.$$

We will show that there exist matrices $C_{1,e} \in \mathcal{M}_{k_1\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$, $B_{j,e} \in \mathcal{M}_{k_j\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ for $1 \leq j \leq e-1$ and $Y_{e,e} \in \mathcal{M}_{k_e\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ such that the code $\mathcal{D}$ is a self-orthogonal code of length n over $\mathcal{R}_{e,r}$, and we will also count the choices for these matrices that give rise to distinct self-orthogonal codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$. By Theorem 2.2.4, we observe that the matrix G' generates a self-orthogonal code over $\mathcal{R}_{e,r}$ if and only if there exist matrices $C_{1,e} \in \mathcal{M}_{k_1\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$, $B_{j,e} \in \mathcal{M}_{k_j\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ for $1 \leq j \leq e-1$ and $Y_{e,e} \in \mathcal{M}_{k_e\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ such that $\overline{Y}_{e,e}$ is a full-row rank matrix over $\overline{\mathcal{R}}_{e,r}$ and satisfying

$$T_iT_j^t \equiv 0 \pmod{u^{e-i-j+2}}$$

for all integers i and j satisfying $1 \leq i \leq j \leq e$ and $i + j \leq e + 1$.

As $\widehat{\mathcal{D}}$ is a self-orthogonal code of length n over $\mathcal{R}_{e-2,r}$, by Theorem 2.2.4, we see that

$$\begin{aligned} \mathcal{S}_1\mathcal{S}_1^t &\equiv 0 \pmod{u^{e-2}}, \\ \mathcal{S}_1\mathcal{S}_j^t &\equiv 0 \pmod{u^{e-j}} \ \text{ for } 2 \leq j \leq e-1, \\ \mathcal{S}_i\mathcal{S}_j^t &\equiv 0 \pmod{u^{e-i-j+2}} \ \text{ for } 2 \leq i \leq j \leq e-1 \text{ and } i+j \leq e+1, \quad (3.4.2) \end{aligned}$$

which implies that

$$\begin{aligned} \mathcal{S}_1\mathcal{S}_1^t &\equiv u^{e-2}J_1 + u^{e-1}J_2 \pmod{u^e}, & (3.4.3) \\ \mathcal{S}_1\mathcal{S}_2^t &\equiv u^{e-2}J_4 \pmod{u^{e-1}}, & (3.4.4) \\ \mathcal{S}_1\mathcal{S}_j^t &\equiv u^{e-j}P_j \pmod{u^{e-j+1}} \ \text{ for } 3 \leq j \leq e-1, & (3.4.5) \\ \mathcal{S}_i\mathcal{S}_j^t &\equiv 0 \pmod{u^{e-i-j+2}} \ \text{ for } 2 \leq i \leq j \leq e-1 \text{ and } i+j \leq e+1, & (3.4.6) \end{aligned}$$

where $J_1, J_2 \in Sym_{k_1}(\mathcal{T}_{e,r})$, $J_4 \in \mathcal{M}_{k_1\times k_2}(\mathcal{T}_{e,r})$ and $P_j \in \mathcal{M}_{k_1\times k_j}(\mathcal{T}_{e,r})$ for $3 \leq j \leq e-1$.

For all integers i and j satisfying $2 \leq i \leq j \leq e-1$ and $i+j \leq e+1$, by (3.4.2), we have $\mathcal{S}_i\mathcal{S}_j^t \equiv 0 \pmod{u^{e-i-j+2}}$, which implies that $T_iT_j^t \equiv 0 \pmod{u^{e-i-j+2}}$. Now it remains to show that there exist matrices $C_{1,e} \in \mathcal{M}_{k_1\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$, $B_{j,e} \in \mathcal{M}_{k_j\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ for $1 \leq j \leq e-1$ and $Y_{e,e} \in \mathcal{M}_{k_e\times(k_e+k_{e+1})}(\mathcal{T}_{e,r})$ such that $\overline{Y}_{e,e}$ is a full-row rank matrix over $\overline{\mathcal{R}}_{e,r}$ and

$$\begin{aligned} T_1T_1^t &\equiv 0 \pmod{u^e}, \\ T_1T_j^t &\equiv 0 \pmod{u^{e-j+1}} \ \text{ for } \ 2 \leq j \leq e-1, \\ T_1T_e^t &\equiv 0 \pmod{u}, \end{aligned}$$

which is equivalent to saying that

$$\begin{aligned} \mathcal{S}_1\mathcal{S}_1^t + u^{e-2}(Y_{1,e}C_{1,e}^t + C_{1,e}Y_{1,e}^t) & \\ +u^{e-1}(Y_{1,e}B_{1,e}^t + B_{1,e}Y_{1,e}^t) &\equiv 0 \pmod{u^e}, \quad (3.4.7)\\ \mathcal{S}_1\mathcal{S}_2^t + u^{e-2}(C_{1,e}Y_{2,e}^t + Y_{1,e}B_{2,e}^t) &\equiv 0 \pmod{u^{e-1}}, \quad (3.4.8)\\ \mathcal{S}_1\mathcal{S}_j^t + Y_{1,e}B_{j,e}^t &\equiv 0 \pmod{u^{e-j+1}} \text{ for } 3 \leq j \leq e-1, \quad (3.4.9)\\ Y_{1,e}Y_{e,e}^t &\equiv 0 \pmod{u}. \quad (3.4.10) \end{aligned}$$

To prove the existence of the matrix $Y_{e,e}$ over $\mathcal{T}_{e,r}$, we first observe that as the map $^{-}\restriction_{\mathcal{T}_{e,r}} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection, choosing a matrix $Y_{e,e}$ over $\mathcal{T}_{e,r}$ such that $\overline{Y}_{e,e}$ is a full-row rank matrix over $\overline{\mathcal{R}}_{e,r}$ and $Y_{1,e}Y_{e,e}^t \equiv 0 \pmod{u}$ is equivalent to choosing a full row-rank matrix $\overline{Y}_{e,e}$ over $\overline{\mathcal{R}}_{e,r}$ satisfying $\overline{Y}_{1,e}\overline{Y}_{e,e}^t = 0$. Further, since $\widehat{\mathcal{D}}$ is a self-orthogonal code over $\mathcal{R}_{e-2,r}$, the Torsion codes $Tor_i(\widehat{\mathcal{D}})$, $1 \leq i \leq e-2$, of the code $\widehat{\mathcal{D}}$ satisfy Lemma 2.2.1, which implies that the Torsion codes $Tor_i(\mathcal{D})$, $1 \leq i \leq e-1$, of the code $\mathcal{D}$ also satisfy Lemma 2.2.1. So we need to choose the matrix $\overline{Y}_{e,e}$ in such a way that the Torsion code $Tor_e(\mathcal{D})$ satisfies the relation $Tor_{e-1}(\mathcal{D}) \subseteq Tor_e(\mathcal{D}) \subseteq Tor_1(\mathcal{D})^{\perp}$. Further, for a given choice of $Tor_{e-1}(\mathcal{D})$, by Theorem 2.3.9, there are precisely $\begin{bmatrix} k_e+k_{e+1}-k_1 \\ k_e \end{bmatrix}_{p^r}$ choices for the code $Tor_e(\mathcal{D})$, and hence the matrix $Y_{e,e}$ has precisely $\begin{bmatrix} k_e+k_{e+1}-k_1 \\ k_e \end{bmatrix}_{p^r}$ relevant choices.

Next by Remark 3.4.1, we see that the matrix $\overline{Y}_{1,e}$ is of full row-rank over $\overline{\mathcal{R}}_{e,r}$.

Now for a given choice of the matrix $Y_{e,e}$ such that $\overline{Y}_{e,e}$ is of full row-rank and satisfying $Y_{1,e}Y_{e,e}^t \equiv 0 \pmod{u}$, we shall count the number of choices of the matrices $C_{1,e}$ and $B_{1,e}$ over $\mathcal{T}_{e,r}$ satisfying (3.4.7). By (3.4.3), we have

$$J_1 + Y_{1,e}C_{1,e}^t + C_{1,e}Y_{1,e}^t + u(J_2 + Y_{1,e}B_{1,e}^t + B_{1,e}Y_{1,e}^t) \equiv 0 \pmod{u^2}. \tag{3.4.11}$$

For this, we first determine the number of possible choices of the matrix $\overline{C}_{1,e}$ over $\overline{\mathcal{R}}_{e,r}$ satisfying

$$\overline{Y}_{1,e}\overline{C}_{1,e}^t + \overline{C}_{1,e}\overline{Y}_{1,e}^t = -\overline{J}_1. \tag{3.4.12}$$

Since $\overline{J}_1 \in Sym_{k_1}(\overline{\mathcal{R}}_{e,r})$, the matrix $\overline{Y}_{1,e}$ is of full row-rank and $^{-}\restriction_{\mathcal{T}_{e,r}} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection, by Lemma 2.1.1, we see that the matrix $C_{1,e}$ satisfying (3.4.12) has precisely

$$|\text{Ker } \Phi_{\overline{Y}_{1,e}}| = (p^r)^{\frac{k_1(2k_e+2k_{e+1}-k_1-1)}{2}}$$

distinct choices. So for a given choice of the matrix $C_{1,e}$ satisfying (3.4.12), we have

$$J_1 + Y_{1,e}C_{1,e}^t + C_{1,e}Y_{1,e}^t \equiv uJ_3 \pmod{u^2}$$

for some $J_3 \in Sym_{k_1}(\mathcal{T}_{e,r})$. Now on substituting this in (3.4.11), we obtain

$$J_2 + J_3 + Y_{1,e}B_{1,e}^t + B_{1,e}Y_{1,e}^t \equiv 0 \pmod{u}. \tag{3.4.13}$$

Further, we note that the number of choices of the matrix $B_{1,e}$ over $\mathcal{T}_{e,r}$ satisfying (3.4.13) is equal to the number of choices of the matrix $\overline{B}_{1,e}$ over $\overline{\mathcal{R}}_{e,r}$ satisfying

$$\overline{Y}_{1,e}\overline{B}_{1,e}^t + \overline{B}_{1,e}\overline{Y}_{1,e}^t = -(\overline{J}_2 + \overline{J}_3). \tag{3.4.14}$$

Since $\overline{J}_2$, $\overline{J}_3 \in Sym_{k_1}(\overline{\mathcal{R}}_{e,r})$ and the matrix $\overline{Y}_{1,e}$ is of full row-rank, by applying Lemma 2.1.1 again, the matrix $\overline{B}_{1,e}$ satisfying (3.4.14) has

$$|\text{Ker } \Phi_{\overline{Y}_{1,e}}| = (p^r)^{\frac{k_1(2k_e+2k_{e+1}-k_1-1)}{2}}$$

relevant choices. Next we count the number of possible choices of the matrix $B_{2,e}$

over $\mathcal{T}_{e,r}$ satisfying (3.4.8). By (3.4.4), we have

$$J_4 + C_{1,e}Y_{2,e}^t + Y_{1,e}B_{2,e}^t \equiv 0 \pmod{u}. \tag{3.4.15}$$

Now the number of choices of the matrix $B_{2,e}$ over $\mathcal{T}_{e,r}$ satisfying (3.4.15) is equal to the number of choices of the matrix $\overline{B}_{2,e}$ over $\overline{\mathcal{R}}_{e,r}$ satisfying

$$\overline{Y}_{1,e}\overline{B}_{2,e}^t = -(\overline{J}_4 + \overline{C}_{1,e}\overline{Y}_{2,e}^t). \tag{3.4.16}$$

To count the number of choices of the matrix $\overline{B}_{2,e}$, let $\overline{Y}_{1,e} = (\mathbf{a}_i)$ and $\overline{B}_{2,e} = (\mathbf{x}_j)$, where $\mathbf{a}_i$'s and $\mathbf{x}_j$'s are the rows of the matrices $\overline{Y}_{1,e}$ and $\overline{B}_{2,e}$, respectively. Moreover, let us suppose that $-(\overline{J}_4 + \overline{C}_{1,e}\overline{Y}_{2,e}^t) = (m_{ij})$, where m_{ij} denotes the (i,j)-th entry of the matrix $-(\overline{J}_4 + \overline{C}_{1,e}\overline{Y}_{2,e}^t)$ for $1 \leq i \leq k_1$ and $1 \leq j \leq k_2$. In view of this, the matrix equation (3.4.16) is equivalent to the following system of equations over $\overline{\mathcal{R}}_{e,r}$:

$$\mathbf{a}_i \cdot \mathbf{x}_j = m_{ij} \quad \text{for } 1 \leq i \leq k_1 \text{ and } 1 \leq j \leq k_2.$$

Since the matrix $\overline{Y}_{1,e}$ is of full-row rank, the number of possible choices of $\overline{B}_{2,e}$ satisfying (3.4.16) is given by $(p^r)^{k_2(k_e+k_{e+1}-k_1)}$.

Further, for $3 \leq j \leq e-1$, we count the number of possible choices of the matrix $B_{j,e}$ over $\mathcal{T}_{e,r}$ satisfying (3.4.9). By (3.4.5), we obtain

$$P_j + Y_{1,e}B_{j,e}^t \equiv 0 \pmod{u}. \tag{3.4.17}$$

Now the number of choices of the matrix $B_{j,e}$ over $\mathcal{T}_{e,r}$ satisfying (3.4.17) is equal to the number of choices of the matrix $\overline{B}_{j,e}$ over $\overline{\mathcal{R}}_{e,r}$ satisfying

$$\overline{Y}_{1,e}\overline{B}_{j,e}^t = -\overline{P}_j. \tag{3.4.18}$$

Since the matrix $\overline{Y}_{1,e}$ is of full-row rank, the number of possible choices of $\overline{B}_{j,e}$ satisfying (3.4.18) is equal to

$$(p^r)^{k_j(k_e+k_{e+1}-k_1)}$$

for $3 \leq j \leq e-1$. Hence for given choices of the matrices $C_{1,e}$ and $B_{1,e}$ satisfying (3.4.11), $B_{2,e}$ satisfying (3.4.15) and $B_{j,e}$ satisfying (3.4.17) for $3 \leq j \leq e-1$, we get a self-orthogonal code $\mathcal{D}$ over $\mathcal{R}_{e,r}$.

Further, let us define

$$G'' = \begin{bmatrix} I_{k_1} & Y_{1,1} & Y_{1,2} & Y_{1,3} & \cdots & Y_{1,e-2} & Y_{1,e} + u^{e-2}C'_{1,e} + u^{e-1}B'_{1,e} \\ 0 & uI_{k_2} & uY_{2,2} & uY_{2,3} & \cdots & uY_{2,e-2} & u(Y_{2,e} + u^{e-2}B'_{2,e}) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & u^{e-2}I_{k_{e-1}} & u^{e-2}(Y_{e-1,e} + uB'_{e-1,e}) \\ 0 & 0 & 0 & 0 & \cdots & 0 & u^{e-1}Y_{e,e} \end{bmatrix},$$

where $C'_{1,e}$, $B'_{1,e} \in \mathcal{M}_{k_1 \times (k_e+k_{e+1})}(\mathcal{T}_{e,r})$, $B'_{j,e} \in \mathcal{M}_{k_j \times (k_e+k_{e+1})}(\mathcal{T}_{e,r})$ for $2 \leq j \leq e-1$. One can easily observe that the matrices G' and G'' generate the same code $\mathcal{D}$ over $\mathcal{R}_{e,r}$ if and only if $C_{1,e} = C'_{1,e}$ and $B'_{j,e} \equiv B_{j,e} + K_jY_{e,e} \pmod{u}$, where $K_j \in \mathcal{M}_{k_j \times k_e}(\mathcal{T}_{e,r})$ for $1 \leq j \leq e-1$.

In view of the above, one can easily observe that each self-orthogonal code of the type $\{k_1+k_2, k_3, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$ gives rise to precisely

$$\begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e+k_{e+1}-k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{i=3}^{e-1} k_1k_i + k_1(2k_e+2k_{e+1}-k_1-1) + \sum\limits_{j=2}^{e-1} k_j(k_e+k_{e+1}-k_1) - \sum\limits_{\ell=1}^{e-1} k_\ell k_e}$$
$$= \begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e+k_{e+1}-k_1 \\ k_e \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1) + \sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)}$$

distinct self-orthogonal codes of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$.

From this, the desired result follows immediately. □

From now on, let us define

$$s = \left\lfloor \frac{e}{2} \right\rfloor.$$

Next, let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$. We further define $n_0 = 0$ and $n_i = k_1 + k_2 + \cdots + k_i$ for $1 \leq i \leq e+1$. Here we note, by Remark 2.2.1, that if there exists a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$, then we must have $n_{e-i+1} + n_i \leq n$ for $s+1 \leq i \leq e$. In the following theorem, we count all self-orthogonal codes of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$, where $e \geq 4$ is an integer.

Theorem 3.4.2. *Let $e \geq 4$ be an integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$.*

(a) When e is even, we have

$$\mathcal{N}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{p^r}(n, n_s) \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} \prod\limits_{j=s+1}^{e} \begin{bmatrix} k_j + n - n_j - n_{e-j+1} \\ k_j \end{bmatrix}_{p^r} \\ \times (p^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(n-n_{\ell+1}-1)+n_{s+\ell}(n-n_{s+1+\ell}-n_{s-\ell})+n_s(n-n_{s+1})-\frac{n_s(n_s+1)}{2}} \\ \textit{if } n_{e-i+1} + n_i \leq n \textit{ for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathcal{N}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{p^r}(n, n_{s+1}) \prod\limits_{i=1}^{s+1} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} \prod\limits_{j=s+2}^{e} \begin{bmatrix} k_j + n - n_j - n_{e-j+1} \\ k_j \end{bmatrix}_{p^r} \\ \times (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(n-n_{\ell+1}-1)+n_{s+\ell}(n-n_{s+1+\ell}-n_{s+1-\ell})} \\ \textit{if } n_{e-i+1} + n_i \leq n \textit{ for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

Proof. By Remark 2.2.1, we note that $\mathcal{N}_e(n; k_1, k_2, \ldots, k_e) = 0$ if $n_{e-i+1} + n_i > n$ for some integer i satisfying $s + 1 \leq i \leq e$.

On the other hand, when $n_{e-i+1} + n_i \leq n$ for $s + 1 \leq i \leq e$, we see, by repeatedly applying Theorem 3.4.1(c), that

$$\mathcal{N}_e(n; k_1, k_2, \ldots, k_e) = \mathcal{N}_{e-2}(n; k_1 + k_2, k_3, \ldots, k_{e-1})(p^r)^{k_1(n-k_1-k_2-1)+\sum\limits_{i=1}^{e-1} k_i(k_{e+1}-k_1)} \\ \times \begin{bmatrix} k_1 + k_2 \\ k_1 \end{bmatrix}_{p^r} \begin{bmatrix} k_e + k_{e+1} - k_1 \\ k_e \end{bmatrix}_{p^r}$$

$$= \begin{cases} \mathcal{N}_2\big(n; n_s, k_{s+1}\big)\,(p^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(n-n_{\ell+1}-1)+n_{s+\ell}(n-n_{s+1+\ell}-n_{s-\ell})} & \\ \times \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} \prod\limits_{j=s+2}^{e} \begin{bmatrix} k_j+n-n_j-n_{e-j+1} \\ k_j \end{bmatrix}_{p^r} & \text{if } e \text{ is even;} \\ \mathcal{N}_3\big(n; n_s, k_{s+1}, k_{s+2}\big)\,(p^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(n-n_{\ell+1}-1)+\sum\limits_{a=s+2}^{e-1} n_a(n-n_{a+1}-n_{e-a})} & \\ \times \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} \prod\limits_{j=s+3}^{e} \begin{bmatrix} k_j+n-n_j-n_{e-j+1} \\ k_j \end{bmatrix}_{p^r} & \text{if } e \text{ is odd.} \end{cases}$$

From this and by applying Theorems 3.2.2 and 3.3.2(b), the desired result follows immediately. □

In the following theorem, we derive a recurrence relation between the numbers $\mathcal{M}_e(n; k_1, k_2, \ldots, k_{e-1}, k_e)$ and $\mathcal{M}_{e-2}(n; k_1+k_2, k_3, \ldots, k_{e-1})$, where $e \geq 4$ is an integer. The proof of this theorem also provides a recursive method to construct a self-dual code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$ from a self-dual code of the type $\{k_1+k_2, k_3, \ldots, k_{e-1}\}$ and of the same length n over $\mathcal{R}_{e-2,r}$, and vice versa.

Theorem 3.4.3. *For an integer $e \geq 4$, let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $k_j = k_{e-j+2}$ for $1 \leq j \leq e+1$. The following hold.*

(a) There exists a self-dual code of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over $\mathcal{R}_{e,r}$ if and only if there exists a self-dual code of the type $\{k_1+k_2, k_3, k_4, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$. In fact, each self-dual code of the type $\{k_1+k_2, k_3, k_4, \ldots, k_{e-1}\}$ and length n over $\mathcal{R}_{e-2,r}$ gives rise to precisely

$$\begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)}$$

distinct self-dual codes of the type $\{k_1, k_2, k_3, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$.

(b) We have

$$\mathcal{M}_e(n; k_1, k_2, \ldots, k_e) = \mathcal{M}_{e-2}(n; k_1+k_2, k_3, \ldots, k_{e-1}) \begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)}.$$

Proof. Part (a) follows immediately from Theorems 2.2.4 and 3.4.1, while part (b) follows from part (a). □

In the following theorem, we count all self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathcal{R}_{e,r}$.

Theorem 3.4.4. *Let $e \geq 4$ be an integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$.*

(a) When e is even, we have

$$\mathcal{M}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{p^r}(n, n_s) \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(n-n_{\ell+1}-1) - \frac{n_s(n_s-1)}{2}} \\ \textit{if } k_j = k_{e-j+2} \ \textit{ for } \ 1 \leq j \leq e+1; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathcal{M}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} 2 \prod\limits_{b=1}^{\frac{n}{2}-1} (p^{rb}+1) \prod\limits_{i=1}^{s+1} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(n-n_{\ell+1}-1)} \\ \textit{if } n \textit{ is even, } (-1)^{\frac{n}{2}} \textit{ is a square in } \overline{\mathcal{R}}_{e,r} \textit{ and} \\ k_j = k_{e-j+2} \textit{ for } 1 \leq j \leq e+1; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

Proof. (a) By Theorem 2.2.4(b), we note that $\mathcal{M}_e(n; k_1, k_2, \ldots, k_e) = 0$ if $k_j \neq k_{e-j+2}$ for some integer j satisfying $1 \leq j \leq e+1$.

On the other hand, when $k_j = k_{e-j+2}$ for $1 \leq j \leq e+1$, we see, by repeatedly applying Theorem 3.4.3(b), that

$$\mathcal{M}_e(n; k_1, k_2, \ldots, k_e) = \mathcal{M}_{e-2}(n; k_1+k_2, k_3, \ldots, k_{e-1}) \begin{bmatrix} k_1+k_2 \\ k_1 \end{bmatrix}_{p^r} (p^r)^{k_1(n-k_1-k_2-1)}$$

$$= \mathcal{M}_2\big(n; n_s, k_{s+1}\big) \prod_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(n-n_{\ell+1}-1)}.$$

Now by applying Theorem 3.2.4(b), the desired result follows immediately.

(b) By Theorem 2.2.4(b) again, we note that $\mathcal{M}_e(n;k_1,k_2,\ldots,k_e)=0$ if either $k_j\neq k_{e-j+2}$ for some integer j satisfying $1\leq j\leq e+1$ or n is odd.

When $k_j=k_{e-j+2}$ for $1\leq j\leq e+1$ and n is even, we see, by repeatedly applying Theorem 3.4.3(b), that

$$\mathcal{M}_e(n;k_1,k_2,\ldots,k_e)=\mathcal{M}_{e-2}(n;k_1{+}k_2,k_3,\ldots,k_{e-1})\begin{bmatrix}k_1+k_2\\k_1\end{bmatrix}_{p^r}(p^r)^{k_1(n-k_1-k_2-1)}$$

$$=\mathcal{M}_3\big(n;n_s,k_{s+1},k_{s+1}\big)\prod_{i=1}^{s}\begin{bmatrix}n_i\\k_i\end{bmatrix}_{p^r}(p^r)^{\sum\limits_{\ell=1}^{s-1}n_\ell(n-n_{\ell+1}-1)}.$$

Now by applying Theorem 3.3.4(b), the desired result follows immediately. By Theorem 3.3.4(b), we note that $\mathcal{M}_e(n;k_1,k_2,\ldots,k_{e-1},k_e)=0$ when n is even and $(-1)^{\frac{n}{2}}$ is not a square in $\overline{\mathcal{R}}_{e,r}$.

□

Remark 3.4.2. *Theorem 1 of Nagata et al. [77] follows from Theorem 3.4.4 as a special case.*

Now for an integer d satisfying $2\leq d\leq e$ and for non-negative integers $k_1,k_2,\ldots,k_d$, let us define

$$h_\ell(k_1,k_2,\ldots,k_d)=(k_1+k_2+\cdots+k_\ell)\big(n-(k_1+k_2+\cdots+k_{\ell+1})-1\big)\quad\text{for } 1\leq\ell\leq d-1, \tag{3.4.19}$$

and let us define

$$m_j(k_1,k_2,\ldots,k_d)=h_j(k_1,k_2,\ldots,k_d)+(k_1+k_2+\cdots+k_{\lfloor\frac{d}{2}\rfloor+j})\big(n-(k_1+k_2+\cdots+k_{\lceil\frac{d+1}{2}\rceil+j})-(k_1+k_2+\cdots+k_{\lfloor\frac{d+1}{2}\rfloor-j})\big) \tag{3.4.20}$$

for $1\leq j\leq\lfloor\frac{d}{2}\rfloor-\beta$, where $\beta=1$ if e is even, while $\beta=0$ if e is odd.

In the following theorem, we provide the enumeration formula for all self-orthogonal codes of length n over $\mathcal{R}_{e,r}$.

Theorem 3.4.5. *(a) When e is even, we have*

$$\begin{aligned}\mathcal{N}_e(n)\;&=\;\sum\sigma_{p^r}\left(n,k_1+k_2+\cdots+k_s\right)(p^r)^{\sum\limits_{\ell=1}^{s-1}m_\ell(k_1,k_2,\ldots,k_e)+\Theta_e(k_1,k_2,\ldots,k_e)}\\&\quad\times\prod_{j=s+1}^{e}\begin{bmatrix}k_j+n-(k_1+k_2+\cdots+k_j)-(k_1+k_2+\cdots+k_{e-j+1})\\k_j\end{bmatrix}_{p^r}\end{aligned}$$

$$\times \prod_{i=1}^{s} \begin{bmatrix} k_1 + k_2 + \cdots + k_i \\ k_i \end{bmatrix}_{p^r},$$

where $\Theta_e(k_1, k_2, \ldots, k_e) = (k_1+k_2+\cdots+k_s)\left(\frac{2n-2(k_1+k_2+\cdots+k_{s+1})-(k_1+k_2+\cdots+k_s)-1}{2}\right)$ *and the summation* $\sum$ *runs over all non-negative integers* $k_1, k_2, \ldots, k_e$ *satisfying* $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ *for* $s+1 \leq i \leq e$.

(b) When e is odd, we have

$$\mathcal{N}_e(n) = \sum \sigma_{p^r}\big(n, k_1 + k_2 + \cdots + k_{s+1}\big)(p^r)^{\sum\limits_{\ell=1}^{s} m_\ell(k_1,k_2,\ldots,k_e)} \prod_{i=1}^{s+1} \begin{bmatrix} k_1 + k_2 + \cdots + k_i \\ k_i \end{bmatrix}_{p^r}$$
$$\times \prod_{j=s+2}^{e} \begin{bmatrix} k_j + n - (k_1 + k_2 + \cdots + k_j) - (k_1 + k_2 + \cdots + k_{e-j+1}) \\ k_j \end{bmatrix}_{p^r},$$

where the summation $\sum$ *runs over all non-negative integers* $k_1, k_2, \ldots, k_e$ *satisfying* $2k_1+2k_2+\cdots+2k_{e-i+1}+k_{e-i+2}+k_{e-i+3}+\cdots+k_i \leq n$ *for* $s+1 \leq i \leq e$.

Proof. It follows immediately from Theorem 3.4.2. □

In the following theorem, we provide the enumeration formula for all self-dual codes of length n over $\mathcal{R}_{e,r}$.

Theorem 3.4.6. *(a) When e is even, we have*

$$\mathcal{M}_e(n) = \sum \sigma_{p^r}(n, k_1 + k_2 + \cdots + k_s) \prod_{i=1}^{s} \begin{bmatrix} k_1 + k_2 + \cdots + k_i \\ k_i \end{bmatrix}_{p^r}$$
$$\times (p^r)^{\sum\limits_{\ell=1}^{s-1} h_\ell(k_1,k_2,\ldots,k_s)+\lambda_e(k_1,k_2,\ldots,k_s)},$$

where the summation $\sum$ *runs over all non-negative integers* $k_1, k_2, \ldots, k_{s+1}$ *satisfying* $2(k_1 + k_2 + \cdots + k_s) + k_{s+1} = n$ *and the number* $\lambda_e(k_1, k_2, \ldots, k_s)$ *is given by*

$$\lambda_e(k_1, k_2, \ldots, k_s) = (k_1 + k_2 + \cdots + k_s)\left(\frac{k_1 + k_2 + \cdots + k_s - 1}{2}\right).$$

(b) When e is odd, we have

$$\mathcal{M}_e(n)=\begin{cases}\sum 2\prod\limits_{b=1}^{\frac{n}{2}-1}(p^{rb}+1)(p^r)^{\sum\limits_{\ell=1}^{s}h_\ell(k_1,k_2,\ldots,k_s)}\prod\limits_{i=1}^{s+1}\begin{bmatrix}k_1+k_2+\cdots+k_i\\ k_i\end{bmatrix}_{p^r}\\ \textit{if } n \textit{ is even and } (-1)^{\frac{n}{2}} \textit{ is a square in } \overline{\mathcal{R}}_{e,r};\\ 0 \qquad \textit{otherwise,}\end{cases}$$

where the summation $\sum$ runs over all non-negative integers $k_1,k_2,\ldots,k_{s+1}$ satisfying $2(k_1+k_2+\cdots+k_{s+1})=n$.

Proof. It follows immediately from Theorem 3.4.4. □

The enumeration formulae for $\mathcal{N}_e(n)$ and $\mathcal{M}_e(n)$ are useful in the classification of self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,r}$, respectively. We illustrate the same in the following section by classifying all self-orthogonal and self-dual codes of lengths $2,3,4$ and 5 over $\mathbb{F}_5[u]/\langle u^2\rangle$ and of lengths $2,3$ and 4 over $\mathbb{F}_7[u]/\langle u^2\rangle$.

3.5 Classification of self-orthogonal and self-dual codes

Two self-orthogonal (*resp.* self-dual) codes of length n over $\mathcal{R}_{e,r}$ are said to be equivalent if one code can be obtained from the other by a combination of operations of the following two types:

(A) Permutation of the n coordinate positions of the code.

(B) Multiplication of the code symbols appearing in a given coordinate position by the element $-1\in\mathcal{T}_{e,r}$.

Otherwise, the codes are said to be inequivalent.

Next, let $\mathcal{E}_n$ be the group generated by transformations of the types (A) and (B) as defined above. If $\mathcal{C}$ is a self-orthogonal (*resp.* self-dual) code of length n over $\mathcal{R}_{e,r}$, then by Theorem 7.4 of [46], we note that the number of distinct self-orthogonal (*resp.* self-dual) codes of length n over $\mathcal{R}_{e,r}$ that are equivalent to the code $\mathcal{C}$ is given by $\frac{|\mathcal{E}_n|}{|\mathcal{A}\mathrm{ut}(\mathcal{C})|}$, where $\mathcal{A}\mathrm{ut}(\mathcal{C})(\subseteq\mathcal{E}_n)$ is the automorphism group of the code $\mathcal{C}$. In view of this, we see that the total number $\mathcal{N}_e(n)$ of distinct self-orthogonal codes of length n over $\mathcal{R}_{e,r}$ can be expressed as

$$\mathcal{N}_e(n) = \sum_{\mathcal{C}} \frac{|\mathcal{E}_n|}{|\mathcal{A}\mathrm{ut}(\mathcal{C})|}, \tag{3.5.1}$$

where the summation $\sum\limits_{\mathcal{C}}$ runs over all the inequivalent self-orthogonal codes $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$. Analogously, the total number $\mathcal{M}_e(n)$ of distinct self-dual codes of length n over $\mathcal{R}_{e,r}$ can be expressed as

$$\mathcal{M}_e(n) = \sum_{\mathcal{C}} \frac{|\mathcal{E}_n|}{|\mathcal{A}\mathrm{ut}(\mathcal{C})|}, \tag{3.5.2}$$

where the summation $\sum\limits_{\mathcal{C}}$ runs over all the inequivalent self-dual codes $\mathcal{C}$ of length n over $\mathcal{R}_{e,r}$. The mass formulae (3.5.1) and (3.5.2) are useful in the determination of complete lists of inequivalent self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,r}$, respectively (cf. [13], [53, Sec. 9.6 and 9.7]). To illustrate this, we will classify all self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over $\mathbb{F}_5[u]/\langle u^2\rangle$ and of lengths $2, 3$ and 4 over $\mathbb{F}_7[u]/\langle u^2\rangle$ up to equivalence, by carrying out computations in the Magma Computational Algebra System and by applying the classification algorithm that has been used in most of the earlier classification attempts ([53, Sec. 9.6 and 9.7]). We also explicitly determine a generator matrix of the code representative for each equivalence class of self-orthogonal and self-dual codes.

I. There are precisely 5 inequivalent non-zero self-orthogonal codes of length 2 over $\mathbb{F}_5[u]/\langle u^2\rangle$ with generator matrices uI_2, $\begin{bmatrix} 1 & 2 \end{bmatrix}$, $\begin{bmatrix} u & 0 \end{bmatrix}$, $\begin{bmatrix} u & u \end{bmatrix}$ and $\begin{bmatrix} u & 2u \end{bmatrix}$.

II. There are precisely 14 inequivalent non-zero self-orthogonal codes of length 3 over $\mathbb{F}_5[u]/\langle u^2\rangle$ with generator matrices uI_3, $\begin{bmatrix} 1 & 0 & 2 \end{bmatrix}$, $\begin{bmatrix} 1 & u & 2 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & u & u \end{bmatrix}$, $\begin{bmatrix} u & 2u & u \end{bmatrix}$, $\begin{bmatrix} u & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 3u \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 2 \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & u \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 2u \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 4u \\ 0 & u & 2u \end{bmatrix}$ and $\begin{bmatrix} u & 0 & 4u \\ 0 & u & u \end{bmatrix}$.

III. There are precisely 63 inequivalent non-zero self-orthogonal codes of length 4 over $\mathbb{F}_5[u]/\langle u^2\rangle$, whose generator matrices are as listed below:

- $\begin{bmatrix}1 & xu & yu & 2\end{bmatrix}$ with $(x,y)\in\big\{(0,0),(1,1),(1,2),(0,2)\big\}$;

- $\begin{bmatrix}1 & xu+1 & yu+2 & zu+2\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(1,0,2),(1,3,4),$ $(0,3,2),(2,4,0)\big\}$;

- $\begin{bmatrix}1 & 0 & xu & 2\\ 0 & u & yu & 0\end{bmatrix}$ with $(x,y)\in\big\{(0,0),(1,0),(0,1),(1,1),(0,2),(1,2)\big\}$;

- $\begin{bmatrix}1 & 1 & xu+2 & yu+2\\ 0 & u & zu & wu\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,2),(1,4,0,2),(2,3,0,2),$ $(0,0,1,1),(1,4,1,1),(3,2,1,1),(0,0,3,4),(1,4,3,4)\big\}$;

- uI_4, $\begin{bmatrix}1 & 0 & 0 & 2\\ 0 & 1 & 2 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & 2\\ 0 & 1 & 2 & 4u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 2\\ 0 & u & 0 & 0\\ 0 & 0 & u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1 & 2 & 2\\ 0 & u & 0 & 2u\\ 0 & 0 & u & 4u\end{bmatrix}$;

- $\begin{bmatrix}u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(1,0,0),(1,1,0),(1,1,1),(2,3,4),$ $(1,2,4),(2,1,0),(2,0,0)\big\}$;

- $\begin{bmatrix}u & 0 & xu & yu\\ 0 & u & zu & wu\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(1,0,0,0),(1,1,0,0),(3,0,2,0),$ $(0,3,1,2),(1,0,0,1),(4,0,2,1),(3,4,2,1),(1,0,0,2),(0,0,0,2),(0,0,1,2),$ $(4,2,1,2),(4,2,2,2),(4,2,2,1),(4,4,4,0),(4,2,4,1),(2,0,0,2),(1,0,1,0)\big\}$;

- $\begin{bmatrix}u & 0 & 0 & xu\\ 0 & u & 0 & yu\\ 0 & 0 & u & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(1,0,0),(4,1,0),(2,0,0),(3,1,0),$ $(1,4,1),(4,4,3),(2,4,3)\big\}$.

IV. There are precisely 321 inequivalent non-zero self-orthogonal codes of length 5 over $\mathbb{F}_5[u]/\langle u^2\rangle$, whose generator matrices are as listed below:

- $\begin{bmatrix}1 & xu & yu & zu & 2\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,0,1),(0,1,1),(0,1,2),(1,1,1),$ $(1,1,2)\big\}$;

- $\begin{bmatrix}1 & xu & yu+1 & zu+2 & wu+2\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(0,0,1,4),$

$(0,0,2,3),(0,1,0,2),(0,1,3,4),(0,2,0,4),(3,0,2,3),(1,0,0,0),(1,0,1,4),$
$(1,0,2,3),(1,1,0,2),(1,1,1,1),(1,1,3,4),(1,2,0,4),(1,2,1,3)\big\}$;

- $\begin{bmatrix}1 & xu+1 & yu+1 & zu+1 & wu+1\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(0,0,1,4),$
$(0,0,2,3),(0,1,1,3),(0,1,2,2),(1,2,3,4)\big\}$;

- $\begin{bmatrix}1 & 0 & xu & yu & 2\\ 0 & u & zu & wu & 0\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(0,1,0,0),(1,1,0,0),(1,2,0,0),$
$(4,2,0,1),(0,0,0,1),(0,1,0,1),(1,0,0,1),(1,1,0,1),(4,2,1,1),(0,0,1,1),$
$(0,1,1,1),(0,0,0,2),(0,0,1,2),(0,1,0,2),(0,1,1,2),(0,1,2,0),(0,1,2,1),$
$(1,1,4,3),(1,1,0,2),(1,1,1,3)\big\}$;

- $\begin{bmatrix}1 & 0 & 1 & 2 & 2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),(1,3,4),$
$(2,1,3)\big\}$;

- $\begin{bmatrix}1 & 0 & 1 & u+2 & 4u+2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),$
$(1,1,1),(1,3,4),(2,0,4),(2,1,3),(3,3,3)\big\}$;

- $\begin{bmatrix}1 & 0 & 1 & 2u+2 & 3u+2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),$
$(1,1,1),(1,3,4),(2,0,4),(2,1,3),(2,2,2)\big\}$;

- $\begin{bmatrix}1 & 0 & u+1 & 2 & 2u+2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),$
$(1,2,0),(1,3,4),(2,1,3)\big\}$;

- $\begin{bmatrix}1 & 0 & u+1 & 3u+2 & 4u+2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),$
$(1,1,1),(1,2,0),(1,4,3),(1,3,4),(2,0,4),(2,1,3),(2,2,2),(2,3,1),(2,4,0)\big\}$;

- $\begin{bmatrix}1 & 0 & 2u+1 & 2 & 4u+2\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,1,4),(0,2,3),(1,0,2),$
$(1,2,0),(1,3,4),(2,1,3)\big\}$;

- $\begin{bmatrix}1 & 1 & 1 & 1 & 1\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,4),(0,1,3),(2,3,4)\big\}$;

- $\begin{bmatrix}1 & 1 & 1 & u+1 & 4u+1\\ 0 & u & xu & yu & zu\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,4),(0,1,3),(0,2,2),(0,4,0),$ $(2,0,2),(2,1,1),(2,3,4)\big\}$;

- $\begin{bmatrix}1 & 1 & xu+1 & yu+1 & 3u+1\\ 0 & u & zu & wu & au\end{bmatrix}$ with $(x,y,z,w,a)\in\big\{(0,2,0,0,4),(0,2,0,4,0),$ $(0,2,2,0,2),(0,2,2,1,1),(1,1,0,2,2),(1,1,2,4,3)\big\}$;

- $\begin{bmatrix}1 & 3 & 1 & 3 & xu\\ 0 & u & yu & zu & wu\end{bmatrix}$ with $(x,y,z,w)\in\big\{(1,0,4,0),(1,1,2,0),(1,2,0,0),(1,4,1,0),$ $(0,0,4,0),(0,1,2,0),(0,2,0,0)\big\}$;

- $\begin{bmatrix}1 & 3 & u+1 & 3u+3 & xu\\ 0 & u & yu & zu & wu\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,4,0),(0,1,2,0),(0,2,0,0),$ $(1,0,4,0),(1,1,2,0),(1,3,3,0),(1,4,1,0),(1,2,0,0)\big\}$;

- $\begin{bmatrix}1 & 3 & 3u+1 & 4u+3 & xu\\ 0 & u & yu & zu & wu\end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,2,0,0),(1,2,0,0),(1,0,4,0)\big\}$;

- uI_5, $\begin{bmatrix}1 & 1 & 1 & 1 & 1\\ 0 & 1 & u+2 & 3u+3 & u+4\end{bmatrix}$, $\begin{bmatrix}1 & 3 & 2u+1 & u+3 & xu\\ 0 & u & 4u & u & 0\end{bmatrix}$ with $x\in\big\{0,1\big\}$;

- $\begin{bmatrix}1 & 1 & u+1 & 2u+1 & 2u+1\\ 0 & u & 3u & 2u & 4u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 0 & 2\\ 0 & u & 0 & 0 & 0\\ 0 & 0 & u & 0 & 0\\ 0 & 0 & 0 & u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 2 & 2\\ 0 & u & 0 & 0 & 0\\ 0 & 0 & u & 0 & 2u\\ 0 & 0 & 0 & u & 4u\end{bmatrix}$, $\begin{bmatrix}1 & 1 & 1 & 1 & 1\\ 0 & u & 0 & 0 & 4u\\ 0 & 0 & u & u & 3u\\ 0 & 0 & 0 & u & 4u\end{bmatrix}$;

- $\begin{bmatrix}1 & 0 & 0 & xu & 2\\ 0 & u & 0 & yu & 0\\ 0 & 0 & u & zu & 0\end{bmatrix}$ with $(x,y,z)\in\big\{(0,0,0),(0,0,1),(0,0,2),(1,0,0),(1,0,1),(1,0,2),$ $(3,1,1),(4,1,2),(0,1,3),(0,1,1)\big\}$;

- $\begin{bmatrix} 1 & 0 & 1 & xu+2 & yu+2 \\ 0 & u & 0 & zu & wu \\ 0 & 0 & u & vu & au \end{bmatrix}$ with $(x,y,z,w,v,a) \in \big\{(0,0,0,0,0,2),(0,0,0,0,1,1),$ $(0,0,0,0,3,4),(0,0,1,4,3,4),(0,0,1,4,0,2),(0,0,1,4,1,1),(1,4,1,4,0,2),$ $(0,0,2,3,1,1),(0,0,2,3,3,4),(1,4,0,0,2,0),(1,4,0,0,1,1),(1,4,0,0,3,4),$ $(1,4,1,4,4,3),(1,4,1,4,1,1),(1,4,2,3,3,4),(1,4,2,3,1,1),(2,3,0,0,2,0),$ $(2,3,0,0,1,1),(2,3,1,4,1,1),(2,3,1,4,0,2),(2,3,2,3,1,1)\big\}$;

- $\begin{bmatrix} 1 & 1 & 1 & xu+1 & yu+1 \\ 0 & u & 0 & zu & wu \\ 0 & 0 & u & vu & au \end{bmatrix}$ with $(x,y,z,w,v,a) \in \big\{(0,0,0,4,1,3),(0,0,0,4,2,2),$ $(1,4,0,4,4,0),(1,4,0,4,0,4),(0,0,1,3,3,1),(2,3,0,4,1,3),(2,3,0,4,2,2),$ $(1,4,1,3,3,1)\big\}$;

- $\begin{bmatrix} 1 & 3 & 1 & 3 & xu \\ 0 & u & 0 & 4u & 0 \\ 0 & 0 & u & 3u & 0 \end{bmatrix}$ with $x \in \big\{0,1\big\}$;

- $\begin{bmatrix} u & xu & yu & zu & wu \end{bmatrix}$ with $(x,y,z,w) \in \big\{(0,0,0,2),(0,1,2,2),(1,1,1,1),$ $(0,0,0,0),(1,0,0,0),(1,1,0,0),(1,1,1,0),(2,1,1,0),(2,3,1,1),(2,3,3,3),$ $(2,1,0,0)\big\}$;

- $\begin{bmatrix} u & 0 & xu & yu & zu \\ 0 & u & wu & vu & au \end{bmatrix}$ with $(x,y,z,w,v,a) \in \big\{(0,0,0,0,0,0),(0,0,0,0,0,1),$ $(0,0,0,0,0,2),(0,0,0,0,1,1),(0,0,0,0,1,2),(0,0,0,1,1,1),(0,0,0,1,1,2),$ $(0,0,0,1,3,3),(0,0,1,4,3,1),(0,0,1,0,0,1),(0,0,1,0,0,2),(0,0,1,0,1,4),$ $(0,0,1,0,1,0),(0,0,1,0,1,2),(0,0,1,0,2,0),(0,0,1,0,2,1),(0,0,1,1,1,1),$ $(0,0,1,1,1,2),(0,0,1,1,2,0),(0,0,1,1,2,2),(0,0,1,1,4,0),(0,1,1,3,4,0),$ $(0,1,1,3,4,1),(0,1,1,4,2,1),(0,1,1,1,1,3),(0,1,1,1,2,0),(0,1,1,1,4,0),$ $(0,1,1,2,0,0),(0,1,1,0,4,3),(0,1,1,0,4,2),(0,1,1,0,3,3),(0,1,2,2,4,3),$ $(0,1,2,0,2,0),(0,1,2,0,2,1),(0,1,2,1,0,2),(0,1,2,1,1,1),(0,1,2,1,1,3),$ $(0,1,2,1,2,0),(0,1,2,1,2,1),(0,1,2,1,2,2),(0,1,2,2,0,0),(0,1,2,2,1,1),$

$(0,1,2,2,1,3),(2,3,2,0,0,2),(1,2,3,1,1,1),(1,2,2,1,3,4),(1,2,2,2,1,3),$ $(1,1,1,0,0,2),(0,0,2,3,0,0)\big\}$;

- $\begin{bmatrix} u & 0 & 0 & xu & yu \\ 0 & u & 0 & zu & wz \\ 0 & 0 & u & vu & au \end{bmatrix}$ with $(x,y,z,w,v,a)\in\big\{(0,0,0,0,0,0),(0,0,0,0,0,1),$ $(0,0,0,0,0,2),(0,0,0,0,1,1),(0,0,0,0,1,2),(0,0,0,1,4,4),(0,0,0,1,0,1),$ $(0,0,0,1,0,2),(0,0,0,1,1,0),(0,0,0,1,1,2),(0,0,0,1,2,0),(0,0,0,2,1,4),$ $(0,0,0,1,2,1),(0,0,0,2,2,3),(0,0,0,2,2,0),(0,0,1,1,1,2),(0,0,1,1,1,3),$ $(0,0,2,3,4,3),(0,1,2,0,4,4),(0,1,3,2,0,1),(0,1,3,3,0,2),(0,1,3,0,0,4),$ $(0,1,4,0,1,4),(0,1,4,2,1,1),(0,1,4,3,1,2),(0,1,1,4,3,3),(0,1,1,3,3,2),$ $(0,1,1,2,3,1),(0,1,0,1,4,4),(0,1,0,1,0,1),(0,1,0,1,0,2),(0,1,0,1,1,3),$ $(0,1,0,1,1,0),(0,1,0,2,4,3),(0,1,0,2,0,2),(0,1,0,2,1,4),(0,1,0,2,1,0),$ $(0,1,0,2,2,0),(0,1,1,4,4,4),(0,1,1,4,2,4),(0,1,1,0,2,2),(1,1,4,3,4,1),$ $(1,1,4,3,0,2),(1,1,4,3,2,4),(2,2,3,0,4,4),(2,2,1,4,0,2),(2,2,4,2,1,3),$ $(1,2,2,1,1,4),(1,2,2,1,2,3)\big\}$;

- $\begin{bmatrix} u & 0 & 0 & 0 & xu \\ 0 & u & 0 & 0 & yu \\ 0 & 0 & u & 0 & zu \\ 0 & 0 & 0 & u & wu \end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(0,0,0,1),(0,0,0,2),(0,0,1,4),$ $(0,0,1,2),(0,1,1,2),(0,1,2,3),(0,1,1,4),(1,1,1,2),(1,4,2,3),(1,4,1,1)\big\}$;

- $\begin{bmatrix} 1 & 0 & xu & yu & 2 \\ 0 & 1 & zu & 2 & wu \end{bmatrix}$ with $(x,y,z,w)\in\big\{(0,0,0,0),(0,0,1,0),(0,1,0,4),(0,1,1,4),$ $(1,0,1,0),(1,1,1,4),(1,1,2,4)\big\}$;

- $\begin{bmatrix} 1 & 0 & 1 & xu+2 & yu+2 \\ 0 & 1 & zu+2 & wu+1 & au+3 \end{bmatrix}$ with $(x,y,z,w,a)\in\big\{(0,0,0,0,0),(0,0,1,4,3),$ $(0,0,2,3,1),(1,4,0,4,2),(1,4,1,3,0),(1,4,2,2,3),(2,3,0,3,4),(2,3,2,1,0)\big\}$;

- $\begin{bmatrix} 1 & 0 & 0 & xu & 2 \\ 0 & 1 & 0 & 2 & yu \\ 0 & 0 & u & 0 & 0 \end{bmatrix}$ with $(x,y)\in\big\{(0,0),(1,4)\big\}$;

- $\begin{bmatrix} 1 & 0 & 1 & xu+2 & yu+2 \\ 0 & 1 & 2 & zu+1 & wu+3 \\ 0 & 0 & u & 4u & 3u \end{bmatrix}$ with $(x,y,z,w) \in \big\{(0,0,0,0),(1,4,4,2)\big\}$.

V. There are precisely 4 inequivalent non-zero self-orthogonal codes of length 2 over $\mathbb{F}_7[u]/\langle u^2\rangle$ with generator matrices uI_2, $\begin{bmatrix} u & 0 \end{bmatrix}$, $\begin{bmatrix} u & u \end{bmatrix}$ and $\begin{bmatrix} u & 2u \end{bmatrix}$.

VI. There are precisely 19 inequivalent non-zero self-orthogonal codes of length 3 over $\mathbb{F}_7[u]/\langle u^2\rangle$ with generator matrices uI_3, $\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$, $\begin{bmatrix} 1 & u+2 & 4u+3 \end{bmatrix}$, $\begin{bmatrix} 1 & 3u+2 & 5u+3 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 2u \end{bmatrix}$, $\begin{bmatrix} u & u & u \end{bmatrix}$, $\begin{bmatrix} u & u & 2u \end{bmatrix}$, $\begin{bmatrix} u & u & 3u \end{bmatrix}$, $\begin{bmatrix} u & 2u & 3u \end{bmatrix}$, $\begin{bmatrix} 1 & 2 & 3 \\ 0 & u & 4u \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \\ 0 & u & u \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \\ 0 & u & 2u \end{bmatrix}$, $\begin{bmatrix} u & 0 & u \\ 0 & u & u \end{bmatrix}$, $\begin{bmatrix} u & 0 & 2u \\ 0 & u & 3u \end{bmatrix}$, $\begin{bmatrix} u & 0 & u \\ 0 & u & 2u \end{bmatrix}$ and $\begin{bmatrix} u & 0 & u \\ 0 & u & 4u \end{bmatrix}$.

VII. There are precisely 118 inequivalent non-zero self-orthogonal codes of length 4 over $\mathbb{F}_7[u]/\langle u^2\rangle$, whose generator matrices are as listed below:

- $\begin{bmatrix} 1 & xu & yu+2 & zu+3 \end{bmatrix}$ with $(x,y,z) \in \big\{(0,0,0),(0,1,4),(0,3,5),(1,0,0),$ $(1,1,4),(1,2,1),(1,3,5),(1,5,6),(1,6,3),(3,2,1)\big\}$;

- $\begin{bmatrix} 1 & xu+1 & yu+1 & zu+2 \end{bmatrix}$ with $(x,y,z) \in \big\{(0,0,0),(0,1,3),(0,2,6),(0,3,2),$ $(0,4,5),(0,5,1),(0,6,4),(1,2,2),(1,3,5),(1,4,1),(1,5,4),(2,4,4)\big\}$;

- $\begin{bmatrix} 1 & 0 & xu+2 & yu+3 \\ 0 & u & zu & wu \end{bmatrix}$ with $(x,y,z,w) \in \big\{(0,0,0,0),(1,4,0,0),(3,5,0,0),$ $(0,0,1,4),(1,4,1,4),(3,5,1,4),(0,0,2,1),(1,4,2,1),(3,5,2,1),(0,0,3,5),$ $(1,4,3,5),(3,5,3,5)\big\}$;

- $\begin{bmatrix} 1 & 1 & xu+1 & yu+2 \\ 0 & u & zu & wu \end{bmatrix}$ with $(x,y,z,w) \in \big\{(0,0,0,3),(1,3,0,3),(2,6,0,3),$ $(3,2,0,3),(0,0,2,2),(1,3,2,2),(2,6,2,2),(3,2,2,2),(4,5,2,2),(5,1,2,2),$ $(6,4,2,2),(0,0,3,5),(1,3,3,5),(3,2,3,5)\big\}$;

- uI_4, $\begin{bmatrix} 1 & 5 & 4 & 0 \\ 0 & u & 4u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 5 & 4 & u \\ 0 & u & 4u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 2 & 3 \\ 0 & u & 0 & 0 \\ 0 & 0 & u & 4u \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & 1 & 2 \\ 0 & u & 0 & 3u \\ 0 & 0 & u & 3u \end{bmatrix}$;
- $\begin{bmatrix} u & xu & yu & zu \end{bmatrix}$ with $(x, y, z) \in \big\{(0,0,0), (1,0,0), (1,1,0), (1,1,1), (2,1,1), (2,2,1), (2,2,2), (2,3,1), (0,2,1), (0,2,0), (0,3,5), (0,3,6)\big\}$;
- $\begin{bmatrix} u & 0 & xu & yu \\ 0 & u & zu & wu \end{bmatrix}$ with $(x, y, z, w) \in \big\{(0,0,0,0), (0,1,0,0), (1,1,0,0), (2,0,0,0), (2,1,0,0), (2,2,0,0), (2,3,0,0), (6,1,1,0), (0,1,1,0), (1,0,1,0), (2,1,1,0), (2,0,1,0), (3,0,1,0), (3,1,1,0), (0,2,1,0), (2,0,1,1), (2,1,1,1), (3,1,1,1), (3,0,1,1), (3,4,1,1), (3,5,1,1), (0,1,2,1), (2,3,2,1), (2,4,2,1), (3,3,2,1), (3,2,2,1), (3,0,2,1), (4,2,2,1), (5,2,2,1), (5,0,2,2), (5,2,2,2), (0,1,2,2), (3,0,2,2), (3,1,2,2), (2,3,2,3), (3,5,2,3), (0,2,0,4), (2,0,0,4)\big\}$;
- $\begin{bmatrix} u & 0 & 0 & xu \\ 0 & u & 0 & yu \\ 0 & 0 & u & zu \end{bmatrix}$ with $(x, y, z) \in \big\{(0,0,0), (1,0,0), (2,0,0), (2,1,0), (1,1,0), (3,1,0), (3,6,1), (1,6,1), (2,6,1), (2,4,2), (1,4,3), (2,4,0)\big\}$;
- $\begin{bmatrix} 1 & 0 & xu+2 & yu+3 \\ 0 & 1 & zu+3 & wu+5 \end{bmatrix}$ with $(x, y, z, w) \in \big\{(0,0,0,0), (1,4,4,6), (5,6,6,2)\big\}$.

VIII. Next, by applying Theorem 3.2.4(a), we see that a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathbb{F}_q[u]/\langle u^2\rangle$ is self-dual if and only if $2k_1 + k_2 = n$. In view of this, we see that there are precisely 2 inequivalent self-dual codes of length 2, 2 inequivalent self-dual codes of length 3, 5 inequivalent self-dual codes of length 4 and 8 inequivalent self-dual codes of length 5 over $\mathbb{F}_5[u]/\langle u^2\rangle$. Moreover, we note that there is only one inequivalent self-dual code of length 2 over $\mathbb{F}_7[u]/\langle u^2\rangle$, while there are precisely 2 inequivalent self-dual codes of length 3 and 6 inequivalent self-dual codes of length 4 over $\mathbb{F}_7[u]/\langle u^2\rangle$.

As special cases, one can deduce enumeration formulae for all self-orthogonal and self-dual codes over quasi-Galois rings and Galois rings of odd characteristic from Theorems 3.2.3,3.2.5, 3.3.3, 3.3.5, 3.4.5 and 3.4.6. When $\mathcal{R}_{e,r}$ is a quasi-Galois ring or a Galois ring of even characteristic, we will observe, in Chapters 4 and 5, that each self-orthogonal (*resp.* self-dual) code over $\mathcal{R}_{e-2,r}$ can not be lifted to a self-orthogonal (*resp.* self-dual) code over $\mathcal{R}_{e,r}$ by employing the construction method given in the proof of Theorem 3.4.1 (see Examples 4.2.1 and 5.2.1). Thus, the enumeration technique employed here cannot be extended as it is to count self-orthogonal and self-dual codes over finite commutative chain rings of even characteristic. In Chapters 4 and 5, we shall obtain explicit enumeration formulae for self-orthogonal and self-dual codes of an arbitrary length over quasi-Galois rings and Galois rings of even characteristic, respectively.

4

Enumeration formulae for self-orthogonal and self-dual codes over quasi-Galois rings of even characteristic

4.1 Introduction

Recall that a quasi-Galois ring is a quotient ring of the form $\mathbb{F}_q[u]/\langle u^e\rangle$. It is easy to see that $\mathbb{F}_q[u]/\langle u^e\rangle$ is a finite commutative chain ring with the maximal ideal $\langle u\rangle$ of nilpotency index e and the residue field $\mathbb{F}_q$. One can easily see that the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^e\rangle$ is of even characteristic if and only if q is an even prime power. In this chapter, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over the quasi-Galois ring $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$ for each integer $e \geq 2$.

This chapter is organized as follows: In Section 4.2, we first outline the recursive construction method employed in Chapter 3 (see the proofs of Theorems 3.4.1 and 3.4.3) in the particular case of codes over the quasi-Galois ring $\mathbb{F}_q[u]/\langle u^\ell \rangle$, and we further note that when q is an even prime power, say $q = 2^r$, each self-orthogonal (*resp.* self-dual) code over $\mathbb{F}_{2^r}[u]/\langle u^{\ell-2} \rangle$ can not be lifted to a self-orthogonal (*resp.* self-dual) code over $\mathbb{F}_{2^r}[u]/\langle u^\ell \rangle$ by applying this construction method. We also derive a necessary and sufficient condition under which a self-orthogonal code over $\mathbb{F}_{2^r}[u]/\langle u^{\ell-2} \rangle$ can be lifted to a self-orthogonal code over $\mathbb{F}_{2^r}[u]/\langle u^\ell \rangle$ using this construction method, where $\ell \geq 4$ is an integer (Theorem 4.2.1). In Section 4.3, for a positive integer n and non-negative integers $k_1, k_2, \ldots, k_e$ satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$, we provide a modified recursive method to construct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathbb{F}_{2^r}[u]/\langle u^e \rangle$ from a self-orthogonal code of the same length n and dimension $k_1 + k_2 + \cdots + k_{\lceil \frac{e}{2} \rceil}$ over $\mathbb{F}_{2^r}$, and vice versa. In Section 4.4, we provide explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathbb{F}_{2^r}[u]/\langle u^e \rangle$ for each integer $e \geq 2$ by applying the modified recursive method (Theorems 4.4.3 and 4.4.4). In Section 4.5, with the help of the enumeration formulae obtained in Section 4.4 and by applying the classification algorithm, we obtain complete lists of inequivalent self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over the ring $\mathbb{F}_2[u]/\langle u^3 \rangle$ and of lengths $2, 3$ and 4 over the ring $\mathbb{F}_4[u]/\langle u^2 \rangle$.

Throughout this chapter, let p be a prime number and r be a positive integer. Let R_e denote the quasi-Galois ring $\mathbb{F}_{p^r}[u]/\langle u^e \rangle$, where $e \geq 2$ is an integer. Here we recall, from Chapter 2, that the quasi-Galois ring R_e is a finite commutative chain ring, all of whose ideals are given by $\{0\}$, R_e, $\langle u \rangle$, $\langle u^2 \rangle$,..., $\langle u^{e-1} \rangle$ and that $|\langle u^j \rangle| = (p^r)^{e-j}$ for $0 \leq j \leq e$. From this, it follows that the ideal $\langle u \rangle$ is the unique maximal ideal of R_e whose nilpotency index is e and that the quotient ring $R_e/\langle u \rangle \simeq \mathbb{F}_{p^r}$ is the finite field of order p^r. Further, we note, by Theorem 2.1.4(d), that each element $a \in R_e$ can be uniquely expressed as $a = a_0 + ua_1 + \cdots + u^{e-1}a_{e-1}$, where $a_0, a_1, \ldots, a_{e-1} \in \mathbb{F}_{p^r}$. Note that the element $a \in R_e$ is a unit in R_e if and only if $a_0 \neq 0$. It is easy to observe that each matrix $A \in \mathcal{M}_{m \times k}(R_e)$ can be uniquely expressed as $A = A_0 + uA_1 + \cdots + u^{e-1}A_{e-1}$, where $A_0, A_1, \ldots, A_{e-1} \in \mathcal{M}_{m\times k}(\mathbb{F}_{p^r})$. From this point on, let $[B]_\alpha$ denote the column block matrix whose ith block is the matrix $B_i \in \mathcal{M}_{k_i\times n}(\mathbb{F}_{p^r})$ for $1 \le i \le \alpha$.

In the following section, we will outline the recursive construction method employed in Chapter 3 in the particular case of codes over the quasi-Galois ring R_e and illustrate that not every self-orthogonal code over $R_{\ell-2}$ can be lifted to a self-orthogonal code over R_ℓ using this method in the case when $p = 2$, where $\ell \ge 4$ is an integer. We will also characterize all self-orthogonal (*resp.* self-dual) codes over $R_{\ell-2}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes over R_ℓ.

4.2 Outline of the recursive construction method

Throughout this section, let $\ell \ge 4$ be an integer, and let $\kappa_1, \kappa_2, \ldots, \kappa_{\ell+1}$ be non-negative integers satisfying $n = \kappa_1 + \kappa_2 + \cdots + \kappa_\ell + \kappa_{\ell+1}$ and $2\kappa_1 + 2\kappa_2 + \cdots + 2\kappa_{\ell-i+1} + \kappa_{\ell-i+2} + \kappa_{\ell-i+3} + \cdots + \kappa_i \le n$ for $\lceil \frac{\ell+1}{2} \rceil \le i \le \ell$. Here we observe that the map $\widehat{\ }: R_\ell \to R_{\ell-2}$, defined as $\widehat{a} = a_0 + ua_1 + \cdots + u^{\ell-3}a_{\ell-3}$ for all $a = a_0 + ua + \cdots + u^{\ell-1}a_{\ell-1} \in R_\ell$, is a canonical epimorphism from R_ℓ onto $R_{\ell-2}$. In fact, for each element $a = a_0 + ua_1 + \cdots + u^{\ell-1}a_{\ell-1} \in R_\ell$ with $a_0, a_1, \ldots, a_{\ell-1} \in \mathbb{F}_{p^r}$, there corresponds a unique element $\widehat{a} = a_0 + ua_1 + \cdots + u^{\ell-3}a_{\ell-3} \in R_{\ell-2}$.

Now let $\mathcal{C}_{\ell-2}$ be a linear code of the type $\{\kappa_1 + \kappa_2, \kappa_3, \ldots, \kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ with a generator matrix

$$G_{\ell-2} = \begin{bmatrix} T_1' \\ T_2' \\ uT_3' \\ \vdots \\ u^{\ell-3}T_{\ell-1}' \end{bmatrix}, \tag{4.2.1}$$

where

$$\begin{bmatrix} T_1' \\ T_2' \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & A_{1,2}^{(0)} & \cdots & A_{1,\ell-2}^{(0)} & A_{1,\ell}^{(0)} \\ 0 & I_{k_2} & A_{2,2}^{(0)} & \cdots & A_{2,\ell-2}^{(0)} & A_{2,\ell}^{(0)} \end{bmatrix} + \sum_{j=1}^{\ell-3} u^j \begin{bmatrix} U_1^{(j)} \\ U_2^{(j)} \end{bmatrix}$$

with I_{κ_i} as the $\kappa_i \times\ \kappa_i$ identity matrix over $\mathbb{F}_{p^r}$, $A_{i,j}^{(0)} \in \mathcal{M}_{\kappa_i\times\kappa_{j+1}}(\mathbb{F}_{p^r})$ for $1 \le i \le 2$ and $i \le j \le \ell - 2$, $A_{1,\ell}^{(0)} \in \mathcal{M}_{\kappa_1\times(\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $A_{2,\ell}^{(0)} \in \mathcal{M}_{\kappa_2\times(\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $[U^{(j)}]_2 \in$

$\mathcal{M}_{(\kappa_1+\kappa_2)\times n}(\mathbb{F}_{p^r})$ for $1 \leq j \leq \ell-3$, and the matrix $T'_y \in \mathcal{M}_{\kappa_y \times n}(R_{\ell-2})$ is of the form $T'_y = Z_y^{(0)} + uZ_y^{(1)} + \cdots + u^{\ell-y-1}Z_y^{(\ell-y-1)}$ with $Z_y^{(0)}, Z_y^{(1)}, \ldots, Z_y^{(\ell-y-1)} \in \mathcal{M}_{\kappa_y \times n}(\mathbb{F}_{p^r})$ for $3 \leq y \leq \ell-1$.

Next, let $\mathcal{C}_\ell$ be a linear code of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_{\ell-1}, \kappa_\ell\}$ and length n over R_ℓ with a generator matrix

$$G_\ell = \begin{bmatrix} T_1 \\ uT_2 \\ u^2T_3 \\ \vdots \\ u^{\ell-2}T_{\ell-1} \\ u^{\ell-1}T_\ell \end{bmatrix}, \tag{4.2.2}$$

where

$$T_1 = T'_1 + u^{\ell-2}\begin{bmatrix} 0 & \cdots & 0 & 0 & U_{1,\ell}^{(\ell-2)} \end{bmatrix} + u^{\ell-1}\begin{bmatrix} 0 & \cdots & 0 & 0 & U_{1,\ell}^{(\ell-1)} \end{bmatrix}$$

with $U_{1,\ell}^{(\ell-2)} \in \mathcal{M}_{\kappa_1 \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $U_{1,\ell}^{(\ell-1)} \in \mathcal{M}_{\kappa_1 \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, the matrix T_y is of the form

$$T_y = T'_y + u^{\ell-y}\begin{bmatrix} 0 \; 0 & \cdots & 0 & A_{y,\ell}^{(\ell-y)} \end{bmatrix} \text{ with } A_{y,\ell}^{(\ell-y)} \in \mathcal{M}_{\kappa_y \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$$

for $2 \leq y \leq \ell-1$, and the matrix T_ℓ is of the form

$$T_\ell = \begin{bmatrix} 0 & 0 & \cdots & 0 & A_{\ell,\ell}^{(0)} \end{bmatrix} \text{ with } A_{\ell,\ell}^{(0)} \in \mathcal{M}_{\kappa_\ell \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r}).$$

Now if the code $\mathcal{C}_\ell$ is self-orthogonal (*resp.* self-dual), then by Theorem 2.2.4(a), we see that the code $\mathcal{C}_{\ell-2}$ is also self-orthogonal (*resp.* self-dual). Conversely, if the code $\mathcal{C}_{\ell-2}$ is self-orthogonal (*resp.* self-dual), then the code $\mathcal{C}_\ell$ is self-orthogonal (*resp.* self-dual) if and only if there exist matrices $U_{1,\ell}^{(\ell-2)} \in \mathcal{M}_{\kappa_1 \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $U_{1,\ell}^{(\ell-1)} \in \mathcal{M}_{\kappa_1 \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $A_{y,\ell}^{(\ell-y)} \in \mathcal{M}_{\kappa_y \times (\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$ for $2 \leq y \leq \ell$, satisfying the following system of matrix equations over $\mathbb{F}_{p^r}$:

$$\left.\begin{aligned}
A^{(0)}_{1,\ell}U^{(\ell-2)t}_{1,\ell} + U^{(\ell-2)}_{1,\ell}A^{(0)t}_{1,\ell} &= -\sum_{i=1}^{\ell-3} U_1^{(j)}U_1^{(\ell-2-j)t}, \\
A^{(0)}_{1,\ell}U^{(\ell-1)t}_{1,\ell} + U_1^{(1)}\left[0 \ \cdots \ 0 \ U^{(\ell-2)}_{1,\ell}\right]^t & \\
+U^{(\ell-1)}_{1,\ell}A^{(0)t}_{1,\ell} + \left[0 \ \cdots \ 0 \ U^{(\ell-2)}_{1,\ell}\right]U_1^{(1)t} &= -\sum_{i=2}^{\ell-3} U_1^{(j)}U_1^{(\ell-1-j)t}, \\
A^{(0)}_{1,\ell}A^{(\ell-2)t}_{2,\ell} &= -\sum_{j=1}^{\ell-3} U_1^{(j)}U_2^{(\ell-2-j)t} + U^{(\ell-2)}_{1,\ell}A^{(0)t}_{2,\ell}, \\
A^{(0)}_{1,\ell}A^{(\ell-y)t}_{y,\ell} &= -\sum_{i=1}^{\ell-y} U_1^{(i)}Z_y^{(\ell-y-i)t} \ \text{ for } 3 \le y \le \ell-1, \\
A^{(0)}_{1,\ell}A^{(0)t}_{\ell,\ell} &= 0.
\end{aligned}\right\} \tag{4.2.3}$$

When p is an odd prime, working as in Theorem 3.4.1, we see that the system (4.2.3) of matrix equations has a solution, which implies that the code $\mathcal{C}_\ell$ is self-orthogonal (*resp.* self-dual), from which it follows that each self-orthogonal (*resp.* self-dual) code of the type $\{\kappa_1+\kappa_2, \kappa_3, \ldots, \kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ can be lifted to a self-orthogonal (*resp.* self-dual) code of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_\ell\}$ and length n over R_ℓ. On the other hand, when $p = 2$ (*i.e.*, $R_\ell = \mathbb{F}_{2^r}[u]/\langle u^\ell\rangle$), the system (4.2.3) of matrix equations need not have a solution, and hence every self-orthogonal (*resp.* self-dual) code of the type $\{\kappa_1+\kappa_2, \kappa_3, \ldots, \kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ can not be lifted to a self-orthogonal (*resp.* self-dual) code of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_\ell\}$ and length n over R_ℓ, which we illustrate in the following example.

Example 4.2.1. *Let $p = 2$, $r = 1$, $\ell = 4$, $n = 3$, $\kappa_1 = 1$ and $\kappa_2 = \kappa_3 = \kappa_4 = 0$. Here we have $R_4 = \mathbb{F}_2[u]/\langle u^4\rangle$ and $R_2 = \mathbb{F}_2[u]/\langle u^2\rangle$. Let $\mathcal{D}_2$ be a linear code of the type $\{1, 0\}$ and length 3 over R_2 with a generator matrix $G_2 = [1 \ \ 1 \ \ 0] + u[0 \ \ 1 \ \ 0]$. By Theorem 2.2.4(a), we see that the code $\mathcal{D}_2$ is a self-orthogonal code over R_2. Now consider the linear code $\mathcal{D}_4$ of the type $\{1, 0, 0, 0\}$ and length 3 over R_4 with a generator matrix*

$$[1 \ \ 1 \ \ 0] + u[0 \ \ 1 \ \ 0] + u^2[0 \ \ a \ \ c] + u^3[0 \ \ b \ \ d], \ \textit{where } a, b, c, d \in \mathbb{F}_2.$$

Note that corresponding to the codes $\mathcal{D}_2$ and $\mathcal{D}_4$, we have $A^{(0)}_{1,4} = [1 \ \ 0]$, $U_1^{(1)} = [0 \ \ 1 \ \ 0]$, $U^{(2)}_{1,4} = [a \ \ c]$ and $U^{(3)}_{1,4} = [b \ \ d]$, and one can observe that the resulting *system* (4.2.3) *of matrix equations has no solution. From this, it follows that the self-orthogonal code* $\mathcal{D}_2$ *can not be lifted to a self-orthogonal code of the type* $\{1,0,0,0\}$ *and length* 3 *over* R_4.

However, there are self-orthogonal codes of the type $\{\kappa_1+\kappa_2,\kappa_3,\ldots,\kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ that can be lifted to self-orthogonal codes of the type $\{\kappa_1,\kappa_2,\ldots,\kappa_\ell\}$ and of the same length n over R_ℓ. The following example illustrates this.

Example 4.2.2. *Let* $p=2$, $r=1$, $n=3$, $\ell=4$, $\kappa_1=1$ *and* $\kappa_2=\kappa_3=\kappa_4=0$. *Here we have* $R_4=\mathbb{F}_2[u]/\langle u^4\rangle$ *and* $R_2=\mathbb{F}_2[u]/\langle u^2\rangle$. *Let* $\mathcal{B}_2$ *be a linear code of the type* $\{1,0\}$ *and length* 3 *over* R_2 *with a generator matrix* $[1\ \ 1\ \ 0]+u[0\ \ 1\ \ 1]$. *By Theorem 2.2.4(a), we see that the code* $\mathcal{B}_2$ *is a self-orthogonal code over* R_2. *Now consider the linear code* $\mathcal{B}_4$ *of the type* $\{1,0,0,0\}$ *and length* 3 *over* R_4 *with a generator matrix*

$$[1\ \ 1\ \ 0]+u[0\ \ 1\ \ 1]+u^2[0\ \ a\ \ c]+u^3[0\ \ b\ \ d],\ \ \text{where } a,b,c,d\in\mathbb{F}_2.$$

Corresponding to the codes $\mathcal{B}_2$ *and* $\mathcal{B}_4$, *we have* $A_{1,4}^{(0)}=[1\ \ 0]$, $U_1^{(1)}=[0\ \ 1\ \ 1]$, $U_{1,4}^{(2)}=[a\ \ c]$ *and* $U_{1,4}^{(3)}=[b\ \ d]$, *and the resulting system* (4.2.3) *of matrix equations has a solution. In fact, one of the solutions of the system* (4.2.3) *is given by* $U_{1,4}^{(2)}=[1\ \ 1]$ *and* $U_{1,4}^{(3)}=[1\ \ 1]$, *which gives rise to a self-orthogonal code* $\mathcal{B}_4$ *of the type* $\{1,0,0,0\}$ *and length* 3 *over* R_4 *with a generator matrix*

$$[1\ \ 1\ \ 0]+u[0\ \ 1\ \ 1]+u^2[0\ \ 1\ \ 1]+u^3[0\ \ 1\ \ 1].$$

This shows that the self-orthogonal code $\mathcal{B}_2$ *of the type* $\{1,0\}$ *and length* 3 *over* R_2 *can be lifted to a self-orthogonal code of the type* $\{1,0,0,0\}$ *and length* 3 *over* R_4.

This suggests that when $p=2$ and $\ell\geq 4$, only those self-orthogonal codes of the type $\{\kappa_1+\kappa_2,\kappa_3,\ldots,\kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ can be lifted to self-orthogonal codes of the type $\{\kappa_1,\kappa_2,\kappa_3,\ldots,\kappa_\ell\}$ and of the same length n over R_ℓ for which the corresponding system (4.2.3) of matrix equations has a solution.

A symmetric matrix A is said to be alternating if it satisfies $\mathcal{D}iag(A)=0$. In the following theorem, we characterize all self-orthogonal (*resp.* self-dual) codes of the type $\{\kappa_1+\kappa_2, \kappa_3, \ldots, \kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_{\ell-1}, \kappa_\ell\}$ and length n over R_ℓ with the help of the construction method outlined above.

Theorem 4.2.1. *Let $p=2$, and let $\ell \geq 4$ be a fixed integer. Let $\mathcal{C}_{\ell-2}$ be a self-orthogonal (resp. self-dual) code of the type $\{\kappa_1+\kappa_2, \kappa_3, \ldots, \kappa_{\ell-1}\}$ and length n over $R_{\ell-2}$ with a generator matrix $G_{\ell-2}$ (as defined by (4.2.1)). Then the code $\mathcal{C}_{\ell-2}$ can be lifted to a self-orthogonal (resp. self-dual) code $\mathcal{C}_\ell$ of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_{\ell-1}, \kappa_\ell\}$ and length n over R_ℓ with a generator matrix G_ℓ (as defined by (4.2.2)) if and only if the matrix $U_1^{(\lfloor\frac{\ell-1}{2}\rfloor)} \in \mathcal{M}_{\kappa_1\times n}(\mathbb{F}_{2^r})$ satisfies*

$$\mathcal{D}iag\big(U_1^{(\lfloor\frac{\ell-1}{2}\rfloor)}U_1^{(\lfloor\frac{\ell-1}{2}\rfloor)t}\big)=0,$$

i.e., the matrix $U_1^{(\lfloor\frac{\ell-1}{2}\rfloor)}U_1^{(\lfloor\frac{\ell-1}{2}\rfloor)t}$ is alternating.

Proof. By Remark 3.4.1, we see that $A_{1,\ell}^{(0)}$ is a full-row rank matrix over $\mathbb{F}_{2^r}$. Here one can easily see that the code $\mathcal{C}_{\ell-2}$ can be lifted to a self-orthogonal (*resp.* self-dual) code $\mathcal{C}_\ell$ of the type $\{\kappa_1, \kappa_2, \ldots, \kappa_{\ell-1}, \kappa_\ell\}$ and length n over R_ℓ with a generator matrix G_ℓ if and only if the system (4.2.3) of matrix equations in unknowns $U_{1,\ell}^{(\ell-2)} \in \mathcal{M}_{\kappa_1\times(\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $U_{1,\ell}^{(\ell-1)} \in \mathcal{M}_{\kappa_1\times(\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$, $A_{y,\ell}^{(\ell-y)} \in \mathcal{M}_{\kappa_y\times(\kappa_\ell+\kappa_{\ell+1})}(\mathbb{F}_{p^r})$ for $2 \leq y \leq \ell$, admits a solution. Now by applying Lemma 2.1.1, the desired result follows. □

In the next section, we will present a modified recursive method to construct self-orthogonal and self-dual codes over R_e from self-orthogonal codes over $\mathbb{F}_{2^r}$, and vice versa.

4.3 A modified recursive method to construct self-orthogonal and self-dual codes over the ring R_e from self-orthogonal codes over $\mathbb{F}_{2^r}$

From now on, throughout this chapter, we assume that $p=2$ and $e \geq 2$. Let us define

$$s=\Big\lfloor\frac{e}{2}\Big\rfloor.$$

This gives $\lceil \frac{e}{2} \rceil = s + \theta$, where $\theta = 0$ if e is even, while $\theta = 1$ if e is odd. Let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s+1 \leq i \leq e$. Further, we define $n_0 = 0$ and $n_i = k_1 + k_2 + \cdots + k_i$ for $1 \leq i \leq e+1$. For positive integers α and $\beta \leq e$, let $(B)_{\alpha,\beta}$ denote the block matrix whose (i,j)th block is the matrix $B_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq \alpha$ and $\beta \leq j \leq e$. Now we define linear codes satisfying the property $(*)$ as follows:

Linear codes satisfying the property $(*)$: *For an integer $e \geq 3$, let ℓ be a fixed integer satisfying $2 \leq \ell \leq e$, and let $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$. Let $\mathcal{C}_\ell$ be a linear code of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ with a generator matrix*

$$G_\ell = \begin{bmatrix} T_1 \\ T_2 \\ \vdots \\ T_{s-\ell_1+1} \\ uT_{s-\ell_1+2} \\ \vdots \\ u^{\ell-1}T_{s+\theta+\ell_1} \end{bmatrix}, \tag{4.3.1}$$

where for $1 \leq h \leq s - \ell_1 + 1$,

$$T_h = T_h^{(0)} + \sum_{j=1}^{\ell-1} u^j U_h^{(j)}$$

with $T_h^{(0)} \in \mathcal{M}_{k_h \times n}(\mathbb{F}_{2^r})$, $U_h^{(j)} \in \mathcal{M}_{k_h \times n}(\mathbb{F}_{2^r})$ for $1 \leq j \leq \ell - 1$, and the matrix $T_{s-\ell_1+i} \in \mathcal{M}_{k_{s-\ell_1+i} \times n}(R_\ell)$ to be considered modulo $u^{\ell-i+1}$ for $2 \leq i \leq \ell$. We say that the code $\mathcal{C}_\ell$ satisfies the property $(*)$ if the matrices $U_h^{(y)} U_h^{(y)t}$ are alternating for all integers h and y satisfying $1 \leq h \leq \min\{s - \ell_1 + 1, s + \theta - y\}$ and $1 \leq y \leq \min\{\ell - 1, s + \theta\}$ with $y \neq s + \theta$.

Example 4.3.1. *Let $e = 5$, $r = 1$, $n = 6$, $k_1 = k_2 = k_3 = k_4 = k_5 = 1$ and $\ell = 3$. Here we have $R_5 = \mathbb{F}_2[u]/\langle u^5 \rangle$ and $R_3 = \mathbb{F}_2[u]/\langle u^3 \rangle$. Let $\mathcal{C}_3$ be a linear code of the type $\{2, 1, 1\}$ and length 6 over R_3 with a generator matrix*

$$\begin{bmatrix} 1 & 0 & 1 & u+u^2 & 1+u^2 & 1+u \\ 0 & 1 & 0 & 1+u & u & 0 \\ 0 & 0 & u & u+u^2 & u^2 & 0 \\ 0 & 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}.$$

Note that

$$\begin{bmatrix} U_1^{(1)} \\ U_2^{(1)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} U_1^{(2)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

It is easy to observe that the matrices $U_1^{(1)}U_1^{(1)t}$, $U_2^{(1)}U_2^{(1)t}$ and $U_1^{(2)}U_1^{(2)t}$ are alternating, which implies that the code $\mathcal{C}_3$ satisfies the property $(*)$.

One can easily observe that any self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfies the property $(*)$. In this section, we will start with a self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$, and we will construct a self-orthogonal code of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{C}_0$ if e is even (see the proof of Proposition 4.3.1), while we will construct a self-orthogonal code of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and with the 2-th Torsion code as $\mathcal{C}_0$ if e is odd (see the proof of Proposition 4.3.2). We will also count such codes over R_2 and R_3 (see Propositions 4.3.1 and 4.3.2). Further, for $4 \leq \ell \leq e$, given a self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, we will construct a self-orthogonal code of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and with the $(i+1)$-th Torsion code as $Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$, and we will count such codes for $4 \leq \ell \leq e$, where $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$ (see Propositions 4.3.3 and 4.3.4). These results give rise to a modified recursive method to construct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e from a self-orthogonal code of the same length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$. We will employed this modified recursive construction method to count all self-orthogonal and self-dual codes of length n over R_e in Section 4.4.

Now if $\mathcal{C}_e$ is a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e, then we see, by Lemma 2.2.1, that its Torsion code $Tor_{s+\theta}(\mathcal{C}_e)$ is a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$. We next make the following observation.

Remark 4.3.1. *Let us consider a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ with a generator matrix*

$$G_0=\begin{bmatrix} T_1^{(0)}\\ T_2^{(0)}\\ \vdots\\ T_{s+\theta}^{(0)}\end{bmatrix}=\begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & A_{1,2}^{(0)} & \cdots & A_{1,s+\theta-1}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)}\\ 0 & I_{k_2} & A_{2,2}^{(0)} & \cdots & A_{2,s+\theta-1}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & I_{k_{s+\theta}} & \cdots & A_{s+\theta,e-1}^{(0)} & A_{s+\theta,e}^{(0)}\end{bmatrix}, \quad (4.3.2)$$

where columns of the matrix G_0 are grouped into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$ and $A_{i,j}^{(0)} \in \mathcal{M}_{k_i\times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \le i \le s+\theta$ and $i \le j \le e$. Since the matrix G_0 generates a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$, we have $G_0G_0^t = 0$, which implies that the matrix $(A^{(0)})_{s+\theta,s+\theta}$ is a full row-rank matrix over $\mathbb{F}_{2^r}$. Further, by permuting the columns of the matrix G_0, we can assume, without any loss of generality, that the matrices $(A^{(0)})_{s,s+\theta+1}$, $(A^{(0)})_{s-1,s+\theta+2}, \ldots, (A^{(0)})_{2,e-1}$, $A_{1,e}^{(0)}$ are of full row-rank.

We also need the following key lemma to count self-orthogonal and self-dual codes over R_e.

Lemma 4.3.1. *Let υ and τ be fixed integers satisfying $1 \le \upsilon \le s$ and $1 \le \tau \le s+\theta-1$. Let A, $X \in \mathcal{M}_{n_\upsilon\times n}(\mathbb{F}_{2^r})$ be two matrices of the form*

$$A=\begin{bmatrix} I_{k_1} & A_{1,1} & A_{1,2} & \cdots & A_{1,\upsilon-1} & \cdots & A_{1,e-1} & A_{1,e}\\ 0 & I_{k_2} & A_{2,2} & \cdots & A_{2,\upsilon-1} & \cdots & A_{2,e-1} & A_{2,e}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & I_{k_\upsilon} & \cdots & A_{\upsilon,e-1} & A_{\upsilon,e}\end{bmatrix}$$

and

$$X=\begin{bmatrix} X_1\\ X_2\\ \vdots\\ X_\upsilon\end{bmatrix}=\begin{bmatrix} 0 & \cdots & 0 & X_{1,\tau+1} & X_{1,\tau+2} & \cdots & X_{1,\tau+\upsilon} & \cdots & X_{1,e}\\ 0 & \cdots & 0 & 0 & X_{2,\tau+2} & \cdots & X_{2,\tau+\upsilon} & \cdots & X_{2,e}\\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & \cdots & 0 & 0 & 0 & \cdots & X_{\upsilon,\tau+\upsilon} & \cdots & X_{\upsilon,e}\end{bmatrix},$$

where columns of the matrices A and X are grouped into blocks of sizes $k_1, k_2, \ldots, k_e$, k_{e+1}, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$, $A_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq \upsilon$ and $i \leq j \leq e$ and $X_{i_1,j_1} \in \mathcal{M}_{k_{i_1} \times k_{j_1+1}}(\mathbb{F}_{2^r})$ for $1 \leq i_1 \leq \upsilon$ and $i_1 + \tau \leq j_1 \leq e$. Suppose that the matrix $(A)_{\upsilon,\tau+\upsilon} \in \mathcal{M}_{n_\upsilon \times (n-n_{\tau+\upsilon})}(\mathbb{F}_{2^r})$ is of full row-rank. Let $B \in \mathcal{M}_{n_\upsilon \times n_\upsilon}(\mathbb{F}_{2^r})$ be such that $\mathcal{D}iag(B) = 0$. Then for $1 \leq \omega \leq \upsilon$, the number of solutions of the system

$$\left.\begin{array}{rcl} AX^t + XA^t & = & B \\ \textit{and} \quad \mathcal{D}iag\big(X_h X_h^t\big) & = & 0 \quad \textit{for } 1 \leq h \leq \omega \end{array}\right\} \tag{4.3.3}$$

of matrix equations in the unknown matrix $X \in \mathcal{M}_{n_\upsilon \times n}(\mathbb{F}_{2^r})$ is given by

$$(2^r)^{\sum\limits_{i=\tau+2}^{\tau+\upsilon} k_i n_{i-\tau-1} + n_\upsilon(n_{e+1} - n_{\tau+\upsilon}) - n_\omega - \frac{n_\upsilon(n_\upsilon - 1)}{2}}.$$

Proof. To prove the result, let ω be a fixed integer satisfying $1 \leq \omega \leq \upsilon$. Let us write $A = (\mathbf{a}_i)$ and $X = (\mathbf{x}_j)$, where $\mathbf{a}_i$'s and $\mathbf{x}_j$'s are the rows of the matrices A and X, respectively. Let $d_{i,j}$ denote the (i,j)-th entry of the matrix B for $1 \leq i, j \leq n_\upsilon$. We note that $d_{i,i} = 0$ for $1 \leq i \leq n_\upsilon$. We next observe that the system (4.3.3) of matrix equations is equivalent to the following system of equations in unknowns $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{n_\upsilon}$ over $\mathbb{F}_{2^r}$:

$$\mathbf{a}_i \cdot \mathbf{x}_j + \mathbf{a}_j \cdot \mathbf{x}_i = d_{i,j} \qquad \text{for } 1 \leq i < j \leq n_\upsilon, \tag{4.3.4}$$

$$\mathbf{x}_i \cdot \mathbf{x}_i = 0 \qquad \text{for } 1 \leq i \leq n_\omega. \tag{4.3.5}$$

We further observe that for each integer j satisfying $1 \leq j \leq n_\upsilon$, there exists a unique integer b_j satisfying $1 \leq b_j \leq \upsilon$ and $n_{b_j - 1} + 1 \leq j \leq n_{b_j}$ and that the corresponding unknown $\mathbf{x}_j$ is of the form $\mathbf{x}_j = (\mathbf{0}\ \mathbf{x}_j^{n-n_{b_j+\tau}})$, where $\mathbf{0}$ denotes the zero vector of length $n_{b_j+\tau}$ and $\mathbf{x}_j^{n-n_{b_j+\tau}}$ denotes the vector of length $n - n_{b_j+\tau}$ obtained from $\mathbf{x}_j$ after deleting the first $n_{b_j+\tau}$ coordinates. This implies that the first $n_{b_j+\tau}$ coordinates of $\mathbf{x}_j$ are zero for $n_{b_j-1} + 1 \leq j \leq n_{b_j}$, which further implies that the number of variables in $\mathbf{x}_j$ are $n - n_{b_j+\tau}$ for $n_{b_j-1} + 1 \leq j \leq n_{b_j}$. For $1 \leq j \leq n_\upsilon$, let $\widetilde{\mathbf{x}}_j = \mathbf{x}_j^{n-n_{b_j+\tau}}$ (*resp.* $\widetilde{\mathbf{a}}_j = \mathbf{a}_j^{n-n_{b_j+\tau}}$) denote the vector of length $n - n_{b_j+\tau}$ obtained from $\mathbf{x}_j$ (*resp.* $\mathbf{a}_j$) after deleting the first $n_{b_j+\tau}$ coordinates. In view of this, equations (4.3.4) and (4.3.5) are equivalent to the following system of equations in unknowns $\widetilde{\mathbf{x}}_1, \widetilde{\mathbf{x}}_2, \ldots, \widetilde{\mathbf{x}}_{n_\upsilon}$ over $\mathbb{F}_{2^r}$:

$$\begin{aligned} \widetilde{\mathbf{a}}_i \cdot \widetilde{\mathbf{x}}_j + \widetilde{\mathbf{a}}_j \cdot \widetilde{\mathbf{x}}_i = d_{i,j} &\qquad \text{for } 1 \leq i < j \leq n_\upsilon, \\ \widetilde{\mathbf{x}}_i \cdot \widetilde{\mathbf{x}}_i = 0 &\qquad \text{for } 1 \leq i \leq n_\omega. \end{aligned}$$

This is equivalent to the following system of equations

$$\begin{aligned} \widetilde{\mathbf{a}}_i \cdot \widetilde{\mathbf{x}}_j + \widetilde{\mathbf{a}}_j \cdot \widetilde{\mathbf{x}}_i &= d_{i,j} &\qquad \text{for } 1 \leq i < j \leq n_\upsilon, \\ \widetilde{\mathbf{1}} \cdot \widetilde{\mathbf{x}}_i &= 0 &\qquad \text{for } 1 \leq i \leq n_\omega, \end{aligned}$$

(here $\widetilde{\mathbf{1}}$ denotes the all-one vector having the same length as that of $\widetilde{\mathbf{x}}_i$), which can be represented in the matrix form as follows:

$$\mathcal{A} \begin{bmatrix} \widetilde{\mathbf{x}}_1^t \\ \widetilde{\mathbf{x}}_2^t \\ \vdots \\ \widetilde{\mathbf{x}}_{n_\omega}^t \\ \widetilde{\mathbf{x}}_{n_\omega+1}^t \\ \vdots \\ \widetilde{\mathbf{x}}_{n_\upsilon-1}^t \\ \widetilde{\mathbf{x}}_{n_\upsilon}^t \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ d_{1,2} \\ \vdots \\ d_{1,n_\upsilon} \\ \vdots \\ d_{n_\upsilon-1,n_\upsilon} \end{bmatrix}, \quad \text{where } \mathcal{A} = \begin{bmatrix} \widetilde{\mathbf{1}} & & & & & & \\ & & \ddots & & & & \\ & & & & \widetilde{\mathbf{1}} & & \\ \widetilde{\mathbf{a}}_2 & \widetilde{\mathbf{a}}_1 & & & & & \\ \vdots & \vdots & \ddots & & & & \\ \widetilde{\mathbf{a}}_{n_\upsilon} & & & & & & \widetilde{\mathbf{a}}_1 \\ & & & \vdots & \vdots & \vdots & \\ & & & & & \widetilde{\mathbf{a}}_{n_\upsilon} & \widetilde{\mathbf{a}}_{n_\upsilon-1} \end{bmatrix}.$$

Since $(A)_{\upsilon,\upsilon+\tau}$ is a full row-rank matrix over $\mathbb{F}_{2^r}$, we observe that the vectors $\mathbf{a}_1^{n-n_{c+\tau}}, \mathbf{a}_2^{n-n_{c+\tau}}, \ldots, \mathbf{a}_{n_\upsilon}^{n-n_{c+\tau}}$ (obtained by deleting the first $n_{c+\tau}$ coordinates from $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n_\upsilon}$, respectively) are linearly independent over $\mathbb{F}_{2^r}$ for $1 \leq c \leq \upsilon$. In particular, the vectors $\widetilde{\mathbf{a}}_1, \widetilde{\mathbf{a}}_2, \ldots, \widetilde{\mathbf{a}}_{n_\upsilon}$ are linearly independent over $\mathbb{F}_{2^r}$. We further note that the matrix $\mathcal{A}$ has order $\left(n_\omega + \frac{n_\upsilon(n_\upsilon-1)}{2}\right) \times \left(\sum\limits_{i=\tau+2}^{\tau+\upsilon} k_i n_{i-\tau-1} + n_\upsilon(n_{e+1} - n_{\tau+\upsilon})\right)$. Now we assert that the rows of the matrix $\mathcal{A}$ are linearly independent over $\mathbb{F}_{2^r}$.

To prove this assertion, we suppose, on the contrary, that the rows of the matrix $\mathcal{A}$ are linearly dependent over $\mathbb{F}_{2^r}$, which implies that there exists a non-zero symmetric matrix $(\beta_{i,j}) \in \mathcal{M}_{n_\upsilon \times n_\upsilon}(\mathbb{F}_{2^r})$ such that

$$\beta_{i,i}\widetilde{\mathbf{1}} + \sum_{\substack{j=1 \\ j \neq i}}^{n_\upsilon} \beta_{i,j}\widetilde{\mathbf{a}}_j \;=\; 0 \quad \text{for } 1 \leq i \leq n_\omega, \tag{4.3.6}$$

$$\sum_{\substack{j=1\\ j\neq i_1}}^{n_\upsilon} \beta_{i_1,j}\widetilde{\mathbf{a}}_j \;=\; 0 \quad \text{for } n_\omega+1\leq i_1\leq n_\upsilon \tag{4.3.7}$$

and $\beta_{i,i}=0$ for $n_\omega+1\leq i\leq n_\upsilon$. Since the vectors $\widetilde{\mathbf{a}}_1,\widetilde{\mathbf{a}}_2,\ldots,\widetilde{\mathbf{a}}_{n_\upsilon}$ are linearly independent over $\mathbb{F}_{2^r}$, the system (4.3.7) of equations implies that $\beta_{i,j}=0$ for $n_\omega+1\leq i\leq n_\upsilon$ and $1\leq j(\neq i)\leq n_\upsilon$. This gives $\beta_{i,j}=0$ for $n_\omega+1\leq i\leq n_\upsilon$ and $1\leq j\leq n_\upsilon$. As the vectors $\widetilde{\mathbf{a}}_1,\widetilde{\mathbf{a}}_2,\ldots,\widetilde{\mathbf{a}}_{n_\upsilon}$ are linearly independent over $\mathbb{F}_{2^r}$, by (4.3.6), we must have $\beta_{z,z}\neq 0$ for some integer z satisfying $1\leq z\leq n_\omega$. Further, by (4.3.6), we get $\mathbf{1}^{n-n_{\ell+\tau}}=\sum\limits_{\substack{j=1\\ j\neq z}}^{n_\omega}\beta_{z,z}^{-1}\beta_{z,j}\mathbf{a}_j^{n-n_{\ell+\tau}}$ for some integer ℓ satisfying $1\leq\ell\leq\upsilon$, from which it follows that $\beta_{z,g}\neq 0$ for some integer g satisfying $1\leq g(\neq z)\leq n_\omega$. By (4.3.6) again, we get $\beta_{g,g}\widetilde{\mathbf{1}}=\sum\limits_{\substack{j=1\\ j\neq g}}^{n_\omega}\beta_{g,j}\widetilde{\mathbf{a}}_j$, which implies that $\beta_{g,g}\mathbf{1}^{n-n_{y+\tau}}=\sum\limits_{\substack{j=1\\ j\neq g}}^{n_\omega}\beta_{g,j}\mathbf{a}_j^{n-n_{y+\tau}}$ for some integer y satisfying $1\leq y\leq\upsilon$. From this, it follows that

$$\mathbf{1}^{n-n_{\ell+\tau}} \;=\; \sum_{\substack{j=1\\ j\neq z}}^{n_\omega}\beta_{z,z}^{-1}\beta_{z,j}\mathbf{a}_j^{n-n_{\ell+\tau}} \quad\text{and} \tag{4.3.8}$$

$$\beta_{g,g}\mathbf{1}^{n-n_{y+\tau}} \;=\; \sum_{\substack{j_1=1\\ j_1\neq g}}^{n_\omega}\beta_{g,j_1}\mathbf{a}_{j_1}^{n-n_{y+\tau}}. \tag{4.3.9}$$

Now the following two cases arise: (i) $\ell=y$ and (ii) $\ell\neq y$.

(i) Let $\ell=y$. In this case, equation (4.3.9) is equivalent to

$$\beta_{g,g}\mathbf{1}^{n-n_{\ell+\tau}}=\sum_{\substack{j_1=1\\ j_1\neq g}}^{n_\omega}\beta_{g,j_1}\mathbf{a}_{j_1}^{n-n_{\ell+\tau}}.$$

From this and by equation (4.3.8), we get

$$\sum_{\substack{j=1\\ j\neq z}}^{n_\omega}\beta_{g,g}\beta_{z,z}^{-1}\beta_{z,j}\mathbf{a}_j^{n-n_{\ell+\tau}}=\sum_{\substack{j_1=1\\ j_1\neq g}}^{n_\omega}\beta_{g,j_1}\mathbf{a}_{j_1}^{n-n_{\ell+\tau}}.$$

Since the vectors $\mathbf{a}_1^{n-n_{\ell+\tau}},\mathbf{a}_2^{n-n_{\ell+\tau}},\ldots,\mathbf{a}_{n_\omega}^{n-n_{\ell+\tau}}$ are linearly independent over $\mathbb{F}_{2^r}$, we get $\beta_{g,z}=0$, which is a contradiction.

(ii) Let $\ell \neq y$. In this case, let us suppose, without any loss of generality, that $\ell < y$, which implies that $n - n_{\ell+\tau} \geq n - n_{y+\tau}$. Now by equation (4.3.8), we get $\mathbf{1}^{n-n_{y+\tau}} = \sum\limits_{\substack{j=1\\ j\neq z}}^{n_\omega} \beta_{z,z}^{-1}\beta_{z,j}\mathbf{a}_j^{n-n_{y+\tau}}$. From this and by equation (4.3.9), we get

$$\sum_{\substack{j=1\\ j\neq z}}^{n_\omega} \beta_{g,g}\beta_{z,z}^{-1}\beta_{z,j}\mathbf{a}_j^{n-n_{y+\tau}} = \sum_{\substack{j_1=1\\ j_1\neq g}}^{n_\omega} \beta_{g,j_1}\mathbf{a}_{j_1}^{n-n_{y+\tau}}.$$

Since the vectors $\mathbf{a}_1^{n-n_{y+\tau}}, \mathbf{a}_2^{n-n_{y+\tau}}, \ldots, \mathbf{a}_{n_\omega}^{n-n_{y+\tau}}$ are linearly independent over $\mathbb{F}_{2^r}$, we get $\beta_{g,z} = 0$, which is a contradiction.

This implies that the rows of the matrix $\mathcal{A}$ are linearly independent over $\mathbb{F}_{2^r}$. From this, the desired result follows immediately. □

In the following proposition, we show that given a self-orthogonal code $\mathcal{C}_0$ of length n and dimension n_s over $\mathbb{F}_{2^r}$, there exists a self-orthogonal code $\mathcal{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and $Tor_1(\mathcal{C}_2) = \mathcal{C}_0$. We also count all distinct self-orthogonal codes of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{C}_0$. The proof of the following proposition also provides a method to construct a self-orthogonal code of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ from a given self-orthogonal code of length n and dimension n_s over $\mathbb{F}_{2^r}$.

Proposition 4.3.1. *Let $\mathcal{C}_0$ be a self-orthogonal code of length n and dimension n_s over $\mathbb{F}_{2^r}$.*

(a) There exists a self-orthogonal code $\mathcal{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and $Tor_1(\mathcal{C}_2) = \mathcal{C}_0$.

(b) Moreover, each self-orthogonal code $\mathcal{C}_0$ of length n and dimension n_s over $\mathbb{F}_{2^r}$ gives rise to precisely

$$(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + n_s(n-n_{s+2}) - n_{s-1} - \frac{n_s(n_s-1)}{2}} \begin{bmatrix} k_{s+1} + n - n_{s+1} - n_s \\ k_{s+1} \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{C}_0$.

Proof. To prove the result, we assume, without any loss of generality, that the code $\mathcal{C}_0$ has a generator matrix

$$G_0 = [T^{(0)}]_s = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_s^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & A_{1,2}^{(0)} & \cdots & A_{1,s-1}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)} \\ 0 & I_{k_2} & A_{2,2}^{(0)} & \cdots & A_{2,s-1}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_s} & \cdots & A_{s,e-1}^{(0)} & A_{s,e}^{(0)} \end{bmatrix},$$

where columns of the matrix G_0 are grouped into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$ and $A_{i,j}^{(0)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s$ and $i \leq j \leq e$. By Remark 4.3.1, we assume, without any loss of generality, that the matrices $(A^{(0)})_{s,s+1}$, $(A^{(0)})_{s-1,s+2}, \ldots, (A^{(0)})_{2,e-1}$, $A_{1,e}^{(0)}$ are of full row-rank. Since the code $\mathcal{C}_0$ is self-orthogonal, we have $G_0 G_0^t = [T^{(0)}]_s [T^{(0)}]_s^t = 0$.

Now to show that there exists a self-orthogonal code of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{C}_0$, let us define a matrix G_2 over R_2 as

$$G_2 = \begin{bmatrix} T_1^{(2)} \\ T_2^{(2)} \\ \vdots \\ T_s^{(2)} \\ uT_{s+1}^{(2)} \end{bmatrix} = \begin{bmatrix} T_1^{(0)} + uU_1^{(1)} \\ T_2^{(0)} + uU_2^{(1)} \\ \vdots \\ T_s^{(0)} + uU_s^{(1)} \\ uT_{s+1}^{(2)} \end{bmatrix}$$

with the matrix $[U^{(1)}]_s$ of the form

$$[U^{(1)}]_s = \begin{bmatrix} U_1^{(1)} \\ U_2^{(1)} \\ \vdots \\ U_s^{(1)} \end{bmatrix} = \begin{bmatrix} 0 & 0 & A_{1,2}^{(1)} & A_{1,3}^{(1)} & \cdots & A_{1,s+1}^{(1)} & \cdots & A_{1,e}^{(1)} \\ 0 & 0 & 0 & A_{2,3}^{(1)} & \cdots & A_{2,s+1}^{(1)} & \cdots & A_{2,e}^{(1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & A_{s,s+1}^{(1)} & \cdots & A_{s,e}^{(1)} \end{bmatrix},$$

where $A_{i,j}^{(1)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s$ and $i < j \leq e$ and the matrix $T_{s+1}^{(2)}$ is of the form

$$T_{s+1}^{(2)} = \begin{bmatrix} 0 & \cdots & 0 & I_{k_{s+1}} & A_{s+1,s+1}^{(0)} & \cdots & A_{s+1,e}^{(0)} \end{bmatrix}$$

with $A^{(0)}_{s+1,j} \in \mathcal{M}_{k_{s+1}\times k_{j+1}}(\mathbb{F}_{2^r})$ for $s+1 \leq j \leq e$.

Let $\mathcal{C}_2$ be a linear code of length n over R_2 with a generator matrix G_2. It is easy to see that the code $\mathcal{C}_2$ is of the type $\{n_s, k_{s+1}\}$ and $Tor_1(\mathcal{C}_2) = \mathcal{C}_0$. By Theorem 2.2.4(a), we see that the code $\mathcal{C}_2$ is a self-orthogonal code over R_2 satisfying the property $(*)$ if and only if there exist matrices $[U^{(1)}]_s$ and $T^{(2)}_{s+1}$ satisfying the following system of matrix equations over $\mathbb{F}_{2^r}$:

$$\begin{aligned}
[T^{(0)}]_s[U^{(1)}]^t_s + [U^{(1)}]_s[T^{(0)}]^t_s &= 0, && (4.3.10)\\
\mathcal{D}iag\big(U^{(1)}_h U^{(1)t}_h\big) &= 0 \text{ for } 1 \leq h \leq s-1, && (4.3.11)\\
[T^{(0)}]_s T^{(2)t}_{s+1} &= 0. && (4.3.12)
\end{aligned}$$

Since the matrix $(A^{(0)})_{s,s+1}$ is of full row-rank, we see, by Lemma 4.3.1, that there exists a matrix $[U^{(1)}]_s$ satisfying (4.3.10) and (4.3.11) and that such a matrix $[U^{(1)}]_s$ has precisely

$$(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + n_s(n-n_{s+2}) - n_{s-1} - \frac{n_s(n_s-1)}{2}}$$

distinct choices. Further, by Lemma 2.2.1 and by equation (2.2.2), we observe that there exists a matrix $T^{(2)}_{s+1}$ satisfying (4.3.12) if and only if the Torsion code $Tor_2(\mathcal{C}_2)$ satisfies $\mathcal{C}_0 \subseteq Tor_2(\mathcal{C}_2) \subseteq \mathcal{C}_0^{\perp}$. From this, we observe that the number of choices for the matrix $T^{(2)}_{s+1}$ satisfying (4.3.12) is equal to the number of choices for a linear code $\mathcal{C}'$ of length n and dimension n_{s+1} over $\mathbb{F}_{2^r}$ satisfying $\mathcal{C}_0 \subseteq \mathcal{C}' \subseteq \mathcal{C}_0^{\perp}$ for a given choice of $\mathcal{C}_0$. Further, for a given choice of $\mathcal{C}_0$, we see, by Theorem 2.3.9, that there are precisely $\begin{bmatrix} k_{s+1}+n-n_{s+1}-n_s \\ k_{s+1} \end{bmatrix}_{2^r}$ distinct choices for the code $\mathcal{C}'$ satisfying $\mathcal{C}_0 \subseteq \mathcal{C}' \subseteq \mathcal{C}_0^{\perp}$, and hence the matrix $T^{(2)}_{s+1}$ has precisely $\begin{bmatrix} k_{s+1}+n-n_{s+1}-n_s \\ k_{s+1} \end{bmatrix}_{2^r}$ distinct choices. Further, one can easily observe that each of the distinct choices of the matrices $[U^{(1)}]_s$ and $T^{(2)}_{s+1}$ satisfying (4.3.10)-(4.3.12) gives rise to a distinct self-orthogonal code $\mathcal{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and $Tor_1(\mathcal{C}_2) = \mathcal{C}_0$. From this, the desired result follows immediately. □

In the following proposition, we show that given a self-orthogonal code $\mathcal{C}_0$ of length n and dimension n_{s+1} over $\mathbb{F}_{2^r}$, there exists a self-orthogonal code $\mathcal{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and $Tor_2(\mathcal{C}_3) =$

$\mathcal{C}_0$. We also count all distinct self-orthogonal codes of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and with the 2-th Torsion code as $\mathcal{C}_0$. The proof of the following proposition also provides a method to construct a self-orthogonal code $\mathcal{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ from a given self-orthogonal code $\mathcal{C}_0$ of length n and dimension n_{s+1} over $\mathbb{F}_{2^r}$.

Proposition 4.3.2. *Let $\mathcal{C}_0$ be a self-orthogonal code of length n and dimension n_{s+1} over $\mathbb{F}_{2^r}$.*

(a) There exists a self-orthogonal code $\mathcal{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and $Tor_2(\mathcal{C}_3) = \mathcal{C}_0$.

(b) Moreover, each self-orthogonal code $\mathcal{C}_0$ of length n and dimension n_{s+1} over $\mathbb{F}_{2^r}$ gives rise to precisely

$$(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + \sum\limits_{j=4}^{s+2} k_j n_{j-3} + (n_{s+1}+n_s)(n-n_{s+2}-n_s) + n_s^2 - n_{s-1}} \begin{bmatrix} n_{s+1} \\ n_s \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+2} + n - n_{s+2} - n_s \\ k_{s+2} \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and with the 2-th Torsion code as $\mathcal{C}_0$.

Proof. To prove the result, we first choose an n_s-dimensional linear subcode $\mathcal{B}_1$ of the code $\mathcal{C}_0$. By Theorem 2.3.9, we see that the subcode $\mathcal{B}_1$ has precisely $\left[\begin{smallmatrix} n_{s+1} \\ n_s \end{smallmatrix}\right]_{2^r}$ distinct choices. Further, without any loss of generality, we assume that the code $\mathcal{C}_0$ has a generator matrix

$$G_0 = [T^{(0)}]_{s+1} = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_{s+1}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & A_{1,2}^{(0)} & \cdots & A_{1,s}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)} \\ 0 & I_{k_2} & A_{2,2}^{(0)} & \cdots & A_{2,s}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_{s+1}} & \cdots & A_{s+1,e-1}^{(0)} & A_{s+1,e}^{(0)} \end{bmatrix}$$

and its subcode $\mathcal{B}_1$ has a generator matrix

$$[T^{(0)}]_s = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_s^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & A_{1,2}^{(0)} & \cdots & A_{1,s}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)} \\ 0 & I_{k_2} & A_{2,2}^{(0)} & \cdots & A_{2,s}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_s} & \cdots & A_{s,e-1}^{(0)} & A_{s,e}^{(0)} \end{bmatrix},$$

where columns of the matrices G_0 and $[T^{(0)}]_s$ are grouped into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$ and $A^{(0)}_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s+1$ and $i \leq j \leq e$. Further, by Remark 4.3.1, we assume, without any loss of generality, that the matrices $(A^{(0)})_{s,s+2}$, $(A^{(0)})_{s-1,s+3}, \ldots, (A^{(0)})_{2,e-1}$, $A^{(0)}_{1,e}$ are of full row-rank. Since the code $\mathcal{C}_0$ is self-orthogonal, we have $G_0G_0^t = [T^{(0)})]_{s+1}[T^{(0)}]^t_{s+1} = 0$.

Now to show that there exists a self-orthogonal code of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$ and with the 2-th Torsion code as $\mathcal{C}_0$, let us define a matrix G_3 over R_3 as

$$G_3 = \begin{bmatrix} T_1^{(3)} \\ T_2^{(3)} \\ \vdots \\ T_s^{(3)} \\ uT_{s+1}^{(3)} \\ u^2T_{s+2}^{(3)} \end{bmatrix} = \begin{bmatrix} T_1^{(0)} + uU_1^{(1)} + u^2U_1^{(2)} \\ T_2^{(0)} + uU_2^{(1)} + u^2U_2^{(2)} \\ \vdots \\ T_s^{(0)} + uU_s^{(1)} + u^2U_s^{(2)} \\ uT_{s+1}^{(3)} \\ u^2T_{s+2}^{(3)} \end{bmatrix}$$

with the matrices $[U^{(\alpha)}]_s$ for $\alpha \in \{1,2\}$, $T^{(3)}_{s+1}$ and $T^{(3)}_{s+2}$ of the forms

$$\begin{aligned} [U^{(\alpha)}]_s = \begin{bmatrix} U_1^{(\alpha)} \\ U_2^{(\alpha)} \\ \vdots \\ U_s^{(\alpha)} \end{bmatrix} &= \begin{bmatrix} 0 & \cdots & 0 & A^{(\alpha)}_{1,\alpha+1} & A^{(\alpha)}_{1,\alpha+2} & \cdots & A^{(\alpha)}_{1,\alpha+s} & \cdots & A^{(\alpha)}_{1,e} \\ 0 & \cdots & 0 & 0 & A^{(\alpha)}_{2,\alpha+2} & \cdots & A^{(\alpha)}_{2,\alpha+s} & \cdots & A^{(\alpha)}_{2,e} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & A^{(\alpha)}_{s,\alpha+s} & \cdots & A^{(\alpha)}_{s,e} \end{bmatrix}, \\ T^{(3)}_{s+1} &= T^{(0)}_{s+1} + u\begin{bmatrix} 0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e} \end{bmatrix} \text{ and} \\ T^{(3)}_{s+2} &= \begin{bmatrix} 0 & \cdots & 0 & I_{k_{s+2}} & A^{(0)}_{s+2,s+2} & \cdots & A^{(0)}_{s+2,e} \end{bmatrix}, \end{aligned}$$

where $A^{(\alpha)}_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s$ and $i+\alpha \leq j \leq e$, $A^{(1)}_{s+1,v} \in \mathcal{M}_{k_{s+1} \times k_{v+1}}(\mathbb{F}_{2^r})$ for $s+2 \leq v \leq e$ and $A^{(0)}_{s+2,b} \in \mathcal{M}_{k_{s+2} \times k_{b+1}}(\mathbb{F}_{2^r})$ for $s+2 \leq b \leq e$.

Next, let $\mathcal{C}_3$ be a linear code of length n over R_3 with a generator matrix G_3. It is easy to see that the code $\mathcal{C}_3$ is of the type $\{n_s, k_{s+1}, k_{s+2}\}$, $Tor_1(\mathcal{C}_3) = \mathcal{B}_1$ and $Tor_2(\mathcal{C}_3) = \mathcal{C}_0$. By Theorem 2.2.4(a), we see that the code $\mathcal{C}_3$ is a self-orthogonal code over R_3 satisfying the property $(*)$ if and only if there exist matrices $[U^{(1)}]_s$,

$[U^{(2)}]_s$, $\begin{bmatrix}0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}$ and $T^{(3)}_{s+2}$ satisfying the following system of matrix equations over $\mathbb{F}_{2^r}$:

$$\begin{aligned} [T^{(0)}]_s[U^{(1)}]_s^t + [U^{(1)}]_s[T^{(0)}]_s^t &= 0, && (4.3.13)\\ \mathcal{D}iag\big(U_h^{(1)}U_h^{(1)t}\big) &= 0 \text{ for } 1 \leq h \leq s, && (4.3.14)\\ [T^{(0)}]_s[U^{(2)}]_s^t + [U^{(2)}]_s[T^{(0)}]_s^t &= [U^{(1)}]_s[U^{(1)}]_s^t, && (4.3.15)\\ \mathcal{D}iag\big(U_\ell^{(2)}U_\ell^{(2)t}\big) &= 0 \text{ for } 1 \leq \ell \leq s-1, && (4.3.16)\\ [T^{(0)}]_s\begin{bmatrix}0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}^t &= [U^{(1)}]_s T^{(0)t}_{s+1}, && (4.3.17)\\ [T^{(0)}]_s\begin{bmatrix}0 & \cdots & 0 & I_{k_{s+2}} & A^{(0)}_{s+2,s+2} & \cdots & A^{(0)}_{s+2,e}\end{bmatrix}^t &= 0. && (4.3.18)\end{aligned}$$

As the matrix $(A^{(0)})_{s,s+2}$ is of full row-rank, we see, by Lemma 4.3.1, that there exist matrices $[U^{(1)}]_s$ and $[U^{(2)}]_s$ satisfying (4.3.13)-(4.3.16), and that there are precisely

$$(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + \sum\limits_{j=4}^{s+2} k_j n_{j-3} + 2n_s(n-n_{s+2}) - n_s^2 - n_{s-1}}$$

distinct choices for such a pair of matrices $[U^{(1)}]_s$ and $[U^{(2)}]_s$. Further, for given choices of the matrices $[U^{(1)}]_s$ and $[U^{(2)}]_s$ satisfying (4.3.13)-(4.3.16), we observe that the matrix equation (4.3.17) is equivalent to the following matrix equation

$$(A^{(0)})_{s,s+2}\begin{bmatrix}A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}^t = [U^{(1)}]_s T^{(0)t}_{s+1} \qquad (4.3.19)$$

over $\mathbb{F}_{2^r}$. As the matrix $(A^{(0)})_{s,s+2}$ is of full row-rank, the total number of choices for the matrix $\begin{bmatrix}A^{(1)}_{s+1,s+2} \cdots A^{(1)}_{s+1,e}\end{bmatrix}$ satisfying (4.3.19) (and hence the matrix $\begin{bmatrix}0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}$ satisfying (4.3.17)) has precisely $(2^r)^{k_{s+1}(n-n_{s+2}-n_s)}$ distinct choices. Further, by applying Theorem 2.3.9 and Lemma 2.2.1 and working as in Proposition 4.3.1, we can show that there exists a matrix $T^{(3)}_{s+2}$ satisfying (4.3.18) and that the matrix $T^{(3)}_{s+2}$ has precisely $\begin{bmatrix}k_{s+2}+n-n_{s+2}-n_s \\ k_{s+2}\end{bmatrix}_{2^r}$ distinct choices. This shows that there exist matrices $[U^{(1)}]_s$, $[U^{(2)}]_s$, $\begin{bmatrix}0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}$ and $T^{(3)}_{s+2}$ satisfying (4.3.13)-(4.3.18), which implies that there exists a self-orthogonal code $\mathcal{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$, $Tor_1(\mathcal{C}_3) = \mathcal{B}_1$ and $Tor_2(\mathcal{C}_3) = \mathcal{C}_0$. Further, one can easily observe that each of the distinct choices of the matrices $[U^{(1)}]_s$, $[U^{(2)}]_s$, $\begin{bmatrix}0 & \cdots & 0 & A^{(1)}_{s+1,s+2} & \cdots & A^{(1)}_{s+1,e}\end{bmatrix}$ and

$T^{(3)}_{s+2}$ satisfying (4.3.13)-(4.3.18) give rise to distinct self-orthogonal codes $\mathcal{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over R_3 satisfying the property $(*)$, $Tor_1(\mathcal{C}_3) = \mathcal{B}_1$ and $Tor_2(\mathcal{C}_3) = \mathcal{C}_0$. From this, the desired result follows. □

Now let $\theta_1 = 0$ if s is even, while $\theta_1 = 1$ if s is odd. Let ℓ be a positive integer satisfying $4 \leq \ell \leq s+\theta+\theta_1$, and let $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$. In the following proposition, we show that given a self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, there exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$. We also count all such distinct self-orthogonal codes of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ.

Proposition 4.3.3. *Let $\theta_1 = 0$ if s is even, while $\theta_1 = 1$ if s is odd. Let ℓ be a fixed integer satisfying $4 \leq \ell \leq s+\theta+\theta_1$, and let $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$. Let $\mathcal{C}_{\ell-2}$ be a self-orthogonal code of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$. Then the following hold.*

(a) There exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$.

(b) Moreover, each self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, k_{s-\ell_1+4}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$ gives rise to precisely

$$(2^r)^{\sum\limits_{i=\ell}^{s+\theta+\ell_1} k_i n_{i-\ell+1} + \sum\limits_{j=\ell+1}^{s+\theta+\ell_1} k_j n_{j-\ell} + \Lambda} \begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+\theta+\ell_1} + n - n_{s+\theta+\ell_1} - n_{s-\ell_1+1} \\ k_{s+\theta+\ell_1} \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and with the $(i+1)$-th Torsion code as $Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$, where $\Lambda = (n_{s+\theta+\ell_1-1} + n_{s-\ell_1+1})(n - n_{s+\ell_1+\theta} - n_{s-\ell_1+1}) + n_{s-\ell_1+1} + n^2_{s-\ell_1+1} - n_{s-\ell+2} - n_{s-\ell+1}$.

Proof. To prove the result, we first note that the Torsion code $Tor_1(\mathcal{C}_{\ell-2})$ is an $n_{s-\ell_1+2}$-dimensional code over $\mathbb{F}_{2^r}$. So we first choose an $n_{s-\ell_1+1}$-dimensional linear subcode $\mathcal{B}_1$ of the code $Tor_1(\mathcal{C}_{\ell-2})$. By Theorem 2.3.9, we see that the subcode $\mathcal{B}_1$ has precisely $\begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r}$ distinct choices. Further, without any loss of generality, we assume that the code $Tor_1(\mathcal{C}_{\ell-2})$ has a generator matrix

$$H = [T^{(0)}]_{s-\ell_1+2} = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_{s-\ell_1+2}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & \cdots & A_{1,s-\ell_1+1}^{(0)} & \cdots & A_{1,e}^{(0)} \\ 0 & I_{k_2} & \cdots & A_{2,s-\ell_1+1}^{(0)} & \cdots & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-\ell_1+2}} & \cdots & A_{s-\ell_1+2,e}^{(0)} \end{bmatrix}$$

and its subcode $\mathcal{B}_1$ has a generator matrix

$$[T^{(0)}]_{s-\ell_1+1} = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_{s-\ell_1+1}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & \cdots & A_{1,s-\ell_1}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)} \\ 0 & I_{k_2} & \cdots & A_{2,s-\ell_1}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-\ell_1+1}} & \cdots & A_{s-\ell_1+1,e-1}^{(0)} & A_{s-\ell_1+1,e}^{(0)} \end{bmatrix},$$

where columns of the matrices H and $[T^{(0)}]_{s-\ell_1+1}$ are grouped into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$ and $A_{i,j}^{(0)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s - \ell_1 + 2$ and $i \leq j \leq e$. Furthermore, by Remark 4.3.1, we assume, without any loss of generality, that the matrix $(A^{(0)})_{s-\ell_1+1,s+\theta+\ell_1}$ is of full row-rank. We next assume, without any loss of generality, that the code $\mathcal{C}_{\ell-2}$ has a generator matrix

$$G_{\ell-2} = \begin{bmatrix} T_1^{(\ell-2)} \\ T_2^{(\ell-2)} \\ \vdots \\ T_{s-\ell_1+2}^{(\ell-2)} \\ uT_{s-\ell_1+3}^{(\ell-2)} \\ \vdots \\ u^{\ell-3}T_{s+\theta+\ell_1-1}^{(\ell-2)} \end{bmatrix} = \begin{bmatrix} T_1^{(0)} + uU_1^{(1)} + u^2U_1^{(2)} + \cdots + u^{\ell-3}U_1^{(\ell-3)} \\ T_2^{(0)} + uU_2^{(1)} + u^2U_2^{(2)} + \cdots + u^{\ell-3}U_2^{(\ell-3)} \\ \vdots \\ T_{s-\ell_1+2}^{(0)} + uU_{s-\ell_1+2}^{(1)} + u^2U_{s-\ell_1+2}^{(2)} + \cdots + u^{\ell-3}U_{s-\ell_1+2}^{(\ell-3)} \\ uT_{s-\ell_1+3}^{(\ell-2)} \\ \vdots \\ u^{\ell-3}T_{s+\theta+\ell_1-1}^{(\ell-2)} \end{bmatrix},$$

where $[T^{(0)}]_{s-\ell_1+2} \in \mathcal{M}_{n_{s-\ell_1+2}\times n}(\mathbb{F}_{2^r})$, $[U^{(j)}]_{s-\ell_1+2} \in \mathcal{M}_{n_{s-\ell_1+2}\times n}(\mathbb{F}_{2^r})$ for $1 \leq j \leq \ell-3$, and the matrix $T^{(\ell-2)}_{s-\ell_1+i} \in \mathcal{M}_{k_{s-\ell_1+i}\times n}(R_{\ell-2})$ is of the form $T^{(\ell-2)}_{s-\ell_1+i} = Z^{(0)}_{s-\ell_1+i} + uZ^{(1)}_{s-\ell_1+i} + \cdots + u^{\ell-i-1}Z^{(\ell-i-1)}_{s-\ell_1+i}$ with $Z^{(0)}_{s-\ell_1+i}, Z^{(1)}_{s-\ell_1+i}, \ldots, Z^{(\ell-i-1)}_{s-\ell_1+i} \in \mathcal{M}_{k_{s-\ell_1+i}\times n}(\mathbb{F}_{2^r})$ for $3 \leq i \leq \ell-1$.

Since $\mathcal{C}_{\ell-2}$ is a self-orthogonal code over $R_{\ell-2}$ satisfying the property $(*)$, by applying Theorem 2.2.4(a), we get

$$\begin{aligned}
[T^{(\ell-2)}]_{s-\ell_1+1}[T^{(\ell-2)}]^t_{s-\ell_1+1} &\equiv 0 \pmod{u^{\ell-2}},\\
[T^{(\ell-2)}]_{s-\ell_1+1}T^{(\ell-2)t}_{s-\ell_1+2+\beta} &\equiv 0 \pmod{u^{\ell-2-\beta}} \text{ for } 0 \leq \beta \leq \ell-3,\\
T^{(\ell-2)}_{s-\ell_1+i}T^{(\ell-2)t}_{s-\ell_1+j} &\equiv 0 \pmod{u^{\ell+2-i-j}} \text{ for } 2 \leq i,j \leq \ell-1 \text{ and } i+j \leq \ell+1,\\
\mathcal{D}iag\big(U^{(\nu)}_h U^{(\nu)t}_h\big) &= 0 \text{ for } 1 \leq h \leq \min\{s-\ell_1+2, s+\theta-\nu\} \text{ and } 1 \leq \nu \leq \ell-3.
\end{aligned}$$

Now to show that there exists a self-orthogonal code of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{B}_1$ and the $(i+1)$-th Torsion code as $Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$, let us define a matrix G_ℓ over R_ℓ as

$$G_\ell = \begin{bmatrix} T^{(\ell)}_1 \\ T^{(\ell)}_2 \\ \vdots \\ T^{(\ell)}_{s-\ell_1+1} \\ uT^{(\ell)}_{s-\ell_1+2} \\ \vdots \\ u^{\ell-1}T^{(\ell)}_{s+\theta+\ell_1} \end{bmatrix} = \begin{bmatrix} T^{(\ell-2)}_1 + u^{\ell-2}U^{(\ell-2)}_1 + u^{\ell-1}U^{(\ell-1)}_1 \\ T^{(\ell-2)}_2 + u^{\ell-2}U^{(\ell-2)}_2 + u^{\ell-1}U^{(\ell-1)}_2 \\ \vdots \\ T^{(\ell-2)}_{s-\ell_1+1} + u^{\ell-2}U^{(\ell-2)}_{s-\ell_1+1} + u^{\ell-1}U^{(\ell-1)}_{s-\ell_1+1} \\ uT^{(\ell)}_{s-\ell_1+2} \\ \vdots \\ u^{\ell-1}T^{(\ell)}_{s+\theta+\ell_1} \end{bmatrix} \tag{4.3.20}$$

with the matrices $[U^{(\alpha)}]_{s-\ell_1+1}$ for $\alpha \in \{\ell-2, \ell-1\}$, $T^{(\ell)}_{s-\ell_1+y}$ for $2 \leq y \leq \ell-1$ and $T^{(\ell)}_{s+\theta+\ell_1}$ of the forms

$$\begin{bmatrix} U^{(\alpha)}_1 \\ U^{(\alpha)}_2 \\ \vdots \\ U^{(\alpha)}_{s-\ell_1+1} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & A^{(\alpha)}_{1,\alpha+1} & \cdots & A^{(\alpha)}_{1,s-\ell_1+1+\alpha} & \cdots & A^{(\alpha)}_{1,e} \\ 0 & \cdots & 0 & 0 & \cdots & A^{(\alpha)}_{2,s-\ell_1+1+\alpha} & \cdots & A^{(\alpha)}_{2,e} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & A^{(\alpha)}_{s-\ell_1+1,s-\ell_1+1+\alpha} & \cdots & A^{(\alpha)}_{s-\ell_1+1,e} \end{bmatrix},$$

$$T^{(\ell)}_{s-\ell_1+y} = T^{(\ell-2)}_{s-\ell_1+y} + u^{\ell-y}\Big[0 \ \cdots \ 0 \ \ A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} \ \ \cdots \ \ A^{(\ell-y)}_{s-\ell_1+y,e}\Big] \text{ and}$$

$$T^{(\ell)}_{s+\theta+\ell_1} = \Big[0 \ \cdots \ 0 \ \ I_{k_{s+\theta+\ell_1}} \ \ A^{(0)}_{s+\theta+\ell_1,s+\theta+\ell_1} \ \ \cdots \ \ A^{(0)}_{s+\theta+\ell_1,e}\Big],$$

where $A^{(\alpha)}_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s-\ell_1+1$ and $i+\alpha \leq j \leq e$, $A^{(\ell-y)}_{s-\ell_1+y,v} \in \mathcal{M}_{k_{s-\ell_1+y} \times k_{v+1}}(\mathbb{F}_{2^r})$ for $s+\theta+\ell_1 \leq v \leq e$ and $A^{(0)}_{s+\theta+\ell_1,b} \in \mathcal{M}_{k_{s+\theta+\ell_1} \times k_{b+1}}(\mathbb{F}_{2^r})$ for $s+\theta+\ell_1 \leq b \leq e$.

Next, let $\mathcal{C}_\ell$ be a linear code of length n over R_ℓ with a generator matrix G_ℓ. It is easy to see that the code $\mathcal{C}_\ell$ is of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$, $Tor_1(\mathcal{C}_\ell) = \mathcal{B}_1$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$. By Theorem 2.2.4(a), we see that the code $\mathcal{C}_\ell$ is a self-orthogonal code over R_ℓ satisfying the property $(*)$ if and only if there exist matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$, $[U^{(\ell-1)}]_{s-\ell_1+1}$, $\big[\ 0 \ \cdots \ 0 \ \ A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} \ \cdots \ A^{(\ell-y)}_{s-\ell_1+y,e}\ \big]$ for $2 \leq y \leq \ell-1$ and $T^{(\ell)}_{s+\theta+\ell_1}$ satisfying the following system of matrix equations (4.3.21)-(4.3.27) over $\mathbb{F}_{2^r}$:

$$[T^{(0)}]_{s-\ell_1+1}[U^{(\ell-2)}]^t_{s-\ell_1+1} + [U^{(\ell-2)}]_{s-\ell_1+1}[T^{(0)}]^t_{s-\ell_1+1} = \sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-2-j)}]^t_{s-\ell_1+1}, \tag{4.3.21}$$

$$[T^{(0)}]_{s-\ell_1+1}[U^{(\ell-1)}]^t_{s-\ell_1+1} + [U^{(\ell-1)}]_{s-\ell_1+1}[T^{(0)}]^t_{s-\ell_1+1} = \sum_{j=1}^{\ell-2}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-1-j)}]^t_{s-\ell_1+1}, \tag{4.3.22}$$

$$[T^{(0)}]_{s-\ell_1+1}\Big[0 \ \cdots \ 0 \ A^{(\ell-2)}_{s-\ell_1+2,s+\theta+\ell_1} \ \cdots \ A^{(\ell-2)}_{s-\ell_1+2,e}\Big]^t = \sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}U^{(\ell-2-j)t}_{s-\ell_1+2} + [U^{(\ell-2)}]_{s-\ell_1+1}T^{(0)t}_{s-\ell_1+2}, \tag{4.3.23}$$

$$[T^{(0)}]_{s-\ell_1+1}\Big[0 \ \cdots \ 0 \ A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} \ \cdots \ A^{(\ell-y)}_{s-\ell_1+y,e}\Big]^t = \sum_{i=1}^{\ell-y}[U^{(i)}]_{s-\ell_1+1}Z^{(\ell-y-i)t}_{s-\ell_1+y} \quad \text{for } 3 \leq y \leq \ell-1, \tag{4.3.24}$$

$$[T^{(0)}]_{s-\ell_1+1}\Big[0 \cdots 0 \ I_{k_{s+\theta+\ell_1}} \ A^{(0)}_{s+\theta+\ell_1,s+\theta+\ell_1} \cdots A^{(0)}_{s+\theta+\ell_1,e}\Big]^t = 0, \tag{4.3.25}$$

$$\mathcal{D}iag\big(U^{(\ell-2)}_h U^{(\ell-2)t}_h\big) = 0, \tag{4.3.26}$$

$$\mathcal{D}iag\big(U^{(\ell-1)}_\nu U^{(\ell-1)t}_\nu\big) = 0, \tag{4.3.27}$$

where $1 \leq h \leq s-\ell+2$ and $1 \leq \nu \leq s-\ell+1$.

Since the code $\mathcal{C}_{\ell-2}$ is a self-orthogonal code satisfying the property $(*)$, so we have

$$\mathcal{D}iag\left(\sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-2-j)}]^t_{s-\ell_1+1}\right)=0.$$

We also note that $(A^{(0)})_{s-\ell_1+1,s+\theta+\ell_1}$ is a full row-rank matrix over $\mathbb{F}_{2^r}$. Now by applying Lemma 4.3.1, we see that there exist matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$ and $[U^{(\ell-1)}]_{s-\ell_1+1}$ satisfying (4.3.21),(4.3.22), (4.3.26) and (4.3.27) and that there are precisely

$$(2^r)^{\sum\limits_{i=\ell}^{s+\theta+\ell_1}k_in_{i-\ell+1}+\sum\limits_{j=\ell+1}^{s+\theta+\ell_1}k_jn_{j-\ell}+2n_{s-\ell_1+1}(n-n_{s+\ell_1+\theta})-n_{s-\ell+2}-n_{s-\ell+1}+n_{s-\ell_1+1}-n^2_{s-\ell_1+1}}$$

distinct choices for such a pair of matrices. Further, for a given choice of the pair of matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$ and $[U^{(\ell-1)}]_{s-\ell_1+1}$ satisfying (4.3.21),(4.3.22), (4.3.26) and (4.3.27), one can easily observe, for $2\leq y\leq \ell-1$, that there exists a matrix $\begin{bmatrix}0 & \cdots & 0 & A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} & \cdots & A^{(\ell-y)}_{s-\ell_1+y,e}\end{bmatrix}$ satisfying (4.3.23) and (4.3.24) and that such a matrix has precisely $(2^r)^{k_{s-\ell_1+y}(n-n_{s+\theta+\ell_1}-n_{s-\ell_1+1})}$ distinct choices. Furthermore, by applying Lemma 2.2.1 and Theorem 2.3.9 and working as in Proposition 4.3.1, we see that there exists a matrix $T^{(\ell)}_{s+\theta+\ell_1}$ satisfying (4.3.25) and that such a matrix has precisely

$$\begin{bmatrix}k_{s+\theta+\ell_1}+n-n_{s+\theta+\ell_1}-n_{s-\ell_1+1}\\ k_{s+\theta+\ell_1}\end{bmatrix}_{2^r}$$

distinct choices. Next, one can easily observe that each of the distinct choices of the matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$, $[U^{(\ell-1)}]_{s-\ell_1+1}$, $\begin{bmatrix}0 & \cdots & 0 & A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} & \cdots & A^{(\ell-y)}_{s-\ell_1+y,e}\end{bmatrix}$ for $2\leq y\leq \ell-1$ and $T^{(\ell)}_{s+\theta+\ell_1}$ satisfying (4.3.21)-(4.3.27) gives rise to a distinct and desired self-orthogonal code of the type $\{n_{s-\ell_1+1},k_{s-\ell_1+2},\ldots,k_{s+\theta+\ell_1}\}$ and length n over R_ℓ. From this, we get the desired result. □

Finally, let ℓ be a fixed positive integer satisfying $s+\theta+\theta_1+1\leq\ell\leq e$, and let $\ell_1=\lfloor\frac{\ell}{2}\rfloor$. In the following proposition, we show that given a self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2},k_{s-\ell_1+3},\ldots,k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, there exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1},k_{s-\ell_1+2},\ldots,k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell)=Tor_i(\mathcal{C}_{\ell-2})$ for $1\leq i\leq \ell-2$. We also count all such distinct self-orthogonal codes of the type $\{n_{s-\ell_1+1},k_{s-\ell_1+2},\ldots,k_{s+\theta+\ell_1}\}$ and length n over R_ℓ.

Proposition 4.3.4. *Let ℓ be a fixed integer satisfying $s+\theta+\theta_1+1 \leq \ell \leq e$, and let $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$. Let $\mathcal{C}_{\ell-2}$ be a self-orthogonal code of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$. Then the following hold.*

(a) There exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$.

(b) Moreover, each self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, k_{s-\ell_1+4}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$ gives rise to precisely

$$(2^r)^{\sum\limits_{i=\ell}^{s+\theta+\ell_1} k_i n_{i-\ell+1} + \sum\limits_{j=\ell+1}^{s+\theta+\ell_1} k_j n_{j-\ell} + (n_{s+\theta+\ell_1-1} + n_{s-\ell_1+1})(n - n_{s+\ell_1+\theta} - n_{s-\ell_1+1}) + n_{s-\ell_1+1} + n^2_{s-\ell_1+1}} \\ \times \begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+\theta+\ell_1} + n - n_{s+\theta+\ell_1} - n_{s-\ell_1+1} \\ k_{s+\theta+\ell_1} \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and with the $(i+1)$-th Torsion code as $Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$.

Proof. To prove the result, we first note that the code $Tor_1(\mathcal{C}_{\ell-2})$ is an $n_{s-\ell_1+2}$-dimensional code over $\mathbb{F}_{2^r}$. So we first choose an $n_{s-\ell_1+1}$-dimensional linear subcode (*i.e.*, subspace) $\mathcal{B}_1$ of the code $Tor_1(\mathcal{C}_{\ell-2})$. By Theorem 2.3.9, we see that the subcode $\mathcal{B}_1$ has precisely $\begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r}$ distinct choices. Further, without any loss of generality, we assume that the code $Tor_1(\mathcal{C}_{\ell-2})$ has a generator matrix

$$H = [T^{(0)}]_{s-\ell_1+2} = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_{s-\ell_1+2}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & \cdots & A_{1,s-\ell_1+1}^{(0)} & \cdots & A_{1,e}^{(0)} \\ 0 & I_{k_2} & \cdots & A_{2,s-\ell_1+1}^{(0)} & \cdots & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-\ell_1+2}} & \cdots & A_{s-\ell_1+2,e}^{(0)} \end{bmatrix}$$

and its subcode $\mathcal{B}_1$ has a generator matrix

$$[T^{(0)}]_{s-\ell_1+1} = \begin{bmatrix} T_1^{(0)} \\ T_2^{(0)} \\ \vdots \\ T_{s-\ell_1+1}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & A_{1,1}^{(0)} & \cdots & A_{1,s-\ell_1}^{(0)} & \cdots & A_{1,e-1}^{(0)} & A_{1,e}^{(0)} \\ 0 & I_{k_2} & \cdots & A_{2,s-\ell_1}^{(0)} & \cdots & A_{2,e-1}^{(0)} & A_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-\ell_1+1}} & \cdots & A_{s-\ell_1+1,e-1}^{(0)} & A_{s-\ell_1+1,e}^{(0)} \end{bmatrix},$$

where columns of the matrices H and $[T^{(0)}]_{s-\ell_1+1}$ are grouped into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathbb{F}_{2^r}$ and $A_{i,j}^{(0)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s - \ell_1 + 2$ and $i \leq j \leq e$. Furthermore, by Remark 4.3.1, we assume, without any loss of generality, that the matrix $(A^{(0)})_{s-\ell_1+1,s+\theta+\ell_1}$ is of full row-rank. We next assume, without any loss of generality, that the code $\mathcal{C}_{\ell-2}$ has a generator matrix

$$G_{\ell-2} = \begin{bmatrix} T_1^{(\ell-2)} \\ T_2^{(\ell-2)} \\ \vdots \\ T_{s-\ell_1+2}^{(\ell-2)} \\ uT_{s-\ell_1+3}^{(\ell-2)} \\ u^2T_{s-\ell_1+4}^{(\ell-2)} \\ \vdots \\ u^{\ell-3}T_{s+\theta+\ell_1-1}^{(\ell-2)} \end{bmatrix} = \begin{bmatrix} T_1^{(0)} + uU_1^{(1)} + u^2U_1^{(2)} + \cdots + u^{\ell-3}U_1^{(\ell-3)} \\ T_2^{(0)} + uU_2^{(1)} + u^2U_2^{(2)} + \cdots + u^{\ell-3}U_2^{(\ell-3)} \\ \vdots \\ T_{s-\ell_1+2}^{(0)} + uU_{s-\ell_1+2}^{(1)} + u^2U_{s-\ell_1+2}^{(2)} + \cdots + u^{\ell-3}U_{s-\ell_1+2}^{(\ell-3)} \\ uT_{s-\ell_1+3}^{(\ell-2)} \\ u^2T_{s-\ell_1+4}^{(\ell-2)} \\ \vdots \\ u^{\ell-3}T_{s+\theta+\ell_1-1}^{(\ell-2)} \end{bmatrix},$$

where $[T^{(0)}]_{s-\ell_1+2} \in \mathcal{M}_{n_{s-\ell_1+2}\times n}(\mathbb{F}_{2^r})$, $[U^{(j)}]_{s-\ell_1+2} \in \mathcal{M}_{n_{s-\ell_1+2}\times n}(\mathbb{F}_{2^r})$ for $1 \leq j \leq \ell - 3$, and the matrix $T_{s-\ell_1+i}^{(\ell-2)} \in \mathcal{M}_{k_{s-\ell_1+i}\times n}(R_{\ell-2})$ is of the form $T_{s-\ell_1+i}^{(\ell-2)} = Z_{s-\ell_1+i}^{(0)} + uZ_{s-\ell_1+i}^{(1)} + \cdots + u^{\ell-i-1}Z_{s-\ell_1+i}^{(\ell-i-1)}$ with $Z_{s-\ell_1+i}^{(0)}, Z_{s-\ell_1+i}^{(1)}, \ldots, Z_{s-\ell_1+i}^{(\ell-i-1)} \in \mathcal{M}_{k_{s-\ell_1+i}\times n}(\mathbb{F}_{2^r})$ for $3 \leq i \leq \ell - 1$.

Since $\mathcal{C}_{\ell-2}$ is a self-orthogonal code of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\theta+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, by applying Theorem 2.2.4(a), we get

$$\begin{aligned} [T^{(\ell-2)}]_{s-\ell_1+1}[T^{(\ell-2)}]_{s-\ell_1+1}^t &\equiv 0 \pmod{u^{\ell-2}}, \\ [T^{(\ell-2)}]_{s-\ell_1+1}T_{s-\ell_1+2+\beta}^{(\ell-2)t} &\equiv 0 \pmod{u^{\ell-2-\beta}} \text{ for } 0 \leq \beta \leq \ell-3, \\ T_{s-\ell_1+i}^{(\ell-2)}T_{s-\ell_1+j}^{(\ell-2)t} &\equiv 0 \pmod{u^{\ell+2-i-j}} \text{ for } 2 \leq i,j \leq \ell-1 \text{ and } i+j \leq \ell+1, \\ \mathcal{D}iag\big(U_h^{(\nu)}U_h^{(\nu)^t}\big) &= 0 \quad \text{for } 1 \leq h \leq \min\{s-\ell_1+2, s+\theta-\nu\} \quad \text{and} \\ & \qquad 1 \leq \nu \leq s-1+\theta. \end{aligned}$$

Now to show that there exists a self-orthogonal code of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and with the 1-th Torsion code as $\mathcal{B}_1$ and the $(i+1)$-th Torsion code as $Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell - 2$, let us define a matrix G_ℓ over R_ℓ as

$$G_\ell = \begin{bmatrix} T_1^{(\ell)} \\ T_2^{(\ell)} \\ \vdots \\ T_{s-\ell_1+1}^{(\ell)} \\ uT_{s-\ell_1+2}^{(\ell)} \\ \vdots \\ u^{\ell-1}T_{s+\theta+\ell_1}^{(\ell)} \end{bmatrix} = \begin{bmatrix} T_1^{(\ell-2)} + u^{\ell-2}U_1^{(\ell-2)} + u^{\ell-1}U_1^{(\ell-1)} \\ T_2^{(\ell-2)} + u^{\ell-2}U_2^{(\ell-2)} + u^{\ell-1}U_2^{(\ell-1)} \\ \vdots \\ T_{s-\ell_1+1}^{(\ell-2)} + u^{\ell-2}U_{s-\ell_1+1}^{(\ell-2)} + u^{\ell-1}U_{s-\ell_1+1}^{(\ell-1)} \\ uT_{s-\ell_1+2}^{(\ell)} \\ \vdots \\ u^{\ell-1}T_{s+\theta+\ell_1}^{(\ell)} \end{bmatrix} \tag{4.3.28}$$

with the matrices $[U^{(\alpha)}]_{s-\ell_1+1}$ for $\alpha \in \{\ell-2, \ell-1\}$, $T_{s-\ell_1+y}^{(\ell)}$ for $2 \leq y \leq \ell - 1$ and $T_{s+\theta+\ell_1}^{(\ell)}$ of the forms

$$\begin{bmatrix} U_1^{(\alpha)} \\ U_2^{(\alpha)} \\ \vdots \\ U_{s-\ell_1+1}^{(\alpha)} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & A_{1,\alpha+1}^{(\alpha)} & A_{1,\alpha+2}^{(\alpha)} & \cdots & A_{1,s-\ell_1+1+\alpha}^{(\alpha)} & \cdots & A_{1,e}^{(\alpha)} \\ 0 & \cdots & 0 & 0 & A_{2,\alpha+2}^{(\alpha)} & \cdots & A_{2,s-\ell_1+1+\alpha}^{(\alpha)} & \cdots & A_{2,e}^{(\alpha)} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & A_{s-\ell_1+1,s-\ell_1+1+\alpha}^{(\alpha)} & \cdots & A_{s-\ell_1+1,e}^{(\alpha)} \end{bmatrix},$$

$$T_{s-\ell_1+y}^{(\ell)} = T_{s-\ell_1+y}^{(\ell-2)} + u^{\ell-y}\begin{bmatrix} 0 & \cdots & 0 & A_{s-\ell_1+y,s+\theta+\ell_1}^{(\ell-y)} & \cdots & A_{s-\ell_1+y,e}^{(\ell-y)} \end{bmatrix} \text{ and}$$

$$T_{s+\theta+\ell_1}^{(\ell)} = \begin{bmatrix} 0 & \cdots & 0 & I_{k_{s+\theta+\ell_1}} & A_{s+\theta+\ell_1,s+\theta+\ell_1}^{(0)} & \cdots & A_{s+\theta+\ell_1,e}^{(0)} \end{bmatrix},$$

where $A_{i,j}^{(\alpha)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathbb{F}_{2^r})$ for $1 \leq i \leq s - \ell_1 + 1$ and $i + \alpha \leq j \leq e$, $A_{s-\ell_1+y,v}^{(\ell-y)} \in \mathcal{M}_{k_{s-\ell_1+y} \times k_{v+1}}(\mathbb{F}_{2^r})$ for $s+\theta+\ell_1 \leq v \leq e$ and $A_{s+\theta+\ell_1,b}^{(0)} \in \mathcal{M}_{k_{s+\theta+\ell_1} \times k_{b+1}}(\mathbb{F}_{2^r})$ for $s + \theta + \ell_1 \leq b \leq e$.

Now let $\mathcal{C}_\ell$ be a linear code of length n over R_ℓ with a generator matrix G_ℓ. It is easy to see that the code $\mathcal{C}_\ell$ is of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$, $Tor_1(\mathcal{C}_\ell) = \mathcal{B}_1$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell - 2$. By Theorem 2.2.4(a), we see that the code $\mathcal{C}_\ell$ is a self-orthogonal code over R_ℓ satisfying the property $(*)$ if and only if there exist matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$, $[U^{(\ell-1)}]_{s-\ell_1+1}$, $\begin{bmatrix} 0 & \cdots & 0 & A_{s-\ell_1+y,s+\theta+\ell_1}^{(\ell-y)} & \cdots & A_{s-\ell_1+y,e}^{(\ell-y)} \end{bmatrix}$ for $2 \leq y \leq \ell - 1$ and $T_{s+\theta+\ell_1}^{(\ell)}$ satisfying the following system of matrix equations over $\mathbb{F}_{2^r}$:

$$[T^{(0)}]_{s-\ell_1+1}[U^{(\ell-2)}]^t_{s-\ell_1+1} + [U^{(\ell-2)}]_{s-\ell_1+1}[T^{(0)}]^t_{s-\ell_1+1} = \sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-2-j)}]^t_{s-\ell_1+1}, \tag{4.3.29}$$

$$[T^{(0)}]_{s-\ell_1+1}[U^{(\ell-1)}]^t_{s-\ell_1+1} + [U^{(\ell-1)}]_{s-\ell_1+1}[T^{(0)}]^t_{s-\ell_1+1} = \sum_{j=1}^{\ell-2}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-1-j)}]^t_{s-\ell_1+1}, \tag{4.3.30}$$

$$[T^{(0)}]_{s-\ell_1+1}\left[0 \ \cdots \ 0 \ A^{(\ell-2)}_{s-\ell_1+2,s+\theta+\ell_1} \ \cdots \ A^{(\ell-2)}_{s-\ell_1+2,e}\right]^t = \sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}U^{(\ell-2-j)t}_{s-\ell_1+2} + [U^{(\ell-2)}]_{s-\ell_1+1}T^{(0)t}_{s-\ell_1+2}, \tag{4.3.31}$$

$$[T^{(0)}]_{s-\ell_1+1}\left[0 \ \cdots \ 0 \ A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} \ \cdots \ A^{(\ell-y)}_{s-\ell_1+y,e}\right]^t = \sum_{i=1}^{\ell-y}[U^{(i)}]_{s-\ell_1+1}Z^{(\ell-y-i)t}_{s-\ell_1+y} \quad \text{for } 3 \leq y \leq \ell-1, \tag{4.3.32}$$

$$[T^{(0)}]_{s-\ell_1+1}\left[0 \cdots 0 \ I_{k_{s+\theta+\ell_1}} \ A^{(0)}_{s+\theta+\ell_1,s+\theta+\ell_1} \cdots A^{(0)}_{s+\theta+\ell_1,e}\right]^t = 0. \tag{4.3.33}$$

Now to show that there exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\theta+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$, $Tor_1(\mathcal{C}_\ell) = \mathcal{B}_1$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell-2$, it is enough to show that the above system (4.3.29)-(4.3.33) of matrix equations in unknowns $[U^{(\ell-2)}]_{s-\ell_1+1}$, $[U^{(\ell-1)}]_{s-\ell_1+1}$, $T^{(\ell)}_{s+\theta+\ell_1}$ and $\left[0 \ \cdots \ 0 \ A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} \ \cdots \ A^{(\ell-y)}_{s-\ell_1+y,e}\right]$ for $2 \leq y \leq \ell-1$ has a solution.

Towards this, we first see that the code $\mathcal{C}_{\ell-2}$ is a self-orthogonal code satisfying the property $(*)$, so we have

$$\mathcal{D}iag\left(\sum_{j=1}^{\ell-3}[U^{(j)}]_{s-\ell_1+1}[U^{(\ell-2-j)}]^t_{s-\ell_1+1}\right) = 0.$$

Since $(A^{(0)})_{s-\ell_1+1,s+\theta+\ell_1}$ is a full row-rank matrix over $\mathbb{F}_{2^r}$, it is easy to observe that there exists a matrix $[U^{(\ell-2)}]_{s-\ell_1+1}$ satisfying (4.3.29) and that the number of choices for the matrix $[U^{(\ell-2)}]_{s-\ell_1+1}$ satisfying (4.3.29) is given by

$$(2^r)^{\sum\limits_{i=\ell}^{s+\theta+\ell_1} k_i n_{i-\ell+1} + n_{s-\ell_1+1}(n-n_{s+\ell_1+\theta}) - \frac{n_{s-\ell_1+1}(n_{s-\ell_1+1}-1)}{2}}.$$

Now for a given choice of the matrix $[U^{(\ell-2)}]_{s-\ell_1+1}$ satisfying (4.3.29), it is easy to observe that there exists a matrix $[U^{(\ell-1)}]_{s-\ell_1+1}$ satisfying (4.3.30) and that the number of choices for the matrix $[U^{(\ell-1)}]_{s-\ell_1+1}$ satisfying (4.3.30) is given by

$$(2^r)^{\sum\limits_{j=\ell+1}^{s+\theta+\ell_1} k_j n_{j-\ell} + n_{s-\ell_1+1}(n-n_{s+\ell_1+\theta}) - \frac{n_{s-\ell_1+1}(n_{s-\ell_1+1}-1)}{2}}.$$

Further, working in a similar manner as in Proposition 4.3.3, we see that for given choices of the matrices $[U^{(\ell-2)}]_{s-\ell_1+1}$ and $[U^{(\ell-1)}]_{s-\ell_1+1}$ satisfying (4.3.29) and (4.3.30), there exist matrices $\begin{bmatrix} 0 & \cdots & 0 & A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} & \cdots & A^{(\ell-y)}_{s-\ell_1+y,e} \end{bmatrix}$ for $2 \leq y \leq \ell - 1$ and $T^{(\ell)}_{s+\theta+\ell_1}$ satisfying (4.3.31)-(4.3.33) and that the number of choices for the matrices $\begin{bmatrix} 0 & \cdots & 0 & A^{(\ell-y)}_{s-\ell_1+y,s+\theta+\ell_1} & \cdots & A^{(\ell-y)}_{s-\ell_1+y,e} \end{bmatrix}$ for $2 \leq y \leq \ell - 1$ and $T^{(\ell)}_{s+\theta+\ell_1}$ satisfying (4.3.31)-(4.3.33) is given by

$$(2^r)^{(n_{s+\theta+\ell_1-1}-n_{s-\ell_1+1})(n-n_{s+\theta+\ell_1}-n_{s-\ell_1+1})} \begin{bmatrix} k_{s+\theta+\ell_1} + n - n_{s+\theta+\ell_1} - n_{s-\ell_1+1} \\ k_{s+\theta+\ell_1} \end{bmatrix}_{2^r}.$$

From this, the desired result follows immediately. □

In the following theorem, we show that if there exists a self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$, then there exists a self-orthogonal code $\mathcal{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfying $Tor_{s+\theta}(\mathcal{C}_e) = \mathcal{C}_0$, and vice versa. We also count all distinct self-orthogonal codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with the $(s+\theta)$-th Torsion code as a given self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$. The proof of the following theorem also provides a method to construct a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with the $(s+\theta)$-th Torsion code as a given self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$.

Theorem 4.3.1. *(a) There exists a self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ if and only if there exists a self-orthogonal code $\mathcal{C}_e$ of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over R_e satisfying $Tor_{s+\theta}(\mathcal{C}_e) = \mathcal{C}_0$.*

(b) Moreover, each self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ gives rise to precisely

$$(2^r)^{\sum\limits_{\ell=1}^{s} n_\ell(n-n_{\ell+1}) + \sum\limits_{v=1}^{s+\theta-1} n_{s+v}(n-n_{s+j+1}-n_{s+\theta-j}) - (1-\theta)\frac{n_s(n_s-1)}{2}}$$

$$\times \prod_{i=1}^{s+\theta} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} \prod_{j=s+1+\theta}^{e} \begin{bmatrix} k_j + n - n_j - n_{e+1-j} \\ k_j \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with the $(s+\theta)$-th Torsion code as $\mathcal{C}_0$.

Proof. To prove the result, let $\mathcal{C}_e$ be a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e. By Lemma 2.2.1, we see that the $(s+\theta)$-th Torsion code $Tor_{s+\theta}(\mathcal{C}_e)$ of $\mathcal{C}_e$ is a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$.

On the other hand, let $\mathcal{C}_0$ be a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$. Here we first observe that any self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e must satisfy the property $(*)$. We will now recursively construct a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfying the property $(*)$ and with the $(s+\theta)$-th Torsion code as $\mathcal{C}_0$. For this, we will distinguish the following two cases: (i) e is even and (ii) e is odd.

(i) First let e be even. In this case, we have $\theta = 0$. Here we will show that there exists a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfying the property $(*)$ and with the s-th Torsion code as $\mathcal{C}_0$, and we will also enumerate such codes. To do this, we see, by applying Proposition 4.3.1, that there exists a self-orthogonal code $\mathcal{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over R_2 satisfying the property $(*)$ and $Tor_1(\mathcal{C}_2) = \mathcal{C}_0$, and that the code $\mathcal{C}_2$ has precisely

$$(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + n_s(n-n_{s+2}) - n_{s-1} - \frac{n_s(n_s-1)}{2}} \begin{bmatrix} k_{s+1} + n - n_{s+1} - n_s \\ k_{s+1} \end{bmatrix}_{2^r}$$

distinct choices for a given choice of $\mathcal{C}_0$. Further, for an even integer ℓ satisfying $4 \leq \ell \leq s + \theta_1$, we see, by applying Proposition 4.3.3, that if there exists a self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, then there exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell - 2$, and that the code $\mathcal{C}_\ell$ has precisely

$$(2^r)^{\sum\limits_{i=\ell}^{s+\ell_1} k_i n_{i-\ell+1} + \sum\limits_{j=\ell+1}^{s+\ell_1} k_j n_{j-\ell} + \Lambda} \begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+\ell_1} + n - n_{s+\ell_1} - n_{s-\ell_1+1} \\ k_{s+\ell_1} \end{bmatrix}_{2^r}$$

distinct choices for a given choice of the code $\mathcal{C}_{\ell-2}$, where $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$ and $\Lambda = (n_{s+\ell_1-1} + n_{s-\ell_1+1})(n - n_{s+\ell_1} - n_{s-\ell_1+1}) + n_{s-\ell_1+1} + n^2_{s-\ell_1+1} - n_{s-\ell+2} - n_{s-\ell+1}$. Further, for an even integer ℓ satisfying $s + \theta_1 + 1 \leq \ell \leq e$, we note, by applying Proposition 4.3.4, that if there exists a self-orthogonal code $\mathcal{C}_{\ell-2}$ of the type $\{n_{s-\ell_1+2}, k_{s-\ell_1+3}, \ldots, k_{s+\ell_1-1}\}$ and length n over $R_{\ell-2}$ satisfying the property $(*)$, then there exists a self-orthogonal code $\mathcal{C}_\ell$ of the type $\{n_{s-\ell_1+1}, k_{s-\ell_1+2}, \ldots, k_{s+\ell_1}\}$ and length n over R_ℓ satisfying the property $(*)$ and $Tor_{i+1}(\mathcal{C}_\ell) = Tor_i(\mathcal{C}_{\ell-2})$ for $1 \leq i \leq \ell - 2$, and that the code $\mathcal{C}_\ell$ has precisely

$$(2^r)^{\sum\limits_{i=\ell}^{s+\ell_1} k_i n_{i-\ell+1} + \sum\limits_{j=\ell+1}^{s+\ell_1} k_j n_{j-\ell} + (n_{s+\ell_1-1} + n_{s-\ell_1+1})(n - n_{s+\ell_1} - n_{s-\ell_1+1}) + n_{s-\ell_1+1} + n^2_{s-\ell_1+1}} \\ \times \begin{bmatrix} n_{s-\ell_1+2} \\ n_{s-\ell_1+1} \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+\ell_1} + n - n_{s+\ell_1} - n_{s-\ell_1+1} \\ k_{s+\ell_1} \end{bmatrix}_{2^r}$$

distinct choices for a given choice of the code $\mathcal{C}_{\ell-2}$, where $\ell_1 = \lfloor \frac{\ell}{2} \rfloor$. From this, it follows that there exists a self-orthogonal code $\mathcal{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfying the property $(*)$ and $Tor_s(\mathcal{C}_e) = \mathcal{C}_0$, and that the code $\mathcal{C}_e$ has precisely

$$(2^r)^{\sum\limits_{\ell=1}^{s} n_\ell (n - n_{\ell+1}) + \sum\limits_{v=1}^{s-1} n_{s+v}(n - n_{s+j+1} - n_{s-j}) - \frac{n_s(n_s-1)}{2}} \prod_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} \\ \times \prod_{j=s+1}^{e} \begin{bmatrix} k_j + n - n_j - n_{e+1-j} \\ k_j \end{bmatrix}_{2^r}$$

distinct choices for a given choice of the code $\mathcal{C}_0$.

(ii) Let e be odd. In this case, we have $\theta = 1$. Here working in a similar manner as in case (i) and by applying Propositions 4.3.2-4.3.4, the desired result follows immediately.

□

In the following theorem, we consider the case $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$ and $k_i = k_{e-i+2}$ for $2 \leq i \leq e$, and we show that there exists a self-orthogonal code

$\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ if and only if there exists a self-dual code $\mathcal{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e satisfying $Tor_{s+\theta}(\mathcal{C}_e) = \mathcal{C}_0$. We also count all distinct self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with the $(s+\theta)$-th Torsion code as a given self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$. The proof of the following theorem also provides a method to construct a self-dual code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with the $(s+\theta)$-th Torsion code as a given self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$.

Theorem 4.3.2. *Let $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$ and $k_i = k_{e-i+2}$ for $2 \leq i \leq e$.*

(a) There exists a self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ if and only if there exists a self-dual code $\mathcal{C}_e$ of the type $\{k_1, k_2, \ldots, k_{e-1}, k_e\}$ and length n over R_e satisfying $Tor_{s+\theta}(\mathcal{C}_e) = \mathcal{C}_0$. (When e is odd, we see that $n_{s+\theta} = \frac{n}{2}$ and that a self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ is a self-dual code. This may not hold in the case when e is even.)

(b) Moreover, each self-orthogonal code $\mathcal{C}_0$ of length n and dimension $n_{s+\theta}$ over $\mathbb{F}_{2^r}$ gives rise to precisely

$$(2^r)^{\sum\limits_{\ell=1}^{s} n_\ell(n-n_{\ell+1})-(1-\theta)\frac{n_s(n_s-1)}{2}} \prod_{i=1}^{s+\theta} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r}$$

distinct self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e with $\mathcal{C}_0$ as the $(s+\theta)$-th Torsion code.

Proof. By Theorem 2.2.4(b), we see that a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over R_e is self-dual if and only if $k_i = k_{e-i+2}$ for $1 \leq i \leq e$. So on taking $k_i = k_{e-i+2}$ for $1 \leq i \leq e$ in Theorem 4.3.1, the desired result follows. □

4.4 Enumeration formulae for self-orthogonal and self-dual codes of length n over R_e

From now on, throughout this chapter, let $\mathcal{S}_e(n; k_1, k_2, \ldots, k_e)$ and $\mathcal{D}_e(n; k_1, k_2, \ldots, k_e)$ denote the number of distinct self-orthogonal and self-dual codes of the type

$\{k_1, k_2, \ldots, k_e\}$ and length n over R_e, respectively. Further, let $\mathcal{S}_e(n)$ and $\mathcal{D}_e(n)$ denote the number of distinct self-orthogonal and self-dual codes of length n over R_e, respectively. In this section, we will obtain enumeration formulae for the numbers $\mathcal{S}_e(n; k_1, k_2, \ldots, k_e)$, $\mathcal{D}_e(n; k_1, k_2, \ldots, k_e)$, $\mathcal{S}_e(n)$ and $\mathcal{D}_e(n)$. Towards this, we recall, from Chapter 2, that $\sigma_{2^r}(n, k)$ equals the number of distinct self-orthogonal codes of length n and dimension k over $\mathbb{F}_{2^r}$, where $0 \leq k \leq n$. Note that $\sigma_{2^r}(n, 0) = 1$ and $\sigma_{2^r}(n, k) = 0$ for all integers $k > \lceil \frac{n}{2} \rceil$. For $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$, let $\sigma_{2^r}(n, k)$ be as determined in Theorem 2.3.11.

In the following theorem, we obtain the explicit enumeration formula for the number $\mathcal{S}_e(n; k_1, k_2, \ldots, k_e)$.

Theorem 4.4.1. *Let $e \geq 2$ be an integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$.*

(a) When e is even, we have

$$\mathcal{S}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{2^r}\left(n, n_s\right) \displaystyle\prod_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} \prod_{j=s+1}^{e} \begin{bmatrix} k_j + n - n_j - n_{e+1-j} \\ k_j \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell (n - n_{\ell+1}) + n_{s+\ell}(n - n_{s+\ell+1} - n_{s-\ell}) + n_s(n - n_{s+1}) - \frac{n_s(n_s-1)}{2}} \\ \text{ \textit{if} } n_{e-v+1} + n_v \leq n \quad \textit{for } s+1 \leq v \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathcal{S}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{2^r}\left(n, n_{s+1}\right) \displaystyle\prod_{i=1}^{s+1} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} \prod_{j=s+2}^{e} \begin{bmatrix} k_j + n - n_j - n_{e+1-j} \\ k_j \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{\ell=1}^{s} n_\ell (n - n_{\ell+1}) + n_{s+\ell}(n - n_{s+1+\ell} - n_{s+1-\ell})} \\ \text{ \textit{if} } n_{e-v+1} + n_v \leq n \quad \textit{for } s+1 \leq v \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

Proof. To prove the result, we see, by Remark 2.2.1, that $\mathcal{S}_e(n; k_1, k_2, \ldots, k_e) = 0$ if $n_{e-v+1} + n_v > n$ for some integer v satisfying $s + 1 \leq v \leq e$. On the other hand, when $n_{e-v+1}+n_v \leq n$ for $s+1 \leq v \leq e$, by applying Theorems 2.3.11 and 4.3.1, the desired result follows immediately. □

In the following theorem, we obtain the explicit enumeration formula for the number $\mathcal{D}_e(n; k_1, k_2, \ldots, k_e)$.

Theorem 4.4.2. *Let $e \geq 2$ be an integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$. Then we have the following:*

(a) When e is even, we have

$$\mathcal{D}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \sigma_{2^r}(n, n_s) \prod_{i=1}^{s} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} (2^r)^{\sum_{\ell=1}^{s-1} n_\ell(n-n_{\ell+1}) + \frac{n_s(n_s+1)}{2}} \\ \text{if } k_v = k_{e-v+2} \quad \text{for} \quad 1 \leq v \leq e+1; \\ 0 \qquad \text{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathcal{D}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \prod_{j=1}^{\frac{n}{2}-1} ((2^r)^{\frac{n}{2}-j}+1) \prod_{i=1}^{s+1} \begin{bmatrix} n_i \\ k_i \end{bmatrix}_{2^r} (2^r)^{\sum_{\ell=1}^{s} n_\ell(n-n_{\ell+1})} \\ \text{if } n \text{ is even and } k_v = k_{e-v+2} \text{ for } 1 \leq v \leq e+1; \\ 0 \qquad \text{otherwise.} \end{cases}$$

Proof. To prove the result, we see, by Theorem 2.2.4(b), that $\mathcal{D}_e(n; k_1, k_2, \ldots, k_e) = 0$ if $k_v \neq k_{e-v+2}$ for some integer v satisfying $1 \leq v \leq e+1$. On the other hand, when $k_v = k_{e-v+2}$ for $1 \leq v \leq e+1$, the desired result follows on taking $k_v = k_{e-v+2}$ for $1 \leq v \leq e+1$ in Theorem 4.4.1 and by applying Theorem 2.3.11. □

We will next determine the numbers $\mathcal{S}_e(n)$ and $\mathcal{D}_e(n)$. To do this, for an integer d satisfying $1 \leq d \leq e$ and for non-negative integers $k_1, k_2, \ldots, k_d$, let the numbers $h_j(k_1, k_2, \ldots, k_d)$ and $m_\ell(k_1, k_2, \ldots, k_d)$ be as defined by (3.4.19) and (3.4.20), respectively, for $1 \leq j \leq d-1$ and $1 \leq \ell \leq \lceil \frac{d}{2} \rceil - 1$.

In the following theorem, we obtain the explicit enumeration formula for the number $\mathcal{S}_e(n)$.

Theorem 4.4.3. *For an integer $e \geq 2$, we have the following:*

(a) When e is even, we have

$$\begin{aligned}\mathcal{S}_e(n) &= \sum \sigma_{2^r}\big(n, k_1+k_2+\cdots+k_s\big)\prod_{i=1}^{s}\begin{bmatrix}k_1+k_2+\cdots+k_i\\ k_i\end{bmatrix}_{2^r}\\ &\quad\times\prod_{j=s+1}^{e}\begin{bmatrix}k_j+n-(k_1+k_2+\cdots+k_j)-(k_1+k_2+\cdots+k_{e+1-j})\\ k_j\end{bmatrix}_{2^r}\\ &\quad\times(2^r)^{\sum\limits_{\ell=1}^{s-1} m_\ell(k_1,k_2,\ldots,k_e)+\sum\limits_{a=1}^{s}(k_1+k_2+\cdots+k_a)+h_s(k_1,k_2,\ldots,k_e)-\lambda'_e(k_1,k_2,\ldots,k_e)},\end{aligned}$$

where $\lambda'_e(k_1,k_2,\ldots,k_e) = (k_1+k_2+\cdots+k_s)\left(\frac{k_1+k_2+\cdots+k_s-1}{2}\right)$ and the summation $\sum$ runs over all non-negative integers $k_1,k_2,\ldots,k_e$ satisfying $2k_1+2k_2+\cdots+2k_{e-i+1}+k_{e-i+2}+k_{e-i+3}+\cdots+k_i \leq n$ for $s+1 \leq i \leq e$.

(b) When e is odd, we have

$$\begin{aligned}\mathcal{S}_e(n) &= \sum \sigma_{2^r}\big(n, k_1+k_2+\cdots+k_{s+1}\big)\prod_{i=1}^{s+1}\begin{bmatrix}k_1+k_2+\cdots+k_i\\ k_i\end{bmatrix}_{2^r}\\ &\quad\times\prod_{j=s+2}^{e}\begin{bmatrix}k_j+n-(k_1+k_2+\cdots+k_j)-(k_1+k_2+\cdots+k_{e+1-j})\\ k_j\end{bmatrix}_{2^r}\\ &\qquad\qquad\times(2^r)^{\sum\limits_{\ell=1}^{s} m_\ell(k_1,k_2,\ldots,k_e)+(k_1+k_2+\cdots+k_\ell)},\end{aligned}$$

where the summation $\sum$ runs over all non-negative integers $k_1,k_2,\ldots,k_e$ satisfying $2k_1+2k_2+\cdots+2k_{e-i+1}+k_{e-i+2}+k_{e-i+3}+\cdots+k_i \leq n$ for $s+1 \leq i \leq e$.

Proof. It follows immediately from Theorem 4.4.1. □

In the following theorem, we obtain the explicit enumeration formula for the number $\mathcal{D}_e(n)$.

Theorem 4.4.4. *(a) When e is even, we have*

$$\begin{aligned}\mathcal{D}_e(n) &= \sum \sigma_{2^r}(n, k_1+k_2+\cdots+k_s)\prod_{i=1}^{s}\begin{bmatrix}k_1+k_2+\cdots+k_i\\ k_i\end{bmatrix}_{2^r}\\ &\quad\times(2^r)^{\sum\limits_{\ell=1}^{s-1} h_\ell(k_1,k_2,\ldots,k_s)+(k_1+k_2+\cdots+k_\ell)+\lambda''_e(k_1,k_2,\ldots,k_s)},\end{aligned}$$

where the summation $\sum$ *runs over all non-negative integers* $k_1, k_2, \ldots, k_{s+1}$ *satisfying* $2(k_1 + k_2 \cdots + k_s) + k_{s+1} = n$ *and the number* $\lambda_e^{''}(k_1, k_2, \ldots, k_s)$ *is given by*

$$\lambda_e^{''}(k_1, k_2, \ldots, k_s) = (k_1 + k_2 + \cdots + k_s) \left(\frac{k_1 + k_2 + \cdots + k_s + 1}{2} \right).$$

(b) When e is odd, we have

$$\mathcal{D}_e(n) = \begin{cases} \sum \prod\limits_{j=1}^{\frac{n}{2}-1} ((2^r)^{\frac{n}{2}-j} + 1) \prod\limits_{i=1}^{s+1} \begin{bmatrix} k_1 + k_2 + \cdots + k_i \\ k_i \end{bmatrix}_{2^r} & \\ \times (2^r)^{\sum\limits_{\ell=1}^{s} h_\ell(k_1,k_2,\ldots,k_s) + (k_1+k_2+\cdots+k_\ell)} & \text{if } n \text{ is even;} \\ 0 \quad \text{otherwise,} & \end{cases}$$

where the summation $\sum$ *runs over all non-negative integers* $k_1, k_2, \ldots, k_{s+1}$ *satisfying* $2(k_1 + k_2 \cdots + k_{s+1}) = n$.

Proof. It follows immediately from Theorem 4.4.2. □

Remark 4.4.1. *Theorem 2 and Corollary 1 of Galvez et al. [47] follow, as special cases, on taking* $e = 2$ *in Theorems 4.4.1 and 4.4.4, respectively, while Theorem 1 of Betty et al. [13] follows on taking* $e = 3$ *in Theorem 4.4.4.*

The following example illustrates Theorems 4.4.3 and 4.4.4.

Example 4.4.1. *When* $r = 1$, *we see, by carrying out computations in the Magma Computational Algebra System, that* $\mathcal{S}_4(2) = 25$, $\mathcal{S}_4(3) = 459$, $\mathcal{S}_4(4) = 18321$, $\mathcal{S}_4(5) = 1616679$, $\mathcal{S}_5(2) = 32$, $\mathcal{S}_5(3) = 1014$, $\mathcal{S}_5(4) = 83991$, $\mathcal{S}_5(5) = 18404093$, $\mathcal{D}_4(2) = 7$, $\mathcal{D}_4(3) = 31$, $\mathcal{D}_4(4) = 823$, $\mathcal{D}_4(5) = 11191$, $\mathcal{D}_5(2) = 7$, $\mathcal{D}_5(3) = 0$, $\mathcal{D}_5(4) = 1719$ *and* $\mathcal{D}_5(5) = 0$, *which agree with Theorems 4.4.3 and 4.4.4.*

The enumeration formulae for $\mathcal{S}_e(n)$ and $\mathcal{D}_e(n)$, obtained in Theorems 4.4.3 and 4.4.4, are useful in the classification of self-orthogonal and self-dual codes of length n over R_e, which we illustrate in the following section in certain specific cases.

4.5 Classification of self-orthogonal and self-dual codes

The enumeration formulae for self-orthogonal and self-dual codes of length n over R_e, obtained in Theorems 4.4.3 and 4.4.4, are useful in the determination of complete lists of inequivalent self-orthogonal and self-dual codes of length n over R_e (cf. [13], [53, Sec. 9.6 and 9.7]). We will illustrate this in certain specific cases by applying the classification algorithm ([53, Sec. 9.7]) and by carrying out computations in the Magma Computational Algebra System. More precisely, we will classify all self-orthogonal and self-dual codes of lengths $2, 3, 4$ and 5 over $\mathbb{F}_2[u]/\langle u^3\rangle$ and of lengths $2, 3$ and 4 over $\mathbb{F}_4[u]/\langle u^2\rangle$ up to monomial equivalence. We will also explicitly determine a generator matrix of the code representative of each equivalence class of these codes.

I. There are precisely 6 inequivalent non-zero self-orthogonal codes of length 2 over $\mathbb{F}_2[u]/\langle u^3\rangle$. Among these codes, there are

- 3 self-orthogonal codes of Hamming distance 1, whose generator matrices are u^2I_2, $\begin{bmatrix} u^2 & 0 \end{bmatrix}$ and $\begin{bmatrix} u & u \\ 0 & u^2 \end{bmatrix}$; and
- 3 self-orthogonal codes of Hamming distance 2, whose generator matrices are $\begin{bmatrix} u & u \end{bmatrix}$, $\begin{bmatrix} 1 & 1 \end{bmatrix}$ and $\begin{bmatrix} u^2 & u^2 \end{bmatrix}$.

II. There are precisely 19 inequivalent non-zero self-orthogonal codes of length 3 over $\mathbb{F}_2[u]/\langle u^3\rangle$. Among these codes, there are

- 10 self-orthogonal codes of Hamming distance 1, whose generator matrices are u^2I_3, $\begin{bmatrix} u^2 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & u & 0 \\ 0 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} u & u & u^2 \\ 0 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & u+u^2 \\ 0 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} u^2 & 0 & 0 \\ 0 & u^2 & u^2 \end{bmatrix}$, $\begin{bmatrix} u^2 & 0 & 0 \\ 0 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & u & 1+u \\ 0 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 1+u^2 \\ 0 & u^2 & 0 \end{bmatrix}$ and $\begin{bmatrix} u & 0 & u \\ 0 & u^2 & 0 \\ 0 & 0 & u^2 \end{bmatrix}$;
- 8 self-orthogonal codes of Hamming distance 2, whose generator matrices are

$$\begin{bmatrix}1 & 1 & 0\end{bmatrix}, \begin{bmatrix}1 & u^2 & 1\end{bmatrix}, \begin{bmatrix}1 & u & 1+u\end{bmatrix}, \begin{bmatrix}u & u & 0\end{bmatrix}, \begin{bmatrix}u & u^2 & u+u^2\end{bmatrix}, \begin{bmatrix}u^2 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}u & u & u^2\\ 0 & u^2 & u^2\end{bmatrix} \text{ and } \begin{bmatrix}u^2 & 0 & u^2\\ 0 & u^2 & u^2\end{bmatrix}; \text{ and}$$

- 1 self-orthogonal code of Hamming distance 3 and with a generator matrix $\begin{bmatrix}u^2 & u^2 & u^2\end{bmatrix}$.

III. There are precisely 83 inequivalent non-zero self-orthogonal codes of length 4 over $\mathbb{F}_2[u]/\langle u^3\rangle$. Among these codes, there are

- 37 self-orthogonal codes of Hamming distance 1, whose generator matrices are

$$u^2 I_4, \begin{bmatrix}u^2 & 0 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & u+u^2 & u^2 & 0\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & u & 0 & 0\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & u^2 & 0 & u\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & u & u^2\\ 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}u & u & u & u\\ 0 & u^2 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}u & u & u^2 & u^2\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & 0\\ 0 & u^2 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & 0\\ 0 & u^2 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & u & 0 & 1+u\\ 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}u^2 & 0 & 0 & 0\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 1 & u^2\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u & 1+u\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & u & u+u^2 & 1\\ 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & u & u^2 & 1+u+u^2\\ 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & u & u & u\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u+u^2\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix}u & 0 & u & 0\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & u & 0\\ 0 & u^2 & 0 & u^2\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & u & u^2\\ 0 & u^2 & 0 & u^2\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u & u & 0 & u^2\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u\\ 0 & u & u & 0\\ 0 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix}u & 0 & u & u^2\\ 0 & u & 0 & u\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & u^2\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & 0\\ 0 & u^2 & 0 & u^2\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & 0\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & u & u & 1+u^2\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u & 1+u\\ 0 & u^2 & 0 & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & u+u^2 & u & 1\\ 0 & u & u & 0\\ 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & 1+u\\ 0 & u & u+u^2 & u^2\\ 0 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u^2 \\ 0 & u & 0 & u \\ 0 & 0 & u^2 & 0 \\ 0 & 0 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 \\ 0 & u^2 & 0 & 0 \\ 0 & 0 & u^2 & 0 \\ 0 & 0 & 0 & u^2 \end{bmatrix} \text{ and } \begin{bmatrix} u & u & u & u \\ 0 & u^2 & 0 & 0 \\ 0 & 0 & u^2 & 0 \\ 0 & 0 & 0 & u^2 \end{bmatrix};$$

- 42 self-orthogonal codes of Hamming distance 2, whose generator matrices are

$$\begin{bmatrix} u & u & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 \end{bmatrix}, \begin{bmatrix} u & u & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & u^2 & u^2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & u^2 & 1 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 1 & u & 0 & 1+u \end{bmatrix}, \begin{bmatrix} 1 & 1+u & u & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & u & u \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 \\ 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & u^2 & 0 & u \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u^2 & 0 & u \\ 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u^2 & u^2 \\ 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u^2 & 0 \\ 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & u & u^2 & u^2 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1+u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & u^2 \\ 0 & 1 & u^2 & 1+u^2 \end{bmatrix}, \begin{bmatrix} u & u+u^2 & u & u+u^2 \\ 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & u^2 \\ 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & u^2 & 0 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 1+u+u^2 \\ 0 & 1 & 1+u+u^2 & u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & u & u^2 & u+u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1+u^2 \\ 0 & u & u & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 1+u+u^2 \\ 0 & u & u & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u^2 & u^2 \\ 0 & u & 0 & u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & u & 0 & u \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u+u^2 \\ 0 & u & u & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u^2 & u+u^2 \\ 0 & u & u & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u+u^2 & 0 \\ 0 & u & 0 & u+u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 1+u^2 & u+u^2 \\ 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & 1+u+u^2 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u^2 & 1 \\ 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1+u^2 \\ 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1+u^2 & 1 \\ 0 & u & u^2 & u+u^2 \\ 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 \\ 0 & u^2 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u & u \\ 0 & u^2 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u+u^2 \\ 0 & u & u & 0 \\ 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 \\ 0 & u^2 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1+u & 1 & 1+u+u^2 \\ 0 & u^2 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 \end{bmatrix};$$

- 1 self-orthogonal code of Hamming distance 3 and with a generator matrix

$\begin{bmatrix} u^2 & u^2 & 0 & u^2 \end{bmatrix}$; and

- 3 self-orthogonal codes of Hamming distance 4, whose generator matrices are $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$, $\begin{bmatrix} u & u+u^2 & u & u \end{bmatrix}$ and $\begin{bmatrix} u^2 & u^2 & u^2 & u^2 \end{bmatrix}$.

IV. There are precisely 334 inequivalent non-zero self-orthogonal codes of length 5 over $\mathbb{F}_2[u]/\langle u^3\rangle$. Among these codes, there are

- 157 self-orthogonal codes of Hamming distance 1, whose generator matrices are

$$u^2 I_5,\ \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & u & u & u & 0 \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix},\ \begin{bmatrix} u & u & 0 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & u & u^2 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & u & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & 0 & u+u^2 & u+u^2 & u \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & u & u & u^2 \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & 0 & u^2 & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u & 0 & u^2 & u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 0 & 0 & 1+u \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & 1 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & u^2 & u^2 \end{bmatrix},\ \begin{bmatrix} 1 & u & u^2 & 0 & 1+u \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & u^2 & 1+u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u^2 & 0 & 0 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} u^2 & 0 & u^2 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 1 & u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & u & u & 0 & 1 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & u+u^2 & u & 1 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & u^2 & u & 1+u \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 1+u & 1+u^2 & 1 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & 1 & 1+u+u^2 & 1+u \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & 1+u+u^2 & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 1+u & u & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & u & u^2 & 1+u & u^2 \\ 0 & u^2 & 0 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & u+u^2 & 1+u+u^2 & u^2 \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & u^2 & u^2 & 1 \\ 0 & u & 0 & u+u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & 0 & u+u^2 & 1+u^2 & u \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},\ \begin{bmatrix} 1 & u^2 & u+u^2 & 0 & 1+u \\ 0 & u & 0 & u+u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u^2 & 1 & 0\\ 0 & u & u+u^2 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1+u+u^2 & u & 1 & 1\\ 0 & u & u^2 & u^2 & u\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & u+u^2 & 1+u+u^2 & 1\\ 0 & u & u^2 & u+u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u & u^2 & 1+u\\ 0 & u & u & u^2 & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u^2 & 1 & u^2\\ 0 & u & u+u^2 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1+u & u^2 & 1+u^2 & 1+u\\ 0 & u & u^2 & u & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u^2 & 0 & 1\\ 0 & u & u & u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u^2 & u & 1+u\\ 0 & u & u+u^2 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & 0 & 1+u\\ 0 & u & u^2 & u+u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & u & u^2 & u & 1\\ 0 & u & u & u^2 & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & 0 & 1+u+u^2\\ 0 & u & u+u^2 & 0 & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & u+u^2 & u+u^2 & 0 & 1\\ 0 & u & 0 & u & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & u & 0 & u & 1\\ 0 & u & 0 & u & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u^2 & u+u^2 & 1+u+u^2\\ 0 & u & u & u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & u^2 & u^2 & 1+u+u^2 & u\\ 0 & u & 0 & u^2 & u\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & u^2 & u^2 & u^2 & 1\\ 0 & u & u+u^2 & u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1+u^2 & 0 & 1+u & 1+u\\ 0 & u & 0 & u+u^2 & 0\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u & u+u^2 & 1+u^2\\ 0 & 1 & u & 1+u^2 & u\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u & u^2 & 1+u\\ 0 & 1 & 0 & 1 & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u & 1+u+u^2 & u^2\\ 0 & 1 & u & 0 & 1+u\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & u^2 & 1+u^2\\ 0 & 1 & 0 & 1+u^2 & u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & 1+u^2 & 0\\ 0 & 1 & 0 & 0 & 1\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u & 1+u^2 & u\\ 0 & 1 & 0 & u+u^2 & 1+u+u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1+u^2 & 0\\ 0 & 1 & u & 0 & 1+u\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}u^2 & 0 & 0 & 0 & 0\\ 0 & u^2 & 0 & u^2 & u^2\\ 0 & 0 & u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u^2 & 0 & 0 & 0 & 0\\ 0 & u^2 & 0 & 0 & u^2\\ 0 & 0 & u^2 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1+u+u^2 & u+u^2\\ 0 & 1 & 0 & u+u^2 & 1+u+u^2\\ 0 & 0 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u+u^2 & 0 \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u & 0 & u+u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 1+u+u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u+u^2 & 0 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & 0 & 1+u+u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 0 & 1+u^2 & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1+u^2 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & 1 & 1+u+u^2 & 1 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u^2 & u+u^2 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 1+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & u & 1+u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 0 & u^2 & 1+u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & u^2 & 1+u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 0 & 1+u+u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1+u & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 0 & 1 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 0 & 1+u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 1 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 0 & 1 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u & u^2 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & u & 0 & 0 & u^2 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u & u & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & u^2 \\ 0 & u & 0 & u & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u \\ 0 & u & u & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u & 0 & 0 & u \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u & 0 & u^2 & u+u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & u & 1 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & u^2 \\ 0 & u & 0 & 0 & u \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & u & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & 0 & u+u^2 & u \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & 0 & u+u^2 & u \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & u^2 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & 0 & u & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & 0 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & 0 & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u & u \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u & u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u & u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & u & 1 & 1+u+u^2 \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & 1+u+u^2 \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & u & 0 & 1+u \\ 0 & u & 0 & u & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 0 & 1+u+u^2 \\ 0 & u^2 & 0 & 0 & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1+u & 0 & 1+u \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1+u^2 \\ 0 & u & 0 & u & 0 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & 1 & 0 & 1+u \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & u & 1 & 1 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix}1 & u & 0 & u & 1+u^2\\ 0 & u^2 & 0 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 0 & 1+u^2\\ 0 & u^2 & 0 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & u & u & u & 1+u\\ 0 & u^2 & 0 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u & u & 1\\ 0 & u & u & 0 & u^2\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & 0 & u\\ 0 & u & 0 & u & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\\ 0 & 0 & 0 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & u & u & u & 0\\ 0 & u^2 & 0 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\\ 0 & 0 & 0 & 0 & u^2\end{bmatrix} \text{ and}$$

$$\begin{bmatrix}u & 0 & 0 & 0 & u\\ 0 & u^2 & 0 & 0 & 0\\ 0 & 0 & u^2 & 0 & 0\\ 0 & 0 & 0 & u^2 & 0\\ 0 & 0 & 0 & 0 & u^2\end{bmatrix};$$

- 165 self-orthogonal codes of Hamming distance 2, whose generator matrices are

$$\begin{bmatrix}u & u+u^2 & u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & u^2 & 0 & 0 & u\end{bmatrix}, \begin{bmatrix}u & 0 & u & 0 & 0\end{bmatrix}, \begin{bmatrix}u & u^2 & u+u^2 & u^2 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & 1 & 0\end{bmatrix}, \begin{bmatrix}1 & u^2 & 1+u^2 & u & u\end{bmatrix}, \begin{bmatrix}1 & 0 & u & u^2 & 1+u+u^2\end{bmatrix}, \begin{bmatrix}1 & u^2 & 0 & 1 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & u^2 & u^2 & 1 & u^2\end{bmatrix}, \begin{bmatrix}u^2 & 0 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1+u+u^2 & u^2 & u^2 & u\end{bmatrix}, \begin{bmatrix}1 & 0 & 1 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & u & 1+u & u & u\end{bmatrix}, \begin{bmatrix}1 & u & 0 & u & 1\end{bmatrix}, \begin{bmatrix}1 & 1+u & 0 & u & 0\end{bmatrix}, \begin{bmatrix}u & 0 & u^2 & u+u^2 & 0\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}u & u & u^2 & u^2 & u^2\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}u & 0 & u & 0 & 0\\ 0 & u^2 & u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & u^2 & u & 0\\ 0 & u & 0 & u^2 & u\end{bmatrix}, \begin{bmatrix}u & 0 & u & u^2 & u^2\\ 0 & u & u^2 & u+u^2 & u^2\end{bmatrix},$$

$$\begin{bmatrix}u & u & u^2 & 0 & 0\\ 0 & u^2 & u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u & 0\\ 0 & u & u & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u & u^2\\ 0 & u & 0 & 0 & u+u^2\end{bmatrix}, \begin{bmatrix}u & u & u^2 & u^2 & u^2\\ 0 & u^2 & u^2 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix}u & 0 & u^2 & u+u^2 & 0\\ 0 & u & u^2 & 0 & u\end{bmatrix}, \begin{bmatrix}u & u & 0 & 0 & u^2\\ 0 & u^2 & 0 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & 0 & u & 0\\ 0 & u^2 & u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}u & 0 & u & 0 & 0\\ 0 & u^2 & 0 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u & 0 & u+u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u^2 & 0 & 1 \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & u^2 & u^2 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & u^2 & 1 \\ 0 & 1 & 1 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u^2 & u^2 & 1 \\ 0 & u^2 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 1+u & u+u^2 \\ 0 & u^2 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 & 0 \\ 0 & u^2 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & u^2 & 0 & 0 \\ 0 & u^2 & u^2 & 0 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & u+u^2 & 1+u & 0 \\ 0 & 1 & 1+u^2 & u & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 1+u & u^2 \\ 0 & 1 & u & 0 & 1+u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u & u+u^2 & 0 \\ 0 & 1 & u+u^2 & 1+u & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u+u^2 & 0 & u^2 \\ 0 & u & u^2 & 0 & u \end{bmatrix}, \begin{bmatrix} u & 0 & u^2 & u+u^2 & u^2 \\ 0 & u & u+u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u & u^2 & u^2 & u+u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u^2 & u+u^2 \\ 0 & u^2 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & 0 & u+u^2 & u \\ 0 & u^2 & 0 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u+u^2 & 0 & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & u & u & u+u^2 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u+u^2 \\ 0 & u^2 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u+u^2 & u^2 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u^2 & u^2 & u+u^2 \\ 0 & u^2 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u^2 & u^2 & u+u^2 \\ 0 & u & u & 0 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u+u^2 & u^2 \\ 0 & u^2 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & u & u^2 & u & u+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u^2 & 1 \\ 0 & 1 & u & 1+u & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u & u & 0 \\ 0 & 1 & u & 1+u & u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1+u^2 & u^2 & u^2 \\ 0 & 1 & u^2 & 1 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u^2 & u & u \\ 0 & 1 & u+u^2 & 1 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u & u & u^2 \\ 0 & 1 & u^2 & u^2 & 1+u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & u^2 & 0 & 1 \\ 0 & 1 & 1+u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & u^2 \\ 0 & 1 & 1+u & 0 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1+u & u^2 & u \\ 0 & 1 & u & u^2 & 1+u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1+u & 0 & u \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & u^2 & 0 \\ 0 & 1 & u^2 & 1+u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1+u^2 & u^2 & 1+u^2 \\ 0 & u & u^2 & 0 & u+u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1+u^2 & 1 & u^2 \\ 0 & u & 0 & u & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u+u^2 & u^2 & 1+u \\ 0 & u & u^2 & u+u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u^2 & 1+u^2 & u^2 \\ 0 & u & u & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & u^2 & 1+u^2\\ 0 & u & u^2 & u & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & u+u^2 & 1\\ 0 & u & u+u^2 & 0 & u^2\end{bmatrix}, \begin{bmatrix}1 & 0 & u & 0 & 1+u+u^2\\ 0 & u & u & u^2 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u^2 & 1 & u^2\\ 0 & u & u^2 & 0 & u+u^2\end{bmatrix}, \begin{bmatrix}1 & 0 & 1+u^2 & 0 & 0\\ 0 & u & 0 & u+u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & 1+u & 1+u+u^2 & 0\\ 0 & u & u & u^2 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & 1 & 1 & 1 & 0\\ 0 & u & u^2 & u+u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & 1+u & 0\\ 0 & u & u+u^2 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 1+u+u^2 & u^2 & u+u^2\\ 0 & u & u^2 & 0 & u\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u+u^2 & 1+u & 0\\ 0 & u & u^2 & 0 & u\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & u^2 & 1\\ 0 & u & u & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1+u+u^2 & u+u^2\\ 0 & u & u+u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & u^2 & 1\\ 0 & u & u+u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 1+u^2 & u+u^2 & u\\ 0 & u & u^2 & u^2 & u\end{bmatrix}, \begin{bmatrix}1 & 1 & u+u^2 & 1+u+u^2 & 1\\ 0 & u & 0 & 0 & u\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & 0 & 1+u^2\\ 0 & 1 & 1 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u^2 & 1+u^2 & 0\\ 0 & u & u+u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & 1+u & 1+u+u^2 & 0\\ 0 & u & u+u^2 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & 0 & 0 & 1\\ 0 & u & u+u^2 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 1+u+u^2 & u^2 & u\\ 0 & u & 0 & u & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & u+u^2 & 1 & 1+u+u^2\\ 0 & u & u^2 & u^2 & u\end{bmatrix},$$

$$\begin{bmatrix}u^2 & 0 & 0 & u^2 & 0\\ 0 & u^2 & u^2 & u^2 & u^2\end{bmatrix}, \begin{bmatrix}1 & u & 0 & 1+u & u^2\\ 0 & u^2 & 0 & 0 & u^2\end{bmatrix}, \begin{bmatrix}1 & 1 & 1+u+u^2 & 0 & 1+u+u^2\\ 0 & u & u+u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}u^2 & 0 & 0 & 0 & u^2\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & u & 1+u+u^2 & u & u\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 0 & 1+u+u^2 & u+u^2\\ 0 & u^2 & u^2 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & u & u & 0 & 1\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & 1+u+u^2 & u+u^2 & 1\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & 1+u+u^2 & 0\\ 0 & u^2 & 0 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u & u & 1\\ 0 & u^2 & u^2 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u+u^2 & u+u^2 & 1\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & u^2 & 1+u+u^2 & u+u^2\\ 0 & u^2 & u^2 & 0 & u^2\end{bmatrix},$$

$$\begin{bmatrix}1 & u & 1 & u & u^2\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 1+u & 1+u+u^2 & 1 & 0\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 1 & 1+u & 1+u+u^2 & u^2\\ 0 & u^2 & u^2 & 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}1 & 0 & u & u^2 & 1+u+u^2\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & 0 & 1+u^2 & 0 & u^2\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix}, \begin{bmatrix}1 & u & 1+u & 0 & u^2\\ 0 & u^2 & 0 & u^2 & 0\end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & u^2 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u+u^2 & u+u^2 & 1+u^2 \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & u^2 & 1+u & 1 \\ 0 & u & u^2 & u+u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u+u^2 & u^2 & 1 & u \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1+u^2 & 1+u^2 & u^2 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u^2 & 1 & u^2 \\ 0 & u & u+u^2 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & u & 0 & u^2 & 1+u \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 1+u & u \\ 0 & u & u+u^2 & 0 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1+u^2 & 1+u & u & 1+u^2 \\ 0 & u & 0 & u^2 & u \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1+u^2 & 0 \\ 0 & u & u+u^2 & u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1+u^2 & 1+u^2 & u+u^2 & 1+u \\ 0 & u & 0 & u^2 & u+u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & u^2 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u^2 & 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & u^2 & 1+u+u^2 & 1+u^2 \\ 0 & u & 0 & u+u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u+u^2 & 0 \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u & 0 & u^2 & u+u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & 1+u & 0 & 1+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u & 0 & u^2 & u+u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u & 0 & u+u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1+u & 0 & 1+u & 1 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & u+u^2 & 1+u \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & u^2 & 1+u+u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & u & u^2 & 0 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & u & 0 & u+u^2 & 1+u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & u & 1+u \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & u & 1+u+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1+u^2 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & u^2 & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u^2 & u \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1+u & u^2 & 1+u+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & u^2 \\ 0 & u & 0 & u^2 & u+u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u+u^2 \\ 0 & u & u & 0 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u+u^2 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & u^2 \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & u^2 \\ 0 & u & 0 & 0 & u \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & 0 & u+u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u+u^2 & 0 \\ 0 & u^2 & 0 & u^2 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u & u \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u+u^2 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & 0 & u \\ 0 & u & 0 & u & u^2 \\ 0 & 0 & u^2 & 0 & 0 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u & 0 & 0 & u+u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & u & 0 & u+u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & u & 0 & u^2 & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix}, \begin{bmatrix} u & u & u & u+u^2 & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & 0 \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & u & u^2 & u^2 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & u & u^2 & 0 \\ 0 & u^2 & 0 & u^2 & 0 \\ 0 & 0 & u^2 & u^2 & u^2 \end{bmatrix}, \begin{bmatrix} u & 0 & 0 & u^2 & u \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \end{bmatrix},$$

$$\begin{bmatrix} u^2 & 0 & 0 & 0 & u^2 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix} \text{ and } \begin{bmatrix} u & 0 & u & 0 & 0 \\ 0 & u^2 & 0 & 0 & u^2 \\ 0 & 0 & u^2 & 0 & u^2 \\ 0 & 0 & 0 & u^2 & u^2 \end{bmatrix};$$

- 5 self-orthogonal codes of Hamming distance 3, whose generator matrices are $\begin{bmatrix} u^2 & 0 & 0 & u^2 & u^2 \end{bmatrix}$, $\begin{bmatrix} u^2 & 0 & 0 & u^2 & u^2 \\ 0 & u^2 & u^2 & u^2 & u^2 \end{bmatrix}$, $\begin{bmatrix} u & 0 & u & u+u^2 & u \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1 & u^2 & 1+u+u^2 & 1+u+u^2 \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & u & 1+u & 1+u+u^2 & 1+u \\ 0 & u^2 & u^2 & u^2 & 0 \end{bmatrix}$;
- 6 self-orthogonal codes of Hamming distance 4, whose generator matrices are $\begin{bmatrix} 1 & 1 & 1 & 1 & u^2 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 1+u & 1+u^2 & 1+u \end{bmatrix}$, $\begin{bmatrix} u^2 & u^2 & u^2 & 0 & u^2 \end{bmatrix}$, $\begin{bmatrix} u & u & u & u^2 & u \end{bmatrix}$, $\begin{bmatrix} 1 & 1+u & 1 & u & 1 \end{bmatrix}$ and $\begin{bmatrix} u & 0 & u+u^2 & u & u \end{bmatrix}$; and
- 1 self-orthogonal code of Hamming distance 5, whose generator matrix is $\begin{bmatrix} u^2 & u^2 & u^2 & u^2 & u^2 \end{bmatrix}$.

V. By Theorem 2.2.4(b), we see that a self-orthogonal code of the type $\{k_1, k_2, k_3\}$ and length n over $\mathbb{F}_q[u]/\langle u^3\rangle$ is self-dual if and only if n is even, $k_2 = k_3$ and $2(k_1+k_2) = n$. From this and by parts **I-IV**, we deduce the following:

- There is only one inequivalent self-dual code of length 2 and Hamming distance 1, and one inequivalent self-dual code of length 2 and Hamming distance 2 over $\mathbb{F}_3[u]/\langle u^3\rangle$.
- There are precisely 3 inequivalent self-dual codes of length 4 and Hamming distance 1, and 4 inequivalent self-dual codes of length 4 and Hamming distance 2 over $\mathbb{F}_3[u]/\langle u^3\rangle$.

Now to classify self-orthogonal and self-dual codes of lengths $2, 3$ and 4 over $\mathbb{F}_4[u]/\langle u^2\rangle$, we assume, from this point on, that ζ is a primitive element of $\mathbb{F}_4$.

VI. There are precisely 4 inequivalent non-zero self-orthogonal codes of length 2 over $\mathbb{F}_4[u]/\langle u^2\rangle$. Among these codes, there are

- 2 self-orthogonal codes of Hamming distance 1, whose generator matrices are $\begin{bmatrix} u & 0 \end{bmatrix}$ and $\begin{bmatrix} u & 0 \\ 0 & u \end{bmatrix}$; and
- 2 self-orthogonal codes of Hamming distance 2, whose generator matrices are $\begin{bmatrix} u & u \end{bmatrix}$ and $\begin{bmatrix} 1 & 1+u \end{bmatrix}$.

VII. There are precisely 12 inequivalent non-zero self-orthogonal codes of length 3 over $\mathbb{F}_4[u]/\langle u^2 \rangle$. Among these codes, there are

- 5 self-orthogonal codes of Hamming distance 1, whose generator matrices are $\begin{bmatrix} u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & \zeta u \\ 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & \zeta^2 u & 1+\zeta u \\ 0 & u & 0 \end{bmatrix}$ and $\begin{bmatrix} u & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & u \end{bmatrix}$;
- 5 self-orthogonal codes of Hamming distance 2, whose generator matrices are $\begin{bmatrix} u & \zeta^2 u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & u & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 1 \end{bmatrix}$, $\begin{bmatrix} u & 0 & u \\ 0 & u & u \end{bmatrix}$ and $\begin{bmatrix} 1 & \zeta^2 & \zeta+\zeta^2 u \\ 0 & u & \zeta u \end{bmatrix}$; and
- 2 self-orthogonal codes of Hamming distance 3, whose generator matrices are $\begin{bmatrix} u & u & u \end{bmatrix}$ and $\begin{bmatrix} 1 & \zeta & \zeta^2 \end{bmatrix}$.

VIII. There are precisely 42 inequivalent non-zero self-orthogonal codes of length 4 over $\mathbb{F}_4[u]/\langle u^2 \rangle$. Among these codes, there are

- 14 self-orthogonal codes of Hamming distance 1, whose generator matrices are $\begin{bmatrix} u & 0 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & u & u \\ 0 & u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & \zeta^2 u \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & \zeta u & 1 & \zeta u \\ 0 & u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & \zeta u & \zeta^2 & \zeta+\zeta u \\ 0 & u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 1+\zeta^2 u & 0 \\ 0 & u & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & u \\ 0 & 0 & u & u \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & \zeta^2 u \\ 0 & 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & 0 \\ 0 & 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & u & 0 & 1 \\ 0 & u & 0 & 0 \\ 0 & 0 & u & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 1+\zeta u & 1 & 1+\zeta u \\ 0 & u & 0 & u \\ 0 & 0 & u & u \end{bmatrix}$, $\begin{bmatrix} 1 & \zeta^2 u & \zeta^2+\zeta u & \zeta \\ 0 & u & 0 & 0 \\ 0 & 0 & u & \zeta u \end{bmatrix}$

and $\begin{bmatrix} u & 0 & 0 & 0 \\ 0 & u & 0 & 0 \\ 0 & 0 & u & 0 \\ 0 & 0 & 0 & u \end{bmatrix}$;

- 19 self-orthogonal codes of Hamming distance 2, whose generator matrices are

$$\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} u & u & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & u & u & 1 \end{bmatrix}, \begin{bmatrix} 1 & u & 1 & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 \\ 0 & u & \zeta u & u \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & \zeta^2 u \\ 0 & u & 0 & \zeta u \end{bmatrix}, \begin{bmatrix} u & 0 & u & 0 \\ 0 & u & 0 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & \zeta u \\ 0 & u & 0 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & \zeta u & 1 \\ 0 & 1 & 1 & \zeta u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & \zeta^2 u & 1 \\ 0 & 1 & 1+u & \zeta^2 u \end{bmatrix}, \begin{bmatrix} 1 & \zeta+\zeta^2 u & \zeta & 1 \\ 0 & u & u & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & u & 1+\zeta u \\ 0 & 1 & 1 & u \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2 u & 1 & \zeta u \\ 0 & u & 0 & \zeta^2 u \end{bmatrix},$$

$$\begin{bmatrix} 1 & \zeta+\zeta u & \zeta^2 & \zeta^2 u \\ 0 & u & \zeta^2 u & 0 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2+u & 1+u & \zeta^2+u \\ 0 & u & \zeta^2 u & 0 \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2+\zeta^2 u & 0 & \zeta+\zeta^2 u \\ 0 & u & 0 & \zeta u \end{bmatrix},$$

$$\begin{bmatrix} u & 0 & 0 & u \\ 0 & u & 0 & \zeta u \\ 0 & 0 & u & \zeta^2 u \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1+\zeta^2 u & \zeta^2 & \zeta^2+u \\ 0 & u & 0 & \zeta u \\ 0 & 0 & u & u \end{bmatrix};$$

- 7 self-orthogonal codes of Hamming distance 3, whose generator matrices are

$$\begin{bmatrix} 1 & 0 & \zeta^2 & \zeta \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2 u & \zeta+\zeta^2 u & \zeta^2 \end{bmatrix}, \begin{bmatrix} u & u & u & 0 \end{bmatrix}, \begin{bmatrix} u & 0 & \zeta^2 u & u \\ 0 & u & \zeta^2 u & \zeta^2 u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1+u & 1+\zeta u & 1+u \\ 0 & u & \zeta^2 u & \zeta u \end{bmatrix}, \begin{bmatrix} 1 & \zeta^2+\zeta u & u & \zeta+\zeta u \\ 0 & u & \zeta u & \zeta u \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & \zeta+u & \zeta^2+u \\ 0 & 1 & \zeta^2+u & \zeta+u \end{bmatrix};$$

and

- 2 self-orthogonal codes of Hamming distance 4, whose generator matrices are

$$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} u & u & u & u \end{bmatrix}.$$

IX. By applying Lemma 2.2.4(b), we observe that a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathbb{F}_q[u]/\langle u^2 \rangle$ is self-dual if and only if $2k_1 + k_2 = n$. From this and by parts **VI-VIII**, we deduce the following:

- There is only one inequivalent self-dual code of length 2 and Hamming distance 1, and one inequivalent self-dual code of length 2 and Hamming distance 2 over $\mathbb{F}_4[u]/\langle u^2\rangle$.
- There are precisely 2 inequivalent self-dual codes of length 3 and Hamming distance 1, and one inequivalent self-dual code of length 3 and Hamming distance 2 over $\mathbb{F}_4[u]/\langle u^2\rangle$.
- There are precisely 4 inequivalent self-dual codes of length 4 and Hamming distance 1, 5 inequivalent self-dual codes of length 4 and Hamming distance 2, and 1 inequivalent self-dual code of length 4 and Hamming distance 3 over $\mathbb{F}_4[u]/\langle u^2\rangle$.

Note that Theorems 4.4.3 and 4.4.4 together with Theorems 3.2.3,3.2.5, 3.3.3, 3.3.5, 3.4.5 and 3.4.6 provide enumeration formulae for all self-orthogonal and self-dual codes over quasi-Galois rings. Thus the problem of determination of enumeration formulae for self-orthogonal and self-dual codes over quasi-Galois rings is now completely solved. Apart from this, as a consequence of Theorems 3.2.3,3.2.5, 3.3.3, 3.3.5, 3.4.5 and 3.4.6, the enumeration formulae for self-orthogonal and self-dual codes over Galois rings of odd characteristic are also known. In the next chapter, we will count all self-orthogonal and self-dual codes of an arbitrary length over Galois rings of even characteristic.

5

Enumeration formulae for self-orthogonal and self-dual codes over Galois rings of even characteristic

5.1 Introduction

In this chapter, we will count all self-orthogonal and self-dual codes of an arbitrary length over Galois rings of even characteristic. For this, we assume, throughout this chapter, that $e \geq 2$ and r are fixed positive integers. Here we recall, from Chapter 2, that $GR(p^e, r)$ denotes the Galois ring of characteristic p^e and cardinality p^{er}, where p is a prime number. We also recall that the Galois ring $GR(p^e, r)$

is a finite commutative chain ring with the maximal ideal $\langle p \rangle$ of nilpotency index e and the residue field $\overline{GR(p^e,r)} = GR(p^e,r)/\langle p \rangle$ of order p^r. Further, there exists an element $\xi \in GR(p^e,r)$ whose multiplicative order is p^r-1 and the set $\mathcal{T}_{e,r} = \{0,1,\xi,\xi^2,\ldots,\xi^{p^r-2}\}$ is the Teichm*ü*ller set of the Galois ring $GR(p^e,r)$.

Next, for an integer μ satisfying $1 \leq \mu < e$, we observe that the quotient ring $GR(p^e,r)/\langle p^\mu \rangle$ is the Galois ring $GR(p^\mu,r)$ of characteristic p^μ and cardinality $p^{r\mu}$ and has a unique maximal ideal $\langle p + \langle p^\mu \rangle \rangle$. We further observe that the element $\xi_\mu := \xi + \langle p^\mu \rangle \in GR(p^\mu,r)$ has multiplicative order p^r-1 and that the set $\mathcal{T}_{\mu,r} = \{0,1,\xi_\mu,\xi_\mu^2,\ldots,\xi_\mu^{p^r-2}\}$ is the Teichm*ü*ller set of $GR(p^\mu,r)$. One can define a canonical epimorphism from $GR(p^e,r)$ onto $GR(p^\mu,r)$ as $a \mapsto a + \langle p^\mu \rangle$ for all $a \in GR(p^e,r)$. In view of this, we shall identify each element $a + \langle p^\mu \rangle \in GR(p^\mu,r)$ with the element $a \in GR(p^e,r)$, and we shall perform addition and multiplication in $GR(p^\mu,r)$ modulo p^μ. In particular, we shall identify the element $\xi_\mu \in \mathcal{T}_{\mu,r}$ with the element $\xi \in \mathcal{T}_{e,r}$. So we assume, throughout this chapter, that

$$\mathcal{T}_{1,r} = \mathcal{T}_{2,r} = \cdots = \mathcal{T}_{e-1,r} = \mathcal{T}_{e,r} = \{0,1,\xi,\xi^2,\ldots,\xi^{p^r-2}\} = \mathcal{T}_r \text{ (say)}.$$

Further, for $1 \leq \mu \leq e$, we see, by Theorem 14.8 of [101], that each element $a \in GR(p^\mu,r)$ can be uniquely expressed as $a = a_0 + a_1p + a_2p^2 + \cdots + a_{\mu-1}p^{\mu-1}$, where $a_0,a_1,a_2,\ldots,a_{\mu-1} \in \mathcal{T}_r$. Define a map $\gamma_0 : GR(p^\mu,r) \to \mathcal{T}_r$ as $\gamma_0(a) = a_0$ for all $a = a_0 + a_1p + a_2p^2 + \cdots + a_{\mu-1}p^{\mu-1} \in GR(p^\mu,r)$ with $a_0,a_1,a_2,\ldots,a_{\mu-1} \in \mathcal{T}_r$. Furthermore, for $a,b \in \mathcal{T}_r$, let us define $a \oplus b \in \mathcal{T}_r$ as $a \oplus b = \gamma_0(a+b)$. Note that $\oplus$ is a binary operation on $\mathcal{T}_r$. One can easily observe that the Teichm*ü*ller set $\mathcal{T}_r$ of the Galois ring $GR(p^e,r)$ can be viewed as the finite field of order p^r under the addition operation $\oplus$ and the usual multiplication operation of $GR(p^e,r)$. In view of this, we assume, without any loss of generality, that

$$GR(p,r) = \overline{GR(p,r)} = \overline{GR(p^2,r)} = \cdots = \overline{GR(p^e,r)} = \mathcal{T}_r$$

from this point on. Throughout this chapter, we shall denote the Galois ring $GR(2^\mu,r)$ by $\mathscr{R}_{\mu,r}$ for $1 \leq \mu \leq e$. The main goal of this chapter is to count all self-orthogonal and self-dual codes of an arbitrary length over $\mathscr{R}_{e,r} = GR(2^e,r)$.

When $p=2$, a linear code $\mathscr{C}$ of length n over $\mathcal{T}_r$ is said to be k-doubly even if it has a k-dimensional linear subcode $\mathscr{C}_0$ satisfying $c \cdot c \equiv 0 \pmod 4$ for all $c \in \mathscr{C}_0$, where each $c \in \mathscr{C}_0$ is viewed as an element of $\mathscr{R}_{e,r}^n$ and $\cdot$ denotes the Euclidean bilinear form on $\mathscr{R}_{e,r}^n$. A k-doubly even code of length n and dimension k over $\mathcal{T}_r$ is simply called a doubly even code. In this chapter, we will consider the case $p = 2$, and we will first count all doubly even codes over $\mathcal{T}_r$ and their two special classes, *viz.* the codes containing the all-one vector and the codes that do not contain the all-one vector by studying the geometry of a certain special quadratic space over $\mathcal{T}_r$. We will further provide a recursive method to construct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ from a $(k_1+k_2+\cdots+k_{\lfloor \frac{e}{2} \rfloor})$-doubly even self-orthogonal code of the same length n and dimension $k_1+k_2+\cdots+k_{\lceil \frac{e}{2} \rceil}$ over $\mathcal{T}_r$, where n is a positive integer and $k_1, k_2, \ldots, k_e$ are non-negative integers satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. With the help of this recursive construction method and the enumeration formulae for doubly even codes over $\mathcal{T}_r$ and their two special classes, we will obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathscr{R}_{e,r}$.

This chapter is organized as follows: In Section 5.2, we first outline the recursive construction method employed in Chapter 3 (see the proofs of Theorems 3.4.1 and 3.4.3) in the particular case of codes over the Galois ring $GR(p^\ell, r)$, where $\ell \geq 4$ is an integer. Here we note that when $p = 2$, each self-orthogonal (*resp.* self-dual) code over $\mathscr{R}_{\ell-2,r}$ can not be lifted to a self-orthogonal (*resp.* self-dual) code over $\mathscr{R}_{\ell,r}$ by applying this construction method. We further derive a necessary and sufficient condition under which a self-orthogonal code over $\mathscr{R}_{\ell-2,r}$ can be lifted to a self-orthogonal code over $\mathscr{R}_{\ell,r}$ using this construction method (Theorem 5.2.1). In Section 5.3, we consider the case $p = 2$ and count all doubly even codes over $\mathcal{T}_r$ and their two special classes consisting of the codes containing the all-one vector and the codes that do not contain the all-one vector (Theorems 5.3.1-5.3.3). In Section 5.4, we extend the recursive construction method provided by Nagata *et al.* [75] to construct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ from a $(k_1+k_2+\cdots+k_{\lfloor \frac{e}{2} \rfloor})$-doubly even self-orthogonal code of the same length n and dimension $k_1 + k_2 + \cdots + k_{\lceil \frac{e}{2} \rceil}$ over $\mathcal{T}_r$, where $k_1, k_2, \ldots, k_e$ are non-negative integers satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. In Section 5.5, we obtain explicit enumeration formulae for all self-orthogonal and self-dual codes of an arbitrary length over $\mathscr{R}_{e,r}$ by applying the recursive construction method provided in Section 5.4 and the results derived in Section 5.3. In Section 5.6, we classify all self-orthogonal and self-dual codes of lengths $2, 3$ and 4 over $\mathscr{R}_{2,2} = GR(4, 2)$.

In the following section, we assume that $\ell \geq 4$ is an integer, and we outline the recursive construction method employed in Chapter 3 in the particular case of codes over the Galois ring $GR(p^\ell, r)$. Here when $p = 2$ (*i.e.*, when $GR(p^\ell, r) = GR(2^\ell, r) = \mathscr{R}_{\ell,r}$), we illustrate that not every self-orthogonal code over $\mathscr{R}_{\ell-2,r}$ can be lifted to a self-orthogonal code over $\mathscr{R}_{\ell,r}$ using this method. We also characterize all self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell,r}$.

5.2 Outline of the recursive construction method

Throughout this section, let $\ell \geq 4$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{\ell+1}$ be non-negative integers satisfying $n = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_\ell + \mathtt{k}_{\ell+1}$ and $2\mathtt{k}_1 + 2\mathtt{k}_2 + \cdots + 2\mathtt{k}_{\ell-i+1} + \mathtt{k}_{\ell-i+2} + \mathtt{k}_{\ell-i+3} + \cdots + \mathtt{k}_i \leq n$ for $\lceil \frac{\ell+1}{2} \rceil \leq i \leq \ell$.

Now let $\mathcal{D}_{\ell-2}$ be a self-orthogonal (*resp.* self-dual) code of the type $\{\mathtt{k}_1 + \mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $GR(p^{\ell-2}, r)$ with a generator matrix

$$\mathcal{G}_{\ell-2} = \begin{bmatrix} Z_1' \\ Z_2' \\ pZ_3' \\ \vdots \\ p^{\ell-4}Z_{\ell-2}' \\ p^{\ell-3}Z_{\ell-1}' \end{bmatrix} \tag{5.2.1}$$

with

$$\begin{bmatrix} Z_1' \\ Z_2' \end{bmatrix} = \begin{bmatrix} I_{\mathtt{k}_1} & A_{1,1} & A_{1,2} & \cdots & A_{1,\ell-2} & A_{1,\ell} \\ 0 & I_{\mathtt{k}_2} & A_{2,2} & \cdots & A_{2,\ell-2} & A_{2,\ell} \end{bmatrix} + \sum_{j=1}^{\ell-3} p^j \begin{bmatrix} V_1^{(j)} \\ V_2^{(j)} \end{bmatrix},$$

where the matrix $I_{\mathtt{k}_i}$ is the $\mathtt{k}_i \times \mathtt{k}_i$ identity matrix over $\mathcal{T}_r$, $A_{i,j} \in \mathcal{M}_{\mathtt{k}_i \times \mathtt{k}_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq 2$ and $i \leq j \leq \ell - 2$, $A_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $A_{2,\ell} \in \mathcal{M}_{\mathtt{k}_2 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $V_b^{(y)} \in \mathcal{M}_{\mathtt{k}_b \times n}(\mathcal{T}_r)$ for $1 \leq b \leq 2$ and $1 \leq y \leq \ell - 3$, and the matrix $Z_\mu' \in$

$\mathcal{M}_{\mathtt{k}_\mu \times n}(GR(p^{\ell-2},r))$ is to be considered modulo $p^{\ell-\mu}$ for $3 \leq \mu \leq \ell-1$, (*i.e.*, the matrix $Z'_\mu \in \mathcal{M}_{\mathtt{k}_\mu \times n}(GR(p^{\ell-2},r))$ is of the form $Z'_\mu = Z'_{\mu,0} + pZ'_{\mu,1} + p^2 Z'_{\mu,2} + \cdots + p^{\ell-\mu-1}Z'_{\mu,\ell-\mu-1}$, where $Z'_{\mu,0}, Z'_{\mu,1}, \ldots, Z'_{\mu,\ell-\mu-1} \in \mathcal{M}_{\mathtt{k}_\mu \times n}(\mathcal{T}_r)$ for $3 \leq \mu \leq \ell-1$).

Further, let $\mathcal{D}_\ell$ be a linear code of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{\ell-1}, \mathtt{k}_\ell\}$ and length n over $GR(p^\ell, r)$ with a generator matrix

$$\mathcal{G}_\ell = \begin{bmatrix} Z_1 \\ pZ_2 \\ p^2 Z_3 \\ \vdots \\ p^{\ell-2}Z_{\ell-1} \\ p^{\ell-1}Z_\ell \end{bmatrix}, \qquad (5.2.2)$$

where

$$Z_1 = Z'_1 + p^{\ell-2}\begin{bmatrix} 0 & \cdots & 0 & 0 & V_{1,\ell} \end{bmatrix} + p^{\ell-1}\begin{bmatrix} 0 & \cdots & 0 & 0 & U_{1,\ell} \end{bmatrix}$$

with $V_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $U_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, the matrix Z_μ is of the form

$$Z_\mu = Z'_\mu + p^{\ell-\mu}\begin{bmatrix} 0 & 0 & \cdots & 0 & A_{\mu,\ell} \end{bmatrix} \text{ with } A_{\mu,\ell} \in \mathcal{M}_{\mathtt{k}_\mu \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$$

for $2 \leq \mu \leq \ell-1$, and the matrix Z_ℓ is of the form

$$Z_\ell = \begin{bmatrix} 0 & 0 & \cdots & 0 & A_{\ell,\ell} \end{bmatrix} \text{ with } A_{\ell,\ell} \in \mathcal{M}_{\mathtt{k}_\ell \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r).$$

Since $\mathcal{D}_{\ell-2}$ is a self-orthogonal (*resp.* self-dual) code of the type $\{\mathtt{k}_1+\mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $GR(p^{\ell-2}, r)$ with a generator matrix $\mathcal{G}_{\ell-2}$ (as defined by (5.2.1)), we see, by Theorem 2.2.4, that

$$\begin{aligned} Z'_1 Z'^t_1 &\equiv p^{\ell-2}B_1 + p^{\ell-1}B_2 \pmod{p^\ell}, \\ Z'_1 Z'^t_2 &\equiv p^{\ell-2}J_2 \pmod{p^{\ell-1}}, \\ Z'_1 Z'^t_\mu &\equiv p^{\ell-\mu}J_\mu \pmod{p^{\ell-\mu+1}} \text{ for } 3 \leq \mu \leq \ell-1, \\ Z'_i Z'^t_j &\equiv 0 \pmod{p^{\ell-i-j+2}} \text{ for } 2 \leq i \leq j \leq \ell-1 \text{ and } i+j \leq \ell+1, \end{aligned}$$

where $B_1 \in Sym_{\mathtt{k}_1}(\mathcal{T}_r)$, $B_2 \in Sym_{k_1}(\mathcal{T}_r)$ and $J_\mu \in \mathcal{M}_{\mathtt{k}_1 \times \mathtt{k}_\mu}(\mathcal{T}_r)$ for $2 \leq \mu \leq \ell-1$.

Now by applying Theorem 2.2.4, we observe that the code $\mathcal{D}_{\ell-2}$ can be lifted to a self-orthogonal (*resp.* self-dual) code $\mathcal{D}_\ell$ of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_\ell\}$ and length n over $GR(p^\ell, r)$ with a generator matrix $\mathcal{G}_\ell$ (as defined by (5.2.2)) if and only if there exist matrices $V_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $U_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1 \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $A_{\mu,\ell} \in \mathcal{M}_{\mathtt{k}_\mu \times (\mathtt{k}_\ell + \mathtt{k}_{\ell+1})}(\mathcal{T}_r)$ for $2 \leq \mu \leq \ell$, satisfying the following system of matrix equations:

$$\left.\begin{array}{rcll} B_1 + A_{1,\ell}V_{1,\ell}^t + V_{1,\ell}A_{1,\ell}^t & & & \\ +p(B_2 + A_{1,\ell}U_{1,\ell}^t + U_{1,\ell}A_{1,\ell}^t) & \equiv & 0 & \pmod{p^2}, \\ A_{1,\ell}A_{2,\ell}^t + V_{1,\ell}B_{2,\ell}^t + J_2 & \equiv & 0 & \pmod{p}, \\ A_{1,\ell}A_{i,\ell}^t + J_i & \equiv & 0 & \pmod{p} \text{ for } 3 \leq i \leq \ell - 1, \\ A_{1,\ell}A_{\ell,\ell}^t & \equiv & 0 & \pmod{p}. \end{array}\right\} \quad (5.2.3)$$

Working in a similar manner as in Remark 3.4.1, we note that the matrix $A_{1,\ell}$ is a full-row rank matrix over $\mathcal{T}_r$. When p is an odd prime, by applying Lemma 2.1.1, one can show that there exist matrices $V_{1,\ell}$, $U_{1,\ell}$, $A_{i,\ell}$ for $2 \leq i \leq \ell$, such that the code $\mathcal{D}_\ell$ is a self-orthogonal (*resp.* self-dual) code over $GR(p^\ell, r)$ (see the proof of Theorem 3.4.1 for more details). However when $p = 2$, we recall that $GR(p^\ell, r) = \mathscr{R}_{\ell,r}$ and $GR(p^{\ell-2}, r) = \mathscr{R}_{\ell-2,r}$, and we observe that for each self-orthogonal code $\mathcal{D}_{\ell-2}$ of the type $\{\mathtt{k}_1 + \mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $\mathscr{R}_{\ell-2,r}$, the system (5.2.3) of matrix equations need not have a solution. The following example illustrates this.

Example 5.2.1. *Let $p = 2$, $r = 2$, $\ell = 4$, and let $\mathscr{R}_{4,2} = GR(2^4, 2) = \mathbb{Z}_{16}[\xi]$, where ξ is a root of the monic basic irreducible polynomial $x^2 + x + 1 \in \mathbb{Z}_{16}[x]$. Here we have $\mathscr{R}_{2,2} = GR(2^2, 2) = \mathbb{Z}_{16}[\xi]/\langle 2^2 \rangle \simeq \mathbb{Z}_4[\xi]$. Let $n = 4$, $\mathtt{k}_1 = 2$ and $\mathtt{k}_2 = \mathtt{k}_3 = \mathtt{k}_4 = 0$. Let $\mathscr{C}$ be a linear code of the type $\{2, 0\}$ and length 4 over $\mathscr{R}_{2,2}$ with a generator matrix*

$$\begin{bmatrix} 1 & 0 & \xi^2 & \xi \\ 0 & 1 & \xi & \xi^2 \end{bmatrix} + 2\begin{bmatrix} 0 & 0 & 0 & \xi^2 \\ 0 & 0 & 0 & \xi \end{bmatrix}.$$

Note that the code $\mathscr{C}$ is a self-orthogonal code over $\mathscr{R}_{2,2}$. Next, consider the linear code $\mathscr{D}$ of the type $\{2, 0, 0, 0\}$ and length 4 over $\mathscr{R}_{4,2}$ with a generator matrix

$$\begin{bmatrix} 1 & 0 & \xi^2 & \xi \\ 0 & 1 & \xi & \xi^2 \end{bmatrix} + 2\begin{bmatrix} 0 & 0 & 0 & \xi^2 \\ 0 & 0 & 0 & \xi \end{bmatrix} + 2^2\begin{bmatrix} 0 & 0 & a_0 & a_1 \\ 0 & 0 & a_2 & a_3 \end{bmatrix} + 2^3\begin{bmatrix} 0 & 0 & b_0 & b_1 \\ 0 & 0 & b_2 & b_3 \end{bmatrix},$$

where $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathcal{T}_2 = \{0, 1, \xi, \xi^2\}$. *Here we have*

$$A_{1,4} = \begin{bmatrix} \xi^2 & \xi \\ \xi & \xi^2 \end{bmatrix}, V_{1,4} = \begin{bmatrix} a_0 & a_1 \\ a_2 & a_3 \end{bmatrix}, U_{1,4} = \begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \end{bmatrix}, B_1 = \begin{bmatrix} \xi^2 & 1 \\ 1 & \xi \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} \xi^2 & 0 \\ 0 & \xi \end{bmatrix}$$

corresponding to the codes $\mathscr{C}$ *and* $\mathscr{D}$. *Further, it is easy to see that the resulting system* (5.2.3) *of matrix equations in unknown matrices* $V_{1,4}$ *and* $U_{1,4}$ *has no simultaneous solution. This shows that the self-orthogonal code* $\mathscr{C}$ *can not be lifted to a self-orthogonal code of the type* $\{2, 0, 0, 0\}$ *and length* 4 *over* $\mathscr{R}_{4,2}$ *using the construction method outlined above.*

Now in the following example, we illustrate that there are self-orthogonal codes of the type $\{\mathtt{k}_1 + \mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_\ell\}$ and length n over $\mathscr{R}_{\ell,r}$.

Example 5.2.2. *Let* $p = 2$, $r = 2$, $\ell = 4$, *and let* $\mathscr{R}_{4,2} = GR(2^4, 2) = \mathbb{Z}_{16}[\xi]$, *where* ξ *is a root of the monic basic irreducible polynomial* $x^2 + x + 1 \in \mathbb{Z}_{16}[x]$. *Here we have* $\mathscr{R}_{2,2} = GR(2^2, 2) = \mathbb{Z}_{16}[\xi]/\langle 2^2 \rangle \simeq \mathbb{Z}_4[\xi]$. *Let* $n = 4$, $\mathtt{k}_1 = 2$ *and* $\mathtt{k}_2 = \mathtt{k}_3 = \mathtt{k}_4 = 0$. *Let* $\mathscr{C}$ *be a linear code of the type* $\{2, 0\}$ *and length* 4 *over* $\mathscr{R}_{2,2}$ *with a generator matrix*

$$\begin{bmatrix} 1 & 0 & \xi^2 & \xi \\ 0 & 1 & \xi & \xi^2 \end{bmatrix} + 2 \begin{bmatrix} 0 & 0 & \xi^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Note that the code $\mathscr{C}$ *is a self-orthogonal code over* $\mathscr{R}_{2,2}$. *Next, consider the linear code* $\mathscr{D}$ *of the type* $\{2, 0, 0, 0\}$ *and length* 4 *over* $\mathscr{R}_{4,2}$ *with a generator matrix*

$$\begin{bmatrix} 1 & 0 & \xi^2 & \xi \\ 0 & 1 & \xi & \xi^2 \end{bmatrix} + 2 \begin{bmatrix} 0 & 0 & \xi^2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + 2^2 \begin{bmatrix} 0 & 0 & a_0 & a_1 \\ 0 & 0 & a_2 & a_3 \end{bmatrix} + 2^3 \begin{bmatrix} 0 & 0 & b_0 & b_1 \\ 0 & 0 & b_2 & b_3 \end{bmatrix},$$

where $a_0, a_1, a_2, a_3, b_0, b_1, b_2, b_3 \in \mathcal{T}_2 = \{0, 1, \xi, \xi^2\}$. *Here we have*

$$A_{1,4} = \begin{bmatrix} \xi^2 & \xi \\ \xi & \xi^2 \end{bmatrix}, V_{1,4} = \begin{bmatrix} a_0 & a_1 \\ a_2 & a_3 \end{bmatrix}, U_{1,4} = \begin{bmatrix} b_0 & b_1 \\ b_2 & b_3 \end{bmatrix}, B_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } B_2 = \begin{bmatrix} \xi & 0 \\ 0 & 0 \end{bmatrix}$$

corresponding to the codes $\mathscr{C}$ *and* $\mathscr{D}$. *By applying Theorem 2.2.4, we see that the resulting system* (5.2.3) *of matrix equations in unknown matrices* $V_{1,4}$ *and* $U_{1,4}$ *has a simultaneous solution. In particular, one of the solutions of the system* (5.2.3) *is* *given by*

$$V_{1,4} = \begin{bmatrix} 0 & 1 \\ 1 & \xi^2 \end{bmatrix} \text{ and } U_{1,4} = \begin{bmatrix} \xi^2 & \xi \\ \xi^2 & \xi \end{bmatrix}.$$

From this, it follows that the self-orthogonal code $\mathscr{C}$ can be lifted to a self-orthogonal code of the type $\{2,0,0,0\}$ and length 4 over $\mathscr{R}_{4,2}$ using the above construction method.

From the above discussion, we see that it is not always possible to lift a self-orthogonal (*resp.* self-dual) code of the type $\{\mathtt{k}_1+\mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $\mathscr{R}_{\ell-2,r}$ to a self-orthogonal (*resp.* self-dual) code of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_\ell\}$ and length n over $\mathscr{R}_{\ell,r}$ via the construction method outlined above.

From now on, we assume, throughout this chapter, that $p = 2$. In the next section, we will first characterize all self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell,r}$.

5.2.1 A characterization of self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell,r}$

To characterize all self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes over $\mathscr{R}_{\ell,r}$, we will first define a special class of linear codes over $\mathscr{R}_{\mu,r}$, which are called doubly even codes, where $1 \leq \mu < e$.

Definition 5.2.1. *Let $p = 2$, and let μ be an integer satisfying $1 \leq \mu < e$. A free linear code $\mathscr{C}$ of length n over $\mathscr{R}_{\mu,r}$ is said to be doubly even if it satisfies $z \cdot z \equiv 0 \pmod{2^{\mu+1}}$ for all $z \in \mathscr{C}$, where each $z \in \mathscr{C}$ is viewed as an element of $\mathscr{R}_{e,r}^n$. Further, a linear code $\mathscr{C}$ of length n over $\mathscr{R}_{\mu,r}$ is said to be k-doubly even if it has a free linear doubly even subcode of rank k.*

In particular, when $p = 2$ and $\mu = 1$, we recall that $\mathscr{R}_{1,r} = \mathcal{T}_r$ is the finite field of order 2^r. So in this particular case, we say that a linear code $\mathscr{C}$ of length n over $\mathcal{T}_r$ is doubly even if it satisfies $z \cdot z \equiv 0 \pmod 4$ for all $z \in \mathscr{C}$, where each $z \in \mathscr{C}$ is viewed as an element of $\mathscr{R}_{e,r}^n$. Further, a linear code $\mathscr{C}$ of length n over $\mathcal{T}_r$ is said to be k-doubly even if it has a k-dimensional doubly even subcode.

When $\mu = r = 1$ (*i.e.*, when $\mathscr{R}_{\mu,r} = \mathcal{T}_r \simeq \mathbb{F}_2$), the above definition of doubly even codes over $\mathcal{T}_r$ coincides with that of binary doubly even codes, which are studied and enumerated by Gaborit [45]. We refer the reader to Section 1.4 of [53] for more details on the properties of binary doubly even codes. Note that the enumeration formula for doubly even codes over $\mathcal{T}_r$ is known only when $r = 1$, *i.e.*, when $\mathcal{T}_r \simeq \mathbb{F}_2$ (see Theorem 7 of Gaborit [45]). However, when $r \geq 2$, the enumeration formula for doubly even codes over $\mathcal{T}_r$ is not known, which we will obtain in Section 5.3. In general, the enumeration of k-doubly even codes over the Galois ring $\mathscr{R}_{\mu,r}$ is an open problem when either $r = 1$ and $2 \leq \mu < e$ or $r \geq 2$ and $1 \leq \mu < e$.

Example 5.2.3. *Let $\mathscr{R}_{2,2} = GR(2^2, 2) = \mathbb{Z}_4[\xi]$, where ξ is a root of the monic basic irreducible polynomial $x^2 + x + 1 \in \mathbb{Z}_4[x]$. Here we see that $\mathscr{R}_{1,2} = \mathcal{T}_2 = \{0, 1, \xi, \xi^2\}$ is the finite field of order 4 under the addition operation $\oplus$ and the multiplication operation in $\mathscr{R}_{1,2}$. Let $\mathcal{C}$ be a linear code of length 6 and rank 2 over $\mathscr{R}_{1,2}$ with a generator matrix*

$$\begin{bmatrix} 1 & 0 & \xi & \xi^2 & 0 & 0 \\ 0 & 1 & 0 & 0 & \xi & \xi^2 \end{bmatrix}.$$

It is easy to see that $z \cdot z \equiv 0 \pmod 4$ for all $z \in \mathcal{C}$, (here $z \in \mathcal{C}$ is viewed as an element of $\mathscr{R}_{2,2}^6$). This implies that the code $\mathcal{C}$ is a doubly even code over $\mathscr{R}_{1,2}$.

In the following theorem, we consider the case $p = 2$ and characterize all self-orthogonal (*resp.* self-dual) codes of the type $\{\mathtt{k}_1 + \mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $\mathscr{R}_{\ell-2,r}$ that can be lifted to self-orthogonal (*resp.* self-dual) codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{\ell-1}, \mathtt{k}_\ell\}$ and length n over $\mathscr{R}_{\ell,r}$ with the help of the construction method outlined above.

Theorem 5.2.1. *Let $p = 2$, and let $\ell \geq 4$ be a fixed integer. Let $\mathcal{D}_{\ell-2}$ be a self-orthogonal (resp. self-dual) code of the type $\{\mathtt{k}_1 + \mathtt{k}_2, \mathtt{k}_3, \ldots, \mathtt{k}_{\ell-1}\}$ and length n over $\mathscr{R}_{\ell-2,r}$ with a generator matrix $\mathcal{G}_{\ell-2}$ (as defined by (5.2.1)). Then the code $\mathcal{D}_{\ell-2}$ can be lifted to a self-orthogonal (resp. self-dual) code $\mathcal{D}_\ell$ of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{\ell-1}, \mathtt{k}_\ell\}$ and length n over $\mathscr{R}_{\ell,r}$ with a generator matrix $\mathcal{G}_\ell$ (as defined by (5.2.2)) if and only if the free linear code $\mathcal{D}'_{\ell-2}$ generated by the rows of the matrix Z'_1 is a $\mathtt{k}_1$-doubly even code over $\mathscr{R}_{\ell-2,r}$, i.e, $v \cdot v \equiv 0 \pmod{2^{\ell-1}}$ for all $v \in \mathcal{D}'_{\ell-2}$.*

Proof. To prove the result, one can easily observe that the code $\mathcal{D}_\ell$ is a self-orthogonal code over $\mathscr{R}_{\ell,r}$ if and only if the system (5.2.3) of matrix equations in unknown matrices $V_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1\times(\mathtt{k}_\ell+\mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $U_{1,\ell} \in \mathcal{M}_{\mathtt{k}_1\times(\mathtt{k}_\ell+\mathtt{k}_{\ell+1})}(\mathcal{T}_r)$, $A_{\mu,\ell} \in \mathcal{M}_{\mathtt{k}_\mu\times(\mathtt{k}_\ell+\mathtt{k}_{\ell+1})}(\mathcal{T}_r)$ for $2 \leq \mu \leq \ell$ admits a solution. Working in a similar manner as in Remark 3.4.1, we see that the matrix $A_{1,\ell}$ is a full-row rank matrix over $\mathcal{T}_r$. Now by applying Lemma 2.1.1, the desired result follows immediately. □

In the following section, we will count all doubly even codes of given length and dimension over $\mathcal{T}_r$, and their two special subclasses, *viz.* the codes containing the all-one vector and the codes that do not contain the all-one vector.

5.3 Enumeration of doubly even codes over $\mathcal{T}_r$

To count all doubly even codes over $\mathcal{T}_r$, we first observe that the set $\mathcal{V}_r = \mathcal{T}_r^n$ of all n-tuples over $\mathcal{T}_r$ can be viewed as an n-dimensional vector space over $\mathcal{T}_r$ under the component-wise addition induced by $\oplus$ and the component-wise scalar multiplication induced by the usual multiplication operation in $\mathscr{R}_{e,r}$. Next, let us define a map $\mathcal{B}_r : \mathcal{V}_r \times \mathcal{V}_r \to \mathcal{T}_r$ as

$$\mathcal{B}_r(a,b) = \gamma_0(a\cdot b) \ \text{ for all } a,b \in \mathcal{V}_r,$$

where both $a, b \in \mathcal{V}_r$ are viewed as elements of $\mathscr{R}_{e,r}^n$ to compute $a \cdot b$. Note that the map $\mathcal{B}_r$ is a non-degenerate and symmetric bilinear form on $\mathcal{V}_r$. Now a linear code $\mathscr{C}$ of length n over $\mathcal{T}_r$ is defined as a $\mathcal{T}_r$-linear subspace of $\mathcal{V}_r$. The dual code of the linear code $\mathscr{C}$ is defined as

$$\mathscr{C}^{\perp_{\mathcal{B}_r}} = \{a \in \mathcal{V}_r : \mathcal{B}_r(c,a) = 0 \text{ for all } c \in \mathscr{C}\}.$$

Note that the dual code $\mathscr{C}^{\perp_{\mathcal{B}_r}}$ is also a linear code of length n over $\mathcal{T}_r$. Further, a linear code $\mathscr{C}$ of length n over $\mathcal{T}_r$ is said to be (i) self-orthogonal if it satisfies $\mathscr{C} \subseteq \mathscr{C}^{\perp_{\mathcal{B}_r}}$ and (ii) self-dual if it satisfies $\mathscr{C} = \mathscr{C}^{\perp_{\mathcal{B}_r}}$. It is easy to see that a doubly even code of length n over $\mathcal{T}_r$ is self-orthogonal. We next observe that

$$\mathcal{I}(\mathcal{V}_r) = \{v \in \mathcal{V}_r : \mathcal{B}_r(v,v) = \gamma_0(v\cdot v) = 0\}$$

is an $(n-1)$-dimensional $\mathcal{T}_r$-linear subspace of $\mathcal{V}_r$, where each $v \in \mathcal{I}(\mathcal{V}_r)$ is viewed as an element of $\mathscr{R}_{e,r}^n$ to compute $v \cdot v$. Note that

$$\mathcal{I}(\mathcal{V}_r)^{\perp_{\mathcal{B}_r}} = \langle \mathbf{1} \rangle,$$

where $\mathbf{1}$ denotes the all-one vector $(1, 1, \ldots, 1) \in \mathcal{V}_r$ from now on. We further define a map $\mathcal{Q}_r : \mathcal{I}(\mathcal{V}_r) \to \mathcal{T}_r$ as

$$\mathcal{Q}_r(v) = \gamma_0(\frac{1}{2} v \cdot v) \in \mathcal{T}_r \text{ for all } v \in \mathcal{I}(\mathcal{V}_r),$$

(recall that each $v \in \mathcal{I}(\mathcal{V}_r)$ satisfies $v \cdot v \equiv 0 \pmod 2$). One can easily observe that $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ is a quadratic space over $\mathcal{T}_r$ with the associated symmetric bilinear form $\mathcal{B}_r\restriction_{\mathcal{I}(\mathcal{V}_r)\times\mathcal{I}(\mathcal{V}_r)}$ on $\mathcal{I}(\mathcal{V}_r)$. Note that any self-orthogonal code of length n over $\mathcal{T}_r$ is contained in $\mathcal{I}(\mathcal{V}_r)$. Further, one can easily observe that a doubly even code of length n and dimension k over $\mathcal{T}_r$ is a k-dimensional totally singular subspace of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$, and vice versa.

Next, we observe that $(\mathcal{T} = \{0, 1\}, \oplus, \cdot)$ is the subfield of $(\mathcal{T}_r, \oplus, \cdot)$ of order 2 and that $\mathcal{V} = \mathcal{T}^n$ is an n-dimensional vector space over $\mathcal{T}$. Further, since the vector space $\mathcal{V}$ can be viewed as a subset of $\mathcal{V}_r$, the map $\mathcal{B} = \mathcal{B}_r\restriction_{\mathcal{V}\times\mathcal{V}}$ is a non-degenerate and symmetric bilinear form on $\mathcal{V}$. We next see that the set

$$\mathcal{I}(\mathcal{V}) = \{v \in \mathcal{V} : \mathcal{B}(v, v) = 0\}$$

is an $(n-1)$-dimensional $\mathcal{T}$-linear subspace of $\mathcal{V}$, $\mathcal{I}(\mathcal{V}) \subseteq \mathcal{I}(\mathcal{V}_r)$ and that $\mathcal{I}(\mathcal{V})^{\perp_{\mathcal{B}}} = \langle \mathbf{1} \rangle$. Furthermore, the mapping $\mathcal{Q} = \mathcal{Q}_r\restriction_{\mathcal{I}(\mathcal{V})}$ is a quadratic form on $\mathcal{I}(\mathcal{V})$ with the associated symmetric bilinear form $\mathcal{B}\restriction_{\mathcal{I}(\mathcal{V})\times\mathcal{I}(\mathcal{V})}$ on $\mathcal{I}(\mathcal{V})$. We next observe that $\mathbf{1} = (1, 1, \ldots, 1) \in \mathcal{I}(\mathcal{V})$ if and only if n is even. From this, it is easy to see that the quadratic space $(\mathcal{I}(\mathcal{V}), \mathcal{Q})$ is non-defective if and only if n is odd.

When n is even, we choose an $(n-2)$-dimensional $\mathcal{T}$-linear subspace $\mathcal{V}_0$ of $\mathcal{I}(\mathcal{V})$ such that $\mathbf{1} \notin \mathcal{V}_0$. Note that $\mathcal{I}(\mathcal{V}) = \mathcal{V}_0 \perp \langle \mathbf{1} \rangle$. It is easy to observe that $(\mathcal{V}_0, \mathcal{Q}\restriction_{\mathcal{V}_0})$ is non-defective.

Now by the discussion in Section 5 of Wood [102, pp. 452-458] and by Theorem

2.3.7(a), we see that the Witt index ν of the quadratic space $(\mathcal{I}(\mathcal{V}), \mathcal{Q})$ is given by

$$\nu = \begin{cases} \frac{n-1}{2} & \text{if } n \equiv 1, 7 \pmod 8; \\ \frac{n-3}{2} & \text{if } n \equiv 3, 5 \pmod 8; \\ \frac{n}{2} & \text{if } n \equiv 0 \pmod 8; \\ \frac{n-2}{2} & \text{if } n \equiv 2, 4, 6 \pmod 8 \end{cases} \tag{5.3.1}$$

and that the quadratic space $(\mathcal{I}(\mathcal{V}), \mathcal{Q})$ admits an orthogonal direct sum decomposition of the form

$$\mathcal{I}(\mathcal{V}) = \begin{cases} \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{n-1}{2}}, b_{\frac{n-1}{2}}\rangle & \text{if } n \equiv 1, 7 \pmod 8; \\ \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{n-3}{2}}, b_{\frac{n-3}{2}}\rangle \perp W & \text{if } n \equiv 3, 5 \pmod 8; \\ \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{n-2}{2}}, b_{\frac{n-2}{2}}\rangle \perp \langle \mathbf{1}\rangle & \text{if } n \equiv 0, 2, 6 \pmod 8; \\ \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{n-4}{2}}, b_{\frac{n-4}{2}}\rangle \perp W \perp \langle \mathbf{1}\rangle & \text{if } n \equiv 4 \pmod 8), \end{cases} \tag{5.3.2}$$

where (a_i, b_i)'s are hyperbolic pairs in $\mathcal{I}(\mathcal{V})$ and W is a 2-dimensional non-singular subspace of $\mathcal{I}(\mathcal{V})$.

Now in the following lemma, we study the geometry of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ and obtain its Witt index ν_r.

Lemma 5.3.1. *(a) The Witt index ν_r of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ is given by*

$$\nu_r = \begin{cases} \frac{n-1}{2} & \textit{if either } n \equiv 1, 7 \pmod 8 \textit{ or } n \equiv 3, 5 \pmod 8 \textit{ and } r \textit{ is even}; \\ \frac{n-3}{2} & \textit{if } n \equiv 3, 5 \pmod 8 \textit{ and } r \textit{ is odd}; \\ \frac{n}{2} & \textit{if either } n \equiv 0 \pmod 8 \textit{ or } n \equiv 4 \pmod 8 \textit{ and } r \textit{ is even}; \\ \frac{n-2}{2} & \textit{if either } n \equiv 2, 6 \pmod 8 \textit{ or } n \equiv 4 \pmod 8 \textit{ and } r \textit{ is odd.} \end{cases}$$

(b) The quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form:

$$\mathcal{I}(\mathcal{V}_r)=\begin{cases}\langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_{\frac{n-1}{2}},b_{\frac{n-1}{2}}\rangle & \textit{if either } n\equiv 1,7 \pmod 8 \textit{ or}\\ & n\equiv 3,5 \pmod 8 \textit{ and } r \textit{ is even;}\\ \langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_{\frac{n-3}{2}},b_{\frac{n-3}{2}}\rangle\perp W_r & \textit{if } n\equiv 3,5 \pmod 8 \textit{ and } r \textit{ is odd;}\\ \langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_{\frac{n-2}{2}},b_{\frac{n-2}{2}}\rangle\perp\langle \mathbf{1}\rangle & \textit{if either } n\equiv 0,2,6 \pmod 8 \textit{ or}\\ & n\equiv 4 \pmod 8 \textit{ and } r \textit{ is even;}\\ \langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_{\frac{n-4}{2}},b_{\frac{n-4}{2}}\rangle\perp W_r\perp\langle \mathbf{1}\rangle & \textit{if } n\equiv 4 \pmod 8 \textit{ and } r \textit{ is odd,}\end{cases}$$

where (a_i,b_i)*'s are hyperbolic pairs in* $\mathcal{I}(\mathcal{V}_r)$ *and* W_r *is a* 2*-dimensional non-singular subspace of* $\mathcal{I}(\mathcal{V}_r)$*.*

Proof. Recall that $\mathbf{1}\in\mathcal{I}(\mathcal{V}_r)$ if and only if n is even. Accordingly, we will distinguish the following two cases: (i) n is odd and (ii) n is even.

(i) Let n be odd. Here by (5.3.1), the Witt index ν of the quadratic space $(\mathcal{I}(\mathcal{V}),\mathcal{Q})$ is given by $\nu=\frac{n-1}{2}$ if $n\equiv 1,7 \pmod 8$, while the Witt index ν of $(\mathcal{I}(\mathcal{V}),\mathcal{Q})$ is given by $\nu=\frac{n-3}{2}$ if $n\equiv 3,5 \pmod 8$. Further, by (5.3.2), we see that the space $(\mathcal{I}(\mathcal{V}),\mathcal{Q})$ admits an orthogonal direct sum decomposition of the form:

$$\mathcal{I}(\mathcal{V})=\langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_\nu,b_\nu\rangle\perp W,$$

where $(a_1,b_1),(a_2,b_2),\ldots,(a_\nu,b_\nu)$ are hyperbolic pairs in $\mathcal{I}(\mathcal{V})$ and W is a non-singular subspace of $\mathcal{I}(\mathcal{V})$ having dimension $n-1-2\nu$. Note that $\dim_{\mathcal{T}}(W)=0$ if $n\equiv 1,7 \pmod 8$, while $\dim_{\mathcal{T}}(W)=2$ if $n\equiv 3,5 \pmod 8$. As $\mathcal{I}(\mathcal{V})\subseteq\mathcal{I}(\mathcal{V}_r)$, we see that $(a_1,b_1),(a_2,b_2),\ldots,(a_\nu,b_\nu)$ are also hyperbolic pairs in $\mathcal{I}(\mathcal{V}_r)$. This implies that $\nu\leq\nu_r\leq\frac{n-1}{2}$. So when $n\equiv 1,7 \pmod 8$, we see that $\nu_r=\nu=\frac{n-1}{2}$ and that the quadratic space $(\mathcal{I}(\mathcal{V}_r),\mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form:

$$\mathcal{I}(\mathcal{V}_r)=\langle a_1,b_1\rangle\perp\langle a_2,b_2\rangle\perp\cdots\perp\langle a_{\frac{n-1}{2}},b_{\frac{n-1}{2}}\rangle.$$

Further, let $n\equiv 3,5 \pmod 8$. Here we have $\dim_{\mathcal{T}}(W)=2$. By Proposition 12.7 of [49], we note that $W=\langle\upsilon_1,\upsilon_2\rangle$, where $\upsilon_1,\upsilon_2\in\mathcal{I}(\mathcal{V})$ satisfy $\mathcal{Q}(\upsilon_1)=\mathcal{Q}(\upsilon_2)=1$ and $\mathcal{B}(\upsilon_1,\upsilon_2)=1$. Let W_r be a $\mathcal{T}_r$-span of $\{\upsilon_1,\upsilon_2\}$, *i.e.*, W_r is a

$\mathcal{T}_r$-linear subspace of $\mathcal{I}(\mathcal{V}_r)$. By applying Theorem 2.3.10, we observe that the quadratic space $(W_r, \mathcal{Q}_r \restriction_{W_r})$ has a singular vector if and only if r is even.

In view of this, we see that when $n \equiv 3, 5 \pmod 8$ and r is odd, the space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form:

$$\mathcal{I}(\mathcal{V}_r) = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_\nu, b_\nu\rangle \perp W_r,$$

where $(a_1, b_1), (a_2, b_2), \ldots, (a_\nu, b_\nu)$ are hyperbolic pairs in $\mathcal{I}(\mathcal{V}_r)$ and W_r is a 2-dimensional non-singular subspace of $\mathcal{I}(\mathcal{V}_r)$. This implies that $\nu_r = \nu$ when $n \equiv 3, 5 \pmod 8$ and r is odd.

On the other hand, when $n \equiv 3, 5 \pmod 8$ and r is even, by applying Proposition 2.3.1, we see that $W_r = \langle w_1, w_2\rangle$, where (w_1, w_2) is a hyperbolic pair in $\mathcal{I}(\mathcal{V}_r)$. Hence the space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form

$$\mathcal{I}(\mathcal{V}_r) = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_\nu, b_\nu\rangle \perp \langle w_1, w_2\rangle,$$

where $(a_1, b_1), (a_2, b_2), \ldots, (a_\nu, b_\nu), (w_1, w_2)$ are hyperbolic pairs in $\mathcal{I}(\mathcal{V}_r)$. This implies that $\nu_r = \nu + 1$ when $n \equiv 3, 5 \pmod 8$ and r is even.

From this and by (5.3.1), parts (a) and (b) follow immediately in the case when n is odd.

(ii) Next, let n be even. Here $\mathbf{1}$ belongs to both $\mathcal{I}(\mathcal{V})$ and $\mathcal{I}(\mathcal{V}_r)$. Further, by (5.3.1), we see that the Witt index ν of the quadratic space $(\mathcal{I}(\mathcal{V}), \mathcal{Q})$ is given by $\nu = \frac{n}{2}$ if $n \equiv 0 \pmod 8$, while $\nu = \frac{n-2}{2}$ if $n \equiv 2, 4, 6 \pmod 8$. We further observe that $\nu \le \nu_r \le \frac{n}{2}$. We note that $\mathcal{Q}_r(\mathbf{1}) = 1$ when $n \equiv 2, 6 \pmod 8$, which implies that the all-one vector $\mathbf{1}$ does not belong to any totally singular subspace of $\mathcal{I}(\mathcal{V}_r)$. We also note that $\mathcal{Q}_r(\mathbf{1}) = 0$ when $n \equiv 0, 4 \pmod 8$. Now working in a similar manner as in case (i), parts (a) and (b) follow immediately in the case when n is even.

□

From now on, let ν_r denote the Witt index of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$. Now for $0 \le k \le n$, let $\mathfrak{D}_r(n; k)$ denote the number of distinct doubly even codes of length n and dimension k over $\mathcal{T}_r$, or equivalently, the number of distinct k-dimensional totally singular subspaces of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$. Note that $\mathfrak{D}_r(n;0) = 1$ and $\mathfrak{D}_r(n;k) = 0$ for $\nu_r < k \leq n$. In the following theorem, we obtain the explicit value of the number $\mathfrak{D}_r(n;k)$ for $1 \leq k \leq \nu_r$.

Theorem 5.3.1. *For $1 \leq k \leq \nu_r$, the following hold.*

(a) When n is odd, we have

$$\mathfrak{D}_r(n;k) = \begin{cases} \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} + 2^{r(\frac{n-1}{2}-i)} - 2^{r(\frac{n-1}{2}-i-1)} - 1}{2^{r(i+1)} - 1} \right) \\ \textit{if either } n \equiv 1,7 \pmod 8 \textit{ or } n \equiv 3,5 \pmod 8 \textit{ and } r \textit{ is even;} \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} - 2^{r(\frac{n-1}{2}-i)} + 2^{r(\frac{n-1}{2}-i-1)} - 1}{2^{r(i+1)} - 1} \right) \\ \textit{if } n \equiv 3,5 \pmod 8 \textit{ and } r \textit{ is odd.} \end{cases}$$

(b) When n is even, we have

$$\mathfrak{D}_r(n;k) = \begin{cases} \displaystyle\left(\frac{2^{r(n-k-1)} + 2^{r(\frac{n}{2})} - 2^{r(\frac{n}{2}-1)} - 1}{2^{rk} - 1} \right) \prod_{i=0}^{k-2} \left(\frac{(2^{r(\frac{n-4}{2}-i)} + 1)(2^{r(\frac{n-2}{2}-i)} - 1)}{2^{r(i+1)} - 1} \right) \\ \textit{if either } n \equiv 0 \pmod 8 \textit{ or } n \equiv 4 \pmod 8 \textit{ and } r \textit{ is even;} \\ \displaystyle\left(\frac{2^{r(n-k-1)} - 2^{r(\frac{n}{2})} + 2^{r(\frac{n}{2}-1)} - 1}{2^{rk} - 1} \right) \prod_{i=0}^{k-2} \left(\frac{(2^{r(\frac{n-4}{2}-i)} - 1)(2^{r(\frac{n-2}{2}-i)} + 1)}{2^{r(i+1)} - 1} \right) \\ \textit{if } n \equiv 4 \pmod 8 \textit{ and } r \textit{ is odd;} \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2-2i)} - 1}{2^{r(i+1)} - 1} \right) \quad \textit{if } n \equiv 2,6 \pmod 8. \end{cases}$$

Proof. To prove the result, let k be a fixed integer satisfying $1 \leq k \leq \nu_r$. We first note that $\mathbf{1} \in \mathcal{I}(\mathcal{V}_r)$ if and only if n is even. Accordingly, we will distinguish the following two cases: **(I)** n is odd and **(II)** n is even.

(I) First let n be odd. Here by Lemma 5.3.1, we see that the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form

$$\mathcal{I}(\mathcal{V}_r) = \langle \alpha_1, \beta_1 \rangle \perp \langle \alpha_2, \beta_2 \rangle \perp \cdots \perp \langle \alpha_{\nu_r}, \beta_{\nu_r} \rangle \perp W_r,$$

where ν_r is the Witt index of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$, the pairs (α_1, β_1), (α_2, β_2), $\ldots$, $(\alpha_{\nu_r}, \beta_{\nu_r})$ are hyperbolic pairs in $\mathcal{I}(\mathcal{V}_r)$ and W_r is a non-singular subspace of $\mathcal{I}(\mathcal{V}_r)$ having dimension $n-1-2\nu_r$. By Lemma 5.3.1(a), we note that $\nu_r = \frac{n-1}{2}$ if either $n \equiv 1, 7 \pmod 8$ or $n \equiv 3, 5 \pmod 8$ and r is even, while $\nu_r = \frac{n-3}{2}$ if $n \equiv 3, 5 \pmod 8$ and r is odd. We next observe that any k-dimensional totally singular subspace U of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ is of the form $U = \langle \upsilon_1, \upsilon_2, \ldots, \upsilon_k \rangle$, where $\upsilon_1, \upsilon_2, \ldots, \upsilon_k$ are mutually orthogonal singular vectors in $\mathcal{I}(\mathcal{V}_r)$ that are linearly independent over $\mathcal{T}_r$. Now by applying Theorems 2.3.2, 2.3.7 and 2.3.8, we see that

$$\mathfrak{D}_r(n;k) = \begin{cases} \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(2\nu_r-2i-1)} + 2^{r(\nu_r-i)} - 2^{r(\nu_r-i-1)} - 1}{2^{r(i+1)} - 1} \right) & \text{if } \nu_r = \frac{n-1}{2}; \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(2\nu_r-2i+1)} - 2^{r(\nu_r+1-i)} + 2^{r(\nu_r-i)} - 1}{2^{r(i+1)} - 1} \right) & \text{if } \nu_r = \frac{n-3}{2}. \end{cases}$$

From this and by Lemma 5.3.1(a), the desired result follows.

(II) Next, let n be even. Here we see that $\mathbf{1} \in \mathcal{I}(\mathcal{V}_r)$. Let $\mathcal{V}_r'$ be an $(n-2)$-dimensional $\mathcal{T}_r$-linear subspace of $\mathcal{I}(\mathcal{V}_r)$ satisfying $\mathbf{1} \notin \mathcal{V}_r'$. Then we have $\mathcal{I}(\mathcal{V}_r) = \mathcal{V}_r' \perp \langle \mathbf{1} \rangle$. By Lemma 5.3.1, we see that the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ admits an orthogonal direct sum decomposition of the form

$$\mathcal{I}(\mathcal{V}_r) = \begin{cases} \langle \alpha_1, \beta_1 \rangle \perp \langle \alpha_2, \beta_2 \rangle \perp \cdots \perp \langle \alpha_{\nu_r}, \beta_{\nu_r} \rangle \perp \langle \mathbf{1} \rangle \\ \text{if } n \equiv 2, 6 \pmod 8; \\ \langle \alpha_1, \beta_1 \rangle \perp \langle \alpha_2, \beta_2 \rangle \perp \cdots \perp \langle \alpha_{\nu_r-1}, \beta_{\nu_r-1} \rangle \perp \langle \mathbf{1} \rangle \\ \text{if either } n \equiv 0 \pmod 8 \text{ or } n \equiv 4 \pmod 8 \text{ and } r \text{ is even;} \\ \langle \alpha_1, \beta_1 \rangle \perp \langle \alpha_2, \beta_2 \rangle \perp \cdots \perp \langle \alpha_{\nu_r-1}, \beta_{\nu_r-1} \rangle \perp W_r \perp \langle \mathbf{1} \rangle \\ \text{if } n \equiv 4 \pmod 8 \text{ and } r \text{ is odd,} \end{cases}$$

where ν_r is the Witt index of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$, the pairs $(\alpha_1, \beta_1), (\alpha_2, \beta_2), \ldots, (\alpha_{\nu_r}, \beta_{\nu_r})$ are hyperbolic pairs in $\mathcal{I}(\mathcal{V}_r)$ and W_r is a 2-dimensional non-singular subspace of $\mathcal{I}(\mathcal{V}_r)$. By Lemma 5.3.1(a), we note that $\nu_r = \frac{n}{2}$ if either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even, while $\nu_r = \frac{n-2}{2}$ if either $n \equiv 2, 6 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is odd. One can observe that any totally singular $\mathcal{T}_r$-linear subspace of $\mathcal{I}(\mathcal{V}_r)$ is either (i) contained in $\mathcal{V}_r'$, or (ii) contained in $\mathcal{I}(\mathcal{V}_r)$ but not in $\mathcal{V}_r'$.

(i) Now we will first count all distinct totally singular $\mathcal{T}_r$-linear subspaces of $\mathcal{I}(\mathcal{V}_r)$ that are contained in $\mathcal{V}_r'$. To do this, we see that any k-dimensional totally singular subspace U of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ contained in $\mathcal{V}_r'$ is of the form $U = \langle v_1, v_2, \ldots, v_k \rangle$, where $v_1, v_2, \ldots, v_k$ are mutually orthogonal singular vectors in $\mathcal{V}_r'$ that are linearly independent over $\mathcal{T}_r$. By Theorems 2.3.2, 2.3.7 and 2.3.8, we see that the total number $\mathfrak{D}_0$ of distinct k-dimensional totally singular $\mathcal{T}_r$-linear subspaces of $\mathcal{I}(\mathcal{V}_r)$ that are contained in $\mathcal{V}_r'$ is given by

$$\mathfrak{D}_0 = \begin{cases} \dfrac{(2^{r(\frac{n}{2}-1)}-1)(2^{r(\frac{n}{2}-k-1)}+1)}{2^r-1} \displaystyle\prod_{i=1}^{k-1} \left(\frac{2^{r(n-2-2i)}-1}{2^{r(i+1)}-1} \right) \\ \text{if } n \equiv 2, 6 \pmod 8; \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-3)} + 2^{r(\frac{n}{2}-1-i)} - 2^{r(\frac{n}{2}-i-2)} - 1}{2^{r(i+1)}-1} \right) \\ \text{if either } n \equiv 0 \pmod 8 \text{ or } n \equiv 4 \pmod 8 \text{ and } r \text{ is even;} \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-3)} - 2^{r(\frac{n}{2}-1-i)} + 2^{r(\frac{n}{2}-i-2)} - 1}{2^{r(i+1)}-1} \right) \\ \text{if } n \equiv 4 \pmod 8 \text{ and } r \text{ is odd.} \end{cases} \tag{5.3.3}$$

(ii) Next, we will count all distinct k-dimensional totally singular $\mathcal{T}_r$-linear subspaces of $\mathcal{I}(\mathcal{V}_r)$ that are not contained in $\mathcal{V}_r'$. Towards this, we first observe that any k-dimensional $\mathcal{T}_r$-linear subspace U of $\mathcal{I}(\mathcal{V}_r)$ that is not contained in $\mathcal{V}_r'$ is of the form

$$U = \langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle,$$

where $v_1, v_2, \ldots, v_k \in \mathcal{V}_r'$ are such that the vectors $v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k$ are linearly independent over $\mathcal{T}_r$. We further observe that such a subspace U is totally singular if and only if $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1}\rangle$ is a $(k-1)$-dimensional totally singular $\mathcal{T}_r$-linear subspace of $\mathcal{V}_r'$ and the vector υ_k is either 0 or a singular vector in $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1}\rangle^{\perp_{\mathcal{B}_r}} \setminus \langle \upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1}\rangle$ when $n \equiv 0, 4 \pmod 8$, while the vector υ_k is a non-singular vector in $\langle \upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1}\rangle^{\perp_{\mathcal{B}_r}} \setminus \langle \upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1}\rangle$ satisfying $\mathcal{Q}_r(\upsilon_k) = 1$ when $n \equiv 2, 6 \pmod 8$. Now by applying Theorems 2.3.2, 2.3.7 and 2.3.8 again, we see that the total number $\mathfrak{D}_1$ of distinct k-dimensional totally singular $\mathcal{T}_r$-linear subspaces of $\mathcal{I}(\mathcal{V}_r)$ that are not contained in $\mathcal{V}_r'$ is given by

$$\mathfrak{D}_1 = \begin{cases} \left(2^{r(n-2k-1)} - 2^{r(\frac{n}{2}-k-1)}\right) \prod\limits_{i=0}^{k-2} \left(\frac{2^{r(n-2i-3)}+2^{r(\frac{n}{2}-1-i)}-2^{r(\frac{n}{2}-2-i)}-1}{2^{r(i+1)}-1}\right) \\ \text{if } n \equiv 2, 6 \pmod 8; \\ \left(2^{r(n-2k-1)} + 2^{r(\frac{n}{2}-k)} - 2^{r(\frac{n}{2}-k-1)}\right) \prod\limits_{i=0}^{k-2} \left(\frac{2^{r(n-2i-3)}+2^{r(\frac{n}{2}-1-i)}-2^{r(\frac{n}{2}-i-2)}-1}{2^{r(i+1)}-1}\right) \\ \text{if either } n \equiv 0 \pmod 8 \text{ or } n \equiv 4 \pmod 8 \text{ and } r \text{ is even;} \\ \left(2^{r(n-2k-1)} - 2^{r(\frac{n}{2}-k)} + 2^{r(\frac{n}{2}-k-1)}\right) \prod\limits_{i=0}^{k-2} \left(\frac{2^{r(n-2i-3)}+2^{r(\frac{n}{2}-i-1)}-2^{r(\frac{n}{2}-i-2)}-1}{2^{r(i+1)}-1}\right) \\ \text{if } n \equiv 4 \pmod 8 \text{ and } r \text{ is odd.} \end{cases} \tag{5.3.4}$$

The desired result follows by noting that $\mathfrak{D}_r(n;k) = \mathfrak{D}_0 + \mathfrak{D}_1$ and on substituting the values of $\mathfrak{D}_0$ and $\mathfrak{D}_1$ from equations (5.3.3) and (5.3.4), respectively.

□

Remark 5.3.1. *Theorem 7 of Gaborit [45] follows, as a special case, on taking $r = 1$ in the above theorem.*

Next, for $1 \leq k \leq n$, let $\widehat{\sigma}_r(n;k)$ denote the number of distinct doubly even codes of length n and dimension k over $\mathcal{T}_r$ containing the all-one vector $\mathbf{1} \in \mathcal{V}_r$, or equivalently, the number of distinct k-dimensional totally singular subspaces of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ containing the all-one vector $\mathbf{1} \in \mathcal{V}_r$. Note that $\widehat{\sigma}_r(n;k) = 0$ for $\nu_r < k \leq n$. In the following theorem, we determine the explicit value of the number $\widehat{\sigma}_r(n;k)$ for $1 \leq k \leq \nu_r$.

Theorem 5.3.2. *For $1 \leq k \leq \nu_r$, we have*

$$\widehat{\sigma}_r(n;k) = \begin{cases} \prod\limits_{i=0}^{k-2} \left(\dfrac{2^{r(n-2i-3)} + 2^{r(\frac{n}{2}-i-1)} - 2^{r(\frac{n}{2}-i-2)} - 1}{2^{r(i+1)} - 1} \right) & \textit{if either } n \equiv 4 \pmod 8 \textit{ and } \\ & r \textit{ is even or } n \equiv 0 \pmod 8; \\ \prod\limits_{i=0}^{k-2} \left(\dfrac{2^{r(n-2i-3)} - 2^{r(\frac{n}{2}-i-1)} + 2^{r(\frac{n}{2}-i-2)} - 1}{2^{r(i+1)} - 1} \right) & \textit{if } n \equiv 4 \pmod 8 \textit{ and } r \textit{ is odd}; \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. To prove the result, let k be a fixed integer satisfying $1 \leq k \leq \nu_r$. We recall that the number $\widehat{\sigma}_r(n;k)$ equals the number of distinct k-dimensional totally singular subspaces of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ containing the all-one vector $\mathbf{1} \in \mathcal{V}_r$. We further note that $\mathbf{1} \in \mathcal{I}(\mathcal{V}_r)$ if and only if n is even. This implies $\widehat{\sigma}_r(n;k) = 0$ when n is odd. Further, it is easy to observe that $\mathcal{Q}_r(\mathbf{1}) = 1$ when $n \equiv 2, 6 \pmod{8}$. This implies that when $n \equiv 2, 6 \pmod{8}$, the vector $\mathbf{1}$ does not belong to any totally singular subspace of $\mathcal{I}(\mathcal{V}_r)$, which further implies that $\widehat{\sigma}_r(n;k) = 0$ in this case.

When $n \equiv 0, 4 \pmod{8}$, we recall that $\mathcal{I}(\mathcal{V}_r) = \mathcal{V}_r' \perp \langle \mathbf{1} \rangle$, where $\mathcal{V}_r'$ is an $(n-2)$-dimensional $\mathcal{T}_r$-linear subspace of $\mathcal{I}(\mathcal{V}_r)$ satisfying $\mathbf{1} \notin \mathcal{V}_r'$. It is easy to see that any k-dimensional totally singular subspace U of the quadratic space $(\mathcal{I}(\mathcal{V}_r), \mathcal{Q}_r)$ containing $\mathbf{1}$ is of the form $U = \langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} \rangle$, where $v_1, v_2, \ldots, v_{k-1}$ are mutually orthogonal and linearly independent singular vectors in $\mathcal{V}_r'$. By Lemma 5.3.1, one can easily observe that the Witt index ν_r' of the quadratic space $(\mathcal{V}_r', \mathcal{Q}_r \restriction_{\mathcal{V}_r' \times \mathcal{V}_r'})$ is given by

$$\nu_r' = \nu_r - 1 = \begin{cases} \frac{n-2}{2} & \text{if either } n \equiv 0 \pmod 8 \text{ or } n \equiv 4 \pmod 8 \text{ and } r \text{ is even;} \\ \frac{n-4}{2} & \text{if } n \equiv 4 \pmod 8 \text{ and } r \text{ is odd.} \end{cases}$$

Now working as in Theorem 5.3.1 and applying Theorems 2.3.2, 2.3.7 and 2.3.8, the desired result follows. □

Next, let $\widetilde{\sigma}_r(n;k)$ denote the number of distinct doubly even codes of length n and dimension k over $\mathcal{T}_r$ that do not contain the all-one vector $\mathbf{1} \in \mathcal{V}_r$ for $0 \leq k \leq n$. Note that $\widetilde{\sigma}_r(n;0) = 1$ and $\widetilde{\sigma}_r(n;k) = 0$ for $\nu_r < k \leq n$. In the following theorem, we determine the explicit value of the number $\widetilde{\sigma}_r(n;k)$ for $1 \leq k \leq \nu_r$.

Theorem 5.3.3. *For $1 \leq k \leq \nu_r$, we have*

$$\widetilde{\sigma}_r(n;k) = \begin{cases} \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} + 2^{r(\frac{n-1}{2}-i)} - 2^{r(\frac{n-1}{2}-i-1)} - 1}{2^{r(i+1)} - 1} \right) \\ \text{\textit{if either} } n \equiv 3, 5 \pmod 8 \text{ \textit{and} } r \text{ \textit{is even or} } n \equiv 1, 7 \pmod 8; \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} - 2^{r(\frac{n-1}{2}-i)} + 2^{r(\frac{n-1}{2}-i-1)} - 1}{2^{r(i+1)} - 1} \right) \\ \text{\textit{if} } n \equiv 3, 5 \pmod 8 \text{ \textit{and} } r \text{ \textit{is odd};} \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} + 2^{r(\frac{n}{2}-i)} - 2^{r(\frac{n}{2}-i-1)} - 2^r}{2^{r(i+1)} - 1} \right) \\ \text{\textit{if either} } n \equiv 4 \pmod 8 \text{ \textit{and} } r \text{ \textit{is even or} } n \equiv 0 \pmod 8; \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2i-2)} - 2^{r(\frac{n}{2}-i)} + 2^{r(\frac{n}{2}-i-1)} - 2^r}{2^{r(i+1)} - 1} \right) \\ \text{\textit{if} } n \equiv 4 \pmod 8 \text{ \textit{and} } r \text{ \textit{is odd};} \\ \displaystyle\prod_{i=0}^{k-1} \left(\frac{2^{r(n-2-2i)} - 1}{2^{r(i+1)} - 1} \right) \quad \text{\textit{if} } n \equiv 2, 6 \pmod 8. \end{cases}$$

Proof. It follows immediately from Theorems 5.3.1 and 5.3.2 by noting that $\mathfrak{D}_r(n;k) = \widehat{\sigma}_r(n;k) + \widetilde{\sigma}_r(n;k)$ for $0 \leq k \leq n$. □

The numbers $\mathfrak{D}_r(n;k)$, $\widehat{\sigma}_r(n;k)$ and $\widetilde{\sigma}_r(n;k)$ are needed to count all self-orthogonal and self-dual codes of length n over $\mathscr{R}_{e,r}$. In the following section, we will extend the recursive method employed by Nagata *et al.* [75] to construct self-orthogonal and self-dual codes over the Galois ring $\mathscr{R}_{e,r}$.

5.4 A modified recursive method to construct and enumerate self-orthogonal and self-dual codes over $\mathscr{R}_{e,r}$

Throughout this section, let us assume that

$$s = \left\lfloor \frac{e}{2} \right\rfloor.$$

One can easily see that $\lceil \frac{e}{2} \rceil = s + \theta$, where $\theta = 0$ if e is even, while $\theta = 1$ if e is odd. Next, let n be a positive integer, and let $k_1, k_2, \ldots, k_e, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_e + k_{e+1}$ and $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s+1 \leq i \leq e$. Further, let us define $n_0 = 0$ and $n_i = k_1 + k_2 + \cdots + k_i$ for $1 \leq i \leq e+1$.

In this section, we will extend the recursive construction method employed by Nagata *et al.* [75] to construct and count self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ from an n_s-doubly even self-orthogonal code of the same length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$ (see the proofs of Theorems 5.4.1-5.4.4). Towards this, for positive integers α and β satisfying $\beta \leq e$, let $(D)_{\alpha,\beta}$ denote the block matrix whose (i,j)th block is the matrix $D_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq \alpha$ and $\beta \leq j \leq e$. Moreover, for a positive integer ω, let $[H]_\omega$ denote the column block matrix whose ith block is the matrix $H_\ell \in \mathcal{M}_{k_\ell \times n}(\mathcal{T}_r)$ for $1 \leq \ell \leq \omega$.

We need the following lemma to count self-orthogonal and self-dual codes over $\mathscr{R}_{e,r}$.

Lemma 5.4.1. *Let $e \geq 3$. Let $\mathcal{A} \in \mathcal{M}_{n_{s+\theta} \times n}(\mathcal{T}_r)$ and $Y \in \mathcal{M}_{n_s \times n}(\mathcal{T}_r)$ be two matrices of the form*

$$\mathcal{A} = \begin{bmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_{s+\theta} \end{bmatrix} = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1} & \mathcal{A}_{1,2} & \cdots & \mathcal{A}_{1,s+\theta-1} & \cdots & \mathcal{A}_{1,e-1} & \mathcal{A}_{1,e} \\ 0 & I_{k_2} & \mathcal{A}_{2,2} & \cdots & \mathcal{A}_{2,s+\theta-1} & \cdots & \mathcal{A}_{2,e-1} & \mathcal{A}_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_{s+\theta}} & \cdots & \mathcal{A}_{s+\theta,e-1} & \mathcal{A}_{s+\theta,e} \end{bmatrix}$$

and

$$Y = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_s \end{bmatrix} = \begin{bmatrix} 0 & 0 & Y_{1,2} & Y_{1,3} & \cdots & Y_{1,s+1} & \cdots & Y_{1,e-1} & Y_{1,e} \\ 0 & 0 & 0 & Y_{2,3} & \cdots & Y_{2,s+1} & \cdots & Y_{2,e-1} & Y_{2,e} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & Y_{s,s+1} & \cdots & Y_{s,e-1} & Y_{s,e} \end{bmatrix},$$

where columns of the matrices $\mathcal{A}$ and Y are partitioned into blocks of sizes $k_1, k_2, \ldots,$ k_e, k_{e+1}, the matrix I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathcal{T}_r$, $\mathcal{A}_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s+\theta$ and $i \leq j \leq e$, and $Y_{a,b} \in \mathcal{M}_{k_a \times k_{b+1}}(\mathcal{T}_r)$ for $1 \leq a \leq s$ and $a < b \leq e$. Suppose that the matrix $\mathcal{A}$ satisfies the condition $\mathcal{A}\mathcal{A}^t \equiv 0 \pmod 2$ and that the *matrix* $(\mathcal{A})_{s,s+1+\theta} \in \mathcal{M}_{n_s \times (n-n_{s+1+\theta})}(\mathcal{T}_r)$ *is of full row-rank. Let us write*

$$[\mathcal{A}]_s[\mathcal{A}]_s^t \equiv 2F + 4H \pmod 8,$$

where $F \in Alt_{n_s}(\mathcal{T}_r)$ *and* $H \in Sym_{n_s}(\mathcal{T}_r)$*, (here the matrix* $[\mathcal{A}]_s$ *is viewed over* $\mathscr{R}_{e,r}$*). Next, let* ω *be a fixed integer satisfying* $1 \leq \omega \leq s-1+\theta$*, and let* H_ω *be the matrix over* $\mathcal{T}_r$ *whose rows are the first* n_ω *rows of the matrix* H*. Then consider the following system*

$$\left.\begin{array}{rcl} [\mathcal{A}]_s Y^t + Y[\mathcal{A}]_s^t & \equiv & F \pmod 2 \\ \text{and } \mathcal{D}iag\big(H_\omega + [\mathcal{A}]_\omega [Y]_\omega^t + [Y]_\omega [Y]_\omega^t\big) & \equiv & 0 \pmod 2 \end{array}\right\} \tag{5.4.1}$$

of matrix equations in the unknown matrix $Y \in \mathcal{M}_{n_s \times n}(\mathcal{T}_r)$*. Then the following hold.*

(a) If $\mathbf{1}$ *does not belong to the* $\mathcal{T}_r$*-span of the rows of the matrix* $[\mathcal{A}]_\omega$*, then the system* (5.4.1) *always has a solution.*

(b) If $\mathbf{1}$ *belongs to the* $\mathcal{T}_r$*-span of the rows of the matrix* $[\mathcal{A}]_\omega$*, then the system* (5.4.1) *has a solution if and only if either* $n \equiv 0 \pmod 8$ *or* $n \equiv 4 \pmod 8$ *and* r *is even.*

Moreover, if the system (5.4.1) *has a solution, then the number of its solutions is given by*

$$2^\epsilon (2^r)^{\sum\limits_{i=3}^{s+1} k_i n_{i-2} + n_s(n-n_{s+1}) - n_\omega - \frac{n_s(n_s-1)}{2}},$$

where $\epsilon = 0$ *if* $\mathbf{1}$ *does not belong to the* $\mathcal{T}_r$*-span of the rows of the matrix* $[\mathcal{A}]_\omega$*, while* $\epsilon = 1$ *if* $\mathbf{1}$ *belongs to the* $\mathcal{T}_r$*-span of the rows of the matrix* $[\mathcal{A}]_\omega$ *with either* $n \equiv 0 \pmod 8$ *or* $n \equiv 4 \pmod 8$ *and* r *is even.*

Proof. To prove the result, let us suppose that $\mathcal{A} = (\mathbf{a}_i)$ and $Y = (\mathbf{y}_j)$, where $\mathbf{a}_i$'s and $\mathbf{y}_j$'s are the rows of the matrices $\mathcal{A}$ and Y, respectively. Let $F = (f_{i,j})$, where $f_{i,j} \in \mathcal{T}_r$ denotes the (i,j)-th entry of the matrix F for $1 \leq i,j \leq n_s$. Here we note that $f_{i,i} = 0$ for $1 \leq i \leq n_s$. Further, let $H = (h_{i,j})$, where $h_{i,j} \in \mathcal{T}_r$ denotes the (i,j)-th entry of the matrix H for $1 \leq i,j \leq n_s$. We next observe that the system (5.4.1) of matrix equations is equivalent to the following system of equations in unknowns $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{n_s}$ over $\mathcal{T}_r$:

$$\left.\begin{array}{rcll} \mathbf{a}_i \cdot \mathbf{y}_j + \mathbf{a}_j \cdot \mathbf{y}_i & \equiv & f_{i,j} \pmod 2 & \text{for } 1 \leq i < j \leq n_s \text{ and} \\ \mathbf{a}_i \cdot \mathbf{y}_i + \mathbf{y}_i \cdot \mathbf{y}_i & \equiv & h_{i,i} \pmod 2 & \text{for } 1 \leq i \leq n_\omega. \end{array}\right\} \tag{5.4.2}$$

When $r = 1$, we see that the equation $\mathbf{a}_i \cdot \mathbf{y}_i + \mathbf{y}_i \cdot \mathbf{y}_i = h_{i,i}$ can be rewritten as $\mathbf{a}_i \cdot \mathbf{y}_i + \mathbf{1} \cdot \mathbf{y}_i = h_{i,i}$ for $1 \leq i \leq n_\omega$, and hence the system (5.4.2) is indeed a system of linear equations. However, when $r \geq 2$, the system (5.4.2) consists of both linear and non-linear equations. Further, we observe that counting solutions of the system (5.4.2) of equations in unknowns $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{n_s}$ over $\mathcal{T}_r$ is equivalent to counting solutions of the following systems of equations in unknowns $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{n_s}$ over $\mathcal{T}_r$:

$$\left.\begin{array}{rcll} \mathbf{a}_i \cdot \mathbf{y}_j + \mathbf{a}_j \cdot \mathbf{y}_i & \equiv & f_{i,j} \pmod 2 & \text{for } 1 \leq i < j \leq n_s, \\ \mathbf{a}_i \cdot \mathbf{y}_i & \equiv & \Theta_i + h_{i,i} \pmod 2 & \text{for } 1 \leq i \leq n_\omega \text{ and} \\ \mathbf{y}_i \cdot \mathbf{y}_i & \equiv & \Theta_i \pmod 2 & \text{for } 1 \leq i \leq n_\omega, \end{array}\right\} \tag{5.4.3}$$

where $(\Theta_1, \Theta_2, \ldots, \Theta_{n_\omega})$ runs over $(\mathcal{T}_r)^{n_\omega}$.

To count solutions of the system (5.4.3), let $(\Theta_1, \Theta_2, \ldots, \Theta_{n_\omega}) \in (\mathcal{T}_r)^{n_\omega}$ be fixed arbitrarily. For this particular choice of $(\Theta_1, \Theta_2, \ldots, \Theta_{n_\omega}) \in (\mathcal{T}_r)^{n_\omega}$, we observe that the system (5.4.3) of equations is equivalent to the following system of equations in unknowns $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_{n_s}$ over $\mathcal{T}_r$:

$$\left.\begin{array}{rcll} \mathbf{a}_i \cdot \mathbf{y}_j + \mathbf{a}_j \cdot \mathbf{y}_i & \equiv & f_{i,j} \pmod 2 & \text{for } 1 \leq i < j \leq n_s, \\ \mathbf{a}_i \cdot \mathbf{y}_i & \equiv & \Theta_i + h_{i,i} \pmod 2 & \text{for } 1 \leq i \leq n_\omega \text{ and} \\ \mathbf{1} \cdot \mathbf{y}_i & \equiv & \Theta_i^{2^{r-1}} \pmod 2 & \text{for } 1 \leq i \leq n_\omega. \end{array}\right\} \tag{5.4.4}$$

We further note that for each integer ℓ satisfying $1 \leq \ell \leq n_s$, there exists a unique integer c_ℓ satisfying $1 \leq c_\ell \leq s$ and $n_{c_\ell - 1} + 1 \leq \ell \leq n_{c_\ell}$ and that the corresponding unknown vector $\mathbf{y}_\ell$ is of the form $\mathbf{y}_\ell = (\mathbf{0}\; \mathbf{y}_\ell^{n - n_{c_\ell+1}})$, where $\mathbf{0}$ denotes the zero vector of length $n_{c_\ell+1}$ and $\mathbf{y}_\ell^{n-n_{c_\ell+1}}$ denotes the vector of length $n - n_{c_\ell+1}$ obtained from $\mathbf{y}_\ell$ after deleting the first $n_{c_\ell+1}$ coordinates. From this, we see that for $n_{c_\ell - 1} + 1 \leq \ell \leq n_{c_\ell}$, the first $n_{c_\ell+1}$ coordinates of $\mathbf{y}_\ell$ are zero, which implies that there are $n - n_{c_\ell+1}$ variables in $\mathbf{y}_\ell$. Now for $1 \leq \ell \leq n_s$, let $\widetilde{\mathbf{y}}_\ell = \mathbf{y}_\ell^{n-n_{c_\ell+1}}$ (*resp.* $\widetilde{\mathbf{a}}_\ell = \mathbf{a}_\ell^{n-n_{c_\ell+1}}$) denote the vector of length $n - n_{c_\ell+1}$ obtained from $\mathbf{y}_\ell$ (*resp.* $\mathbf{a}_\ell$) after deleting the first

$n_{c_\ell+1}$ coordinates. In view of this, we observe that the system (5.4.4) of equations is equivalent to the following system of equations in unknowns $\widetilde{\mathbf{y}}_1, \widetilde{\mathbf{y}}_2, \ldots, \widetilde{\mathbf{y}}_{n_s}$ over $\mathcal{T}_r$:

$$\begin{aligned}
\widetilde{\mathbf{a}}_i \cdot \widetilde{\mathbf{y}}_j + \widetilde{\mathbf{a}}_j \cdot \widetilde{\mathbf{y}}_i &\equiv f_{i,j} \pmod 2 && \text{for } 1 \leq i < j \leq n_s, \\
\widetilde{\mathbf{a}}_i \cdot \widetilde{\mathbf{y}}_i &\equiv \Theta_i + h_{i,i} \pmod 2 && \text{for } 1 \leq i \leq n_\omega \text{ and} \\
\widetilde{\mathbf{1}} \cdot \widetilde{\mathbf{y}}_i &\equiv \Theta_i^{2^{r-1}} \pmod 2 && \text{for } 1 \leq i \leq n_\omega,
\end{aligned}$$

where $\widetilde{\mathbf{1}}$ denotes the all-one vector having the same length as that of $\widetilde{\mathbf{y}}_i$ for each i. Note that the above system of equations can be represented by the following matrix equation:

$$\mathcal{M} \begin{bmatrix} \widetilde{\mathbf{y}}_1^t \\ \widetilde{\mathbf{y}}_2^t \\ \widetilde{\mathbf{y}}_3^t \\ \vdots \\ \widetilde{\mathbf{y}}_{n_\omega-1}^t \\ \widetilde{\mathbf{y}}_{n_\omega}^t \\ \widetilde{\mathbf{y}}_{n_\omega+1}^t \\ \vdots \\ \widetilde{\mathbf{y}}_{n_s}^t \end{bmatrix} \equiv \begin{bmatrix} \Theta_1^{2^{r-1}} \\ \vdots \\ \Theta_{n_\omega}^{2^{r-1}} \\ \Theta_1 + h_{1,1} \\ \vdots \\ \Theta_{n_\omega} + h_{\omega,\omega} \\ f_{1,2} \\ \vdots \\ f_{n_{s-1},n_s} \end{bmatrix} \pmod 2, \tag{5.4.5}$$

where

$$\mathcal{M} = \begin{bmatrix}
\widetilde{\mathbf{1}} & & & & & & \\
 & & \ddots & & & & \\
 & & & & \widetilde{\mathbf{1}} & & \\
\widetilde{\mathbf{a}}_1 & & & & & & \\
 & & \ddots & & & & \\
 & & & & \widetilde{\mathbf{a}}_{n_\omega} & & \\
\widetilde{\mathbf{a}}_2 & \widetilde{\mathbf{a}}_1 & & & & & \\
\vdots & \vdots & \vdots & & & & \\
\widetilde{\mathbf{a}}_{n_s} & & & & & & \widetilde{\mathbf{a}}_1 \\
 & & & \vdots & \vdots & \vdots & \\
 & & & & & \widetilde{\mathbf{a}}_{n_s} & \widetilde{\mathbf{a}}_{n_s-1}
\end{bmatrix}.$$

It is easy to see that the matrix $\mathcal{M}$ is of order $\big(2n_\omega + \frac{n_s(n_s-1)}{2}\big) \times \big(\sum\limits_{i=3}^{s+1} k_i n_{i-2} + n_s(n-n_{s+1})\big)$.

We next assert that the rows of the matrix $\mathcal{M}$ are linearly dependent over $\mathcal{T}_r$ if and only if $\mathbf{1}$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$. To prove this assertion, we first note that the matrix $(\mathcal{A})_{s,s+1+\theta}$ is a full row-rank matrix over $\mathcal{T}_r$, which implies that the vectors $\mathbf{a}_1^{n-n_{c+1}}, \mathbf{a}_2^{n-n_{c+1}}, \ldots, \mathbf{a}_{n_s}^{n-n_{c+1}}$, obtained by deleting the first n_{c+1} coordinates from the vectors $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n_s}$ respectively, are linearly independent over $\mathcal{T}_r$ for $1 \leq c \leq s$. From this, it follows that the vectors $\widetilde{\mathbf{a}}_1, \widetilde{\mathbf{a}}_2, \ldots, \widetilde{\mathbf{a}}_{n_s}$ are linearly independent over $\mathcal{T}_r$. Next, it is easy to see that if the rows of the matrix $\mathcal{M}$ over $\mathcal{T}_r$ are linearly dependent, then there exist integers $i_1, i_2, \ldots, i_\ell$ satisfying $1 \leq i_1 < i_2 < \cdots < i_\ell \leq n_\omega$ and

$$\beta_{i_1}\widetilde{\mathbf{a}}_{i_1} + \beta_{i_2}\widetilde{\mathbf{a}}_{i_2} + \cdots + \beta_{i_\ell}\widetilde{\mathbf{a}}_{i_\ell} \equiv \widetilde{\mathbf{1}} \pmod{2} \quad \text{for some } \beta_{i_1}, \beta_{i_2}, \ldots, \beta_{i_\ell} \in \mathcal{T}_r \setminus \{0\}.$$

This implies that $\beta_{i_1}\mathbf{a}_{i_1}^{n-n_{c+1}} + \beta_{i_2}\mathbf{a}_{i_2}^{n-n_{c+1}} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell}^{n-n_{c+1}} \equiv \mathbf{1}^{n-n_{c+1}} \pmod{2}$ for some integer c satisfying $1 \leq c \leq s$, which further implies that $\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell} \equiv (\mathbf{0}\ \mathbf{a}\ \mathbf{a}'\ \mathbf{1}^{n-n_{c+1}}) \pmod{2}$, where $\mathbf{a}$ and $\mathbf{a}'$ are vectors of lengths k_c and k_{c+1} over $\mathcal{T}_r$, respectively.

Here we claim that $\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell} \equiv (\mathbf{0}\ \mathbf{1}^{n-n_{c-1}}) \pmod{2}$, *i.e.*, $\mathbf{a} \equiv \mathbf{1}^{k_c} \pmod{2}$ and $\mathbf{a}' \equiv \mathbf{1}^{k_{c+1}} \pmod{2}$.

To prove this, we see that if both k_c and k_{c+1} are zero, then we are through. Now if $k_{c+1} > 0$, we note that for an integer j_1 satisfying $n_c + 1 \leq j_1 \leq n_{c+1}$, the vector $\mathbf{a}_{j_1}$ is of the form $(\mathbf{0}\ \mathbf{e}_{j_1}\ \mathbf{a}_{j_1}^{n-n_{c+1}})$, where $\mathbf{e}_{j_1}$ is a vector of length k_{c+1} having 1 at the $(j_1 - n_c)$-th position and 0s elsewhere. Since the matrix $\mathcal{A}$ satisfies $\mathcal{A}\mathcal{A}^t \equiv \mathbf{0} \pmod{2}$, we have $\mathbf{a}_{j_1} \cdot \mathbf{a}_{j_1} \equiv 0 \pmod{2}$ and $\mathbf{a}_{j_1} \cdot (\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell}) \equiv 0 \pmod{2}$. From this, we obtain $\mathbf{a}' \equiv \mathbf{1}^{k_{c+1}} \pmod{2}$, which implies that $\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell} \equiv (\mathbf{0}\ \mathbf{a}\ \mathbf{1}^{n-n_c}) \pmod{2}$. Now if $k_c = 0$, then we have $\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell} \equiv (\mathbf{0}\ \mathbf{1}^{n-n_{c-1}}) \pmod{2}$. On the other hand, if $k_c > 0$, then for an integer j satisfying $n_{c-1} + 1 \leq j \leq n_c$, we note that the vector $\mathbf{a}_j$ is of the form $(\mathbf{0}\ \mathbf{e}_j\ \mathbf{a}_j^{n-n_c})$, where $\mathbf{e}_j$ is a vector of length k_c having 1 at the $(j - n_{c-1})$-th position and 0s elsewhere. Using again the fact that the matrix $\mathcal{A}$ satisfies $\mathcal{A}\mathcal{A}^t \equiv 0 \pmod{2}$, one can show that $\mathbf{a} \equiv \mathbf{1}^{k_c} \pmod{2}$, which further implies that $\beta_{i_1}\mathbf{a}_{i_1} + \beta_{i_2}\mathbf{a}_{i_2} + \cdots + \beta_{i_\ell}\mathbf{a}_{i_\ell} \equiv (\mathbf{0}\ \mathbf{1}^{n-n_{c-1}})$

(mod 2). From this, we obtain $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv(\mathbf{0}\ \mathbf{1}^{n-n_{c-1}})\pmod 2$ in all the cases, which proves our claim.

Now if $k_j=0$ for $1\leq j\leq c-1$, then we have $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv\mathbf{1}^n$ (mod 2), which implies that $\mathbf{1}=(1,1,\ldots,1)$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$.

Next, suppose that there exists a positive integer α satisfying $1\leq\alpha\leq c-1$, $k_\alpha>0$ and $k_{\alpha+1}=k_{\alpha+2}=\cdots=k_{c-1}=0$. This implies that $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv(\mathbf{0}\ \mathbf{1}^{n-n_\alpha})\pmod 2$. Now for an integer g satisfying $n_{\alpha-1}+1\leq g\leq n_\alpha$, the vector $\mathbf{a}_g$ is of the form $(\mathbf{0}\ \mathbf{e}_g\ \mathbf{a}_g^{n-n_\alpha})$, where $\mathbf{e}_g$ is a vector of length k_α having 1 at the $(g-n_{\alpha-1})$-th position and 0s elsewhere. Since the matrix $\mathcal{A}$ satisfies $\mathcal{A}\mathcal{A}^t\equiv 0$ (mod 2), we have $\mathbf{a}_g\cdot\mathbf{a}_g\equiv 0\pmod 2$ and $\mathbf{a}_g\cdot(\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell})\equiv 0$ (mod 2). This implies that $1+\mathbf{1}^{n-n_\alpha}\cdot\mathbf{a}_g^{n-n_\alpha}\equiv 0\pmod 2$ and $\mathbf{1}^{n-n_\alpha}\cdot\mathbf{a}_g^{n-n_\alpha}\equiv 0$ (mod 2), which is a contradiction.

This proves that $c=1$. From this, it follows that $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv(\mathbf{b}\ \mathbf{b}'\ \mathbf{1}^{n-n_2})\pmod 2$, where $\mathbf{b}$ and $\mathbf{b}'$ are vectors of lengths k_1 and k_2 over $\mathcal{T}_r$, respectively. Here working as above, one can show that $\mathbf{b}\equiv\mathbf{1}^{k_1}\pmod 2$ and $\mathbf{b}'\equiv\mathbf{1}^{k_2}\pmod 2$. This implies that $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv\mathbf{1}\pmod 2$, which further implies that the all-one vector $\mathbf{1}$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$. This shows that if rows of the matrix $\mathcal{M}$ are linearly dependent over $\mathcal{T}_r$, then $\mathbf{1}$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$. Further, since the vectors $\mathbf{a}_1,\mathbf{a}_2,\ldots,\mathbf{a}_{n_\omega}$ are linearly independent over $\mathcal{T}_r$, we see that there exist unique scalars $\beta_{i_1},\beta_{i_2},\ldots,\beta_{i_\ell}\in\mathcal{T}_r$ such that $\beta_{i_1}\mathbf{a}_{i_1}+\beta_{i_2}\mathbf{a}_{i_2}+\cdots+\beta_{i_\ell}\mathbf{a}_{i_\ell}\equiv\mathbf{1}\pmod 2$.

Conversely, if $\mathbf{1}$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$, then the rows of the matrix $\mathcal{M}$ are linearly dependent over $\mathcal{T}_r$. This proves the assertion.

(a) First of all, suppose that $\mathbf{1}$ belongs to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$. Here we see that $\mathbf{1}$ can be uniquely expressed as a linear combination of the rows of the matrix $[\mathcal{A}]_\omega$ over $\mathcal{T}_r$. We further see that all the rows of the matrix $\mathcal{M}$ except the last row are linearly independent over $\mathcal{T}_r$, which implies that the row-rank of the matrix $\mathcal{M}$ is $2n_\omega+\frac{n_s(n_s-1)}{2}-1$. We next observe that the matrix equation (5.4.5) has a solution if and only if $(\Theta_1,\Theta_2,\ldots,\Theta_{n_\omega})\in$

$(\mathcal{T}_r)^{n_\omega}$ satisfies

$$\Big(\sum_{b=1}^{\ell}\beta_{i_b}\Theta_{i_b}^{2^{r-1}}\Big)^2+\sum_{v=1}^{\ell}\beta_{i_v}\Theta_{i_v}^{2^{r-1}}\equiv\frac{n}{4}\pmod 2$$

and the number of its solutions is independent of such a choice of $(\Theta_1,\Theta_2,\ldots,\Theta_{n_\omega})\in(\mathcal{T}_r)^{n_\omega}$. From this and by applying Theorems 2.3.10 and 5.3.2, we observe that there exists a matrix $Y\in\mathcal{M}_{n_s\times n}(\mathcal{T}_r)$ satisfying the system (5.4.1) of matrix equations if and only if either $n\equiv 0\pmod 8$ or $n\equiv 0\pmod 4$ and r is even and that such a matrix Y has precisely

$$\begin{aligned}&2\times(2^r)^{n_\omega-1}\times(2^r)^{\sum\limits_{i=3}^{s+1}k_in_{i-2}+n_s(n-n_{s+1})-2n_\omega-\frac{n_s(n_s-1)}{2}+1}\\=\;&2(2^r)^{\sum\limits_{i=3}^{s+1}k_in_{i-2}+n_s(n-n_{s+1})-n_\omega-\frac{n_s(n_s-1)}{2}}\end{aligned}$$

distinct choices.

(b) Suppose that $\mathbf{1}$ does not belong to the $\mathcal{T}_r$-span of the rows of the matrix $[\mathcal{A}]_\omega$. This, by the above assertion, implies that the rows of the matrix $\mathcal{M}$ are linearly independent over $\mathcal{T}_r$. This further implies that the row-rank of the matrix $\mathcal{M}$ is $2n_\omega+\frac{n_s(n_s-1)}{2}$ and that the matrix equation (5.4.5) always has a solution. Further, the number of solutions of the system (5.4.3) in the unknown matrix $Y\in\mathcal{M}_{n_s\times n}(\mathcal{T}_r)$ is independent of the choice of $(\Theta_1,\Theta_2,\ldots,\Theta_{n_\omega})\in(\mathcal{T}_r)^{n_\omega}$ and is given by

$$(2^r)^{\sum\limits_{i=3}^{s+1}k_in_{i-2}+n_s(n-n_{s+1})-2n_\omega-\frac{n_s(n_s-1)}{2}}.$$

From this, we observe that there exists a matrix $Y\in\mathcal{M}_{n_s\times n}(\mathcal{T}_r)$ satisfying the system (5.4.1) of matrix equations and that such a matrix Y has precisely

$$\begin{aligned}&(2^r)^{n_\omega}\times(2^r)^{\sum\limits_{i=3}^{s+1}k_in_{i-2}+n_s(n-n_{s+1})-2n_\omega-\frac{n_s(n_s-1)}{2}}\\&=(2^r)^{\sum\limits_{i=3}^{s+1}k_in_{i-2}+n_s(n-n_{s+1})-n_\omega-\frac{n_s(n_s-1)}{2}}\end{aligned}$$

distinct choices.

This proves the lemma. □

Now we shall distinguish the following two cases: (i) $e = 2$ and (ii) $e \geq 3$.

5.4.1 The case $e = 2$

Throughout this section, let us assume that $e = 2$. Here k_1, k_2, k_3 are non-negative integers satisfying $n = k_1 + k_2 + k_3$ and $k_1 \leq k_3$. In the following theorem, we show that if there exists a doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$, then there exists a self-orthogonal code $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$, and vice versa. We also count all distinct self-orthogonal codes $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$ for a given choice of $\mathscr{B}_0$.

Theorem 5.4.1. *(a) There exists a doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$ if and only if there exists a self-orthogonal code $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$.*

(b) Furthermore, each doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$ gives rise to precisely

$$2^{\frac{rk_1(2n-3k_1-2k_2+1)}{2}} \begin{bmatrix} k_2 + k_3 - k_1 \\ k_2 \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$.

Proof. To prove the result, let $\mathscr{B}_2$ be a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$. We see, using Lemma 2.2.1, that $\mathscr{B}_0 = Tor_1(\mathscr{B}_2)$ is a k_1-dimensional doubly even code over $\mathcal{T}_r$.

From now on, let $\mathscr{B}_0$ be a doubly even code of length n over $\mathcal{T}_r$. Here by Remark 4.3.1, we assume, without any loss of generality, that the code $\mathscr{B}_0$ has a generator matrix

$$G_0 = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \mathcal{A}_{1,2}^{(0)} \end{bmatrix},$$

where columns of the matrix G_0 are partitioned into blocks of sizes k_1, k_2, k_3, the matrix I_{k_1} is the $k_1 \times k_1$ identity matrix over $\mathcal{T}_r$, $\mathcal{A}_{1,1}^{(0)} \in \mathcal{M}_{k_1 \times k_2}(\mathcal{T}_r)$ and $\mathcal{A}_{1,2}^{(0)} \in \mathcal{M}_{k_1 \times k_3}(\mathcal{T}_r)$, and the matrix $\mathcal{A}_{1,2}^{(0)}$ is of full row-rank over $\mathcal{T}_r$. Since the matrix G_0

generates a doubly even code over $\mathcal{T}_r$, we have

$$G_0G_0^t = I_{k_1} + \mathcal{A}_{1,1}^{(0)}\mathcal{A}_{1,1}^{(0)t} + \mathcal{A}_{1,2}^{(0)}\mathcal{A}_{1,2}^{(0)t} \equiv\ 2F \pmod 4, \text{ where } F \in Alt_{k_1}(\mathcal{T}_r),$$

(note that the matrix $G_0G_0^t$ is viewed over $\mathscr{R}_{2,r}$). Now let us define a matrix G_2 over $\mathscr{R}_{2,r}$ as

$$G_2 = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \mathcal{A}_{1,2}^{(0)} + 2\mathcal{A}_{1,2}^{(1)} \\ 0 & 2I_{k_2} & 2\mathcal{A}_{2,2}^{(0)} \end{bmatrix},$$

where $\mathcal{A}_{1,2}^{(1)} \in \mathcal{M}_{k_1\times k_3}(\mathcal{T}_r)$ and $\mathcal{A}_{2,2}^{(0)} \in \mathcal{M}_{k_2\times k_3}(\mathcal{T}_r)$. Let $\mathscr{B}_2$ be the linear code of length n over $\mathscr{R}_{2,r}$ with a generator matrix G_2. It is easy to see that $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$ and that the code $\mathscr{B}_2$ is of the type $\{k_1, k_2\}$. Further, by Theorem 2.2.4, we observe that the code $\mathscr{B}_2$ is a self-orthogonal code over $\mathscr{R}_{2,r}$ if and only if there exist matrices $\mathcal{A}_{1,2}^{(1)} \in \mathcal{M}_{k_1\times k_3}(\mathcal{T}_r)$ and $\mathcal{A}_{2,2}^{(0)} \in \mathcal{M}_{k_2\times k_3}(\mathcal{T}_r)$ satisfying the following two matrix equations:

$$\begin{aligned} \mathcal{A}_{1,2}^{(0)}\mathcal{A}_{1,2}^{(1)t} + \mathcal{A}_{1,2}^{(1)}\mathcal{A}_{1,2}^{(0)t} &\equiv F \pmod 2, &(5.4.6)\\ \mathcal{A}_{1,1}^{(0)} + \mathcal{A}_{1,2}^{(0)}\mathcal{A}_{2,2}^{(0)t} &\equiv 0 \pmod 2. &(5.4.7)\end{aligned}$$

To show that there exists a matrix $\mathcal{A}_{1,2}^{(1)}$ satisfying (5.4.6), we note that $\mathcal{D}iag(F) = 0$ and that the matrix $\mathcal{A}_{1,2}^{(0)}$ is a full row-rank matrix over $\mathcal{T}_r$. By applying Lemma 2.1.1, we see that there exists a matrix $\mathcal{A}_{1,2}^{(1)}$ satisfying (5.4.6) and that such a matrix $\mathcal{A}_{1,2}^{(1)}$ has precisely

$$2^{\frac{rk_1(2n-3k_1-2k_2+1)}{2}}$$

distinct choices. Further, to show that there exists a matrix $\mathcal{A}_{2,2}^{(0)}$ satisfying (5.4.7), we observe, by Lemma 2.2.1 and by (2.2.2), that there exists a matrix $\mathcal{A}_{2,2}^{(0)}$ satisfying (5.4.7) if and only if the Torsion code $Tor_2(\mathscr{B}_2)$ satisfies $\mathscr{B}_0 \subseteq Tor_2(\mathscr{B}_2) \subseteq \mathscr{B}_0^{\perp}$. Furthermore, for a given choice of the code $\mathscr{B}_0$, we see that the number of choices for the matrix $\mathcal{A}_{2,2}^{(0)}$ satisfying (5.4.7) is equal to the number of choices for a linear code $\mathscr{B}$ of length n and dimension $k_1 + k_2$ over $\mathcal{T}_r$ satisfying $\mathscr{B}_0 \subseteq \mathscr{B} \subseteq \mathscr{B}_0^{\perp}$, which, by Theorem 2.3.9, has precisely $\begin{bmatrix} k_2+k_3-k_1 \\ k_2 \end{bmatrix}_{2^r}$ distinct choices. Moreover, one can easily see that each of the distinct choices for the pair of matrices $\mathcal{A}_{1,2}^{(1)}$ and $\mathcal{A}_{2,2}^{(0)}$ satisfying (5.4.6) and (5.4.7) gives rise to a distinct self-orthogonal code $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$. From this, the desired result follows immediately. □

By Theorem 2.2.4(b), we see that a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ is self-dual if and only if $2k_1 + k_2 = n$. In the following theorem, we show that if there exists a doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$, then there exists a self-dual code $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$ and vice versa, where $k_2 = n - 2k_1$. We also count all such distinct self-dual codes $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$ for a given choice of $\mathscr{B}_0$.

Theorem 5.4.2. *Let k_1, k_2 be non-negative integers satisfying $n = 2k_1 + k_2$. The following hold.*

- *(a) There exists a doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$ if and only if there exists a self-dual code $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$.*

- *(b) Furthermore, each doubly even code $\mathscr{B}_0$ of length n and dimension k_1 over $\mathcal{T}_r$ gives rise to precisely $2^{\frac{rk_1(k_1+1)}{2}}$ distinct self-dual codes $\mathscr{B}_2$ of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ satisfying $Tor_1(\mathscr{B}_2) = \mathscr{B}_0$.*

Proof. On substituting $k_3 = k_1 = n - (k_1 + k_2)$ in Theorem 5.4.1, the desired result follows immediately. □

5.4.2 The case $e \geq 3$

Throughout this section, let us suppose that $e \geq 3$. Here $k_1, k_2, \ldots, k_{e+1}$ are non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s + 1 \leq i \leq e$. In the following proposition, we consider a doubly even code $\mathscr{C}_0$ of length n and dimension n_s over $\mathcal{T}_r$ and an n_{s-1}-dimensional linear subcode $\mathscr{D}_0$ of the code $\mathscr{C}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and we provide a method to construct an n_{s-1}-doubly even self-orthogonal code $\mathscr{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over $\mathscr{R}_{2,r}$ with a free linear doubly even subcode $\mathscr{D}_2$ satisfying $Tor_1(\mathscr{C}_2) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_2) = \mathscr{D}_0$. We also count all such distinct n_{s-1}-doubly even self-orthogonal codes $\mathscr{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over $\mathscr{R}_{2,r}$.

Proposition 5.4.1. *Let $\mathscr{C}_0$ be a doubly even code of length n and dimension n_s over $\mathcal{T}_r$, and let $\mathscr{D}_0$ be an n_{s-1}-dimensional linear subcode of $\mathscr{C}_0$ satisfying the additional property that $\boldsymbol{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd.*

(a) There exists an n_{s-1}-doubly even self-orthogonal code $\mathscr{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over $\mathscr{R}_{2,r}$ with a free linear doubly even subcode $\mathscr{D}_2$ satisfying $Tor_1(\mathscr{C}_2) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_2) = \mathscr{D}_0$.

(b) Furthermore, the pair $(\mathscr{C}_0, \mathscr{D}_0)$ of codes over $\mathcal{T}_r$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=3}^{s+1} k_i n_{i-2} + n_s(n-n_{s+1}) - n_{s-1} - \frac{n_s(n_s-1)}{2}} \begin{bmatrix} k_{s+1} + n - n_{s+1} - n_s \\ k_{s+1} \end{bmatrix}_{2^r}$$

distinct n_{s-1}-doubly even self-orthogonal codes $\mathscr{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over $\mathscr{R}_{2,r}$ with a free linear doubly even subcode $\mathscr{D}_2$ satisfying $Tor_1(\mathscr{C}_2) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_2) = \mathscr{D}_0$, where $\epsilon = 1$ if $\boldsymbol{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise.

Proof. By Remark 4.3.1, we assume, without any loss of generality, that the code $\mathscr{C}_0$ has a generator matrix

$$\mathcal{G}_0 = [Z^{(0)}]_s = \begin{bmatrix} Z_1^{(0)} \\ Z_2^{(0)} \\ \vdots \\ Z_s^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \mathcal{A}_{1,2}^{(0)} & \cdots & \mathcal{A}_{1,s-1}^{(0)} & \cdots & \mathcal{A}_{1,e-1}^{(0)} & \mathcal{A}_{1,e}^{(0)} \\ 0 & I_{k_2} & \mathcal{A}_{2,2}^{(0)} & \cdots & \mathcal{A}_{2,s-1}^{(0)} & \cdots & \mathcal{A}_{2,e-1}^{(0)} & \mathcal{A}_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_s} & \cdots & \mathcal{A}_{s,e-1}^{(0)} & \mathcal{A}_{s,e}^{(0)} \end{bmatrix}$$

and its subcode $\mathscr{D}_0$ has a generator matrix

$$[Z^{(0)}]_{s-1} = \begin{bmatrix} Z_1^{(0)} \\ Z_2^{(0)} \\ \vdots \\ Z_{s-1}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \mathcal{A}_{1,2}^{(0)} & \cdots & \mathcal{A}_{1,s-2}^{(0)} & \cdots & \mathcal{A}_{1,e-1}^{(0)} & \mathcal{A}_{1,e}^{(0)} \\ 0 & I_{k_2} & \mathcal{A}_{2,2}^{(0)} & \cdots & \mathcal{A}_{2,s-2}^{(0)} & \cdots & \mathcal{A}_{2,e-1}^{(0)} & \mathcal{A}_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_{s-1}} & \cdots & \mathcal{A}_{s-1,e-1}^{(0)} & \mathcal{A}_{s-1,e}^{(0)} \end{bmatrix},$$

where columns of the matrices $\mathcal{G}_0$ and $[Z^{(0)}]_{s-1}$ are partitioned into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, the matrix I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathcal{T}_r$, $\mathcal{A}_{i,j}^{(0)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s$ and $i \leq j \leq e$, and each of the matrices $(\mathcal{A}^{(0)})_{s,s+1}$,

$(\mathcal{A}^{(0)})_{s-1,s+2},\ldots,(\mathcal{A}^{(0)})_{2,e-1}$, $\mathcal{A}^{(0)}_{1,e}$ are of full row-rank over $\mathcal{T}_r$. Since the matrix $\mathcal{G}_0$ generates a doubly even code over $\mathcal{T}_r$, we have

$$\mathcal{G}_0\mathcal{G}_0^t=[Z^{(0)}]_s[Z^{(0)}]_s^t\equiv\ 2F+4H \pmod 8,$$

where $F\in Alt_{n_s}(\mathcal{T}_r)$ and $H\in Sym_{n_s}(\mathcal{T}_r)$, (note that the matrix $\mathcal{G}_0\mathcal{G}_0^t$ is viewed over $\mathscr{R}_{e,r}$). Now to prove the result, let us define a matrix $\mathcal{G}_2$ over $\mathscr{R}_{2,r}$ as

$$\mathcal{G}_2=\begin{bmatrix} Z_1^{(2)}\\ Z_2^{(2)}\\ \vdots\\ Z_s^{(2)}\\ 2Z_{s+1}^{(2)}\end{bmatrix}=\begin{bmatrix} Z_1^{(0)}+2V_1^{(1)}\\ Z_2^{(0)}+2V_2^{(1)}\\ \vdots\\ Z_s^{(0)}+2V_s^{(1)}\\ 2Z_{s+1}^{(2)}\end{bmatrix},$$

where the matrix $[V^{(1)}]_s\in\mathcal{M}_{n_s\times n}(\mathcal{T}_r)$ is of the form

$$[V^{(1)}]_s=\begin{bmatrix} V_1^{(1)}\\ V_2^{(1)}\\ \vdots\\ V_s^{(1)}\end{bmatrix}=\begin{bmatrix} 0 & 0 & \mathcal{A}^{(1)}_{1,2} & \mathcal{A}^{(1)}_{1,3} & \cdots & \mathcal{A}^{(1)}_{1,s+1} & \cdots & \mathcal{A}^{(1)}_{1,e}\\ 0 & 0 & 0 & \mathcal{A}^{(1)}_{2,3} & \cdots & \mathcal{A}^{(1)}_{2,s+1} & \cdots & \mathcal{A}^{(1)}_{2,e}\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & \mathcal{A}^{(1)}_{s,s+1} & \cdots & \mathcal{A}^{(1)}_{s,e}\end{bmatrix}$$

with $\mathcal{A}^{(1)}_{i,j}\in\mathcal{M}_{k_i\times k_{j+1}}(\mathcal{T}_r)$ for $1\le i\le s$ and $i<j\le e$, and the matrix $Z^{(2)}_{s+1}\in\mathcal{M}_{k_{s+1}\times n}(\mathcal{T}_r)$ is of the form

$$Z^{(2)}_{s+1}=\begin{bmatrix}0 & \cdots & 0 & I_{k_{s+1}} & \mathcal{A}^{(0)}_{s+1,s+1} & \cdots & \mathcal{A}^{(0)}_{s+1,e}\end{bmatrix}$$

with $\mathcal{A}^{(0)}_{s+1,j}\in\mathcal{M}_{k_{s+1}\times k_{j+1}}(\mathcal{T}_r)$ for $s+1\le j\le e$.

Further, let $\mathscr{C}_2$ and $\mathscr{D}_2$ be linear codes of length n over $\mathscr{R}_{2,r}$ with generator matrices $\mathcal{G}_2$ and $[Z^{(2)}]_{s-1}$, respectively. We also note that the code $\mathscr{D}_2$ is a free linear subcode of $\mathscr{C}_2$ of rank n_{s-1}. It is easy to see that $Tor_1(\mathscr{D}_2)=\mathscr{D}_0$ and $Tor_1(\mathscr{C}_2)=\mathscr{C}_0$ and that the code $\mathscr{C}_2$ is of the type $\{n_s,k_{s+1}\}$. Now by Theorem 2.2.4, we observe that the code $\mathscr{C}_2$ is an n_{s-1}-doubly even self-orthogonal code over $\mathscr{R}_{2,r}$ with a free doubly even linear subcode as $\mathscr{D}_2$ if and only if there exist matrices $[V^{(1)}]_s$ and $Z^{(2)}_{s+1}$

satisfying the following system of matrix equations:

$$\begin{aligned} [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[Z^{(0)}]_s^t &\equiv F \pmod 2, & (5.4.8)\\ \mathcal{D}iag\Big(H' + [Z^{(0)}]_{s-1}[V^{(1)}]_{s-1}^t + [V^{(1)}]_{s-1}[V^{(1)}]_{s-1}^t\Big) &\equiv 0 \pmod 2, & (5.4.9)\\ [Z^{(0)}]_s Z_{s+1}^{(2)t} &\equiv 0 \pmod 2, & (5.4.10)\end{aligned}$$

where H' is an $n_{s-1} \times n_{s-1}$ matrix over $\mathcal{T}_r$ whose rows are the first n_{s-1} rows of the matrix H. Now by applying Lemma 5.4.1, we observe that there exists a matrix $[V^{(1)}]_s$ satisfying (5.4.8) and (5.4.9) and that such a matrix $[V^{(1)}]_s$ has precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=3}^{s+1} k_i n_{i-2} + n_s(n-n_{s+1}) - n_{s-1} - \frac{n_s(n_s-1)}{2}}$$

distinct choices, where $\epsilon = 1$ if $\mathbf{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise. Further, by applying Lemma 2.2.1 and Theorem 2.3.9 and working as in Theorem 5.4.1, we see that there exists a matrix $Z_{s+1}^{(2)}$ satisfying (5.4.10) and that such a matrix $Z_{s+1}^{(2)}$ has precisely $\begin{bmatrix} k_{s+1}+n-n_{s+1}-n_s \\ k_{s+1} \end{bmatrix}_{2^r}$ relevant choices. Further, it is easy to see that each of the distinct choices for the pair of matrices $[V^{(1)}]_s$ and $Z_{s+1}^{(2)}$ satisfying the system (5.4.8)-(5.4.10) of matrix equations gives rise to a distinct n_{s-1}-doubly even self-orthogonal code $\mathscr{C}_2$ of the type $\{n_s, k_{s+1}\}$ and length n over $\mathscr{R}_{2,r}$ with a free linear doubly even subcode $\mathscr{D}_2$ satisfying $Tor_1(\mathscr{C}_2) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_2) = \mathscr{D}_0$. From this, the desired result follows immediately. □

In the following proposition, we consider an n_s-doubly even self-orthogonal code $\mathscr{C}_0$ of length n and dimension n_{s+1} over $\mathcal{T}_r$, an n_s-dimensional doubly even linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and an n_{s-1}-dimensional linear subcode $\mathscr{D}_1$ of the code $\mathscr{D}_0$, and we provide a method to construct an n_{s-1}-doubly even self-orthogonal code $\mathscr{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over $\mathscr{R}_{3,r}$ with a free linear doubly even subcode $\mathscr{D}_3$ satisfying $Tor_1(\mathscr{C}_3) = \mathscr{D}_0$, $Tor_2(\mathscr{C}_3) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_3) = \mathscr{D}_1$. We also count all such distinct n_{s-1}-doubly even self-orthogonal codes $\mathscr{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over $\mathscr{R}_{3,r}$.

Proposition 5.4.2. *Let $\mathscr{C}_0$ be an n_s-doubly even self-orthogonal code of length n and dimension n_{s+1} over $\mathcal{T}_r$, and let $\mathscr{D}_0$ be an n_s-dimensional doubly even linear subcode of the code $\mathscr{C}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd. Let $\mathscr{D}_1$ be an n_{s-1}-dimensional linear subcode of $\mathscr{D}_0$. The following hold.*

(a) There exists an n_{s-1}-doubly even self-orthogonal code $\mathscr{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over $\mathscr{R}_{3,r}$ with a free linear doubly even subcode $\mathscr{D}_3$ satisfying $Tor_1(\mathscr{C}_3) = \mathscr{D}_0$, $Tor_2(\mathscr{C}_3) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_3) = \mathscr{D}_1$.

(b) Furthermore, the triplet $(\mathscr{C}_0, \mathscr{D}_0, \mathscr{D}_1)$ of codes over $\mathcal{T}_r$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + \sum\limits_{j=4}^{s+2} k_j n_{j-3} + n_s^2 - n_{s-1} + (n_s+n_{s+1})(n-n_{s+2}-n_s)} \begin{bmatrix} k_{s+2} + n - n_{s+2} - n_s \\ k_{s+2} \end{bmatrix}_{2^r}$$

distinct n_{s-1}-doubly even self-orthogonal codes $\mathscr{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over $\mathscr{R}_{3,r}$ with a free linear doubly even subcode $\mathscr{D}_3$ satisfying $Tor_1(\mathscr{C}_3) = \mathscr{D}_0$, $Tor_2(\mathscr{C}_3) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_3) = \mathscr{D}_1$, where $\epsilon = 1$ if $\mathbf{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise.

Proof. Here by Remark 4.3.1, we assume, without any loss of generality, that the code $\mathscr{C}_0$ has a generator matrix

$$\mathcal{G}_0 = [Z^{(0)}]_{s+1} = \begin{bmatrix} Z_1^{(0)} \\ Z_2^{(0)} \\ \vdots \\ Z_{s+1}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \mathcal{A}_{1,2}^{(0)} & \cdots & \mathcal{A}_{1,s}^{(0)} & \cdots & \mathcal{A}_{1,e-1}^{(0)} & \mathcal{A}_{1,e}^{(0)} \\ 0 & I_{k_2} & \mathcal{A}_{2,2}^{(0)} & \cdots & \mathcal{A}_{2,s}^{(0)} & \cdots & \mathcal{A}_{2,e-1}^{(0)} & \mathcal{A}_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I_{k_{s+1}} & \cdots & \mathcal{A}_{s+1,e-1}^{(0)} & \mathcal{A}_{s+1,e}^{(0)} \end{bmatrix},$$

the subcode $\mathscr{D}_0$ of $\mathscr{C}_0$ has a generator matrix $[Z^{(0)}]_s$ and the subcode $\mathscr{D}_1$ of $\mathscr{D}_0$ has a generator matrix $[Z^{(0)}]_{s-1}$, where columns of the matrices $\mathcal{G}_0$, $[Z^{(0)}]_s$ and $[Z^{(0)}]_{s-1}$ are partitioned into blocks of sizes $k_1, k_2, \ldots, k_e, k_{e+1}$, the matrix I_{k_i} is the $k_i \times k_i$ identity matrix over $\mathcal{T}_r$, $\mathcal{A}_{i,j}^{(0)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s+1$ and $i \leq j \leq e$, and each of the matrices $(\mathcal{A}^{(0)})_{s,s+2}$, $(\mathcal{A}^{(0)})_{s-1,s+3}, \ldots, (\mathcal{A}^{(0)})_{2,e-1}$, $\mathcal{A}_{1,e}^{(0)}$ are of full row-rank over $\mathcal{T}_r$.

Since $\mathscr{C}_0$ is an n_s-doubly even self-orthogonal code of length n and dimension

n_{s+1} over $\mathcal{T}_r$ with an n_s-dimensional doubly even linear subcode as $\mathscr{D}_0$, we have

$$\begin{aligned} [Z^{(0)}]_s[Z^{(0)}]_s^t &\equiv 2F + 4H \pmod 8, \\ [Z^{(0)}]_s Z_{s+1}^{(0)t} &\equiv 2P \pmod 4), \end{aligned}$$

where $F \in Alt_{n_s}(\mathcal{T}_r)$, $H \in Sym_{n_s}(\mathcal{T}_r)$ and $P \in \mathcal{M}_{n_s \times k_{s+1}}(\mathcal{T}_r)$, (note that the matrices $[Z^{(0)}]_s[Z^{(0)}]_s^t$ and $[Z^{(0)}]_s Z_{s+1}^{(0)t}$ are viewed over $\mathscr{R}_{e,r}$). Now to prove the result, let us define a matrix $\mathcal{G}_3$ over $\mathscr{R}_{3,r}$ as

$$\mathcal{G}_3 = \begin{bmatrix} Z_1^{(3)} \\ Z_2^{(3)} \\ \vdots \\ Z_s^{(3)} \\ 2Z_{s+1}^{(3)} \\ 4Z_{s+2}^{(3)} \end{bmatrix} = \begin{bmatrix} Z_1^{(0)} + 2V_1^{(1)} + 4V_1^{(2)} \\ Z_2^{(0)} + 2V_2^{(1)} + 4V_2^{(2)} \\ \vdots \\ Z_s^{(0)} + 2V_s^{(1)} + 4V_s^{(2)} \\ 2Z_{s+1}^{(3)} \\ 4Z_{s+2}^{(3)} \end{bmatrix},$$

where for $\ell \in \{1, 2\}$, the matrix $[V^{(\ell)}]_s \in \mathcal{M}_{n_s \times n}(\mathcal{T}_r)$ is of the form

$$[V^{(\ell)}]_s = \begin{bmatrix} V_1^{(\ell)} \\ V_2^{(\ell)} \\ \vdots \\ V_s^{(\ell)} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & \mathcal{A}_{1,\ell+1}^{(\ell)} & \mathcal{A}_{1,\ell+2}^{(\ell)} & \cdots & \mathcal{A}_{1,\ell+s}^{(\ell)} & \cdots & \mathcal{A}_{1,e}^{(\ell)} \\ 0 & \cdots & 0 & 0 & \mathcal{A}_{2,\ell+2}^{(\ell)} & \cdots & \mathcal{A}_{2,\ell+s}^{(\ell)} & \cdots & \mathcal{A}_{2,e}^{(\ell)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \mathcal{A}_{s,\ell+s}^{(\ell)} & \cdots & \mathcal{A}_{s,e}^{(\ell)} \end{bmatrix}$$

with $\mathcal{A}_{i,j}^{(\ell)} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s$ and $i + \ell \leq j \leq e$, the matrix $Z_{s+1}^{(3)} \in \mathcal{M}_{k_{s+1} \times n}(\mathscr{R}_{3,r})$ is of the form

$$Z_{s+1}^{(3)} = Z_{s+1}^{(0)} + 2\begin{bmatrix} 0 & \cdots & 0 & \mathcal{A}_{s+1,s+2}^{(1)} & \cdots & \mathcal{A}_{s+1,e}^{(1)} \end{bmatrix}$$

with $\mathcal{A}_{s+1,j}^{(1)} \in \mathcal{M}_{k_{s+1} \times k_{j+1}}(\mathcal{T}_r)$ for $s+2 \leq j \leq e$, and the matrix $Z_{s+2}^{(3)} \in \mathcal{M}_{k_{s+2} \times n}(\mathcal{T}_r)$ is of the form

$$Z_{s+2}^{(3)} = \begin{bmatrix} 0 & \cdots & 0 & I_{k_{s+2}} & \mathcal{A}_{s+2,s+2}^{(0)} & \cdots & \mathcal{A}_{s+2,e}^{(0)} \end{bmatrix}$$

with $\mathcal{A}_{s+2,j}^{(0)} \in \mathcal{M}_{k_{s+2} \times k_{j+1}}(\mathcal{T}_r)$ for $s + 2 \leq j \leq e$.

Now let $\mathscr{C}_3$ and $\mathscr{D}_3$ be linear codes of length n over $\mathscr{R}_{3,r}$ with generator matrices $\mathcal{G}_3$ and $[Z^{(3)}]_{s-1}$, respectively. We also note that the code $\mathscr{D}_3$ is a free linear subcode of $\mathscr{C}_3$ of rank n_{s-1}. We also observe that $Tor_1(\mathscr{D}_3) = \mathscr{D}_1$, $Tor_1(\mathscr{C}_3) = \mathscr{D}_0$ and $Tor_2(\mathscr{C}_3) = \mathscr{C}_0$ and that the code $\mathscr{C}_3$ is of the type $\{n_s, k_{s+1}, k_{s+2}\}$. Further, by Theorem 2.2.4, we observe that the code $\mathscr{C}_3$ is an n_{s-1}-doubly even self-orthogonal code over $\mathscr{R}_{3,r}$ with a free linear doubly even subcode as $\mathscr{D}_3$ if and only if there exist matrices $[V^{(1)}]_s, [V^{(2)}]_s$, $[0 \ \cdots \ 0 \ \mathcal{A}^{(1)}_{s+1,s+2} \ \cdots \ \mathcal{A}^{(1)}_{s+1,e}]$ and $Z^{(3)}_{s+2}$ satisfying the following system of matrix equations:

$$\begin{aligned} F + [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[Z^{(0)}]_s^t + 2\Big([Z^{(0)}]_s[V^{(2)}]_s^t \qquad & \\ +[V^{(2)}]_s[Z^{(0)}]_s^t + [V^{(1)}]_s[V^{(1)}]_s^t + H\Big) &\equiv 0 \pmod 4, \qquad (5.4.11) \\ \mathcal{D}iag\Big(H' + [Z^{(0)}]_{s-1}[V^{(1)}]_{s-1}^t + [V^{(1)}]_{s-1}[V^{(1)}]_{s-1}^t \qquad & \\ +2[Z^{(0)}]_{s-1}[V^{(2)}]_{s-1}^t\Big) &\equiv 0 \pmod 4, \qquad (5.4.12) \\ P + [Z^{(0)}]_s \Big[0 \ \cdots \ 0 \ \mathcal{A}^{(1)}_{s+1,s+2} \ \cdots \ \mathcal{A}^{(1)}_{s+1,e}\Big]^t &\equiv 0 \pmod 2, \qquad (5.4.13) \\ [Z^{(0)}]_s Z^{(3)t}_{s+2} &\equiv 0 \pmod 2, \qquad (5.4.14) \end{aligned}$$

where H' is an $n_{s-1} \times n_{s-1}$ matrix over $\mathcal{T}_r$ whose rows are the first n_{s-1} rows of the matrix H.

First of all, we see, by Lemma 5.4.1, that there exists a matrix $[V^{(1)}]_s \in \mathcal{M}_{n_s \times n}(\mathcal{T}_r)$ satisfying the following two matrix equations simultaneously:

$$\begin{aligned} [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[Z^{(0)}]_s^t &\equiv F \pmod 2, \qquad (5.4.15) \\ \mathcal{D}iag\Big(H + [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[V^{(1)}]_s^t\Big) &\equiv 0 \pmod 2, \qquad (5.4.16) \end{aligned}$$

and that such a matrix $[V^{(1)}]_s$ has precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=3}^{s+2} k_i n_{i-2} + n_s(n-n_{s+2}) - \frac{n_s(n_s+1)}{2}}$$

distinct choices, where $\epsilon = 1$ if $\mathbf{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even, while $\epsilon = 0$ otherwise. Next, for a given choice of the matrix $[V^{(1)}]_s$

satisfying (5.4.15) and (5.4.16), we obtain

$$\begin{aligned} [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[Z^{(0)}]_s^t + F &\equiv 2J_1 \pmod 4, && (5.4.17)\\ \mathcal{D}iag\Big(H + [Z^{(0)}]_s[V^{(1)}]_s^t + [V^{(1)}]_s[V^{(1)}]_s^t\Big) &\equiv 2J_2 \pmod 4 && (5.4.18)\end{aligned}$$

for some $J_1 \in Sym_{n_s}(\mathcal{T}_r)$ and an $n_s \times n_s$ diagonal matrix J_2 over $\mathcal{T}_r$. From this and by equations (5.4.11) and (5.4.12), we get

$$\begin{aligned} [Z^{(0)}]_s[V^{(2)}]_s^t + [V^{(2)}]_s[Z^{(0)}]_s^t &\equiv J_1 + H + [V^{(1)}]_s[V^{(1)}]_s^t \pmod 2, && (5.4.19)\\ \mathcal{D}iag\Big([Z^{(0)}]_{s-1}[V^{(2)}]_{s-1}^t\Big) &\equiv J_2' \pmod 2, && (5.4.20)\end{aligned}$$

where J_2' is an $n_{s-1} \times n_{s-1}$ diagonal matrix over $\mathcal{T}_r$ whose rows are the first n_{s-1} rows of the matrix J_2. Here we note that

$$\mathcal{D}iag(J_1 + H + [V^{(1)}]_s[V^{(1)}]_s^t) = 0 \pmod 2.$$

Now using the fact that the matrix $(\mathcal{A}^{(0)})_{s,s+2}$ is a full row-rank matrix over $\mathcal{T}_r$, we see that there exists a matrix $[V^{(2)}]_s$ satisfying equations (5.4.19) and (5.4.20) and that such a matrix $[V^{(2)}]_s$ has precisely

$$(2^r)^{\sum\limits_{i=4}^{s+2} k_i n_{i-3} + n_s(n-n_{s+2}) - \frac{n_s(n_s-1)}{2} - n_{s-1}}$$

distinct choices. Further, using the fact that the matrix $(\mathcal{A}^{(0)})_{s,s+2}$ is of full row-rank over $\mathcal{T}_r$, we see that there exists a matrix $\big[0 \ \cdots \ 0 \ \mathcal{A}^{(1)}_{s+1,s+2} \ \cdots \ \mathcal{A}^{(1)}_{s+1,e}\big]$ satisfying (5.4.13) and that such a matrix has precisely $(2^r)^{k_{s+1}(n-n_{s+2}-n_s)}$ distinct choices. Further, by applying Lemma 2.2.1 and Theorem 2.3.9 and working as in Theorem 5.4.1, we see that there exists a matrix $Z^{(3)}_{s+2}$ satisfying (5.4.14) and that such a matrix $Z^{(3)}_{s+2}$ has precisely

$$\begin{bmatrix} k_{s+2} + n - n_{s+2} - n_s \\ k_{s+2} \end{bmatrix}_{2^r}$$

relevant choices. Further, it is easy to see that each of the distinct choices of the matrices $[V^{(1)}]_s$, $[V^{(2)}]_s$, $\begin{bmatrix}0 & \cdots & 0 & \mathcal{A}^{(1)}_{s+1,s+2} & \cdots & \mathcal{A}^{(1)}_{s+1,e}\end{bmatrix}$ and $Z^{(3)}_{s+2}$ satisfying (5.4.11)-(5.4.14) gives rise to a distinct n_{s-1}-doubly self-orthogonal code $\mathscr{C}_3$ of the type $\{n_s, k_{s+1}, k_{s+2}\}$ and length n over $\mathscr{R}_{3,r}$ with a free linear doubly even subcode $\mathscr{D}_3$ satisfying $Tor_1(\mathscr{C}_3) = \mathscr{D}_0$, $Tor_2(\mathscr{C}_3) = \mathscr{C}_0$ and $Tor_1(\mathscr{D}_3) = \mathscr{D}_1$. From this, the desired result follows immediately. □

Next, let μ be a fixed integer satisfying $4 \leq \mu \leq e$, and let us define $\mu_1 = \lfloor \frac{\mu}{2} \rfloor$. In the following proposition, we consider an $n_{s-\mu_1+1}$-doubly even self-orthogonal code $\mathscr{C}_{\mu-2}$ of the type $\{n_{s-\mu_1+2}, k_{s-\mu_1+3}, \ldots, k_{s+\theta+\mu_1-1}\}$ and length n over $\mathscr{R}_{\mu-2,r}$ and a free linear doubly even subcode $\mathscr{D}_{\mu-2}$ of the code $\mathscr{C}_{\mu-2}$ of rank $n_{s-\mu_1+1}$, and we provide a method to construct an $n_{s-\mu_1}$-doubly even self-orthogonal code $\mathscr{C}_\mu$ of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ and length n over $\mathscr{R}_{\mu,r}$ satisfying $Tor_1(\mathscr{C}_\mu) = Tor_1(\mathscr{D}_{\mu-2})$ and $Tor_{i+1}(\mathscr{C}_\mu) = Tor_i(\mathscr{C}_{\mu-2})$ for $1 \leq i \leq \mu - 2$. We also count all such distinct $n_{s-\mu_1}$-doubly even self-orthogonal codes $\mathscr{C}_\mu$ of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ and length n over $\mathscr{R}_{\mu,r}$.

Proposition 5.4.3. *Let μ be a fixed integer satisfying $4 \leq \mu \leq e$, and let us define $\mu_1 = \lfloor \frac{\mu}{2} \rfloor$. Let $\mathscr{C}_{\mu-2}$ be an $n_{s-\mu_1+1}$-doubly even self-orthogonal code of the type $\{n_{s-\mu_1+2}, k_{s-\mu_1+3}, \ldots, k_{s+\theta+\mu_1-1}\}$ and length n over $\mathscr{R}_{\mu-2,r}$, and let $\mathscr{D}_{\mu-2}$ be a free linear doubly even subcode of the code $\mathscr{C}_{\mu-2}$ of rank $n_{s-\mu_1+1}$. The following hold.*

(a) There exists an $n_{s-\mu_1}$-doubly even self-orthogonal code $\mathscr{C}_\mu$ of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ and length n over $\mathscr{R}_{\mu,r}$ satisfying $Tor_1(\mathscr{C}_\mu) = Tor_1(\mathscr{D}_{\mu-2})$ and $Tor_{i+1}(\mathscr{C}_\mu) = Tor_i(\mathscr{C}_{\mu-2})$ for $1 \leq i \leq \mu - 2$.

(b) Furthermore, the pair $(\mathscr{C}_{\mu-2}, \mathscr{D}_{\mu-2})$ of codes over $\mathscr{R}_{\mu-2,r}$ gives rise to precisely

$$(2^r)^{\sum\limits_{i=\mu}^{s+\theta+\mu_1} k_i n_{i-\mu+1} + \sum\limits_{j=\mu+1}^{s+\theta+\mu_1} k_j n_{j-\mu} + (n_{s+\theta+\mu_1-1}+n_{s-\mu_1+1})(n-n_{s+\theta+\mu_1}-n_{s-\mu_1+1}) - n_{s-\mu_1} + n^2_{s-\mu_1+1}} \times \begin{bmatrix} n_{s-\mu_1+1} \\ n_{s-\mu_1} \end{bmatrix}_{2^r} \begin{bmatrix} k_{s+\theta+\mu_1} + n - n_{s+\theta+\mu_1} - n_{s-\mu_1+1} \\ k_{s+\theta+\mu_1} \end{bmatrix}_{2^r}$$

distinct $n_{s-\mu_1}$-doubly even self-orthogonal codes $\mathscr{C}_\mu$ of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ and length n over $\mathscr{R}_{\mu,r}$ satisfying $Tor_1(\mathscr{C}_\mu) = Tor_1(\mathscr{D}_{\mu-2})$ and $Tor_{i+1}(\mathscr{C}_\mu) = Tor_i(\mathscr{C}_{\mu-2})$ for $1 \leq i \leq \mu - 2$.

Proof. To prove the result, we assume, without any loss of generality, that the code $\mathscr{C}_{\mu-2}$ has a generator matrix

$$\mathcal{G}_{\mu-2} = \begin{bmatrix} Z_1^{(\mu-2)} \\ Z_2^{(\mu-2)} \\ \vdots \\ Z_{s-\mu_1+2}^{(\mu-2)} \\ 2Z_{s-\mu_1+3}^{(\mu-2)} \\ \vdots \\ 2^{\mu-3}Z_{s+\mu_1+\theta-1}^{(\mu-2)} \end{bmatrix} = \begin{bmatrix} Z_1^{(0)} + 2V_1^{(1)} + 4V_1^{(2)} + \cdots + 2^{\mu-3}V_1^{(\mu-3)} \\ Z_2^{(0)} + 2V_2^{(1)} + 4V_2^{(2)} + \cdots + 2^{\mu-3}V_2^{(\mu-3)} \\ \vdots \\ Z_{s-\mu_1+2}^{(0)} + 2V_{s-\mu_1+2}^{(1)} + 4V_{s-\mu_1+2}^{(2)} + \cdots + 2^{\mu-3}V_{s-\mu_1+2}^{(\mu-3)} \\ 2Z_{s-\mu_1+3}^{(\mu-2)} \\ \vdots \\ 2^{\mu-3}Z_{s+\mu_1+\theta-1}^{(\mu-2)} \end{bmatrix}$$

and that the free linear doubly even subcode $\mathscr{D}_{\mu-2}$ of the code $\mathscr{C}_{\mu-2}$ of rank $n_{s-\mu_1+1}$ has a generator matrix $[Z^{(\mu-2)}]_{s-\mu_1+1}$, where the matrix $[Z^{(0)}]_{s-\mu_1+2} \in \mathcal{M}_{n_{s-\mu_1+2}\times n}(\mathcal{T}_r)$ is of the form

$$[Z^{(0)}]_{s-\mu_1+2} = \begin{bmatrix} Z_1^{(0)} \\ Z_2^{(0)} \\ \vdots \\ Z_{s-\mu_1+2}^{(0)} \end{bmatrix} = \begin{bmatrix} I_{k_1} & \mathcal{A}_{1,1}^{(0)} & \cdots & \mathcal{A}_{1,s-\mu_1+1}^{(0)} & \cdots & \mathcal{A}_{1,e-1}^{(0)} & \mathcal{A}_{1,e}^{(0)} \\ 0 & I_{k_2} & \cdots & \mathcal{A}_{2,s-\mu_1+1}^{(0)} & \cdots & \mathcal{A}_{2,e-1}^{(0)} & \mathcal{A}_{2,e}^{(0)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & I_{k_{s-\mu_1+2}} & \cdots & \mathcal{A}_{s-\mu_1+2,e-1}^{(0)} & \mathcal{A}_{s-\mu_1+2,e}^{(0)} \end{bmatrix}$$

with I_{k_i} as the $k_i \times k_i$ identity matrix over $\mathcal{T}_r$ and $\mathcal{A}_{i,j}^{(0)} \in \mathcal{M}_{k_i\times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s-\mu_1+2$ and $i \leq j \leq e$, the matrix $[V^{(\ell)}]_{s-\mu_1+2} \in \mathcal{M}_{n_{s-\mu_1+2}\times n}(\mathcal{T}_r)$ for $1 \leq \ell \leq \mu-3$, and the matrix $Z_{s-\mu_1+i}^{(\mu-2)} \in \mathcal{M}_{k_{s-\mu_1+i}\times n}(\mathscr{R}_{\mu-2,r})$ is to be considered modulo $2^{\mu-i}$ for $3 \leq i \leq \mu-1$. We next see that the Torsion code $Tor_1(\mathscr{C}_{\mu-2})$ is an $n_{s-\mu_1+2}$-dimensional code over $\mathcal{T}_r$ and has a generator matrix $[Z^{(0)}]_{s-\mu_1+2}$ and that the Torsion code $Tor_1(\mathscr{D}_{\mu-2})$ has a generator matrix $[Z^{(0)}]_{s-\mu_1+1}$. Now we choose an $n_{s-\mu_1}$-dimensional subcode $\mathscr{D}$ of the code $Tor_1(\mathscr{D}_{\mu-2})$. By Theorem 2.3.9, we see that the code $\mathscr{D}$ has precisely $\begin{bmatrix} n_{s-\mu_1+1} \\ n_{s-\mu_1} \end{bmatrix}_{2^r}$ distinct choices. We assume, without any loss of generality, that the code $\mathscr{D}$ has a generator matrix $[Z^{(0)}]_{s-\mu_1}$. Furthermore, by Remark 4.3.1, we assume, without any loss of generality, that the matrix $(\mathcal{A}^{(0)})_{s-\mu_1+1,s+\theta+\mu_1}$ is of full row-rank.

Since $\mathscr{C}_{\mu-2}$ is an $n_{s-\mu_1+1}$-doubly even code over $\mathscr{R}_{\mu-2,r}$ with a free linear doubly even subcode as $\mathscr{D}_{\mu-2}$, we have

$$\begin{aligned}
[Z^{(\mu-2)}]_{s-\mu_1+1}[Z^{(\mu-2)}]^t_{s-\mu_1+1} &\equiv 0 \pmod{2^{\mu-2}},\\
\mathcal{D}iag\Big([Z^{(\mu-2)}]_{s-\mu_1+1}[Z^{(\mu-2)}]^t_{s-\mu_1+1}\Big) &\equiv 0 \pmod{2^{\mu-1}},\\
[Z^{(\mu-2)}]_{s-\mu_1+1}Z^{(\mu-2)t}_{s-\mu_1+\alpha} &\equiv 0 \pmod{2^{\mu-\alpha}} \text{ for } 2 \leq \alpha \leq \mu-1,\\
Z^{(\mu-2)}_{s-\mu_1+i}Z^{(\mu-2)t}_{s-\mu_1+j} &\equiv 0 \pmod{2^{\mu+2-i-j}} \text{ for } 2 \leq i,j \leq \mu-1\\
&\qquad \text{and } i+j \leq \mu+1,
\end{aligned}$$

which implies that

$$\begin{aligned}
[Z^{(\mu-2)}]_{s-\mu_1+1}[Z^{(\mu-2)}]^t_{s-\mu_1+1} &\equiv 2^{\mu-2}F + 2^{\mu-1}H \pmod{2^{\mu}},\\
[Z^{(\mu-2)}]_{s-\mu_1+1}Z^{(\mu-2)t}_{s-\mu_1+\alpha} &\equiv 2^{\mu-\alpha}J_\alpha \pmod{2^{\mu-\alpha+1}} \text{ for } 2 \leq \alpha \leq \mu-1,\\
Z^{(\mu-2)}_{s-\mu_1+i}Z^{(\mu-2)t}_{s-\mu_1+j} &\equiv 0 \pmod{2^{\mu+2-i-j}} \text{ for } 2 \leq i,j \leq \mu-1\\
&\qquad \text{and } i+j \leq \mu+1
\end{aligned}$$

for some $F \in Alt_{n_{s-\mu_1+1}}(\mathcal{T}_r)$, $H \in Sym_{n_{s-\mu_1+1}}(\mathcal{T}_r)$ and $J_\alpha \in \mathcal{M}_{n_{s-\mu_1+1}\times k_{s-\mu_1+\alpha}}(\mathcal{T}_r)$ for $2 \leq \alpha \leq \mu-1$. Now to prove the result, let us define a matrix $\mathcal{G}_\mu$ over $\mathscr{R}_{\mu,r}$ as

$$\mathcal{G}_\mu = \begin{bmatrix} Z_1^{(\mu)} \\ Z_2^{(\mu)} \\ \vdots \\ Z^{(\mu)}_{s-\mu_1+1} \\ 2Z^{(\mu)}_{s-\mu_1+2} \\ \vdots \\ 2^{\mu-1}Z^{(\mu)}_{s+\theta+\mu_1} \end{bmatrix} = \begin{bmatrix} Z_1^{(\mu-2)} + 2^{\mu-2}V_1^{(\mu-2)} + 2^{\mu-1}V_1^{(\mu-1)} \\ Z_2^{(\mu-2)} + 2^{\mu-2}V_2^{(\mu-2)} + 2^{\mu-1}V_2^{(\mu-1)} \\ \vdots \\ Z^{(\mu-2)}_{s-\mu_1+1} + 2^{\mu-2}V^{(\mu-2)}_{s-\mu_1+1} + 2^{\mu-1}V^{(\mu-1)}_{s-\mu_1+1} \\ 2Z^{(\mu)}_{s-\mu_1+2} \\ \vdots \\ 2^{\mu-1}Z^{(\mu)}_{s+\theta+\mu_1} \end{bmatrix}, \tag{5.4.21}$$

where the matrices $[V^{(\tau)}]_{s-\mu_1+1} \in \mathcal{M}_{n_{s-\mu_1+1}\times n}(\mathcal{T}_r)$ for $\tau \in \{\mu-2, \mu-1\}$, $Z^{(\mu)}_{s-\mu_1+\alpha} \in \mathcal{M}_{k_{s-\mu_1+\alpha}\times n}(\mathscr{R}_{\mu,r})$ for $2 \leq \alpha \leq \mu-1$ and $Z^{(\mu)}_{s+\theta+\mu_1} \in \mathcal{M}_{k_{s+\theta+\mu_1}\times n}(\mathcal{T}_r)$ are of the forms

$$\begin{bmatrix} V_1^{(\tau)} \\ V_2^{(\tau)} \\ \vdots \\ V^{(\tau)}_{s-\mu_1+1} \end{bmatrix} = \begin{bmatrix} 0 & \cdots & 0 & \mathcal{A}^{(\tau)}_{1,\tau+1} & \mathcal{A}^{(\tau)}_{1,\tau+2} & \cdots & \mathcal{A}^{(\tau)}_{1,s-\mu_1+1+\tau} & \cdots & \mathcal{A}^{(\tau)}_{1,e} \\ 0 & \cdots & 0 & 0 & \mathcal{A}^{(\tau)}_{2,\tau+2} & \cdots & \mathcal{A}^{(\tau)}_{2,s-\mu_1+1+\tau} & \cdots & \mathcal{A}^{(\tau)}_{2,e} \\ \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & \mathcal{A}^{(\tau)}_{s-\mu_1+1,s-\mu_1+1+\tau} & \cdots & \mathcal{A}^{(\tau)}_{s-\mu_1+1,e} \end{bmatrix},$$

$$Z^{(\mu)}_{s-\mu_1+\alpha} = Z^{(\mu-2)}_{s-\mu_1+\alpha} + 2^{\mu-\alpha}\Big[0 \ \ \cdots \ \ 0 \ \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \ \cdots \ \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\Big] \text{ and}$$

$$Z^{(\mu)}_{s+\theta+\mu_1} = \Big[0 \ \ \cdots \ \ 0 \ \ I_{k_{s+\theta+\mu_1}} \ \ \mathcal{A}^{(0)}_{s+\theta+\mu_1,s+\theta+\mu_1} \ \ \cdots \ \ \mathcal{A}^{(0)}_{s+\theta+\mu_1,e}\Big]$$

with $\mathcal{A}^{(\tau)}_{i,j} \in \mathcal{M}_{k_i \times k_{j+1}}(\mathcal{T}_r)$ for $1 \leq i \leq s-\mu_1+1$ and $i+\tau \leq j \leq e$, $\mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,v} \in \mathcal{M}_{k_{s-\mu_1+\alpha} \times k_{v+1}}(\mathcal{T}_r)$ for $s+\theta+\mu_1 \leq v \leq e$ and $\mathcal{A}^{(0)}_{s+\theta+\mu_1,y} \in \mathcal{M}_{k_{s+\theta+\mu_1} \times k_{y+1}}(\mathcal{T}_r)$ for $s+\theta+\mu_1 \leq y \leq e$.

Next, let $\mathscr{C}_\mu$ and $\mathscr{D}_\mu$ be linear codes of length n over $\mathscr{R}_{\mu,r}$ with generator matrices $\mathcal{G}_\mu$ and $[Z^{(\mu)}]_{s-\mu_1}$, respectively. We also note that the code $\mathscr{D}_\mu$ is a free linear subcode of $\mathscr{C}_\mu$ of rank $n_{s-\mu_1}$ and that $Tor_1(\mathscr{D}_\mu) = \mathscr{D}$. We also observe that the code $\mathscr{C}_\mu$ is of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ satisfying $Tor_1(\mathscr{C}_\mu) = Tor_1(\mathscr{D}_{\mu-2})$ and $Tor_{i+1}(\mathscr{C}_\mu) = Tor_i(\mathscr{C}_{\mu-2})$ for $1 \leq i \leq \mu-2$. Further, by Theorem 2.2.4, we observe that the code $\mathscr{C}_\mu$ is an $n_{s-\mu_1}$-doubly even self-orthogonal code over $\mathscr{R}_{\mu,r}$ with a free linear doubly even subcode as $\mathscr{D}_\mu$ if and only if there exist matrices $[V^{(\mu-2)}]_{s-\mu_1+1}$, $[V^{(\mu-1)}]_{s-\mu_1+1}$, $\Big[0\cdots 0 \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \cdots \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\Big]$ for $2 \leq \alpha \leq \mu-1$ and $Z^{(\mu)}_{s+\theta+\mu_1}$ satisfying the following system of matrix equations:

$$\begin{aligned} &F + [Z^{(0)}]_{s-\mu_1+1}[V^{(\mu-2)}]^t_{s-\mu_1+1} + [V^{(\mu-2)}]_{s-\mu_1+1}[Z^{(0)}]^t_{s-\mu_1+1} \\ &+2\Big(H + [Z^{(0)}]_{s-\mu_1+1}[V^{(\mu-1)}]^t_{s-\mu_1+1} + [V^{(\mu-1)}]_{s-\mu_1+1}[Z^{(0)}]^t_{s-\mu_1+1} \\ &\qquad +[V^{(1)}]_{s-\mu_1+1}[V^{(\mu-2)}]^t_{s-\mu_1+1} + [V^{(\mu-2)}]_{s-\mu_1+1}[V^{(1)}]^t_{s-\mu_1+1}\Big) \ \equiv \ 0 \pmod 4, \end{aligned} \tag{5.4.22}$$

$$\begin{aligned} \mathcal{D}iag\Big(H' + [Z^{(0)}]_{s-\mu_1}[V^{(\mu-2)}]^t_{s-\mu_1} + 2\Big([V^{(1)}]_{s-\mu_1}[V^{(\mu-2)}]^t_{s-\mu_1} \\ +[Z^{(0)}]_{s-\mu_1}[V^{(\mu-1)}]^t_{s-\mu_1}\Big) \ \equiv \ 0 \pmod 4, \end{aligned} \tag{5.4.23}$$

$$J_\alpha + [Z^{(0)}]_{s-\mu_1+1}\Big[0 \ \cdots \ 0 \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \cdots \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\Big]^t \ \equiv \ 0 \pmod 2, \tag{5.4.24}$$

$$[Z^{(0)}]_{s-\mu_1+1} Z^{(\mu)t}_{s+\mu_1+\theta} \ \equiv \ 0 \pmod 2, \tag{5.4.25}$$

where H' is the $n_{s-\mu_1} \times n_{s-\mu_1}$ matrix over $\mathcal{T}_r$ whose rows are the first $n_{s-\mu_1}$ rows of the matrix H. Now we will show that there exist matrices $[V^{(\mu-2)}]_{s-\mu_1+1}$, $[V^{(\mu-1)}]_{s-\mu_1+1}$, $\Big[0 \ \cdots \ 0 \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \cdots \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\Big]$ for $2 \leq \alpha \leq \mu-1$ and $Z^{(\mu)}_{s+\theta+\mu_1}$ satisfying the system (5.4.22)-(5.4.25) of matrix equations. Towards this, we first note that $\mathcal{D}iag(F) = 0$ and that the matrix $(\mathcal{A}^{(0)})_{s-\mu_1+1,s+\mu_1+\theta}$ is of full row-rank over $\mathcal{T}_r$. Now working similarly as in Proposition 5.4.2, we see that there exist matrices $[V^{(\mu-2)}]_{s-\mu_1+1}$ and $[V^{(\mu-1)}]_{s-\mu_1+1}$ satisfying (5.4.22) and (5.4.23) and that such a pair of matrices has precisely

$$(2^r)^{\sum\limits_{i=\mu}^{s+\theta+\mu_1} k_i n_{i-\mu+1} + \sum\limits_{j=\mu+1}^{s+\theta+\mu_1} k_j n_{j-\mu} + 2n_{s-\mu_1+1}(n-n_{s+\mu_1+\theta}) - n_{s-\mu_1} - n^2_{s-\mu_1+1}}$$

distinct choices. Using again the fact that the matrix $(\mathcal{A}^{(0)})_{s-\mu_1+1,s+\mu_1+\theta}$ is of full row-rank matrix over $\mathscr{R}_{\mu,r}$, one can easily observe that for $2 \leq \alpha \leq \mu - 1$, there exists a matrix $\left[0 \ \cdots \ 0 \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \cdots \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\right]$ satisfying (5.4.24) and that such a matrix has precisely

$$(2^r)^{k_{s-\mu_1+\alpha}(n-n_{s+\theta+\mu_1}-n_{s-\mu_1+1})}$$

distinct choices. Further, by Lemma 2.2.1 and Theorem 2.3.9 and working as in Theorem 5.4.1, one can show that there exists a matrix $Z^{(\mu)}_{s+\theta+\mu_1}$ satisfying (5.4.25) and that such a matrix $Z^{(\mu)}_{s+\theta+\mu_1}$ has precisely

$$\begin{bmatrix} k_{s+\theta+\mu_1} + n - n_{s+\theta+\mu_1} - n_{s-\mu_1+1} \\ k_{s+\theta+\mu_1} \end{bmatrix}_{2^r}$$

distinct choices. Further, it is easy to see that each of the distinct choices of the matrices $[V^{(\mu-2)}]_{s-\mu_1+1}$, $[V^{(\mu-1)}]_{s-\mu_1+1}$, $\left[0 \ \cdots \ 0 \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,s+\theta+\mu_1} \ \cdots \ \mathcal{A}^{(\mu-\alpha)}_{s-\mu_1+\alpha,e}\right]$ for $2 \leq \alpha \leq \mu - 1$ and $Z^{(\mu)}_{s+\theta+\mu_1}$ satisfying (5.4.22)-(5.4.25) gives rise to a distinct $n_{s-\mu_1}$-doubly even self-orthogonal code $\mathscr{C}_\mu$ of the type $\{n_{s-\mu_1+1}, k_{s-\mu_1+2}, \ldots, k_{s+\theta+\mu_1}\}$ and length n over $\mathscr{R}_{\mu,r}$ with a free linear doubly even subcode as $\mathscr{D}_\mu$ satisfying $Tor_1(\mathscr{C}_\mu) = Tor_1(\mathscr{D}_{\mu-2})$ and $Tor_{i+1}(\mathscr{C}_\mu) = Tor_i(\mathscr{C}_{\mu-2})$ for $1 \leq i \leq \mu - 2$. From this, the desired result follows immediately. □

In the following theorem, we show that there exists a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ if and only if there exists an n_s-doubly even self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$, where $\theta = 0$ when e is even, while $\theta = 1$ when e is odd. The following theorem and the proofs of Propositions 5.4.1-5.4.3 also provide a method to construct such self-orthogonal codes over $\mathscr{R}_{e,r}$ from a given n_s-doubly even self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$.

Theorem 5.4.3. *For an integer $e \geq 3$, let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s+1 \leq i \leq e$.*

(a) Let e be even. There exists a doubly even code $\mathscr{C}_0$ of length n and dimension n_s over $\mathcal{T}_r$ with an n_{s-1}-dimensional linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\boldsymbol{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd if and only if there exists a self-orthogonal code $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_s(\mathscr{C}_e) = \mathscr{C}_0$. Furthermore, each such pair $(\mathscr{C}_0, \mathscr{D}_0)$ of codes over $\mathcal{T}_r$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s-1} n_i(n-n_{i+1}-1)+\sum\limits_{j=1}^{s-1} n_{s+j}(n-n_{s+j+1}-n_{s-j})+n_s(n-n_{s+1})-\frac{n_s(n_s-1)}{2}} \\ \times \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r} \prod_{\ell=s+1}^{e} \begin{bmatrix} k_\ell + n - n_\ell - n_{e+1-\ell} \\ k_\ell \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_s(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\boldsymbol{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise.

(b) Let e be odd. There exists an n_s-doubly even self-orthogonal code $\mathscr{C}_0$ of length n and dimension n_{s+1} over $\mathcal{T}_r$ with an n_s-dimensional doubly even linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\boldsymbol{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and an n_{s-1}-dimensional linear subcode of the code $\mathscr{D}_0$ as $\mathscr{D}_1$ if and only if there exists a self-orthogonal code $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_1$, $Tor_s(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_{s+1}(\mathscr{C}_e) = \mathscr{C}_0$. Furthermore, each such triplet $(\mathscr{C}_0, \mathscr{D}_0, \mathscr{D}_1)$ of codes over $\mathcal{T}_r$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s} n_i(n-n_{i+1}-1)+\sum\limits_{j=1}^{s} n_{s+j}(n-n_{s+j+1}-n_{s+1-j})+n_s} \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r}$$

$$\times \prod_{\ell=s+2}^{e} \begin{bmatrix} k_\ell + n - n_\ell - n_{e+1-\ell} \\ k_\ell \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_1$, $Tor_s(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_{s+1}(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\boldsymbol{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise.

Proof. By applying Propositions 5.4.1-5.4.3, we get the desired result. □

Next, by Theorem 2.2.4(b), we see that a self-orthogonal code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ is self-dual if and only if $k_1 = k_{e+1} = n - (k_1 + k_2 + \cdots + k_e)$ and $k_i = k_{e-i+2}$ for $2 \le i \le e$. On taking $k_i = k_{e-i+2}$ for $1 \le i \le e$ in the above theorem, we see that there exists a self-dual code of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ if and only if there exists an n_s-doubly even self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$. Note that when e is odd, we have $\theta = 1$ and $n_{s+\theta} = \frac{n}{2}$. This implies that an n_s-doubly even self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$ is self-dual if e is odd. The following theorem and the proofs of Propositions 5.4.1-5.4.3 provide a method to construct such self-dual codes over $\mathscr{R}_{e,r}$ from a given n_s-doubly even self-orthogonal code of length n and dimension $n_{s+\theta}$ over $\mathcal{T}_r$.

Theorem 5.4.4. *For an integer $e \ge 3$, let n be a positive integer, and let $k_1, k_2, \ldots, k_{e+1}$ be non-negative integers satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$ and $k_i = k_{e-i+2}$ for $1 \le i \le e+1$.*

(a) *Let e be even. There exists a doubly even code $\mathscr{C}_0$ of length n and dimension n_s over $\mathcal{T}_r$ with an n_{s-1}-dimensional linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\boldsymbol{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd if and only if there exists a self-dual code $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_s(\mathscr{C}_e) = \mathscr{C}_0$. Furthermore, each such pair $(\mathscr{C}_0, \mathscr{D}_0)$ of codes over $\mathcal{T}_r$ gives rise to precisely*

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s-1} n_i(n-n_{i+1}-1)+\frac{n_s(n_s+1)}{2}} \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r}$$

distinct self-dual codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_s(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\boldsymbol{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even, while $\epsilon = 0$ otherwise.

(b) Let e be odd. There exists an n_s-doubly even self-dual code $\mathscr{C}_0$ of length n and dimension n_{s+1} over $\mathcal{T}_r$ with an n_s-dimensional doubly even linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\boldsymbol{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and an n_{s-1}-dimensional linear subcode of the code $\mathscr{D}_0$ as $\mathscr{D}_1$ if and only if there exists a self-dual code $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_1$, $Tor_s(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_{s+1}(\mathscr{C}_e) = \mathscr{C}_0$. Furthermore, each such triplet $(\mathscr{C}_0, \mathscr{D}_0, \mathscr{D}_1)$ of codes over $\mathcal{T}_r$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s} n_i(n-n_{i+1}-1)+n_s} \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r}$$

distinct self-dual codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ with $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_1$, $Tor_s(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_{s+1}(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\boldsymbol{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even, while $\epsilon = 0$ otherwise.

Proof. On substituting $k_i = k_{e-i+2}$ for $1 \leq i \leq e+1$ in Theorem 5.4.3, the desired result follows immediately. □

5.5 Enumeration formulae for self-orthogonal and self-dual codes over $\mathscr{R}_{e,r}$

Throughout this section, for an integer $e \geq 2$ and non-negative integers $k_1, k_2, \ldots, k_{e+1}$ satisfying $n = k_1 + k_2 + \cdots + k_{e+1}$, let us define $n_i = k_1 + k_2 + \cdots + k_i$ for $1 \leq i \leq e+1$, and let $\mathfrak{B}_e(n; k_1, k_2, \ldots, k_e)$ and $\mathcal{W}_e(n; k_1, k_2, \ldots, k_e)$ denote the number of distinct self-orthogonal and self-dual codes of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$, respectively. Further, let $\mathfrak{B}_e(n)$ and $\mathcal{W}_e(n)$ denote the number of distinct self-orthogonal and self-dual codes of length n over $\mathscr{R}_{e,r}$, respectively. In this section, we will obtain explicit values of these numbers by applying the results derived in Sections 5.3 and 5.4. For this, we will distinguish the following two cases: (i) $e = 2$ and (ii) $e \geq 3$.

In the following theorem, we consider the case $e = 2$ and obtain enumeration formulae for the numbers $\mathfrak{B}_2(n; k_1, k_2)$ and $\mathfrak{B}_2(n)$.

Theorem 5.5.1. *We have*

$$\mathfrak{B}_2(n; k_1, k_2) = \begin{cases} \mathfrak{D}_r(n; k_1) 2^{\frac{rk_1(2n-3k_1-2k_2+1)}{2}} \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{2^r} & \text{if } 2k_1 + k_2 \leq n; \\ 0 & \text{otherwise} \end{cases}$$

and

$$\mathfrak{B}_2(n) = \sum_{k_1=0}^{\lfloor \frac{n}{2} \rfloor} \mathfrak{D}_r(n; k_1) \sum_{k_2=0}^{n-2k_1} 2^{\frac{rk_1(2n-3k_1-2k_2+1)}{2}} \begin{bmatrix} n-2k_1 \\ k_2 \end{bmatrix}_{2^r},$$

where the number $\mathfrak{D}_r(n; k_1)$ is as obtained in Theorem 5.3.1.

Proof. It follows immediately from Theorems 5.3.1 and 5.4.1. □

In the following theorem, we consider the case $e = 2$ and obtain enumeration formulae for the numbers $\mathcal{W}_2(n; k_1, k_2)$ and $\mathcal{W}_2(n)$.

Theorem 5.5.2. *We have*

$$\mathcal{W}_2(n; k_1, k_2) = \begin{cases} \mathfrak{D}_r(n; k_1) 2^{\frac{rk_1(k_1+1)}{2}} & \text{if } 2k_1 + k_2 = n; \\ 0 & \text{otherwise} \end{cases}$$

and

$$\mathcal{W}_2(n) = \sum_{k_1=0}^{\lfloor \frac{n}{2} \rfloor} \mathfrak{D}_r(n; k_1) 2^{\frac{rk_1(k_1+1)}{2}},$$

where the number $\mathfrak{D}_r(n; k_1)$ is as obtained in Theorem 5.3.1.

Proof. To prove the result, we first note, by Theorem 2.2.4(b), that $\mathcal{W}_2(n; k_1, k_2) = 0$ if $2k_1 + k_2 \neq n$. Further, by Theorem 2.2.4(b) again, we see that a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ is self-dual if and only if $2k_1 + k_2 = n$. Now the desired result follows on substituting $2k_1 + k_2 = n$ in Theorem 5.5.1. □

Remark 5.5.1. *Corollaries 1 and 2 of Betty and Munemasa [12] follow, as special cases, on taking $r = 1$ in Theorems 5.5.1 and 5.5.2, respectively.*

Example 5.5.1. *By carrying out computations in the Magma Computational Algebra System, we see that there are precisely* 6 *non-zero self-orthogonal codes of length* 2, 83 *non-zero self-orthogonal codes of length* 3 *and* 1988 *non-zero self-orthogonal codes of length* 4 *over* $\mathscr{R}_{2,2}$, *which agree with Theorem 5.5.1. Besides this, we see that there is exactly one self-dual code of length* 2, 9 *self-dual codes of length* 3 *and* 165 *self-dual codes of length* 4 *over* $\mathscr{R}_{2,2}$, *which agree with Theorem 5.5.2.*

In the following theorem, we consider the case $e \geq 3$ and obtain an enumeration formula for the number $\mathfrak{B}_e(n; k_1, k_2, \ldots, k_e)$.

Theorem 5.5.3. *For an integer* $e \geq 3$, *we have the following:*

(a) When e is even, we have

$$\mathfrak{B}_e(n; k_1, k_2, \ldots, k_e) = \begin{cases} \lambda_0(n; k_1, k_2, \ldots, k_s) \prod\limits_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r} \prod\limits_{\ell=s+1}^{e} \begin{bmatrix} k_\ell + n - n_\ell - n_{e+1-\ell} \\ k_\ell \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{i=1}^{s-1} n_i(n-n_{i+1}-1) + \sum\limits_{j=1}^{s-1} n_{s+j}(n-n_{s+j+1}-n_{s-j}) + n_s(n-n_{s+1}) - \frac{n_s(n_s-1)}{2}} \\ \textit{if } n_{e-i+1} + n_i \leq n \textit{ for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise,} \end{cases}$$

where $\lambda_0(n; k_1, k_2, \ldots, k_s)$ *equals*

- $\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ k_s \end{bmatrix}_{2^r}$ *if either* $n \equiv 1, 2, 3, 5, 6, 7 \pmod 8$ *or* $n_{s-1} \neq 0$ *with* $n \equiv 4 \pmod 8$ *and r is odd;*
- $2\widehat{\sigma}_r(n; n_s) \begin{bmatrix} n_s - 1 \\ k_s \end{bmatrix}_{2^r} + \widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ k_s \end{bmatrix}_{2^r}$ *if* $n_{s-1} \neq 0$ *with either* $n \equiv 4 \pmod 8$ *and r is even or* $n \equiv 0 \pmod 8$;
- $\mathfrak{D}_r(n; n_s)$ *if* $n_{s-1} = 0$ *with* $n \equiv 0, 4 \pmod 8$.

(b) When e is odd, we have

$$\mathfrak{B}_e(n;k_1,k_2,\ldots,k_e)=\begin{cases}\lambda_1(n;k_1,k_2,\ldots,k_{s+1})\prod\limits_{\ell=s+2}^{e}\begin{bmatrix}k_\ell+n-n_\ell-n_{e+1-\ell}\\ k_\ell\end{bmatrix}_{2^r}\\ \times\prod\limits_{v=1}^{s-1}\begin{bmatrix}n_v\\ k_v\end{bmatrix}_{2^r}(2^r)^{\sum\limits_{i=1}^{s}n_i(n-n_{i+1}-1)+\sum\limits_{j=1}^{s}n_{s+j}(n-n_{s+j+1}-n_{s+1-j})+n_s}\\ \textit{if } n_{e-i+1}+n_i\leq n \textit{ for } s+1\leq i\leq e;\\ 0\qquad \textit{otherwise,}\end{cases}$$

where $\lambda_1(n;k_1,k_2,\ldots,k_{s+1})$ equals

- $\widetilde{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}\prod\limits_{i=n_s}^{n_{s+1}-1}\left(\dfrac{2^{r(n-2i-1)}-1}{2^{r(i+1-n_s)}-1}\right)$ *if $k_{s+1}\neq 0$ and $n\equiv 1,3,5,7 \pmod 8$;*
- $\widetilde{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}\left(\dfrac{2^{r(n-2n_s-k_{s+1})}-1}{2^{rk_{s+1}}-1}\right)\prod\limits_{i=n_s}^{n_{s+1}-2}\left(\dfrac{2^{r(n-2i-2)}-1}{2^{r(i+1-n_s)}-1}\right)$ *if $k_{s+1}\neq 0$ with either $n\equiv 4 \pmod 8$ and r is odd or $n\equiv 2,6 \pmod 8$;*
- $\widetilde{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}\left(\dfrac{2^{r(n-2n_s-k_{s+1})}-1}{2^{rk_{s+1}}-1}\right)\prod\limits_{i=n_s}^{n_{s+1}-2}\left(\dfrac{2^{r(n-2i-2)}-1}{2^{r(i+1-n_s)}-1}\right)$ $+2\widehat{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}\prod\limits_{i=n_s}^{n_{s+1}-1}\left(\dfrac{2^{r(n-2i)}-1}{2^{r(i+1-n_s)}-1}\right)$ *if $k_{s+1}\neq 0$ with either $n\equiv 0 \pmod 8$ or $n\equiv 4 \pmod 8$ and r is even;*
- $\widetilde{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}$ *if $k_{s+1}=0$ with either $n\equiv 1,2,3,5,6,7 \pmod 8$ or $n\equiv 4 \pmod 8$ and r is odd;*
- $2\widehat{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}+\widetilde{\sigma}_r\big(n;n_s\big)\begin{bmatrix}n_s\\ k_s\end{bmatrix}_{2^r}$ *if $k_{s+1}=0$ with either $n\equiv 0 \ (\bmod\ 8)$*

  or $n\equiv 4 \pmod 8$ and r is even.

(Here the numbers $\widehat{\sigma}_r\,(n;n_s)$ and $\widetilde{\sigma}_r\,(n;n_s)$ are as obtained in Theorems 5.3.2 and 5.3.3, respectively.)

Proof. To prove the result, we first note, by Remark 2.2.1, that $\mathfrak{B}_e(n;k_1,k_2,\ldots,k_e)=0$ if $n_{e-i+1}+n_i>n$ for some integer i satisfying $s+1\leq i\leq e$. So from now on, throughout the proof, we assume that $n_{e-i+1} + n_i \leq n$ for $s+1 \leq i \leq e$. Here, we shall distinguish the following two cases: (a) e is even, and (b) e is odd.

(a) First let e be even. Here we see, by Theorem 5.4.3(a), that each pair $(\mathscr{C}_0, \mathscr{D}_0)$ of an n_s-doubly even code $\mathscr{C}_0$ of length n and dimension n_s over $\mathcal{T}_r$ and an n_{s-1}-dimensional linear subcode $\mathscr{D}_0$ of $\mathscr{C}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s-1} n_i(n-n_{i+1}-1)+\sum\limits_{j=1}^{s-1} n_{s+j}(n-n_{s+j+1}-n_{s-j})+n_s(n-n_{s+1})-\frac{n_s(n_s-1)}{2}} \times \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r} \prod_{\ell=s+1}^{e} \begin{bmatrix} k_\ell + n - n_\ell - n_{e+1-\ell} \\ k_\ell \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_s(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\mathbf{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r even, while $\epsilon = 0$ otherwise. Now we will count the number of choices for the pair $(\mathscr{C}_0, \mathscr{D}_0)$, where $\mathscr{C}_0$ is an n_s-doubly even code of length n and dimension n_s over $\mathcal{T}_r$ and $\mathscr{D}_0$ is an n_{s-1}-dimensional linear subcode of the code $\mathscr{C}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd.

When $n_{s-1} = 0$, we see that the desired result follows by applying Theorems 5.3.1 and 5.3.3. So from this point on, we assume, throughout the proof, that $n_{s-1} \neq 0$. Here, by Theorem 5.3.2, we see that a doubly even code of length n over $\mathcal{T}_r$ contains $\mathbf{1}$ if and only if $n \equiv 0, 4 \pmod 8$.

When $n \equiv 1, 2, 3, 5, 6, 7 \pmod 8$, we see, by Theorems 2.3.9 and 5.3.3, that the pair $(\mathscr{C}_0, \mathscr{D}_0)$ has precisely

$$\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ n_{s-1} \end{bmatrix}_{2^r}$$

distinct choices.

When $n \equiv 0, 4 \pmod 8$, working as in Proposition 5.4.1 and Lemma 5.4.1, we observe that if $\mathbf{1} \in \mathscr{C}_0$, then $\mathbf{1} \in \mathscr{D}_0$, which, by Theorem 2.3.10, holds if and only if either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even.

Now when $n \equiv 4 \pmod 8$ and r is odd, we see, by Theorems 2.3.9 and 5.3.3, that the pair $(\mathscr{C}_0, \mathscr{D}_0)$ has precisely

$$\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ n_{s-1} \end{bmatrix}_{2^r}$$

distinct choices.

Finally, let us suppose that either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even. Here the following two cases arise: (i) $\mathbf{1} \notin \mathscr{C}_0$ and (ii) $\mathbf{1} \in \mathscr{C}_0$.

(i) When $\mathbf{1} \notin \mathscr{C}_0$, we note, by Theorems 2.3.9 and 5.3.3, that the pair $(\mathscr{C}_0, \mathscr{D}_0)$ has precisely

$$\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ n_{s-1} \end{bmatrix}_{2^r}$$

distinct choices.

(ii) When $\mathbf{1} \in \mathscr{C}_0$, working as in Proposition 5.4.1 and Lemma 5.4.1, we observe that $\mathbf{1} \in \mathscr{D}_0$. This, by Theorems 2.3.9 and 5.3.2, implies that the pair $(\mathscr{C}_0, \mathscr{D}_0)$ has precisely

$$\widehat{\sigma}_r(n; n_s) \begin{bmatrix} n_s - 1 \\ n_{s-1} - 1 \end{bmatrix}_{2^r}$$

distinct choices.

From this, we get the desired result.

(b) Next, let e be odd. Here we see, by Theorem 5.4.3(b), that each triplet $(\mathscr{C}_0, \mathscr{D}_0, \mathscr{D}_1)$ of an n_s-doubly even self-orthogonal code $\mathscr{C}_0$ of length n and dimension n_{s+1} over $\mathcal{T}_r$ with an n_s-dimensional doubly even linear subcode as $\mathscr{D}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and an n_{s-1}-dimensional linear subcode of the code $\mathscr{D}_0$ as $\mathscr{D}_1$ gives rise to precisely

$$2^{\epsilon}(2^r)^{\sum\limits_{i=1}^{s} n_i(n-n_{i+1}-1)+\sum\limits_{j=1}^{s} n_{s+j}(n-n_{s+j+1}-n_{s+1-j})+n_s} \prod_{v=1}^{s-1} \begin{bmatrix} n_v \\ k_v \end{bmatrix}_{2^r}$$

$$\times \prod_{\ell=s+2}^{e} \begin{bmatrix} k_\ell + n - n_\ell - n_{e+1-\ell} \\ k_\ell \end{bmatrix}_{2^r}$$

distinct self-orthogonal codes $\mathscr{C}_e$ of the type $\{k_1, k_2, \ldots, k_e\}$ and length n over $\mathscr{R}_{e,r}$ satisfying $Tor_{s-1}(\mathscr{C}_e) = \mathscr{D}_1$, $Tor_s(\mathscr{C}_e) = \mathscr{D}_0$ and $Tor_{s+1}(\mathscr{C}_e) = \mathscr{C}_0$, where $\epsilon = 1$ if $\mathbf{1} \in \mathscr{D}_0$ with either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even, while $\epsilon = 0$ otherwise. We will now count the number of choices for the triplet $(\mathscr{C}_0, \mathscr{D}_0, \mathscr{D}_1)$, where $\mathscr{C}_0$ is an n_s-doubly even self-orthogonal code of length n and dimension n_{s+1} over $\mathcal{T}_r$, $\mathscr{D}_0$ is an n_s-dimensional doubly even linear subcode of the code $\mathscr{C}_0$ satisfying the additional property that $\mathbf{1} \notin \mathscr{D}_0$ when $n \equiv 4 \pmod 8$ and r is odd, and $\mathscr{D}_1$ is an n_{s-1}-dimensional linear subcode of the code $\mathscr{D}_0$.

For this, we see, by Theorem 5.3.2 and by applying Theorem 2.3.10, that $\mathbf{1} \in \mathscr{D}_0$ if and only if either $n \equiv 0 \pmod 8$ or $n \equiv 4 \pmod 8$ and r is even. When $k_{s+1} = 0$, we see, by Theorems 2.3.9, 5.3.2 and 5.3.3, that the desired result follows immediately. So from this point on, we assume, throughout the proof, that $k_{s+1} \neq 0$. Here we recall that any self-orthogonal code over $\mathcal{T}_r$ is contained in $\mathcal{I}(\mathcal{V}_r) = \{v \in \mathcal{V}_r : \mathcal{B}_r(v,v) = 0\}$. We next note that $\mathbf{1} \in \mathcal{I}(\mathcal{V}_r)$ if and only if n is even. Accordingly, we will distinguish two cases: (i) n is odd, and (ii) n is even.

(i) First of all, let n be odd. In this case, we see that the pair $(\mathscr{D}_0, \mathscr{D}_1)$ has precisely

$$\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ k_s \end{bmatrix}_{2^r}$$

distinct choices. Further, for a given choice of $(\mathscr{D}_0, \mathscr{D}_1)$, we see that the number of choices for $\mathscr{C}_0$ is equal to the number of choices for a k_{s+1}-dimensional self-orthogonal $\mathcal{T}_r$-linear subspace U of $\mathcal{I}(\mathcal{V}_r)$ satisfying $U \subseteq (\mathscr{D}_0)^{\perp_{\mathcal{B}_r}} \setminus \mathscr{D}_0$. Further, since $(\mathcal{I}(\mathcal{V}_r), \mathcal{B}_r\restriction_{\mathcal{I}(\mathcal{V}_r)\times\mathcal{I}(\mathcal{V}_r)})$ is an $(n-1)$-dimensional symplectic space over $\mathcal{T}_r$, we see, by Theorem 2.3.3(e), that such a subspace U of $\mathcal{I}(\mathcal{V}_r)$ has precisely

$$\prod_{i=n_s}^{n_{s+1}-1} \left(\frac{2^{r(n-2i-1)} - 1}{2^{r(i+1-n_s)} - 1} \right)$$

distinct choices.

(ii) Next, let n be even. In this case, we see that $\mathbf{1} \in \mathcal{I}(\mathcal{V}_r)$. Here we choose an $(n-2)$-dimensional $\mathcal{T}_r$-linear subspace $\mathcal{V}_r'$ of $\mathcal{I}(\mathcal{V}_r)$ such that $\mathbf{1} \notin \mathcal{V}_r'$. This gives $\mathcal{I}(\mathcal{V}_r) = \mathcal{V}_r' \perp \langle \mathbf{1} \rangle$. It is easy to observe that $(\mathcal{V}_r', \mathcal{B}_r\restriction_{\mathcal{V}_r' \times \mathcal{V}_r'})$ is an $(n-2)$-dimensional symplectic space over $\mathcal{T}_r$. When either $n \equiv 2, 6 \pmod{8}$ or $n \equiv 4 \pmod{8}$ and r is odd, we see that the pair $(\mathscr{D}_0, \mathscr{D}_1)$ has precisely

$$\widetilde{\sigma}_r(n; n_s) \begin{bmatrix} n_s \\ k_s \end{bmatrix}_{2^r}$$

distinct choices. Now for a given choice of $(\mathscr{D}_0, \mathscr{D}_1)$, we see that the number of choices for $\mathscr{C}_0$ is equal to the number of choices for a k_{s+1}-dimensional self-orthogonal $\mathcal{T}_r$-linear subspace U of $\mathcal{I}(\mathcal{V}_r)$ satisfying $U \subseteq (\mathscr{D}_0)^{\perp_{\mathcal{B}_r}} \setminus \mathscr{D}_0$. We further observe that any such k_{s+1}-dimensional $\mathcal{T}_r$-linear subspace of $\mathcal{I}(\mathcal{V}_r)$ is either of the form $U = \langle u_1, u_2, \ldots, u_{k_{s+1}} \rangle$ or of the form $U = \langle u_1, u_2, \ldots, u_{k_{s+1}-1}, \mathbf{1} \rangle$, where $u_1, u_2, \ldots, u_{k_{s+1}}$ are mutually orthogonal and linearly independent vectors in $\mathcal{V}_r'$. Now by Theorem 2.3.3 (e), we see that such a subspace U of $\mathcal{I}(\mathcal{V}_r)$ has precisely

$$\prod_{i=n_s}^{n_{s+1}-2} \left(\frac{2^{r(n-2i-2)} - 1}{2^{r(i+1-n_s)} - 1} \right) \left(\frac{2^{r(n-2n_s-k_{s+1})} - 1}{2^{rk_{s+1}} - 1} \right)$$

distinct choices. On the other hand, when either $n \equiv 0 \pmod{8}$ or $n \equiv 4 \pmod{8}$ and r is even, working similarly as above, we get the desired result.

□

In the following theorem, we consider the case $e \geq 3$ and obtain the explicit enumeration formula for the number $\mathcal{W}_e(n; k_1, k_2, \ldots, k_e)$.

Theorem 5.5.4. *For an integer $e \geq 3$, we have the following:*

(a) When e is even, we have

$$\mathcal{W}_e(n;k_1,k_2,\ldots,k_e)=\begin{cases}\lambda_0(n;k_1,k_2,\ldots,k_s)(2^r)^{\sum\limits_{i=1}^{s-1}n_i(n-n_{i+1}-1)+\frac{n_s(n_s+1)}{2}}\prod\limits_{j=1}^{s-1}{\begin{bmatrix}n_j\\k_j\end{bmatrix}}_{2^r}\\ \textit{if } k_v=k_{e-v+2} \textit{ for } 1\leq v\leq e+1;\\ 0 \quad \textit{otherwise,}\end{cases}$$

where the number $\lambda_0(n;k_1,k_2,\ldots,k_s)$ is as obtained in Theorem 5.5.3(a).

(b) When e is odd, we have

$$\mathcal{W}_e(n;k_1,k_2,\ldots,k_e)=\begin{cases}\lambda_1(n;k_1,k_2,\ldots,k_{s+1})(2^r)^{\sum\limits_{i=1}^{s}n_i(n-n_{i+1}-1)+n_s}\prod\limits_{j=1}^{s-1}{\begin{bmatrix}n_j\\k_j\end{bmatrix}}_{2^r}\\ \textit{if } n \textit{ is even and } k_v=k_{e-v+2} \textit{ for } 1\leq v\leq e+1;\\ 0 \quad \textit{otherwise,}\end{cases}$$

where the number $\lambda_1(n;k_1,k_2,\ldots,k_{s+1})$ is as obtained in Theorem 5.5.3(b).

Proof. To prove the result, we first note, by Theorem 2.2.4(b), that $\mathcal{W}_e(n;k_1,k_2,\ldots,k_e)=0$ if $k_v\neq k_{e-v+2}$ for some integer v satisfying $1\leq v\leq e+1$. Further, by Theorem 2.2.4(b) again, we see that a self-orthogonal code of the type $\{k_1,k_2,\ldots,k_e\}$ and length n over $\mathscr{R}_{e,r}$ is self-dual if and only if $k_i=k_{e-i+2}$ for $1\leq i\leq e+1$. Now the desired result follows on substituting $k_i=k_{e-i+2}$ for $1\leq i\leq e+1$ in Theorem 5.5.3. □

Remark 5.5.2. *Theorems 4.1 and 4.2 of Nagata et al. [75] follow, as special cases, on taking $r=1$ and $e\geq 4$ in the above theorem.*

We now proceed to determine enumeration formulae for the numbers $\mathfrak{B}_e(n)$ and $\mathcal{W}_e(n)$ for each integer $e\geq 3$. To do this, for an integer d satisfying $1\leq d\leq e$ and for non-negative integers $k_1,k_2,\ldots,k_d$, let $h_j(k_1,k_2,\ldots,k_d)$ and $m_\ell(k_1,k_2,\ldots,k_d)$ be as defined by (3.4.19) and (3.4.20), respectively, for $1\leq j\leq d-1$ and $1\leq \ell\leq \lceil\frac{d}{2}\rceil-1$.

In the following theorem, we obtain an enumeration formula for the number $\mathfrak{B}_e(n)$ when $e\geq 3$.

Theorem 5.5.5. *For an integer $e\geq 3$, the following hold.*

(a) When e is even, we have

$$\mathfrak{B}_e(n) = \sum \lambda_0(n; k_1, k_2, \ldots, k_s)(2^r)^{\Lambda(k_1,k_2,\ldots,k_e)} \prod_{j=1}^{s-1} \begin{bmatrix} k_1 + k_2 + \cdots + k_j \\ k_j \end{bmatrix}_{2^r}$$
$$\times \prod_{\ell=s+1}^{e} \begin{bmatrix} k_\ell + n - (k_1 + k_2 + \cdots + k_\ell) - (k_1 + k_2 + \cdots + k_{e+1-\ell}) \\ k_\ell \end{bmatrix}_{2^r},$$

where the summation $\sum$ runs over all non-negative integers $k_1, k_2, \ldots, k_e$ satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s+1 \leq i \leq e$ and the number $\Lambda(k_1, k_2, \ldots, k_e)$ is given by

$$\begin{aligned} \Lambda(k_1, k_2, \ldots, k_e) &= \sum_{i=1}^{s} m_i(k_1, k_2, \ldots, k_e) + k_1 + k_2 + \cdots + k_s \\ &\quad -(k_1 + k_2 + \cdots + k_s)\left(\frac{k_1 + k_2 + \cdots + k_s - 1}{2}\right). \end{aligned}$$

(b) When e is odd, we have

$$\mathfrak{B}_e(n) = \sum \lambda_1(n; k_1, k_2, \ldots, k_{s+1})(2^r)^{\Lambda'(k_1,k_2,\ldots,k_e)} \prod_{j=1}^{s-1} \begin{bmatrix} k_1 + k_2 + \cdots + k_j \\ k_j \end{bmatrix}_{2^r}$$
$$\times \prod_{\ell=s+2}^{e} \begin{bmatrix} k_\ell + n - (k_1 + k_2 + \cdots + k_\ell) - (k_1 + k_2 + \cdots + k_{e+1-\ell}) \\ k_\ell \end{bmatrix}_{2^r},$$

where the summation $\sum$ runs over all non-negative integers $k_1, k_2, \ldots, k_e$ satisfying $2k_1 + 2k_2 + \cdots + 2k_{e-i+1} + k_{e-i+2} + k_{e-i+3} + \cdots + k_i \leq n$ for $s+1 \leq i \leq e$ and the number $\Lambda'(k_1, k_2, \ldots, k_e)$ is given by

$$\Lambda'(k_1, k_2, \ldots, k_e) = \sum_{i=1}^{s} m_i(k_1, k_2, \ldots, k_e) + (k_1 + k_2 + \cdots + k_s).$$

(Here the numbers $\lambda_0(n; k_1, k_2, \ldots, k_s)$ and $\lambda_1(n; k_1, k_2, \ldots, k_{s+1})$ are as obtained in Theorem 5.5.3.)

Proof. It follows immediately from Theorem 5.5.3. □

In the following theorem, we obtain explicit enumeration formula for the number

$\mathcal{W}_e(n)$ when $e \geq 3$.

Theorem 5.5.6. *For an integer $e \geq 3$, the following hold.*

(a) When e is even, we have

$$\begin{aligned}\mathcal{W}_e(n) &= \sum \lambda_0(n; k_1, k_2, \ldots, k_s) \prod_{j=1}^{s-1} \begin{bmatrix} k_1 + k_2 + \cdots + k_j \\ k_j \end{bmatrix}_{2^r} \\ &\quad \times (2^r)^{\sum\limits_{i=1}^{s-1} h_i(k_1,k_2,\ldots,k_{s+1}) + (k_1+k_2+\cdots+k_s)\left(\frac{k_1+k_2+\cdots+k_s+1}{2}\right)},\end{aligned}$$

where the summation $\sum$ runs over all non-negative integers $k_1, k_2, \ldots, k_{s+1}$ satisfying $2(k_1 + k_2 + \cdots + k_s) + k_{s+1} = n$.

(b) When e is odd, we have

$$\mathcal{W}_e(n) = \begin{cases} \sum \lambda_1(n; k_1, k_2, \ldots, k_{s+1}) \prod\limits_{j=1}^{s-1} \begin{bmatrix} k_1 + k_2 + \cdots + k_j \\ k_j \end{bmatrix}_{2^r} & \\ \times (2^r)^{\sum\limits_{i=1}^{s} h_i(k_1,k_2,\ldots,k_{s+1}) + k_1 + k_2 + \cdots + k_s} & \textit{if } n \textit{ is even;} \\ 0 \quad \textit{otherwise,} & \end{cases}$$

where the summation $\sum$ runs over all non-negative integers $k_1, k_2, \ldots, k_{s+1}$ satisfying $2(k_1 + k_2 + \cdots + k_{s+1}) = n$.

(Here the numbers $\lambda_0(n; k_1, k_2, \ldots, k_s)$ and $\lambda_1(n; k_1, k_2, \ldots, k_{s+1})$ are as obtained in Theorem 5.5.3.)

Proof. It follows immediately from Theorem 5.5.4. □

Remark 5.5.3. *Theorem 4.1 of Nagata et al. [76] follow, as a special case, on taking $r = 1$ and $e = 3$ in the above theorem.*

Example 5.5.2. *Let $e = 3$ and $r = 2$. By carrying out computations in the Magma Computational Algebra System, we see that there are precisely 11 non-zero self-orthogonal codes of length* 2, 388 *non-zero self-orthogonal codes of length* 3 *and* 41998 *non-zero self-orthogonal codes of length* 4 *over $\mathscr{R}_{3,2}$, which agree with Theorem 5.5.5. We also see that there is exactly one self-dual code of length* 2 *and* 1317 *self-dual* *codes of length* 4 *over* $\mathscr{R}_{3,2}$ *and that there does not exist any self-dual code of length* 3 *over* $\mathscr{R}_{3,2}$*, which agree with Theorem 5.5.6(b).*

The above enumeration formulae for self-orthogonal and self-dual codes over $\mathscr{R}_{e,r}$ are useful in classifying these two classes of codes up to monomial equivalence. We illustrate this by classifying self-orthogonal and self-dual codes of lengths $2, 3$ and 4 over the Galois ring $\mathscr{R}_{2,2} = GR(2^2, 2)$ in the following section.

5.6 Classification of self-orthogonal and self-dual codes

With the help of the enumeration formulae for self-orthogonal and self-dual codes of length n over $\mathscr{R}_{e,r}$ (obtained in Section 5.5) and by applying the classification algorithm [53, Sec. 9.6 and 9.7], one can obtain complete lists of monomially inequivalent self-orthogonal and self-dual codes of length n over $\mathscr{R}_{e,r}$. We will now illustrate this in certain specific cases by carrying out computations in the Magma Computational Algebra System. For this, we first note, by Example 5.5.1, that there are precisely 6 non-zero self-orthogonal codes of length 2, 83 non-zero self-orthogonal codes of length 3 and 1988 non-zero self-orthogonal codes of length 4 over $\mathscr{R}_{2,2}$ and that there is only 1 self-dual code of length 2 over $\mathscr{R}_{2,2}$, while there are precisely 9 self-dual codes of length 3 and 165 self-dual codes of length 4 over $\mathscr{R}_{2,2}$. In this section, we will obtain all inequivalent codes belonging to these classes of codes. To do this, we see that there exists $\zeta \in \mathscr{R}_{2,2}$ satisfying $\zeta^2 + \zeta + 1 = 0$. Now the following hold.

I. There are precisely 3 inequivalent non-zero self-orthogonal codes of length 2 over $\mathscr{R}_{2,2}$. Among these codes, there are

- 2 self-orthogonal codes of Hamming distance 1 and with generator matrices $\begin{bmatrix} 2 & 0 \end{bmatrix}$ and $2I_2$; and
- 1 self-orthogonal code of Hamming distance 2 and with a generator matrix $\begin{bmatrix} 2 & 2+2\zeta \end{bmatrix}$.

II. There are precisely 9 inequivalent non-zero self-orthogonal codes of length 3 over $\mathscr{R}_{2,2}$. Among these codes, there are

- 4 self-orthogonal codes of Hamming distance 1 and with generator matrices $2I_3$, $\begin{bmatrix}2 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0\\ 0 & 2 & 2\end{bmatrix}$ and $\begin{bmatrix}2 & 0 & 0\\ 0 & 2 & 0\end{bmatrix}$;
- 3 self-orthogonal codes of Hamming distance 2 and with generator matrices $\begin{bmatrix}2 & 0 & 2\end{bmatrix}$, $\begin{bmatrix}1 & \zeta & 1+3\zeta\\ 0 & 2 & 2+2\zeta\end{bmatrix}$ and $\begin{bmatrix}2 & 0 & 2\\ 0 & 2 & 2+2\zeta\end{bmatrix}$; and
- 2 self-orthogonal codes of Hamming distance 3 and with generator matrices $\begin{bmatrix}1 & 3+\zeta & 2+3\zeta\end{bmatrix}$ and $\begin{bmatrix}2 & 2+2\zeta & 2+2\zeta\end{bmatrix}$.

III. There are precisely 28 inequivalent non-zero self-orthogonal codes of length 4 over $\mathscr{R}_{2,2}$. Among these codes, there are

- 10 self-orthogonal codes of Hamming distance 1 and with generator matrices $2I_4$, $\begin{bmatrix}2 & 0 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 2 & 2+2\zeta\\ 0 & 2 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 2 & 1+\zeta & \zeta\\ 0 & 2 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 2+2\zeta & 0\\ 0 & 2 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 2\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 2\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 0\\ 0 & 0 & 2 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 0\\ 0 & 2 & 0 & 2+2\zeta\\ 0 & 0 & 2 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 2+3\zeta & 2\zeta & 1+3\zeta\\ 0 & 2 & 0 & 2+2\zeta\\ 0 & 0 & 2 & 0\end{bmatrix}$;
- 9 self-orthogonal codes of Hamming distance 2 and with generator matrices $\begin{bmatrix}2 & 2\zeta & 0 & 0\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 2 & 0\\ 0 & 2 & 2 & 2+2\zeta\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 2\\ 0 & 2 & 0 & 2\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 2\zeta\\ 0 & 2 & 2\zeta & 0\end{bmatrix}$, $\begin{bmatrix}1 & \zeta & 3+\zeta & 2\\ 0 & 2 & 2+2\zeta & 0\end{bmatrix}$, $\begin{bmatrix}1 & 3+2\zeta & 3 & 1+2\zeta\\ 0 & 2 & 2 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1+3\zeta & 0 & 2+\zeta\\ 0 & 2 & 0 & 2\zeta\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 0 & 2\zeta\\ 0 & 2 & 0 & 2+2\zeta\\ 0 & 0 & 2 & 2\zeta\end{bmatrix}$ and $\begin{bmatrix}1 & 1 & 1+2\zeta & 3\\ 0 & 2 & 0 & 2\\ 0 & 0 & 2 & 2\end{bmatrix}$;
- 7 self-orthogonal codes of Hamming distance 3 and with generator matrices $\begin{bmatrix}1 & 1+\zeta & 0 & 2+\zeta\end{bmatrix}$, $\begin{bmatrix}2 & 2\zeta & 0 & 2\zeta\end{bmatrix}$, $\begin{bmatrix}1 & 2\zeta & 3+\zeta & 2+3\zeta\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta & 1+3\zeta\\ 0 & 1 & 3+3\zeta & 2+\zeta\end{bmatrix}$, $\begin{bmatrix}1 & 1 & 1+2\zeta & 1\\ 0 & 2 & 2\zeta & 2+2\zeta\end{bmatrix}$, $\begin{bmatrix}2 & 0 & 2\zeta & 2\zeta\\ 0 & 2 & 2 & 2+2\zeta\end{bmatrix}$

and $\begin{bmatrix} 1 & 0 & 3+3\zeta & 2+3\zeta \\ 0 & 2 & 2 & 2\zeta \end{bmatrix}$; and

- 2 self-orthogonal codes of Hamming distance 4 and with generator matrices $\begin{bmatrix} 1 & 1 & 3+2\zeta & 1+2\zeta \end{bmatrix}$ and $\begin{bmatrix} 2 & 2+2\zeta & 2+2\zeta & 2+2\zeta \end{bmatrix}$.

IV. By Theorem 2.2.4(b), we see that a self-orthogonal code of the type $\{k_1, k_2\}$ and length n over $\mathscr{R}_{2,r}$ is self-dual if and only if $2k_1 + k_2 = n$. From this, it follows that

- there is exactly one inequivalent self-dual code of length 2 and Hamming distance 1 over $\mathscr{R}_{2,2}$.
- there is exactly one inequivalent self-dual code of length 3 and Hamming distance 1 and one inequivalent self-dual code of length 3 and Hamming distance 2 over $\mathscr{R}_{2,2}$.
- there are 2 inequivalent self-dual codes of length 4 and Hamming distance 1, one inequivalent self-dual code of length 4 and Hamming distance 2 and one inequivalent self-dual code of length 4 and Hamming distance 3 over $\mathscr{R}_{2,2}$.

Note that Theorems 5.5.1, 5.5.2, 5.5.5 and 5.5.6 together with Theorems 3.2.3,3.2.5, 3.3.3, 3.3.5, 3.4.5 and 3.4.6 provide enumeration formulae for all self-orthogonal and self-dual codes over Galois rings. Thus the problem of determination of enumeration formulae for self-orthogonal and self-dual codes over Galois rings is now completely solved. In the next chapter, we will study and enumerate LCD codes over finite commutative chain rings.

6

On σ-LCD codes over finite commutative chain rings

6.1 Introduction

Recall that $\mathcal{R}_{e,r}$ is a finite commutative chain ring with the maximal ideal $\langle u\rangle$ of nilpotency index $e \geq 2$ and the residue field $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u\rangle$ of order p^r, where p is a prime and r is a positive integer. The set $\mathcal{T}_{e,r} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is the Teichm$\ddot{u}$ller set of the chain ring $\mathcal{R}_{e,r}$.

Now let F be a mapping from $\mathcal{R}_{e,r}^n$ into itself satisfying the following three conditions:

(1) $F(a+b) = F(a) + F(b)$ for all $a, b \in \mathcal{R}_{e,r}^n$.

(2) $d_H(F(a), F(b)) = d_H(a, b)$ for all $a, b \in \mathcal{R}_{e,r}^n$.

(3) If C is a linear code of length n over $\mathcal{R}_{e,r}$, then $F(C)$ is also a linear code of

the same length n over $\mathcal{R}_{e,r}$.

For a mapping $F : \mathcal{R}_{e,r}^n \to \mathcal{R}_{e,r}^n$ satisfying conditions (1)-(3), the F-inner product on $\mathcal{R}_{e,r}^n$ is defined as

$$[a,b]_F = a \cdot F(b) = \sum_{i=1}^{n} a_i c_i \text{ for all } a, b \in \mathcal{R}_{e,r}^n,$$

where $a = (a_1, a_2, \ldots, a_n)$ and $F(b) = (c_1, c_2, \ldots, c_n)$. The F-dual code of a linear code C of length n over $\mathcal{R}_{e,r}$ is defined as

$$C^{\perp_F} = \{a \in \mathcal{R}_{e,r}^n \ : \ [a,b]_F = 0 \text{ for all } b \in C\}.$$

The code C is said to be F-LCD if it satisfies $C \cap C^{\perp_F} = \{0\}$. The F-LCD codes of length n over $\mathcal{R}_{e,r}$ are recently introduced and studied by Liu and Liu [66]. One can easily observe that each automorphism σ_0 of $\mathcal{R}_{e,r}$ can be naturally extended to an automorphism σ of $\mathcal{R}_{e,r}^n$, defined as

$$\sigma(a) = (\sigma_0(a_1), \sigma_0(a_2), \ldots, \sigma_0(a_n)) \text{ for all } \quad a = (a_1, a_2, \ldots, a_n) \in \mathcal{R}_{e,r}^n. \qquad (6.1.1)$$

Note that the map σ satisfies conditions (1)-(3).

From now on, throughout this chapter, let σ_0 be an automorphism of $\mathcal{R}_{e,r}$, and let $\overline{\sigma}_0$ be the corresponding automorphism of the residue field $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u \rangle$ of $\mathcal{R}_{e,r}$, defined as

$$\overline{\sigma}_0(\overline{a}) = \sigma_0(a) + \langle u \rangle = \overline{\sigma_0(a)}$$

for all $\overline{a} = a + \langle u \rangle \in \overline{\mathcal{R}}_{e,r}$. Corresponding to the automorphism σ_0 of $\mathcal{R}_{e,r}$, let σ be the automorphism of $\mathcal{R}_{e,r}^n$ as defined by (6.1.1). Now the σ-inner product on $\mathcal{R}_{e,r}^n$ is a map $[\cdot,\cdot]_\sigma : \mathcal{R}_{e,r}^n \times \mathcal{R}_{e,r}^n \to \mathcal{R}_{e,r}$, defined as

$$[a,b]_\sigma = a \cdot \sigma(b) = a_1\sigma_0(b_1) + a_2\sigma_0(b_2) + \cdots + a_n\sigma_0(b_n)$$

for all $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n) \in \mathcal{R}_{e,r}^n$. Note that the σ-inner product $[\cdot,\cdot]_\sigma$ is a non-degenerate σ-sesquilinear form on $\mathcal{R}_{e,r}^n$. Further, if C is a linear code of length n over $\mathcal{R}_{e,r}$, then the σ-dual code of C is defined as

$$C^{\perp_\sigma} = \{v \in \mathcal{R}_{e,r}^n \ : \ [v, c]_\sigma = 0 \text{ for all } c \in C\}.$$

Note that the σ-dual code $C^{\perp_\sigma}$ of the code C coincides with the (Euclidean) dual code $C^\perp$ of the code C when σ_0 is the identity automorphism of $\mathcal{R}_{e,r}$. The code C is said to be a linear code with complementary σ-dual (or a σ-LCD code) if it satisfies $C \cap C^{\perp_\sigma} = \{0\}$. In particular, when σ_0 is the identity automorphism of $\mathcal{R}_{e,r}$, σ-LCD codes are called Euclidean LCD codes (or simply called LCD codes). When $\mathcal{R}_{e,r}$ is a finite field, the σ-inner product on $\mathcal{R}_{e,r}^n$ is called the Galois inner product, which was introduced and studied by Fan and Zhang [42] as a generalization of Euclidean and Hermitian forms over finite fields. When $\mathcal{R}_{e,r}$ is the finite field of order q^2 and σ_0 is the automorphism of $\mathcal{R}_{e,r}(\simeq \mathbb{F}_{q^2})$ of order 2, the σ-inner product matches with the Hermitian form, and hence σ-LCD codes are called Hermitian LCD codes.

The main goal of this chapter is to obtain the explicit enumeration formula for all σ-LCD codes of an arbitrary length n over the chain ring $\mathcal{R}_{e,r}$ when $\overline{\sigma}_0^2$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$. Note that Corollaries 2.1.1 and 2.1.2 characterize all automorphisms σ_0 of $\mathcal{R}_{e,r}$ (and hence all the corresponding automorphisms σ of $\mathcal{R}_{e,r}^n$) for which $\overline{\sigma}_0^2$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$. Besides this, we will show that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good and that every free linear $[n, k, d]$-code over $\mathcal{R}_{e,r}$ is equivalent to a σ-LCD $[n, k, d]$-code over $\mathcal{R}_{e,r}$ when $|\overline{\mathcal{R}}_{e,r}| > 4$. We will also explicitly determine all inequivalent σ-LCD $[n, 1, d]$-codes and $[n, n-1, d]$-codes over $\mathcal{R}_{e,r}$ for $1 \leq d \leq n$.

This chapter is organized as follows: In Section 6.2, we state some basic results needed to derive our main results. In Section 6.3, we first enumerate all k-dimensional Euclidean and Hermitian LCD codes of length n over $\mathbb{F}_q$ by applying the Witt decomposition theory, where q is a prime power (see Theorems 6.3.2, 6.3.3 and 6.3.6). It is worth mentioning that Carlet *et al.* [27, Sec. IV and V] also recently enumerated all k-dimensional Euclidean LCD codes of length n over $\mathbb{F}_q$ when either $q = 2$ or q is an odd prime power, and Liu and Wang [69] later counted all Euclidean and Hermitian LCD codes over $\mathbb{F}_q$ by using cogredience theories of matrices. However, our proof technique to enumerate all k-dimensional Euclidean and Hermitian LCD codes over $\mathbb{F}_q$ is quite different from the ones employed by Carlet *et al.* [27, Sec.

IV and V] and Liu and Wang [69]. Further, with the help of the enumeration formulae for Euclidean and Hermitian LCD codes over $\mathbb{F}_q$, we obtain explicit enumeration formulae for all σ-LCD codes of an arbitrary length over $\mathcal{R}_{e,r}$ when $\overline{\sigma}_0^2$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$ (Theorems 6.3.5 and 6.3.8). In Section 6.4, we show that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good (Theorem 6.4.1). In Section 6.5, we show that every free linear $[n,k,d]$-code over $\mathcal{R}_{e,r}$ is equivalent to a σ-LCD $[n,k,d]$-code over $\mathcal{R}_{e,r}$ when $|\overline{\mathcal{R}}_{e,r}| > 4$ (Theorem 6.5.1). Besides this, we explicitly determine all inequivalent σ-LCD $[n,1,d]$-codes and $[n,n-1,d]$-codes over $\mathcal{R}_{e,r}$ for $1 \leq d \leq n$ (Theorems 6.5.2 and 6.5.3). With the help of the enumeration formulae obtained in Section 6.3 and by applying the classification algorithm, we classify all Euclidean LCD codes of lengths $2,3,4$ and 5 over the chain ring $\mathbb{F}_2[u]/\langle u^2\rangle$ and of lengths $2,3$ and 4 over the chain ring $\mathbb{F}_3[u]/\langle u^2\rangle$, and all σ-LCD codes of lengths $2,3$ and 4 over the chain ring $\mathbb{F}_4[u]/\langle u^2\rangle$, where σ_0 is an automorphism of $\mathbb{F}_4[u]/\langle u^2\rangle$ such that the corresponding automorphism $\overline{\sigma}_0$ of the residue field $\mathbb{F}_4$ has order 2 (see Section 6.5.2).

6.2 Some preliminaries

In this section, we will state some basic results needed to derive our main results. Towards this, we first note, by Theorem 2 of Bhowmick *et al.* [14], that any Euclidean LCD code over a finite commutative chain ring is a free code. In the following theorem, we extend this result to σ-LCD codes over $\mathcal{R}_{e,r}$.

Theorem 6.2.1. *Every σ-LCD code over $\mathcal{R}_{e,r}$ is a free code.*

Proof. To prove the result, let C be a σ-LCD code of length n over $\mathcal{R}_{e,r}$. Now let us define

$$\sigma(C) = \big\{(\sigma_0(c_1), \sigma_0(c_2), \ldots, \sigma_0(c_n)) \ : \ (c_1, c_2, \ldots, c_n) \in C\big\}.$$

One can easily see that $\sigma(C)$ is also a linear code of length n over $\mathcal{R}_{e,r}$ and that $C^{\perp_\sigma} = \sigma(C)^\perp$, where $\sigma(C)^\perp$ denotes the (Euclidean) dual code of the code $\sigma(C)$. Since $\mathcal{R}_{e,r}$ is a finite commutative chain ring, the code C satisfies

$$|C| \times |C^{\perp_\sigma}| = |C| \times |\sigma(C)^\perp| = |\sigma(C)| \times |\sigma(C)^\perp| = |\mathcal{R}_{e,r}^n|,$$

which implies that $C \oplus C^{\perp_\sigma} = \mathcal{R}_{e,r}^n$. This shows that the code C is a projective $\mathcal{R}_{e,r}$-module. Now by applying Theorem 2 of Kaplansky [59], we see that the code C is a free code. □

For any $m \times n$ matrix $\mathcal{B}$ over $\mathcal{R}_{e,r}$ with the (i,j)-th entry as $b_{i,j}$, let $\sigma_0(\mathcal{B})$ denote an $m \times n$ matrix over $\mathcal{R}_{e,r}$ whose (i,j)-th entry is $\sigma_0(b_{i,j})$ for each i and j. Recall that a square matrix A over $\mathcal{R}_{e,r}$ is said to be non-singular if the determinant of the matrix A is a unit in $\mathcal{R}_{e,r}$. Now the following theorem provides a necessary and sufficient condition under which a linear code over $\mathcal{R}_{e,r}$ is a σ-LCD code in terms of its generator matrix.

Theorem 6.2.2. *[66, Th. 3.7] A linear code C of length n over $\mathcal{R}_{e,r}$ with a generator matrix G is a σ-LCD code if and only if the matrix $G\sigma_0(G)^t$ is non-singular.*

Next, corresponding to the automorphism σ of $\mathcal{R}_{e,r}^n$ as defined by (6.1.1), one can define an automorphism $\overline{\sigma}$ of $\overline{\mathcal{R}}_{e,r}^n$ as

$$\overline{\sigma}(\overline{a}) = (\overline{\sigma}_0(\overline{a}_1), \overline{\sigma}_0(\overline{a}_2), \ldots, \overline{\sigma}_0(\overline{a}_n)) \text{ for all } \overline{a} = (\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_n) \in \overline{\mathcal{R}}_{e,r}^n.$$

Now the $\overline{\sigma}$-inner product on $\overline{\mathcal{R}}_{e,r}^n$ is a map $[\cdot,\cdot]_{\overline{\sigma}} : \overline{\mathcal{R}}_{e,r}^n \times \overline{\mathcal{R}}_{e,r}^n \to \overline{\mathcal{R}}_{e,r}$, defined as

$$[\overline{c}, \overline{d}]_{\overline{\sigma}} = \overline{c} \cdot \overline{\sigma}(\overline{d}) = \overline{c}_1\overline{\sigma}_0(\overline{d}_1) + \overline{c}_2\overline{\sigma}_0(\overline{d}_2) + \cdots + \overline{c}_n\overline{\sigma}_0(\overline{d}_n)$$

for all $\overline{c} = (\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_n)$ and $\overline{d} = (\overline{d}_1, \overline{d}_2, \ldots, \overline{d}_n)$ in $\overline{\mathcal{R}}_{e,r}^n$. If D is a linear code of length n over $\overline{\mathcal{R}}_{e,r}$, then its $\overline{\sigma}$-dual code $D^{\perp_{\overline{\sigma}}}$ is defined as

$$D^{\perp_{\overline{\sigma}}} = \{\overline{b} \in \overline{\mathcal{R}}_{e,r}^n : [\overline{b}, \overline{a}]_{\overline{\sigma}} = 0 \text{ for all } \overline{a} \in D\}.$$

Note that $D^{\perp_{\overline{\sigma}}}$ is also a linear code of length n over $\overline{\mathcal{R}}_{e,r}$. The code D is said to be a linear code with complementary $\overline{\sigma}$-dual (or a $\overline{\sigma}$-LCD code) if it satisfies $D \cap D^{\perp_{\overline{\sigma}}} = \{0\}$.

Now by Theorem 2.2.2, we see that every free linear code C of length n over $\mathcal{R}_{e,r}$ is permutation equivalent to a code with a generator matrix in the standard form

$$G = \Big[I_k \mid A \Big],$$

where I_k is the $k \times k$ identity matrix over $\mathcal{R}_{e,r}$ and A is a $k \times (n-k)$ matrix over $\mathcal{R}_{e,r}$. Recall that the integer k is the rank of the code C. One can easily observe that $|C| = |\overline{\mathcal{R}}_{e,r}|^{ke} = p^{rke}$. Moreover, for $1 \leq i \leq e$, by (2.2.2), we see that the i-th Torsion code $Tor_i(C)$ of the code C is permutation equivalent to a code with a generator matrix in the standard form

$$\overline{G} = \left[\overline{I}_k \mid \overline{A}\right].$$

From this, we see that $Tor_1(C) = Tor_2(C) = Tor_3(C) = \cdots = Tor_e(C)$. In a recent work, Liu and Wang [68, Cor. 17] provided a necessary and sufficient condition under which a linear code over $\mathcal{R}_{e,r}$ is a Euclidean LCD code in terms of its Torsion codes. The following theorem extends this result to σ-LCD codes over the finite commutative chain ring $\mathcal{R}_{e,r}$ for each automorphism σ_0 of $\mathcal{R}_{e,r}$.

Theorem 6.2.3. *Let C be a linear code of length n over $\mathcal{R}_{e,r}$ with a generator matrix G. Then the following three statements are equivalent:*

(a) The code C is a σ-LCD code.

(b) For $1 \leq i \leq e$, the Torsion code $Tor_i(C)$ is a $\overline{\sigma}$-LCD code over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix $\overline{G}$.

(c) The code C is a free code and the matrix $\overline{G}\overline{\sigma}_0(\overline{G})^t$ is non-singular.

Proof. To prove the result, we see, by Theorem 6.2.2, that the code C is σ-LCD if and only if the matrix $G\sigma_0(G)^t$ is non-singular, *i.e.,* the determinant of the matrix $G\sigma_0(G)^t$ is a unit in $\mathcal{R}_{e,r}$. Further, we observe that $\overline{\det(G\sigma_0(G)^t)} = \det(\overline{G}\overline{\sigma}_0(\overline{G})^t)$, which implies that the determinant of the matrix $G\sigma_0(G)^t$ is a unit in $\mathcal{R}_{e,r}$ if and only if the determinant of the matrix $\overline{G}\overline{\sigma}_0(\overline{G})^t$ is non-zero. Thus by Theorem 6.2.2, it follows that the code C is σ-LCD if and only if its Torsion code $Tor_1(C)$ is a $\overline{\sigma}$-LCD over $\overline{\mathcal{R}}_{e,r}$. From this, the desired result follows immediately. □

In view of Corollaries 2.1.1 and 2.1.2, we note that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is a much broader class as compared to that of Euclidean LCD codes over $\mathcal{R}_{e,r}$ even if we assume that $\sigma_0 \in Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$.

From now on, we shall follow the same notations as in Section 6.2. In the following section, we will count all σ-LCD codes of length n over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$.

6.3 Enumeration of σ-LCD codes over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$

Throughout this section, we assume that $\sigma_0 \in Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$. We recall, by Theorem 6.2.3, that a linear code C of length n over $\mathcal{R}_{e,r}$ is a σ-LCD code if and only if $Tor_1(C) = Tor_2(C) = \cdots = Tor_e(C)$ and the Torsion code $Tor_1(C)$ is a $\overline{\sigma}$-LCD code of length n over $\overline{\mathcal{R}}_{e,r}$. We next recall that the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ has order p^r, where p is a prime number and r is a positive integer. Now to count all σ-LCD codes of an arbitrary length n over $\mathcal{R}_{e,r}$, we will first count all σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$ with a prescribed 1-th Torsion code. To do this, we assume, throughout this section, that C_1 is a k-dimensional linear code of length n over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix

$$\left[\overline{I}_k \mid L\right],$$

where L is a $k \times (n-k)$ matrix over $\overline{\mathcal{R}}_{e,r}$. Further, since the map $^{-}\restriction_{\mathcal{T}_{e,r}} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection, there exists a unique $k \times (n-k)$ matrix A_0 over $\mathcal{T}_{e,r}$ satisfying $\overline{A}_0 = L$. Now we make the following observation.

Lemma 6.3.1. *If C is a free linear code of length n over $\mathcal{R}_{e,r}$ with $Tor_1(C) = C_1$, then there exist $k \times (n-k)$ matrices $A_1, A_2, \ldots, A_{e-1}$ over $\mathcal{T}_{e,r}$ such that the matrix*

$$\left[I_k \mid A_0 + uA_1 + \cdots + u^{e-1}A_{e-1}\right] \tag{6.3.1}$$

is a generator matrix of the code C.

Proof. As $Tor_1(C) = C_1$, there exist $k \times k$ matrices $M_1, M_2, \ldots, M_{e-1}$ and $k \times (n-k)$ matrices $P_1, P_2, \ldots, P_{e-1}$ over $\mathcal{T}_{e,r}$ such that

$$\mathcal{R}_{e,r}^k \left[I_k + uM_1 + \cdots + u^{e-1}M_{e-1} \mid A_0 + uP_1 + \cdots + u^{e-1}P_{e-1}\right] \subseteq C.$$

Now by applying the elementary row operations, we obtain

$$\begin{aligned}\mathcal{R}_{e,r}^{k}&\Big[I_k+uB_1+\cdots+u^{e-1}B_{e-1}\Big]\\ &\qquad\times\Big[I_k+uM_1+\cdots+u^{e-1}M_{e-1}\mid A_0+uP_1+\cdots+u^{e-1}P_{e-1}\Big]\subseteq C,\end{aligned}$$

where $B_1, B_2, \ldots, B_{e-1}$ are $k\times k$ matrices over $\mathcal{R}_{e,r}$, given by

$$B_1=-M_1$$

and

$$B_j=-M_j-\sum_{i=1}^{j-1}B_iM_{j-i}$$

for $2\le j\le e-1$. From this, it follows that

$$\mathcal{R}_{e,r}^{k}\Big[I_k\mid A_0+uA_1'+u^2A_2'+\cdots+u^{e-1}A_{e-1}'\Big]\subseteq C,$$

where $A_1', A_2', \ldots, A_{e-1}'$ are $k\times(n-k)$ matrices over $\mathcal{R}_{e,r}$, given by

$$A_1'=P_1+B_1A_0$$

and

$$A_j'=P_j+B_jA_0+\sum_{i=1}^{j-1}B_iP_{j-i}$$

for $2\le j\le e-1$. It is easy to observe that there exist unique $k\times(n-k)$ matrices A_1, A_2, …, A_{e-1} over $\mathcal{T}_{e,r}$ satisfying

$$A_1'+uA_2'+\cdots+u^{e-2}A_{e-1}'\equiv A_1+uA_2+\cdots+u^{e-2}A_{e-1}\ (\mathrm{mod}\ u^{e-1}).$$

This implies that

$$\mathcal{R}_{e,r}^{k}\Big[I_k\mid A_0+uA_1+u^2A_2+\cdots+u^{e-1}A_{e-1}\Big]\subseteq C.$$

Furthermore, we see that

$$|C| = |Tor_1(C)|^e = (p^r)^{ke} = \left|\mathcal{R}_{e,r}^k \left[I_k \mid A_0 + uA_1 + u^2A_2 + \cdots + u^{e-1}A_{e-1}\right]\right| \leq |C|,$$

from which it follows that the code C has a generator matrix of the form (6.3.1). □

In the following theorem, we enumerate all σ-LCD codes C of length n over $\mathcal{R}_{e,r}$ with $Tor_1(C) = C_1$.

Theorem 6.3.1. *If the code C_1 is a k-dimensional $\overline{\sigma}$-LCD code of length n over $\overline{\mathcal{R}}_{e,r}$, then there are precisely*

$$p^{rk(n-k)(e-1)}$$

distinct σ-LCD codes C of length n over $\mathcal{R}_{e,r}$ with $Tor_1(C) = C_1$.

Proof. To prove the result, let C be a free linear code of length n over $\mathcal{R}_{e,r}$ with $Tor_1(C) = C_1$. Here by Lemma 6.3.1, we see that there exist $k \times (n-k)$ matrices $A_1, A_2, \ldots, A_{e-1}$ over $\mathcal{T}_{e,r}$ such that the matrix

$$G = \left[I_k \mid A_0 + uA_1 + \cdots + u^{e-1}A_{e-1}\right]$$

is a generator matrix of the code C. By applying Theorem 6.2.3, we see that the code C is σ-LCD if and only if the matrix

$$\overline{G}\overline{\sigma}_0(\overline{G})^t = \overline{I}_k + \overline{A}_0\overline{\sigma}_0(\overline{A}_0)^t = \overline{I}_k + L\overline{\sigma}_0(L)^t$$

is non-singular. This implies that the code C is σ-LCD for arbitrary choices of the $k \times (n-k)$ matrices $A_1, A_2, \ldots, A_{e-1}$ over $\mathcal{T}_{e,r}$. Furthermore, one can easily observe that the distinct choices of the $k \times (n-k)$ matrices $A_1, A_2, \ldots, A_{e-1}$ over $\mathcal{T}_{e,r}$ give rise to distinct σ-LCD codes of length n over $\mathcal{R}_{e,r}$ with $Tor_1(C) = C_1$. From this and by using the fact that the matrices $A_1, A_2, \ldots, A_{e-1}$ have precisely $p^{rk(n-k)(e-1)}$ distinct choices, the desired result follows immediately. □

Now we shall distinguish the following two cases: (i) $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$ and (ii) $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$.

6.3.1 The case $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$

Throughout this section, we assume that $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$, *i.e.*, σ_0 is an automorphism of $\mathcal{R}_{e,r}$ such that $\overline{\sigma}_0$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$. Now to enumerate all σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$, we shall first count all k-dimensional Euclidean LCD codes of length n over the finite field $\mathbb{F}_q$ of order q by distinguishing the following two cases: (i) q is an even prime power and (ii) q is an odd prime power. It is worth mentioning that Carlet *et al.* [27, Cor. 17 and 32] also enumerated all k-dimensional Euclidean LCD codes of length n over $\mathbb{F}_q$ when either $q = 2$ or q is an odd prime power. Recently, Liu and Wang [69] also counted all Euclidean and Hermitian LCD codes over $\mathbb{F}_q$ by using cogredience theories of matrices. However, our proof technique is quite different from the ones employed by Carlet *et al.* [27, Sec. IV and V] and Liu and Wang [69].

Now to count all Euclidean LCD codes of length n and dimension k over $\mathbb{F}_q$ when q is an even prime power, we need to study derangements of the set $\{1, 2, \ldots, n\}$. A derangement of a non-empty set $\{1, 2, \ldots, n\}$ is defined as a permutation π of $\{1, 2, \ldots, n\}$ satisfying $\pi(i) \neq i$ for all $i \in \{1, 2, \ldots, n\}$. Next, let $\mathscr{X}_n$ be the set consisting of all the derangements of the set $\{1, 2, \ldots, n\}$. By Exercise 21 of [19, Ch. 6], we have the following lemma.

Lemma 6.3.2. *$|\mathscr{X}_n|$ is even if and only if n is an odd integer.*

We also need the following lemma by Sharma and Kaur [91].

Lemma 6.3.3. *[91, Lem. 3.7] Let $(V, \mathcal{B})$ be an m-dimensional symplectic space over $\mathbb{F}_q$. Then the integer m is even. Further, for $0 \leq k \leq m$, the number $\mathcal{M}_k$ of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of V is given by*

$$\mathcal{M}_k = \begin{cases} q^{\frac{k(m-k)}{2}} \begin{bmatrix} m/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}$$

From now on, let $\mathcal{L}_q(n; k)$ denote the number of distinct k-dimensional Euclidean LCD codes of length n over $\mathbb{F}_q$ for $0 \leq k \leq n$. It is easy to see that $\mathcal{L}_q(n; 0) = \mathcal{L}_q(n; n) = 1$. So we assume, throughout this section, that $1 \leq k \leq n - 1$.

Determination of the number $\mathcal{L}_q(n;k)$ when q is an even prime power

Throughout this section, we assume that q is an even prime power. In the following theorem, we explicitly determine the number $\mathcal{L}_q(n;k)$ of distinct k-dimensional Euclidean LCD codes of length n over $\mathbb{F}_q$ for $1 \leq k \leq n-1$.

Theorem 6.3.2. *Let q be an even prime power. For $1 \leq k \leq n-1$, we have*

$$\mathcal{L}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are odd;} \\ q^{\frac{nk-k^2+n-1}{2}} \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd and } n \text{ is even;} \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even and } n \text{ is odd;} \\ q^{\frac{nk-k^2-2}{2}} \Big((q^k+q-1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \\ +(q^{n-k+1}-q^{n-k}+1) \begin{bmatrix} (n-2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2} \Big) & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

To prove the above theorem, let $\cdot$ denote the Euclidean bilinear form on $\mathbb{F}_q^n$. It is easy to see that the Euclidean bilinear form $\cdot$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_q^n$, *i.e.,* the formed space $\left(\mathbb{F}_q^n, \cdot\right)$ is an n-dimensional orthogonal space over $\mathbb{F}_q$. We further observe that each Euclidean LCD code of length n and dimension k over $\mathbb{F}_q$ can also be viewed as a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of the orthogonal space $(\mathbb{F}_q^n, \cdot)$. In view of this, the number $\mathcal{L}_q(n;k)$ equals the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of the orthogonal space $(\mathbb{F}_q^n, \cdot)$. Now we define

$$\mathcal{W}_0 = \Big\{(w_1, w_2, \ldots, w_n) \in \mathbb{F}_q^n \ : \ \sum_{i=1}^{n} w_i = 0\Big\}.$$

It is easy to observe that the set $\mathcal{W}_0$ is an $(n-1)$-dimensional $\mathbb{F}_q$-linear subspace of the orthogonal space $\mathbb{F}_q^n$. Further, we see that $(\mathcal{W}_0, \cdot \restriction_{\mathcal{W}_0 \times \mathcal{W}_0})$ is a symplectic space over $\mathbb{F}_q$. We also note that the all-one vector $\mathbf{1} = (1, 1, \ldots, 1) \in \mathcal{W}_0$ if and only if n is an even integer. Accordingly, we will distinguish the following two cases: A. n is odd and B. n is even.

In the following proposition, we determine the number $\mathcal{L}_q(n;k)$ when q is even and n is odd, where $1 \leq k \leq n-1$.

Proposition 6.3.1. *Let q be an even prime power, and let n be an odd integer. For $1 \leq k \leq n-1$, we have*

$$\mathcal{L}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd;} \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even.} \end{cases}$$

Proof. To prove the result, we first note that the all-one vector $\mathbf{1} = (1, 1, \ldots, 1) \notin \mathcal{W}_0$ and that $w_0 \cdot \mathbf{1} = 0$ for all $w_0 \in \mathcal{W}_0$. This implies that $\mathbb{F}_q^n = \mathcal{W}_0 \perp \langle \mathbf{1} \rangle$. We further observe that any k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ is either contained in $\mathcal{W}_0$ or not contained in $\mathcal{W}_0$.

First of all, we will count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_0$. For this, we see, by Lemma 6.3.3, that there does not exist any k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ contained in $\mathcal{W}_0$ when k is odd, while the number of such k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathcal{W}_0$ is given by

$$\mathfrak{C}_k^{(e_1)} = q^{\frac{k(n-k-1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2}$$

when k is even.

Next, we observe that any k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ not contained in $\mathcal{W}_0$ is of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$, where $v_i \in \mathcal{W}_0 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_0$. Here we will distinguish the following two cases: (i) k is odd and (ii) k is even.

(i) Let k be odd. When $v_k = 0$, we see, by applying Theorem 2.3.1 and Lemma 6.3.2, that the k-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} \rangle$ of $\mathbb{F}_q^n$ is non-degenerate if and only if $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_0$. Now by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{(k-1)(n-k)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} \rangle$, where $v_i \in \mathcal{W}_0 \setminus \{0\}$ for $1 \leq i \leq k-1$.

Next, let $v_k \neq 0$. Here by applying Theorem 2.3.1 and Lemma 6.3.2 again, we see that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_0$. Further, we observe that each $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ of $\mathcal{W}_0$ gives rise to precisely $(q^{n-k}-1)$ distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$, where $v_k(\neq 0) \in \mathcal{W}_0$. From this and by applying Lemma 6.3.3 again, we see that there are precisely

$$q^{\frac{(k-1)(n-k)}{2}} (q^{n-k}-1) \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the form $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$, where $v_i \in \mathcal{W}_0 \setminus \{0\}$ for $1 \leq i \leq k$.

On combining both the cases, we see that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the form $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$ with $v_i \in \mathcal{W}_0 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_0$, is given by

$$\begin{aligned} \mathfrak{C}_k^{(o)} &= q^{\frac{(k-1)(n-k)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} + q^{\frac{(k-1)(n-k)}{2}} (q^{n-k}-1) \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} \\ &= q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2}. \end{aligned}$$

(ii) Let k be even. When $v_k = 0$, we see, by applying Theorem 2.3.1 and Lemma 6.3.2, that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} \rangle$ is a degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$.

Next, let $v_k \neq 0$. Here by applying Theorem 2.3.1 and Lemma 6.3.2, we see that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_0$. Further, we observe that each k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_0$ gives rise to precisely (q^k-1) distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1}+v_k\rangle$. From this and by applying Lemma 6.3.3 again, we see that there are precisely

$$\mathfrak{C}_k^{(e_2)} = q^{\frac{k(n-k-1)}{2}}(q^k-1)\begin{bmatrix}(n-1)/2\\ k/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the form $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1}+v_k\rangle$, where $v_i \in \mathcal{W}_0 \setminus \{0\}$ for $1 \leq i \leq k$.

On combining the above cases, we get

$$\mathcal{L}_q(n;k) = \mathfrak{C}_k^{(o)} = q^{\frac{(n-k)(k+1)}{2}}\begin{bmatrix}(n-1)/2\\ (k-1)/2\end{bmatrix}_{q^2} \text{ when } k \text{ is odd,}$$

and

$$\mathcal{L}_q(n;k) = \mathfrak{C}_k^{(e_1)} + \mathfrak{C}_k^{(e_2)} = q^{\frac{k(n-k+1)}{2}}\begin{bmatrix}(n-1)/2\\ k/2\end{bmatrix}_{q^2} \text{ when } k \text{ is even.}$$

□

Next, let n be an even integer. In this case, we first note that $\mathbf{1} = (1, 1, \ldots, 1) \in \mathcal{W}_0$. Now to enumerate all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$, let $\mathcal{W}_1$ be an $(n-2)$-dimensional $\mathbb{F}_q$-linear subspace of $\mathcal{W}_0$ such that $\mathbf{1} \notin \mathcal{W}_1$. One can easily observe that there exists an element $z \in \mathcal{W}_1^{\perp}\setminus\mathcal{W}_0$. In view of this, we can write $\mathbb{F}_q^n = \mathcal{W}_1 \oplus \langle \mathbf{1}\rangle \oplus \langle z\rangle$. We further see that $(\mathcal{W}_1, \cdot \restriction_{\mathcal{W}_1\times\mathcal{W}_1})$ is an $(n-2)$-dimensional symplectic space over $\mathbb{F}_q$. We next observe that any k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ is either contained in $\mathcal{W}_1$, or contained in $\mathcal{W}_1 \oplus \langle \mathbf{1}\rangle$ but not in $\mathcal{W}_1$, or contained in $\mathcal{W}_1 \oplus \langle z\rangle$ but not in $\mathcal{W}_1$, or contained in $\mathbb{F}_q^n = \mathcal{W}_1 \oplus \langle \mathbf{1}\rangle \oplus \langle z\rangle$ but not in any of the subspaces $\mathcal{W}_1$, $\mathcal{W}_1 \oplus \langle \mathbf{1}\rangle$ and $\mathcal{W}_1 \oplus \langle z\rangle$. Accordingly, we proceed as follows:

In the following lemma, we count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_1$.

Lemma 6.3.4. *Let q be an even prime power, n be an even integer, and let k be an integer satisfying $1 \leq k \leq n-1$. The number $\mathfrak{D}_k^{(1)}$ of distinct k-dimensional* *non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$, that are contained in $\mathcal{W}_1$ is given by*

$$\mathfrak{D}_k^{(1)} = \begin{cases} q^{\frac{k(n-k-2)}{2}} \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The desired result follows by applying Lemma 6.3.3. □

In the following lemma, we count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_1 \oplus \langle \mathbf{1} \rangle$ but not in $\mathcal{W}_1$.

Lemma 6.3.5. *Let q be an even prime power, n be an even integer, and let k be an integer satisfying $1 \leq k \leq n-1$. The number $\mathfrak{D}_k^{(2)}$ of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_1 \oplus \langle \mathbf{1} \rangle$ but not in $\mathcal{W}_1$, is given by*

$$\mathfrak{D}_k^{(2)} = \begin{cases} q^{\frac{k(n-k-2)}{2}} (q^k - 1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even;} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Working as in Proposition 6.3.1, the desired result follows. □

In the following lemma, we count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_1 \oplus \langle z \rangle$ but not in $\mathcal{W}_1$.

Lemma 6.3.6. *Let q be an even prime power, n be an even integer, and let k be an integer satisfying $1 \leq k \leq n-1$. The number $\mathfrak{D}_k^{(3)}$ of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathcal{W}_1 \oplus \langle z \rangle$ but not in $\mathcal{W}_1$, is given by*

$$\mathfrak{D}_k^{(3)} = \begin{cases} q^{\frac{(k+1)(n-k-1)}{2}} \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd;} \\ q^{\frac{k(n-k-2)}{2}} (q^k - 1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even.} \end{cases}$$

Proof. Working as in Proposition 6.3.1, the desired result follows. □

Finally, we proceed to enumerate all distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ that are contained in $\mathbb{F}_q^n = \mathcal{W}_1 \oplus \langle \mathbf{1} \rangle \oplus \langle z \rangle$ but not in any of the subspaces $\mathcal{W}_1$, $\mathcal{W}_1 \oplus \langle \mathbf{1} \rangle$ and $\mathcal{W}_1 \oplus \langle z \rangle$. For this, we first observe that any such k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace U of $\mathbb{F}_q^n$ is exactly one of the following two types:

(a) $U = \langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k + \lambda z \rangle$, where $\lambda (\neq 0) \in \mathbb{F}_q$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_1$.

(b) $U = \langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k \rangle$, where $k \geq 2$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-2$ and $v_{k-1}, v_k \in \mathcal{W}_1$.

Now in the following lemma, we first count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k + \lambda z \rangle$, where $\lambda (\neq 0) \in \mathbb{F}_q$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_1$.

Lemma 6.3.7. *Let q be an even prime power, n be an even integer, and let k be an integer satisfying $1 \leq k \leq n-1$. The number $\mathfrak{D}_k^{(4)}$ of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + v_k + \lambda z \rangle$, where $\lambda (\neq 0) \in \mathbb{F}_q$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_1$, is given by*

$$\mathfrak{D}_k^{(4)} = \begin{cases} q^{\frac{k(n-k-2)}{2}} (q^k - 1)(q-1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even;} \\ q^{\frac{(k+1)(n-k-1)}{2}} (q-1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd.} \end{cases}$$

Proof. To prove the result, we will consider the following two cases separately: k is even and k is odd.

(i) Let k be even. When $v_k = 0$, we see, by applying Theorem 2.3.1 and Lemma 6.3.2, that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z \rangle$ is a degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. On the other hand, when $v_k \neq 0$, we see, by applying Theorem 2.3.1 and Lemma 6.3.2 again, that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z + v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We further observe that each k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k \rangle$ of $\mathcal{W}_1$ gives rise to precisely $(q^k - 1)(q-1)$ distinct k-dimensional non-degenerate

$\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z + v_k \rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$. From this and by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{k(n-k-2)}{2}}(q^k - 1)(q - 1)\begin{bmatrix}(n-2)/2\\ k/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1}+\lambda z+v_k \rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_1$.

(ii) Next, let k be odd. Here by applying Theorem 2.3.1 and Lemma 6.3.2, we see that $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z + v_k \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We further observe that each element $\lambda(\neq 0) \in \mathbb{F}_q$ and each element $v_k \in \langle v_1, v_2, \ldots, v_{k-1} \rangle^{\perp}$ give rise to a distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z + v_k \rangle$. This implies that each $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ of $\mathcal{W}_1$ gives rise to precisely $q^{n-k-1}(q-1)$ distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1} + \lambda z + v_k \rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$ and $v_k \in \mathcal{W}_1$. From this and by applying Lemma 6.3.3 again, we see that there are precisely

$$q^{\frac{(k+1)(n-k-1)}{2}}(q - 1)\begin{bmatrix}(n-2)/2\\ (k-1)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-1}, \mathbf{1}+\lambda z+v_k \rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$ and $v_k \in \mathcal{W}_1$.

□

In the following lemma, we proceed to count all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + v_k \rangle$, where $2 \leq k \leq n-1$, $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-2$ and $v_{k-1}, v_k \in \mathcal{W}_1$.

Lemma 6.3.8. *Let q be an even prime power, n be an even integer, and let k be an integer satisfying $2 \leq k \leq n-1$. The number $\mathfrak{D}_k^{(5)}$ of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + v_k \rangle$ with $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-2$ and $v_{k-1}, v_k \in \mathcal{W}_1$, is given by*

$$\mathfrak{D}_k^{(5)} = \begin{cases} q^{\frac{k(n-k)+(n-2k+1)}{2}}(q^{k-1}-1)\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2} & \text{if } k \text{ is odd;} \\ q^{\frac{nk-k^2-2}{2}}(q^{n-k+1}-q^{n-k}+1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2} & \\ +q^{\frac{k(n-k-2)}{2}}(q^{k+1}-q)(q^{k-2}-1)\begin{bmatrix}(n-2)/2\\k/2\end{bmatrix}_{q^2} & \text{if } k \text{ is even.} \end{cases}$$

Proof. To prove the result, we will distinguish the following two cases: k is odd and k is even.

(i) Let k be odd. Here when $v_{k-1} = 0$, by applying Theorem 2.3.1 and Lemma 6.3.2, we see that the k-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z + v_k \rangle$ of $\mathbb{F}_q^n$ is degenerate.

When $v_{k-1} \neq 0$ and $v_k = 0$, by applying Theorem 2.3.1 and Lemma 6.3.2 again, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z \rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}, v_{k-1} \rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We further observe that each $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-1} \rangle$ of $\mathcal{W}_1$ gives rise to precisely $(q^{k-1}-1)$ distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z \rangle$ of $\mathbb{F}_q^n$. Further, by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{(k-1)(n-k-1)}{2}}(q^{k-1}-1)\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z \rangle$, where $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$.

Now let v_{k-1}, $v_k \in \mathcal{W}_1$ both be non-zero. Here we will consider the following two cases separately: v_{k-1}, v_k are linearly dependent over $\mathbb{F}_q$ and v_{k-1}, v_k are linearly independent over $\mathbb{F}_q$.

First let $v_{k-1},\ v_k \in \mathcal{W}_1$ be linearly dependent over $\mathbb{F}_q$. Here we have $v_k = av_{k-1}$ for some $a(\neq 0) \in \mathbb{F}_q$. Further, it is easy to observe that

$$\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + v_k\rangle = \langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$$

for some $\lambda(\neq 0) \in \mathbb{F}_q$. Next by applying Theorem 2.3.1 and Lemma 6.3.2, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}, v_{k-1}\rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. Now working as in Proposition 6.3.1(ii) and by applying Lemma 6.3.3 again, we see that there are precisely

$$q^{\frac{(k-1)(n-k-1)}{2}}(q-1)(q^{k-1}-1)\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$, $v_i(\neq 0) \in \mathcal{W}_1$ for $1 \leq i \leq k$, such that v_{k-1} and v_k are linearly dependent over $\mathbb{F}_q$.

Next, let $v_{k-1},\ v_k \in \mathcal{W}_1$ be linearly independent over $\mathbb{F}_q$. By applying Theorem 2.3.1 and Lemma 6.3.2 again, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}, v_{k-1}\rangle$ is a $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. Further, working as in Proposition 6.3.1(ii), we observe that each $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-1}\rangle$ of $\mathcal{W}_1$ gives rise to precisely $(q^{k-1}-1)$ distinct $(k-1)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}\rangle$, where $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$. Furthermore, by applying Theorem 2.3.2, we can write $v_k = \sum\limits_{j=1}^{k-1} a_j v_j + \widetilde{w}$, where $a_j \in \mathbb{F}_q$ for $1 \leq j \leq k-1$ and $\widetilde{w} \in \langle v_1, v_2, \ldots, v_{k-1}\rangle^{\perp}\setminus\{0\}$. We next observe that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle = \langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + a_{k-1}v_{k-1} + \widetilde{w}\rangle$. It is easy to observe that $a_{k-1}v_{k-1} + \widetilde{w} \neq 0$. Further, each element $a_{k-1} \in \mathbb{F}_q$ and each non-zero element $\widetilde{w} \in \langle v_1, v_2, \ldots, v_{k-1}\rangle^{\perp}$ gives rise to a distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + v_k\rangle$. From this and by applying Lemma 6.3.3 again, we see that there are precisely

$$q^{\frac{(k-1)(n-k-1)}{2}}(q^{k-1}-1)(q^{n-k}-q)\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$, where $v_i(\neq 0) \in \mathcal{W}_1$ for $1 \leq i \leq k$, such that v_{k-1} and v_k are linearly independent over $\mathbb{F}_q$.

On combining the above cases, we see that when k is odd, there are precisely

$$q^{\frac{k(n-k)+(n-2k+1)}{2}}(q^{k-1}-1)\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$, where $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-2$ and $v_{k-1}, v_k \in \mathcal{W}_1$.

(ii) Next, let k be even. Here when $v_{k-1} = v_k = 0$, by applying Theorem 2.3.1 and Lemma 6.3.2, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ is a $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. Now by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{(k-2)(n-k)}{2}}\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z\rangle$, where $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-2$.

When $v_{k-1} \neq 0$ and $v_k = 0$, by applying Theorem 2.3.1 and Lemma 6.3.2 again, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ is a $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. Further, working as in Proposition 6.3.1(i) and by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{(k-2)(n-k)}{2}}(q^{n-k}-1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z\rangle$, where $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \leq i \leq k-1$.

When $v_{k-1} = 0$ and $v_k \neq 0$, by applying Theorem 2.3.1 and Lemma 6.3.2 again, we see that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z + v_k\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ is a $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We next observe that each element $v_k \in \langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp} \setminus \{0\}$ gives rise to a distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z{+}v_k\rangle$ of $\mathbb{F}_q^n$. Now by applying Lemma 6.3.3, we see that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}, z + v_k\rangle$ is given by

$$q^{\frac{(k-2)(n-k)}{2}}(q^{n-k}-1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}.$$

Now let v_{k-1}, $v_k \in \mathcal{W}_1$ both be non-zero. Here we will consider the following two cases separately: v_{k-1} and v_k are linearly dependent over $\mathbb{F}_q$, and v_{k-1} and v_k are linearly independent over $\mathbb{F}_q$.

First let v_{k-1} and v_k be linearly dependent over $\mathbb{F}_q$. Here we observe that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, z + v_k\rangle = \langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$ for some $\lambda(\neq 0) \in \mathbb{F}_q$. Further, for each $\lambda(\neq 0) \in \mathbb{F}_q$, we see, by applying Theorem 2.3.1 and Lemma 6.3.2, that $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$ is a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ if and only if $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ is a $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We next observe that each element $\lambda(\neq 0) \in \mathbb{F}_q$ and each element $v_{k-1} \in \langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp} \setminus \{0\}$ give rise to a distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$. Now by applying Lemma 6.3.3 again, we see that there are precisely

$$q^{\frac{(k-2)(n-k)}{2}}(q^{n-k}-1)(q-1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1} + v_{k-1}, \mathbf{1} + \lambda z\rangle$, where $\lambda(\neq 0) \in \mathbb{F}_q$ and $v_i \in \mathcal{W}_1 \setminus \{0\}$ for

$1 \leq i \leq k-1$.

Finally, let v_{k-1} and v_k be linearly independent over $\mathbb{F}_q$. Let $\mathfrak{G}(v_1, v_2, \ldots, v_k)$, $\mathfrak{G}(v_1, v_2, \ldots, v_{k-2})$ and $\mathfrak{G}(v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k)$ denote the Gram matrices of $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ with respect to the bases $\{v_1, v_2, \ldots, v_k\}$, $\{v_1, v_2, \ldots, v_{k-2}\}$ and $\{v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\}$, respectively. Then by applying Theorem 2.3.1 and Lemma 6.3.2, we observe that

$$\begin{aligned}\det(\mathfrak{G}(v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k)) &= \det(\mathfrak{G}(v_1, v_2, \ldots, v_{k-2})) \\ &\quad + \det(\mathfrak{G}(v_1, v_2, \ldots, v_k)).\end{aligned}$$

This implies that the k-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ of $\mathbb{F}_q^n$ is non-degenerate if and only if either

($\star$) the k-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ is degenerate but the $(k-2)$-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ of $\mathcal{W}_1$ is non-degenerate, or

($\diamond$) the k-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ is non-degenerate but the $(k-2)$-dimensional $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ of $\mathcal{W}_1$ is degenerate, or

($\dagger$) both $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ and $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ are non-degenerate, and $\det(\mathfrak{G}(v_1, v_2, \ldots, v_{k-2})) \neq \det(\mathfrak{G}(v_1, v_2, \ldots, v_k))$.

We will first enumerate all k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ satisfying ($\star$). For this, we see, by Lemma 6.3.3, that the number of distinct $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathcal{W}_1$ of the type $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ is given by

$$q^{\frac{(k-2)(n-k)}{2}} \begin{bmatrix} (n-2)/2 \\ (k-2)/2 \end{bmatrix}_{q^2}.$$

Further, by applying Theorem 2.3.2, we can write $\mathcal{W}_1 = \langle v_1, v_2, \ldots, v_{k-2}\rangle \perp \langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$, where $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$ is an $(n-k)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. We next observe that each pair (v_{k-1}, v_k)

of linearly independent vectors in $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$ gives rise to a distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$. It is easy to observe that $\langle v_1, v_2, \ldots, v_k\rangle = \langle v_1, v_2, \ldots, v_{k-2}\rangle \perp \langle v_{k-1}, v_k\rangle$, which implies that

$$\det(\mathfrak{G}(v_1, v_2, \ldots, v_k)) = \det(\mathfrak{G}(v_1, v_2, \ldots, v_{k-2}))\det(\mathfrak{G}(v_{k-1}, v_k)).$$

From this, we note that the $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ is degenerate if and only if $\det(\mathfrak{G}(v_{k-1}, v_k)) = 0$ if and only if $v_k \in \langle v_1, v_2, \ldots, v_{k-1}\rangle^{\perp}$. This implies that there are precisely $(q^{n-k}-1)(q^{n-k-1}-q)$ relevant choices for the pair (v_{k-1}, v_k). Now by applying Lemma 6.3.3, we see that there are precisely

$$q^{\frac{(k-2)(n-k)}{2}}(q^{n-k}-1)(q^{n-k-1}-q)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}$$

distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ of $\mathbb{F}_q^n$ satisfying $(\star)$.

Next we will enumerate all k-dimensional $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ of $\mathbb{F}_q^n$ satisfying $(\diamond)$. For this, we see, by Lemma 6.3.3, that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ is given by

$$q^{\frac{k(n-k-2)}{2}}\begin{bmatrix}(n-2)/2\\k/2\end{bmatrix}_{q^2}.$$

Further, we observe that every k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ has precisely

$$q^{k-2}\begin{bmatrix}k/2\\(k-2)/2\end{bmatrix}_{q^2}$$

distinct $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces. From this and by Theorem 2.3.9, we see that there are precisely

$$\left(\begin{bmatrix}k\\k-2\end{bmatrix}_q - q^{k-2}\begin{bmatrix}k/2\\(k-2)/2\end{bmatrix}_{q^2}\right)$$

distinct $(k-2)$-dimensional degenerate $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}\rangle$

of the k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$. Next let $\langle y_1, y_2, \ldots, y_{k-2}\rangle$ be a fixed $(k-2)$-dimensional degenerate $\mathbb{F}_q$-linear subspace of $\langle v_1, v_2, \ldots, v_k\rangle$. Now we will choose two linearly independent vectors y_{k-1}, y_k belonging to the $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ such that $\langle y_1, y_2, \ldots, y_k\rangle = \langle v_1, v_2, \ldots, v_k\rangle$. Note that the pair (y_{k-1}, y_k) has $(q^2-1)(q^2-q)$ distinct choices. From this and by applying Lemma 6.3.3, we see that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ satisfying $(\diamond)$ is given by

$$q^{\frac{k(n-k-2)}{2}}(q^2-1)(q^2-q)\begin{bmatrix}(n-2)/2\\ k/2\end{bmatrix}_{q^2}\left(\begin{bmatrix}k\\ k-2\end{bmatrix}_q - q^{k-2}\begin{bmatrix}k/2\\ (k-2)/2\end{bmatrix}_{q^2}\right).$$

Finally, we will enumerate all k-dimensional $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ of $\mathbb{F}_q^n$ satisfying $(\dagger)$. For this, we see, by Lemma 6.3.3, that the number of distinct $(k-2)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ of $\mathcal{W}_1$ is given by

$$q^{\frac{(k-2)(n-k)}{2}}\begin{bmatrix}(n-2)/2\\ (k-2)/2\end{bmatrix}_{q^2}.$$

By Theorem 2.3.2, we can write $\mathcal{W}_1 = \langle v_1, v_2, \ldots, v_{k-2}\rangle \perp \langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$, where $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$ is an $(n-k)$-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of $\mathcal{W}_1$. It is easy to observe that $\langle v_1, v_2, \ldots, v_k\rangle = \langle v_1, v_2, \ldots, v_{k-2}\rangle \perp \langle v_{k-1}, v_k\rangle$, which implies that

$$\det(\mathfrak{G}(v_1, v_2, \ldots, v_k)) = \det(\mathfrak{G}(v_1, v_2, \ldots, v_{k-2}))\det(\mathfrak{G}(v_{k-1}, v_k)).$$

This further implies that the $\mathbb{F}_q$-linear subspace $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ is non-degenerate if and only if $\det(\mathfrak{G}(v_{k-1}, v_k)) \neq 0$ if and only if $v_k \notin \langle v_{k-1}\rangle^{\perp}$ and (v_{k-1}, v_k) is not a hyperbolic pair in $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$. Thus there are precisely $q^{n-k-1}(q-1)(q^{n-k}-1)$ distinct choices for the pair (v_{k-1}, v_k) such that the $\mathbb{F}_q$-linear subspaces $\langle v_1, v_2, \ldots, v_{k-2}\rangle$ and $\langle v_1, v_2, \ldots, v_k\rangle$ of $\mathcal{W}_1$ are non-degenerate. Next by Theorem 2.3.3, we see that the Witt index of $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$ is $(n-k)/2$ and that the number of hyperbolic pairs in $\langle v_1, v_2, \ldots, v_{k-2}\rangle^{\perp}$

is $\mathcal{H}_{\frac{n-k}{2},0} = q^{n-k-1}(q^{n-k}-1)$. This implies that there are precisely $(q^{n-k}-1)(q-2)q^{n-k-1}$ relevant choices of the pair (v_{k-1}, v_k). From this, we see that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ satisfying (†) is given by

$$q^{\frac{k(n-k)-2}{2}}(q-2)(q^{n-k}-1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}.$$

From the above discussion, we see that the number of distinct k-dimensional non-degenerate $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ of the type $\langle v_1, v_2, \ldots, v_{k-2}, \mathbf{1}+v_{k-1}, z+v_k\rangle$ with $v_i \in \mathcal{W}_1 \setminus \{0\}$ for $1 \le i \le k-2$ and $v_{k-1}, v_k \in \mathcal{W}_1$, is given by

$$\begin{aligned}&q^{\frac{nk-k^2-2}{2}}(q^{n-k+1}-q^{n-k}+1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}\\&+q^{\frac{k(n-k-2)}{2}}(q^{k+1}-q)(q^{k-2}-1)\begin{bmatrix}(n-2)/2\\k/2\end{bmatrix}_{q^2}.\end{aligned}$$

□

Now in the following proposition, we determine the number $\mathcal{L}_q(n;k)$ when both q and n are even, where $1 \le k \le n-1$.

Proposition 6.3.2. *Let q be an even prime power, and let n be an even integer. For $1 \le k \le n-1$, we have*

$$\mathcal{L}_q(n;k) = \begin{cases} q^{\frac{(k+1)n-(k^2+1)}{2}}\begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{q^2} & \text{if } k \text{ is odd;}\\ q^{\frac{nk-k^2-2}{2}}\Bigg((q^k+q-1)\begin{bmatrix}(n-2)/2\\k/2\end{bmatrix}_{q^2} & \\ +(q^{n-k+1}-q^{n-k}+1)\begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{q^2}\Bigg) & \text{if } k \text{ is even.}\end{cases}$$

Proof. The desired result follows from Lemmas 6.3.4-6.3.8 by noting that

$$\mathcal{L}_q(n;k) = \mathfrak{D}_k^{(1)} + \mathfrak{D}_k^{(2)} + \mathfrak{D}_k^{(3)} + \mathfrak{D}_k^{(4)} + \mathfrak{D}_k^{(5)}.$$

□

Proof of Theorem 6.3.2. It follows immediately from Propositions 6.3.1 and 6.3.2.

Determination of the number $\mathcal{L}_q(n;k)$ when q is an odd prime power

Throughout this section, let us suppose that q is an odd prime power. In the following theorem, we determine the number $\mathcal{L}_q(n;k)$ for $1 \leq k \leq n-1$.

Theorem 6.3.3. *Let q be an odd prime power. For $1 \leq k \leq n-1$, we have*

$$\mathcal{L}_q(n;k) = \begin{cases} q^{\frac{(n-k)(k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are odd;} \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}}-1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd and } n \text{ is even with either } q \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 4 \text{ and } q \equiv 3 \pmod 4; \\ q^{\frac{nk-k^2-1}{2}} (q^{\frac{n}{2}}+1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is odd, } q \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4; \\ q^{\frac{k(n-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if } k \text{ is even and } n \text{ is odd;} \\ q^{\frac{k(n-k)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{q^2} & \text{if both } k \text{ and } n \text{ are even.} \end{cases}$$

Proof. To prove the result, let $\cdot$ denote the Euclidean bilinear form on $\mathbb{F}_q^n$. It is easy to see that the Euclidean bilinear form $\cdot$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_q^n$, *i.e.*, the formed space $(\mathbb{F}_q^n, \cdot)$ is an n-dimensional orthogonal space over $\mathbb{F}_q$. Since q is an odd prime power, one can easily observe that the orthogonal space $(\mathbb{F}_q^n, \cdot)$ can also be viewed as a non-degenerate quadratic space with respect to the quadratic map $\mathcal{Q} : \mathbb{F}_q^n \to \mathbb{F}_q$, defined as

$$\mathcal{Q}(v) = \frac{1}{2} v \cdot v \text{ for each } v \in \mathbb{F}_q^n.$$

We further observe that each Euclidean LCD code of length n and dimension k over $\mathbb{F}_q$ can also be viewed as a k-dimensional non-degenerate $\mathbb{F}_q$-linear subspace of the n-dimensional quadratic space $(\mathbb{F}_q^n, \mathcal{Q})$. In view of this, the number $\mathcal{L}_q(n;k)$ equals the number of distinct k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspaces of the quadratic space $(\mathbb{F}_q^n, \mathcal{Q})$ for $0 \leq k \leq n$. Further, it is easy to see that $\mathcal{L}_q(n;0) = \mathcal{L}_q(n;n) = 1$. So from this point on, we assume that $1 \leq k \leq n-1$.

By Theorem 2.3.6(b), we see that a k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace U of $\mathbb{F}_q^n$ has a Witt decomposition of the form $U = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\nu_k}, b_{\nu_k} \rangle \perp U_k$, where ν_k is the Witt index of U, (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_q^n$ for $1 \leq i \leq \nu_k$, and U_k is an anisotropic $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ satisfying $\dim_{\mathbb{F}_q}(U_k) = k - 2\nu_k \leq 2$. Now we shall distinguish the following two cases: (a) k is odd and (b) k is even.

(a) First let k be odd. Here by Theorem 2.3.6(a), we see that $\nu_k = (k-1)/2$, which implies that $\dim_{\mathbb{F}_q}(U_k) = 1$. This implies that the k-dimensional $\mathbb{F}_q$-linear subspace U of $\mathbb{F}_q^n$ has a Witt decomposition of the form

$$U = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}} \rangle \perp \langle w \rangle,$$

where (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_q^n$ for $1 \leq i \leq \frac{k-1}{2}$ and w is a non-singular vector of the quadratic space $(\mathbb{F}_q^n, \mathcal{Q})$. The set $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}, w\}$ is called a Witt basis of U over $\mathbb{F}_q$. Further, we observe that

$$\mathcal{L}_q(n;k) = \mathcal{D}_{\frac{k-1}{2},\nu} / \mathcal{D}_{\frac{k-1}{2}},$$

where $\mathcal{D}_{\frac{k-1}{2},\nu}$ is the number of Witt bases of the form $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}, w\}$ in $\mathbb{F}_q^n$ and $\mathcal{D}_{\frac{k-1}{2}}$ is the number of Witt bases of a k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. Now by applying Theorems 2.3.2, 2.3.5 and 2.3.6, we see that

$$\begin{aligned} \mathcal{D}_{\frac{k-1}{2},\nu} &= \mathcal{H}_{\nu,n-2\nu}\mathcal{H}_{\nu-1,n-2\nu}\cdots\mathcal{H}_{\nu-\frac{(k-3)}{2},n-2\nu}\left(q^{n-k+1} - 1 - \mathcal{I}_{\nu-\frac{(k-1)}{2},n-2\nu}\right) \\ &= \begin{cases} q^{\frac{2n(k+1)-k(k+4)+1}{4}}(q-1)\prod\limits_{v=0}^{(k-3)/2}(q^{n-2v-1}-1) & \text{if } \nu = \frac{n-1}{2}; \\ q^{\frac{2nk-(k+1)^2}{4}}(q^{\frac{n}{2}}-1)(q-1)\prod\limits_{v=1}^{(k-1)/2}(q^{n-2v}-1) & \text{if } \nu = \frac{n}{2}; \\ q^{\frac{2nk-(k+1)^2}{4}}(q^{\frac{n}{2}}+1)(q-1)\prod\limits_{v=1}^{(k-1)/2}(q^{n-2v}-1) & \text{if } \nu = \frac{n-2}{2} \end{cases} \end{aligned}$$

and that

$$\mathcal{D}_{\frac{k-1}{2}} = \mathcal{H}_{\frac{k-1}{2},1}\mathcal{H}_{\frac{k-3}{2},1}\cdots\mathcal{H}_{1,1}(q-1) = q^{\frac{(k-1)^2}{4}}(q-1)\prod_{v=0}^{(k-3)/2}(q^{k-2v-1}-1).$$

From this and by Theorem 2.3.6(a), the desired result follows immediately in the case when k is odd.

(b) Next let k be even. Here by Theorem 2.3.6(a), we see that either $\nu_k = \frac{k-2}{2}$ or $\nu_k = \frac{k}{2}$. Now let $\widetilde{\mathcal{S}}_q(n;k)$ and $\widehat{\mathcal{S}}_q(n;k)$ denote the number of distinct k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ having the Witt indices $\frac{k-2}{2}$ and $\frac{k}{2}$, respectively. We note that

$$\mathcal{L}_q(n;k) = \widetilde{\mathcal{S}}_q(n;k) + \widehat{\mathcal{S}}_q(n;k).$$

First of all, we will enumerate all distinct k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ having the Witt index $\frac{k-2}{2}$. In this case, we have $\dim_{\mathbb{F}_q}(U_k) = 2$. Here working in a similar manner as in Lemmas 3.2 and 3.3 of Sharma and Kaur [91], we see that each 2-dimensional anisotropic $\mathbb{F}_q$-linear subspace of U has an orthogonal basis and that the number of distinct orthogonal bases of a 2-dimensional anisotropic $\mathbb{F}_q$-linear subspace of U is given by

$$\mathfrak{A}_{k,\nu} = \begin{cases} \dfrac{q^{n-k}(q-1)^2(q^{n-k+1}-1)}{2} & \text{if } \nu = \frac{n-1}{2}; \\ \dfrac{q^{n-k}(q-1)^2(q^{\frac{n-k}{2}}-1)(q^{\frac{n-k+2}{2}}-1)}{2} & \text{if } \nu = \frac{n}{2}; \\ \dfrac{q^{n-k}(q-1)^2(q^{\frac{n-k}{2}}+1)(q^{\frac{n-k+2}{2}}+1)}{2} & \text{if } \nu = \frac{n-2}{2}. \end{cases}$$

From this, it follows that the k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace U of $\mathbb{F}_q^n$ having the Witt index $\frac{k-2}{2}$ has a Witt decomposition of the form

$$U = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{k-2}{2}}, b_{\frac{k-2}{2}}\rangle \perp \langle w_1, w_2\rangle,$$

where (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_q^n$ for $1 \le i \le \frac{k-2}{2}$ and $\{w_1, w_2\}$ is an orthogonal basis of the 2-dimensional anisotropic $\mathbb{F}_q$-linear subspace U_k of U.

The set $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-2}{2}}, b_{\frac{k-2}{2}}, w_1, w_2\}$ is called a Witt basis of U over $\mathbb{F}_q$. We next observe that

$$\widetilde{\mathcal{S}}_q(n;k) = \mathcal{D}_{\frac{k-2}{2},\nu}/\mathcal{D}_{\frac{k-2}{2}},$$

where $\mathcal{D}_{\frac{k-2}{2},\nu}$ is the number of distinct Witt bases of the form $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-2}{2}}, b_{\frac{k-2}{2}}, w_1, w_2\}$ in $\mathbb{F}_q^n$ and $\mathcal{D}_{\frac{k-2}{2}}$ is the number of distinct Witt bases of a k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ having the Witt index $\frac{k-2}{2}$. Now by applying Theorems 2.3.2, 2.3.5 and 2.3.6(d), we see that

$$\mathcal{D}_{\frac{k-2}{2},\nu} = \mathcal{H}_{\nu,n-2\nu}\mathcal{H}_{\nu-1,n-2\nu}\cdots\mathcal{H}_{\nu-\frac{(k-4)}{2},n-2\nu}\mathfrak{A}_{k,\nu}$$

and that

$$\mathcal{D}_{\frac{k-2}{2}} = \mathcal{H}_{\frac{k-2}{2},2}\mathcal{H}_{\frac{k-4}{2},2}\cdots\mathcal{H}_{1,2}(q^2-1)(q-1).$$

Further, by Theorem 2.3.6, we obtain

$$\widetilde{\mathcal{S}}_q(n;k) = \begin{cases} \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}-1)}{2}\begin{bmatrix}(n-1)/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n-1}{2};\\ \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}-1)(q^{\frac{n-k}{2}}-1)}{2(q^{\frac{n}{2}}+1)}\begin{bmatrix}n/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n}{2};\\ \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}-1)(q^{\frac{n-k}{2}}+1)}{2(q^{\frac{n}{2}}-1)}\begin{bmatrix}n/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n-2}{2}.\end{cases}$$

We will next count all distinct k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^n$ having the Witt index $\frac{k}{2}$. In this case, we note that $\dim_{\mathbb{F}_q}(U_k) = 0$. This implies that the k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace U of $\mathbb{F}_q^n$ having the Witt index $\frac{k}{2}$ has a Witt decomposition of the form

$$U = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{k}{2}}, b_{\frac{k}{2}}\rangle,$$

where (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_q^n$ for $1 \leq i \leq \frac{k}{2}$. The set $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k}{2}}, b_{\frac{k}{2}}\}$ is called a Witt basis of U over $\mathbb{F}_q$. This implies that

$$\widehat{\mathcal{S}}_q(n;k) = \mathcal{D}_{\frac{k}{2},\nu}/\mathcal{D}_{\frac{k}{2}},$$

where $\mathcal{D}_{\frac{k}{2},\nu}$ is the number of Witt bases of the type $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k}{2}}, b_{\frac{k}{2}}\}$ in $\mathbb{F}_q^n$ and $\mathcal{D}_{\frac{k}{2}}$ is the number of Witt bases of a k-dimensional non-degenerate quadratic $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ having the Witt index $\frac{k}{2}$. Further, by applying Theorems 2.3.2, 2.3.5 and 2.3.6(d), we see that

$$\mathcal{D}_{\frac{k}{2},\nu} = \mathcal{H}_{\nu,n-2\nu}\mathcal{H}_{\nu-1,n-2\nu}\cdots\mathcal{H}_{\nu-\frac{(k-2)}{2},n-2\nu}$$

and

$$\mathcal{D}_{\frac{k}{2}} = \mathcal{H}_{\frac{k}{2},0}\mathcal{H}_{\frac{k-2}{2},0}\cdots\mathcal{H}_{1,0}.$$

Now by Theorem 2.3.6, we get

$$\widehat{\mathcal{S}}_q(n;k) = \begin{cases} \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}+1)}{2}\begin{bmatrix}(n-1)/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n-1}{2};\\ \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}+1)(q^{\frac{n-k}{2}}+1)}{2(q^{\frac{n}{2}}+1)}\begin{bmatrix}n/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n}{2};\\ \dfrac{q^{\frac{k(n-k)}{2}}(q^{\frac{k}{2}}+1)(q^{\frac{n-k}{2}}-1)}{2(q^{\frac{n}{2}}-1)}\begin{bmatrix}n/2\\ k/2\end{bmatrix}_{q^2} & \text{if } \nu = \frac{n-2}{2}.\end{cases}$$

From this and by Theorem 2.3.6(a), the desired result follows immediately in the case when k is even.

□

In the following theorem, we provide the explicit enumeration formulae for all distinct σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$.

Theorem 6.3.4. *Let $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$ be fixed. For $0 \leq k \leq n$, let $\mathcal{Q}_{p^r}(n;k)$ denote the number of distinct σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$. Here we have $\mathcal{Q}_{p^r}(n;0) = \mathcal{Q}_{p^r}(n;n) = 1$. Further, for $1 \leq k \leq n-1$, we have the following:*

(a) When $p = 2$, we have

$$\mathcal{Q}_{2^r}(n;k) = \begin{cases} 2^{\frac{r(n-k)(2ke-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{2^{2r}} & \textit{if both } k \textit{ and } n \textit{ are odd;} \\ 2^{\frac{r(k(n-k)(2e-1)+n-1)}{2}} \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{2^{2r}} & \textit{if } k \textit{ is odd and } n \textit{ is even;} \\ 2^{\frac{rk((n-k)(2e-1)+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{2^{2r}} & \textit{if } k \textit{ is even and } n \textit{ is odd;} \\ 2^{\frac{r(k(n-k)(2e-1)-2)}{2}} \Big((2^{rk} + 2^r - 1) \begin{bmatrix} (n-2)/2 \\ k/2 \end{bmatrix}_{2^{2r}} & \\ +(2^{r(n-k+1)} - 2^{r(n-k)} + 1) \begin{bmatrix} (n-2)/2 \\ (k-2)/2 \end{bmatrix}_{2^{2r}} \Big) & \textit{if both } k \textit{ and } n \textit{ are even.} \end{cases}$$

(b) When p is an odd prime, we have

$$\mathcal{Q}_{p^r}(n;k) = \begin{cases} p^{\frac{r(n-k)(2ke-k+1)}{2}} \begin{bmatrix} (n-1)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \textit{if both } k \textit{ and } n \textit{ are odd;} \\ p^{\frac{r(k(n-k)(2e-1)-1)}{2}} (p^{\frac{rn}{2}} - 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \textit{if } k \textit{ is odd and } n \textit{ is even with} \\ & \textit{either } p^r \equiv 3 \pmod 4 \textit{ and} \\ & n \equiv 0 \pmod 4 \textit{ or } p^r \equiv 1 \pmod 4; \\ p^{\frac{r(k(n-k)(2e-1)-1)}{2}} (p^{\frac{rn}{2}} + 1) \begin{bmatrix} (n-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \textit{if } k \textit{ is odd, } p^r \equiv 3 \pmod 4 \\ & \textit{and } n \equiv 2 \pmod 4; \\ p^{\frac{rk((n-k)(2e-1)+1)}{2}} \begin{bmatrix} (n-1)/2 \\ k/2 \end{bmatrix}_{p^{2r}} & \textit{if } k \textit{ is even and } n \textit{ is odd;} \\ p^{\frac{rk(n-k)(2e-1)}{2}} \begin{bmatrix} n/2 \\ k/2 \end{bmatrix}_{p^{2r}} & \textit{if both } k \textit{ and } n \textit{ are even.} \end{cases}$$

Proof. To prove the result, we see, by Theorem 6.2.3, that a linear code $\mathcal{D}$ of length n and rank k over $\mathcal{R}_{e,r}$ is a σ-LCD code if and only if $\mathcal{D}$ is a free code and its Torsion code $Tor_1(\mathcal{D})$ is a k-dimensional $\overline{\sigma}$-LCD code of length n over $\overline{\mathcal{R}}_{e,r}$. Further, we see, by Theorem 6.3.1, that there are precisely $p^{rk(n-k)(e-1)}$ distinct σ-LCD codes of length n over $\mathcal{R}_{e,r}$ with a prescribed Torsion code. Therefore if $\mathcal{L}_{p^r}(n;k)$ denotes the number of distinct Euclidean LCD (or $\overline{\sigma}$-LCD) codes of length n and dimension k over $\overline{\mathcal{R}}_{e,r}(\simeq \mathbb{F}_{p^r})$, then the total number of distinct σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$ is given by

$$\mathcal{Q}_{p^r}(n;k) = \mathcal{L}_{p^r}(n;k) p^{rk(n-k)(e-1)}.$$

Now on substituting the values of the number $\mathcal{L}_{p^r}(n;k)$ from Theorems 6.3.2 and 6.3.3 in the respective cases, we get the desired result. □

In the following theorem, we provide the explicit enumeration formulae for all σ-LCD codes of length n over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$.

Theorem 6.3.5. *Let $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$ be fixed. Let $\mathcal{Q}_{p^r}(n)$ denote the number of distinct σ-LCD codes of length n over $\mathcal{R}_{e,r}$.*

(a) When p is an odd prime, we have

$$\mathcal{Q}_{p^r}(n)=\begin{cases} 2+\sum\limits_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(n-k)(2ke-k+1)}{2}} \begin{bmatrix}(n-1)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}+\sum\limits_{\substack{k=1\\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk((n-k)(2e-1)+1)}{2}} \begin{bmatrix}(n-1)/2\\k/2\end{bmatrix}_{p^{2r}} \\ \textit{if } n \textit{ is odd;} \\ 2+\sum\limits_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(k(n-k)(2e-1)-1)}{2}} (p^{\frac{rn}{2}}-1) \begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}+\sum\limits_{\substack{k=1\\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk(n-k)(2e-1)}{2}} \begin{bmatrix}n/2\\k/2\end{bmatrix}_{p^{2r}} \\ \textit{if } n \textit{ is even with either } p^r\equiv 1 \pmod 4 \textit{ or } n\equiv 0 \pmod 4 \textit{ and } p^r\equiv 3 \pmod 4; \\ 2+\sum\limits_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{n-1} p^{\frac{r(k(n-k)(2e-1)-1)}{2}} (p^{\frac{rn}{2}}+1) \begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}+\sum\limits_{\substack{k=1\\ k\equiv 0 \pmod 2}}^{n-1} p^{\frac{rk(n-k)(2e-1)}{2}} \begin{bmatrix}n/2\\k/2\end{bmatrix}_{p^{2r}} \\ \textit{if } p^r\equiv 3 \pmod 4 \textit{ and } n\equiv 2 \pmod 4. \end{cases}$$

(b) When $p=2$, we have

$$\mathcal{Q}_{2^r}(n)=\begin{cases} 2+\sum\limits_{\substack{k=1\\ k\equiv 0 \pmod 2}}^{n-1} 2^{\frac{rk((n-k)(2e-1)+1)}{2}} \begin{bmatrix}(n-1)/2\\k/2\end{bmatrix}_{2^{2r}}+\sum\limits_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{n-1} 2^{\frac{r(n-k)(2ke-k+1)}{2}} \begin{bmatrix}(n-1)/2\\(k-1)/2\end{bmatrix}_{2^{2r}} \\ \textit{if } n \textit{ is odd;} \\ 2+\sum\limits_{\substack{k=1\\ k\equiv 0 \pmod 2}}^{n-1} 2^{\frac{r(k(n-k)(2e-1)-2)}{2}} \Big((2^{r(n-k+1)}-2^{r(n-k)}+1) \begin{bmatrix}(n-2)/2\\(k-2)/2\end{bmatrix}_{2^{2r}} \\ +(2^{rk}+2^r-1)\begin{bmatrix}(n-2)/2\\k/2\end{bmatrix}_{2^{2r}}\Big)+\sum\limits_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{n-1} 2^{\frac{r(k(n-k)(2e-1)+n-1)}{2}} \begin{bmatrix}(n-2)/2\\(k-1)/2\end{bmatrix}_{2^{2r}} \\ \textit{if } n \textit{ is even.} \end{cases}$$

Proof. It follows immediately from Theorem 6.3.4. □

6.3.2 The case $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$

Here we recall, by Corollary 2.1.2, that $Aut_2(\mathcal{R}_{e,r}) = \emptyset$ when r is odd. So we assume, throughout this section, that $r \geq 2$ is an even integer and $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$, *i.e.*, σ_0 is an automorphism of $\mathcal{R}_{e,r}$ such that $\overline{\sigma}_0$ is the automorphism of $\overline{\mathcal{R}}_{e,r} (\simeq \mathbb{F}_{p^r})$ of order 2. Now to count all σ-LCD codes of length n over $\mathcal{R}_{e,r}$, we first enumerate all distinct k-dimensional Hermitian LCD codes of length n over the finite field $\mathbb{F}_{q^2}$ of order q^2 in the following theorem.

Theorem 6.3.6. *For $0 \leq k \leq n$, let $\widehat{\mathcal{L}}_{q^2}(n;k)$ denote the number of distinct k-dimensional Hermitian LCD codes of length n over $\mathbb{F}_{q^2}$. Then we have $\widehat{\mathcal{L}}_{q^2}(n;0) = \widehat{\mathcal{L}}_{q^2}(n;n) = 1$. Further, for $1 \leq k \leq n-1$, we have*

$$\widehat{\mathcal{L}}_{q^2}(n;k) = q^{k(n-k)} \prod_{\upsilon=0}^{k-1} \left(\frac{q^{n-\upsilon} - (-1)^{n-\upsilon}}{q^{k-\upsilon} - (-1)^{k-\upsilon}} \right).$$

Proof. To prove the result, let $[\cdot,\cdot]_\delta$ denote the Hermitian δ-sesquilinear form on $\mathbb{F}_{q^2}^n$, where δ is the automorphism of $\mathbb{F}_{q^2}$ of order 2. One can easily observe that the formed space $(\mathbb{F}_{q^2}^n, [\cdot,\cdot]_\delta)$ is an n-dimensional unitary space over $\mathbb{F}_{q^2}$. Further, by Theorem 2.3.4(a), we see that the Witt index ν of the unitary space $(\mathbb{F}_{q^2}^n, [\cdot,\cdot]_\delta)$ is given by

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

We next observe that each Hermitian LCD code of length n and dimension k over $\mathbb{F}_{q^2}$ can be viewed as a k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspace of $\mathbb{F}_{q^2}^n$. In view of this, the number $\widehat{\mathcal{L}}_{q^2}(n;k)$ equals the number of distinct k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspaces of the n-dimensional unitary space $(\mathbb{F}_{q^2}^n, [\cdot,\cdot]_\delta)$.

First of all, we observe that $\widehat{\mathcal{L}}_{q^2}(n;0) = \widehat{\mathcal{L}}_{q^2}(n;n) = 1$. So from this point on, we assume that $1 \leq k \leq n-1$. Now to determine the number $\widehat{\mathcal{L}}_{q^2}(n;k)$, we see, by Theorem 2.3.4(b), that a k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspace U of $\mathbb{F}_{q^2}^n$ has a Witt decomposition of the form

$$U = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\nu_k}, b_{\nu_k} \rangle \perp U_k,$$

where ν_k is the Witt index of U, (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_{q^2}^n$ for $1 \leq i \leq \nu_k$, and

U_k is an anisotropic $\mathbb{F}_{q^2}$-linear subspace of $\mathbb{F}_{q^2}^n$ satisfying $\dim_{\mathbb{F}_{q^2}}(U_k) = k - 2\nu_k \leq 1$. Now we shall distinguish the following two cases: (i) k is odd and (ii) k is even.

(i) First let k be odd. Here we see that the k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspace U of $\mathbb{F}_{q^2}^n$ has a Witt decomposition of the form $U = \langle a_1, b_1\rangle \perp \langle a_2, b_2\rangle \perp \cdots \perp \langle a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}\rangle \perp \langle w\rangle$, where (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_{q^2}^n$ for $1 \leq i \leq \frac{k-1}{2}$ and w is an anisotropic vector in $\mathbb{F}_{q^2}^n$. The basis set $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}, w\}$ is called a Witt basis of U. Now one can easily observe that the number of distinct Witt bases of the type $\{a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}, w\}$ in $\mathbb{F}_{q^2}^n$ is given by

$$\begin{aligned}\mathcal{D}_{n,k} = \mathcal{H}_{\varphi_1,n-2\varphi_1}\mathcal{H}_{\varphi_2,n-2-2\varphi_2}\mathcal{H}_{\varphi_3,n-4-2\varphi_3}\cdots\mathcal{H}_{\varphi_{\frac{k-1}{2}},n-k+3-2\varphi_{\frac{k-1}{2}}}\\ \times\Big(q^{2(n-k+1)} - 1 - \mathcal{I}_{\varphi_{\frac{k+1}{2}},n-k+1-2\varphi_{\frac{k+1}{2}}}\Big),\end{aligned}$$

where φ_i denotes the Witt index of the unitary space $\langle a_1, b_1, a_2, b_2, \ldots, a_{i-1}, b_{i-1}\rangle^{\perp_\delta}$ and $\mathcal{H}_{\varphi_i,n-2i+2-2\varphi_i}$ denotes the number of hyperbolic pairs in the unitary space $\langle a_1, b_1, a_2, b_2, \ldots, a_{i-1}, b_{i-1}\rangle^{\perp_\delta}$ for $1 \leq i \leq \frac{k+1}{2}$, and $\mathcal{I}_{\varphi_{\frac{k+1}{2}},n-k+1-2\varphi_{\frac{k+1}{2}}}$ denotes the number of isotropic vectors in the unitary space $\langle a_1, b_1, a_2, b_2, \ldots, a_{\frac{k-1}{2}}, b_{\frac{k-1}{2}}\rangle^{\perp_\delta}$. Now by Theorem 2.3.4, we get

$$\mathcal{D}_{n,k} = q^{\frac{k(2n-k-1)}{2}}(q-1)\prod_{i=0}^{k-1}\big(q^{n-i} - (-1)^{n-i}\big).$$

Further, working in a similar manner as above and by applying Theorem 2.3.4, we see that the number of distinct Witt bases of a k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspace of $\mathbb{F}_{q^2}^n$ is given by

$$\mathcal{D}_{k,k} = \mathcal{H}_{\frac{k-1}{2},1}\mathcal{H}_{\frac{k-3}{2},1}\cdots\mathcal{H}_{1,1}(q^2-1) = q^{\frac{k(k-1)}{2}}(q-1)\prod_{i=0}^{k-1}(q^{k-i} - (-1)^{k-i}).$$

From this, we obtain

$$\widehat{\mathcal{L}}_{q^2}(n;k) = \frac{\mathcal{D}_{n,k}}{\mathcal{D}_{k,k}} = q^{k(n-k)}\prod_{\upsilon=0}^{k-1}\left(\frac{q^{n-\upsilon} - (-1)^{n-\upsilon}}{q^{k-\upsilon} - (-1)^{k-\upsilon}}\right).$$

(ii) When k is even, we see that the k-dimensional unitary $\mathbb{F}_{q^2}$-linear subspace U of $\mathbb{F}_{q^2}^n$ has a Witt decomposition of the form

$$U = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\frac{k}{2}}, b_{\frac{k}{2}} \rangle,$$

where (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_{q^2}^n$ for $1 \leq i \leq \frac{k}{2}$. Now working in a similar manner as in case (i) and by applying Theorem 2.3.4, the desired result follows.

□

In the following theorem, we provide the explicit enumeration formula for all σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$.

Theorem 6.3.7. *Let the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ be of order p^r, where p is a prime number and $r \geq 2$ is an even integer. Let $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$ be fixed. For $0 \leq k \leq n$, let $\widehat{\mathcal{Q}}_{p^r}(n;k)$ denote the number of distinct σ-LCD codes of length n and rank k over $\mathcal{R}_{e,r}$. Then we have $\widehat{\mathcal{Q}}_{p^r}(n;0) = \widehat{\mathcal{Q}}_{p^r}(n;n) = 1$. Further, for $1 \leq k \leq n-1$, we have*

$$\widehat{\mathcal{Q}}_{p^r}(n;k) = p^{\frac{rk(n-k)(2e-1)}{2}} \prod_{v=0}^{k-1} \left(\frac{p^{\frac{r(n-v)}{2}} - (-1)^{n-v}}{p^{\frac{r(k-v)}{2}} - (-1)^{k-v}} \right).$$

Proof. Working in a similar manner as in Theorem 6.3.4 and by applying Theorem 6.3.6, the desired result follows. □

In the following theorem, we provide the explicit enumeration formula for all σ-LCD codes of length n over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$.

Theorem 6.3.8. *Let the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ be of order p^r, where p is a prime number and $r \geq 2$ is an even integer. Let $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$ be fixed. The number $\widehat{\mathcal{Q}}_{p^r}(n)$ of distinct σ-LCD codes of length n over $\mathcal{R}_{e,r}$ is given by*

$$\widehat{\mathcal{Q}}_{p^r}(n) = 2 + \sum_{k=1}^{n-1} p^{\frac{rk(n-k)(2e-1)}{2}} \prod_{v=0}^{k-1} \left(\frac{p^{\frac{r(n-v)}{2}} - (-1)^{n-v}}{p^{\frac{r(k-v)}{2}} - (-1)^{k-v}} \right).$$

Proof. It follows immediately from Theorem 6.3.7. □

6.4 The class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good

In this section, we will show that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good. To do this, we recall that the Hamming distance of a linear code C of length n over $\mathcal{R}_{e,r}$ is the smallest of the Hamming weights of its non-zero codewords. From now on, we shall refer to a linear code C of length n, rank k and Hamming distance d over $\mathcal{R}_{e,r}$ as a linear $[n,k,d]$-code over $\mathcal{R}_{e,r}$.

Now let $\mathfrak{F} = \{C_1, C_2, \ldots\ldots\}$ be a sequence of codes, where the code C_i is a free linear $[n_i, k_i, d_i]$-code over $\mathcal{R}_{e,r}$ such that $\lim\limits_{i\to\infty} n_i = \infty$. The rate $\mathfrak{R}$ of the sequence $\mathfrak{F}$ is defined as

$$\mathfrak{R} = \limsup_{i\to\infty} \frac{k_i}{n_i}$$

and the relative distance Δ of the sequence $\mathfrak{F}$ is defined as

$$\Delta = \liminf_{i\to\infty} \frac{d_i}{n_i}.$$

The family $\mathfrak{F}$ of linear codes over $\mathcal{R}_{e,r}$ is said to be asymptotically good if it satisfies $\mathfrak{R}\Delta > 0$.

In the following proposition, we provide a method to construct a σ-LCD code over $\mathcal{R}_{e,r}$ from a linear code over the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$.

Proposition 6.4.1. *Let $\mathcal{C}'$ be a linear $[n,k,d']$-code over $\overline{\mathcal{R}}_{e,r}$. Then there exists a σ-LCD $[N,k,d]$-code over the chain ring $\mathcal{R}_{e,r}$, where $d \geq d'$ and*

$$N = \begin{cases} 2n-k & \textit{if } p = 2; \\ 4n-3k & \textit{if } p \textit{ is an odd prime.} \end{cases}$$

Proof. To prove the result, without any loss of generality, let us suppose that $\mathcal{C}'$ is a linear code whose generator matrix G' is in the standard form

$$G' = \left[\ \overline{I}_k \mid A_0 \right],$$

where $\overline{I}_k$ denotes the $k \times k$ identity matrix and A_0 is a $k \times (n-k)$ matrix over $\overline{\mathcal{R}}_{e,r}$. As the mapping $^{-} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection, there exists a unique $k \times (n-k)$

matrix A over $\mathcal{T}_{e,r}$ such that $\overline{A} = A_0$. Now we shall distinguish the following two cases: (i) $p = 2$ and (ii) p is an odd prime.

(i) Let $p = 2$. Let us consider the linear code $\mathcal{C}$ over $\mathcal{R}_{e,r}$ with a generator matrix

$$G = \Big[I_k \mid A + uA \mid A + uA \Big].$$

Now by applying Theorem 6.2.3, we observe that the code $\mathcal{C}$ is a σ-LCD $[2n - k, k, d]$-code over $\mathcal{R}_{e,r}$. Further, one can easily observe that $d \geq d'$.

(ii) Let p be an odd prime. Here by Lagrange's Four-Square Theorem, we see that there exist non-negative integers a_0, b_0, c_0 and d_0 (not all zero) such that $p = a_0^2 + b_0^2 + c_0^2 + d_0^2$. This implies that $\overline{a}_0^2 + \overline{b}_0^2 + \overline{c}_0^2 + \overline{d}_0^2 = \overline{0}$ in $\overline{\mathcal{R}}_{e,r}$. We further see that the elements $\overline{a}_0, \overline{b}_0, \overline{c}_0, \overline{d}_0$ in $\overline{\mathcal{R}}_{e,r}$ are not all zero. Since the mapping $\overline{} : \mathcal{T}_{e,r} \to \overline{\mathcal{R}}_{e,r}$ is a bijection, there exist unique elements a, b, c, $d \in \mathcal{T}_{e,r}$ such that $\overline{a} = \overline{a}_0$, $\overline{b} = \overline{b}_0$, $\overline{c} = \overline{c}_0$ and $\overline{d} = \overline{d}_0$. Now let us consider the linear code $\mathcal{C}$ over $\mathcal{R}_{e,r}$ with a generator matrix

$$G = \Big[I_k \mid aA + uA \mid bA + uA \mid cA + uA \mid dA + uA \Big].$$

We next observe that

$$\overline{G} = \Big[\ \overline{I}_k \mid \overline{a}_0 A_0 \mid \overline{b}_0 A_0 \mid \overline{c}_0 A_0 \mid \overline{d}_0 A_0 \Big],$$

$\overline{\sigma}_0(\overline{a}_0) = \overline{a}_0$, $\overline{\sigma}_0(\overline{b}_0) = \overline{b}_0$, $\overline{\sigma}_0(\overline{c}_0) = \overline{c}_0$ and $\overline{\sigma}_0(\overline{d}_0) = \overline{d}_0$. From this and by applying Theorem 6.2.3 again, we observe that the code $\mathcal{C}$ is a σ-LCD $[4n - 3k, k, d]$-code over $\mathcal{R}_{e,r}$. Further, one can easily observe that $d \geq d'$.

This completes the proof of the theorem. □

In the following theorem, we show that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good.

Theorem 6.4.1. *The class of σ-LCD codes over $\mathcal{R}_{e,r}$ is asymptotically good.*

Proof. To prove the result, we see, by Theorem 3 of Sendrier [89], that the class of linear codes over $\overline{\mathcal{R}}_{e,r}$ is asymptotically good. Further, by Proposition 6.4.1, we see that corresponding to a linear $[n, k, d']$-code over $\overline{\mathcal{R}}_{e,r}$, we can construct a σ-LCD $[N, k, d]$-code over $\mathcal{R}_{e,r}$, where $d \geq d'$, and $N = 2n - k$ if $p = 2$, while $N = 4n - 3k$ if p is an odd prime. From this, it follows that the class of σ-LCD codes over $\mathcal{R}_{e,r}$ is also asymptotically good. □

In the following theorem, we show that a linear code C over $\mathcal{R}_{e,r}$ is a σ-LCD MDS code if and only if its σ-dual code $C^{\perp_\sigma}$ is a σ^{-1}-LCD MDS code.

Theorem 6.4.2. *A linear code C of length n over $\mathcal{R}_{e,r}$ is a σ-LCD MDS code if and only if its σ-dual code $C^{\perp_\sigma}$ is a σ^{-1}-LCD MDS code.*

Proof. To prove the result, we see, by applying Theorem 5.3 of Norton and Sălăgean [81] and by Theorem 6.2.3, that the σ-LCD code C is an MDS $[n, k, d]$-code over $\mathcal{R}_{e,r}$ if and only if the code C is a free code and its Torsion code $Tor_1(C)$ is a $\overline{\sigma}$-LCD MDS $[n, k, d]$-code over $\overline{\mathcal{R}}_{e,r}$. We next observe that the Torsion code $Tor_1(C)$ is a $\overline{\sigma}$-LCD code if and only if its $\overline{\sigma}$-dual code $Tor_1(C)^{\perp_{\overline{\sigma}}}$ is a $\overline{\sigma}^{-1}$-LCD code over $\overline{\mathcal{R}}_{e,r}$. Now by applying Proposition 2.10 of Liu *et al.* [64] and using the fact that $\overline{\sigma}\big(Tor_1(C)\big) = Tor_1\big(\sigma(C)\big)$, we see that the Torsion code $Tor_1(C)$ is a $\overline{\sigma}$-LCD MDS $[n, k, d]$-code over $\overline{\mathcal{R}}_{e,r}$ if and only if the code $Tor_1(C)^{\perp_{\overline{\sigma}}} = Tor_1\big(\sigma(C)\big)^{\perp}$ is a $\overline{\sigma}^{-1}$-LCD MDS $[n, n-k, k+1]$-code over $\overline{\mathcal{R}}_{e,r}$, where $Tor_1\big(\sigma(C)\big)^{\perp}$ denotes the Euclidean dual code of the code $Tor_1\big(\sigma(C)\big)$. Next, by applying Theorem 3.10(ii) of Norton and Sălăgean [80], we see that

$$Tor_1\big(\sigma(C)\big)^{\perp} = Tor_1\big(\sigma(C)^{\perp}\big) = Tor_1(C^{\perp_\sigma}).$$

From this, it follows that the code C is a σ-LCD MDS $[n, k, d]$-code over $\mathcal{R}_{e,r}$ if and only if the code $C^{\perp_\sigma}$ is a free code and the code $Tor_1(C^{\perp_\sigma})$ is a $\overline{\sigma}^{-1}$-LCD MDS $[n, n-k, k+1]$-code over $\overline{\mathcal{R}}_{e,r}$, which, by applying Theorem 5.3 of Norton and Sălăgean [81] and Theorem 6.2.3 again, holds if and only if the code $C^{\perp_\sigma}$ is a σ^{-1}-LCD MDS $[n, n-k, k+1]$-code over $\mathcal{R}_{e,r}$. From this, the desired result follows. □

6.5 Classification of σ-LCD codes over $\mathcal{R}_{e,r}$

We first recall that two linear codes of length n over $\mathcal{R}_{e,r}$ are monomially equivalent if a generator matrix of one code can be obtained from the generator matrix of the other code by post multiplying it with an $n \times n$ monomial matrix. Otherwise, these two codes are said to be inequivalent.

In a recent work, Carlet *et al.* [29] showed that every linear code over the finite field $\mathbb{F}_q$ is equivalent to a Euclidean LCD code over $\mathbb{F}_q$ when $q > 3$, and that every linear code over $\mathbb{F}_{q^2}$ is equivalent to a Hermitian LCD code over $\mathbb{F}_{q^2}$ when $q > 2$. In the following theorem, we extend this result to σ-LCD codes over $\mathcal{R}_{e,r}$.

Theorem 6.5.1. *Let the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ be of order $p^r > 4$, where p is a prime number and r is a positive integer. Let $\mathcal{C}$ be a free linear $[n,k,d]$-code over $\mathcal{R}_{e,r}$. Then there exists a word $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ of length n over the unit group $\mathcal{R}^*_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ such that the linear code $\mathcal{C}_\beta$, defined as*

$$\mathcal{C}_\beta = \{(\beta_1 c_1, \beta_2 c_2, \ldots, \beta_n c_n) \in \mathcal{R}^n_{e,r} \ : \ (c_1, c_2, \ldots, c_n) \in \mathcal{C}\},$$

is a σ-LCD $[n,k,d]$-code over $\mathcal{R}_{e,r}$.

Proof. To prove the result, without any loss of generality, let $\mathcal{C}$ be a free linear $[n,k,d]$-code over $\mathcal{R}_{e,r}$ with a generator matrix $G = \Big[I_k \mid A \Big]$, where A is a $k \times (n-k)$ matrix over $\mathcal{R}_{e,r}$. It is easy to see that its Torsion code $\mathcal{D} = Tor_1(\mathcal{C})$ is a linear $[n,k,d]$-code over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix $\overline{G} = \Big[\ \overline{I}_k \mid \overline{A} \ \Big]$. Working in a similar manner as in Theorem 16 and Corollary 18 of Carlet *et al.* [29], we see that there exists a word $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ of length n over $\overline{\mathcal{R}}_{e,r} \setminus \{0\}$ such that the code

$$\mathcal{D}_\alpha = \{(\alpha_1 d_1, \alpha_2 d_2, \ldots, \alpha_n d_n) \in \overline{\mathcal{R}}^n_{e,r} \ : \ (d_1, d_2, \ldots, d_n) \in \mathcal{D}\}$$

is a $\overline{\sigma}$-LCD $[n,k,d]$-code over $\overline{\mathcal{R}}_{e,r}$. Now corresponding to the word $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, we observe that there exists a word $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ of length n over $\mathcal{R}^*_{e,r}$ such that $\overline{\beta}_i = \alpha_i$ for $1 \leq i \leq n$. Further, let us consider the code $\mathcal{C}_\beta$ of length n over $\mathcal{R}_{e,r}$, defined as

$$\mathcal{C}_\beta = \{(\beta_1 c_1, \beta_2 c_2, \ldots, \beta_n c_n) \in \mathcal{R}^n_{e,r} \ : \ (c_1, c_2, \ldots, c_n) \in \mathcal{C}\}.$$

It is easy to see that $Tor_1(\mathcal{C}_\beta) = \mathcal{D}_\alpha$. From this and by applying Theorem 6.2.3, we see that the code $\mathcal{C}_\beta$ is a σ-LCD $[n, k, d]$-code over $\mathcal{R}_{e,r}$. □

6.5.1 Classification of σ-LCD $[n, 1, d]$-codes and $[n, n-1, d]$-codes over $\mathcal{R}_{e,r}$

Let $\mathcal{B}(n, k)$ denote the set consisting of all inequivalent σ-LCD $[n, k]$-codes over the chain ring $\mathcal{R}_{e,r}$, and let $\mathcal{B}(n, k, d)$ denote the set of all inequivalent σ-LCD $[n, k, d]$-codes over the chain ring $\mathcal{R}_{e,r}$, where $1 \le k, d \le n$ and $\sigma_0 \in Aut(\mathcal{R}_{e,r})$. Note that

$$\mathcal{B}(n,k) = \bigcup_{d=1}^{n} \mathcal{B}(n,k,d) \text{ (a disjoint union)} \quad \text{for } 1 \le k \le n. \tag{6.5.1}$$

In this section, we shall explicitly determine the sets $\mathcal{B}(n, k)$ and $\mathcal{B}(n, k, d)$ for $1 \le d \le n$ when $k \in \{1, n-1\}$. To do this, for $a = (a_1, a_2, \ldots, a_n) \in \mathcal{R}_{e,r}^n$, let $\mathcal{C}_n(a)$ denote the linear $[n, 1]$-code over $\mathcal{R}_{e,r}$ with a generator matrix $[a_1\ a_2\ \cdots\ a_n]$. Next for an integer $j \ge 1$, let Y_j denote the set of all j-tuples $(i_1, i_2, \ldots, i_j)$ of integers $i_1, i_2, \ldots, i_j$ satisfying $1 \le i_1 \le i_2 \le \cdots \le i_j \le e$. In the following lemma, we determine the cardinality of the set Y_j.

Lemma 6.5.1. *For an integer $j \ge 1$, we have*

$$|Y_j| = \frac{e(e+1)\cdots(e+j-1)}{j!} = \binom{e+j-1}{j}.$$

Proof. Its proof is a straightforward exercise. □

We recall that the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ is of order p^r, where p is a prime number and r is a positive integer. Next, we see, by Theorem 2.21 of [62], that $Aut(\mathcal{R}_{e,r}) = Aut_1(\mathcal{R}_{e,r})$ when $p^r = |\overline{\mathcal{R}}_{e,r}|$ is either 2 or 3 (or equivalently, when $r = 1$ and $p \in \{2, 3\}$), while $Aut(\mathcal{R}_{e,r}) = Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$ when $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ (or equivalently, when $p = r = 2$).

In the following theorem, we explicitly determine the sets $\mathcal{B}(n, 1, d)$, $\mathcal{B}(n, n-1, d)$ for $1 \le d \le n$, $\mathcal{B}(n, 1)$ and $\mathcal{B}(n, n-1)$ when either $p^r = |\overline{\mathcal{R}}_{e,r}| \in \{2, 3\}$ and $\sigma_0 \in Aut(\mathcal{R}_{e,r}) = Aut_1(\mathcal{R}_{e,r})$ or $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ and $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$.

Theorem 6.5.2. *Suppose that either* $p^r = |\overline{\mathcal{R}}_{e,r}| \in \{2,3\}$ *and* $\sigma_0 \in Aut(\mathcal{R}_{e,r})$ *or* $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ *and* $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$.

(a) For $1 \le d \le n$, *we have*

$$\mathcal{B}(n,1,d) = \begin{cases} \{\mathcal{C}_n(1,1,\dots,1,u^{i_1},u^{i_2},\dots,u^{i_{n-d}}) \ : \ (i_1,i_2,\dots,i_{n-d}) \in Y_{n-d}\} \\ \text{if } d \not\equiv 0 \pmod{p}; \\ \emptyset \qquad \text{otherwise.} \end{cases}$$

As a consequence, we have

$$|\mathcal{B}(n,1,d)| = \begin{cases} \binom{e+n-d-1}{n-d} & \text{if } d \not\equiv 0 \pmod{p}; \\ 0 & \text{otherwise} \end{cases}$$

for $1 \le d \le n$, *and*

$$|\mathcal{B}(n,1)| = |\mathcal{B}(n,n-1)| = \sum_{\substack{d=1 \\ d \not\equiv 0 \pmod{p}}}^{n} \binom{e+n-d-1}{n-d}.$$

(b) For $n \ge 2$ *and* $1 \le d \le n$, *we have*

$$\mathcal{B}(n,n-1,d) = \begin{cases} \{\mathcal{C}_n(1,1,\dots,1,u^{i_1},u^{i_2},\dots,u^{i_{n-j}})^{\perp_{\sigma^{-1}}} : \ (i_1,i_2,\dots,i_{n-j}) \in Y_{n-j}, \\ 1 \le j \le n-1 \text{ and } j \not\equiv 0 \pmod{p}\} & \text{if } d = 1; \\ \{\mathcal{C}_n(1,1,\dots,1)^{\perp_{\sigma^{-1}}}\} & \text{if } d = 2 \text{ and } n \not\equiv 0 \pmod{p}; \\ \emptyset & \text{otherwise.} \end{cases}$$

As a consequence, for $n \ge 2$ *and* $1 \le d \le n$, *we have*

$$|\mathcal{B}(n,n-1,d)| = \begin{cases} \sum_{\substack{j=1 \\ j \not\equiv 0 \pmod{p}}}^{n-1} \binom{e+n-j-1}{n-j} & \text{if } d = 1; \\ 1 & \text{if } d = 2 \text{ and } n \not\equiv 0 \pmod{p}; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. **(a)** When $p^r = |\overline{\mathcal{R}}_{e,r}|$ is either 2 or 3 and $\sigma_0 \in Aut(\mathcal{R}_{e,r})$, by Theorem 2.21 of

[62], we see that $Aut(\mathcal{R}_{e,r}) = Aut_1(\mathcal{R}_{e,r})$, *i.e.,* $\overline{\sigma}_0$ is the identity automorphism of $\overline{\mathcal{R}}_{e,r}$ for every automorphism σ_0 of $\mathcal{R}_{e,r}$. Further, by Propositions 4 and 5 of Araya and Harada [3], we note that there does not exist any $\overline{\sigma}$-LCD (or equivalently, Euclidean LCD) $[n, 1, d]$-code over $\overline{\mathcal{R}}_{e,r}$ when $d \equiv 0 \pmod{p}$, while up to equivalence, there exists a unique $\overline{\sigma}$-LCD $[n, 1, d]$-code over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix

$$\big[\underbrace{1\;1\;\cdots\;1}_{d}\;0\;0\;\cdots\;0\big] \quad \text{when } d \not\equiv 0 \pmod{p}.$$

On the other hand, when $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ and $\sigma_0 \in Aut_2(\mathcal{R}_{e,r})$, working as in Propositions 4 and 5 of Araya and Harada [3], we see that every $\overline{\sigma}$-LCD $[n, 1, d]$-code over $\overline{\mathcal{R}}_{e,r}$ is equivalent to the $\overline{\sigma}$-LCD code over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix

$$\big[\underbrace{1\;1\;\cdots\;1}_{d}\;0\;0\;\cdots\;0\big] \quad \text{when } d \not\equiv 0 \pmod{p},$$

while there does not exist any $\overline{\sigma}$-LCD $[n, 1, d]$-code over $\overline{\mathcal{R}}_{e,r}$ when $d \equiv 0 \pmod{p}$.

Now by applying Theorem 4.2(ii) of Norton and Sălăgean [81] and Theorem 6.2.3, we see that the set $\mathcal{B}(n, 1, d)$ is empty when $d \equiv 0 \pmod{p}$. Next, to determine the set $\mathcal{B}(n, 1, d)$ when $d \not\equiv 0 \pmod{p}$, we first observe that if $\mathcal{C}_1$ and $\mathcal{C}_2$ are two σ-LCD $[n, 1, d]$-codes over $\mathcal{R}_{e,r}$ such that their Torsion codes $Tor_1(\mathcal{C}_1)$ and $Tor_1(\mathcal{C}_2)$ over $\overline{\mathcal{R}}_{e,r}$ are inequivalent, then the codes $\mathcal{C}_1$ and $\mathcal{C}_2$ over $\mathcal{R}_{e,r}$ are inequivalent. Further, up to equivalence, we can assume that a σ-LCD $[n, 1, d]$-code over $\mathcal{R}_{e,r}$ has a generator matrix of the form

$$[1\;1\;\cdots\;1\;u^{i_1}\;u^{i_2}\;\cdots\;u^{i_{n-d}}],$$

where $(i_1, i_2, \ldots, i_{n-d}) \in Y_{n-d}$. We next observe that if $(i_1, i_2, \ldots, i_{n-d})$ and $(j_1, j_2, \ldots, j_{n-d})$ are distinct elements of Y_{n-d}, then the codes $\mathcal{C}_n(1, 1, \ldots, 1, u^{i_1}, u^{i_2}, \ldots, u^{i_{n-d}})$ and $\mathcal{C}_n(1, 1, \ldots, 1, u^{j_1}, u^{j_2}, \ldots, u^{j_{n-d}})$ over $\mathcal{R}_{e,r}$ are inequivalent.

From this, we obtain

$$\mathcal{B}(n,1,d) = \left\{\mathcal{C}_n(1,1,\ldots,1,u^{i_1},u^{i_2},\ldots,u^{i_{n-d}}) : (i_1,i_2,\ldots,i_{n-d}) \in Y_{n-d}\right\}$$

when $d \not\equiv 0 \pmod{p}$. Further, by Lemma 6.5.1, we get

$$|\mathcal{B}(n,1,d)| = |Y_{n-d}| = \frac{e(e+1)\cdots(e+n-d-1)}{(n-d)!} = \binom{e+n-d-1}{n-d}$$

when $d \not\equiv 0 \pmod{p}$. Finally, we observe that two σ-LCD codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of length n over $\mathcal{R}_{e,r}$ are equivalent if and only if their σ-dual codes $\mathcal{C}_1^{\perp_\sigma}$ and $\mathcal{C}_2^{\perp_\sigma}$ over $\mathcal{R}_{e,r}$ are equivalent, which implies that $|\mathcal{B}(n,n-1)| = |\mathcal{B}(n,1)|$. From this and by (6.5.1), part (a) follows immediately.

(b) We will next determine the set $\mathcal{B}(n,n-1,d)$ for $n \geq 2$ and $1 \leq d \leq n$. For this, we see that the code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)$ with $(a_1,a_2,\ldots,a_n) \in \mathcal{R}_{e,r}^n$ is a σ^{-1}-LCD $[n,1]$-code over $\mathcal{R}_{e,r}$ if and only if its σ^{-1}-dual code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)^{\perp_{\sigma^{-1}}}$ is a σ-LCD $[n,n-1]$-code over $\mathcal{R}_{e,r}$ with a parity-check matrix $[a_1\ a_2\ \cdots\ a_n]$. Further, by applying Theorem 4.2(ii) of Norton and Sălăgean [81] and Corollary 1.4.14 of [53], we observe that the σ^{-1}-dual code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)^{\perp_{\sigma^{-1}}}$ has Hamming distance at most 2. From this, it follows that

$$\mathcal{B}(n,n-1,d) = \emptyset \quad \text{when } d \geq 3.$$

Moreover, the code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)^{\perp_{\sigma^{-1}}}$ has Hamming distance 1 if and only if $\overline{a}_j = 0$ for some j but not all $\overline{a}_i$'s are zero, which, by Theorem 4.2(ii) of Norton and Sălăgean [81], holds if and only if the code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)$ has Hamming distance strictly less than n.

From this and by part (a), we get

$$\mathcal{B}(n,n-1,1) = \big\{\mathcal{C}_n(1,1,\ldots,1,u^{i_1},u^{i_2},\ldots,u^{i_{n-j}})^{\perp_{\sigma^{-1}}} : (i_1,i_2,\ldots,i_{n-j}) \in Y_{n-j},$$
$$1 \leq j \leq n-1 \text{ and } j \not\equiv 0 \pmod{p}\big\}.$$

Now to determine the set $\mathcal{B}(n,n-1,2)$, we see that the code $\mathcal{C}_n(a_1,a_2,\ldots,a_n)^{\perp_{\sigma^{-1}}}$ has Hamming distance 2 if and only if all $\overline{a}_i$'s are non-zero, which, by Theorem

4.2(ii) of Norton and Sălăgean [81], holds if and only if the code $\mathcal{C}_n(a_1, a_2, \ldots, a_n)$ has Hamming distance n. We next see that there exists a σ^{-1}-LCD $[n, 1, n]$-code over $\mathcal{R}_{e,r}$ if and only if $n \not\equiv 0 \pmod{p}$. Further, when $n \not\equiv 0 \pmod{p}$, there exists a unique σ^{-1}-LCD $[n, 1, n]$-code $\mathcal{C}_n(1, 1, \ldots, 1)$ over $\mathcal{R}_{e,r}$ up to equivalence. From this, we get $\mathcal{B}(n, n-1, 2) = \emptyset$ if $n \equiv 0 \pmod{p}$, while $\mathcal{B}(n, n-1, 2) = \{\mathcal{C}_n(1, 1, \ldots, 1)^{\perp_{\sigma^{-1}}}\}$ when $n \not\equiv 0 \pmod{p}$. This proves (b).

□

In the following theorem, we explicitly determine the sets $\mathcal{B}(n, 1, d)$, $\mathcal{B}(n, n-1, d)$ for $1 \leq d \leq n$, $\mathcal{B}(n, 1)$ and $\mathcal{B}(n, n-1)$ when either $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ and $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$ or $p^r = |\overline{\mathcal{R}}_{e,r}| > 4$ and $\sigma_0 \in Aut(\mathcal{R}_{e,r})$.

Theorem 6.5.3. *Suppose that either $p^r = |\overline{\mathcal{R}}_{e,r}| = 4$ and $\sigma_0 \in Aut_1(\mathcal{R}_{e,r})$ or $p^r = |\overline{\mathcal{R}}_{e,r}| > 4$ and $\sigma_0 \in Aut(\mathcal{R}_{e,r})$. Let ξ be a unit in $\mathcal{R}_{e,r}$ having order $p^r - 1$ (so that the Teichmüller set $\mathcal{T}_{e,r}$ of $\mathcal{R}_{e,r}$ is given by $\mathcal{T}_{e,r} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$; such an element ξ exists in $\mathcal{R}_{e,r}$ by Theorem 2.1.4(c)).*

(a) For $1 \leq d \leq n$, we have

$$\mathcal{B}(n,1,d) = \begin{cases} \left\{\mathcal{C}_n(1,1,\ldots,1,u^{i_1},u^{i_2},\ldots,u^{i_{n-d}}) \ : \ (i_1,i_2,\ldots,i_{n-d}) \in Y_{n-d}\right\} \\ \text{if } d \not\equiv 0 \pmod{p}; \\ \left\{\mathcal{C}_n(1,1,\ldots,1,\xi,u^{i_1},u^{i_2},\ldots,u^{i_{n-d}}) \ : \ (i_1,i_2,\ldots,i_{n-d}) \in Y_{n-d}\right\} \\ \text{if } d \equiv 0 \pmod{p}. \end{cases}$$

As a consequence, we have

$$|\mathcal{B}(n,1,d)| = \binom{e+n-d-1}{n-d} \quad \text{for } 1 \leq d \leq n,$$

and

$$|\mathcal{B}(n,1)| = |\mathcal{B}(n,n-1)| = \binom{e+n-1}{n-1}.$$

(b) For $n \geq 2$ and $1 \leq d \leq n$, we have

$$\mathcal{B}(n,n-1,d) = \begin{cases} \big\{\mathcal{C}_n(1,1,\ldots,1,u^{i_1},u^{i_2},\ldots,u^{i_{n-j}})^{\perp_{\sigma^{-1}}} : (i_1,i_2,\ldots,i_{n-j}) \in Y_{n-j}, \\ 1 \leq j \leq n-1 \textit{ and } j \not\equiv 0 \pmod p\big\} \cup \big\{\mathcal{C}_n(1,1,\ldots,1,\xi,u^{i_1},u^{i_2},\ldots, \\ u^{i_{n-j}})^{\perp_{\sigma^{-1}}} : (i_1,i_2,\ldots,i_{n-j}) \in Y_{n-j}, 1 \leq j \leq n-1 \textit{ and } j \equiv 0 \pmod p\big\} \\ \textit{if } d=1; \\ \big\{\mathcal{C}_n(1,1,\ldots,1)^{\perp_{\sigma^{-1}}}\big\} & \textit{if } d=2 \textit{ and } n \not\equiv 0 \pmod p; \\ \big\{\mathcal{C}_n(1,1,\ldots,1,\xi)^{\perp_{\sigma^{-1}}}\big\} & \textit{if } d=2 \textit{ and } n \equiv 0 \pmod p; \\ \qquad\emptyset & \textit{otherwise.} \end{cases}$$

As a consequence, for $n \geq 2$ and $1 \leq d \leq n$, we have

$$|\mathcal{B}(n,n-1,d)| = \begin{cases} \binom{e+n-1}{n-1} - 1 & \textit{if } d=1; \\ 1 & \textit{if } d=2; \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. **(a)** To determine the set $\mathcal{B}(n,1,d)$, we will first determine the set $\overline{\mathcal{B}}(n,1,d)$ consisting of all inequivalent $\overline{\sigma}$-LCD $[n,1,d]$-codes over $\overline{\mathcal{R}}_{e,r}$. For this, let $\mathcal{D}_n(y_1,y_2,\ldots,y_n)$ denote the linear $[n,1]$-code over $\overline{\mathcal{R}}_{e,r}$ with a generator matrix $[y_1\ y_2\ \cdots\ y_n]$. We next observe that if $a=(a_1,a_2,\ldots,a_n)$, $b=(b_1,b_2,\ldots,b_n) \in \overline{\mathcal{R}}_{e,r}^n$ are such that their Hamming weights are not equal, then the linear codes $\mathcal{D}_n(a_1,a_2,\ldots,a_n)$ and $\mathcal{D}_n(b_1,b_2,\ldots,b_n)$ over $\overline{\mathcal{R}}_{e,r}$ are inequivalent. We further observe that each $\overline{\sigma}$-LCD $[n,1,d]$-code over $\overline{\mathcal{R}}_{e,r}$ is equivalent to the $\overline{\sigma}$-LCD code

$$\mathcal{D}_n(\underbrace{1,1,\ldots,1}_{d},0,0,\ldots,0)$$

when $d \not\equiv 0 \pmod p$, while each $\overline{\sigma}$-LCD $[n,1,d]$-code over $\overline{\mathcal{R}}_{e,r}$ is equivalent to the $\overline{\sigma}$-LCD code

$$\mathcal{D}_n(\underbrace{1,1,\ldots,1}_{d-1},\overline{\xi},0,0,\ldots,0)$$

when $d \equiv 0 \pmod p$. From this, it follows that there exists a unique $\overline{\sigma}$-LCD $[n,1,d]$-code over $\overline{\mathcal{R}}_{e,r}$ up to equivalence for $1 \leq d \leq n$. Further, working as in

Theorem 6.5.2(a) and by applying Lemma 6.5.1, part (a) follows.

(b) Working in a similar manner as in Theorem 6.5.2(b) and by using part (a), the desired result follows.

□

6.5.2 Classification of Euclidean LCD codes over the chain rings $\mathbb{F}_2[u]/\langle u^2\rangle$ and $\mathbb{F}_3[u]/\langle u^2\rangle$, and σ-LCD codes over the chain ring $\mathbb{F}_4[u]/\langle u^2\rangle$ when $\sigma_0 \in Aut_2(\mathbb{F}_4[u]/\langle u^2\rangle)$

The enumeration formulae obtained in Theorems 6.3.5 and 6.3.8 are useful in the determination of complete lists of inequivalent σ-LCD codes of length n over $\mathcal{R}_{e,r}$ when $\sigma_0 \in Aut_1(\mathcal{R}_{e,r}) \cup Aut_2(\mathcal{R}_{e,r})$. To illustrate the same, we will now classify all Euclidean LCD codes of lengths $2, 3, 4$ and 5 over $\mathbb{F}_2[u]/\langle u^2\rangle$ and of lengths $2, 3$ and 4 over $\mathbb{F}_3[u]/\langle u^2\rangle$, and all σ-LCD codes of lengths $2, 3$ and 4 over the chain ring $\mathbb{F}_4[u]/\langle u^2\rangle$ when $\sigma_0 \in Aut_2(\mathbb{F}_4[u]/\langle u^2\rangle)$ (or equivalently, when $\overline{\sigma}_0$ is the automorphism of $\mathbb{F}_4$ of order 2) up to monomial equivalence, by carrying out computations in the Magma Computational Algebra System and by applying the classification algorithm [53, Sec. 9.7] that has been used in most of the earlier classification attempts [3]. We will also explicitly determine a generator matrix of the code representative of each equivalence class of these codes.

I. There are precisely 3 inequivalent non-zero Euclidean LCD codes of length 2 over $\mathbb{F}_2[u]/\langle u^2\rangle$. Among these codes, there are

- 2 Euclidean LCD $[2, 1, 1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & u \end{bmatrix}$; and
- 1 Euclidean LCD $[2, 2, 1]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix I_2.

II. There are precisely 9 inequivalent non-zero Euclidean LCD codes of length 3 over $\mathbb{F}_2[u]/\langle u^2\rangle$. Among these codes, there are

- 3 Euclidean LCD $[3, 1, 1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices

$\begin{bmatrix}1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u\end{bmatrix}$ and $\begin{bmatrix}1 & u & u\end{bmatrix}$;

- 3 Euclidean LCD $[3,2,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u\\ 0 & 1 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & u\\ 0 & 1 & u\end{bmatrix}$;
- 1 Euclidean LCD $[3,1,3]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix $\begin{bmatrix}1 & 1 & 1\end{bmatrix}$;
- 1 Euclidean LCD $[3,3,1]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix I_3; and
- 1 Euclidean LCD $[3,2,2]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix $\begin{bmatrix}1 & 0 & 1+u\\ 0 & 1 & 1+u\end{bmatrix}$.

III. There are precisely 26 inequivalent non-zero Euclidean LCD codes of length 4 over $\mathbb{F}_2[u]/\langle u^2\rangle$. Among these codes, there are

- 4 inequivalent Euclidean LCD $[4,1,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & u & u & u\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$;
- 2 inequivalent Euclidean LCD $[4,1,3]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & u & 1+u & 1\end{bmatrix}$;
- 9 inequivalent Euclidean LCD $[4,2,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 1\\ 0 & 1 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & 0\\ 0 & 1 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1+u & 1+u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & u\\ 0 & 1 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & u & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$;
- 4 inequivalent Euclidean LCD $[4,2,2]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 1 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 1+u\\ 0 & 1 & u & 1+u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 1+u\\ 0 & 1 & 1 & 0\end{bmatrix}$ and

$\begin{bmatrix}1 & 0 & 1+u & 0\\ 0 & 1 & 1+u & 0\end{bmatrix}$;

- 6 inequivalent Euclidean LCD $[4,3,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1&0&0&0\\0&1&0&1\\0&0&1&1\end{bmatrix}$, $\begin{bmatrix}1&0&0&1\\0&1&0&u\\0&0&1&1\end{bmatrix}$, $\begin{bmatrix}1&0&0&u\\0&1&0&0\\0&0&1&0\end{bmatrix}$, $\begin{bmatrix}1&0&0&u\\0&1&0&u\\0&0&1&u\end{bmatrix}$, $\begin{bmatrix}1&0&0&u\\0&1&0&0\\0&0&1&u\end{bmatrix}$ and $\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}$; and
- 1 Euclidean LCD $[4,4,1]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix I_4.

IV. There are precisely 85 inequivalent non-zero Euclidean LCD codes of length 5 over $\mathbb{F}_2[u]/\langle u^2\rangle$. Among these codes, there are

- 5 Euclidean LCD $[5,1,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1&0&0&0&0\end{bmatrix}$, $\begin{bmatrix}1&u&0&0&0\end{bmatrix}$, $\begin{bmatrix}1&u&u&0&0\end{bmatrix}$, $\begin{bmatrix}1&u&u&u&0\end{bmatrix}$ and $\begin{bmatrix}1&u&u&u&u\end{bmatrix}$;
- 3 Euclidean LCD $[5,1,3]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1&1&1&0&0\end{bmatrix}$, $\begin{bmatrix}1&1&1&u&0\end{bmatrix}$ and $\begin{bmatrix}1&1&1&u&u\end{bmatrix}$;
- 1 Euclidean LCD $[5,1,5]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix $\begin{bmatrix}1&1&1&1&1\end{bmatrix}$;
- 21 Euclidean LCD $[5,2,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1&0&1&1&u\\0&1&u&u&0\end{bmatrix}$, $\begin{bmatrix}1&0&u&u&u\\0&1&1&1&0\end{bmatrix}$, $\begin{bmatrix}1&0&0&0&0\\0&1&1&1&u\end{bmatrix}$, $\begin{bmatrix}1&0&0&0&u\\0&1&1&1&0\end{bmatrix}$, $\begin{bmatrix}1&0&0&0&0\\0&1&1&1&0\end{bmatrix}$, $\begin{bmatrix}1&0&1&1&0\\0&1&u&u&0\end{bmatrix}$, $\begin{bmatrix}1&0&1&1&u\\0&1&u&0&u\end{bmatrix}$, $\begin{bmatrix}1&0&1&1&u\\0&1&0&0&u\end{bmatrix}$, $\begin{bmatrix}1&0&0&u&0\\0&1&0&u&u\end{bmatrix}$, $\begin{bmatrix}1&0&u&0&0\\0&1&0&u&u\end{bmatrix}$, $\begin{bmatrix}1&0&0&0&0\\0&1&0&u&0\end{bmatrix}$, $\begin{bmatrix}1&0&u&u&u\\0&1&0&u&0\end{bmatrix}$, $\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\end{bmatrix}$, $\begin{bmatrix}1&0&u&u&u\\0&1&0&0&0\end{bmatrix}$, $\begin{bmatrix}1&0&u&u&0\\0&1&u&u&u\end{bmatrix}$,

$$\begin{bmatrix}1&0&u&u&0\\0&1&u&0&u\end{bmatrix},\begin{bmatrix}1&0&u&u&0\\0&1&u&u&0\end{bmatrix},\begin{bmatrix}1&0&u&u&0\\0&1&0&0&0\end{bmatrix},\begin{bmatrix}1&0&0&0&u\\0&1&0&0&u\end{bmatrix},\begin{bmatrix}1&0&u&u&u\\0&1&u&u&u\end{bmatrix}$$

and $\begin{bmatrix}1&0&0&0&u\\0&1&0&u&0\end{bmatrix}$;

- 12 Euclidean LCD $[5,2,2]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices

$$\begin{bmatrix}1&0&1+u&u&1\\0&1&1&0&1+u\end{bmatrix},\begin{bmatrix}1&0&1&u&u\\0&1&1&1&1\end{bmatrix},\begin{bmatrix}1&0&1+u&1&u\\0&1&1&u&0\end{bmatrix},\begin{bmatrix}1&0&1&1&u\\0&1&1&0&0\end{bmatrix},$$

$$\begin{bmatrix}1&0&1+u&1+u&0\\0&1&1&0&0\end{bmatrix},\begin{bmatrix}1&0&1&u&u\\0&1&1&0&1\end{bmatrix},\begin{bmatrix}1&0&u&1+u&u\\0&1&u&1+u&u\end{bmatrix},\begin{bmatrix}1&0&1&1&1\\0&1&1&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&0&1+u&1+u&0\\0&1&1&u&0\end{bmatrix},\begin{bmatrix}1&0&u&1+u&0\\0&1&0&1&u\end{bmatrix},\begin{bmatrix}1&0&0&1+u&0\\0&1&0&1&0\end{bmatrix}\text{ and}$$

$$\begin{bmatrix}1&0&0&1+u&u\\0&1&0&1&0\end{bmatrix};$$

- 31 Euclidean LCD $[5,3,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices

$$\begin{bmatrix}1&0&0&1&1\\0&1&0&u&1+u\\0&0&1&u&0\end{bmatrix},\begin{bmatrix}1&0&0&0&u\\0&1&0&1&1\\0&0&1&0&1\end{bmatrix},\begin{bmatrix}1&0&0&0&u\\0&1&0&1+u&0\\0&0&1&1+u&0\end{bmatrix},\begin{bmatrix}1&0&0&0&u\\0&1&0&u&u\\0&0&1&0&u\end{bmatrix},$$

$$\begin{bmatrix}1&0&0&1+u&u\\0&1&0&1+u&0\\0&0&1&0&0\end{bmatrix},\begin{bmatrix}1&0&0&1&1\\0&1&0&0&u\\0&0&1&u&u\end{bmatrix},\begin{bmatrix}1&0&0&1&u\\0&1&0&1+u&u\\0&0&1&0&u\end{bmatrix},\begin{bmatrix}1&0&0&u&u\\0&1&0&0&0\\0&0&1&u&u\end{bmatrix},$$

$$\begin{bmatrix}1&0&0&u&1\\0&1&0&1&1+u\\0&0&1&0&0\end{bmatrix},\begin{bmatrix}1&0&0&0&0\\0&1&0&1&0\\0&0&1&1&0\end{bmatrix},\begin{bmatrix}1&0&0&1&0\\0&1&0&u&u\\0&0&1&1+u&0\end{bmatrix},\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&0&0&0&0\\0&1&0&u&0\\0&0&1&1+u&1\end{bmatrix},\begin{bmatrix}1&0&0&u&0\\0&1&0&u&u\\0&0&1&0&u\end{bmatrix},\begin{bmatrix}1&0&0&1+u&0\\0&1&0&u&0\\0&0&1&1&0\end{bmatrix},\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&u&0\end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & u \\ 0 & 1 & 0 & 1+u & 1 \\ 0 & 0 & 1 & 1 & 1+u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & u & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & u \\ 0 & 1 & 0 & u & u \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & u \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & u & u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1 & u \\ 0 & 1 & 0 & u & 0 \\ 0 & 0 & 1 & 1+u & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & u \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & 0 \\ 0 & 1 & 0 & u & u \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & u & u \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 1+u & 1+u \\ 0 & 1 & 0 & 1+u & 1 \\ 0 & 0 & 1 & u & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & u \\ 0 & 1 & 0 & u & u \\ 0 & 0 & 1 & u & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & 0 \\ 0 & 1 & 0 & u & 0 \\ 0 & 0 & 1 & 0 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & u & 0 \\ 0 & 1 & 0 & u & 0 \\ 0 & 0 & 1 & u & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & u & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 1+u & 1+u \\ 0 & 1 & 0 & 0 & 1+u \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix};$$

- 2 Euclidean LCD $[5,3,2]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices

$$\begin{bmatrix} 1 & 0 & 0 & u & 1 \\ 0 & 1 & 0 & 1+u & 1+u \\ 0 & 0 & 1 & u & 1+u \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 0 & 1+u \\ 0 & 1 & 0 & 1+u & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix};$$

- 8 Euclidean LCD $[5,4,1]$-codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ with generator matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 1 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 1+u \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 1 & u \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 & u \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 1 & u \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & u \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 & u \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix};$$

- 1 Euclidean LCD $[5,4,2]$-code over $\mathbb{F}_2[u]/\langle u^2\rangle$ with a generator matrix

$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1+u \\ 0 & 0 & 1 & 0 & 1+u \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$; and

- 1 Euclidean LCD $[5,5,1]$-code over $\mathbb{F}_2[u]/\langle u^2 \rangle$ with a generator matrix I_5.

V. There are precisely 4 inequivalent non-zero Euclidean LCD codes of length 2 over $\mathbb{F}_3[u]/\langle u^2 \rangle$. Among these codes, there are

- 2 inequivalent Euclidean LCD $[2,1,1]$-codes over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with generator matrices $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & u \end{bmatrix}$;
- 1 Euclidean LCD $[2,1,2]$-code over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with a generator matrix $\begin{bmatrix} 1 & 1 \end{bmatrix}$; and
- 1 Euclidean LCD $[2,2,1]$-code over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with a generator matrix I_2.

VI. There are precisely 11 inequivalent non-zero Euclidean LCD codes of length 3 over $\mathbb{F}_3[u]/\langle u^2 \rangle$. Among these codes, there are

- 3 Euclidean LCD $[3,1,1]$-codes over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with generator matrices $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & u \end{bmatrix}$ and $\begin{bmatrix} 1 & u & u \end{bmatrix}$;
- 2 Euclidean LCD $[3,1,2]$-codes over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with generator matrices $\begin{bmatrix} 1 & 1 & u \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 & 0 \end{bmatrix}$;
- 5 Euclidean LCD $[3,2,1]$-codes over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with generator matrices $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & u \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & u \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & 2u \\ 0 & 1 & u \end{bmatrix}$; and
- 1 Euclidean LCD $[3,3,1]$-code over $\mathbb{F}_3[u]/\langle u^2 \rangle$ with a generator matrix I_3.

VII. There are precisely 38 inequivalent non-zero Euclidean LCD codes of length 4 over $\mathbb{F}_3[u]/\langle u^2 \rangle$. Among these codes, there are

- 4 Euclidean LCD $[4,1,1]$-codes over $\mathbb{F}_3[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & u & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & u\end{bmatrix}$ and $\begin{bmatrix}1 & u & u & u\end{bmatrix}$;
- 3 Euclidean LCD $[4,1,2]$-codes over $\mathbb{F}_3[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1 & 0 & u\end{bmatrix}$ and $\begin{bmatrix}1 & 1 & u & u\end{bmatrix}$;
- 1 Euclidean LCD $[4,1,4]$-code over $\mathbb{F}_3[u]/\langle u^2\rangle$ with a generator matrix $\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$;
- 16 Euclidean LCD $[4,2,1]$-codes over $\mathbb{F}_3[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & u\\ 0 & 1 & 2u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & u\\ 0 & 1 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 2u & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1+u & 0\\ 0 & 1 & 2u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & u\\ 0 & 1 & 2u & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 2u & 2u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & 2u\\ 0 & 1 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & 2u\\ 0 & 1 & u & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 2u & 2u\\ 0 & 1 & 2u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & u & 0\\ 0 & 1 & 2u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 2u & 0\\ 0 & 1 & 0 & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 2u\\ 0 & 1 & 0 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 1+2u & u\\ 0 & 1 & 0 & 0\end{bmatrix}$;
- 5 Euclidean LCD $[4,2,2]$-codes over $\mathbb{F}_3[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 2 & 1+u\\ 0 & 1 & 1 & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1 & 2+u\\ 0 & 1 & 1 & 2+u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1+u & u\\ 0 & 1 & u & 1\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 1+u & u\\ 0 & 1 & 0 & 1\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 1+u & 0\\ 0 & 1 & 0 & 1\end{bmatrix}$;
- 7 Euclidean LCD $[4,3,1]$-codes over $\mathbb{F}_3[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & u\\ 0 & 0 & 1 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 2u\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 2u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & u\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 2u\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 2u\\ 0 & 1 & 0 & 2+2u\\ 0 & 0 & 1 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}$;
- 1 Euclidean LCD $[4,3,2]$-code over $\mathbb{F}_3[u]/\langle u^2\rangle$ with a generator matrix

$\begin{bmatrix} 1 & 0 & 0 & 2+u \\ 0 & 1 & 0 & 2+2u \\ 0 & 0 & 1 & 1 \end{bmatrix}$; and

- 1 Euclidean LCD $[4,4,1]$-code over $\mathbb{F}_3[u]/\langle u^2\rangle$ with a generator matrix I_4.

VIII. Let $\sigma_0 \in Aut_2(\mathbb{F}_4[u]/\langle u^2\rangle)$, and let ζ be a primitive element of $\mathbb{F}_4$. There are precisely 3 inequivalent non-zero σ-LCD codes of length 2 over $\mathbb{F}_4[u]/\langle u^2\rangle$. Among these codes, there are

- 2 σ-LCD $[2,1,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & \zeta^2 u \end{bmatrix}$; and
- 1 σ-LCD $[2,2,1]$-code over $\mathbb{F}_4[u]/\langle u^2\rangle$ with a generator matrix I_2.

IX. Let $\sigma_0 \in Aut_2(\mathbb{F}_4[u]/\langle u^2\rangle)$, and let ζ be a primitive element of $\mathbb{F}_4$. There are precisely 9 inequivalent non-zero σ-LCD codes of length 3 over $\mathbb{F}_4[u]/\langle u^2\rangle$. Among these codes, there are

- 3 σ-LCD $[3,1,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & u \end{bmatrix}$ and $\begin{bmatrix} 1 & u & u \end{bmatrix}$;
- 1 σ-LCD $[3,1,3]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with a generator matrix $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$;
- 4 σ-LCD $[3,2,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & \zeta u \\ 0 & 1 & u \end{bmatrix}$, $\begin{bmatrix} 1 & 0 & \zeta u \\ 0 & 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 & 1+\zeta^2 u \\ 0 & 1 & \zeta^2+\zeta^2 u \end{bmatrix}$; and
- 1 σ-LCD $[3,3,1]$-code over $\mathbb{F}_4[u]/\langle u^2\rangle$ with a generator matrix I_3.

X. Let $\sigma_0 \in Aut_2(\mathbb{F}_4[u]/\langle u^2\rangle)$, and let ζ be a primitive element of $\mathbb{F}_4$. There are precisely 31 inequivalent non-zero σ-LCD codes of length 4 over $\mathbb{F}_4[u]/\langle u^2\rangle$. Among these codes, there are

- 4 inequivalent σ-LCD $[4,1,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & u & u & u\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$;
- 2 inequivalent σ-LCD $[4,1,3]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & u & 1 & 1\end{bmatrix}$;
- 11 inequivalent σ-LCD $[4,2,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & \zeta u & \zeta u\\ 0 & 1 & \zeta^2 u & \zeta^2 u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta u & u\\ 0 & 1 & \zeta+\zeta^2 u & 1+u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta^2 u & \zeta^2 u\\ 0 & 1 & \zeta+\zeta^2 u & 1\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta u & \zeta^2 u\\ 0 & 1 & \zeta u & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta u & \zeta u\\ 0 & 1 & \zeta^2 u & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta+u & 1+\zeta^2 u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta^2 u & u\\ 0 & 1 & 0 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & 0\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & \zeta u\\ 0 & 1 & \zeta^2 u & 0\end{bmatrix}$;
- 7 inequivalent σ-LCD $[4,2,2]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0 & \zeta^2+\zeta u\\ 0 & 1 & 0 & \zeta\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta^2 u & \zeta^2+\zeta^2 u\\ 0 & 1 & \zeta u & \zeta\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta u & \zeta^2+u\\ 0 & 1 & 1+\zeta^2 u & 1\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta^2 u & \zeta^2+\zeta^2 u\\ 0 & 1 & u & \zeta\end{bmatrix}$, $\begin{bmatrix}1 & 0 & \zeta^2 u & \zeta^2+\zeta u\\ 0 & 1 & 1+\zeta u & 1+u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & \zeta^2+\zeta u\\ 0 & 1 & 1+u & 1+u\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & u & \zeta^2+u\\ 0 & 1 & 1+u & 1+u\end{bmatrix}$;
- 6 inequivalent σ-LCD $[4,3,1]$-codes over $\mathbb{F}_4[u]/\langle u^2\rangle$ with generator matrices $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & \zeta^2 u\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & \zeta^2\\ 0 & 1 & 0 & \zeta+u\\ 0 & 0 & 1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & \zeta u\\ 0 & 1 & 0 & u\\ 0 & 0 & 1 & \zeta^2 u\end{bmatrix}$, $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & \zeta^2+\zeta^2 u\\ 0 & 0 & 1 & \zeta^2+\zeta^2 u\end{bmatrix}$ and $\begin{bmatrix}1 & 0 & 0 & u\\ 0 & 1 & 0 & \zeta u\\ 0 & 0 & 1 & 0\end{bmatrix}$; and
- 1 σ-LCD $[4,4,1]$-code over $\mathbb{F}_4[u]/\langle u^2\rangle$ with a generator matrix I_4.

In the next chapter, we will study S-additive codes over R and their dual codes with respect to the ordinary trace bilinear form, where R and S are two finite commutative chain rings such that R is the Galois extension of S of degree $m \geq 2$, (recall that an S-additive code of length n over R is defined as an S-submodule of R^n). We will also study their three special classes such as S-additive self-orthogonal codes, S-additive self-dual codes and S-additive codes with complementary duals (ACD codes) and further apply the results derived in Chapters 3-6 to enumerate these three classes of codes.

7

Additive self-orthogonal, additive self-dual and ACD codes over finite commutative chain rings

7.1 Introduction

Additive codes over finite commutative chain rings are natural extensions of linear codes. These codes have rich algebraic structures [23, 71, 93] and are useful in constructing quantum error-correcting codes [22, 93]. This motivated several researchers to study these codes and provide methods to construct these codes. Mahmoudi and Samei [71] studied algebraic structures of additive codes over Galois rings by establishing a one-to-one correspondence between linear codes over the ring $\mathbb{Z}_{p^e}$ of integers modulo p^e and additive codes over the Galois ring $GR(p^e, r)$, where p is a prime number and e, r are positive integers. They also studied permutation equivalent additive codes and decomposable additive codes over Galois rings. Besides this, they proved the MacWilliams identity and Delsarte's Theorem for additive codes over Galois rings. Cao *et al.* [23] studied cyclic additive codes over Galois rings and provided a canonical form decomposition for these codes. With the help of this decomposition, they further enumerated all cyclic additive codes of an arbitrary length over Galois rings. Moro *et al.* [74] studied cyclic additive codes over finite commutative chain rings with respect to two different notions of additivity, *viz.* Galois-additivity and Eisenstein-additivity. Recently, Sidana and Kashyap [93] constructed entanglement-assisted quantum error-correcting codes (EAQECCs) from additive codes over finite commutative local Frobenius rings. They also provided a formula for the minimum number of entanglement qudits required to construct an EAQECC from an additive code over a Galois ring.

Throughout this chapter, let $r \geq 1$, $m \geq 2$ and $e \geq 2$ be integers. Let

$$\mathcal{R}_{e,r} = \frac{GR(p^{\mathfrak{s}}, r)[x]}{\langle g(x), p^{\mathfrak{s}-1}x^t \rangle}$$

and

$$\mathcal{R}_{e,rm} = \frac{GR(p^{\mathfrak{s}}, rm)[x]}{\langle g(x), p^{\mathfrak{s}-1}x^t \rangle}$$

be two finite commutative chain rings, where $g(x) = x^\kappa + p(a_{\kappa-1}x^{\kappa-1} + \cdots + a_1x + a_0) \in GR(p^{\mathfrak{s}}, r)[x]$ is an Eisenstein polynomial with a_0 as a unit in $GR(p^{\mathfrak{s}}, r)$, $e = \kappa(\mathfrak{s} - 1) + t$, and $1 \leq t \leq \kappa$ when $\mathfrak{s} \geq 2$, while $t = \kappa$ when $\mathfrak{s} = 1$. Note that $\mathcal{R}_{e,r}$ is a subring of $\mathcal{R}_{e,rm}$. By Theorem 4.3.1 of [16], we see that $\mathcal{R}_{e,rm}$ is the Galois extension of $\mathcal{R}_{e,r}$ of degree m. If $u := x + \langle g(x), p^{\mathfrak{s}-1}x^t \rangle$, then one can easily see that e is the least positive integer satisfying $u^e = 0$ in $\mathcal{R}_{e,r}$ (and in $\mathcal{R}_{e,rm}$) and $\langle u \rangle$ is the unique maximal ideal of both $\mathcal{R}_{e,r}$ and $\mathcal{R}_{e,rm}$. Note that the residue field $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u \rangle$ of $\mathcal{R}_{e,r}$ is of order p^r and the residue field $\overline{\mathcal{R}}_{e,rm} = \mathcal{R}_{e,rm}/\langle u \rangle$ of $\mathcal{R}_{e,rm}$ is of order p^{rm}. One can easily see that the set $\mathcal{R}_{e,rm}^n$ of all n-tuples over $\mathcal{R}_{e,rm}$ can be viewed as an $\mathcal{R}_{e,r}$-module under the component-wise addition and the component-wise scalar multiplication. Now an additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ is defined as an $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$.

The main goal of this chapter is to study additive codes over $\mathcal{R}_{e,rm}$ and their dual codes with respect to the ordinary trace bilinear form. We will also study their three special classes, *viz.* additive self-orthogonal codes, additive self-dual codes and additive codes with complementary duals (ACD codes) with respect to the ordinary trace bilinear form. We will also derive necessary and sufficient conditions under which an additive code over $\mathcal{R}_{e,rm}$ is (i) self-orthogonal, (ii) self-dual, and (iii) ACD. We will derive necessary and sufficient conditions for the existence of an additive self-dual code over $\mathcal{R}_{e,rm}$. As an application of these results, we will obtain explicit enumeration formulae for all additive self-orthogonal and self-dual codes of an arbitrary length over $\mathcal{R}_{e,rm}$ in the following three cases: (i) both p and m are odd (ii) $p = 2$ and $\mathfrak{s} = 1$, and (iii) $p = 2$, $\kappa = 1$ and m is odd. We will also count all ACD codes of an arbitrary length over $\mathcal{R}_{e,rm}$, where $e \geq 2$, $r \geq 1$ and $m \geq 2$ are arbitrary integers.

This chapter is organized as follows: In Section 7.2, we state some preliminaries and study algebraic structures of additive codes over $\mathcal{R}_{e,rm}$ by establishing a one-to-one correspondence between additive codes over $\mathcal{R}_{e,rm}$ and linear codes over $\mathcal{R}_{e,r}$. In Section 7.3, we derive necessary and sufficient conditions under which an additive code over $\mathcal{R}_{e,rm}$ is self-orthogonal or self-dual (Theorem 7.3.1). We further obtain explicit enumeration formulae for all additive self-orthogonal and self-dual codes of an arbitrary length over $\mathcal{R}_{e,rm}$ in the following three cases: (i) both p and m are odd (ii) $p = 2$ and $\mathfrak{s} = 1$, and (iii) $p = 2$, $\kappa = 1$ and m is odd (Theorems 7.3.4,7.3.5, 7.3.8-7.3.11, 7.3.14 and 7.3.15). In Section 7.4, we first show that any ACD code of length n over $\mathcal{R}_{e,rm}$ is a free code, *i.e.,* it is a free $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$ (Theorem 7.4.1). We further derive necessary and sufficient conditions under which an additive code over $\mathcal{R}_{e,rm}$ is ACD (Theorem 7.4.2). We also obtain explicit enumeration formula for all ACD codes of an arbitrary length over $\mathcal{R}_{e,rm}$, where $e \geq 2$, $r \geq 1$ and $m \geq 2$ are integers (Theorems 7.4.10 and 7.4.11).

7.2 Additive codes over finite commutative chain rings

In this section, we will state some basic definitions and results needed to prove our main results. We will also study algebraic structures of additive codes over

$\mathcal{R}_{e,rm}$ and their dual codes with respect to the ordinary trace bilinear form. Since $GR(p^{\mathfrak{s}}, rm)$ is the Galois extension of $GR(p^{\mathfrak{s}}, r)$ of degree m, we see, by Theorem 14.23 of [101], that there exists an element $\zeta \in GR(p^{\mathfrak{s}}, rm)$ of multiplicative order $p^{rm} - 1$, such that

$$\begin{aligned} GR(p^{\mathfrak{s}}, rm) &= GR(p^{\mathfrak{s}}, r)[\zeta] \\ &= \{v_0 + v_1\zeta + \cdots + v_{m-1}\zeta^{m-1} \ : \ v_i \in GR(p^{\mathfrak{s}}, r) \text{ for } 0 \leq i \leq m-1\}. \end{aligned}$$

Further, by Theorem 2.4 of Moro *et al.* [74], we see that

$$\mathcal{R}_{e,rm} = \mathcal{R}_{e,r}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1} \ : \ a_i \in \mathcal{R}_{e,r} \text{ for } 0 \leq i \leq m-1\}.$$

Thus $\mathcal{R}_{e,rm}$ is a free module over $\mathcal{R}_{e,r}$ with a basis set $\{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}$. Note that the set $\mathcal{T}_{e,rm} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^{rm}-2}\}$ is the Teichm*ü*ller set of the chain ring $\mathcal{R}_{e,rm}$ and the set $\mathcal{T}_{e,r} = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is the Teichm*ü*ller set of the chain ring $\mathcal{R}_{e,r}$, where $\xi = \zeta^{\frac{p^{rm}-1}{p^r-1}}$. Further, if $u := x + \langle g(x), p^{\mathfrak{s}-1}x^t \rangle$, then the ideal $\langle u \rangle$ is the unique maximal ideal of both the chain rings $\mathcal{R}_{e,r}$ and $\mathcal{R}_{e,rm}$ and has nilpotency index $e = \kappa(\mathfrak{s} - 1) + t$. Further, all the ideals of $\mathcal{R}_{e,r}$ are given by $\{0\} \subset \langle u^{e-1} \rangle \subset \langle u^{e-2} \rangle \subset \cdots \subset \langle u \rangle \subset \langle 1 \rangle = \mathcal{R}_{e,r}$ and all the ideals of $\mathcal{R}_{e,rm}$ are given by $\{0\} \subset \langle u^{e-1} \rangle \subset \langle u^{e-2} \rangle \subset \cdots \subset \langle u \rangle \subset \langle 1 \rangle = \mathcal{R}_{e,rm}$. Moreover, if $\overline{\mathcal{R}}_{e,r} = \mathcal{R}_{e,r}/\langle u \rangle$ and $\overline{\mathcal{R}}_{e,rm} = \mathcal{R}_{e,rm}/\langle u \rangle$, then $\overline{\mathcal{R}}_{e,r}$ is the residue field of $\mathcal{R}_{e,r}$ of order p^r and $\overline{\mathcal{R}}_{e,rm}$ is the residue field of $\mathcal{R}_{e,rm}$ of order p^{rm}. Let us define $\overline{a} = a + \langle u \rangle$ for all $a \in \mathcal{R}_{e,rm}$. It is easy to see that $\overline{\mathcal{R}}_{e,rm} = \overline{\mathcal{R}}_{e,r}[\overline{\zeta}] = \{\overline{z}_0 + \overline{z}_1\overline{\zeta} + \cdots + \overline{z}_{m-1}\overline{\zeta}^{m-1} \ : \ \overline{z}_i \in \overline{\mathcal{R}}_{e,r} \text{ for } 0 \leq i \leq m-1\}$, *i.e.,* $\overline{\mathcal{R}}_{e,rm}$ is the Galois extension of $\overline{\mathcal{R}}_{e,r}$ of degree m.

Next, let n be a positive integer, and let $\mathcal{R}_{e,rm}^n$ be the set of all n-tuples over $\mathcal{R}_{e,rm}$. The set $\mathcal{R}_{e,rm}^n$ can be viewed as an $\mathcal{R}_{e,r}$-module under the component-wise addition and the component-wise scalar multiplication. An additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ is defined as an $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$. Elements of the code $\mathscr{C}$ are called codewords. Further, a matrix over $\mathcal{R}_{e,rm}$ is called a generator matrix of the code $\mathscr{C}$ if its rows form a minimal generating set of the code $\mathscr{C}$. The rank of the code $\mathscr{C}$ is defined as the cardinality of a minimal generating set of the code $\mathscr{C}$. The Hamming distance of the code $\mathscr{C}$, denoted by $d_H(\mathscr{C})$, is given by

$$d_H(\mathscr{C}) = \min\{w_H(c) : c(\neq 0) \in \mathscr{C}\}.$$

Further, the additive code $\mathscr{C}$ is said to be free if it is a free $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$. The rank of the free additive code $\mathscr{C}$ equals the rank of $\mathscr{C}$ as a free $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$.

Further, for $1 \leq i \leq e$, the i-th Torsion code of the additive code $\mathscr{C}$ is defined as

$$Tor_i(\mathscr{C}) = \{\overline{z} \in \overline{\mathcal{R}}_{e,rm}^n \ : \ u^{i-1}z' \in \mathscr{C} \text{ for some } z' \in \mathcal{R}_{e,rm}^n \text{ satisfying } \overline{z'} = \overline{z}\}.$$

One can easily observe that the i-th Torsion code $Tor_i(\mathscr{C})$ of $\mathscr{C}$ is an $\overline{\mathcal{R}}_{e,r}$-linear subspace of $\overline{\mathcal{R}}_{e,rm}^n$, *i.e.,* $Tor_i(\mathscr{C})$ is an additive code of length n over $\overline{\mathcal{R}}_{e,rm}$. Further, the additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ is said to be of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ if $\mathtt{k}_1 = \dim_{\overline{\mathcal{R}}_{e,r}}(Tor_1(\mathscr{C}))$ and $\mathtt{k}_i = \dim_{\overline{\mathcal{R}}_{e,r}}(Tor_i(\mathscr{C})) - \dim_{\overline{\mathcal{R}}_{e,r}}(Tor_{i-1}(\mathscr{C}))$ for $2 \leq i \leq e$.

The mapping $\varphi : \mathcal{R}_{e,rm} \to \mathcal{R}_{e,rm}$, defined as

$$\varphi(a) = a_0 + a_1\zeta^{p^r} + \cdots + a_{m-1}\zeta^{p^r(m-1)}$$

for all $a = a_0 + a_1\zeta + \cdots + a_{m-1}\zeta^{m-1} \in \mathcal{R}_{e,rm}$ with $a_0, a_1, \ldots, a_{m-1} \in \mathcal{R}_{e,r}$, is an automorphism of $\mathcal{R}_{e,rm}$ which fixes each element of $\mathcal{R}_{e,r}$. By Corollary 5.1.5 and Theorem 5.1.6 of [16], we see that the automorphism group $\mathcal{A}ut_{\mathcal{R}_{e,r}}(\mathcal{R}_{e,rm})$ of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ is the cyclic group $\{\varphi^i \ : \ 0 \leq i \leq m-1\}$ generated by the element φ. We next observe that the mapping $Tr_{p^r,m} : \mathcal{R}_{e,rm} \to \mathcal{R}_{e,r}$, defined as

$$Tr_{p^r,m}(a) = a + \varphi(a) + \varphi^2(a) + \cdots + \varphi^{m-1}(a) \text{ for all } a \in \mathcal{R}_{e,rm},$$

is a surjective $\mathcal{R}_{e,r}$-module homomorphism and is called the generalized trace map. Now define a map $\langle \cdot, \cdot \rangle : \mathcal{R}_{e,rm}^n \times \mathcal{R}_{e,rm}^n \to \mathcal{R}_{e,r}$ as

$$\langle a, b \rangle = \sum_{i=1}^{n} Tr_{p^r,m}(a_i b_i)$$

for all $a = (a_1, a_2, \ldots, a_n)$, $b = (b_1, b_2, \ldots, b_n) \in \mathcal{R}_{e,rm}^n$. One can easily see that $\langle \cdot, \cdot \rangle$ is a non-degenerate and symmetric bilinear form on $\mathcal{R}_{e,rm}^n$ and is called the ordinary trace bilinear form. Further, if $\mathscr{C}$ is an additive code of length n over $\mathcal{R}_{e,rm}$, then its dual code $\mathscr{C}^{\perp}$ is defined as

$$\mathscr{C}^{\perp}=\big\{z\in\mathcal{R}_{e,rm}^{n}\ :\ \langle z,c\rangle=0\text{ for all }c\in\mathscr{C}\big\}.$$

Note that the dual code $\mathscr{C}^{\perp}$ is also an $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^{n}$, and hence it is an additive code of length n over $\mathcal{R}_{e,rm}$. A generator matrix of the dual code $\mathscr{C}^{\perp}$ is called a parity-check matrix of the code $\mathscr{C}$. Further, the additive code $\mathscr{C}$ is said to be (i) self-orthogonal if it satisfies $\mathscr{C}\subseteq\mathscr{C}^{\perp}$, (ii) self-dual if it satisfies $\mathscr{C}=\mathscr{C}^{\perp}$ and (iii) an additive code with complementary dual (an ACD code) if it satisfies $\mathscr{C}\cap\mathscr{C}^{\perp}=\{0\}$.

Further, corresponding to the automorphism φ, we observe that the mapping $\overline{\varphi}:\overline{\mathcal{R}}_{e,rm}\to\overline{\mathcal{R}}_{e,rm}$, defined as $\overline{\varphi}(\overline{z})=\overline{z}_0+\overline{z}_1\overline{\zeta}^{p^r}+\cdots+\overline{z}_{m-1}\overline{\zeta}^{p^r(m-1)}$ for all $\overline{z}=\overline{z}_0+\overline{z}_1\overline{\zeta}+\cdots+\overline{z}_{m-1}\overline{\zeta}^{m-1}\in\overline{\mathcal{R}}_{e,rm}$ with $\overline{z}_0,\overline{z}_1,\ldots,\overline{z}_{m-1}\in\overline{\mathcal{R}}_{e,r}$, is an automorphism of $\overline{\mathcal{R}}_{e,rm}$ that fixes each element of $\overline{\mathcal{R}}_{e,r}$ and is called the Frobenius automorphism of $\overline{\mathcal{R}}_{e,rm}$ over $\overline{\mathcal{R}}_{e,r}$. Next, we observe that the mapping $\overline{T}r_{p^r,m}:\overline{\mathcal{R}}_{e,rm}\to\overline{\mathcal{R}}_{e,r}$, defined as $\overline{T}r_{p^r,m}(\overline{a})=\overline{a}+\overline{\varphi}(\overline{a})+\overline{\varphi}^2(\overline{a})+\cdots+\overline{\varphi}^{m-1}(\overline{a})$ for all $\overline{a}\in\overline{\mathcal{R}}_{e,rm}$, is a surjective $\overline{\mathcal{R}}_{e,r}$-module homomorphism, which coincides with the usual trace map from $\overline{\mathcal{R}}_{e,rm}$ onto $\overline{\mathcal{R}}_{e,r}$. Now the ordinary trace bilinear form on $\overline{\mathcal{R}}_{e,rm}^{n}$ is a map $\langle\cdot,\cdot\rangle:\overline{\mathcal{R}}_{e,rm}^{n}\times\overline{\mathcal{R}}_{e,rm}^{n}\to\overline{\mathcal{R}}_{e,r}$, defined as

$$\langle v,w\rangle=\sum_{i=1}^{n}\overline{T}r_{p^r,m}(v_iw_i)$$

for all $v=(v_1,v_2,\ldots,v_n)$, $w=(w_1,w_2,\ldots,w_n)\in\overline{\mathcal{R}}_{e,rm}^{n}$. By Lemma 1 of Huffman [52], we see that $\langle\cdot,\cdot\rangle$ is a non-degenerate and symmetric bilinear form on $\overline{\mathcal{R}}_{e,rm}^{n}$.

An additive code $\mathscr{D}$ of length n over $\overline{\mathcal{R}}_{e,rm}$ is defined as an $\overline{\mathcal{R}}_{e,r}$-submodule of $\overline{\mathcal{R}}_{e,rm}^{n}$. The dual code $\mathscr{D}^{\perp}$ of the code $\mathscr{D}$ is defined as

$$\mathscr{D}^{\perp}=\big\{a\in\overline{\mathcal{R}}_{e,rm}^{n}\ :\ \langle a,d\rangle=0\text{ for all }d\in\mathscr{D}\big\}.$$

It is easy to observe that the dual code $\mathscr{D}^{\perp}$ is also an additive code of length n over $\overline{\mathcal{R}}_{e,rm}$. By Theorem 2.3.2, we see that $\dim_{\overline{\mathcal{R}}_{e,r}}(\mathscr{D})+\dim_{\overline{\mathcal{R}}_{e,r}}(\mathscr{D}^{\perp})=nm$. From now on, throughout this thesis, for each $k\times\ell$ matrix $\mathcal{B}$ over $\mathcal{R}_{e,rm}$ with the (i,j)-th entry as $b_{i,j}$, let $Tr_{p^r,m}(\mathcal{B})$ denote the $k\times\ell$ matrix over $\mathcal{R}_{e,r}$ whose (i,j)-th entry is

$Tr_{p^r,m}(b_{i,j})$ and $\overline{T}r_{p^r,m}(\overline{\mathcal{B}})$ denote the $k \times \ell$ matrix over $\overline{\mathcal{R}}_{e,r}$ whose (i,j)-th entry is $\overline{T}r_{p^r,m}(\overline{b}_{i,j})$, where $1 \leq i \leq k$ and $1 \leq j \leq \ell$. Note that $Tr_{p^r,m}(\mathcal{B})$ and $\overline{T}r_{p^r,m}(\overline{\mathcal{B}})$ are not equal to the usual traces of the matrices $\mathcal{B}$ and $\overline{\mathcal{B}}$, respectively.

Let $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be a basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$. Now let us define a map $\Pi_\alpha : \mathcal{R}_{e,rm}^n \to \mathcal{R}_{e,r}^{nm}$ as

$$\Pi_\alpha(v_1, v_2, \ldots, v_n) = (v_{1,1}, v_{1,2}, \ldots, v_{1,m}, v_{2,1}, v_{2,2}, \ldots, v_{2,m}, \ldots, v_{n,1}, v_{n,2}, \ldots, v_{n,m})$$

for all $v_i = v_{i,1}\alpha_1 + v_{i,2}\alpha_2 + \cdots + v_{i,m}\alpha_m \in \mathcal{R}_{e,rm}$, where $v_{i,1}, v_{i,2}, \ldots, v_{i,m} \in \mathcal{R}_{e,r}$ for $1 \leq i \leq n$. It is easy to see that the map Π_α is an $\mathcal{R}_{e,r}$-module isomorphism. From this, it follows that a non-empty subset $\mathscr{C}$ of $\mathcal{R}_{e,rm}^n$ is an additive code of length n over $\mathcal{R}_{e,rm}$ if and only if its image $\Pi_\alpha(\mathscr{C})$ is a linear code of length nm over $\mathcal{R}_{e,r}$. That is, the isomorphism Π_α induces a one-to-one correspondence between additive codes of length n over $\mathcal{R}_{e,rm}$ and linear codes of length nm over $\mathcal{R}_{e,r}$. Further, we observe that $(v_1, v_2, \ldots, v_n) \in \mathcal{R}_{e,rm}^n$ with $v_i \in \langle u^\ell \rangle$ for $1 \leq i \leq n$ if and only if $\Pi_\alpha(v_1, v_2, \ldots, v_n) = (v_{1,1}, v_{1,2}, \ldots, v_{1,m}, v_{2,1}, v_{2,2}, \ldots, v_{2,m}, \ldots, v_{n,1}, v_{n,2}, \ldots, v_{n,m}) \in \mathcal{R}_{e,r}^{nm}$ with $v_{i,j} \in \langle u^\ell \rangle$ for $1 \leq i \leq n$ and $1 \leq j \leq m$, where $0 \leq \ell \leq e$.

Next, we note that if $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$, then $\overline{\alpha} = \{\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_m\}$ is a basis of $\overline{\mathcal{R}}_{e,rm}$ over $\overline{\mathcal{R}}_{e,r}$. Further, corresponding to the mapping Π_α, we define a mapping $\overline{\Pi}_{\overline{\alpha}} : \overline{\mathcal{R}}_{e,rm}^n \to \overline{\mathcal{R}}_{e,r}^{nm}$ as

$$\overline{\Pi}_{\overline{\alpha}}(\overline{z}_1, \overline{z}_2, \ldots, \overline{z}_n) = (\overline{z}_{1,1}, \overline{z}_{1,2}, \ldots, \overline{z}_{1,m}, \overline{z}_{2,1}, \overline{z}_{2,2}, \ldots, \overline{z}_{2,m}, \ldots, \overline{z}_{n,1}, \overline{z}_{n,2}, \ldots, \overline{z}_{n,m})$$

for all $\overline{z}_i = \overline{z}_{i,1}\overline{\alpha}_1 + \overline{z}_{i,2}\overline{\alpha}_2 + \cdots + \overline{z}_{i,m}\overline{\alpha}_m \in \overline{\mathcal{R}}_{e,rm}$, where $\overline{z}_{i,1}, \overline{z}_{i,2}, \ldots, \overline{z}_{i,m} \in \overline{\mathcal{R}}_{e,r}$ for $1 \leq i \leq n$. It is easy to observe that the map $\overline{\Pi}_{\overline{\alpha}}$ is an $\overline{\mathcal{R}}_{e,r}$-linear vector space isomorphism. From this, it follows that the isomorphism $\overline{\Pi}_{\overline{\alpha}}$ induces a one-to-one correspondence between additive codes of length n over $\overline{\mathcal{R}}_{e,rm}$ and linear codes of length nm over $\overline{\mathcal{R}}_{e,r}$, *i.e.,* $\mathscr{D}$ is an additive code of length n over $\overline{\mathcal{R}}_{e,rm}$ if and only if $\overline{\Pi}_{\overline{\alpha}}(\mathscr{D})$ is a linear code of length nm over $\overline{\mathcal{R}}_{e,r}$.

In the following lemma, we relate the Torsion codes of an additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ with the Torsion codes of the linear code $\Pi_\alpha(\mathscr{C})$ of length nm over $\mathcal{R}_{e,r}$.

Lemma 7.2.1. *Let $\mathscr{C}$ be an additive code of length n over $\mathcal{R}_{e,rm}$. We have*

$$Tor_i(\Pi_\alpha(\mathscr{C})) = \overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C})) \quad \text{for} \quad 1 \leq i \leq e.$$

Proof. To prove the result, let $c \in Tor_i(\Pi_\alpha(\mathscr{C}))$. So there exists $c' \in \mathcal{R}_{e,r}^{nm}$ such that $u^{i-1}c' \in \Pi_\alpha(\mathscr{C})$ and $\overline{c'} = c$. Since the map Π_α is an $\mathcal{R}_{e,r}$-module isomorphism, there exists $d \in \mathcal{R}_{e,rm}^n$ such that $u^{i-1}d \in \mathscr{C}$ and $\Pi_\alpha(u^{i-1}d) = u^{i-1}c'$. This implies that $\overline{d} \in Tor_i(\mathscr{C})$, which further implies that $c = \overline{c'} = \overline{\Pi}_{\overline{\alpha}}(\overline{d}) \in \overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C}))$. This shows that

$$Tor_i(\Pi_\alpha(\mathscr{C})) \subseteq \overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C})).$$

Conversely, let $v \in \overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C}))$. So there exists $v' \in Tor_i(\mathscr{C})$ such that $\overline{\Pi}_{\overline{\alpha}}(v') = v$. This implies that there exists $z \in \mathcal{R}_{e,rm}^n$ such that $u^{i-1}z \in \mathscr{C}$ and $\overline{z} = v'$. Further, $u^{i-1}z \in \mathscr{C}$ implies that $u^{i-1}\Pi_\alpha(z) \in \Pi_\alpha(\mathscr{C})$. From this, we get $v = \overline{\Pi}_{\overline{\alpha}}(v') = \overline{\Pi}_{\overline{\alpha}}(\overline{z}) \in Tor_i(\Pi_\alpha(\mathscr{C}))$. This implies that

$$\overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C})) \subseteq Tor_i(\Pi_\alpha(\mathscr{C})).$$

From this, it follows that $Tor_i(\Pi_\alpha(\mathscr{C})) = \overline{\Pi}_{\overline{\alpha}}(Tor_i(\mathscr{C}))$. □

Remark 7.2.1. *By Lemma 7.2.1, we see that an additive code $\mathscr{C}$ is of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$ if and only if the linear code $\Pi_\alpha(\mathscr{C})$ is of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length nm over $\mathcal{R}_{e,r}$. From this, it follows that*

$$|\mathscr{C}| = \prod_{i=1}^{e} |Tor_i(\mathscr{C})| = (p^r)^{\sum\limits_{i=1}^{e}(e-i+1)\mathtt{k}_i}.$$

Given an ordered basis $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$, its trace dual basis is defined as an ordered basis $\beta = \{\beta_1, \beta_2, \ldots, \beta_m\}$ of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ satisfying $Tr_{p^r,m}(\alpha_i\beta_j) = \delta_{i,j}$ for $1 \leq i, j \leq m$, where $\delta_{i,j}$ denotes the Kronecker delta function. Further, if $\alpha = \beta$, then α is said to be a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$. That is, an ordered basis $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ is said to be a self-dual basis if it satisfies $Tr_{p^r,m}(\alpha_i\alpha_j) = \delta_{i,j}$ for $1 \leq i, j \leq m$.

In the following lemma, we note that every ordered basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ has a unique trace dual basis.

Theorem 7.2.1. *Every ordered basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ has a unique trace dual basis.*

Proof. We note that $\mathcal{R}_{e,rm}$ is a free module over $\mathcal{R}_{e,r}$ of rank m, and hence there exists a basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$. Now working as in Lemma 13 of Irwansyah *et al.* [54], the desired result follows.

□

Proposition 7.2.1. *Let $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be an ordered basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ with the trace dual basis $\beta = \{\beta_1, \beta_2, \ldots, \beta_m\}$. For an additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$, we have*

$$\Pi_\beta(\mathscr{C}^\perp) = (\Pi_\alpha(\mathscr{C}))^\perp.$$

In particular, if $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$, then we have $\Pi_\alpha(\mathscr{C}^\perp) = (\Pi_\alpha(\mathscr{C}))^\perp$.

Proof. To prove the result, let $y' \in \Pi_\beta(\mathscr{C}^\perp)$. So there exists $y = (y_1, y_2, \ldots, y_n) \in \mathscr{C}^\perp$ such that $y' = \Pi_\beta(y) = (y_{1,1}, y_{1,2}, \ldots, y_{1,m}, y_{2,1}, y_{2,2}, \ldots, y_{2,m}, \ldots, y_{n,1}, y_{n,2}, \ldots, y_{n,m})$, where $y_i = y_{i,1}\beta_1 + y_{i,2}\beta_2 + \cdots + y_{i,m}\beta_m$ for $1 \leq i \leq n$. This holds if and only if

$$\langle y, c\rangle = \sum_{i=1}^{n} Tr_{p^r,m}(y_i c_i) = 0 \text{ for all } c = (c_1, c_2, \ldots, c_n) \in \mathscr{C},$$

where $c_i = c_{i,1}\alpha_1 + c_{i,2}\alpha_2 + \cdots + c_{i,m}\alpha_m$ for $1 \leq i \leq n$. This further holds if and only if

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{\ell=1}^{m} y_{i,j}c_{i,\ell}Tr_{p^r,m}(\beta_j\alpha_\ell) = \sum_{i=1}^{n}\sum_{j=1}^{m} y_{i,j}c_{i,j} = \Pi_\beta(y)\cdot\Pi_\alpha(c) = 0 \text{ for all } c \in \mathscr{C},$$

(here $\cdot$ denotes the Euclidean bilinear form on $\mathcal{R}_{e,r}^{nm}$). This implies that $\langle y, c\rangle = 0$ for all $c \in \mathscr{C}$ if and only if $y' \cdot \Pi_\alpha(c) = \Pi_\beta(y)\cdot\Pi_\alpha(c) = 0$ for all $c \in \mathscr{C}$, which holds if and only if $y' \in (\Pi_\alpha(\mathscr{C}))^\perp$. From this, the desired result follows immediately. □

In the following theorem, we determine the type of the dual code of an additive code over $\mathcal{R}_{e,rm}$.

Theorem 7.2.2. *Let $\mathscr{C}$ be an additive code of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$. The dual code $\mathscr{C}^\perp$ of $\mathscr{C}$ is an additive code of the type $\{nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_e), \mathtt{k}_e, \mathtt{k}_{e-1}, \ldots, \mathtt{k}_2\}$ over $\mathcal{R}_{e,rm}$.*

Proof. Let $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be an ordered basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$ with the trace dual basis $\beta = \{\beta_1, \beta_2, \ldots, \beta_m\}$, (such a basis β always exists uniquely by Theorem 7.2.1). By Remark 7.2.1, we note that the code $\mathscr{C}$ is of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$ if and only if $\Pi_\alpha(\mathscr{C})$ is of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length nm over $\mathcal{R}_{e,r}$. Now by applying Theorem 3.10 of Norton and Sălăgean [80] and Proposition 7.2.1, the desired result follows. □

In the following lemma, we derive some sufficient conditions under which there exists a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$.

Lemma 7.2.2. *(a) When m is odd, there exists a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$.*

(b) When $\mathcal{R}_{e,rm} = \mathbb{F}_{2^{rm}}[u]/\langle u^e\rangle$ and $\mathcal{R}_{e,r} = \mathbb{F}_{2^r}[u]/\langle u^e\rangle$, there exists a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$.

Proof. (a) It follows from Corollary 3.3 of Bágio *et al.* [6].

(b) By Theorem 1 of [58], we see that there exists a self-dual basis $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathbb{F}_{2^{rm}}$ over $\mathbb{F}_{2^r}$. Now one can easily see that α is also a self-dual basis of $\mathbb{F}_{2^{rm}}[u]/\langle u^e\rangle$ over $\mathbb{F}_{2^r}[u]/\langle u^e\rangle$.

□

7.3 Additive self-orthogonal and self-dual codes over $\mathcal{R}_{e,rm}$

In this section, we will study additive self-orthogonal and self-dual codes over $\mathcal{R}_{e,rm}$. Towards this, we first observe that if $\mathscr{C}$ is an additive code over $\mathcal{R}_{e,rm}$ with a generator matrix $\mathcal{G}$ and a parity-check matrix $\mathcal{H}$, then we must have $Tr_{p^r,m}(\mathcal{G}\mathcal{H}^t) = 0$.

The following theorem provides necessary and sufficient conditions under which an additive code over $\mathcal{R}_{e,rm}$ is self-orthogonal or self-dual.

Theorem 7.3.1. *Let $\mathscr{C}$ be an additive code of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$ with a generator matrix $\mathcal{G}$. Then the code $\mathscr{C}$ is self-orthogonal if and* *only if the matrix*

$$Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t) = 0.$$

Furthermore, the code $\mathscr{C}$ *is self-dual if and only if the code* $\mathscr{C}$ *is self-orthogonal,* $\mathtt{k}_1 = nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_e)$ *and* $\mathtt{k}_i = \mathtt{k}_{e-i+2}$ *for* $2 \leq i \leq e$.

Proof. Its proof is a straightforward exercise. □

Now the following lemma relates Torsion codes of an additive self-orthogonal code over $\mathcal{R}_{e,rm}$.

Lemma 7.3.1. *Let* $\mathscr{C}$ *be an additive self-orthogonal code of length* n *over* $\mathcal{R}_{e,rm}$. *The following hold.*

(a) $Tor_i(\mathscr{C}) \subseteq Tor_i(\mathscr{C})^{\perp}$ *for* $1 \leq i \leq \lfloor \frac{e+1}{2} \rfloor$.

(b) $Tor_i(\mathscr{C}) \subseteq Tor_{e-i+1}(\mathscr{C})^{\perp}$ *for* $\lfloor \frac{e+1}{2} \rfloor + 1 \leq i \leq e$.

In particular, if $\mathscr{C}$ *is an additive self-dual code of length* n *over* $\mathcal{R}_{e,rm}$, *then we have*

$$Tor_i(\mathscr{C}) = Tor_{e-i+1}(\mathscr{C})^{\perp} \text{ for } \left\lceil \frac{e+1}{2} \right\rceil \leq i \leq e.$$

Proof. Working in a similar manner as in Lemma 2.2.1, the desired result follows. □

As a consequence of Lemma 7.3.1, we deduce the following:

Remark 7.3.1. *If* $\mathscr{C}$ *is an additive self-orthogonal code of the type* $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ *and length* n *over* $\mathcal{R}_{e,rm}$, *then we have*

$$2\mathtt{k}_1 + 2\mathtt{k}_2 + \cdots + 2\mathtt{k}_{e-i+1} + \mathtt{k}_{e-i+2} + \mathtt{k}_{e-i+3} + \cdots + \mathtt{k}_i \leq nm$$

for $\lceil \frac{e+1}{2} \rceil \leq i \leq e$. *From this, it follows that* $nm \geq 2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\frac{e}{2}}) + \mathtt{k}_{\frac{e}{2}+1}$ *if* e *is even, while* $nm \geq 2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\frac{e+1}{2}})$ *if* e *is odd.*

In particular, if $\mathscr{C}$ *is an additive self-dual code of the type* $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ *and length* n *over* $\mathcal{R}_{e,rm}$, *then we have*

$$\mathtt{k}_i = \mathtt{k}_{e-i+2} \text{ for } 1 \leq i \leq e.$$

From this, it follows that $nm = 2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\frac{e}{2}}) + \mathtt{k}_{\frac{e}{2}+1}$ *if* e *is even, while* $nm = 2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\frac{e+1}{2}})$ *if* e *is odd.*

In Chapter 3, we obtained enumeration formulae for all linear self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings of odd characteristic. In Chapters 4 and 5, we counted all linear self-orthogonal and self-dual codes of an arbitrary length over quasi-Galois rings and Galois rings of even characteristic, respectively. By Lemma 7.2.2, we see that when either m is odd or $\mathcal{R}_{e,rm} = \mathbb{F}_{2^{rm}}[u]/\langle u^e\rangle$ and $\mathcal{R}_{e,r} = \mathbb{F}_{2^r}[u]/\langle u^e\rangle$, there exists a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$. Further, by Proposition 7.2.1, we observe that if $\alpha = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$, then Π_α is a duality preserving $\mathcal{R}_{e,r}$-module homomorphism, *i.e.*, $\Pi_\alpha(\mathscr{C}^\perp) = (\Pi_\alpha(\mathscr{C}))^\perp$. This implies that Π_α induces a one-to-one correspondence between additive self-orthogonal (*resp.* additive self-dual) codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$ and linear self-orthogonal (*resp.* linear self-dual) codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length nm over $\mathcal{R}_{e,r}$. Thus one can obtain enumeration formulae for all additive self-orthogonal and self-dual codes of an arbitrary length over $\mathcal{R}_{e,rm}$ by applying the results obtained in Chapters 3-5 in the following three cases:

(i) both p and m are odd

(ii) $p = 2$ and $\mathfrak{s} = 1$, and

(iii) $p = 2$, $\kappa = 1$ and m is odd.

Throughout this section, let n be a positive integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$. Further, let us define $n_0 = 0$ and $n_i = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_i$ for $1 \le i \le e+1$. Further, let $\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$ and $\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$ denote the number of distinct additive self-orthogonal and self-dual codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$, respectively. Further, let $\mathfrak{N}_e(n)$ and $\mathfrak{M}_e(n)$ denote the number of distinct additive self-orthogonal and self-dual codes of length n over $\mathcal{R}_{e,rm}$, respectively. We also recall that

$$s = \left\lfloor \frac{e}{2} \right\rfloor.$$

7.3.1 The case when both p and m are odd

Throughout this section, we assume that p is an odd prime and m is an odd integer.

In the following theorem, we count all additive self-orthogonal codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.2. *Let $e \geq 2$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.*

(a) When e is even, we have

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{p^r}(nm, n_s) \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} \prod\limits_{j=s+1}^{e} \begin{bmatrix} \mathtt{k}_j + nm - n_j - n_{e-j+1} \\ \mathtt{k}_j \end{bmatrix}_{p^r} \\ \times (p^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(nm - n_{\ell+1} - 1) + n_{s+\ell}(nm - n_{s+1+\ell} - n_{s-\ell}) + n_s(nm - n_{s+1}) - \frac{n_s(n_s+1)}{2}} \\ \textit{if } n_{e-i+1} + n_i \leq nm \quad \textit{for } s+1 \leq i \leq e; \\ 0 \quad \textit{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{p^r}(nm, n_{s+1}) \prod\limits_{i=1}^{s+1} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} \prod\limits_{j=s+2}^{e} \begin{bmatrix} \mathtt{k}_j + nm - n_j - n_{e-j+1} \\ \mathtt{k}_j \end{bmatrix}_{p^r} \\ \times (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(nm - n_{\ell+1} - 1) + n_{s+\ell}(nm - n_{s+1+\ell} - n_{s+1-\ell})} \\ \textit{if } n_{e-i+1} + n_i \leq nm \quad \textit{for } s+1 \leq i \leq e; \\ 0 \quad \textit{otherwise.} \end{cases}$$

Proof. Since m is odd, we see, by Lemma 7.2.2(a), that there exists a self-dual basis of $\mathcal{R}_{e,rm}$ over $\mathcal{R}_{e,r}$. By Proposition 7.2.1, we note that there exists a one-to-one correspondence between additive self-orthogonal codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$ and linear self-orthogonal codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length nm over $\mathcal{R}_{e,r}$. Now the desired result follows by applying Theorems 3.2.2, 3.3.2 and 3.4.2. □

In the following theorem, we count all additive self-dual codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.3. *Let $e \geq 2$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.*

(a) When e is even, we have

$$\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{p^r}\left(nm, n_s\right) \displaystyle\prod_{i=1}^{s} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(nm - n_{\ell+1} - 1) - \frac{n_s(n_s-1)}{2}} \\ \textit{if } \mathtt{k}_v = \mathtt{k}_{e-v+2} \;\; \textit{for} \;\; 1 \leq v \leq e+1; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) When e is odd, we have

$$\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} 2 \displaystyle\prod_{b=1}^{\frac{nm}{2}-1} (p^{rb}+1) \prod_{i=1}^{s+1} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} (p^r)^{\sum\limits_{\ell=1}^{s} n_\ell(nm - n_{\ell+1} - 1)} \\ \textit{if } n \textit{ is an even integer, } (-1)^{\frac{nm}{2}} \textit{ is a square in } \overline{\mathcal{R}}_{e,r} \\ \textit{and } \mathtt{k}_v = \mathtt{k}_{e-v+2} \textit{ for } 1 \leq v \leq e+1; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

Proof. Working as in Theorem 7.3.2 and by applying Theorems 3.2.4, 3.3.4 and 3.4.4, we get the desired result. □

Now for an integer d satisfying $2 \leq d \leq e$ and for non-negative integers $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_d$, let us define

$$z_\ell(k_1, k_2, \ldots, k_d) = (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_\ell)\big(nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\ell+1}) - 1\big) \qquad (7.3.1)$$

for $1 \leq \ell \leq d-1$, and let us define

$$\begin{aligned} \gamma_j(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_d) \;\; &= \;\; z_j(k_1, k_2, \ldots, k_d) + (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\lfloor \frac{d}{2} \rfloor + j})\big(nm - (\mathtt{k}_1 \\ &\quad + \mathtt{k}_2 + \cdots + \mathtt{k}_{\lceil \frac{d+1}{2} \rceil + j}) - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{\lfloor \frac{d+1}{2} \rfloor - j})\big) \qquad (7.3.2) \end{aligned}$$

for $1 \leq j \leq \lceil \frac{d}{2} \rceil - 1$.

The following theorem provides the enumeration formula for all additive self-orthogonal codes of length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.4. *For an integer $e \geq 2$, the following hold.*

(a) When e is even, we have

$$\begin{aligned}\mathfrak{N}_e(n) &= \sum \sigma_{p^r}\left(nm, \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s\right) (p^r)^{\sum\limits_{\ell=1}^{s-1} \gamma_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e) + \widetilde{\Theta}_e(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)} \\ &\quad \times \prod_{j=s+1}^{e} \begin{bmatrix} \mathtt{k}_j + nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_j) - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e-j+1}) \\ \mathtt{k}_j \end{bmatrix}_{p^r} \\ &\quad \times \prod_{i=1}^{s} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{p^r},\end{aligned}$$

where $\widetilde{\Theta}_e(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) \left(\frac{2nm - 2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{s+1}) - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) - 1}{2} \right)$ and the summation $\sum$ runs over all non-negative integers $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e$ satisfying $2\mathtt{k}_1 + 2\mathtt{k}_2 + \cdots + 2\mathtt{k}_{e-i+1} + \mathtt{k}_{e-i+2} + \mathtt{k}_{e-i+3} + \cdots + \mathtt{k}_i \leq nm$ for $s+1 \leq i \leq e$.

(b) When e is odd, we have

$$\begin{aligned}\mathfrak{N}_e(n) &= \sum \sigma_{p^r}\big(nm, \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{s+1}\big) (p^r)^{\sum\limits_{\ell=1}^{s} \gamma_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)} \prod_{i=1}^{s+1} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} \\ &\quad \times \prod_{j=s+2}^{e} \begin{bmatrix} \mathtt{k}_j + nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_j) - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e-j+1}) \\ \mathtt{k}_j \end{bmatrix}_{p^r},\end{aligned}$$

where the summation $\sum$ runs over all non-negative integers $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e$ satisfying $2\mathtt{k}_1 + 2\mathtt{k}_2 + \cdots + 2\mathtt{k}_{e-i+1} + \mathtt{k}_{e-i+2} + \mathtt{k}_{e-i+3} + \cdots + \mathtt{k}_i \leq nm$ for $s+1 \leq i \leq e$.

Proof. It follows immediately from Theorem 7.3.2. □

The following theorem provides the enumeration formula for all additive self-dual codes of length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.5. *For an integer $e \geq 2$, the following hold.*

(a) When e is even, we have

$$\mathfrak{M}_e(n) = \sum \sigma_{p^r}(nm, \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) \prod_{i=1}^{s} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{p^r}$$
$$\times (p^r)^{\sum\limits_{\ell=1}^{s-1} z_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s) + \widetilde{\lambda}_e(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)},$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) + \mathtt{k}_{s+1} = nm$ *and the number* $\widetilde{\lambda}_e(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s)$ *is given by*

$$\widetilde{\lambda}_e(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s) = (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) \left(\frac{\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s - 1}{2} \right).$$

(b) When e is odd, we have

$$\mathfrak{M}_e(n) = \begin{cases} \displaystyle\sum 2 \prod_{b=1}^{\frac{nm}{2}-1} (p^{rb}+1)(p^r)^{\sum\limits_{\ell=1}^{s} z_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)} \prod_{i=1}^{s+1} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{p^r} \\ \textit{if } n \textit{ is an even integer and } (-1)^{\frac{nm}{2}} \textit{ is a square in } \overline{\mathcal{R}}_{e,r}; \\ 0 \qquad \textit{otherwise,} \end{cases}$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{s+1}) = nm$.

Proof. It follows immediately from Theorem 7.3.3. □

7.3.2 The case $p = 2$ and $\mathfrak{s} = 1$

Throughout this section, we assume that $p = 2$ and $\mathfrak{s} = 1$, *i.e.*, $\mathcal{R}_{e,rm} = \mathbb{F}_{2^{rm}}[u]/\langle u^e \rangle$ and $\mathcal{R}_{e,r} = \mathbb{F}_{2^r}[u]/\langle u^e \rangle$.

In the following theorem, we count all additive self-orthogonal codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.6. *Let* $e \geq 2$ *be an integer, and let* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ *be non-negative integers satisfying* $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.

(a) *When e is even, we have*

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{2^r}(nm, n_s) \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{2^r} \prod\limits_{j=s+1}^{e} \begin{bmatrix} \mathtt{k}_j + nm - n_j - n_{e+1-j} \\ \mathtt{k}_j \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(nm - n_{\ell+1}) + n_{s+\ell}(nm - n_{s+\ell+1} - n_{s-\ell}) + n_s(nm - n_{s+1}) - \frac{n_s(n_s-1)}{2}} \\ \textit{if } n_{e-i+1} + n_i \leq nm \quad \textit{for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) *When e is odd, we have*

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{2^r}(nm, n_{s+1}) \prod\limits_{i=1}^{s+1} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{2^r} \prod\limits_{j=s+2}^{e} \begin{bmatrix} \mathtt{k}_j + nm - n_j - n_{e+1-j} \\ \mathtt{k}_j \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{\ell=1}^{s} n_\ell(nm - n_{\ell+1}) + n_{s+\ell}(nm - n_{s+1+\ell} - n_{s+1-\ell})} \\ \textit{if } n_{e-i+1} + n_i \leq nm \quad \textit{for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

Proof. Working in a similar manner as in Theorem 7.3.2 and by applying Lemma 7.2.2(b) and Theorem 4.4.1, the desired result follows immediately. □

In the following theorem, we count all additive self-dual codes of the type $\{\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e\}$ and length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.7. *Let $e \geq 2$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.*

(a) *When e is even, we have*

$$\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \sigma_{2^r}(nm, n_s) \prod\limits_{i=1}^{s} \begin{bmatrix} n_i \\ \mathtt{k}_i \end{bmatrix}_{2^r} (2^r)^{\sum\limits_{\ell=1}^{s-1} n_\ell(nm - n_{\ell+1}) + \frac{n_s(n_s+1)}{2}} \\ \textit{if } \mathtt{k}_v = \mathtt{k}_{e-v+2} \quad \textit{for } \ 1 \leq v \leq e+1; \\ 0 \qquad \textit{otherwise.} \end{cases}$$

(b) *When e is odd, we have*

$$\mathfrak{M}_e(n;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)=\begin{cases}\prod\limits_{j=1}^{\frac{nm}{2}-1}((2^r)^{\frac{nm}{2}-j}+1)\prod\limits_{i=1}^{s+1}\begin{bmatrix}n_i\\ \mathtt{k}_i\end{bmatrix}_{2^r}(2^r)^{\sum\limits_{\ell=1}^{s}n_\ell(nm-n_{\ell+1})}\\ \textit{if } nm \textit{ is an even integer and } \mathtt{k}_v=\mathtt{k}_{e-v+2} \textit{ for } 1\le v\le e+1;\\ \\ 0 \qquad \textit{otherwise.}\end{cases}$$

Proof. Working as in Theorem 7.3.2 and by applying Lemma 7.2.2(b) and Theorem 4.4.2, we get the desired result. □

Now for an integer d satisfying $1\le d\le e$ and for non-negative integers $\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_d$, let $z_j(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_d)$ and $\gamma_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_d)$ be as defined by (7.3.1) and (7.3.2), respectively, where $1\le j\le d-1$ and $1\le \ell\le \lceil\frac{d}{2}\rceil-1$.

In the following theorem, we count all additive self-orthogonal codes of length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.8. *For an integer $e\ge 2$, the following hold.*

(a) When e is even, we have

$$\begin{aligned}\mathfrak{N}_e(n) &= \sum \sigma_{2^r}\big(nm,\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s\big)\prod_{i=1}^{s}\begin{bmatrix}\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_i\\ \mathtt{k}_i\end{bmatrix}_{2^r}\\ &\times\prod_{j=s+1}^{e}\begin{bmatrix}\mathtt{k}_j+nm-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_j)-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_{e+1-j})\\ \mathtt{k}_j\end{bmatrix}_{2^r}\\ &\times(2^r)^{\sum\limits_{\ell=1}^{s-1}\gamma_\ell(k_1,k_2,\ldots,k_e)+\sum\limits_{a=1}^{s}(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_a)+z_s(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)-\lambda'_e(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)},\end{aligned}$$

where $\lambda'_e(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)=(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s)\left(\frac{\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s-1}{2}\right)$ and the summation $\sum$ runs over all non-negative integers $\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e$ satisfying $2\mathtt{k}_1+2\mathtt{k}_2+\cdots+2\mathtt{k}_{e-i+1}+\mathtt{k}_{e-i+2}+\mathtt{k}_{e-i+3}+\cdots+\mathtt{k}_i\le nm$ for $s+1\le i\le e$.

(b) When e is odd, we have

$$\begin{aligned}\mathfrak{N}_e(n) &= \sum \sigma_{2^r}\big(nm,\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_{s+1}\big)\prod_{i=1}^{s+1}\begin{bmatrix}\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_i\\ \mathtt{k}_i\end{bmatrix}_{2^r}\\ &\times\prod_{j=s+2}^{e}\begin{bmatrix}\mathtt{k}_j+nm-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_j)-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_{e+1-j})\\ \mathtt{k}_j\end{bmatrix}_{2^r}\end{aligned}$$

$$\times (2^r)^{\sum\limits_{\ell=1}^{s} \gamma_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)+\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_\ell},$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e$ *satisfying* $2\mathtt{k}_1+2\mathtt{k}_2+\cdots+2\mathtt{k}_{e-i+1}+\mathtt{k}_{e-i+2}+\mathtt{k}_{e-i+3}+\cdots+\mathtt{k}_i \leq nm$ *for* $s+1 \leq i \leq e$.

Proof. It follows immediately from Theorem 7.3.6. □

In the following theorem, we count all additive self-dual codes of length n over $\mathcal{R}_{e,rm}$.

Theorem 7.3.9. *For an integer* $e \geq 2$, *the following hold.*

(a) When e is even, we have

$$\mathfrak{M}_e(n) = \sum \sigma_{2^r}(nm, \mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s) \prod_{i=1}^{s} \begin{bmatrix} \mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{2^r}$$
$$\times (2^r)^{\sum\limits_{\ell=1}^{s-1} z_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)+\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_\ell+\lambda_e''(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)},$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s)+\mathtt{k}_{s+1} = nm$ *and the number* $\lambda_e''(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s)$ *is given by*

$$\lambda_e''(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s) = (\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s)\left(\frac{\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s+1}{2}\right).$$

(b) When e is odd, we have

$$\mathfrak{M}_e(n) = \begin{cases} \sum \prod\limits_{j=1}^{\frac{nm}{2}-1} ((2^r)^{\frac{nm}{2}-j}+1) \prod\limits_{i=1}^{s+1} \begin{bmatrix} \mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_i \\ \mathtt{k}_i \end{bmatrix}_{2^r} & \\ \times (2^r)^{\sum\limits_{\ell=1}^{s} z_\ell(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)+\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_\ell} & \text{if } nm \text{ is an even integer;} \\ 0 \quad \text{otherwise,} & \end{cases}$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_{s+1}) = nm$.

Proof. It follows immediately from Theorem 7.3.7. □

7.3.3 The case when $p = 2$, $\kappa = 1$ and m is odd

Throughout this section, we assume that $p = 2$, $\kappa = 1$ and m is odd, *i.e.*, $\mathcal{R}_{e,rm} = GR(2^e, rm)$ and $\mathcal{R}_{e,r} = GR(2^e, r)$, where m is an odd integer. Here to obtain the enumeration formulae for the numbers $\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$, $\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$, $\mathfrak{N}_e(n)$ and $\mathfrak{M}_e(n)$, we will distinguish the following two cases: (i) $e = 2$ and (ii) $e \geq 3$.

In the following theorem, we consider the case $e = 2$ and obtain enumeration formulae for the numbers $\mathfrak{N}_2(n; \mathtt{k}_1, \mathtt{k}_2)$ and $\mathfrak{N}_2(n)$.

Theorem 7.3.10. *We have*

$$\mathfrak{N}_2(n; \mathtt{k}_1, \mathtt{k}_2) = \begin{cases} \mathfrak{D}_r(nm; \mathtt{k}_1) 2^{\frac{r\mathtt{k}_1(2nm - 3\mathtt{k}_1 - 2\mathtt{k}_2 + 1)}{2}} \begin{bmatrix} nm - 2\mathtt{k}_1 \\ \mathtt{k}_2 \end{bmatrix}_{2^r} & \textit{if } 2\mathtt{k}_1 + \mathtt{k}_2 \leq nm; \\ 0 & \textit{otherwise} \end{cases}$$

and

$$\mathfrak{N}_2(n) = \sum_{\mathtt{k}_1=0}^{\lfloor \frac{nm}{2} \rfloor} \mathfrak{D}_r(nm; \mathtt{k}_1) \sum_{\mathtt{k}_2=0}^{nm-2\mathtt{k}_1} 2^{\frac{r\mathtt{k}_1(2nm - 3\mathtt{k}_1 - 2\mathtt{k}_2 + 1)}{2}} \begin{bmatrix} nm - 2\mathtt{k}_1 \\ \mathtt{k}_2 \end{bmatrix}_{2^r},$$

where the number $\mathfrak{D}_r(nm; \mathtt{k}_1)$ is as obtained in Theorem 5.3.1.

Proof. Working as in Theorem 7.3.2 and by applying Lemma 7.2.2(a) and Theorem 5.5.1, the desired result follows. □

In the following theorem, we consider the case $e = 2$ and obtain enumeration formulae for the numbers $\mathfrak{M}_2(n; \mathtt{k}_1, \mathtt{k}_2)$ and $\mathfrak{M}_2(n)$.

Theorem 7.3.11. *We have*

$$\mathfrak{M}_2(n; \mathtt{k}_1, \mathtt{k}_2) = \begin{cases} \mathfrak{D}_r(nm; \mathtt{k}_1) 2^{\frac{r\mathtt{k}_1(\mathtt{k}_1+1)}{2}} & \textit{if } 2\mathtt{k}_1 + \mathtt{k}_2 = nm; \\ 0 & \textit{otherwise} \end{cases}$$

and

$$\mathfrak{M}_2(n) = \sum_{\mathtt{k}_1=0}^{\lfloor \frac{nm}{2} \rfloor} \mathfrak{D}_r(nm; \mathtt{k}_1) 2^{\frac{r\mathtt{k}_1(\mathtt{k}_1+1)}{2}},$$

where the number $\mathfrak{D}_r(nm; \mathtt{k}_1)$ is as determined in Theorem 5.3.1.

Proof. It follows immediately by applying Theorems 7.3.1 and 7.3.10. □

In the following theorem, we consider the case $e \geq 3$ and obtain an enumeration formula for the number $\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$.

Theorem 7.3.12. *Let $e \geq 3$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.*

(a) When e is even, we have

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \lambda_0(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s) \prod\limits_{v=1}^{s-1} \begin{bmatrix} n_v \\ \mathtt{k}_v \end{bmatrix}_{2^r} \prod\limits_{\ell=s+1}^{e} \begin{bmatrix} \mathtt{k}_\ell + nm - n_\ell - n_{e+1-\ell} \\ \mathtt{k}_\ell \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{i=1}^{s-1} n_i(nm - n_{i+1} - 1) + \sum\limits_{j=1}^{s-1} n_{s+j}(nm - n_{s+j+1} - n_{s-j}) + n_s(nm - n_{s+1}) - \frac{n_s(n_s-1)}{2}} \\ \textit{if } n_{e-i+1} + n_i \leq nm \textit{ for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise,} \end{cases}$$

where the number $\lambda_0(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s)$ is as determined in Theorem 5.5.3(a).

(b) When e is odd, we have

$$\mathfrak{N}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \begin{cases} \lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}) \prod\limits_{\ell=s+2}^{e} \begin{bmatrix} k_\ell + nm - n_\ell - n_{e+1-\ell} \\ \mathtt{k}_\ell \end{bmatrix}_{2^r} \\ \times \prod\limits_{v=1}^{s-1} \begin{bmatrix} n_v \\ \mathtt{k}_v \end{bmatrix}_{2^r} (2^r)^{\sum\limits_{i=1}^{s} n_i(nm - n_{i+1} - 1) + \sum\limits_{j=1}^{s} n_{s+j}(nm - n_{s+j+1} - n_{s+1-j}) + n_s} \\ \textit{if } n_{e-i+1} + n_i \leq nm \quad \textit{for } s+1 \leq i \leq e; \\ 0 \qquad \textit{otherwise,} \end{cases}$$

where the number $\lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1})$ is as determined in Theorem 5.5.3(b).

Proof. Working as in Theorem 7.3.2 and by applying Lemma 7.2.2(a) and Theorem 5.5.3, the desired result follows. □

In the following theorem, we consider the case $e \geq 3$ and obtain an enumeration formula for the number $\mathfrak{M}_e(n; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$.

Theorem 7.3.13. *Let $e \geq 3$ be an integer, and let $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{e+1}$ be non-negative integers satisfying $nm = \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1}$.*

(a) When e is even, we have

$$\mathfrak{M}_e(n;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)=\begin{cases}\lambda_0(nm;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)(2^r)^{\sum\limits_{i=1}^{s-1}n_i(nm-n_{i+1}-1)+\frac{n_s(n_s+1)}{2}}\prod\limits_{j=1}^{s-1}\begin{bmatrix}n_j\\ \mathtt{k}_j\end{bmatrix}_{2^r}\\ \textit{if}\ \ \mathtt{k}_v=\mathtt{k}_{e-v+2}\ \textit{for}\ 1\leq v\leq e+1;\\ 0\qquad \textit{otherwise,}\end{cases}$$

where the number $\lambda_0(nm;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)$ is as obtained in Theorem 5.5.3(a).

(b) When e is odd, we have

$$\mathfrak{M}_e(n;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)=\begin{cases}\lambda_1(nm;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_{s+1})(2^r)^{\sum\limits_{i=1}^{s}n_i(nm-n_{i+1}-1)+n_s}\prod\limits_{j=1}^{s-1}\begin{bmatrix}n_j\\ k_j\end{bmatrix}_{2^r}\\ \textit{if}\ n\ \textit{is even and}\ \mathtt{k}_v=\mathtt{k}_{e-v+2}\ \textit{for}\ 1\leq v\leq e+1;\\ 0\qquad \textit{otherwise,}\end{cases}$$

where the number $\lambda_1(nm;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_{s+1})$ is as obtained in Theorem 5.5.3(b).

Proof. It follows immediately by applying Theorems 7.3.1 and 7.3.12. □

In the following theorem, we consider the case $e\geq 3$ and obtain an enumeration formula for the number $\mathfrak{N}_e(n)$.

Theorem 7.3.14. *For an integer $e\geq 3$, the following hold.*

(a) When e is even, we have

$$\mathfrak{N}_e(n)=\sum\lambda_0(nm;\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_s)(2^r)^{\Lambda^*(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)}\prod_{j=1}^{s-1}\begin{bmatrix}\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_j\\ \mathtt{k}_j\end{bmatrix}_{2^r}$$
$$\times\prod_{\ell=s+1}^{e}\begin{bmatrix}\mathtt{k}_\ell+nm-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_\ell)-(\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_{e+1-\ell})\\ \mathtt{k}_\ell\end{bmatrix}_{2^r},$$

where the summation $\sum$ runs over all non-negative integers $\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e$ satisfying $2\mathtt{k}_1+2\mathtt{k}_2+\cdots+2\mathtt{k}_{e-i+1}+\mathtt{k}_{e-i+2}+\mathtt{k}_{e-i+3}+\cdots+\mathtt{k}_i\leq nm$ for $s+1\leq i\leq e$

and the number $\Lambda^*(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$ is given by

$$\begin{aligned}\Lambda^*(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) &= \sum_{i=1}^{s} \gamma_i(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) + \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s \\ &\quad -(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s)\left(\frac{\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s - 1}{2}\right).\end{aligned}$$

(b) When e is odd, we have

$$\begin{aligned}\mathfrak{N}_e(n) = \sum \lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1})(2^r)^{\Lambda''(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_e)} \prod_{j=1}^{s-1} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_j \\ \mathtt{k}_j \end{bmatrix}_{2^r} \\ \times \prod_{\ell=s+2}^{e} \begin{bmatrix} \mathtt{k}_\ell + nm - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_\ell) - (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{e+1-\ell}) \\ \mathtt{k}_\ell \end{bmatrix}_{2^r},\end{aligned}$$

where the summation $\sum$ runs over all non-negative integers $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e$ satisfying $2\mathtt{k}_1 + 2\mathtt{k}_2 + \cdots + 2\mathtt{k}_{e-i+1} + \mathtt{k}_{e-i+2} + \mathtt{k}_{e-i+3} + \cdots + \mathtt{k}_i \leq nm$ for $s+1 \leq i \leq e$ and the number $\Lambda''(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e)$ is given by

$$\Lambda''(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) = \sum_{i=1}^{s} \gamma_i(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_e) + (\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s).$$

(Here the numbers $\lambda_0(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s)$ and $\lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1})$ are as obtained in Theorem 5.5.3.)

Proof. It follows immediately from Theorem 7.3.12. □

In the following theorem, we consider the case $e \geq 3$ and obtain an enumeration formula for the number $\mathfrak{M}_e(n)$.

Theorem 7.3.15. *For an integer $e \geq 3$, the following hold.*

(a) When e is even, we have

$$\begin{aligned}\mathcal{M}_e(n) = \sum \lambda_0(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s) \prod_{j=1}^{s-1} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_j \\ \mathtt{k}_j \end{bmatrix}_{2^r} \\ \times (2^r)^{\sum\limits_{i=1}^{s-1} z_i(\mathtt{k}_1,\mathtt{k}_2,\ldots,\mathtt{k}_{s+1}) + (\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s)\left(\frac{\mathtt{k}_1+\mathtt{k}_2+\cdots+\mathtt{k}_s+1}{2}\right)},\end{aligned}$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s) + \mathtt{k}_{s+1} = nm$.

(b) When e *is odd, we have*

$$\mathfrak{M}_e(n) = \begin{cases} \sum \lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1})(2^r)^{\sum\limits_{i=1}^{s} z_i(\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}) + \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_s} & \\ \times \prod\limits_{j=1}^{s-1} \begin{bmatrix} \mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_j \\ \mathtt{k}_j \end{bmatrix}_{2^r} & \text{if } n \text{ is an even integer;} \\ 0 \quad \text{otherwise,} & \end{cases}$$

where the summation $\sum$ *runs over all non-negative integers* $\mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1}$ *satisfying* $2(\mathtt{k}_1 + \mathtt{k}_2 + \cdots + \mathtt{k}_{s+1}) = nm$.
(Here the numbers $\lambda_0(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_s)$ *and* $\lambda_1(nm; \mathtt{k}_1, \mathtt{k}_2, \ldots, \mathtt{k}_{s+1})$ *are as obtained in Theorem 5.5.3.)*

Proof. It follows immediately from Theorem 7.3.13. □

7.4 ACD codes over $\mathcal{R}_{e,rm}$

In this section, we count all ACD codes of an arbitrary length over $\mathcal{R}_{e,rm}$. First of all, we show, in the following theorem, that any ACD code over $\mathcal{R}_{e,rm}$ is a free code, *i.e.*, it is a free $\mathcal{R}_{e,r}$-submodule of $\mathcal{R}_{e,rm}^n$.

Theorem 7.4.1. *Every ACD code over* $\mathcal{R}_{e,rm}$ *is a free code.*

Proof. Working as in Theorem 6.2.1 and applying Theorem 2 of Kaplansky [59], the desired result follows. □

Remark 7.4.1. *Working as in Proposition 3.13 of Norton and Sălăgean [80], we see that an additive code* $\mathscr{C}$ *of length* n *over* $\mathcal{R}_{e,rm}$ *is a free code if and only if* $Tor_1(\mathscr{C}) = Tor_2(\mathscr{C}) = \cdots = Tor_e(\mathscr{C})$. *So we will call* $Tor_1(\mathscr{C})$ *as the Torsion code of the free additive code* $\mathscr{C}$ *over* $\mathcal{R}_{e,rm}$.

From now on, we shall refer to an additive code $\mathscr{C}$ of length n, rank k and Hamming distance d over $\mathcal{R}_{e,rm}$ as an additive $[n, k, d]$-code over $\mathcal{R}_{e,rm}$.

The following theorem provides a necessary and sufficient condition under which a free additive code of length n over $\mathcal{R}_{e,rm}$ is ACD.

Theorem 7.4.2. *Let $\mathcal{C}$ be a free additive code of length n over $\mathcal{R}_{e,rm}$ with a generator matrix $\mathcal{G}$. The code $\mathcal{C}$ is ACD if and only if the matrix $Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t)$ is non-singular, i.e., $\det(Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t))$ is a unit in $\mathcal{R}_{e,r}$.*

Proof. To prove the result, suppose that $\mathcal{C}$ is an ACD code. Here we assert that the matrix $Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t)$ is non-singular.

To prove this assertion, we suppose, on the contrary, that the matrix $Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t)$ is singular. Thus there exists a non-zero vector $z \in \mathcal{R}_{e,r}^k$ satisfying $Tr_{p^r,m}(z\mathcal{G}\mathcal{G}^t) = zTr_{p^r,m}(\mathcal{G}\mathcal{G}^t) = 0$. From this, it follows that the vector $z\mathcal{G} \in \mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$, which gives $z\mathcal{G} = 0$. As the code $\mathcal{C}$ is ACD, we see, by Theorem 7.4.1, that the code $\mathcal{C}$ is a free code over $\mathcal{R}_{e,rm}$, which implies that the rows of the matrix $\mathcal{G}$ are linearly independent over $\mathcal{R}_{e,r}$. From this, we obtain $z = 0$, which is a contradiction.

Conversely, let us assume that the matrix $Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t)$ is non-singular. Here, we assert that the code $\mathcal{C}$ is ACD, *i.e.*, $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. To prove this assertion, let $\upsilon \in \mathcal{C} \cap \mathcal{C}^{\perp}$. One can write $\upsilon = \upsilon'\mathcal{G}$ for some $\upsilon' \in \mathcal{R}_{e,r}^k$. This implies that $\upsilon' Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t) = Tr_{p^r,m}(\upsilon'\mathcal{G}\mathcal{G}^t) = 0$. Since $Tr_{p^r,m}(\mathcal{G}\mathcal{G}^t)$ is non-singular, we get $\upsilon' = 0$, which implies that $\upsilon = 0$. This proves the assertion. □

In the following theorem, we show that if $\mathcal{C}$ and $\mathcal{D}$ are ACD codes over $\mathcal{R}_{e,rm}$, then their direct sum $\mathcal{C} \oplus \mathcal{D}$ is also an ACD code over $\mathcal{R}_{e,rm}$.

Theorem 7.4.3. *Let $\mathcal{C}$ be an ACD $[n_1, k_1, d_1]$-code over $\mathcal{R}_{e,rm}$, and let $\mathcal{D}$ be an ACD $[n_2, k_2, d_2]$-code over $\mathcal{R}_{e,rm}$. The code $\mathcal{C} \oplus \mathcal{D} = \{(c, d) : c \in \mathcal{C}$ and $d \in \mathcal{D}\}$ is an ACD $[n_1 + n_2, k_1 + k_2, \min\{d_1, d_2\}]$-code over $\mathcal{R}_{e,rm}$.*

Proof. Let $G_1 \in \mathcal{M}_{k_1 \times n_1}(\mathcal{R}_{e,rm})$ and $G_2 \in \mathcal{M}_{k_2 \times n_2}(\mathcal{R}_{e,rm})$ be generator matrices of the codes $\mathcal{C}$ and $\mathcal{D}$, respectively. It is easy to observe that their direct sum $\mathcal{C} \oplus \mathcal{D}$ is an additive code of length $n_1 + n_2$ and rank $k_1 + k_2$ over $\mathcal{R}_{e,rm}$ with a generator matrix

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}.$$

Since $\mathcal{C}$ and $\mathcal{D}$ are ACD codes over $\mathcal{R}_{e,rm}$, we see, by Theorem 7.4.2, that $\det(Tr_{p^r,m}(G_1G_1^t))$ and $\det(Tr_{p^r,m}(G_2G_2^t))$ are units in $\mathcal{R}_{e,r}$. We next note that

$$\det(Tr_{p^r,m}(GG^t)) = \det(Tr_{p^r,m}(G_1G_1^t))\det(Tr_{p^r,m}(G_2G_2^t)),$$

which implies that $\det(Tr_{p^r,m}(GG^t))$ is also a unit in $\mathcal{R}_{e,r}$. This, by Theorem 7.4.2, further implies that $\mathcal{C}\oplus\mathcal{D}$ is an ACD code over $\mathcal{R}_{e,rm}$. Further, it is easy to observe that the Hamming distance of the code $\mathcal{C}\oplus\mathcal{D}$ is $\min\{d_1, d_2\}$. □

An additive code C of length n over $\overline{\mathcal{R}}_{e,rm}$ is defined as an $\overline{\mathcal{R}}_{e,r}$-linear subspace of $\overline{\mathcal{R}}_{e,rm}^n$. Further, the code C is called an additive code with complementary dual (*i.e.*, an ACD code) if it satisfies $C\cap C^{\perp} = \{0\}$. We next make the following observation.

Lemma 7.4.1. *Let $\mathscr{C}$ be an additive code of length n over $\mathcal{R}_{e,rm}$ with a generator matrix $\mathcal{G}$. The following three statements are equivalent:*

(a) The code $\mathscr{C}$ is an ACD code.

(b) The code $\mathscr{C}$ is a free code and the matrix $\overline{T}r_{p^r,m}(\overline{\mathcal{G}\mathcal{G}}^t)$ is non-singular.

(c) We have $Tor_1(\mathscr{C}) = Tor_2(\mathscr{C}) = \cdots = Tor_e(\mathscr{C})$ and the Torsion code $Tor_1(\mathscr{C})$ is an ACD code over $\overline{\mathcal{R}}_{e,rm}$ with a generator matrix $\overline{\mathcal{G}}$.

Proof. Working as in Theorem 6.2.3, the desired result follows. □

By the above lemma, we see that an additive code of length n over $\mathcal{R}_{e,rm}$ is an ACD code if and only if it is a free code whose Torsion code is an ACD code of length n over $\overline{\mathcal{R}}_{e,rm}(\simeq \mathbb{F}_{p^{rm}})$. In the following theorem, we provide a method to construct ACD codes over $\mathbb{F}_{2^{rm}}$.

Theorem 7.4.4. *Let n, k be positive integers satisfying $1\leq k\leq n$. Let $\mathcal{C}$ be an $\mathbb{F}_{2^r}$-additive code of length n and dimension k over $\mathbb{F}_{2^{rm}}$ (i.e., k-dimensional $\mathbb{F}_{2^r}$-linear subspace of $\mathbb{F}_{2^{rm}}^n$) with a generator matrix*

$$G = \begin{bmatrix} a & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 & b\\ 0 & a & \cdots & 0 & 1 & 1 & \cdots & 1 & b\\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots\\ 0 & 0 & \cdots & a & 1 & 1 & \cdots & 1 & b \end{bmatrix},$$

where $a \in \mathbb{F}_{2^{rm}}$ satisfies $Tr_{2^r,m}(a^2) \neq 0$ and $b = 0$ if $n-k$ is odd, while $b = 1$ if $n-k$ is even. Then the code $\mathcal{C}$ is an ACD code over $\mathbb{F}_{2^{rm}}$.

Proof. It is easy to see that $\det(Tr_{2^r,m}(GG^t)) = (Tr_{2^r,m}(a^2))^k \neq 0$. Now the desired result follows by applying Theorem 7.4.2. □

Now, we proceed to count all ACD codes of an arbitrary length n over $\mathcal{R}_{e,rm}$. For this, we see, by Lemma 7.4.1, that an additive code $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ is an ACD code if and only if $Tor_1(\mathscr{C}) = Tor_2(\mathscr{C}) = \cdots = Tor_e(\mathscr{C})$ and its Torsion code $Tor_1(\mathscr{C})$ is an ACD code of length n over $\overline{\mathcal{R}}_{e,rm}$. First of all, we will enumerate all ACD codes of length n and rank k over $\mathcal{R}_{e,rm}$ with a prescribed Torsion code. To do this, throughout this section, we assume that $\mathscr{D}$ is an additive code of length n and dimension k over $\overline{\mathcal{R}}_{e,rm}$ with a generator matrix L. Further, since the map $^{-}\restriction_{\mathcal{T}_{e,rm}} : \mathcal{T}_{e,rm} \to \overline{\mathcal{R}}_{e,rm}$ is a bijection, there exists a unique $k \times n$ matrix G_0 over $\mathcal{T}_{e,rm}$ satisfying $\overline{G}_0 = L$. We next make the following observation.

Lemma 7.4.2. *Let $\mathscr{C}$ be a free additive code of length n over $\mathcal{R}_{e,rm}$ with $Tor_1(\mathscr{C}) = \mathscr{D}$. There exist $k \times n$ matrices $G_1, G_2, \ldots, G_{e-1}$ over $\mathcal{T}_{e,rm}$ such that the matrix*

$$G_0 + uG_1 + u^2G_2 + \cdots + u^{e-1}G_{e-1}$$

is a generator matrix of the code $\mathscr{C}$.

In the following theorem, we count all ACD codes $\mathscr{C}$ of length n over $\mathcal{R}_{e,rm}$ with $Tor_1(\mathscr{C}) = \mathscr{D}$.

Theorem 7.4.5. *Let $\mathscr{D}$ be an ACD code of length n and dimension k over $\overline{\mathcal{R}}_{e,rm}$. There are precisely $p^{rk(nm-k)(e-1)}$ distinct ACD codes $\mathscr{C}$ of length n and rank k over $\mathcal{R}_{e,rm}$ with $Tor_1(\mathscr{C}) = \mathscr{D}$.*

Proof. Working as in Theorem 6.3.1 and by applying Lemmas 7.4.1 and 7.4.2, the desired result follows. □

Here we recall that the residue field $\overline{\mathcal{R}}_{e,rm}$ of the chain ring $\mathcal{R}_{e,rm}$ is of order p^{rm} and the residue field $\overline{\mathcal{R}}_{e,r}$ of the chain ring $\mathcal{R}_{e,r}$ is of order p^r, where p is a prime number and r, m are positive integers. Now to count all ACD codes of length n and rank k over $\mathcal{R}_{e,rm}$, we will first count all k-dimensional $\mathbb{F}_{p^r}$-linear subspaces $\mathcal{D}$

of $\mathbb{F}_{p^{rm}}^n$ satisfying $\mathcal{D}\cap\mathcal{D}^{\perp}=\{0\}$, *i.e.,* all ACD codes of length n and dimension k over $\mathbb{F}_{p^{rm}}$ for $0\leq k\leq nm$. Let $\mathfrak{L}_{r,m}(n;k)$ denote the number of distinct ACD codes of length n and dimension k over $\mathbb{F}_{p^{rm}}$ for $0\leq k\leq nm$. One can easily see that $\mathfrak{L}_{r,m}(n;0)=\mathfrak{L}_{r,m}(n;nm)=1$. Here, we will distinguish the following two cases: (i) $p=2$ and (ii) p is an odd prime.

In the following theorem, we consider the case $p=2$ and obtain the explicit enumeration formula for the number $\mathfrak{L}_{r,m}(n;k)$ for $1\leq k\leq nm-1$.

Theorem 7.4.6. *Let $p=2$. For $1\leq k\leq nm-1$, we have*

$$\mathfrak{L}_{r,m}(n;k)=\begin{cases}(2^r)^{\frac{(nm-k)(k+1)}{2}}\begin{bmatrix}(nm-1)/2\\(k-1)/2\end{bmatrix}_{2^{2r}} & \text{if both } k \text{ and } nm \text{ are odd;}\\ (2^r)^{\frac{nmk-k^2+nm-1}{2}}\begin{bmatrix}(nm-2)/2\\(k-1)/2\end{bmatrix}_{2^{2r}} & \text{if } k \text{ is odd and } nm \text{ is even;}\\ (2^r)^{\frac{k(nm-k+1)}{2}}\begin{bmatrix}(nm-1)/2\\k/2\end{bmatrix}_{2^{2r}} & \text{if } k \text{ is even and } nm \text{ is odd;}\\ (2^r)^{\frac{nmk-k^2-2}{2}}\Big((2^{rk}+2^r-1)\begin{bmatrix}(nm-2)/2\\k/2\end{bmatrix}_{2^{2r}} & \\ +(2^{r(nm-k+1)}-2^{r(nm-k)}+1)\begin{bmatrix}(nm-2)/2\\(k-2)/2\end{bmatrix}_{2^{2r}}\Big) & \text{if both } k \text{ and } nm \text{ are even.}\end{cases}$$

Proof. Since $p=2$, we see, by Theorem 1 of [58], that there exists a self-dual basis of $\mathbb{F}_{2^{rm}}$ over $\mathbb{F}_{2^r}$. By Proposition 7.2.1, we note that there exists a one-to-one correspondence between ACD codes of length n and dimension k over $\mathbb{F}_{2^{rm}}$ and LCD codes of length nm and dimension k over $\mathbb{F}_{2^r}$. Now the desired result follows by applying Theorem 6.3.2. □

In the following theorem, we assume that p is an odd prime and obtain the explicit enumeration formula for the number $\mathfrak{L}_{r,m}(n;k)$ for $1\leq k\leq nm-1$.

Theorem 7.4.7. *Let p be an odd prime. For $1\leq k\leq nm-1$, the following hold.*

(a) Let k be odd.

- *When nm is odd, we have*

$$\mathfrak{L}_{r,m}(n;k)=(p^r)^{\frac{(nm-k)(k+1)}{2}}\begin{bmatrix}(nm-1)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}.$$

- *Suppose that either* $p^r \equiv 1 \pmod 4$ *and* n *is even or* $m \equiv 2 \pmod 4$ *and* $p^r \equiv 3 \pmod 4$ *or* m *is odd,* $p^r \equiv 3 \pmod 4$ *and* $n \equiv 0 \pmod 4$ *or* $m \equiv 0 \pmod 4$, $p^r \equiv 3 \pmod 4$ *and* n *is even. Here we have*

$$\mathfrak{L}_{r,m}(n;k) = (p^r)^{\frac{nmk-k^2-1}{2}}((p^r)^{\frac{nm}{2}} - 1)\begin{bmatrix}(nm-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}.$$

- *Suppose that either* m *is odd,* $p^r \equiv 3 \pmod 4$ *and* $n \equiv 2 \pmod 4$ *or* m *is even,* n *is odd and* $p^r \equiv 1 \pmod 4$ *or* $m \equiv 0 \pmod 4$, $p^r \equiv 3 \pmod 4$ *and* n *is odd. Here we have*

$$\mathfrak{L}_{r,m}(n;k) = (p^r)^{\frac{nmk-k^2-1}{2}}((p^r)^{\frac{nm}{2}} + 1)\begin{bmatrix}(nm-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}.$$

(b) Let k *be even.*

- *When* nm *is odd, we have*

$$\mathfrak{L}_{r,m}(n;k) = (p^r)^{\frac{k(nm-k+1)}{2}}\begin{bmatrix}(nm-1)/2\\k/2\end{bmatrix}_{p^{2r}}.$$

- *When* nm *is even, we have*

$$\mathfrak{L}_{r,m}(n;k) = (p^r)^{\frac{k(nm-k)}{2}}\begin{bmatrix}nm/2\\k/2\end{bmatrix}_{p^{2r}}.$$

Proof. To prove the result, we see, by Lemma 1 of Huffman [52], that the ordinary trace bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_{p^{rm}}^n$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{p^{rm}}^n$, *i.e.,* the formed space $\big(\mathbb{F}_{p^{rm}}^n, \langle \cdot, \cdot \rangle\big)$ is an nm-dimensional orthogonal space over $\mathbb{F}_{p^r}$. Since p is an odd prime, it is easy to observe that the orthogonal space $\big(\mathbb{F}_{p^{rm}}^n, \langle \cdot, \cdot \rangle\big)$ can also be viewed as a non-degenerate quadratic space with respect to the quadratic map $\mathfrak{Q} : \mathbb{F}_{p^{rm}}^n \to \mathbb{F}_{p^r}$, defined as $\mathfrak{Q}(a) = \frac{1}{2}\langle a, a \rangle$ for each $a \in \mathbb{F}_{p^{rm}}^n$. We next observe that each ACD code of length n and dimension k over $\mathbb{F}_{p^{rm}}$ can also be viewed as a k-dimensional non-degenerate $\mathbb{F}_{p^r}$-linear subspace of the nm-dimensional quadratic space $(\mathbb{F}_{p^{rm}}^n, \mathfrak{Q})$. In view of this, the number $\mathfrak{L}_{r,m}(n;k)$ equals the number of distinct k-dimensional non-degenerate quadratic $\mathbb{F}_{p^r}$-linear subspaces of the quadratic space $(\mathbb{F}_{p^{rm}}^n, \mathfrak{Q})$ for $1 \leq k \leq nm-1$. Further, by Theorem 7 of

Huffman [52], we note that the Witt index ν of the quadratic space $(\mathbb{F}_{p^{rm}}^n, \mathfrak{Q})$ is given by

$$\nu = \begin{cases} \frac{nm-1}{2} & \text{if } nm \text{ is odd;} \\ \frac{nm-2}{2} & \text{if either } m \text{ is odd, } p^r \equiv 3 \pmod 4 \text{ and } n \equiv 2 \pmod 4 \text{ or } m \text{ is even, } n \text{ is} \\ & \text{odd and } p^r \equiv 1 \pmod 4 \text{ or } m \equiv 0 \pmod 4, p^r \equiv 3 \pmod 4 \text{ and } n \text{ is odd;} \\ \frac{nm}{2} & \text{if either } p^r \equiv 1 \pmod 4 \text{ and } n \text{ is even or } m \text{ is odd, } p^r \equiv 3 \pmod 4 \text{ and} \\ & n \equiv 0 \pmod 4 \text{ or } m \equiv 2 \pmod 4 \text{ and } p^r \equiv 3 \pmod 4 \text{ or } m \equiv 0 \pmod 4, \\ & p^r \equiv 3 \pmod 4 \text{ and } n \text{ is even.} \end{cases} \tag{7.4.1}$$

By Lemma 5 of of Huffman [52], we observe that a k-dimensional non-degenerate quadratic $\mathbb{F}_{p^r}$-linear subspace $\mathcal{W}$ of $\mathbb{F}_{p^{rm}}^n$ has a Witt decomposition of the form

$$\mathcal{W} = \langle a_1, b_1 \rangle \perp \langle a_2, b_2 \rangle \perp \cdots \perp \langle a_{\nu_k}, b_{\nu_k} \rangle \perp \mathcal{W}_k,$$

where ν_k is the Witt index of $\mathcal{W}$, (a_i, b_i) is a hyperbolic pair in $\mathbb{F}_{p^{rm}}^n$ for $1 \leq i \leq \nu_k$, and $\mathcal{W}_k$ is an anisotropic $\mathbb{F}_{p^r}$-linear subspace of $\mathbb{F}_{p^{rm}}^n$ satisfying $\dim_{\mathbb{F}_{p^r}}(\mathcal{W}_k) = k - 2\nu_k \leq 2$. Now we shall distinguish the following two cases: (a) k is odd, and (b) k is even.

(a) First, let k be odd. Here working as in Theorem 6.3.3 and by applying Theorems 2.3.2, 2.3.5 and 2.3.6, we get

$$\mathfrak{L}_{r,m}(n;k) = \begin{cases} (p^r)^{\frac{(nm-k)(k+1)}{2}} \begin{bmatrix} (nm-1)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-1}{2}; \\ (p^r)^{\frac{nmk-k^2-1}{2}} ((p^r)^{\frac{nm}{2}} - 1) \begin{bmatrix} (nm-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm}{2}; \\ (p^r)^{\frac{nmk-k^2-1}{2}} ((p^r)^{\frac{nm}{2}} + 1) \begin{bmatrix} (nm-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-2}{2}. \end{cases}$$

(b) Next, let k be even. Here we see, by Theorem 7 of Huffman [52], that either $\nu_k = \frac{k-2}{2}$ or $\nu_k = \frac{k}{2}$, which implies that $\mathfrak{L}_{r,m}(n;k) = \mathfrak{S}_{r,m}(n;k) + \widehat{\mathfrak{S}}_{r,m}(n;k)$, where $\mathfrak{S}_{r,m}(n;k)$ and $\widehat{\mathfrak{S}}_{r,m}(n;k)$ denote the number of distinct k-dimensional non-degenerate quadratic $\mathbb{F}_{p^r}$-linear subspaces of $\mathbb{F}_{p^{rm}}^n$ having the Witt indices $\frac{k-2}{2}$ and $\frac{k}{2}$, respectively. Further, working as in Theorem 6.3.3 and by applying Theorems 2.3.2, 2.3.5 and 2.3.6, we get

$$\mathfrak{S}_{r,m}(n;k) = \begin{cases} \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}-1)}{2}\begin{bmatrix}(nm-1)/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-1}{2};\\ \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}-1)(p^{\frac{r(nm-k)}{2}}-1)}{2(p^{\frac{rnm}{2}}+1)}\begin{bmatrix}nm/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm}{2};\\ \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}-1)(p^{\frac{r(nm-k)}{2}}+1)}{2(p^{\frac{rnm}{2}}-1)}\begin{bmatrix}nm/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-2}{2} \end{cases}$$

and

$$\widehat{\mathfrak{S}}_{r,m}(n;k) = \begin{cases} \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}+1)}{2}\begin{bmatrix}(nm-1)/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-1}{2};\\ \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}+1)(p^{\frac{r(nm-k)}{2}}+1)}{2(p^{\frac{rnm}{2}}+1)}\begin{bmatrix}nm/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm}{2};\\ \dfrac{p^{\frac{rk(nm-k)}{2}}(p^{\frac{rk}{2}}+1)(p^{\frac{r(nm-k)}{2}}-1)}{2(p^{\frac{rnm}{2}}-1)}\begin{bmatrix}nm/2\\ k/2\end{bmatrix}_{p^{2r}} & \text{if } \nu = \frac{nm-2}{2}. \end{cases}$$

From this and by (7.4.1), the desired result follows when k is even.

□

Next, let $\mathcal{H}_{r,m}(n;k)$ denote the number of distinct ACD codes of length n and rank k over $\mathcal{R}_{e,rm}$ for $0 \le k \le nm$. It is easy to see that $\mathcal{H}_{r,m}(n;0) = \mathcal{H}_{r,m}(n;nm) = 1$. In the following theorem, we consider $p = 2$ and obtain the enumeration formula for the number $\mathcal{H}_{r,m}(n;k)$ for $1 \le k \le nm-1$.

Theorem 7.4.8. *Let $p = 2$. For $1 \le k \le nm-1$, the following hold.*

(a) Let k be odd.

- *When nm is odd, we have*

$$\mathcal{H}_{r,m}(n;k) = 2^{\frac{r(nm-k)(2ke-k+1)}{2}}\begin{bmatrix}(nm-1)/2\\ (k-1)/2\end{bmatrix}_{2^{2r}}.$$

- *When nm is even, we have*

$$\mathcal{H}_{r,m}(n;k) = 2^{\frac{r(k(nm-k)(2e-1)+nm-1)}{2}}\begin{bmatrix}(nm-2)/2\\ (k-1)/2\end{bmatrix}_{2^{2r}}.$$

(b) Let k be even.

- *When nm is odd, we have*

$$\mathcal{H}_{r,m}(n;k) = 2^{\frac{rk((nm-k)(2e-1)+1)}{2}} \begin{bmatrix}(nm-1)/2\\ k/2\end{bmatrix}_{2^{2r}}.$$

- *When nm is even, we have*

$$\begin{aligned}\mathcal{H}_{r,m}(n;k) &= 2^{\frac{r(k(nm-k)(2e-1)-2)}{2}} \Big((2^{rk}+2^{r}-1)\begin{bmatrix}(nm-2)/2\\ k/2\end{bmatrix}_{2^{2r}} \\ &\quad +(2^{r(nm-k+1)}-2^{r(nm-k)}+1)\begin{bmatrix}(nm-2)/2\\ (k-2)/2\end{bmatrix}_{2^{2r}}\Big).\end{aligned}$$

Proof. Working as in Theorem 6.3.4 and by applying Theorem 7.4.5, we see that $\mathcal{H}_{r,m}(n;k) = p^{rk(nm-k)(e-1)}\mathfrak{L}_{r,m}(n;k)$. Now on substituting the values of the number $\mathfrak{L}_{r,m}(n;k)$ from Theorem 7.4.6, the desired result follows. □

In the following theorem, we assume that p is an odd prime and obtain the explicit enumeration formula for the number $\mathcal{H}_{r,m}(n;k)$ for $1 \leq k \leq nm-1$.

Theorem 7.4.9. *Let p be an odd prime. For $1 \leq k \leq nm-1$, the following hold.*

(a) Let k be odd.

- *When nm is odd, we have*

$$\mathcal{H}_{r,m}(n;k) = p^{\frac{r(nm-k)(2ke-k+1)}{2}} \begin{bmatrix}(nm-1)/2\\ (k-1)/2\end{bmatrix}_{p^{2r}}.$$

- *Suppose that either $p^r \equiv 1 \pmod 4$ and n is even or $m \equiv 2 \pmod 4$ and $p^r \equiv 3 \pmod 4$ or m is odd, $p^r \equiv 3 \pmod 4$ and $n \equiv 0 \pmod 4$ or $m \equiv 0 \pmod 4$, $p^r \equiv 3 \pmod 4$ and n is even. Here we have*

$$\mathcal{H}_{r,m}(n;k) = p^{\frac{r(k(nm-k)(2e-1)-1)}{2}} (p^{\frac{rnm}{2}}-1) \begin{bmatrix}(nm-2)/2\\ (k-1)/2\end{bmatrix}_{p^{2r}}.$$

- *Suppose that either m is odd, $p^r \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$ or m is even, n is odd and $p^r \equiv 1 \pmod 4$ or $m \equiv 0 \pmod 4$, $p^r \equiv 3 \pmod 4$*

and n is odd. Here we have

$$\mathcal{H}_{r,m}(n;k) = p^{\frac{r(k(nm-k)(2e-1)-1)}{2}}(p^{\frac{rnm}{2}}+1)\begin{bmatrix}(nm-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}.$$

(b) Let k be even.

- *When nm is odd, we have*

$$\mathcal{H}_{r,m}(n;k) = p^{\frac{rk((nm-k)(2e-1)+1)}{2}}\begin{bmatrix}(nm-1)/2\\k/2\end{bmatrix}_{p^{2r}}.$$

- *When nm is even, we have*

$$\mathcal{H}_{r,m}(n;k) = p^{\frac{rk(nm-k)(2e-1)}{2}}\begin{bmatrix}nm/2\\k/2\end{bmatrix}_{p^{2r}}.$$

Proof. Working as in Theorem 6.3.4 and by applying Theorem 7.4.5, we see that $\mathcal{H}_{r,m}(n;k) = p^{rk(nm-k)(e-1)}\mathfrak{L}_{r,m}(n;k)$. Now on substituting the values of the number $\mathfrak{L}_{r,m}(n;k)$ from Theorem 7.4.7, the desired result follows. □

Further, let $\mathcal{H}_{r,m}(n)$ denote the number of distinct ACD codes of length n over $\mathcal{R}_{e,rm}$. Here, we will distinguish the following two cases: (i) $p=2$ and (ii) p is an odd prime. In the following theorem, we consider the case $p=2$ and obtain the explicit enumeration formula for the number $\mathcal{H}_{r,m}(n)$.

Theorem 7.4.10. *Let $p=2$. Then the following hold.*

- *When nm is odd, we have*

$$\begin{aligned}\mathcal{H}_{r,m}(n) &= 2+\sum_{\substack{k=1\\k\equiv 0 \pmod 2}}^{nm-1} 2^{\frac{rk((nm-k)(2e-1)+1)}{2}}\begin{bmatrix}(nm-1)/2\\k/2\end{bmatrix}_{2^{2r}}\\ &\quad+\sum_{\substack{k=1\\k\equiv 1 \pmod 2}}^{nm-1} 2^{\frac{r(nm-k)(2ke-k+1)}{2}}\begin{bmatrix}(nm-1)/2\\(k-1)/2\end{bmatrix}_{2^{2r}}.\end{aligned}$$

- *When nm is even, we have*

$$\begin{aligned}\mathcal{H}_{r,m}(n) = 2 + \sum_{\substack{k=1\\k\equiv 0 \pmod 2}}^{nm-1} 2^{\frac{r(k(nm-k)(2e-1)-2)}{2}} \Big(& (2^{r(nm-k+1)} - 2^{r(nm-k)} + 1) \begin{bmatrix} (nm-2)/2 \\ (k-2)/2 \end{bmatrix}_{2^{2r}} \\ + (2^{rk} + 2^{r} - 1) \begin{bmatrix} (nm-2)/2 \\ k/2 \end{bmatrix}_{2^{2r}} \Big) & + \sum_{\substack{k=1\\k\equiv 1 \pmod 2}}^{nm-1} 2^{\frac{r(k(nm-k)(2e-1)+nm-1)}{2}} \begin{bmatrix} (nm-2)/2 \\ (k-1)/2 \end{bmatrix}_{2^{2r}}\end{aligned}$$

Proof. It follows immediately from Theorem 7.4.8. □

In the following theorem, we assume that p is an odd prime and obtain the explicit enumeration formula for the number $\mathcal{H}_{r,m}(n)$.

Theorem 7.4.11. *Let p be an odd prime. Then the following hold.*

- *When nm is odd, we have*

$$\begin{aligned}\mathcal{H}_{r,m}(n) &= 2 + \sum_{\substack{k=1\\k\equiv 1 \pmod 2}}^{nm-1} p^{\frac{r(nm-k)(2ke-k+1)}{2}} \begin{bmatrix} (nm-1)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} \\ &\quad + \sum_{\substack{k=1\\k\equiv 0 \pmod 2}}^{nm-1} p^{\frac{rk((nm-k)(2e-1)+1)}{2}} \begin{bmatrix} (nm-1)/2 \\ k/2 \end{bmatrix}_{p^{2r}}.\end{aligned}$$

- *Suppose that either $p^r \equiv 1 \pmod 4$ and n is even or $p^r \equiv 3 \pmod 4$ and $m \equiv 2 \pmod 4$ or $p^r \equiv 3 \pmod 4$, m is odd and $n \equiv 0 \pmod 4$ or $m \equiv 0 \pmod 4$, n is even and $p^r \equiv 3 \pmod 4$. Here we have*

$$\begin{aligned}\mathcal{H}_{r,m}(n) &= 2 + \sum_{\substack{k=1\\k\equiv 1 \pmod 2}}^{nm-1} p^{\frac{r(k(nm-k)(2e-1)-1)}{2}} (p^{\frac{rnm}{2}} - 1) \begin{bmatrix} (nm-2)/2 \\ (k-1)/2 \end{bmatrix}_{p^{2r}} \\ &\quad + \sum_{\substack{k=1\\k\equiv 0 \pmod 2}}^{nm-1} p^{\frac{rk(nm-k)(2e-1)}{2}} \begin{bmatrix} nm/2 \\ k/2 \end{bmatrix}_{p^{2r}}\end{aligned}$$

- *Suppose that either m is odd, $p^r \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$ or m is even, n is odd and $p^r \equiv 1 \pmod 4$ or $m \equiv 0 \pmod 4$, $p^r \equiv 3 \pmod 4$ and n*

is odd. Here we have

$$\begin{aligned}\mathcal{H}_{r,m}(n) &= 2+\sum_{\substack{k=1\\k\equiv 1 \pmod 2}}^{nm-1} p^{\frac{r(k(nm-k)(2e-1)-1)}{2}}(p^{\frac{rnm}{2}}+1)\begin{bmatrix}(nm-2)/2\\(k-1)/2\end{bmatrix}_{p^{2r}}\\ &+\sum_{\substack{k=1\\k\equiv 0 \pmod 2}}^{nm-1} p^{\frac{rk(nm-k)(2e-1)}{2}}\begin{bmatrix}nm/2\\k/2\end{bmatrix}_{p^{2r}}.\end{aligned}$$

Proof. It follows immediately from Theorem 7.4.9. □

The following theorem states the well-known Singleton bound for additive codes over $\mathcal{R}_{e,rm}$.

Theorem 7.4.12. *[94] (Singleton bound for additive codes over $\mathcal{R}_{e,rm}$): For an additive code $\mathcal{C}$ of length n over $\mathcal{R}_{e,rm}$, we have*

$$|\mathcal{C}| \leq |\mathcal{R}_{e,rm}|^{n-d_H(\mathcal{C})+1}.$$

In particular, if $\mathcal{C}$ is a free additive code of length n and rank k over $\mathcal{R}_{e,rm}$, then we have

$$d_H(\mathcal{C}) \leq n - \left\lceil \frac{k}{m} \right\rceil + 1.$$

An additive code $\mathcal{C}$ of length n over $\mathcal{R}_{e,rm}$ is said to be maximum distance separable (MDS) if it satisfies $|\mathcal{C}| = |\mathcal{R}_{e,rm}|^{n-d_H(\mathcal{C})+1}$.

Proposition 7.4.1. *For an additive code $\mathcal{C}$ of length n over $\mathcal{R}_{e,rm}$, we have*

$$d_H(\mathcal{C}) = d_H(Tor_e(\mathcal{C})).$$

Proof. Working as in Theorem 4.2(ii) of Norton and Sălăgean [81], we get the desired result. □

Theorem 7.4.13. *A free additive code $\mathcal{C}$ over $\mathcal{R}_{e,rm}$ is MDS if and only if its Torsion code $Tor_1(\mathcal{C})$ is an additive MDS code over $\overline{\mathcal{R}}_{e,rm}$.*

Proof. It follows immediately from Proposition 7.4.1. □

In the following theorem, we provide a method to construct free additive MDS codes over $\mathcal{R}_{e,rm}$ from additive MDS codes over $\overline{\mathcal{R}}_{e,rm}$. To do this, let $\mathcal{C}_0$ be an additive MDS code of length n and dimension k over $\overline{\mathcal{R}}_{e,rm}$ with a generator matrix $\mathcal{G}_0'$. Further, since the map $^{-}\restriction_{\mathcal{T}_{e,rm}} : \mathcal{T}_{e,rm} \to \overline{\mathcal{R}}_{e,rm}$ is a bijection, there exists a unique $k \times n$ matrix $\mathcal{G}_0$ over $\mathcal{T}_{e,rm}$ satisfying $\overline{\mathcal{G}}_0 = \mathcal{G}_0'$.

Theorem 7.4.14. *Let $\mathcal{C}$ be a free additive code of length n over $\mathcal{R}_{e,rm}$ with a generator matrix $\mathcal{G}_0 + u\mathcal{G}_1 + u^2\mathcal{G}_2 + \cdots + u^{e-1}\mathcal{G}_{e-1}$, where $\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{e-1} \in \mathcal{M}_{k\times n}(\mathcal{T}_{e,rm})$. Then the code $\mathcal{C}$ is an additive MDS code over $\mathcal{R}_{e,rm}$ with $Tor_1(\mathcal{C}) = \mathcal{C}_0$.*

Proof. It follows by applying Theorem 7.4.13. □

The following theorem provides a necessary and sufficient condition for a free additive code over $\mathcal{R}_{e,rm}$ to be an ACD MDS code.

Theorem 7.4.15. *Let $\mathcal{C}$ be a free additive code of length n over $\mathcal{R}_{e,rm}$. Then the code $\mathcal{C}$ is an ACD MDS code over $\mathcal{R}_{e,rm}$ if and only its Torsion code $Tor_1(\mathcal{C})$ is an ACD MDS code over $\overline{\mathcal{R}}_{e,rm}$.*

Proof. The desired result follows by applying Lemma 7.4.1 and Theorem 7.4.13. □

Theorem 7.4.14 provides a method to construct free additive MDS codes over $\mathcal{R}_{e,rm}$ from additive MDS codes over $\overline{\mathcal{R}}_{e,rm}(\simeq \mathbb{F}_{p^{rm}})$. Theorem 7.4.15 provides a construction of ACD MDS codes over $\mathcal{R}_{e,rm}$ from ACD MDS codes over $\overline{\mathcal{R}}_{e,rm}(\simeq \mathbb{F}_{p^{rm}})$. In the next chapter, we will introduce and study two new families of additive codes over finite fields. We will further identify some new classes of additive MDS and almost MDS codes within these two families of codes. We will also provide methods to construct additive MDS self-orthogonal, self-dual, and ACD codes over finite fields.

8

Some new classes of additive MDS and almost MDS codes over finite fields

8.1 Introduction

In this chapter, we introduce and study two new classes of additive codes over finite fields, *viz.* additive generalized Reed-Solomon (additive GRS) codes and additive generalized twisted Reed-Solomon (additive GTRS) codes, which are extensions of linear generalized Reed-Solomon (GRS) codes and twisted Reed-Solomon (GTRS) codes, respectively. Unlike linear GRS codes, additive GRS codes are not maximum distance separable (MDS) codes, and the dual of an additive GRS code need not be an additive GRS code in general. We derive necessary and sufficient conditions under which an additive GRS code is MDS. We further apply this result to identify several new classes of additive MDS codes and a class of additive MDS codes whose dual codes are also MDS within the family of additive GRS codes. We also identify several new classes of additive codes that are either MDS or almost MDS within the family of additive GTRS codes. We also obtain several classes of additive TRS codes that are not monomially equivalent to additive RS codes. Besides this, we identify classes of monomially inequivalent additive MDS TRS codes and additive MDS RS codes, whose dual codes are also MDS. We also provide methods to construct additive MDS self-orthogonal, self-dual, and ACD codes through additive GRS and GTRS codes. Based on additive MDS codes whose dual codes are also MDS, we present a perfect threshold secret-sharing scheme that can detect cheating, identify a certain number of cheaters among the participants, and correctly recover the secret.

This chapter is organized as follows: In Section 8.2, we state some preliminaries needed to derive our main results. In Section 8.3, we establish a one-to-one correspondence between linear codes and additive codes over finite fields, which gives rise to a method to construct additive MDS codes over finite fields as images of linear MDS codes over finite fields (Theorem 8.3.1 and Corollary 8.3.1). We will also show that not every additive MDS code can be obtained as an image of a linear MDS code (Theorem 8.3.2). We next observe that the dual of an additive MDS code is not an MDS code in general (Example 8.3.1). We further provide an elementary proof of Theorem 9 of Ball *et al.* [7], which states that the dual code of a k-dimensional additive MDS code over $\mathbb{F}_{q^m}$ is an MDS code if k is a multiple of m, where $m \geq 2$ is an integer (Theorem 8.3.3). In Section 8.4, we introduce and study additive generalized Reed-Solomon (additive GRS) codes and extended additive generalized Reed-Solomon (extended additive GRS) codes over finite fields. We also derive a necessary and sufficient condition under which an additive GRS (*resp.* extended additive GRS) code is MDS (Theorems 8.4.1 and 8.4.2). With the help of these results, we further identify new classes of additive MDS codes within the family of additive GRS and extended additive GRS codes (Corollaries 8.4.1 and 8.4.2). We also observe that the dual code of an additive GRS code need not be an additive GRS code (Example 8.4.5). We further identify a class of additive MDS codes within the family of additive GRS codes, whose dual codes are also additive MDS GRS codes (Theorem 8.4.3). We also construct some additive MDS self-orthogonal, self-dual, and ACD codes through additive GRS codes (Theorems 8.4.4 and 8.4.5). In Section 8.5, we introduce and study additive generalized twisted Reed-Solomon (additive GTRS) codes and extended additive generalized twisted Reed-Solomon (extended additive GTRS) codes over finite fields. We identify several classes of additive GTRS and extended additive GTRS codes, which are either MDS or almost MDS (Theorems 8.5.1- 8.5.9). We also construct additive self-orthogonal codes through additive GTRS codes (Theorem 8.5.10). In Section 8.6, we identify several classes of additive TRS codes that are not monomially equivalent to additive RS codes (Theorems 8.6.1-8.6.3). We also identify monomially inequivalent classes of additive MDS TRS codes and additive MDS RS codes, whose dual codes are also MDS (see Theorem 8.6.2). In Section 8.7, we provide a perfect threshold secret-sharing scheme that can detect cheating, identify a certain number of cheaters among the participants and recover the secret correctly based on additive MDS codes whose dual codes are also MDS.

8.2 Some preliminaries

In this section, we will state some basic definitions and results needed to derive our main results. For this, we recall that a linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$ is defined as a k-dimensional subspace of $\mathbb{F}_q^n$. We will refer to a linear code of length n, dimension k and Hamming distance d over $\mathbb{F}_q$ as a linear $[n,k,d]$-code over $\mathbb{F}_q$. In the following theorem, we recall the well-known Singleton bound for linear codes.

Theorem 8.2.1. *[94] (Singleton bound for linear codes over $\mathbb{F}_q$): For a linear $[n,k,d]$-code over $\mathbb{F}_q$, we have $d \leq n-k+1$.*

A linear $[n,k,d]$-code over $\mathbb{F}_q$ is said to be maximum distance separable (MDS) if it satisfies $d = n-k+1$. An important and well-known class of linear MDS codes is that of generalized Reed-Solomon (GRS) codes. To recall these codes, let $\mathbb{F}_q[x]$ denote the ring of all polynomials in the indeterminate x with coefficients from $\mathbb{F}_q$. For a positive integer k satisfying $k \leq n$, let us define

$$\mathbb{F}_q[x]_{<k} = \{f(x) \in \mathbb{F}_q[x] : \text{either } f(x) = 0 \text{ or } \deg(f(x)) < k\},$$

which is clearly a k-dimensional subspace of $\mathbb{F}_q[x]$ over $\mathbb{F}_q$ with a basis set $\{1, x, x^2, \ldots, x^{k-1}\}$. Let $n \leq q$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct elements of $\mathbb{F}_q$. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Then the evaluation map $\mathcal{E}_{\alpha,v} : \mathbb{F}_q[x]_{<k} \to \mathbb{F}_q^n$, defined as

$$\mathcal{E}_{\alpha,v}(f(x)) = \big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) \text{ for all } f(x) \in \mathbb{F}_q[x]_{<k},$$

is an injective $\mathbb{F}_q$-linear vector space homomorphism. The code

$$\mathcal{GRS}_k(\alpha, v) = \mathcal{E}_{\alpha,v}(\mathbb{F}_q[x]_{<k})$$

is a linear code of length n and dimension k over $\mathbb{F}_q$ and is called the generalized Reed-Solomon (GRS) code over $\mathbb{F}_q$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$ and column multipliers $v_1, v_2, \ldots, v_n$. In particular, if $v = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the code $\mathcal{GRS}_k(\alpha, v)$ is called the Reed-Solomon (RS) code of length n over $\mathbb{F}_q$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$. By Theorem 5.3.1 of [53], we see that the code $\mathcal{GRS}_k(\alpha, v)$ has Hamming distance $n - k + 1$, and hence it is a linear MDS code over $\mathbb{F}_q$. Further, the extended generalized Reed-Solomon (extended GRS) code of length $n + 1$ over $\mathbb{F}_q$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$ and column multipliers $v_1, v_2, \ldots, v_n, 1$ is defined as

$$\mathcal{GRS}_k(\alpha, v, \infty) = \left\{(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n), f(\infty)) : f(x) \in \mathbb{F}_q[x]_{<k}\right\},$$

where $f(\infty)$ is defined as the coefficient of x^{k-1} in $f(x)$ for each $f(x) \in \mathbb{F}_q[x]_{<k}$. In particular, if $v = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the code $\mathcal{GRS}_k(\alpha, v, \infty)$ is called the extended Reed-Solomon (extended RS) code of length $n + 1$ over $\mathbb{F}_q$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$. By Theorem 5.3.4 of [53], we note that the extended GRS code $\mathcal{GRS}_k(\alpha, v, \infty)$ is a linear MDS code over $\mathbb{F}_q$. Please refer to [53, Sec. 5.2 and 5.3] for more details.

Linear codes over finite fields are further extended to additive codes, which have nice algebraic structures and are useful in constructing quantum stabilizer codes [15, 22]. From now on, throughout this chapter, we assume that $m \geq 2$ is an integer, and $\mathbb{F}_{q^m}$ denotes the finite field of order q^m. Let n be a positive integer, and let $\mathbb{F}_{q^m}^n$ denote the set of all n-tuples over $\mathbb{F}_{q^m}$. The set $\mathbb{F}_{q^m}^n$ can be viewed as an

(nm)-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 $\mathbb{F}_{q^m}$ is defined as an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. We will refer to an additive code $\mathcal{C}$ of length n, dimension k and Hamming distance d over $\mathbb{F}_{q^m}$ as an additive $[n,k,d]$-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$. Further, we recall, from Chapter 7, that the ordinary trace bilinear form on $\mathbb{F}_{q^m}^n$ is a mapping $\langle \cdot,\cdot \rangle : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_q$, defined as

$$\langle a,b\rangle = \sum_{i=1}^{n} Tr_{q,m}(a_i b_i)$$

for all $a=(a_1,a_2,\ldots,a_n), b=(b_1,b_2,\ldots,b_n) \in \mathbb{F}_{q^m}^n$, where $Tr_{q,m} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ denotes the trace map. It is easy to see that $\langle \cdot,\cdot \rangle$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{q^m}^n$. Further, if $\mathcal{C}$ is an additive code of length n over $\mathbb{F}_{q^m}$, then its dual code $\mathcal{C}^{\perp}$ is defined as

$$\mathcal{C}^{\perp} = \left\{ v \in \mathbb{F}_{q^m}^n \ : \ \langle v,c\rangle = 0 \text{ for all } c \in \mathcal{C} \right\}.$$

It is easy to observe that the dual code $\mathcal{C}^{\perp}$ is also an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$, and hence it is an additive code of length n over $\mathbb{F}_{q^m}$. By Theorem 2.3.2, we note that

$$\dim_{\mathbb{F}_q}(\mathcal{C}) + \dim_{\mathbb{F}_q}(\mathcal{C}^{\perp}) = nm.$$

Now, in the following theorem, we recall the well-known Singleton bound for additive codes over $\mathbb{F}_{q^m}$.

Theorem 8.2.2. *[52] (Singleton bound for additive codes over $\mathbb{F}_{q^m}$): For an additive $[n,k,d]$-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$, we have*

$$d \leq n - \left\lceil \frac{k}{m} \right\rceil + 1.$$

An additive $[n,k,d]$-code $\mathcal{C}$ over $\mathbb{F}_{q^m}$ is said to be maximum distance separable (MDS) if it satisfies $d = n - \lceil \frac{k}{m} \rceil + 1$, and the code $\mathcal{C}$ is said to be almost MDS if it satisfies $d = n - \lceil \frac{k}{m} \rceil$.

In the following section, we provide a method to construct additive MDS codes of length n over $\mathbb{F}_{q^m}$ from linear codes of length nm over $\mathbb{F}_q$.

8.3 A construction of additive MDS codes over $\mathbb{F}_{q^m}$

Throughout this section, let $\beta = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$. Let us define a map $\pi_{\beta,v} : \mathbb{F}_q^{nm} \to \mathbb{F}_{q^m}^n$ as

$$\begin{aligned}\pi_{\beta,v}\big(c_{1,1}, c_{1,2}, \ldots, c_{1,m}, c_{2,1}, c_{2,2}, \ldots, c_{2,m}, \ldots, c_{n,1}, c_{n,2}, \ldots, c_{n,m}\big)\\ = \big(v_1(c_{1,1}\beta_1 + c_{1,2}\beta_2 + \cdots + c_{1,m}\beta_m), v_2(c_{2,1}\beta_1 + c_{2,2}\beta_2 + \cdots + c_{2,m}\beta_m),\\ \ldots\ldots, v_n(c_{n,1}\beta_1 + c_{n,2}\beta_2 + \cdots + c_{n,m}\beta_m)\big)\end{aligned}$$

for all $\big(c_{1,1}, c_{1,2}, \ldots, c_{1,m}, c_{2,1}, c_{2,2}, \ldots, c_{2,m}, \ldots\ldots, c_{n,1}, c_{n,2}, \ldots, c_{n,m}\big) \in \mathbb{F}_q^{nm}$. It is easy to see that the map $\pi_{\beta,v}$ is an $\mathbb{F}_q$-linear vector space isomorphism. From this, it follows that a non-empty subset $\mathcal{C}$ of $\mathbb{F}_q^{nm}$ is a linear code of length nm and dimension k over $\mathbb{F}_q$ if and only if its image $\pi_{\beta,v}(\mathcal{C})$ is an additive code of length n and dimension k over $\mathbb{F}_{q^m}$. That is, the isomorphism $\pi_{\beta,v}$ induces a one-to-one correspondence between linear codes of length nm and dimension k over $\mathbb{F}_q$ and additive codes of length n and dimension k over $\mathbb{F}_{q^m}$. In the following theorem, we show that the isomorphism $\pi_{\beta,v}$ maps linear MDS codes of length nm and dimension k over $\mathbb{F}_q$ to additive MDS codes of length n and dimension k over $\mathbb{F}_{q^m}$.

Theorem 8.3.1. *Let $\mathcal{C}$ be a linear MDS code of length nm and dimension k over $\mathbb{F}_q$. Then the code $\pi_{\beta,v}(\mathcal{C})$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.*

Proof. Working as in Theorems 3.1 and 3.2 of Mahmoudi and Samei [71], the desired result follows. □

From the above theorem, we deduce the following:

Corollary 8.3.1. *Let q be a prime power, and let n, k and $m \geq 2$ be positive integers satisfying $1 \leq k \leq nm \leq q$. Let $\alpha = (\alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{1,m}, \alpha_{2,1}, \alpha_{2,2}, \ldots, \alpha_{2,m}, \ldots, \alpha_{n,1},$*

$\alpha_{n,2},\ldots,\alpha_{n,m}) \in \mathbb{F}_q^{nm}$, where $\alpha_{i,j}$'s are distinct elements of $\mathbb{F}_q$. Let $\beta = \{\beta_1,\beta_2,\ldots,\beta_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and let $v = (v_1,v_2,\ldots,v_n) \in (\mathbb{F}_{q^m}^*)^n$. Then for $1 \leq k \leq nm$, the code

$$\begin{aligned}\mathcal{C}_{n,k}(\alpha,v,\beta) \;=\; & \Big\{\ \Big(v_1\big(f(\alpha_{1,1})\beta_1 + f(\alpha_{1,2})\beta_2 + \cdots + f(\alpha_{1,m})\beta_m\big), v_2\big(f(\alpha_{2,1})\beta_1 \\ & + f(\alpha_{2,2})\beta_2 + \cdots + f(\alpha_{2,m})\beta_m\big), \ldots\ldots, v_n\big(f(\alpha_{n,1})\beta_1 + f(\alpha_{n,2})\beta_2 \\ & + \cdots + f(\alpha_{n,m})\beta_m\big)\Big) : f(x) \in \mathbb{F}_q[x]_{<k}\Big\}\end{aligned}$$

is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.

Proof. Here one can easily see that the code $\mathcal{C}_{n,k}(\alpha,v,\beta) = \pi_{\beta,v}\left(\mathcal{GRS}_k(\alpha,\mathbf{1})\right)$, where $\mathbf{1} = (1,1,\ldots,1)$ denotes the all-one vector of length nm. By Theorem 5.3.1 of [53], we see that the RS code $\mathcal{GRS}_k(\alpha,\mathbf{1})$ is a linear MDS code of length nm and dimension k over $\mathbb{F}_q$. Now by applying Theorem 8.3.1, the desired result follows immediately. □

In the following theorem, we construct an additive MDS code over $\mathbb{F}_{q^m}$ whose inverse image under the isomorphism $\pi_{\beta,v}$ is not an MDS (linear) code over $\mathbb{F}_q$, *i.e.*, the converse of Theorem 8.3.1 does not hold in general.

Theorem 8.3.2. *Let $n \leq q$, and let $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_n) \in \mathbb{F}_q^n$, where $\alpha_1,\alpha_2,\ldots,\alpha_n$ are distinct elements of $\mathbb{F}_q$. Let $v = (v_1,v_2,\ldots,v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\beta = \{\beta_1,\beta_2,\ldots,\beta_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Let k be an integer satisfying $1 \leq k < nm$, and let us write $k = m\gamma + \lambda$, where $\gamma = \lfloor \frac{k}{m} \rfloor$ and $0 \leq \lambda \leq m-1$. Let $\mathscr{D}_{n,k}(\alpha,v,\beta)$ be an additive code of length n over $\mathbb{F}_{q^m}$ with a generator matrix*

$$G_{\alpha,v,\beta} = \begin{bmatrix} v_1\beta_1 & v_1\beta_2 & \cdots & v_1\beta_m & v_1\alpha_1\beta_1 & v_1\alpha_1\beta_2 & \cdots & v_1\alpha_1\beta_m & \cdots & v_1\alpha_1^\gamma\beta_1 & v_1\alpha_1^\gamma\beta_2 & \cdots & v_1\alpha_1^\gamma\beta_\lambda \\ v_2\beta_1 & v_2\beta_2 & \cdots & v_2\beta_m & v_2\alpha_2\beta_1 & v_2\alpha_2\beta_2 & \cdots & v_2\alpha_2\beta_m & \cdots & v_2\alpha_2^\gamma\beta_1 & v_2\alpha_2^\gamma\beta_2 & \cdots & v_2\alpha_2^\gamma\beta_\lambda \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ v_n\beta_1 & v_n\beta_2 & \cdots & v_n\beta_m & v_n\alpha_n\beta_1 & v_n\alpha_n\beta_2 & \cdots & v_n\alpha_n\beta_m & \cdots & v_n\alpha_n^\gamma\beta_1 & v_n\alpha_n^\gamma\beta_2 & \cdots & v_n\alpha_n^\gamma\beta_\lambda \end{bmatrix}^t.$$

The additive code $\mathscr{D}_{n,k}(\alpha,v,\beta)$ is an MDS code of length n and dimension k over $\mathbb{F}_{q^m}$. Further, its inverse image $\pi_{\beta,v}^{-1}(\mathscr{D}_{n,k}(\alpha,v,\beta))$ is a linear code of length nm and dimension k over $\mathbb{F}_q$, which is not MDS when $k < n(m-1)+1$, (here $\pi_{\beta,v}^{-1}$ denotes the inverse of the vector space isomorphism $\pi_{\beta,v}$).

Proof. Since $\alpha_1,\alpha_2,\ldots,\alpha_n$ are distinct elements of $\mathbb{F}_q$ and $\beta = \{\beta_1,\beta_2,\ldots,\beta_m\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, one can easily observe that the rows of the matrix $G_{\alpha,v,\beta}$ are linearly independent over $\mathbb{F}_q$. This implies that the code $\mathscr{D}_{n,k}(\alpha,v,\beta)$ is an additive code of length n and dimension k over $\mathbb{F}_{q^m}$. We next assert that the Hamming distance of the code $\mathscr{D}_{n,k}(\alpha,v,\beta)$ is $n-\lceil\frac{k}{m}\rceil+1$. To prove this assertion, let $c=(c_1,c_2,\ldots,c_n)$ be a non-zero codeword of $\mathscr{D}_{n,k}(\alpha,v,\beta)$ with $w_H(c)=s$. This implies that precisely $n-s$ coordinates, say i_1-th, i_2-th, $\ldots$, i_{n-s}-th coordinates, of the codeword c are zero. Now since $c\in\mathscr{D}_{n,k}(\alpha,v,\beta)$, we can write $c=zG_{\alpha,v,\beta}$ for some non-zero $z=(z_{0,1},z_{0,2},\ldots,z_{0,m},z_{1,1},z_{1,2},\ldots,z_{1,m},\ldots,z_{\gamma-1,1},z_{\gamma-1,2},\ldots,z_{\gamma-1,m},z_{\gamma,1},z_{\gamma,2},\ldots,z_{\gamma,\lambda})\in\mathbb{F}_q^k$. This implies, for each $j\in\{i_1,i_2,\ldots,i_{n-s}\}$, that

$$\begin{aligned} z_{0,\ell}+z_{1,\ell}\alpha_j+z_{2,\ell}\alpha_j^2+\cdots+z_{\gamma-1,\ell}\alpha_j^{\gamma-1}+z_{\gamma,\ell}\alpha_j^{\gamma} &= 0 \quad \text{for } 1\leq\ell\leq\lambda \\ \text{and} \qquad z_{0,\ell}+z_{1,\ell}\alpha_j+z_{2,\ell}\alpha_j^2+\cdots+z_{\gamma-1,\ell}\alpha_j^{\gamma-1} &= 0 \quad \text{for } \lambda<\ell\leq m. \end{aligned}$$

That is, each of the elements $\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_{n-s}}$ is a root of the polynomials $z_{0,\ell}+z_{1,\ell}x+\cdots+z_{\gamma,\ell}x^{\gamma}$ for $1\leq\ell\leq\lambda$ and $z_{0,\ell}+z_{1,\ell}x+\cdots+z_{\gamma-1,\ell}x^{\gamma-1}$ for $\lambda+1\leq\ell\leq m$. Since z is non-zero, we see that either the polynomial $z_{0,\ell}+z_{1,\ell}x+\cdots+z_{\gamma,\ell}x^{\gamma}$ is non-zero for some integer ℓ satisfying $1\leq\ell\leq\lambda$ or the polynomial $z_{0,\ell}+z_{1,\ell}x+\cdots+z_{\gamma-1,\ell}x^{\gamma-1}$ is non-zero for some integer ℓ satisfying $\lambda+1\leq\ell\leq m$. This implies that $n-s\leq\gamma-1$ if $\lambda=0$, whereas $n-s\leq\gamma=\lfloor\frac{k}{m}\rfloor$ if $\lambda\neq 0$. From this, we obtain $s\geq n-\lceil\frac{k}{m}\rceil+1$. Thus the Hamming distance of the additive code $\mathscr{D}_{n,k}(\alpha,v,\beta)$ is at least $n-\lceil\frac{k}{m}\rceil+1$. Now by applying Theorem 8.2.2, we obtain

$$d_H(\mathscr{D}_{n,k}(\alpha,v,\beta))=n-\left\lceil\frac{k}{m}\right\rceil+1,$$

from which it follows that the additive code $\mathscr{D}_{n,k}(\alpha,v,\beta)$ is MDS.

We next observe that the code $\pi_{\beta,v}^{-1}(\mathscr{D}_{n,k}(\alpha,v,\beta))$ is a linear code of length nm and dimension k over $\mathbb{F}_q$, whose Hamming distance d satisfies $d\leq n$. We further note that the code $\pi_{\beta,v}^{-1}(\mathscr{D}_{n,k}(\alpha,v,\beta))$ is MDS if and only if $d=nm-k+1$, which holds only if $k\geq n(m-1)+1$, as $d\leq n$. In other words, when $k<n(m-1)+1$, the code $\pi_{\beta,v}^{-1}(\mathscr{D}_{n,k}(\alpha,v,\beta))$ is not MDS. □

Theorem 8.3.1 provides a method to construct additive MDS codes of length n and dimension k over $\mathbb{F}_{q^m}$ from linear MDS codes of length nm and dimension k over

$\mathbb{F}_q$, where $1 \leq k \leq nm$. Theorem 8.3.2 provides a construction of an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ whose pre-image under the isomorphism $\pi_{\beta,v}$ is not an MDS code over $\mathbb{F}_q$ when $k < n(m-1)+1$. This shows that not every additive MDS code over $\mathbb{F}_{q^m}$ can be obtained as an image of a linear MDS code over $\mathbb{F}_q$ under the isomorphism $\pi_{\beta,v}$. In Sections 8.4 and 8.5, we will provide several methods to construct additive MDS codes over $\mathbb{F}_{q^m}$.

Next, by Theorem 2.4.3 of [53], we note that the dual code of a linear MDS code over $\mathbb{F}_q$ is an MDS code. In a recent work, Ball *et al.* [7, Th. 9] showed, using geometric arguments, that when m divides k, the dual code of a k-dimensional additive MDS code over $\mathbb{F}_{q^m}$ is an additive MDS code over $\mathbb{F}_{q^m}$. We provide an elementary proof of this result in the following theorem.

Theorem 8.3.3. *Let k be a positive integer such that $1 \leq k \leq nm$ and m divides k. The dual code of each k-dimensional additive MDS code over $\mathbb{F}_{q^m}$ is an additive MDS code.*

Proof. Let $\mathcal{C}$ be an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ with a parity check matrix H. Since the code $\mathcal{C}$ is MDS, it has Hamming distance $n-\frac{k}{m}+1$. This implies that any $n-\frac{k}{m}$ columns of H are linearly independent over $\mathbb{F}_{q^m}$. By Theorem 2.3.2, we see that the dual code $\mathcal{C}^{\perp}$ has dimension $nm-k$. Now to show that the dual code $\mathcal{C}^{\perp}$ is MDS, it is enough to show that $d_H(\mathcal{C}^{\perp}) = \frac{k}{m}+1$. To prove this, we first assert that $d_H(\mathcal{C}^{\perp}) \geq \frac{k}{m}+1$.

Suppose, on the contrary, that $d_H(\mathcal{C}^{\perp}) \leq \frac{k}{m}$. Then there exists a non-zero codeword $z \in \mathcal{C}^{\perp}$ with $w_H(z) \leq \frac{k}{m}$. This implies that at least $n-\frac{k}{m}$ coordinates, say i_1-th, i_2-th, $\ldots$, $i_{n-\frac{k}{m}}$-th coordinates, of the codeword z are zero. Further, since $z \in \mathcal{C}^{\perp}$, we can write $z = vH$ for some $v \in (\mathbb{F}_q)^{nm-k}$. This implies that $vH' = 0$, where H' is the $(nm-k) \times (n-\frac{k}{m})$ matrix over $\mathbb{F}_{q^m}$ whose j-th column is the i_j-th column of the matrix H for $1 \leq j \leq n-\frac{k}{m}$. Since any $n-\frac{k}{m}$ columns of the matrix H are linearly independent over $\mathbb{F}_{q^m}$, all the columns of the matrix H' are linearly independent over $\mathbb{F}_{q^m}$. This implies that $v=0$, and hence $z=0$, which is a contradiction. This shows that every non-zero codeword of $\mathcal{C}^{\perp}$ has Hamming weight at least $\frac{k}{m}+1$, which proves the assertion.

Now by applying Theorem 8.2.2, we get $d_H(\mathcal{C}^{\perp}) = \frac{k}{m}+1$. This shows that the dual code $\mathcal{C}^{\perp}$ is MDS. □

However, when m does not divide k, the dual code of a k-dimensional additive MDS code over $\mathbb{F}_{q^m}$ need not be an MDS code. The following example illustrates this.

Example 8.3.1. *Let $q = 4$, $m = 2$, $n = 4$ and $k = 3$. Let ξ be a root of the irreducible polynomial $x^2 + x + \zeta \in \mathbb{F}_4[x]$, where ζ is a primitive element of $\mathbb{F}_4$. Let $\mathscr{C}$ be the additive code of length 4 over $\mathbb{F}_{16}$ with a generator matrix*

$$\begin{bmatrix} 1 & \xi & 1 & \xi \\ \xi & \xi^6 & \xi^{14} & 0 \\ 0 & \xi^{12} & \xi^9 & \xi^6 \end{bmatrix}.$$

It is easy to see that the code $\mathscr{C}$ is an additive $[4, 3, 3]$-code over $\mathbb{F}_{16}$, so it is an MDS code. We further observe that the dual code $\mathscr{C}^\perp$ is an additive $[4, 5, 1]$-code over $\mathbb{F}_{16}$ with a generator matrix

$$\begin{bmatrix} 1 & 0 & \xi^9 & \xi^6 \\ \xi & 0 & \xi^3 & \xi^6 \\ 0 & 1 & \xi^{10} & \xi \\ 0 & \xi & \xi^{14} & \xi^6 \\ 0 & 0 & 0 & \xi^4 \end{bmatrix}.$$

Since $d_H(\mathscr{C}^\perp) = 1 < 2 = 4 - \lceil \frac{5}{2} \rceil + 1$, the dual code $\mathscr{C}^\perp$ is not MDS. From this, it follows that when m does not divide k, the dual code of a k-dimensional additive MDS code over $\mathbb{F}_{q^m}$ need not be an MDS code.

In the next section, we will construct a class of k-dimensional additive MDS codes over $\mathbb{F}_{q^m}$ whose dual codes are also additive MDS codes, where k is not necessarily a multiple of m (see Theorem 8.4.3). Later, in Section 8.7, we will present a perfect threshold secret-sharing scheme based on additive MDS codes over finite fields, whose dual codes are also additive MDS codes.

8.4 Additive generalized Reed-Solomon (GRS) codes over finite fields

In this section, we will introduce and study a new class of additive codes over finite fields, *viz.* additive generalized Reed-Solomon (additive GRS) codes, which is an extension of linear GRS codes. We will also study extended additive generalized Reed-Solomon (extended additive GRS) codes in analogy with extended linear GRS codes [53, 86].

To define additive GRS codes, let n, k and $m \geq 2$ be integers satisfying $1 \leq k \leq nm$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n \setminus \mathbb{F}_q^n$ and $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct and $\mathbb{F}_{q^m}^* = \mathbb{F}_{q^m} \setminus \{0\}$. Here one can easily see that the evaluation map $\mathscr{E}_{\alpha,v} : \mathbb{F}_q[x]_{<k} \to \mathbb{F}_{q^m}^n$, defined as

$$\mathscr{E}_{\alpha,v}\big(f(x)\big) = \big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) \text{ for all } f(x) \in \mathbb{F}_q[x]_{<k},$$

is an $\mathbb{F}_q$-linear vector space homomorphism, and hence its image $\mathscr{E}_{\alpha,v}(\mathbb{F}_q[x]_{<k})$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. The additive generalized Reed-Solomon (additive GRS) code of length n over $\mathbb{F}_{q^m}$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$ and column multipliers $v_1, v_2, \ldots, v_n$ is defined as

$$\mathcal{ARS}_{n,k}(\alpha, v) = \mathscr{E}_{\alpha,v}(\mathbb{F}_q[x]_{<k}) = \left\{\big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) : f(x) \in \mathbb{F}_q[x]_{<k}\right\}.$$

In particular, if $v = \mathbf{1} = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is called the additive Reed-Solomon (additive RS) code with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$. Note that the evaluation map $\mathscr{E}_{\alpha,v}$ is not always injective. When the map $\mathscr{E}_{\alpha,v}$ is injective, one can easily see that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ has dimension k and has a generator matrix

$$G = \begin{bmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{bmatrix}. \tag{8.4.1}$$

Further, the extended additive generalized Reed-Solomon (extended additive GRS) code of length $n+1$ over $\mathbb{F}_{q^m}$ with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$ and column multipliers $v_1, v_2, \ldots, v_n, 1$ is defined as

$$\mathcal{ARS}_{n,k}(\alpha, v, \infty) = \left\{ \big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n), f(\infty)\big) : f(x) \in \mathbb{F}_q[x]_{<k} \right\},$$

where $f(\infty)$ is defined as the coefficient of x^{k-1} in $f(x)$ for each $f(x) \in \mathbb{F}_q[x]_{<k}$. In particular, if $v = \mathbf{1} = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is called the extended additive Reed-Solomon (extended additive RS) code with evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$. When the map $\mathscr{E}_{\alpha,v}$ is injective, one can easily see that the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ has dimension k and has a generator matrix

$$G_\infty = \begin{bmatrix} v_1 & v_2 & \cdots & v_n & 0 \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ v_1\alpha_1^{k-2} & v_2\alpha_2^{k-2} & \cdots & v_n\alpha_n^{k-2} & 0 \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} & 1 \end{bmatrix}. \tag{8.4.2}$$

By Theorems 5.3.1 and 5.3.4 of [53], we see that linear GRS and extended linear GRS codes over finite fields are MDS codes. However, additive GRS and extended additive GRS codes need not be MDS codes in general. The following two examples illustrate this.

Example 8.4.1. *Let $q = 5$, $m = 2$, $n = 6$ and $k = 3$, and let ξ be a primitive element of $\mathbb{F}_{25}$. Let us take $\alpha = (\xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6) \in \mathbb{F}_{25}^6$ and $v = (1, 1, 1, 1, 3, 2)$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive $[6, 3, 4]$-code over $\mathbb{F}_{25}$. As $d_H(\mathcal{ARS}_{n,k}(\alpha, v)) = 4 < 5 = 6 - \lceil \frac{3}{2} \rceil + 1 = n - \lceil \frac{k}{m} \rceil + 1$, the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is not MDS.*

Example 8.4.2. *Let $q = 3$, $m = 2$, $n = 3$ and $k = 2$, and let ξ be a primitive element of $\mathbb{F}_9$. Let us take $\alpha = (\xi, \xi^3, \xi^2) \in \mathbb{F}_9^3$ and $v = (1, 1, 2)$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive $[4, 2, 3]$-code over $\mathbb{F}_9$. As $d_H(\mathcal{ARS}_{n,k}(\alpha, v, \infty)) = 3 < 4 = 4 - \lceil \frac{2}{2} \rceil + 1 = (n+1) - \lceil \frac{k}{m} \rceil + 1$, the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is not MDS.*

In the following theorem, we derive necessary and sufficient conditions under which the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$, where $1 \leq k \leq nm$.

Theorem 8.4.1. *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n \setminus \mathbb{F}_q^n$ and $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct. For $1 \leq i \leq n$, let $m_i(x)$ denote the minimal polynomial of α_i over $\mathbb{F}_q$, and let $d_i = \deg(m_i(x))$. For $1 \leq k \leq \sum\limits_{i=1}^{n} d_i$, the following hold.*

(a) When $k \leq m$, the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ if and only if $d_i \geq k$ for $1 \leq i \leq n$.

(b) When $k > m$, the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ if and only if the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$ are distinct and $\sum\limits_{i \in I} d_i \geq k$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil$.

Proof. (a) Let $k \leq m$. To prove the result, we first assume that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$, which implies that the map $\mathscr{E}_{\alpha,v}$ is injective and that the Hamming distance of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is equal to $n - \lceil \frac{k}{m} \rceil + 1 = n - 1 + 1 = n$.

Here we assert that $d_i \geq k$ for $1 \leq i \leq n$. To prove this assertion, we suppose, on the contrary, that there exists an integer ℓ satisfying $1 \leq \ell \leq n$ and $d_\ell < k$, which implies that $m_\ell(x) \in \mathbb{F}_q[x]_{<k}$. As the map $\mathscr{E}_{\alpha,v}$ is injective, we see that $c = \mathscr{E}_{\alpha,v}(m_\ell(x)) = \big(v_1 m_\ell(\alpha_1), v_2 m_\ell(\alpha_2), \ldots, v_n m_\ell(\alpha_n)\big)$ is a non-zero codeword of $\mathcal{ARS}_{n,k}(\alpha, v)$. Since $m_\ell(\alpha_\ell) = 0$, we have $w_H(c) < n$. This implies that the Hamming distance of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is less than n, which is a contradiction. This shows that $d_i \geq k$ for $1 \leq i \leq n$.

Conversely, suppose that $d_i \geq k$ for $1 \leq i \leq n$. Here one can easily observe that the evaluation map $\mathscr{E}_{\alpha,v}$ is injective, which implies that the additive GRS code $\mathcal{ARS}_{n,k}(\alpha, v)$ has dimension k. We will now show that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is MDS. For this, it is enough to show that the Hamming distance of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is n. To prove this, we suppose, on the contrary, that the Hamming distance of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is less than n. This implies that there exists a non-zero polynomial $f(x) \in \mathbb{F}_q[x]_{<k}$ such that the corresponding codeword $c_f = \mathscr{E}_{\alpha,v}(f(x)) = \big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) \in \mathcal{ARS}_{n,k}(\alpha, v)$ has

Hamming weight $w_H(c_f) < n$. This implies that $f(\alpha_i) = 0$ for some integer i satisfying $1 \leq i \leq n$. This implies that $k > \deg(f(x)) \geq \deg(m_i(x)) = d_i$ for some i, which is a contradiction. From this, it follows that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is MDS.

(b) Let $k > m$. To prove the result, we first assume that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$, *i.e.*, the Hamming distance of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is $n - \lceil \frac{k}{m} \rceil + 1$.

Here we first assert that the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$ are distinct. To prove this assertion, we suppose, on the contrary, that $m_i(x) = m_j(x)$ for some integer i and j satisfying $1 \leq i < j \leq n$. Now let us define the polynomial

$$g(x) = m_i(x) \prod_{\ell \in \mathcal{L}} m_\ell(x),$$

where $\mathcal{L} \subseteq \{1, 2, \ldots, n\} \backslash \{i, j\}$ is such that $|\mathcal{L}| = \lfloor \frac{k}{m} \rfloor - 2$ if $\frac{k}{m}$ is an integer, while $|\mathcal{L}| = \lfloor \frac{k}{m} \rfloor - 1$ if $\frac{k}{m}$ is not an integer. We note that $g(x)$ is a non-zero polynomial in $\mathbb{F}_q[x]_{<k}$. This implies that $c_g = \mathscr{E}_{\alpha,v}(g(x)) = \big(v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n)\big)$ is a non-zero codeword of $\mathcal{ARS}_{n,k}(\alpha, v)$ with Hamming weight $w_H(c_g) \leq n - \lceil \frac{k}{m} \rceil$, which is a contradiction. This shows that the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$ are distinct.

We next assert that $\sum\limits_{i \in I} d_i \geq k$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil$. To prove this assertion, we suppose, on the contrary, that there exists a subset J of $\{1, 2, \ldots, n\}$ such that $|J| = \lceil \frac{k}{m} \rceil$ and $\sum\limits_{i \in J} d_i < k$. Here it is easy to see that the polynomial $h(x) = \prod\limits_{i \in J} m_i(x) \in \mathbb{F}_q[x]_{<k}$ and that $c_h = \mathscr{E}_{\alpha,v}(h(x))$ is a non-zero codeword of the code $\mathcal{ARS}_{n,k}(\alpha, v)$ with Hamming weight $w_H(c_h) \leq n - \lceil \frac{k}{m} \rceil$, which is a contradiction. This shows that $\sum\limits_{i \in I} d_i \geq k$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil$.

To prove the converse part, let us assume that the polynomials $m_1(x), m_2(x), \ldots,$ $m_n(x)$ are distinct and that $\sum\limits_{i \in I} d_i \geq k$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil$. As $k \leq \sum\limits_{i=1}^{n} d_i$, we see that the evaluation map $\mathscr{E}_{\alpha,v}$ is injective, which implies that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive code of length n and dimension k over $\mathbb{F}_{q^m}$. Further, it is easy to observe that the code $\mathcal{ARS}_{n,k}(\alpha, v)$ has Hamming distance $n - \lceil \frac{k}{m} \rceil + 1$, and hence it is an MDS code.

This completes the proof of the theorem. □

As a consequence of the above theorem, we identify a class of additive MDS codes within the family of additive GRS codes in the following corollary.

Corollary 8.4.1. *Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then for $1 \leq k \leq nm$, the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.*

Proof. It follows immediately from Theorem 8.4.1. □

The following example illustrates the above corollary.

Example 8.4.3. *Let $q = 5$, $m = 3$, $n = 40$ and $k = 5$, and let ξ be a primitive element of $\mathbb{F}_{125}$. Let $\alpha = (\xi^{39}, \xi^{44}, \xi^{34}, \xi^{47}, \xi^{21}, \xi^{6}, \xi^{42}, \xi^{16}, \xi^{18}, \xi^{94}, \xi^{2}, \xi^{11}, \xi^{14}, \xi^{48}, \xi^{68}, \xi^{7}, \xi^{99}, \xi^{36}, \xi^{13}, \xi^{73}, \xi, \xi^{37}, \xi^{4}, \xi^{41}, \xi^{38}, \xi^{19}, \xi^{17}, \xi^{3}, \xi^{8}, \xi^{69}, \xi^{43}, \xi^{49}, \xi^{74}, \xi^{63}, \xi^{12}, \xi^{22}, \xi^{9}, \xi^{64}, \xi^{24}, \xi^{23}) \in \mathbb{F}_{125}^{40}$, and let $v = \mathbf{1} = (1, 1, \ldots, 1)$ be the all-one vector of length 40. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ is an additive $[40, 5, 39]$-code over $\mathbb{F}_{125}$, and hence it is an MDS code. It agrees with Corollary 8.4.1.*

In the following theorem, we derive necessary and sufficient conditions under which the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive MDS code of length $n + 1$ and dimension k over $\mathbb{F}_{q^m}$.

Theorem 8.4.2. *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n \setminus \mathbb{F}_q^n$ and $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct. For $1 \leq i \leq n$, let $m_i(x)$ denote the minimal polynomial of α_i over $\mathbb{F}_q$, and let $d_i = \deg(m_i(x))$. For $1 < k \leq \sum\limits_{i=1}^{n} d_i + 1$, the following hold.*

(a) When $k \leq m$, the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is not an additive MDS code over $\mathbb{F}_{q^m}$.

(b) When $k > m$, the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive MDS code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ if and only if the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$ are distinct, $k \equiv 1 \pmod{m}$ and $\sum\limits_{i \in I} d_i = k-1$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil - 1$.

Proof. Proof of part (a) is trivial. To prove part (b), we first note that if $\sum\limits_{i \in I} d_i \geq k-1$ holds for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil - 1$, then $\sum\limits_{j \in J} d_j \geq k$ for all subsets J of $\{1, 2, \ldots, n\}$ with $|J| = \lceil \frac{k}{m} \rceil$. Now working in a similar manner as in Theorem 8.4.1(b), we observe that the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive MDS code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ if and only if the polynomials $m_1(x), m_2(x), \ldots, m_n(x)$ are distinct and $\sum\limits_{i \in I} d_i \geq k-1$ for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \lceil \frac{k}{m} \rceil - 1$. We further observe, for all subsets J of $\{1, 2, \ldots, n\}$ with $|J| = \lceil \frac{k}{m} \rceil - 1$, that $\sum\limits_{i \in J} d_i \leq k-2$ when $k \not\equiv 1 \pmod{m}$, while $\sum\limits_{i \in J} d_i \leq k-1$ when $k \equiv 1 \pmod{m}$. From this, the desired result follows. □

As a consequence of the above theorem, we identify a new class of additive MDS codes within the family of extended additive GRS codes in the following corollary.

Corollary 8.4.2. *Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then for $1 \leq k \leq nm+1$ and $k \equiv 1 \pmod{m}$, the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive MDS code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$.*

Proof. It follows immediately from Theorem 8.4.2. □

In the following example, we construct an extended additive MDS GRS code to illustrate the above corollary.

Example 8.4.4. *Let $q = 5$, $m = 2$, $n = 7$ and $k = 7$, and let ξ be a primitive element of $\mathbb{F}_{25}$. Let $\alpha = (\xi^7, \xi^9, \xi^{13}, \xi^4, \xi, \xi^2, \xi^{14})$, and let $v = (3, 2, 1, 1, 1, 1, 1)$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, v, \infty)$ is an additive $[8, 7, 5]$-code over $\mathbb{F}_{25}$, and hence it is an MDS code. It agrees with Corollary 8.4.2.*

By Theorem 5.3.3 of [53], we see that the dual code of a linear GRS code is also a GRS code. However, the dual code of an additive GRS code need not be an additive GRS code. The following example illustrates this.

Example 8.4.5. *Let $q = 2$, $m = 4$, $n = 3$ and $k = 10$, and let ζ be a primitive element of $\mathbb{F}_{16}$. Let us take $\alpha = (\zeta, \zeta^3, \zeta^5) \in \mathbb{F}_{16}^3$ and $v = \mathbf{1} = (1, 1, 1)$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ is an additive $[3, 10, 1]$-code over $\mathbb{F}_{16}$ and its dual code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp}$ is an additive $[3, 2, 1]$-code over $\mathbb{F}_{16}$ with a generator matrix*

$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & \zeta^5 \end{bmatrix}.$$

It is easy to see that $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp} \neq \mathcal{ARS}_{n,nm-k}(\beta, z)$ for any choice of the vectors $\beta = (\beta_1, \beta_2, \beta_3) \in \mathbb{F}_{16}^3$ and $z = (z_1, z_2, z_3) \in (\mathbb{F}_{16}^*)^3$. This shows that the dual code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp}$ is not an additive GRS code.

Further, by Corollary 8.4.1, we see that if $\alpha_1, \alpha_2, \ldots, \alpha_n$ do not form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$, then for any $v \in (\mathbb{F}_{q^m}^*)^n$, the code $\mathcal{ARS}_{n,k}(\alpha, v)$ is MDS. In the following theorem, we make use of this observation to identify a class of additive MDS GRS codes over $\mathbb{F}_{q^m}$, whose dual codes are also additive MDS GRS codes.

Theorem 8.4.3. *Let n, k and $m \geq 2$ be integers satisfying $1 \leq k \leq nm - 1$. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then there exists a vector $w = (w_1, w_2, \ldots, w_n) \in (\mathbb{F}_{q^m}^*)^n$ such that $\mathcal{ARS}_{n,k}(\alpha, v)^{\perp} = \mathcal{ARS}_{n,nm-k}(\alpha, w)$. As a consequence, the dual code of the MDS code $\mathcal{ARS}_{n,k}(\alpha, v)$ is an additive MDS GRS code.*

Proof. To prove the result, let us consider the matrix

$$\mathcal{A} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{nm-2} & \alpha_2^{nm-2} & \cdots & \alpha_n^{nm-2} \end{bmatrix}. \tag{8.4.3}$$

Let a_i denote the i-th row of the matrix $\mathcal{A}$ for $1 \leq i \leq nm-1$. One can easily see that the rows $a_1, a_2, \ldots, a_{nm-1}$ of the matrix $\mathcal{A}$ are linearly independent over $\mathbb{F}_q$. Now let $\mathscr{C}$ be the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$ generated by $a_1, a_2, \ldots, a_{nm-1} \in \mathbb{F}_{q^m}^n$. Clearly, $\mathscr{C}$ is an additive code of length n and dimension $nm-1$ over $\mathbb{F}_q$. Further, since $\langle \cdot, \cdot \rangle : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{F}_q$ is a non-degenerate and symmetric bilinear form on $\mathbb{F}_{q^m}^n$, we see, by Theorem 2.3.2, that $\dim_{\mathbb{F}_q}(\mathscr{C}^{\perp}) = nm - \dim_{\mathbb{F}_q}(\mathscr{C}) = 1$. So there exists a non-zero vector $z = (z_1, z_2, \ldots, z_n) \in \mathscr{C}^{\perp}$. That is, we have $\langle z, a_i \rangle = 0$ for $1 \leq i \leq nm-1$, or equivalently,

$$Tr_{q,m}(\mathcal{A}z^t) = 0. \tag{8.4.4}$$

We next assert that $z_1, z_2, \ldots, z_n$ all are non-zero. To prove this assertion, we suppose, on the contrary, that $z_i = 0$ for some i. Here without any loss of generality, we can assume that $i = n$, *i.e.*, $z_n = 0$. In this case, we see that the matrix equation (8.4.4) reduces to the following matrix equation:

$$Tr_{q,m}\left(\widehat{\mathcal{A}}\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_{n-1}\end{bmatrix}\right) = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \text{ where } \widehat{\mathcal{A}} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{nm-2} & \alpha_2^{nm-2} & \cdots & \alpha_{n-1}^{nm-2} \end{bmatrix}.$$

This implies that $(z_1, z_2, \ldots, z_{n-1}) \in \widehat{\mathscr{C}}^{\perp}$, where $\widehat{\mathscr{C}}$ is the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^{n-1}$ generated by the rows of the matrix $\widehat{\mathcal{A}}$. It is easy to see that $\dim_{\mathbb{F}_q}(\widehat{\mathscr{C}}) = (n-1)m$, which implies that $\widehat{\mathscr{C}} = \mathbb{F}_{q^m}^{n-1}$, and hence $\widehat{\mathscr{C}}^{\perp} = \{0\}$. From this, it follows that $z_1 = z_2 = \cdots = z_n = 0$, which is a contradiction. This shows that $z_1, z_2, \ldots, z_n \in \mathbb{F}_{q^m}^*$.

Next, we see that the additive code $\mathcal{ARS}_{n,k}(\alpha, v)$ has a generator matrix G as defined by (8.4.1). Further, let us define $w = (w_1, w_2, \ldots, w_n) = (v_1^{-1}z_1, v_2^{-1}z_2, \ldots, v_n^{-1}z_n)$. We see that the additive GRS code $\mathcal{ARS}_{n,nm-k}(\alpha, w)$ has a generator matrix

$$H = \begin{bmatrix} w_1 & w_2 & \cdots & w_n \\ w_1\alpha_1 & w_2\alpha_2 & \cdots & w_n\alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ w_1\alpha_1^{nm-k-1} & w_2\alpha_2^{nm-k-1} & \cdots & w_n\alpha_n^{nm-k-1} \end{bmatrix}.$$

It is easy to see that $Tr_{q,m}(GH^t) = 0$, which implies that $\mathcal{ARS}_{n,nm-k}(\alpha, w) \subseteq \mathcal{ARS}_{n,k}(\alpha, v)^{\perp}$. Further, it is easy to see that

$$\dim_{\mathbb{F}_q}(\mathcal{ARS}_{n,nm-k}(\alpha, w)) = \dim_{\mathbb{F}_q}(\mathcal{ARS}_{n,k}(\alpha, v)^{\perp}) = nm - k,$$

which implies that $\mathcal{ARS}_{n,nm-k}(\alpha, w) = \mathcal{ARS}_{n,k}(\alpha, v)^{\perp}$. By Corollary 8.4.1, we see that the code $\mathcal{ARS}_{n,nm-k}(\alpha, w)$ is MDS. This completes the proof of the theorem. □

The following example illustrates the above theorem.

Example 8.4.6. *Let $q = 7$, $m = 2$, $n = 6$ and $k = 5$, and let ξ be a primitive element of $\mathbb{F}_{49}$. Let us take $\alpha = (\xi, \xi^5, \xi^{11}, \xi^{13}, \xi^{17}, \xi^{19}) \in \mathbb{F}_{49}^6$, and let $v = \mathbf{1} = (1, 1, \dots, 1)$ be the all-one vector of length 6. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ is an additive $[6, 5, 4]$-code over $\mathbb{F}_{49}$ and its dual code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp}$ is an additive $[6, 7, 3]$-code over $\mathbb{F}_{49}$, and that $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp} = \mathcal{ARS}_{n,nm-k}(\alpha, w)$, where $w = (\xi^{22}, \xi^{36}, \xi^{21}, \xi^{35}, 4, \xi^{38})$. From this, it follows that both the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ and its dual code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^{\perp} = \mathcal{ARS}_{n,nm-k}(\alpha, w)$ are MDS, which agree with Theorem 8.4.3.*

By closely looking at the proof of Theorem 8.4.3, we observe the following:

Corollary 8.4.3. *Let $\mathcal{A}$ be the matrix as defined by (8.4.3). Then there exists $z \in (\mathbb{F}_{q^m}^*)^n$ satisfying $Tr_{q,m}(\mathcal{A}z^t) = 0$.*

Jin and Xing [56] constructed some classes of linear MDS self-dual codes through linear GRS codes. We extend this result and identify some classes of additive MDS self-orthogonal and self-dual codes within the family of additive GRS codes in the following theorem.

Theorem 8.4.4. *Let n, k and $m \geq 2$ be integers satisfying $1 \leq k \leq \frac{nm}{2}$. Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \dots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $z = (z_1, z_2, \dots, z_n) \in (\mathbb{F}_{q^m}^*)^n$ be such that $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3), (such a vector z exists in $(\mathbb{F}_{q^m}^*)^n$ by Corollary 8.4.3). Let us suppose that $z_i = w_i^2$, where $w_i \in \mathbb{F}_{q^m}^*$ for $1 \leq i \leq n$. Let us define $w = (w_1, w_2, \dots, w_n)$.*

Then for $1 \leq k \leq \frac{nm}{2}$, the code $\mathcal{ARS}_{n,k}(\alpha, w)$ is an additive MDS self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$. In particular, if nm is even and $k = \frac{nm}{2}$, then the code $\mathcal{ARS}_{n,k}(\alpha, w)$ is an additive MDS self-dual code over $\mathbb{F}_{q^m}$.

Proof. The desired result follows by applying Theorem 7.3.1 and Corollary 8.4.1. □

As a consequence of the above theorem, we deduce the following:

Corollary 8.4.4. *Let q be an even prime power, and let n, k and $m \geq 2$ be positive integers satisfying $n \leq \frac{\phi(q^m-1)}{m}$ and $k \leq \frac{nm}{2}$ (here ϕ is the Euler phi function). Then there exists an additive MDS self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$. In particular, when nm is even, there exists an additive MDS self-dual code of length n over $\mathbb{F}_{q^m}$.*

Proof. To prove the result, we see that as $n \leq \frac{\phi(q^m-1)}{m}$, there exist primitive elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $\mathbb{F}_{q^m}$ such that no two elements among α_i's form a conjugate pair. Let us take $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$. Note that each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Now by Corollary 8.4.3, we see that there exists a vector $z = (z_1, z_2, \ldots, z_n) \in (\mathbb{F}_{q^m}^*)^n$ satisfying $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3). Since q is even, we can write $z_i = w_i^2$, where $w_i \in \mathbb{F}_{q^m}^*$ for $1 \leq i \leq n$. Now the desired result follows immediately by applying Theorem 8.4.4. □

In the following examples, we construct additive MDS self-orthogonal and self-dual codes to illustrate Theorem 8.4.4.

Example 8.4.7. *Let $q = 3$, $m = 2$ and $n = 3$, and let ξ be a primitive element of $\mathbb{F}_9$. Let $\alpha = (\xi, \xi^2, \xi^5) \in \mathbb{F}_9^3$, i.e., $\alpha_1 = \xi$, $\alpha_2 = \xi^2$ and $\alpha_3 = \xi^5$. By carrying out computations in the Magma Computational Algebra System, we see that $z = (\xi^2, \xi^2, \xi^6) \in \mathbb{F}_9^3$ satisfies $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3). So let us take $w = (\xi, \xi, \xi^3)$. Further, by carrying out computations in the Magma Computational Algebra System, we see that the code $\mathcal{ARS}_{n,3}(\alpha, w)$ is an additive self-dual $[3, 3, 2]$-code over $\mathbb{F}_9$, while the code $\mathcal{ARS}_{n,2}(\alpha, w)$ is an additive self-orthogonal $[3, 2, 3]$-code over $\mathbb{F}_9$. It is easy to see that both the codes $\mathcal{ARS}_{n,3}(\alpha, w)$ and $\mathcal{ARS}_{n,2}(\alpha, w)$ are MDS. It agrees with Theorem 8.4.4.*

Example 8.4.8. *Let $q = 2$, $m = 5$ and $n = 5$, and let ξ be a primitive element of $\mathbb{F}_{32}$. Let us take $\alpha = (\xi^5, \xi, \xi^{11}, \xi^3, \xi^{23}) \in \mathbb{F}_{32}^5$, i.e., $\alpha_1 = \xi^5$, $\alpha_2 = \xi$, $\alpha_3 = \xi^{11}$,*

$\alpha_4 = \xi^3$ and $\alpha_5 = \xi^{23}$. By carrying out computations in the Magma Computational Algebra System, we see that $z = (\xi^{24}, \xi^{25}, \xi^{28}, \xi^{20}, \xi^8) \in \mathbb{F}_{32}^5$ satisfies $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3). So let us take $w = (\xi^{12}, \xi^{28}, \xi^{14}, \xi^{10}, \xi^4)$. Further, by carrying out computations in the Magma Computational Algebra System, we see, for $1 \leq k \leq 12$, that the code $\mathcal{ARS}_{n,k}(\alpha, w)$ is an additive MDS self-orthogonal code over $\mathbb{F}_{32}$, which agrees with Theorem 8.4.4.

In the following theorem, we construct MDS ACD codes over $\mathbb{F}_{q^m}$ through additive GRS codes.

Theorem 8.4.5. *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $z = (z_1, z_2, \ldots, z_n) \in (\mathbb{F}_{q^m}^*)^n$ be such that $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3), (such a vector z exists in $(\mathbb{F}_{q^m}^*)^n$ by Corollary 8.4.3). Next let $a(x)$ and $b(x)$ be two coprime polynomials in $\mathbb{F}_q[x]$ satisfying $\deg(a(x)) = k$, $\deg(b(x)) = nm - k$, and $a(\alpha_i)b(\alpha_i)z_i = w_i^2$, where $w_i \in \mathbb{F}_{q^m}^*$ for $1 \leq i \leq n$. Then for $w^{(a)} = \left(\frac{w_1}{a(\alpha_1)}, \frac{w_2}{a(\alpha_2)}, \ldots, \frac{w_n}{a(\alpha_n)}\right)$ and $w^{(b)} = \left(\frac{w_1}{b(\alpha_1)}, \frac{w_2}{b(\alpha_2)}, \ldots, \frac{w_n}{b(\alpha_n)}\right)$ in $(\mathbb{F}_{q^m}^*)^n$, the following hold.*

(a) $\mathcal{ARS}_{n,k}(\alpha, w^{(a)})^{\perp} = \mathcal{ARS}_{n,nm-k}(\alpha, w^{(b)})$.

(b) $\mathcal{ARS}_{n,k}(\alpha, w^{(a)}) \cap \mathcal{ARS}_{n,nm-k}(\alpha, w^{(b)}) = \{0\}$.

As a consequence, the code $\mathcal{ARS}_{n,k}(\alpha, w^{(a)})$ is an ACD MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.

Proof. Working as in Theorem 9 of Jin [55] and by applying Corollary 8.4.1, the desired result follows. □

The following example illustrates the above theorem.

Example 8.4.9. *Let $q = 2$, $m = 4$, $n = 3$ and $k = 5$, and let ξ be a primitive element of $\mathbb{F}_{16}$. Let $\alpha = (\xi^7, \xi^3, \xi)$, i.e., $\alpha_1 = \xi^7$, $\alpha_2 = \xi^3$ and $\alpha_3 = \xi$. Let $a(x) = x^5 + x + 1$ and $b(x) = x^7 + x + 1 \in \mathbb{F}_2[x]$. Note that $a(x)$ and $b(x)$ are two coprime polynomials in $\mathbb{F}_q[x]$ with $\deg(a(x)) = 5$ and $\deg(b(x)) = nm - k = 7$. By carrying out computations in the Magma Computational Algebra System, we see that $z = (\xi^5, \xi^{10}, 1) \in (\mathbb{F}_{16})^3$ satisfies $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as* *defined by* (8.4.3). *This implies that* $w^{(a)} = (\xi^{14}, 1, \xi^5)$ *and* $w^{(b)} = (\xi^6, \xi^{10}, \xi^{10})$. *Further, by carrying out computations in the Magma Computational Algebra System, we see that the code* $\mathcal{ARS}_{n,k}(\alpha, w^{(a)})$ *is an additive* $[3, 5, 2]$*-code over* $\mathbb{F}_{16}$ *and that the code* $\mathcal{ARS}_{n,nm-k}(\alpha, w^{(b)})$ *is an additive* $[3, 7, 2]$*-code over* $\mathbb{F}_{16}$*, and hence these are MDS codes. We also see that* $\mathcal{ARS}_{n,k}(\alpha, w^{(a)})^{\perp} = \mathcal{ARS}_{n,nm-k}(\alpha, w^{(b)})$ *and* $\mathcal{ARS}_{n,k}(\alpha, w^{(a)}) \cap \mathcal{ARS}_{n,nm-k}(\alpha, w^{(b)}) = \{0\}$. *It agrees with Theorem 8.4.5.*

8.5 Additive generalized twisted Reed-Solomon codes over finite fields

Recently, Beelen *et al.* [9–11] introduced and studied (linear) twisted Reed-Solomon (TRS) codes over finite fields and showed that these codes are not MDS in general. They also identified several classes of linear MDS codes within the family of TRS codes. In this section, we will introduce and study a new class of additive codes over finite fields, *viz.* additive generalized twisted Reed-Solomon (additive GTRS) codes, which is an extension of linear TRS codes over finite fields.

To define these codes, we assume, throughout this section, that n, k and $m \geq 2$ are integers satisfying $1 \leq k < nm$. Let ℓ be a positive integer, and let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{0, 1, \ldots, k-1\}^\ell$ be such that the pairs $(h_1, t_1), (h_2, t_2), \ldots, (h_\ell, t_\ell)$ are distinct. Let $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in \mathbb{F}_q^\ell$. The positive integer ℓ equals the number of twists, the vector $\boldsymbol{t}$ is called the twist vector, the vector $\boldsymbol{h}$ is called the hook vector and the vector $\boldsymbol{\eta}$ is called the coefficient vector. Then the set $\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ of $(n, k, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$-twisted polynomials over $\mathbb{F}_q$ is defined as

$$\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = \left\{ \sum_{i=0}^{k-1} a_i x^i + \sum_{j=1}^{\ell} \eta_j a_{h_j} x^{k-1+t_j} : a_i \in \mathbb{F}_q \right\} \subseteq \mathbb{F}_q[x].$$

By Lemma 1 of Beelen *et al.* [10], we see that the set $\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ of $(n, k, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$-twisted polynomials over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q[x]$ over $\mathbb{F}_q$ with a basis set $\{p_0(x), p_1(x), \ldots, p_{k-1}(x)\}$, where

$$p_i(x) = x^i + \sum_{\substack{j=1 \\ h_j=i}}^{\ell} \eta_j x^{k-1+t_j} \text{ for } 0 \leq i \leq k-1. \tag{8.5.1}$$

Now to define additive GTRS codes, let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n \setminus \mathbb{F}_q^n$ and $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct. It is easy to see that the evaluation map $\mathcal{E}_{\alpha,v} : \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) \to \mathbb{F}_{q^m}^n$, defined as

$$\mathcal{E}_{\alpha,v}(f(x)) = \big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) \text{ for all } f(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}),$$

is an $\mathbb{F}_q$-linear vector space homomorphism, and hence its image $\mathcal{E}_{\alpha,v}(\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}))$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$. The additive generalized twisted Reed-Solomon (additive GTRS) code of length n over $\mathbb{F}_{q^m}$ with ℓ twists, evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$ and column multipliers $v_1, v_2, \ldots, v_n$ is defined as

$$\begin{array}{rcl} \mathscr{T}_{n,k}(\alpha, v, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) & = & \mathcal{E}_{\alpha,v}\big(\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\big) \\ & = & \big\{\big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n)\big) : f(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\big\}. \end{array}$$

In particular, if $v = \mathbf{1} = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the additive GTRS code $\mathscr{T}_{n,k}(\alpha, v, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ is called the additive twisted Reed-Solomon (additive TRS) code over $\mathbb{F}_{q^m}$ with ℓ twists and evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n$. Further, the extended additive generalized twisted Reed-Solomon (extended additive GTRS) code of length $n+1$ over $\mathbb{F}_{q^m}$ with ℓ twists, evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$ and column multipliers $v_1, v_2, \ldots, v_n, 1$ is defined as

$$\begin{array}{l} \mathscr{T}_{n,k}(\alpha, v, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}, \infty) \\ \qquad = \big\{\big(v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n), f(\infty)\big) : f(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\big\}, \end{array}$$

where $f(\infty)$ is defined as the coefficient of x^{k-1+t_θ} in $f(x)$ for each $f(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ with $t_\theta = \max\limits_{1 \leq j \leq \ell}\{t_j : \eta_j \neq 0\}$. In particular, if $v = \mathbf{1} = (1, 1, \ldots, 1)$ is the all-one vector of length n, then the extended additive GTRS code $\mathscr{T}_{n,k}(\alpha, v, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}, \infty)$ is called the extended additive twisted Reed-Solomon (extended additive TRS) code over $\mathbb{F}_{q^m}$ with ℓ twists and evaluation points $\alpha_1, \alpha_2, \ldots, \alpha_n, \infty$. Note that additive

GTRS (*resp.* extended additive GTRS) codes coincide with additive GRS (*resp.* extended additive GRS) codes when $\boldsymbol{\eta} = (0, 0, \ldots, 0)$. So from now on, we assume that $\eta_1, \eta_2, \ldots, \eta_\ell$ are non-zero elements of $\mathbb{F}_q$. We also assume, throughout this section, that no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and that each α_i has exactly m distinct conjugates over $\mathbb{F}_q$.

Proposition 8.5.1. *Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then for $1 \leq k < nm$, the code $\mathscr{T}_{n,k}(\alpha, v, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ is an additive code of length n and dimension k over $\mathbb{F}_{q^m}$ with a generator matrix*

$$\mathscr{G}_{\alpha,v} = \begin{bmatrix} v_1 p_0(\alpha_1) & v_2 p_0(\alpha_2) & \cdots & v_n p_0(\alpha_n) \\ v_1 p_1(\alpha_1) & v_2 p_1(\alpha_2) & \cdots & v_n p_1(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ v_1 p_{k-1}(\alpha_1) & v_2 p_{k-1}(\alpha_2) & \cdots & v_n p_{k-1}(\alpha_n) \end{bmatrix},$$

where the polynomials $p_0(x), p_1(x), \ldots, p_{k-1}(x)$ are as defined by (8.5.1).

Proof. Working in a similar manner as in Proposition 1 of Beelen *et al.* [10] and by applying Theorem 3.7.4 of [53], the desired result follows. □

We will now identify several classes of additive GTRS and extended additive GTRS codes over $\mathbb{F}_{q^m}$, which are either MDS or almost MDS. Towards this, we assume, throughout this section, that $\ell = 1$ (unless specified otherwise), $\boldsymbol{t} = t_1 = 1$, $\boldsymbol{h} = h_1 = h \in \{0, 1, 2, \ldots, k-1\}$ and $\boldsymbol{\eta} = \eta_1 = \eta \in \mathbb{F}_q^*$. In this case, we see that the set $\mathscr{P}_{n,k}(1, h, \eta)$ of $(n, k, 1, h, \eta)$-twisted polynomials over $\mathbb{F}_q$ is given by

$$\mathscr{P}_{n,k}(1, h, \eta) = \left\{ \sum_{i=0}^{k-1} a_i x^i + \eta a_h x^k : a_i \in \mathbb{F}_q \right\}.$$

In the following theorem, we consider the case when m does not divide k, and we identify a class of additive MDS codes of length n and dimension k over $\mathbb{F}_{q^m}$ within the family of additive GTRS codes with one twist.

Theorem 8.5.1. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m does not divide k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $\ell = 1$, $t_1 = 1$ and $h \in \{0, 1, 2, \ldots, k-1\}$. Then for each $\eta \in \mathbb{F}_q^*$, the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.*

Proof. By Proposition 8.5.1, we see that the additive code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ has dimension k. We next assert that the Hamming distance of the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is $n - \lceil \frac{k}{m} \rceil + 1$.

To prove this assertion, let $c_f = \mathcal{E}_{\alpha,v}(f(x)) = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n))$ be a non-zero codeword of $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ corresponding to the twisted polynomial $f(x) \in \mathscr{P}_{n,k}(1, h, \eta)$ with Hamming weight $w_H(c_f) = s$. This implies that precisely $n - s$ coordinates, say i_1-th, i_2-th, $\ldots$, i_{n-s}-th, of the codeword c_f are zero, which implies that $f(\alpha_j) = 0$ for $j \in \{i_1, i_2, \ldots, i_{n-s}\}$. Now by applying Theorem 3.7.4 of [53], we see that if $f(\alpha_j) = 0$, then $f(\alpha_j^q) = f(\alpha_j^{q^2}) = \cdots = f(\alpha_j^{q^{m-1}}) = 0$, where $j \in \{i_1, i_2, \ldots, i_{n-s}\}$. From this, it follows that the polynomial $f(x)$ has at least $m(n-s)$ distinct roots. Since $\deg(f(x)) \leq k$, we must have $m(n-s) \leq k$, which gives $n - \lceil \frac{k}{m} \rceil < s$. From this and by applying Theorem 8.2.2, we see that the Hamming distance of the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is $n - \lceil \frac{k}{m} \rceil + 1$, and hence it is an MDS code. □

The following example illustrates the above theorem.

Example 8.5.1. *Let $q = 11$, $m = 2$, $n = 55$ and $k = 5$, and let ξ be a primitive element of $\mathbb{F}_{121}$. Let $h = 1$ and $\eta = 2 \in \mathbb{F}_{11}$. Let $\alpha = (\xi^{52}, \xi^{18}, \xi^{9}, \xi^{30}, \xi^{5}, \xi^{20}, \xi^{76}, \xi^{73}, \xi^{4}, \xi^{41}, \xi^{61}, \xi^{97}, \xi^{49}, \xi^{74}, \xi^{25}, \xi^{7}, \xi^{3}, \xi^{31}, \xi^{42}, \xi^{14}, \xi^{39}, \xi^{15}, \xi^{98}, \xi^{43}, \xi^{37}, \xi^{87}, \xi^{62}, \xi^{109}, \xi^{53}, \xi^{54}, \xi^{28}, \xi^{38}, \xi^{51}, \xi^{17}, \xi^{65}, \xi^{19}, \xi^{85}, \xi^{40}, \xi^{13}, \xi^{26}, \xi^{86}, \xi^{63}, \xi^{27}, \xi^{32}, \xi^{75}, \xi^{21}, \xi^{64}, \xi^{8}, \xi^{10}, \xi^{29}, \xi^{50}, \xi, \xi^{6}, \xi^{2}, \xi^{16}) \in \mathbb{F}_{121}^{55}$, and let $v = \mathbf{1} = (1, 1, \ldots, 1)$ be the all-one vector of length 55. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 1, 2)$ is an additive $[55, 5, 53]$-code over $\mathbb{F}_{121}$, and hence it is an MDS code. It agrees with Theorem 8.5.1.*

Theorem 8.5.1 shows that no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$ are sufficient conditions for the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ to be an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$. The following example illustrates that these conditions on the evaluation points α_i's are not necessary for the additive code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ to be MDS.

Example 8.5.2. *Let $q = 3$, $m = 2$, $n = 4$, $k = 3$, $h = 1$, and $\eta = 2 \in \mathbb{F}_3$. Let ξ be a primitive element of $\mathbb{F}_9$. Let us take $\alpha = (\xi, \xi^2, \xi^5, 2) \in \mathbb{F}_9^4$ and $v = \mathbf{1} = (1, 1, 1, 1)$. Note that the evaluation point 2 has exactly one conjugate over $\mathbb{F}_3$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, h, \eta)$ is an additive $[4, 3, 3]$-code over $\mathbb{F}_9$, and hence it is an MDS code.*

In the following theorem, we assume that m does not divide k, and we identify a class of k-dimensional additive codes over $\mathbb{F}_{q^m}$ that are either MDS or almost MDS within the family of extended additive GTRS codes with one twist.

Theorem 8.5.2. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m does not divide k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each $\alpha_i \in \mathbb{F}_{q^m}$ has exactly m distinct conjugates over $\mathbb{F}_q$. Let $\ell = 1$, $t_1 = 1$ and $h \in \{0, 1, 2, \ldots, k-1\}$. Then for any $\eta \in \mathbb{F}_q^*$, the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ is an additive code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ with Hamming distance*

$$d_H(\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)) \geq n + 1 - \left\lceil \frac{k}{m} \right\rceil.$$

As a consequence, the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ is either MDS or almost MDS.

Proof. Working in a similar manner as in Theorem 8.5.1 and by applying Theorem 8.2.2, the desired result follows immediately. □

The following two examples illustrate the above theorem.

Example 8.5.3. *Let $q = 7$, $m = 2$, $n = 21$, $k = 5$, $h = 2$, and $\eta = 1 \in \mathbb{F}_7$. Let ξ be a primitive element of $\mathbb{F}_{49}$. Let $\alpha = (\xi^{25}, \xi^{13}, \xi^{41}, \xi, \xi^9, \xi^{33}, \xi^3, \xi^{34}, \xi^{11}, \xi^{26}, \xi^{19}, \xi^{10}, \xi^{18}, \xi^{20}, \xi^{17}, \xi^5, \xi^4, \xi^{27}, \xi^6, \xi^2, \xi^{12})$, and let $v = \mathbf{1} = (1, 1, \ldots, 1)$ be the all-one vector of length 21. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 2, 1, \infty)$ is an additive $[22, 5, 19]$-code over $\mathbb{F}_{49}$, and hence it is an almost MDS code. It agrees with Theorem 8.5.2.*

Example 8.5.4. *Let $q = 3$, $m = 2$, $n = 3$, $k = 3$, $h = 0$, and $\eta = 2 \in \mathbb{F}_3$. Let ξ be a primitive element of $\mathbb{F}_9$. Let $\alpha = (\xi, \xi^2, \xi^5)$, and let $v = \mathbf{1} = (1, 1, 1)$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 0, 2, \infty)$ is an additive $[4, 3, 3]$-code over $\mathbb{F}_9$, and hence it is an MDS code. It agrees with Theorem 8.5.2.*

In a recent work, Huang *et al.* [51] derived necessary and sufficient conditions under which a linear GTRS code with one twist is either MDS or almost MDS. In the following theorem, we assume that m divides k, and we derive necessary and sufficient conditions under which the additive GTRS code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is either MDS or almost MDS.

Theorem 8.5.3. *Let n, k and $m \geq 2$ be positive integers such that $1 \leq k < nm$ and m divides k. Let $\ell = 1$, $t_1 = 1$, $h \in \{0, 1, 2, \ldots, k-1\}$, and let $\eta \in \mathbb{F}_q^*$. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. For each subset I of $\{1, 2, \ldots, n\}$, let us define $\mathcal{R}_I = \{\alpha_i^{q^j} : i \in I \text{ and } 0 \leq j \leq m-1\}$. Further, let us define the set*

$$\mathscr{X}_{k,h} = \Big\{(-1)^{k-h} \sum_{\substack{J \subseteq \mathcal{R}_I \\ |J| = k-h}} \prod_{\mu \in J} \mu \;:\; I \subseteq \{1, 2, \ldots, n\} \text{ with } |I| = \frac{k}{m}\Big\}. \tag{8.5.2}$$

Then the following hold.

(a) The Hamming distance of the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is at least $n - \frac{k}{m}$.

(b) The code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is MDS if and only if $\eta^{-1} \notin \mathscr{X}_{k,h}$.

(c) The code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is almost MDS if and only if $\eta^{-1} \in \mathscr{X}_{k,h}$.

Proof. (a) By Proposition 8.5.1, we see that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ has dimension k. Further, working in a similar manner as in Theorem 8.5.1, we see that the Hamming distance d of the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ satisfies $d \geq n - \frac{k}{m}$.

(b) To prove (b), let us first assume that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is MDS, *i.e.*, $d = n - \frac{k}{m} + 1$. Here we assert that $\eta^{-1} \notin \mathscr{X}_{k,h}$.

To prove this assertion, we suppose, on the contrary, that $\eta^{-1} \in \mathscr{X}_{k,h}$, *i.e.,* there exists a subset I of $\{1, 2, \ldots, n\}$ such that $|I| = \frac{k}{m}$ and

$$\eta^{-1} = (-1)^{k-h} \sum_{\substack{J \subseteq \mathcal{R}_I \\ |J|=k-h}} \prod_{\mu \in J} \mu.$$

Now consider the polynomial $g(x) = \eta \prod\limits_{i \in I} (x - \alpha_i)(x - \alpha_i^q) \cdots (x - \alpha_i^{q^{m-1}})$. It is easy to see that the polynomial $g(x) \in \mathscr{P}_{n,k}(1, h, \eta)$ and that the codeword

$$c_g = \mathcal{E}_{\alpha,v}(g(x)) = (v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n)) \in \mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$$

has Hamming weight $n - \frac{k}{m}$. This implies that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is not MDS, which is a contradiction.

Conversely, let us assume that $\eta^{-1} \notin \mathscr{X}_{k,h}$. We assert that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is MDS. To prove this, we suppose, on the contrary, that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ is not MDS, which implies that there exists a non-zero codeword

$$c_z = \mathcal{E}_{\alpha,v}(z(x)) = (v_1 z(\alpha_1), v_2 z(\alpha_2), \ldots, v_n z(\alpha_n))$$

of the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta)$ corresponding to the twisted polynomial $z(x) \in \mathscr{P}_{n,k}(1, h, \eta)$ with Hamming weight $w_H(c_z) \leq n - \frac{k}{m}$. This implies that the polynomial $z(x) = \sum\limits_{i=0}^{k-1} a_i x^i + \eta a_h x^k \in \mathscr{P}_{n,k}(1, h, \eta)$ has at least $\frac{k}{m}$ roots among $\alpha_1, \alpha_2, \ldots, \alpha_n$. Now by applying Theorem 3.7.4 of [53], we see that $a_h \neq 0$, and that

$$z(x) = \eta a_h \prod_{i \in I_0} (x - \alpha_i)(x - \alpha_i^q) \cdots (x - \alpha_i^{q^{m-1}})$$

for some subset I_0 of $\{1, 2, \ldots, n\}$ with $|I_0| = \frac{k}{m}$. Since $z(x) \in \mathscr{P}_{n,k}(1, h, \eta)$, we note that the coefficient of x^k is equal to η times the coefficient of x^h in $z(x)$. This gives

$$\eta^{-1} = (-1)^{k-h} \sum_{\substack{J \subseteq \mathcal{R}_{I_0} \\ |J|=k-h}} \prod_{\mu \in J} \mu.$$

This implies that $\eta^{-1} \in \mathscr{X}_{k,h}$, which is a contradiction.

(c) It follows immediately from parts (a) and (b). □

On taking $h = k - 1$ in the above theorem, we deduce the following:

Theorem 8.5.4. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m divides k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then the code $\mathscr{T}_{n,k}(\alpha, v, 1, k-1, \eta)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ if and only if*

$$\eta^{-1} \neq -\sum_{i \in I} Tr_{q,m}(\alpha_i)$$

for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \frac{k}{m}$, where $Tr_{q,m} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is the trace map.

Proof. It follows immediately on taking $h = k - 1$ in Theorem 8.5.3. □

On taking $h = 0$ in Theorem 8.5.3, we deduce the following:

Theorem 8.5.5. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m divides k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then the code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$ if and only if*

$$\eta^{-1} \neq (-1)^k \prod_{i \in I} N_{q,m}(\alpha_i)$$

for all subsets I of $\{1, 2, \ldots, n\}$ with $|I| = \frac{k}{m}$, where $N_{q,m} : \mathbb{F}_{q^m}^* \to \mathbb{F}_q^*$ is the norm map.

Proof. On taking $h = 0$ in Theorem 8.5.3, we get the desired result. □

We will now apply Theorems 8.5.4 and 8.5.5 to identify new classes of additive MDS codes within the family of additive GTRS codes when $\ell = 1$, $t_1 = 1$, $h \in \{0, k-1\}$ and $\eta \in \mathbb{F}_q^*$. Towards this, we see, by Theorem 1 of Cohen [33], that if $m \geq 3$ and $(q, m) \neq (4, 3)$, then for every $\lambda \in \mathbb{F}_q$, there exists a primitive element

$\beta \in \mathbb{F}_{q^m}$ such that $Tr_{q,m}(\beta) = \lambda$. Moreover, if either $m = 2$ or $(q, m) = (4, 3)$, then for every non-zero element $\lambda \in \mathbb{F}_q$, there exists a primitive element $\beta \in \mathbb{F}_{q^m}$ such that $Tr_{q,m}(\beta) = \lambda$. We will apply this result to identify a class of additive MDS codes of length n and dimension k over $\mathbb{F}_{q^m}$ within the family of additive GTRS codes with one twist when m divides k.

Theorem 8.5.6. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m divides k. Let $t_1 = 1$, $h = k - 1$, and let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$. Let H be a proper subgroup of $(\mathbb{F}_q, +)$, and let $\eta^{-1} \in \mathbb{F}_q^* \setminus H$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct primitive elements of $\mathbb{F}_{q^m}$ such that no two primitive elements among α_i's are conjugates over $\mathbb{F}_q$ and $Tr_{q,m}(\alpha_i) \in H$. Further, when either $m = 2$ or $(q, m) = (4, 3)$, suppose that $\alpha_1, \alpha_2, \ldots, \alpha_n$ satisfy the additional condition that $Tr_{q,m}(\alpha_i) \neq 0$ for each i. Then the code $\mathscr{T}_{n,k}(\alpha, v, 1, k-1, \eta)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.*

Proof. It follows immediately by applying Theorem 1 of Cohen [33] and Theorem 8.5.4. □

The following example illustrates the above theorem.

Example 8.5.5. *Let $q = 16$, $m = 2$, $n = 36$, $k = 6$ and $h = 5$. Let ζ be a primitive element of $\mathbb{F}_{16}$, and let ξ be a primitive element of $\mathbb{F}_{256}$. Let $\mathcal{H} = \{0, 1, \zeta, \zeta^2, 1+\zeta, \zeta+\zeta^2, 1+\zeta^2, 1+\zeta+\zeta^2\}$ be a proper subgroup of the additive group of $\mathbb{F}_{16}$, and let $\eta = \zeta^{12} \in \mathbb{F}_{16}$. Let $\alpha = (\xi^{56}, \xi^{112}, \xi^{14}, \xi^{28}, \xi^{239}, \xi^{206}, \xi^{241}, \xi^{73}, \xi^{8}, \xi, \xi^{223}, \xi^{157}, \xi^{227}, \xi^{41}, \xi^{103}, \xi^{4}, \xi^{74}, \xi^{143}, \xi^{127}, \xi^{2}, \xi^{37}, \xi^{191}, \xi^{124}, \xi^{59}, \xi^{52}, \xi^{19}, \xi^{208}, \xi^{23}, \xi^{92}, \xi^{76}, \xi^{137}, \xi^{104}, \xi^{139}, \xi^{38}, \xi^{226}, \xi^{161}) \in \mathbb{F}_{256}^{36}$, and let $v = \mathbf{1} = (1, 1, \ldots, 1)$ be the all-one vector of length 36. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 5, \zeta^{12})$ is an additive $[36, 6, 34]$-code over $\mathbb{F}_{256}$, and hence it is an MDS code. It agrees with Theorem 8.5.6.*

As a consequence of Theorem 8.5.6, we deduce the following:

Corollary 8.5.1. *Let $q = p^r$, where p is a prime number and r is a positive integer. Let n and $m \geq 2$ be integers satisfying $1 \leq n \leq p^{r-1} - \epsilon$, where $\epsilon = 1$ if either $m = 2$ or $(q, m) = (4, 3)$, while $\epsilon = 0$ otherwise. For any integer k satisfying $1 \leq k < nm$ and m divides k, there exists an additive GTRS code of length n and dimension k over $\mathbb{F}_{q^m}$, which is MDS.*

Proof. Let $\mathcal{H}$ be a proper subgroup of the additive group of $\mathbb{F}_q$ of order p^{r-1}. Let $g_1, g_2, \ldots, g_n$ be distinct elements of $\mathcal{H}$. When either $m = 2$ or $(q, m) = (4, 3)$, we also assume that each $g_i \neq 0$. Now for $1 \leq i \leq n$, we see, by applying Theorem 1 of Cohen [33], that there exists a primitive element $\alpha_i \in \mathbb{F}_{q^m}$ such that $Tr_{q,m}(\alpha_i) = g_i$. Note that $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct primitive elements of $\mathbb{F}_{q^m}$, which do not form conjugate pairs over $\mathbb{F}_q$. Since $\mathcal{H}$ is a proper subgroup of the additive group of $\mathbb{F}_q$, there exists an element $\eta \in \mathbb{F}_q^*$ such that $\eta^{-1} \in \mathbb{F}_q^* \setminus \mathcal{H}$. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$ be fixed arbitrarily. Now by applying Theorem 8.5.6, one can easily see that the code $\mathscr{T}_{n,k}(\alpha, v, 1, k-1, \eta)$ is an additive MDS code of length n and dimension k over $\mathbb{F}_{q^m}$. □

From this point on, we assume, throughout this section, that $q \geq 3$ (unless specified otherwise). Let $\mathbb{Z}_{q^m-1}^*$ denote the unit group of the ring $\mathbb{Z}_{q^m-1}$ of integers modulo $q^m - 1$. It is well-known that the group $\mathbb{Z}_{q^m-1}^*$ is of order $\phi(q^m - 1)$, where ϕ is the Euler phi function. Further, when $q \geq 3$, we observe that for each element $a \in \mathbb{Z}_{q^m-1}^*$, there exists an integer j satisfying $1 \leq j \leq q-2$, $\gcd(j, q-1) = 1$ and $a \equiv j \pmod{q-1}$. Now for an integer j satisfying $1 \leq j \leq q-2$ and $\gcd(j, q-1) = 1$, let us define the set

$$\mathcal{S}_j = \big\{a \in \mathbb{Z}_{q^m-1}^* : a \equiv j \pmod{q-1}\big\}. \tag{8.5.3}$$

One can easily see that

$$\mathbb{Z}_{q^m-1}^* = \bigcup_{\substack{j=1\\ \gcd(j,q-1)=1}}^{q-2} \mathcal{S}_j \text{ (a disjoint union).}$$

In the following lemma, we show that each of the $\phi(q-1)$ sets $\mathcal{S}_j$'s have the same cardinality.

Lemma 8.5.1. *Let $q \geq 3$ be a prime power, and let $m \geq 2$ be an integer. For any integer j satisfying $1 \leq j \leq q-2$ and $\gcd(j, q-1) = 1$, we have $|\mathcal{S}_j| = \frac{\phi(q^m-1)}{\phi(q-1)}$.*

Proof. To prove the result, we first note that the set $\mathcal{S}_1 = \big\{a \in \mathbb{Z}_{q^m-1}^* : a \equiv 1 \pmod{q-1}\big\}$ is a subgroup of $\mathbb{Z}_{q^m-1}^*$. We next assert that for each integer j satisfying $1 \leq j \leq q-2$ and $\gcd(j, q-1) = 1$, the set $\mathcal{S}_j$ is a coset of $\mathcal{S}_1$ in $\mathbb{Z}_{q^m-1}^*$.

To prove this assertion, let j be a fixed integer satisfying $1 \leq j \leq q-2$ and $\gcd(j, q-1) = 1$. Now let us consider the arithmetic progression (A.P.):

$$\ldots\ldots, j-2(q-1), j-(q-1), j, j+(q-1), j+2(q-1), \ldots\ldots \tag{8.5.4}$$

By Dirichlet's Theorem on primes in A.P., we see that the A.P. (8.5.4) contains infinitely many primes. We can choose a prime number p_j such that $\gcd(p_j, q^m-1) = 1$ and $p_j \equiv j \pmod{q-1}$. That is, there exists an element $p_j \in \mathcal{S}_j$. Further, one can easily observe that $\mathcal{S}_j = p_j \mathcal{S}_1$, which proves the assertion.

From the above assertion, we see that $|\mathcal{S}_j| = |\mathcal{S}_1|$ for all j satisfying $1 \leq j \leq q-2$ and $\gcd(j, q-1) = 1$. This implies that

$$\phi(q^m-1) = |\mathbb{Z}^*_{q^m-1}| = |\mathcal{S}_1| \times \phi(q-1),$$

from which the desired result follows immediately. □

Now let ξ be a primitive element of $\mathbb{F}_{q^m}$. Note that the set $\mathcal{G} = \{\xi^i : i \in \mathbb{Z}^*_{q^m-1}\}$ consists of all the primitive elements of $\mathbb{F}_{q^m}$. We further observe, for $a, b \in \mathbb{Z}^*_{q^m-1}$, that $N_{q,m}(\xi^a) = N_{q,m}(\xi^b)$ if and only if both $a, b \in \mathcal{S}_j$ for some j. Accordingly, the set $\mathcal{G}$ can be partitioned as

$$\mathcal{G} = \bigcup_{\substack{j=1 \\ \gcd(j,q-1)=1}}^{q-2} \mathcal{G}_j \text{ (a disjoint union)},$$

where $\mathcal{G}_j = \{\xi^a : a \in \mathcal{S}_j\}$ for each j. In the following theorem, we assume that m divides k, and we derive some sufficient conditions under which there exists $\eta \in \mathbb{F}_q^*$ such that the code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is MDS.

Theorem 8.5.7. *Let $q \geq 3$ be a prime power, and let n, k and $m \geq 2$ be integers such that $1 \leq n \leq \frac{\phi(q^m-1)}{m\phi(q-1)}$, $1 \leq k < nm$ and m divides k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}^*_{q^m})^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}^n_{q^m}$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct elements of the set $\mathcal{G}_j$ for some j, which do not form conjugate pairs over $\mathbb{F}_q$, (such a choice of α_i's is possible, as $n \leq \frac{\phi(q^m-1)}{m\phi(q-1)}$). For $1 \leq k < nm$, there exists $\eta \in \mathbb{F}_q^*$ such that the code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is MDS.*

Proof. To prove the result, we first note that $N_{q,m}(\alpha_1) = N_{q,m}(\alpha_2) = \cdots = N_{q,m}(\alpha_n)$. Now by applying Theorem 8.5.5, we see that the code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is MDS if and only if $\eta^{-1} \neq (-1)^k (N_{q,m}(\alpha_1))^{\frac{k}{m}}$. Such an element η exists, as $q \geq 3$. This proves the theorem. □

The following example illustrates above theorem.

Example 8.5.6. *Let $q = 3$, $m = 5$, $n = 22$, $k = 20$, $h = 0$, and $\eta = 2 \in \mathbb{F}_3$. Let ξ be a primitive element of $\mathbb{F}_{243}$. Let $\alpha = (\xi^{13}, \xi^{53}, \xi^{67}, \xi, \xi^{131}, \xi^{17}, \xi^{79}, \xi^{95}, \xi^{71}, \xi^{35}, \xi^{15}, \xi^{23}, \xi^{125}, \xi^{25}, \xi^{47}, \xi^{49}, \xi^{29}, \xi^{161}, \xi^{41}, \xi^{61}, \xi^{31}, \xi^{7}) \in \mathbb{F}_{243}^{22}$, and let $v = \mathbf{1} = (1, 1, \ldots, 1)$ be the all-one vector of length 22. Note that $\xi^{13}, \xi^{53}, \xi^{67}, \xi, \xi^{131}, \xi^{17}, \xi^{79}, \xi^{95}, \xi^{71}, \xi^{35}, \xi^{15}, \xi^{23}, \xi^{125}, \xi^{25}, \xi^{47}, \xi^{49}, \xi^{29}, \xi^{161}, \xi^{41}, \xi^{61}, \xi^{31}, \xi^{7} \in \mathcal{G}_1$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 0, 2)$ is an additive $[22, 20, 19]$-code over $\mathbb{F}_{243}$, which is MDS. It agrees with Theorem 8.5.7.*

In the following theorem, we consider the case when m divides k, and we derive some sufficient conditions under which there exist $\eta \in \mathbb{F}_q^*$ and $\alpha \in \mathbb{F}_{q^m}^n$ such that the code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is MDS.

Theorem 8.5.8. *Let $q \geq 3$ be a prime power, $m \geq 2$ be an integer, $\omega = \left\lfloor \frac{\phi(q^m-1)}{m(\phi(q-1))} \right\rfloor$, and let a be an integer satisfying $1 \leq a \leq \phi(q-1)$. Let n, k be integers such that $(a-1)\omega < n \leq a\omega$, $1 \leq k < nm$ and m divides k. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$. Further, if*

$$q - 1 > \min\left\{\left(\frac{k}{m} + 1\right)^{a-1}, (\omega + 1)^{a-1}\right\}\left(\min\left\{\frac{k}{m}, n - (a-1)\omega\right\} + 1\right)$$

holds, then there exist $\eta \in \mathbb{F}_q^*$ and $\alpha \in \mathbb{F}_{q^m}^n$ such that the additive GTRS code $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta)$ is an MDS code of length n and dimension k over $\mathbb{F}_{q^m}$.

Proof. To prove the result, let $b_1, b_2, \ldots, b_a$ be integers satisfying $1 \leq b_j \leq q-2$ and $\gcd(b_j, q-1) = 1$ for $1 \leq j \leq a$. Let us choose $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are distinct elements of $\mathbb{F}_{q^m}$ that do not form conjugate pairs over $\mathbb{F}_q$, $\alpha_{\omega(j-1)+i} \in \mathcal{G}_{b_j}$ for $1 \leq j \leq a-1$ and $1 \leq i \leq \omega$, and $\alpha_{\omega(a-1)+s} \in \mathcal{G}_{b_a}$ for $1 \leq s \leq n-(a-1)\omega$. Now consider the set

$$Y = \left\{(-1)^k \prod_{j=1}^{a} \left(N_{q,m}(\alpha_{\omega(j-1)+1})\right)^{\ell_j} : 0 \leq \ell_j \leq \min\left\{\frac{k}{m}, \omega\right\} \text{ for } 1 \leq j \leq a-1\right.$$

$$\text{and } 0 \leq \ell_a \leq \min\Big\{\frac{k}{m}, n-(a-1)\omega\Big\}\Big\}.$$

It is easy to see that

$$|Y| \leq \min\Big\{(\frac{k}{m}+1)^{a-1}, (\omega+1)^{a-1}\Big\}\Big(\min\Big\{\frac{k}{m}, n-(a-1)\omega\Big\}+1\Big) < q-1.$$

We next observe that the set

$$\mathscr{X}_{k,0} = \Big\{(-1)^k \prod_{i\in I} N_{q,m}(\alpha_i) : I \subseteq \{1,2,\ldots,n\} \text{ with } |I| = \frac{k}{m}\Big\} \subseteq Y,$$

which implies that $|\mathscr{X}_{k,0}| \leq |Y| < q-1$. Thus there exists an element $\eta \in \mathbb{F}_q^*$ such that $\eta^{-1} \notin \mathscr{X}_{k,0}$. Now the desired result follows by applying Theorem 8.5.5. □

The following example illustrates the above theorem.

Example 8.5.7. *Let $q = 25$, $m = 2$, $n = 23$ and $k = 4$. Let ζ be a primitive element of $\mathbb{F}_{25}$, and let ξ be a primitive element of $\mathbb{F}_{625}$. Let $\eta = \zeta^{21} \in \mathbb{F}_{25}$. Let $\alpha = (\xi^{97}, \xi^{289}, \xi^{193}, \xi^{145}, \xi^{241}, \xi^{217}, \xi, \xi^{265}, \xi^{73}, \xi^{313}, \xi^{121}, \xi^{49}, \xi^{269}, \xi^{341}, \xi^{197}, \xi^{173}, \xi^{365}, \xi^{53}, \xi^{317}, \xi^{149}, \xi^{293}, \xi^{245}, \xi^5) \in \mathbb{F}_{625}^{23}$, and let $v = \mathbf{1} = (1,1,\ldots,1)$ be the all-one vector of length* 23. *We observe that the set Y (as defined in the proof of Theorem 8.5.8) is given by $\{1, \zeta^{11}, \zeta, 4, \zeta^2, \zeta^5, 2, \zeta^7, \zeta^{10}\}$. Further, we note that the elements $\xi^{97}, \xi^{289}, \xi^{193}, \xi^{145}, \xi^{241}, \xi^{217}, \xi, \xi^{265}, \xi^{73}, \xi^{313}, \xi^{121}, \xi^{49} \in \mathcal{G}_1$, while the elements $\xi^{269}, \xi^{341}, \xi^{197}, \xi^{173}, \xi^{365}, \xi^{53}, \xi^{317}, \xi^{149}, \xi^{293}, \xi^{245}, \xi^5 \in \mathcal{G}_5$. By carrying out computations in the Magma Computational Algebra System, we see that the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, 0, \zeta^{21})$ is an additive $[23, 4, 22]$-code over $\mathbb{F}_{625}$, and hence it is an MDS code. It agrees with Theorem 8.5.8.*

In the following theorem, we assume that k is a multiple of m, and we identify a class of additive almost MDS codes of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ within the family of extended additive GTRS codes with one twist.

Theorem 8.5.9. *Let n, k and $m \geq 2$ be integers such that $1 \leq k < nm$ and m divides k. Let $\ell = 1$, $t_1 = 1$, $h \in \{0,1,2,\ldots,k-1\}$, and let $\eta \in \mathbb{F}_q^*$. Let $v = (v_1, v_2, \ldots, v_n) \in (\mathbb{F}_{q^m}^*)^n$, and let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Then the additive code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ is an almost MDS code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$.*

Proof. Working in a similar manner as in Theorem 8.5.3(a) and by applying Proposition 8.5.1, we see that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ is an additive code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ with Hamming distance $d_H(\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)) \geq n - \frac{k}{m} + 1$. Now to show that the code $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ is almost MDS, it is enough to show that $d_H(\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)) \leq n - \frac{k}{m} + 1$.

To prove this, let $m_i(x)$ be the minimal polynomial of α_i over $\mathbb{F}_q$ for $1 \leq i \leq n$. Now we shall distinguish the following three cases: (i) $h = 0$, (ii) $1 \leq h \leq k - m$, and (iii) $k - m < h \leq k - 1$.

(i) Let $h = 0$. Here let us define $g(x) = x \prod\limits_{\ell \in \mathcal{L}} m_\ell(x)$, where $\mathcal{L}$ is a subset of $\{1, 2, \ldots, n\}$ with $|\mathcal{L}| = \frac{k}{m} - 1$. It is easy to observe that $g(x) \in \mathscr{P}_{n,k}(1, h, \eta)$. This implies that $c_g = (v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n), g(\infty))$ is a non-zero codeword of $\mathscr{T}_{n,k}(\alpha, v, 1, 0, \eta, \infty)$ with Hamming weight $w_H(c_g) = n - \frac{k}{m} + 1$.

(ii) Next, let $1 \leq h \leq k - m$. Here let I be any arbitrary subset of $\{1, 2, \ldots, n\}$ with $|I| = \frac{k}{m} - 1$, and consider the polynomial $f_I(x) = \prod\limits_{i \in I} m_i(x)$.

Now if the coefficient of x^h in the polynomial $f_I(x)$ is zero, then we see that $f_I(x) \in \mathscr{P}_{n,k}(1, h, \eta)$, which implies that $c_{f_I} = (v_1 f_I(\alpha_1), v_2 f_I(\alpha_2), \ldots, v_n f_I(\alpha_n), f_I(\infty))$ is a non-zero codeword of $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ with Hamming weight $w_H(c_{f_I}) = n - \frac{k}{m} + 1$.

On the other hand, if the coefficient of x^h in the polynomial $f_I(x)$ is non-zero, then we can choose a non-zero polynomial $s_I(x) = s_0 + s_1 x + \cdots + s_{m-1} x^{m-1} \in \mathbb{F}_q[x]$ such that the polynomial $b_I(x) = s_I(x) f_I(x) \in \mathscr{P}_{n,k}(1, h, \eta)$, which implies that $c_{b_I} = (v_1 b_I(\alpha_1), v_2 b_I(\alpha_2), \ldots, v_n b_I(\alpha_n), b_I(\infty))$ is a non-zero codeword of $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ with Hamming weight $w_H(c_{b_I}) = n - \frac{k}{m} + 1$.

(iii) Finally, when $k - m < h \leq k - 1$, let us define the polynomial $z(x) = \prod\limits_{j \in J} m_j(x)$, where J is a subset of $\{1, 2, \ldots, n\}$ with $|J| = \frac{k}{m} - 1$. One can easily see that the polynomial $z(x) \in \mathscr{P}_{n,k}(1, h, \eta)$, which implies that $c_z = (v_1 z(\alpha_1), v_2 z(\alpha_2), \ldots, v_n z(\alpha_n), z(\infty))$ is a non-zero codeword of $\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)$ with Hamming weight $w_H(c_z) = n - \frac{k}{m} + 1$.

On combining the above cases, we get $d_H(\mathscr{T}_{n,k}(\alpha, v, 1, h, \eta, \infty)) \leq n - \frac{k}{m} + 1$, which completes the proof of the theorem. □

In the following theorem, we construct additive self-orthogonal codes over $\mathbb{F}_{q^m}$ through additive GTRS codes with ℓ twists.

Theorem 8.5.10. *Let $q \geq 2$ be a prime power, and let n, k and $m \geq 2$ be positive integers satisfying $k < \frac{nm}{2}$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $z = (z_1, z_2, \ldots, z_n) \in (\mathbb{F}_{q^m}^*)^n$ be such that $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3), (such a vector z exists in $(\mathbb{F}_{q^m}^*)^n$ by Corollary 8.4.3). Let us suppose that $z_i = w_i^2$, where $w_i \in \mathbb{F}_{q^m}^*$ for $1 \leq i \leq n$. Let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ be such that $2k + t_i + t_j \leq nm$ for $1 \leq i, j \leq \ell$. Let $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{0, 1, \ldots, k-1\}^\ell$, $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$, and let $w = (w_1, w_2, \ldots, w_n)$. Then the code $\mathscr{T}_{n,k}(\alpha, w, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ is an additive self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$.*

Proof. The desired result follows immediately by applying Theorem 7.3.1 and Proposition 8.5.1. □

In the following corollary, we construct additive self-orthogonal codes over $\mathbb{F}_{q^m}$ that are either MDS or almost MDS through additive GTRS codes with one twist.

Corollary 8.5.2. *Let $q \geq 2$ be an even prime power, and let n, k and $m \geq 2$ be positive integers satisfying $n \leq \frac{\phi(q^m-1)}{m}$ and $k \leq \frac{nm-2}{2}$. Then the following hold.*

(a) When m does not divide k, there exists an additive MDS self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$.

(b) When m divides k, there exists an additive self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$, which is either MDS or almost MDS.

Proof. To prove the result, let us choose $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in (\mathbb{F}_{q^m}^*)^n$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are primitive elements of $\mathbb{F}_{q^m}$ that do not form conjugate pairs over $\mathbb{F}_q$. By Corollary 8.4.3, we see that there exists a vector $z = (z_1, z_2, \ldots, z_n) \in (\mathbb{F}_{q^m}^*)^n$ satisfying $Tr_{q,m}(\mathcal{A}z^t) = 0$, where the matrix $\mathcal{A}$ is as defined by (8.4.3). Since q is even, we can write $z_i = w_i^2$, where $w_i \in \mathbb{F}_{q^m}^*$ for $1 \leq i \leq n$. Let us take $w = (w_1, w_2, \ldots, w_n)$. Further, let $\ell = 1$, $t_1 = 1$ and $h \in \{0, 1, \ldots, k-1\}$.

Now if m does not divide k, then we see, by applying Theorems 8.5.1 and 8.5.10, that for every $\eta \in \mathbb{F}_q^*$, the code $\mathscr{T}_{n,k}(\alpha, w, 1, h, \eta)$ is an additive MDS self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$.

On the other hand, if m divides k, then by applying Theorem 8.5.10, we see that the code $\mathscr{T}_{n,k}(\alpha, w, 1, h, \eta)$ is an additive self-orthogonal code of length n and dimension k over $\mathbb{F}_{q^m}$. Further, by Theorem 8.5.3, we observe that the code $\mathscr{T}_{n,k}(\alpha, w, 1, h, \eta)$ is MDS if $\eta^{-1} \notin \mathscr{X}_{k,h}$, while the code $\mathscr{T}_{n,k}(\alpha, w, 1, h, \eta)$ is almost MDS if $\eta^{-1} \in \mathscr{X}_{k,h}$, (here the set $\mathscr{X}_{k,h}$ is as defined by (8.5.2)). From this, the desired result follows immediately. □

8.6 Some classes of additive TRS codes that are not monomially equivalent to additive RS codes

Two additive codes of length n over $\mathbb{F}_{q^m}$ are said to be monomially equivalent if a generator matrix of one code can be obtained from the generator matrix of the other code by post multiplying it with an $n \times n$ monomial matrix over $\mathbb{F}_{q^m}$. Otherwise, these two codes are said to be inequivalent.

The Schur squares of linear codes have recently found several applications in the area of cryptography, and hence this concept has recently attracted a great deal of attention [30, 34, 85]. Recently, Beelen *et al.* [10] and Liu and Liu [65] identified several classes of linear TRS codes that are not monomially equivalent to linear RS codes by studying their Schur squares. In this section, we will define and study Schur squares of additive codes, and identify several classes of additive TRS codes, which are not monomially equivalent to additive RS codes. Since additive codes over $\mathbb{F}_{q^m}$ coincide with linear codes over $\mathbb{F}_q$ when $m = 1$, we will also identify some new classes of linear TRS codes that are not equivalent to linear RS codes as a special case.

Towards this, we recall that the Schur product of two vectors $c = (c_1, c_2, \ldots, c_n)$ and $d = (d_1, d_2, \ldots, d_n)$ in $\mathbb{F}_{q^m}^n$ is defined as $c \star d = (c_1 d_1, c_2 d_2, \ldots, c_n d_n) \in \mathbb{F}_{q^m}^n$. Now let $\mathcal{C}$ be an additive code of length n over $\mathbb{F}_{q^m}$. The Schur square of the code $\mathcal{C}$, denoted by $\mathcal{C}^2$, is defined as the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$ spanned by the set $\{c \star d : c, d \in \mathcal{C}\}$. Note that the Schur square $\mathcal{C}^2$ is an additive code of length n over

$\mathbb{F}_{q^m}$. We further make the following observation.

Lemma 8.6.1. *(a) If $\mathcal{C}$ is an additive code of length n and dimension k over $\mathbb{F}_{q^m}$, then the dimension of its Schur square $\mathcal{C}^2$ satisfies*

$$\dim_{\mathbb{F}_q}(\mathcal{C}^2) \leq \min\Big\{nm, \frac{k(k+1)}{2}\Big\}.$$

(b) If $\mathcal{C}$ and $\mathcal{D}$ are two monomially equivalent additive codes over $\mathbb{F}_{q^m}$, then

$$\dim_{\mathbb{F}_q}(\mathcal{C}^2) = \dim_{\mathbb{F}_q}(\mathcal{D}^2).$$

Proof. Its proof is a straightforward exercise. □

Since additive GRS (*resp.* additive GTRS) and additive RS (*resp.* additive TRS) codes are monomially equivalent, we will consider additive RS (*resp.* additive TRS) codes instead of additive GRS (*resp.* additive GTRS) codes in this section. To begin with, we explicitly determine the dimensions of the Schur squares of the codes belonging to a special class of additive RS codes in the following theorem.

Theorem 8.6.1. *Let n, k and $m \geq 2$ be positive integers satisfying $1 \leq k \leq nm$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. We have $\dim_{\mathbb{F}_q}(\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^2) = min\big\{nm, 2k-1\big\}$.*

Proof. To prove the result, we see that the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ has a generator matrix

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}.$$

Let us define $\alpha^j = (\alpha_1^j, \alpha_2^j, \ldots, \alpha_n^j)$ for any integer $j \geq 0$. Now one can easily observe that the Schur square $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^2$ is the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^m}^n$ spanned by the set $\{\alpha^j \ : \ 0 \leq j \leq 2k-2\}$. We see that the vectors $\mathbf{1}, \alpha, \alpha^2, \ldots, \alpha^{nm-1}$ are linearly independent over $\mathbb{F}_q$. From this, it follows that $\dim_{\mathbb{F}_q}(\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^2) = 2k-1$ if $k < \frac{nm+1}{2}$, while $\dim_{\mathbb{F}_q}(\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^2) = nm$ if $k \geq \frac{nm+1}{2}$. □

Let n, k and $m \geq 2$ be integers satisfying $1 \leq k < nm$. Let $\ell \geq 1$ be any integer, and let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{0, 1, 2, \ldots, k-1\}^\ell$ be such that the pairs $(h_1, t_1), (h_2, t_2), \ldots, (h_\ell, t_\ell)$ are distinct. Let $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$. Recall that $\{p_0(x), p_1(x), \ldots, p_{k-1}(x)\}$ (as defined by (8.5.1)) is a basis set of $\mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$. Further, let

$$\mathcal{D}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = \{\deg(p_i(x)) : 0 \leq i \leq k-1\}.$$

Then by Proposition 5 of Beelen *et al.* [10], we see that

$$\mathcal{D}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = \Big(\{0, 1, \ldots, k-1\} \setminus \{h_j : 1 \leq j \leq \ell\}\Big) \cup \Big\{k - 1 + \max_{\substack{1 \leq s \leq \ell \\ h_s = i}}\{t_s\} : i \in \{h_a : 1 \leq a \leq \ell\}\Big\}. \quad (8.6.1)$$

Next let us define

$$\mathcal{F}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = \big\{d_1 + d_2 : d_1, d_2 \in \mathcal{D}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) \text{ and } d_1 + d_2 < nm\big\}.$$

Further, let $\mathcal{W}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ denote the $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q[x]$ spanned by the set

$$\{f(x)g(x) : f(x), g(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) \text{ and } \deg(f(x)g(x)) < nm\},$$

and let us define

$$\mathcal{V}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = \{\deg(h(x)) : h(x) \in \mathcal{W}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\}.$$

In the following proposition, we derive a lower bound on the dimensions of the Schur squares of the codes belonging to a special class of additive TRS codes with ℓ twists.

Proposition 8.6.1. *Let n, k and $m \geq 2$ be positive integers satisfying $1 \leq k < nm$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{0, 1, 2, \ldots, k-1\}^\ell$ be such that the pairs $(h_1, t_1), (h_2, t_2), \ldots, (h_\ell, t_\ell)$ are distinct, and let $\boldsymbol{\eta} =$*

$(\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$. *Then the Schur square* $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2$ *of the additive TRS code* $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ *is the* $\mathbb{F}_q$*-linear subspace of* $\mathbb{F}_{q^m}^n$ *spanned by the set*

$$\left\{\mathcal{E}_{\alpha,\mathbf{1}}(f(x)g(x)) = \mathcal{E}_{\alpha,\mathbf{1}}(f(x)) \star \mathcal{E}_{\alpha,\mathbf{1}}(g(x)) : f(x), g(x) \in \mathscr{P}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\right\}$$

and

$$\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2) \geq \left|\mathcal{V}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})\right| \geq |\mathcal{F}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})|.$$

Proof. Working in a similar manner as in Lemma 9 and Proposition 5 of Beelen *et al.* [10], the desired result follows. □

In the following theorem, we consider the case $\ell = t_1 = 1$ and $0 \leq h \leq k-1$, and we identify a class of additive TRS codes (consisting of either MDS or almost MDS codes), which are not equivalent to additive MDS RS codes.

Theorem 8.6.2. *Let* n, k *and* $m \geq 2$ *be integers satisfying* $3 \leq k < \frac{nm}{2}$. *Let* $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, *where no two elements among* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *form a conjugate pair over* $\mathbb{F}_q$ *and each* α_i *has exactly* m *distinct conjugates over* $\mathbb{F}_q$. *Let* $\ell = t_1 = 1$, $h \in \{0, 1, 2, \ldots, k-1\}$ *and* $\eta \in \mathbb{F}_q^*$. *Then we have* $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, t_1, h, \eta)^2) \geq 2k$.

As a consequence, the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, h, \eta)$ *is either MDS or almost MDS, but it is not monomially equivalent to the MDS code* $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$. *In particular, if* m *does not divide* k, *then for any* $\eta \in \mathbb{F}_q^*$, *the MDS codes* $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, h, \eta)$ *and* $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ *are not monomially equivalent. On the other hand, if* m *divides* k, *then for any* $\eta^{-1} \notin \mathscr{X}_{k,h}$, *the MDS codes* $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, h, \eta)$ *and* $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ *are not monomially equivalent, where* $\mathscr{X}_{k,h}$ *is as defined by* (8.5.2).

Proof. To prove the result, we first note, by Propositions 8.5.1 and 8.6.1, that $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,3}(\alpha, \mathbf{1}, 1, h, \eta)^2) = 6$ for all $h \in \{0, 1, 2\}$ in the case when $k = 3$. So from now on, we assume, throughout the proof, that $k \geq 4$.

First of all, when $h \in \{0, k-1\}$, working in a similar manner as in Theorems 3 and 4 of Liu and Liu [65], we see that $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, 1, h, \eta)) = 2k$.

Next, when $h \in \{1, 2, \ldots, k-2\}$, we see, by (8.6.1), that the set $\mathcal{D}_{n,k}(1, h, \eta)$ can be partitioned as $\mathcal{D}_{n,k}(1, h, \eta) = A \cup B$, where $A = \{0, 1, \ldots, k-1\} \setminus \{h\}$ and $B = \{k\}$. Note that both $0, k-1 \in A$ and either $1 \in A$ or $k-2 \in A$. We also observe that every $j \in \{0, 1, \ldots, 2k-2\} \setminus \{h, k-1+h\}$ can be written as the sum of two elements of A, which implies that

$$\{0, 1, \ldots, 2k-2\} \setminus \{h, k-1+h\} \subseteq \mathcal{F}_{n,k}(1, h, \eta).$$

Next, if $1 \in A$, then we can write h as the sum $h = (h-1)+1$ of two elements $h-1, 1 \in A$, while if $k-2 \in A$, then we can write $k-1+h$ as the sum $k-1+h = (k-2)+(h+1)$ of two elements $k-2, h+1 \in A$. From this, it follows that either $h \in \mathcal{F}_{n,k}(1, h, \eta)$ or $k-1+h \in \mathcal{F}_{n,k}(1, h, \eta)$. Further, since $k-1 \in A$ and $k \in B$, we see that both $2k-1, 2k \in \mathcal{F}_{n,k}(1, h, \eta)$. This implies that $|\mathcal{F}_{n,k}(1, h, \eta)| \geq 2k$. Now by applying Proposition 8.6.1, we get

$$\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, t_1, h, \eta)^2) \geq 2k.$$

This shows that $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, t_1, h, \eta)^2) \geq 2k$ for all $k \geq 3$. Further, by applying Theorem 8.6.1, we see that the dimension of the Schur square $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})^2$ of the additive RS code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ is $2k-1$. Now by Lemma 8.6.1(b), we see that the additive TRS code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, t_1, h, \eta)$ and the additive RS code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ are not monomially equivalent. Now by applying Corollary 8.4.1 and Theorems 8.5.1 and 8.5.3, the desired result follows immediately. □

Remark 8.6.1. *Additive codes over $\mathbb{F}_{q^m}$ coincide with linear codes over $\mathbb{F}_q$ when $m = 1$. Further, one can observe, in view of Example 1.6 of Randriambololona [85], that the above theorem holds in the case when $m = 1$. When $h \in \{0, k-1\}$, Liu and Liu [65] identified a class of linear TRS codes with one twist and hook h, which are not equivalent to linear RS codes. So the above theorem also gives rise to new classes of linear TRS codes (that are either MDS or almost MDS) with one twist and hook h, which are not equivalent to linear RS codes for all $h \in \{1, 2, \ldots, k-2\}$.*

The following theorem extends Theorem 6 of Beelen *et al.* [10] to additive TRS codes with ℓ twists and additive RS codes over $\mathbb{F}_{q^m}$.

Theorem 8.6.3. *Let n, k and $m \geq 2$ be integers satisfying $3 \leq k < \frac{nm}{2}$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let*

$\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$, and let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ and $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{2, 3, \ldots, k-3\}^\ell$ be such that either $h_i = h_j$ or $h_j - h_i > 1$ for all $1 \leq i < j \leq \ell$. Then we have

$$\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2) \geq 2k.$$

As a consequence, the code $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ is not equivalent to the code $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$.

Proof. Working in a similar manner as in Theorem 6 of Beelen *et al.* [10] and by applying Theorem 8.6.1, the desired result follows. □

In the following theorem, we show that the condition $h_i = h_j$ or $h_j - h_i > 1$ for $1 \leq i < j \leq \ell$ on the hook vector $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell)$ is not necessary for the codes $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ and $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ to be monomially inequivalent. With the help of this observation, we identify another class of additive TRS codes with ℓ twists, which are not equivalent to additive RS codes over $\mathbb{F}_{q^m}$.

Theorem 8.6.4. *Let n, k and $m \geq 2$ be positive integers satisfying $k < \frac{nm}{2}$. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $\boldsymbol{t} = (t_1, t_2, \ldots, t_\ell) \in \{1, 2, \ldots, nm-k\}^\ell$ be such that $2k+t_i+t_j < nm$ for all $1 \leq i, j \leq \ell$. Let $\boldsymbol{\eta} = (\eta_1, \eta_2, \ldots, \eta_\ell) \in (\mathbb{F}_q^*)^\ell$, and let $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{1, 2, \ldots, k-2\}^\ell$ be such that $h_1 < h_2 < \cdots < h_\ell$ with either $h_1 > 1$ or $h_\ell < k-2$. Then we have*

$$\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})^2) \geq 2k.$$

As a consequence, the additive codes $\mathscr{T}_{n,k}(\alpha, \mathbf{1}, \boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ and $\mathcal{ARS}_{n,k}(\alpha, \mathbf{1})$ are not monomially equivalent.

Proof. To prove the result, we will distinguish the following two cases: (i) $h_1 > 1$ and (ii) $h_\ell < k-2$.

(i) Let us suppose that $h_1 > 1$. This implies that $\boldsymbol{h} = (h_1, h_2, \ldots, h_\ell) \in \{2, 3, \ldots, k-2\}^\ell$, where $h_1 < h_2 < \cdots < h_\ell$. Here by (8.6.1), we see that the set $\mathcal{D}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta})$ can be partitioned as $\mathcal{D}_{n,k}(\boldsymbol{t}, \boldsymbol{h}, \boldsymbol{\eta}) = A \cup B$, where $A = \{0, 1, 2, \ldots, k-1\} \setminus \{h_j : 1 \leq j \leq \ell\}$ and $B = \{k-1+t_j : 1 \leq j \leq \ell\}$. Note that

$\{0,1,k-1\}\subset A$. Since $0\in A$, every $j\in A$ can be written as the sum $j=j+0$ of two elements $0,j\in A$, which implies that $j\in\mathcal{F}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$. Next, we observe that both $h_1-1,1\in A$, which implies that $h_1=(h_1-1)+1\in\mathcal{F}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$. We further note that $\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_1}),\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_1}+\eta_1x^{k-1+t_1})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2$, which implies that

$$\mathcal{E}_{\alpha,\mathbf{1}}(x^{k-1+t_1})=\eta_1^{-1}\left(\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_1}+\eta_1x^{k-1+t_1})-\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_1})\right)\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2.$$

Now for all $j\in\{2,3,\ldots,\ell\}$ satisfying $t_j=t_1$, we see that $\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_j})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2$, which implies that $h_j\in\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$.

Further, let us suppose that $t_1=t_{i_1},t_{i_2},\ldots,t_{i_s}$ are distinct integers among $t_1,t_2,\ldots,t_\ell$. Now for $z\in\{i_2,i_3,\ldots,i_s\}$, we observe, for all $j(\neq z)\in\{1,2,\ldots,\ell\}$ satisfying $t_j=t_z$, that both $\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_j}+\eta_jx^{k-1+t_j})$, $\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_z}+\eta_zx^{k-1+t_z})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2$, which implies that

$$\mathcal{E}_{\alpha,\mathbf{1}}(\eta_jx^{h_z}-\eta_zx^{h_j})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2.$$

This implies that $\max\{h_z,h_j\}\in\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$. From this, it follows that

$$\{h_j:1\leq j\leq\ell\text{ and }t_j=t_z\}\setminus\{\min_{1\leq j\leq\ell}\{h_j:t_j=t_z\}\}\subseteq\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$$

for each $z\in\{i_2,i_3,\ldots,i_s\}$. This implies that

$$\big\{0,1,2,\ldots,k-1\big\}\setminus\big\{\min_{1\leq j\leq\ell}\{h_j:t_j=t_z\}:z\in\{i_2,i_3,\ldots,i_s\}\big\}\subseteq\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}).$$

Next, we observe that both $\mathcal{E}_{\alpha,\mathbf{1}}(x^{k-1}),\mathcal{E}_{\alpha,\mathbf{1}}(x^{h_j}+\eta_jx^{k-1+t_j})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$, which implies that

$$\mathcal{E}_{\alpha,\mathbf{1}}(x^{k-1+h_j}+\eta_jx^{2k-2+t_j})\in\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2\text{ for }1\leq j\leq\ell.$$

Further, it is easy to see that

$$\big\{k,k+1,\ldots,2k-2\big\}\setminus\big\{\min_{1\leq j\leq\ell}\{k-1+h_j:t_j=t_z\}:z\in\{i_1,i_2,\ldots,i_s\}\big\}\\ \subseteq\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}).$$

Furthermore, we observe that

$$\{2k-2+t_{i_j} : 1 \leq j \leq s\} \cup \{2k-2+\max_{1\leq\theta\leq s}\{t_{i_\theta}\}+t_{i_j} : 1 \leq j \leq s\} \subseteq \mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}).$$

From this, it follows that $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2) \geq |\mathcal{V}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})| \geq 2k$.

(ii) Next we suppose that $h_\ell < k-2$. This implies that $\boldsymbol{h} = (h_1,h_2,\ldots,h_\ell) \in \{1,2,\ldots,k-3\}^\ell$, where $h_1 < h_2 < \cdots < h_\ell$. By (8.6.1), we see that the set $\mathcal{D}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})$ can be partitioned as $\mathcal{D}_{n,k}(\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}) = C \cup D$, where $C = \{0,1,2,\ldots,k-1\} \setminus \{h_j : 1 \leq j \leq \ell\}$ and $D = \{k-1+t_j : 1 \leq j \leq \ell\}$. Note that $\{0,k-2,k-1\} \subset A$. Now working in a similar manner as in the case (i), we see that $\dim_{\mathbb{F}_q}(\mathscr{T}_{n,k}(\alpha,\mathbf{1},\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta})^2) \geq 2k$.

From this and by applying Theorem 8.6.1, the desired result follows. □

Remark 8.6.2. *One can easily observe, in view of Example 1.6 of Randriambololona [85], that the above theorem also holds when $m = 1$. So it gives rise to new classes of linear TRS codes with ℓ twists, which are not equivalent to linear RS codes.*

In the following section, we will present a perfect threshold secret-sharing scheme based on a class of additive MDS codes whose dual codes are also MDS. We will show that this scheme can detect cheating, identify a certain number of cheaters among the participants and recover the secret correctly.

8.7 A perfect threshold secret-sharing scheme based on additive MDS codes, whose dual codes are also MDS

A secret-sharing scheme is a method to share a secret among a set of participants. Let $\mathcal{P} = \{P_1,P_2,\ldots,P_n\}$ be a set of n participants, and let $\boldsymbol{s}$ be a secret that the dealer wants to share. The dealer assigns each participant P_i some partial information $\boldsymbol{s}_i$ (called the share) about the secret $\boldsymbol{s}$, where $1 \leq i \leq n$. The shares are distributed in a secret manner so that no participant knows any other participant's share. Further, a set of participants $\mathcal{B} = \{P_{j_1}, P_{j_2}, \ldots, P_{j_\ell}\}$ is called a qualified subset of $\mathcal{P}$ if the combiner can determine the secret by combining the shares $\boldsymbol{s}_{j_1}, \boldsymbol{s}_{j_2}, \ldots, \boldsymbol{s}_{j_\ell}$ of the participants in $\mathcal{B}$, where $1 \leq j_1 < j_2 < \cdots < j_\ell \leq n$. The collection of all qualified subsets of $\mathcal{P}$ is called the access structure of the secret-sharing scheme.

Let ω and n be positive integers satisfying $1 \leq \omega \leq n$. An (ω, n)-threshold secret-sharing scheme is a scheme to share a secret $\boldsymbol{s}$ among a set of n participants in such a way that any ω or more than ω participants can determine the secret by polling their shares, but no group of $\omega - 1$ or fewer participants can do so. Further, an (ω, n)-threshold secret-sharing scheme is said to be perfect if no information about the secret can be determined by combining shares of $\omega - 1$ or fewer participants. A perfect (ω, n)-threshold secret-sharing scheme is said to be an ideal (ω, n)-threshold scheme if $|K| = |S_1| = \cdots = |S_n|$, where K is the set of all secrets and S_i is the set of all shares of the i-th participant P_i for $1 \leq i \leq n$. Pieprzyk and Zhang [82] designed an ideal threshold secret-sharing scheme based on linear MDS codes over finite fields. Below, we will extend this construction and present a perfect threshold secret-sharing scheme based on additive MDS codes.

Secret-sharing scheme (A). *Let n, k and $m \geq 2$ be integers such that $1 \leq k \leq nm$ and m divides k. Let us write $k = m\delta$ for some $1 \leq \delta \leq n$. Let $\mathcal{C}$ be an additive MDS code of length $n+1$ and dimension k over $\mathbb{F}_{q^m}$ with a generator matrix $\mathcal{G}' = \begin{bmatrix} \boldsymbol{g}_0 & \boldsymbol{g}_1 & \cdots & \boldsymbol{g}_n \end{bmatrix}$, where $\boldsymbol{g}_i$ denotes the i-th column of the matrix $\mathcal{G}'$ for $0 \leq i \leq n$, (here the columns of $\mathcal{G}'$ are indexed by $0, 1, 2, \ldots, n$). Let $\sigma_0, \sigma_1, \ldots, \sigma_n$ be permutations of $\mathbb{F}_{q^m}$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ be the set of n participants. The dealer chooses a non-zero vector $v = (v_1, v_2, \ldots, v_k) \in \mathbb{F}_q^k$ and computes the word $(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n) \in \mathbb{F}_{q^m}^{n+1}$ as*

$$(\boldsymbol{s}_0, \boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n) = v\mathcal{G}'.$$

The dealer further computes the word $(\widetilde{\boldsymbol{s}}_0, \widetilde{\boldsymbol{s}}_1, \widetilde{\boldsymbol{s}}_2, \ldots, \widetilde{\boldsymbol{s}}_n) \in \mathbb{F}_{q^m}^{n+1}$ using the relation

$$(\widetilde{\boldsymbol{s}}_0, \widetilde{\boldsymbol{s}}_1, \widetilde{\boldsymbol{s}}_2, \ldots, \widetilde{\boldsymbol{s}}_n) = (\sigma_0(\boldsymbol{s}_0), \sigma_1(\boldsymbol{s}_1), \sigma_2(\boldsymbol{s}_2), \ldots, \sigma_n(\boldsymbol{s}_n)).$$

Define $\widetilde{\boldsymbol{s}}_0 \in \mathbb{F}_{q^m}$ to be the secret corresponding to the shares $\widetilde{\boldsymbol{s}}_1, \widetilde{\boldsymbol{s}}_2, \ldots, \widetilde{\boldsymbol{s}}_n$. The *dealer next assigns the share $\widetilde{\boldsymbol{s}}_i$ to the participant P_i for $1 \leq i \leq n$. Here we assume that the combiner knows the matrix $\mathcal{G}'$ and the permutations $\sigma_0, \sigma_1, \ldots, \sigma_n$, but the participants have no information about the matrix $\mathcal{G}'$ and the permutations $\sigma_0, \sigma_1, \ldots, \sigma_n$.*

In the following theorem, we show that the secret-sharing scheme (A) is a perfect (δ, n)-threshold scheme.

Theorem 8.7.1. *The secret-sharing scheme (A) is a perfect (δ, n)-threshold scheme.*

Proof. To prove the result, we note that m divides k, so by Theorem 8.3.3, the dual code $\mathcal{C}^{\perp}$ is also an additive MDS $[n+1, (n+1)m-k, \delta+1]$-code over $\mathbb{F}_{q^m}$ with a parity check matrix $\mathcal{G}'$. We next observe that any δ columns of the matrix $\mathcal{G}'$ are linearly independent over $\mathbb{F}_{q^m}$. Now let $\mathcal{B} = \{P_{j_1}, P_{j_2}, \ldots, P_{j_\ell}\}$ be a set of ℓ participants, who submit their shares $\widetilde{\boldsymbol{s}}_{j_1}, \widetilde{\boldsymbol{s}}_{j_2}, \ldots, \widetilde{\boldsymbol{s}}_{j_\ell}$ to the combiner, where $1 \leq j_1 < j_2 < \cdots < j_\ell \leq n$. Here we assert the following:

(i) When $\ell \geq \delta$, the combiner can determine the secret $\widetilde{\boldsymbol{s}}_0$ by combining the shares of the participants in $\mathcal{B}$.

(ii) When $\ell < \delta$, the combiner can obtain no information about the secret.

(i) Let us first assume that $\ell \geq \delta$. Here, we will show that the combiner can determine the secret $\widetilde{\boldsymbol{s}}_0$ uniquely. We recall that the combiner knows the permutations $\sigma_0, \sigma_1, \ldots, \sigma_n$ and the matrix $\mathcal{G}'$. Thus the combiner first determines the shares $\boldsymbol{s}_{j_1}$, $\boldsymbol{s}_{j_2}, \ldots, \boldsymbol{s}_{j_\ell}$ using the relation

$$(\widetilde{\boldsymbol{s}}_{j_1}, \widetilde{\boldsymbol{s}}_{j_2}, \ldots, \widetilde{\boldsymbol{s}}_{j_\ell}) = (\sigma_{j_1}(\boldsymbol{s}_{j_1}), \sigma_{j_2}(\boldsymbol{s}_{j_2}), \ldots, \sigma_{j_\ell}(\boldsymbol{s}_{j_\ell})).$$

Next, without any loss of generality, the combiner considers the following matrix equation in the unknown $y = (y_1, y_2, \ldots, y_k) \in \mathbb{F}_q^k$:

$$(\boldsymbol{s}_{j_1}, \boldsymbol{s}_{j_2}, \ldots, \boldsymbol{s}_{j_\delta}) = y \begin{bmatrix} \boldsymbol{g}_{j_1} & \boldsymbol{g}_{j_2} & \cdots & \boldsymbol{g}_{j_\delta} \end{bmatrix}. \qquad (8.7.1)$$

Let $g_{i,b}$ denote the (i,b)-th entry of the matrix $\mathcal{G}'$ for $1 \leq i \leq k$ and $0 \leq b \leq n$. Choose a basis $\{\beta_1, \beta_2 \ldots, \beta_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, and write $\boldsymbol{s}_{j_a} = \sum\limits_{i=1}^{m} s_{j_a,i}\beta_i$

and $g_{c,j_a} = \sum_{i=1}^{m} g_{c,j_a}^{(i)}\beta_i$, where $s_{j_a,1}, s_{j_a,2}, \ldots, s_{j_a,m}, g_{c,j_a}^{(1)}, g_{c,j_a}^{(2)}, \ldots, g_{c,j_a}^{(m)} \in \mathbb{F}_q$ for $1 \leq c \leq k$ and $1 \leq a \leq \delta$. It is easy to observe that the matrix equation (8.7.1) is equivalent to the following matrix equation in the unknown $y = (y_1, y_2, \ldots, y_k) \in \mathbb{F}_q^k$:

$$(s_{j_1,1}, s_{j_1,2}, \ldots, s_{j_1,m}, s_{j_2,1}, s_{j_2,2}, \ldots, s_{j_2,m}, \ldots, s_{j_\delta,1}, s_{j_\delta,2}, \ldots, s_{j_\delta,m}) = yU', \tag{8.7.2}$$

where

$$U' = \begin{bmatrix} g_{1,j_1}^{(1)} & g_{1,j_1}^{(2)} & \cdots & g_{1,j_1}^{(m)} & g_{1,j_2}^{(1)} & g_{1,j_2}^{(2)} & \cdots & g_{1,j_2}^{(m)} & \cdots & g_{1,j_\delta}^{(1)} & g_{1,j_\delta}^{(2)} & \cdots & g_{1,j_\delta}^{(m)} \\ g_{2,j_1}^{(1)} & g_{2,j_1}^{(2)} & \cdots & g_{2,j_1}^{(m)} & g_{2,j_2}^{(1)} & g_{2,j_2}^{(2)} & \cdots & g_{2,j_2}^{(m)} & \cdots & g_{2,j_\delta}^{(1)} & g_{2,j_\delta}^{(2)} & \cdots & g_{2,j_\delta}^{(m)} \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ g_{k,j_1}^{(1)} & g_{k,j_1}^{(2)} & \cdots & g_{k,j_1}^{(m)} & g_{k,j_2}^{(1)} & g_{k,j_2}^{(2)} & \cdots & g_{k,j_2}^{(m)} & \cdots & g_{k,j_\delta}^{(1)} & g_{k,j_\delta}^{(2)} & \cdots & g_{k,j_\delta}^{(m)} \end{bmatrix}.$$

Since the columns of the matrix $\begin{bmatrix} \boldsymbol{g}_{j_1} \; \boldsymbol{g}_{j_2} \; \cdots \; \boldsymbol{g}_{j_\delta} \end{bmatrix}$ are linearly independent over $\mathbb{F}_{q^m}$, the rows of the matrix $\begin{bmatrix} \boldsymbol{g}_{j_1} \; \boldsymbol{g}_{j_2} \; \cdots \; \boldsymbol{g}_{j_\delta} \end{bmatrix}$ are linearly independent over $\mathbb{F}_q$. This implies that the rows of the matrix U' are linearly independent over $\mathbb{F}_q$, which further implies that the matrix U' is invertible. This implies that there exists a unique $y = (y_1, y_2, \ldots, y_k) \in \mathbb{F}_q^k$ satisfying the equation (8.7.2), and hence the equation (8.7.1). Further, the combiner computes $\boldsymbol{s}_0 = y_1 g_{1,0} + y_2 g_{2,0} + \cdots + y_k g_{k,0}$ and determines the secret $\widetilde{\boldsymbol{s}}_0 = \sigma_0(\boldsymbol{s}_0)$.

(ii) Next, let us assume that $\ell < \delta$. Here, we will show that the combiner cannot determine any information about the secret. Knowing the permutations $\sigma_0, \sigma_1, \ldots, \sigma_n$, the combiner determines $\boldsymbol{s}_{j_1}$, $\boldsymbol{s}_{j_2}, \ldots, \boldsymbol{s}_{j_\ell}$ using the relation

$$(\widetilde{\boldsymbol{s}}_{j_1}, \widetilde{\boldsymbol{s}}_{j_2}, \ldots, \widetilde{\boldsymbol{s}}_{j_\ell}) = (\sigma_{j_1}(\boldsymbol{s}_{j_1}), \sigma_{j_2}(\boldsymbol{s}_{j_2}), \ldots, \sigma_{j_\ell}(\boldsymbol{s}_{j_\ell})).$$

Now working as in case (i), we see that for all $z \in \mathbb{F}_{q^m}$, there exists $u' = (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^k$ satisfying matrix equation

$$(z, \boldsymbol{s}_{j_1}, \boldsymbol{s}_{j_2}, \ldots, \boldsymbol{s}_{j_\ell}) = u' \begin{bmatrix} \boldsymbol{g}_0 \; \boldsymbol{g}_{j_1} \; \boldsymbol{g}_{j_2} \; \cdots \; \boldsymbol{g}_{j_\ell} \end{bmatrix}. \tag{8.7.3}$$

That is, the secret can be any element of $\mathbb{F}_{q^m}$ with equal probability. Thus, the combiner can determine no information about the secret.

This proves our assertion. □

The following theorem shows that the secret-sharing scheme (A) can detect cheating, identify a certain number of cheaters among the participants and recover the secret correctly.

Theorem 8.7.2. *Assume that a secret $\widetilde{\boldsymbol{s}}_0 \in \mathbb{F}_{q^m}$ is shared using the secret-sharing scheme (A). Let $\mathcal{B} = \{P_{j_1}, P_{j_2}, \ldots, P_{j_\ell}\}$ be a set of ℓ ($\geq \delta$) participants, where $1 \leq j_1 < j_2 < \cdots < j_\ell \leq n$ and the participant P_{j_i} is assigned the share $\widetilde{\boldsymbol{s}}_{j_i}$. Suppose that the participant P_{j_i} modifies its share $\widetilde{\boldsymbol{s}}_{j_i}$ to $\widetilde{\boldsymbol{s}}_{j_i} + \epsilon_i$, where $\epsilon_i \in \mathbb{F}_{q^m}$ for $1 \leq i \leq \ell$, (here the participant P_{j_i} is honest if $\epsilon_i = 0$, otherwise he cheats). Let $\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_\ell)$. Then the following hold.*

(a) If $w_H(\epsilon) \leq \ell - \delta$, then the combiner can detect that some cheating has happened.

(b) If $w_H(\epsilon) \leq \left\lfloor \frac{\ell-\delta}{2} \right\rfloor$, then the combiner can identify the cheaters who submitted incorrect shares and determine the secret correctly.

Proof. Since the participant P_{j_i} modifies its share $\widetilde{\boldsymbol{s}}_{j_i}$ to $\widetilde{\boldsymbol{s}}_{j_i} + \epsilon_i$, the combiner will receive the vector $\boldsymbol{s}' = (\widetilde{\boldsymbol{s}}_{j_1} + \epsilon_1, \widetilde{\boldsymbol{s}}_{j_2} + \epsilon_2, \ldots, \widetilde{\boldsymbol{s}}_{j_\ell} + \epsilon_\ell)$ instead of the vector $\boldsymbol{s} = (\widetilde{\boldsymbol{s}}_{j_1}, \widetilde{\boldsymbol{s}}_{j_2}, \ldots, \widetilde{\boldsymbol{s}}_{j_\ell})$. Now let us consider the set

$$\mathcal{D} = \left\{ \left(\sigma_{j_1}(\boldsymbol{c}_{j_1}), \sigma_{j_2}(\boldsymbol{c}_{j_2}), \ldots, \sigma_{j_\ell}(\boldsymbol{c}_{j_\ell})\right) : (\boldsymbol{c}_{j_1}, \boldsymbol{c}_{j_2}, \ldots, \boldsymbol{c}_{j_\ell}) = v\mathcal{G}'' \text{ for some } v \in \mathbb{F}_q^k \right\},$$

where $\mathcal{G}'' = \begin{bmatrix} \boldsymbol{g}_{j_1} & \boldsymbol{g}_{j_2} & \cdots & \boldsymbol{g}_{j_\ell} \end{bmatrix}$. It is easy to observe that the cardinality of the set $\mathcal{D}$ is q^k and the Hamming distance between any two distinct elements of $\mathcal{D}$ is at least $\ell - \delta + 1$.

(a) When $w_H(\epsilon) \leq \ell - \delta$, we see that $\epsilon = (0, 0, \ldots, 0)$ (*i.e.,* no cheating has happened) if and only if $\boldsymbol{s}' \in \mathcal{D}$. From this, part (a) follows immediately.

(b) When $w_H(\epsilon) \leq \left\lfloor \frac{\ell-\delta}{2} \right\rfloor$, working as in Theorem 4 of Pieprzyk and Zhang [82], we get the desired result.

□

We note that the secret-sharing scheme (A) need not be an ideal scheme, as $|K| = |S_1| = |S_2| = \cdots = |S_n|$ need not hold in general. In the following theorem, we identify a class of additive MDS codes based on which the secret-sharing scheme (A) is an ideal (δ, n)-threshold scheme.

Theorem 8.7.3. *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{n+1}) \in \mathbb{F}_{q^m}^{n+1}$, where no two elements among $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ form a conjugate pair over $\mathbb{F}_q$ and each α_i has exactly m distinct conjugates over $\mathbb{F}_q$. Let $k = m\delta$, where $1 \leq \delta \leq n$. Then the secret sharing scheme (A) based on the additive code $\mathcal{ARS}_{n+1,k}(\alpha, \mathbf{1})$ is an ideal (δ, n)-threshold scheme.*

Proof. To prove this result, we see, by Corollary 8.4.1 and Theorem 8.4.3, that both the additive code $\mathcal{ARS}_{n+1,k}(\alpha, \mathbf{1})$ and its dual code $\mathcal{ARS}_{n+1,k}(\alpha, \mathbf{1})^{\perp}$ are MDS. This, by Theorems 8.7.1 and 8.7.2, implies that the secret-sharing scheme (A) corresponding to the additive code $\mathcal{ARS}_{n+1,k}(\alpha, \mathbf{1})$ is a perfect (δ, n)-threshold scheme. Further, for $1 \leq i \leq n+1$, we observe that $\{1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{m-1}\}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. From this, we observe that the set K of all secrets and the set S_i of all shares of the i-th participant P_i for $1 \leq i \leq n$ are given by

$$K = S_1 = S_2 = \cdots = S_n = \mathbb{F}_{q^m},$$

which implies that the secret-sharing scheme (A) corresponding to the additive code $\mathcal{ARS}_{n+1,k}(\alpha, \mathbf{1})$ is an ideal (δ, n)-threshold scheme. □

9

Conclusion and future work

In this thesis, all self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings of odd characteristic are counted. As special cases of this work, all self-orthogonal and self-dual codes over quasi-Galois rings and Galois rings of odd characteristic are also enumerated. However, it is observed that this enumeration technique can not be extended to count all self-orthogonal (*resp.* self-dual) codes over quasi-Galois rings and Galois rings of even characteristic. This enumeration technique is further modified to count all self-orthogonal and self-dual codes of an arbitrary length over quasi-Galois and Galois rings of even characteristic. Besides this, all σ-LCD codes of an arbitrary length over finite commutative chain rings are enumerated. It is further shown that the class of σ-LCD codes over finite commutative chain rings is asymptotically good and that every free linear code over a finite commutative chain ring is equivalent to a σ-LCD code when the residue field of the chain ring has order at least 5. All inequivalent σ-LCD codes of length n, rank k and Hamming distance d over a finite commutative chain ring are obtained for

$k \in \{1, n-1\}$ and $1 \leq d \leq n$. Below, we list some interesting open problems in this direction:

- It would be interesting to count all self-orthogonal and self-dual codes over arbitrary finite commutative chain rings of even characteristic.
- Another interesting problem would be to classify self-orthogonal and self-dual codes over an arbitrary finite commutative chain ring up to monomial equivalence.
- It would be interesting to explicitly determine all inequivalent σ-LCD codes of length n, rank k and Hamming distance d over a finite commutative chain ring when $2 \leq k \leq n-2$ and $1 \leq d \leq n$.
- It would be interesting to see whether the classes of self-orthogonal and self-dual codes over finite commutative chain rings are asymptotically good.

Furthermore, additive codes over finite commutative chain rings and their dual codes with respect to the ordinary trace bilinear form are studied in the Galois additivity case. Necessary and sufficient conditions are derived under which an additive code over a finite commutative chain ring is (i) self-orthogonal, (ii) self-dual, and (iii) an additive code with complementary dual (or an ACD code). All additive self-orthogonal and self-dual codes of an arbitrary length over finite commutative chain rings are counted in certain special cases. All ACD codes of an arbitrary length over finite commutative chain rings are also enumerated. It is shown that a free additive code over a finite commutative chain ring is a maximum distance separable code (or an MDS code) if and only if its Torsion code is an additive MDS code. This motivated us to introduce and study two new classes of additive codes over finite fields, *viz.* additive generalized Reed-Solomon (additive GRS) codes and additive generalized twisted Reed-Solomon (additive GTRS) codes, which are extensions of linear GRS codes and linear GTRS codes, respectively. Unlike linear GRS codes, it is noted that additive GRS codes are not MDS codes in general. Several new classes of additive MDS and almost MDS codes are identified within the families of additive GRS and GTRS codes. It is also noted that, unlike linear codes, the dual code of an additive MDS code need not be an additive MDS code.

Several classes of additive MDS codes whose dual codes are also MDS are identified within the families of additive GRS and GTRS codes. Constructions of additive MDS self-orthogonal, self-dual and ACD codes over finite fields are provided through additive GRS and GTRS codes. Several classes of additive TRS codes that are not monomially equivalent to additive RS codes are identified. Based on additive MDS codes whose dual codes are also MDS, a perfect threshold secret-sharing scheme that can detect cheating, identify a certain number of cheaters among the participants, and correctly recover the secret, is also provided. Below we state some interesting research questions in this direction.

- It would be interesting to identify new classes of MDS codes within the families of additive GRS and additive GTRS codes.

- Another interesting problem would be to identify new classes of additive MDS GRS (*resp.* additive MDS GTRS) codes whose dual codes are also additive MDS GRS (*resp.* additive MDS GTRS) codes.

- Ketkar *et al.* [61, Th. 15] showed that there exists an additive MDS self-orthogonal code of length n and dimension $2(d-1)$ over $\mathbb{F}_{q^2}$ with respect to the Hermitian trace bilinear form if and only if there exists an $[[n, n-2(d-1), d]]_q$ quantum stabilizer MDS code. Thus, another interesting line of research would be to construct additive MDS self-orthogonal and self-dual codes with respect to the Hermitian trace bilinear form through additive GRS and GTRS codes.

- Another interesting problem would be to provide new methods to construct additive MDS self-orthogonal, self-dual, and ACD codes over finite fields.

Bibliography

[1] Alabiad, S. and Alkhamees, Y.: On automorphism groups of finite chain rings, *Symmetry* 13(4), pp. 681-692 (2021).

[2] Alkhamees, Y.: The determination of the group of automorphisms of a finite chain ring of characteristic p, *Q. J. Math.* 42(1), pp. 387-391 (1991).

[3] Araya, M. and Harada, M.: On the classification of linear complementary dual codes, *Discrete Math.* 342(1), pp. 270-278 (2019).

[4] Ashikhmin, A. and Knill, E.: Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory* 47(7), pp. 3065-3072 (2001).

[5] Bachoc, C. and Gaborit, P.: Designs and self-dual codes with long shadows, *J. Combin. Theory* 105A, pp. 15-34 (2004).

[6] B*á*gio, D., Dias, I. and Paques, A.: On self-dual normal bases, *Indag. Math.* 17(1), pp. 1-11 (2006).

[7] Ball, S., Gamboa, G. and Lavrauw, M.: On additive MDS codes over small fields, *Adv. Math. Commun.* 17(4), pp. 828-844 (2023).

[8] Bannai, E., Dougherty, S. T., Harada, M. and Oura, M.: Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Inform. Theory* 45(4), pp. 1194-1205 (1999).

[9] Beelen, P., Bossert, M., Puchinger, S. and Rosenkilde, J.: Structural properties of twisted Reed-Solomon codes with applications to cryptography, *Proc. IEEE Int. Symp. Inf. Theory*, pp. 946-950 (2018).

[10] Beelen, P., Puchinger, S. and Rosenkilde, J.: Twisted Reed-Solomon codes, *IEEE Trans. Inform. Theory* 68(5), pp. 3047-3061 (2022).

[11] Beelen, P., Puchinger, S. and Rosenkilde né Nielsen, J.: Twisted Reed-Solomon codes, *Proc. IEEE Int. Symp. Inf. Theory*, pp. 336-340 (2017).

[12] Betty, R. A. and Munemasa, A.: Mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$, *J. Combinator. Inform. Syst. Sci.* 34, pp. 51-66 (2009).

[13] Betty, R. A., Nemenzo, F. and Vasquez, T. L.: Mass formula for self-dual codes over $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, *J. Appl. Math. Comput.* 57, pp. 523-546 (2018).

[14] Bhowmick, S., Tabue, A. F., Moro, E. M., Bandi, R. and Bagchi, S.: Do non-free LCD codes over finite commutative Frobenius ring exist?, *Des. Codes Cryptogr.* 88(5), pp. 825-840 (2020).

[15] Bierbrauer, J. and Edel, Y.: Quantum twisted codes, *J. Comb. Des.* 8(3), pp. 174-188 (2000).

[16] Bini, G. and Flamini, F.: *Finite commutative rings and their applications*, in: Kluwer Int. Ser. Eng. Comp. Sci., 680, Kluwer Academic Publ., Boston, MA (2002).

[17] Bouyuklieva, S. and Varbanov, Z.: Some connections between self-dual codes, combinatorial designs and secret sharing schemes, *Adv. Math. Commun.* 5(2), pp. 191-198 (2011).

[18] Bringer, J., Carlet, C., Chabanne, H., Guilley, S. and Maghrebi, H.: Orthogonal direct sum masking, A Smartcard Friendly Computation Paradigm in a code, with builtin protection against side-channel and fault attacks, *Proceedings of WISTP 2014, Lecture Notes in Computer Science 8501*, pp. 40-56 (2014).

[19] Brualdi, R. A.: *Introductory Combinatorics*, Prentice Hall, New Jersey (2009).

[20] Calderbank, A. R., Hammons, A. R., Kumar, P. V., Sloane, N. J. A. and Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* 40(2), pp. 301-319 (1994).

[21] Calderbank, A. R., Hammons, A. R., Kumar, P. V., Sloane, N. J. A. and Solé, P.: A linear construction for certain Kerdock and Preparata codes, *Bull. Amer. Math. Soc.* 29(2), pp. 218-222 (1993).

[22] 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).

[23] Cao, Y., Gao, J., Fu, F. W. and Cao, Y.: Enumeration and construction of additive cyclic codes over Galois rings, *Discrete Math.* 338(6), pp. 922-937 (2015).

[24] Carlet, C., Daif, A., Danger, J. L., Guilley, S., Najm, Z., Ngo, X. T., Porteboeuf, T. and Tavernier, C.: Optimized linear complementary codes implementation for hardware Trojan prevention, *Proceedings of the 22nd ECCTD*, pp. 1-4 (2015).

[25] Carlet, C. and Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks, *Adv. Math. Commun.* 10(1), pp. 131-150 (2016).

[26] Carlet, C., Güneri, C., Mesnager, S. and Özbudak, F.: Codes suitable for both side channel and fault injection attacks, *Proceedings of WAIFI, Bergen,* (2018).

[27] Carlet, C., Mesnager, S., Tang, C. and Qi, Y.: New characterization and parametrization of LCD codes, *IEEE Trans. Inform. Theory* 65(1), pp. 39-49 (2018).

[28] Carlet, C., Mesnager, S., Tang, C. and Qi, Y.: Euclidean and Hermitian LCD MDS codes, *Des. Codes Cryptogr.* 86, pp. 2605-2618 (2018).

[29] Carlet, C., Mesnager, S., Tang, C., Qi, Y., and Pellikaan, R.: Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$, *IEEE Trans. Inform. Theory* 64(4), pp. 3010-3017 (2018).

[30] Cascudo, I., Cramer, R., Mirandola, D. and Zémor, G.: Squares of random linear codes, *IEEE Trans. Inform. Theory* 61(3), pp. 1159-1173 (2015).

[31] Choi, W.: Mass formula of self-dual codes over Galois rings $GR(p^2, 2)$, *Korean J. Math.* 24(4), pp. 751–764 (2016).

[32] Choi, W. H., Güneri, C., Kim, J. L. and Özbudak, F.: Theory of additive complementary dual codes, constructions and computations, *Finite Fields Appl.* 92, 102303 (2023).

[33] Cohen, S. D.: Primitive elements and polynomials with arbitrary trace, *Discrete Math.* 83(1), pp. 1-7 (1990).

[34] Cramer, R., Damgård, I. B. and Nielsen, J. B.: *Secure multiparty computation and secret sharing*, Cambridge Univ. Press, Cambridge, New York, USA, (2015).

[35] Dau, S. H., Song, W., Dong, Z. and Yuen, C.: Balanced sparsest generator matrices for MDS codes, *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1889-1893 (2013).

[36] Dinh, H. Q. and López-Permouth, S. R.: Cyclic and negacyclic codes over finite chain rings, *IEEE Trans. Inform. Theory* 50(8), pp. 1728-1744 (2004).

[37] Dougherty, S. T., Gulliver, T. A. and Harada, M.: Type II self-dual codes over finite rings and even unimodular lattices, *J. Algebraic Comb.* 9(3), pp. 233-250 (1999).

[38] Dougherty, S. T., Kim, J. L. and Liu, H.: Constructions of self-dual codes over finite commutative chain rings, *Int. J. Inf. Coding Theory* 1(2), pp. 171-190 (2010).

[39] Dougherty, S.T., Mesnager, S. and Solé, P.: Secret-sharing schemes based on self-dual codes, *IEEE Inform. Theory workshop*, pp. 338-342 (2008).

[40] Dummit, D. S. and Foote, R. M.: *Abstract algebra (Vol. 3)*, Wiley, Hoboken, USA (2004).

[41] Elman, R., Karpenko, N. and Merkurjev, A.: *The Algebraic and Geometric Theory of Quadratic forms*, American Mathematical Society (2008).

[42] Fan, Y. and Zhang, L.: Galois self-dual constacyclic codes, *Des. Codes Cryptogr.* 84, pp. 473-492, (2017).

[43] Fang, W. and Fu, F. W.: New constructions of MDS Euclidean self-dual codes from GRS codes and extended GRS codes, *IEEE Trans. Inform. Theory* 65(9), pp. 5574-5579 (2019).

[44] Gaborit, P.: Construction of new extremal unimodular lattices, *European J. Combin.* 28A, pp. 549–564 (2004).

[45] Gaborit, P.: Mass formula for self-dual codes over $\mathbb{Z}_4$ and $\mathbb{F}_q + u\mathbb{F}_q$ rings, *IEEE Trans. Inform. Theory* 42(4), pp. 1222-1228 (1996).

[46] Gallian, J. A.: *Contemporary abstract algebra*, Brooks/Cole Cengage Learning, Boston, USA (2013).

[47] Galvez, L.E., Betty, R.A. and Nemenzo, F.: Self-orthogonal codes over $\mathbb{F}_q + u\mathbb{F}_q$ and $\mathbb{F}_q + u\mathbb{F}_q + u^2\mathbb{F}_q$, *Eur. J. Pure Appl. Math.* 13(4), pp. 873-892 (2020).

[48] Glynn, D. G.: A condition for arcs and MDS codes, *Des. Codes Cryptogr.* 58, pp. 215-218 (2011).

[49] Grove, L.C.: *Classical groups and Geometric Algebra*, American Mathematical Society, Providence, Rhode Island (2008).

[50] Heng, Z., Li, C. and Wang, X.: Constructions of MDS, near MDS and almost MDS codes from cyclic subgroups of $\mathbb{F}_{q^2}^*$, *IEEE Trans. Inform. Theory* 68(12), pp. 7817-7831 (2022).

[51] Huang, D., Yue, Q. and Niu, Y.: MDS or NMDS LCD codes from twisted Reed-Solomon codes, *Cryptogr. Commun.* 15, pp. 221-237 (2023).

[52] 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).

[53] Huffman, W. C. and Pless, V.: *Fundamentals of error-correcting codes*, Cambridge Univ. Press, Cambridge, New York, USA (2003).

[54] Irwansyah, I.M.A., Barra, A. and Muchlis, A.: Self-dual normal basis of a Galois ring, *J. Math.,* 258187 (2014).

[55] Jin, L.: Construction of MDS codes with complementary duals, *IEEE Trans. Inform. Theory* 63(5), pp. 2843-2847 (2016).

[56] Jin, L. and Xing, C.: New MDS self-dual codes from generalized Reed-Solomon codes, *IEEE Trans. Inform. Theory* 63(3), pp. 1434-1438 (2016).

[57] Jin, L. and Xing, C.: Euclidean and Hermitian self-orthogonal algebraic geometry codes and their application to quantum codes, *IEEE Trans. Inform. Theory* 58(8), pp. 5484 - 5489 (2011).

[58] Jungnickel, D., Menezes, A. J. and Vanstone, S. A.: On the number of self-dual bases of $GF(q^m)$ over $GF(q)$, *Proc. Am. Math. Soc.* 109(1), pp. 23-29 (1990).

[59] Kaplansky, I.: Projective modules, *Ann. Math.* 68(2), pp. 372–377 (1958).

[60] Kennedy, G. T. and Pless, V.: On designs and formally self-dual codes, *Des. Codes Cryptogr.* 4(1), pp. 43–55 (1994).

[61] Ketkar, A., Klappenecker, A., Kumar, S. and Sarvepalli, P. K.: Nonbinary stabilizer codes over finite fields, *IEEE Trans. Inform. Theory* 52(11), pp. 4892-4914 (2006).

[62] Lidl, R. and Niederreiter, H.: *Introduction to finite fields and their applications*, Cambridge University Press, (1986).

[63] Ling, S. and Xing, C.: *Coding theory: A first course*, Cambridge Univ. Press, Cambridge, New York, USA (2004).

[64] Liu, X., Fan, Y. and Liu, H.: Galois LCD codes over finite fields, *Finite Fields Appl.* 49, pp. 227-242 (2018).

[65] Liu, H. and Liu, S.: Construction of MDS twisted Reed-Solomon codes and LCD MDS codes, *Des. Codes Cryptogr.* 89(9), pp. 2051-2065 (2021).

[66] Liu, X. and Liu, H.: σ-LCD codes over finite chain rings, *Des. Codes Cryptogr.* 88(4), pp. 727-746 (2020).

[67] Liu, X. and Liu, H.: LCD codes over finite chain rings, *Finite Fields Appl.* 34, pp. 1-19 (2015).

[68] Liu, Z. and Wang, J.: Linear complementary dual codes over rings, *Des. Codes Cryptogr.* 87, pp. 3077-3086 (2019).

[69] Liu, Z. and Wang, J.: Further results on Euclidean and Hermitian linear complementary dual codes, *Finite Fields Appl.* 59, pp. 104-133 (2019).

[70] MacWilliams, F. J. and Sloane, N. J. A.: *The theory of error-correcting codes*, North Holland Publishing Co. (1977).

[71] Mahmoudi, S. and Samei, K.: Additive codes over Galois rings, *Finite Fields Appl.* 56, pp. 332-350 (2019).

[72] Massey, J. L.: Linear codes with complementary duals, *Discrete Math.* 106, pp. 337-342 (1992).

[73] McDonald, B. R.: *Finite rings with identity*, New York, USA: Marcel Dekker (1974).

[74] Moro, E. M., Otal, K. and Özbudak, F.: Additive cyclic codes over finite commutative chain rings, *Discrete Math.* 314(7), pp. 1873-1884 (2018).

[75] Nagata, K., Nemenzo, F. and Wada, H.: Mass formula and structure of self-dual codes over $\mathbb{Z}_{2^s}$, *Des. Codes Cryptogr.* 67(3), pp. 293-316 (2013).

[76] Nagata, K., Nemenzo, F. and Wada, H.: The number of self-dual codes over $\mathbb{Z}_{p^3}$, *Des. Codes Cryptogr.* 50(3), pp. 291-303 (2009).

[77] Nagata, K., Nemenzo, F. and Wada, H.: Constructive algorithm of self-dual error correcting codes, *Proc. of 11th International Workshop on ACCT*, pp. 215-220 (2008).

[78] Nechaev, A. A.: *Finite rings with applications*, in Handbook of algebra 5, Amsterdam, The Netherlands: North Holland, pp. 213-320 (2008).

[79] Nechaev, A. A.: Kerdock code in a cyclic form, *Discrete Math. Appl.* 1(4), pp. 365-384 (1991).

[80] Norton, G. H. and Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring, *AAECC* 10(6), pp. 489-506 (2000).

[81] Norton, G. H. and Sălăgean, A.: On the Hamming distance of linear codes over a finite chain ring, *IEEE Trans. Inform. Theory* 46(3), pp. 1060-1067 (2000).

[82] Pieprzyk, J. and Zhang, X. M.: Ideal threshold schemes from MDS codes, *ICISC 2002: 5th International Conference Seoul, Korea*, pp. 253-263 (2003).

[83] Pless, V.: On the uniqueness of Golay codes, *J. Combin. Theory* 5, pp. 215-228 (1968).

[84] Rains, E. M. and Sloane, N. J. A.: The shadow theory of modular and unimodular lattices, *J. Number Theory* 73(2), pp. 359–389 (1998).

[85] Randriambololona, H.: On products and powers of linear codes under componentwise multiplication, *Algorithm. Arith. Geom. Cod. Theory* 637, pp. 3-78 (2015).

[86] Reed, I. S. and Solomon, G.: Polynomial codes over certain finite fields, *SIAM J. Appl. Math.* 8(2), pp. 300-304 (1960).

[87] Roth, R. M. and Lempel, A.: On MDS codes via Cauchy matrices, *IEEE Trans. Inform. Theory* 35(6), pp. 1314-1319 (1989).

[88] Samei, K. and Mahmoudi, S.: Singleton bounds for R-additive codes, *Adv. Math. Commun.* 12(1), pp. 107-114 (2018).

[89] Sendrier, N.: Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.* 285(1-3), pp. 345-347 (2004).

[90] Sendrier, N. and Simos, D. E.: The Hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography, *International Workshop on Post-Quantum Cryptography, Springer, Berlin, Heidelberg* (2013).

[91] Sharma, A. and Kaur, T.: Enumeration formulae for self-dual, self-orthogonal and complementary-dual quasi-cyclic codes over finite fields, *Cryptogr. Commun.* 10, pp. 401-435 (2018).

[92] Shi, M., Liu, N., Kim, J. L. and Solé, P.: Additive complementary dual codes over $\mathbb{F}_4$, *Des. Codes Cryptogr.* 91(1), pp. 1-12 (2022).

[93] Sidana, T. and Kashyap, N.: Entanglement-assisted quantum error-correcting codes over local Frobenius rings, *IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1064-1069 (2022).

[94] Singleton, R.: Maximum distance q-nary codes, *IEEE Trans. Inform. Theory* 10(2), pp. 116-118 (1964).

[95] Szymiczek, K.: *Bilinear Algebra: An introduction to the algebraic theory of quadratic forms*, Gordon and Breach Science Publishers, Amsterdam (1997).

[96] Tamo, I. and Barg, A.: A family of optimal locally recoverable codes, *IEEE Trans. Inform. Theory* 60(8), pp. 4661-4676 (2014).

[97] Tang, Y. and Farnoud, F.: Error-correcting codes for short tandem duplication and edit errors, *IEEE Trans. Inform. Theory* 68(2), pp. 871-880 (2021).

[98] Tang, Y., Lou, H. and Farnoud, F.: Error-correcting codes for short tandem duplications and at most p substitutions, *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1835-1840 (2021).

[99] Taylor, D. E.: *The Geometry of the Classical groups*, Sigma Series in Pure Mathematics, Vol. 9. Heldermann Verlag (1992).

[100] Vasquez, T. L. E. and Petalcorin, G. C.: Mass formula for self-dual codes over Galois rings $GR(p^3, r)$, *Eur. J. Pure Appl. Math.* 12(4), pp. 1701-1716 (2019).

[101] Wan, Z-X.: *Lectures on finite fields and Galois rings*, World scientific publishing company, Singapore (2003).

[102] Wood, J. A.: Witt's extension theorem for mod four valued quadratic forms, *Trans. Amer. Math. Soc.* 336(1), pp. 445-461 (1993).