New quantum codes, minimum distance bounds, and equivalence of codes

by

Reza Dastbasteh

M.Sc., Sabancı University, 2017
B.Sc., Shiraz University, 2014

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Doctor of Philosophy

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Summer 2023

Declaration of Committee

Name:	**Reza Dastbasteh**
Degree:	**Doctor of Philosophy**
Thesis title:	**New quantum codes, minimum distance bounds, and equivalence of codes**
Committee:	**Chair:** Ladislav Stacho Professor, Department of Mathematics
	Petr Lisoněk Supervisor Professor, Department of Mathematics
	Nathan Ilten Committee Member Associate Professor, Department of Mathematics
	Jonathan Jedwab Examiner Professor, Department of Mathematics
	Gary McGuire External Examiner Professor, Department of Mathematics University College Dublin

Abstract

Quantum error-correcting codes (quantum codes) are applied to protect quantum information from errors caused by noise (decoherence) on the quantum channel in a way that is similar to that of classical error-correcting codes. The stabilizer construction is currently the most successful and widely used technique for constructing binary quantum codes. We explore new frontiers beyond the stabilizer construction. Our approach enables integration of a broader class of classical codes into the mathematical framework of quantum stabilizer codes. Our construction is particularly well-suited to certain families of classical codes, including duadic codes and additive twisted codes. For duadic codes, we provide various modifications of our construction and develop new computational strategies to bound the minimum distance. This enabled us to extend the tables of good duadic codes to much larger block lengths.

The primary focus of this thesis is on additive twisted codes, which are highly structured but also technically much more difficult than the more common families of codes. They are widely referenced but have received relatively little development in previous studies. We discover new connections between twisted codes and linear cyclic codes and provide novel lower and upper bounds for the minimum distance of twisted codes. We show that classical tools such as the Hartmann-Tzeng minimum distance bound are applicable to twisted codes. This enabled us to discover five new infinite families and many other examples of record-breaking, and sometimes optimal, binary quantum codes.

Another important contribution is the development of new criteria for code equivalence within the families of linear cyclic, constacyclic, and twisted codes. We introduce novel sufficient conditions for code equivalence and classify all equivalent codes of certain lengths. We prove a recent conjecture on a necessary condition for the formula describing affine equivalence. For twisted codes, we use algebraic methods, such as group actions, to determine many codes with the same parameters. These results have practical implications, as they are useful for pruning the search for new good codes, and they enabled us to discover many new record-breaking linear and binary quantum codes.

Keywords: quantum code; minimum distance bound; equivalence of codes; cyclic code; constacyclic code; duadic code; additive code; dual-containing code; self-dual code

Dedication

To my compassionate wife, Zohreh,
my family, and
my best friend and mentor, Hamed.

Acknowledgements

I would like to acknowledge and thank my supervisor, Dr. Petr Lisoněk, for his patience, support, and guidance throughout the development of this thesis. I am very grateful to him for the wealth of academic advice and for reviewing and correcting my write-ups. I thank my Ph.D. examination committee, Dr. Gary McGuire, Dr. Jonathan Jedwab, and Dr. Nathan Ilten, for reading and examining my thesis. I would like to express my appreciation to Dr. Markus Grassl and Dr. Hiram H. Lopez for inviting me to conferences and many interesting discussions. I wish to thank Dr. Natalia Kouzniak for her constant support and kindness and for allowing me to be involved in her educational research. I am very thankful for the support and encouragement of my previous supervisors and mentors, Dr. Cem Güneri, Dr. Javad Haghighat, Dr. Mohammad Hassan Shirdareh Haghighi, and Dr. Habib Sharif.

This all would not have been possible without the encouragement, consistent love, and tireless support of my wife, parents, parents-in-law, brothers, and sisters. I would like to give special thanks to Payman for all the conversations, coffee breaks, and for his perseverance and kindness. Thanks to Sam and Stefan for many enjoyable conversations and various academic tips. A special thanks to Sepehr for his constant good company and memorable conversations.

I want to thank Sharon, Ahmad, Khalil, Kailyn, Narges, Parisa, Danielle, Ayoola, Dan, Mahsa, Jingzhou, Juan, MacKenzie, Garrett, Federico, Archit, Liam, Damara, Omid, Mahdieh, Akbar, Aliasghar, and Brandon, who have made my time at school more enjoyable. I would like to thank my best friends, Hamed, Farzad, Pouria, Rouzbeh, Ali, and many others who have helped, encouraged, and inspired me throughout my life. I would like to thank the Centre for Experimental and Constructive Mathematics (CECM) for its computational support and Magma license.

I am also grateful for the financial support in the form of research assistantships funded by NSERC, graduate fellowships from SFU, and the Mathematics Department's funding.

Table of Contents

List of Tables

List of Figures

List of Symbols

The list describes some symbols that are used in this thesis.

$\mathbb{F}_q$	finite field of q elements
$\mathbb{F}_q^*$	$\mathbb{F}_q \setminus \{0\}$
$\mathbb{Z}$	integers
$\mathbb{Z}/n\mathbb{Z}$	integers modulo n
$A \setminus B$	difference of sets
$\mathrm{wt}(x)$	weight of vector x (number of non-zero coordinates of x)
$d(C)$	minimum distance of linear or additive code C
$C^{\perp}$	Euclidean dual of C
$C^{\perp_h}$	Hermitian dual of C
$C^{\perp_t}$	trace dual of C
$[n, k, d]$	classical linear code of length n, dimension k, and minimum distance d
$(n, 2^k, d)$	classical quaternary additive code of length n, dimension k, and minimum distance d
$[\![n, k, d]\!]$	binary quantum code of length n, dimension k, and minimum distance d
$u \cdot v$	Euclidean inner product of u and v
$\langle u, v\rangle_h$	Hermitian inner product of u and v
$\langle u, v\rangle_s$	symplectic inner product of u and v
Tr_s^r	$\mathrm{Tr}_s^r : \mathbb{F}_{q^r} \to \mathbb{F}_{q^s}$ defined by $\mathrm{Tr}_s^r(x) = \displaystyle\sum_{i=0}^{\frac{r}{s}-1} x^{q^{is}}$, where $s \mid r$
Tr	$\mathrm{Tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ is the standard trace map defined by $\mathrm{Tr}(x) = \displaystyle\sum_{i=0}^{r-1} x^{q^i}$
ϕ_γ	$\mathbb{F}_2$-linear map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2^2$ defined by $\phi_\gamma(x) = (\mathrm{Tr}(x), \mathrm{Tr}(\gamma x))$ for some $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$
$\mathscr{C}_\gamma(A)$	additive twisted code with defining set A
$\mathrm{ord}_n(a)$	multiplicative order of a modulo n
$\langle v\vert$	Dirac notation of a row vector v
$\vert v\rangle$	Dirac notation of a column vector v
$\deg(f(x))$	degree of the polynomial $f(x)$
$\gcd(a, b)$	the greatest common divisor of integers a and b
μ_a	multiplier defined on $\mathbb{Z}/n\mathbb{Z}$ by $\mu_a(x) = (ax) \bmod n$

Chapter 1

Background

1.1 Introduction

The theory of error control codes (family of error correcting and error detecting codes) is a branch of mathematics and engineering that enables us to deliver digital data reliably over noisy communication channels. A landmark manuscript of Claude Shannon called “A mathematical theory of communication” [91] signified the beginning of coding theory. Since then, many families of error control codes and various error correction and detection schemes have been discovered [50, 75, 84]. One can safely say that the digital revolution was enabled by coding theory. In particular, it is impossible to remove channel noise from analogue signals completely. However, error control codes result in a much higher fidelity of digital signals.

Most digital information channels are not completely reliable because the transmitted data is frequently distorted in the presence of noise. Error control codes are applied to deal with this inevitable situation. Error control codes add some redundancy to a message in the form of extra data to enable the receiver to check the consistency of the delivered message (error detection) and also to recover the original data if it has been corrupted. Some well-known examples of digital communication channels that use error control codes are WiFi, the Internet, cellular telephones, storage devices, computers, satellites, and compact discs. A simple example of an error detection code used to facilitate our everyday shopping is illustrated in the next example.

Example 1.1.1 The Universal Product Code (UPC) is a 12-digit number represented by a bar code on many products. In other words, each UPC is a vector in $(\mathbb{Z}/10\mathbb{Z})^{12}$, where $\mathbb{Z}/10\mathbb{Z}$ is the ring of integers modulo 10. The UPC is used to employ a simple error-detection system to ensure reliability in the scanning of the barcodes. For each product, the first six digits of UPC determine the manufacturer identification number, the next five digits determine the product number, and the last digit is called a parity digit. Provided that the first eleven digits are respectively $u_1, u_2, \ldots, u_{11}$, then the parity digit u_{12} is determined in the way that

$$3(u_1 + u_3 + u_5 + u_7 + u_9 + u_{11}) + (u_2 + u_4 + u_6 + u_8 + u_{10} + u_{12}) \equiv 0 \pmod{10}. \quad (1.1.1)$$

For instance, a product with the manufacturer number 036000 and the product number 29145 has the parity digit 2. When a product with the UPC vector $u = (u_1, u_2, \dots, u_{12})$ is scanned, the scanner computes the value

$$s = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1) \cdot u \bmod 10. \quad (1.1.2)$$

If the parity condition $s \equiv 0 \pmod{10}$ does not hold, then the object will be re-scanned or its number will be entered by hand. Transposition errors are common when entering the numbers by hand. UPC can detect about 89% of transposition errors (when two neighboring digits are transposed).

The equation (1.1.1) is called a *parity check equation.* In general, a check equation is a common approach to verify the validity of a code vector, except that the number of check equations can be more than one, and the computations are not necessarily modulo 10. If the difference of two neighboring digits is a multiple of 5, then UPC is unable to detect the transposition error of these digits. This is because 5 is a zero divisor in $\mathbb{Z}/10\mathbb{Z}$. This is one of the reasons that a majority of error control codes are defined over finite fields. Moreover, most electronic devices operate in binary. This makes binary codes to be the most favourable class of error control codes for practical applications.

Two other error control codes with a similar structure are International Standard Book Number (ISBN) and Social Insurance Number (SIN). In contrast to the previously mentioned codes, some error control codes, such as cyclic redundancy check (CRC), quick response code (QR code), compact disc (CD), and error correcting code memory (ECC memory) can only be used by electronic devices. In practice, error correction schemes are especially important for many applications, such as when

- it is not possible to resend the message (for example when a disc is scratched, block cannot be reread in CD, or memory is damaged),
- there is no return channel to report an error (for example in broadcasting),
- the communication happens over interplanetary distances (for example in deep-space telecommunications).

It should be noted that error correcting codes are only tools, and a decoding algorithm is still needed to fix an error. On the other hand, error detection methods are mainly used when there is a fast return channel to report the occurrence of an error. Main applications of error detection are in the Internet, mobile phone, and data storage.

Linear codes over finite fields are the most studied class of error control codes. The rich algebraic structure of some linear codes provides a framework under which efficient encoding and decoding algorithms can be designed for data transmission. Although codes over rings or non-linear codes are used sparingly for practical applications, they can have better error control capacity than linear codes over finite fields. For instance, there exists a non-linear code consisting of 256 binary vectors of length 16, which is capable of detecting any 5 errors or less [72, Section 2.8, Theorem 32], while the best-known binary linear code with the same length and number of vectors is capable of detecting at most 4 errors [43]. Among all non-linear codes and codes over rings, the research on additive codes is attracting more attention due to their connection to quantum codes. We will discuss such codes in Section 1.7.

In the rest of this chapter, we introduce linear codes over finite fields and their properties, some well-known families of linear codes, and the connection between classical codes and binary quantum codes. This chapter is organized as follows. The preliminary concepts of linear codes are given in Section 1.2. Section 1.3 presents linear cyclic codes. Next, in Section 1.4, we give several minimum distance bounds for linear cyclic codes, including the Bose-Chaudhuri-Hocquenghem (BCH), Hartmann-Tzeng (HT), Roos, and a distance lower bound proposed by van Lint and Wilson. Section 1.5 presents another well-known family of linear codes, namely constacyclic codes. They are a generalization of linear cyclic codes. In Section 1.6, we recall the permutation, monomial, and isometric equivalence of linear codes as well as some known results about them. In Section 1.7, we introduce quantum stabilizer codes. In particular, we recall the mathematical formulation of binary quantum stabilizer codes and give several constructions of such codes that appeared in the literature. Finally, in Section 1.8, we give the summary of our new results and techniques of this thesis.

We facilitate reading the background material in Chapter 1 in shorter pieces for those readers who prefer that. In particular, the directed graph in Figure 1.1 shows which parts of Chapter 1 should be read before reading each of Chapters 2, 3, and 4 that contain our new results.

1.2 Basic concepts of linear codes

Let q be a prime power and n be a positive integer. Throughout this thesis, we will use the following notations. We denote the finite field of q elements by $\mathbb{F}_q$. An $[n, k]$ *linear code* C over $\mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ with dimension k. The field $\mathbb{F}_q$ is referred to as the *alphabet* of the code C. Linear codes over $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_4$ are called *binary*, *ternary* and *quaternary* codes, respectively. Let C be a linear code of length n. Each vector $(a_1, a_2, \ldots, a_n) \in C$ is called a *codeword*.

The most common way to represent a linear code is using a generator matrix or a parity check matrix. Let C be an $[n, k]$ linear code over $\mathbb{F}_q$. A $k \times n$ matrix whose rows

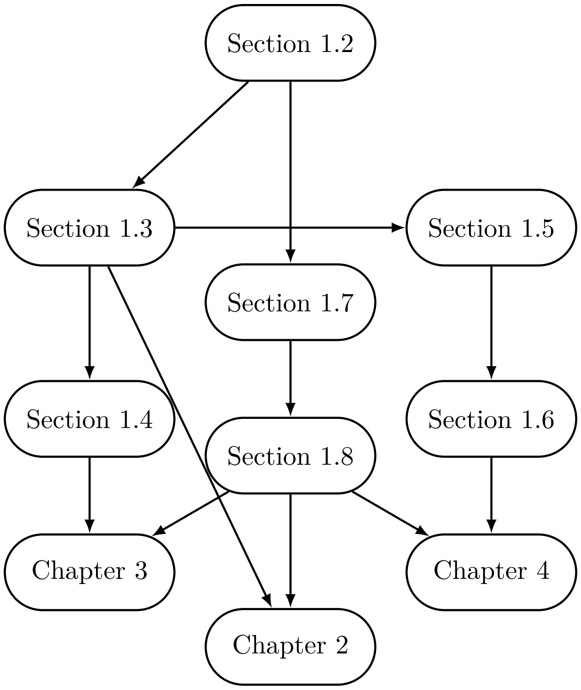

Figure 1.1: Dependency among background sections and new results.

form a basis for C is called a *generator matrix* of C. The code C can have many different generator matrices. A *parity check matrix* for C is an $(n-k)\times n$ matrix H over $\mathbb{F}_q$ such that $C=\{x\in\mathbb{F}_q^n : Hx^T=0\}$. In particular, we agree that all parity check matrices in this thesis will be full rank. A check matrix for the linear code C can also be defined over field extensions of $\mathbb{F}_q$ analogously. A matrix H' defined over $\mathbb{F}_{q^r}$ for some integer $r\geq 2$ such that $C=\{x\in\mathbb{F}_q^n : H'x^T=0\}$ is called a *generalized parity check* matrix. In this thesis, the generalized parity check matrices will be used to describe the family of linear cyclic codes and determine minimum distance lower bounds for them.

Let V be a finite-dimensional vector space over $\mathbb{F}_q$. An *inner product* $\langle,\rangle$ is a function $V\times V\to\mathbb{F}_q$ satisfying the following properties for each $x,y,z\in V$ and $a\in\mathbb{F}_q$:

1. $\langle ax+y,z\rangle = a\langle x,z\rangle+\langle y,z\rangle$.

2. $\langle x,y\rangle=\langle y,x\rangle$.

The space V together with the inner product $\langle,\rangle$ is called an *inner product space.* Recall that the *Euclidean inner product* of vectors $x=(x_1,x_2,\ldots,x_n)$ and $y=(y_1,y_2,\ldots,y_n)$ is defined by

$$x\cdot y=\sum_{i=1}^n x_iy_i.$$

The *dual* of an $[n,k]$ linear code C over $\mathbb{F}_q$ with respect to the Euclidean inner product is defined by

$$C^\perp=\{x\in\mathbb{F}_q^n : x\cdot c=0 \text{ for all } c\in C\}. \tag{1.2.1}$$

It is not difficult to see that $C^\perp$ is an $[n, n-k]$ linear code over $\mathbb{F}_q$. A linear code C is called *self-orthogonal* if $C \subseteq C^\perp$, *dual-containing* if $C^\perp \subseteq C$, and *self-dual* provided that $C = C^\perp$. Obviously, a self-dual linear code has dimension $n/2$. In general, dual-containing and self-dual codes are especially important for constructing quantum stabilizer codes. Moreover, many of the currently best-known linear codes are of these types.

Quaternary linear codes will be one of our main objects in this thesis due to their connection to binary quantum codes. Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the field of four elements, where $\omega^2 = \omega + 1$. For each $a \in \mathbb{F}_4$, we define the *conjugate* of a to be $\overline{a} = a^2$. For each two vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_4^n$, the *Hermitian inner product* of x and y is defined by

$$\langle x, y\rangle_h = \sum_{i=1}^{n} x_i \overline{y_i}.$$

In analogy to (1.2.1), we define the *Hermitian dual* of a linear code $C \subseteq \mathbb{F}_4^n$ to be

$$C^{\perp_h} = \{x \in \mathbb{F}_4^n : \langle x, c\rangle_h = 0 \text{ for all } c \in C\}. \tag{1.2.2}$$

A linear code $C \subseteq \mathbb{F}_4^n$ is called *Hermitian self-orthogonal* if $C \subseteq C^{\perp_h}$, *Hermitian dual-containing* if $C^{\perp_h} \subseteq C$, and *Hermitian self-dual* if $C = C^{\perp_h}$. As we will see in Section 1.7, binary quantum stabilizer codes are constructed using Hermitian dual-containing codes.

Perhaps the most important parameter of a linear code is its minimum distance. The *(Hamming) distance* of vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ is defined by

$$d(x, y) = |\{1 \leq i \leq n : x_i \neq y_i\}|.$$

The distance function d satisfies the following properties for each $x, y, z \in \mathbb{F}_q^n$.

1. $d(x, y) = 0$ if and only if $x = y$.

2. $d(x, y) = d(y, x)$.

3. $d(x, y) \leq d(x, z) + d(y, z)$.

Hence d is a *metric*, and the space $\mathbb{F}_q^n$ with the metric d is a *metric space*. The *minimum distance* of a linear code C is defined by

$$d(C) = \min\{d(x, y) : x \neq y \in C\}.$$

The above definition holds for all codes, even non-linear ones. For linear codes, the minimum distance can be computed alternatively using the weight of vectors. The *(Hamming) weight* of a vector $x \in \mathbb{F}_q^n$ is the number of non-zero coordinates of x and is denoted by $\mathrm{wt}(x)$. Let C be a linear code. For each two codewords x and $y \in C$, we have $\mathrm{wt}(x - y) = d(x, y)$. This implies that

$$d(C) = \min\{\mathrm{wt}(c) : 0 \neq c \in C\}.$$

If the minimum distance d of an $[n, k]$ linear code C is known, we call the code C an $[n, k, d]$ linear code. One of the main computational challenges of linear codes is computing the exact minimum distance for general linear codes, which is NP-hard [104]. Therefore, designing new techniques or algorithms to bound the minimum distance of certain families of linear codes could be extremely valuable. A straightforward connection between the minimum distance of a linear code C and its parity check matrix is provided below.

Proposition 1.2.1 *[55, Section 1.4] Let C be a linear code over $\mathbb{F}_q$ with a parity check matrix H. The code C has minimum distance d if and only if each set of $d-1$ columns of H is linearly independent over $\mathbb{F}_q$ and there exists a set of d linearly dependent columns of H over $\mathbb{F}_q$.*

Example 1.2.2 Let C be a linear code over $\mathbb{F}_3$ with the parity check matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Note that the first three columns of H are linearly independent over $\mathbb{F}_3$ which implies that H has full rank. Thus C is a $[5, 2]$ linear code over $\mathbb{F}_3$. The columns of H are all non-zero, and no column is a scalar multiple of each other column over $\mathbb{F}_3$. Moreover, the first, third, and fourth columns are linearly dependent over $\mathbb{F}_3$. Thus $d(C) = 3$ by Proposition 1.2.1. Hence C is a $[5, 2, 3]$ linear code over $\mathbb{F}_3$.

Next, we briefly recall an encoding and a decoding scheme for linear codes. Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. The code C has q^k codewords, which are in a one-to-one correspondence with q^k different messages. We represent each message by a vector $x \in \mathbb{F}_q^k$. The most common encoding approach is to encode the message x to the codeword $c = xG$, where G is a generator matrix for the code C. The (information) *rate* of C is $R = k/n$, which measures how much information is being transmitted per codeword. We say that an *error* has happened if the received vector is different from the transmitted vector due to noise. Suppose the vector $c \in C$ is transmitted and the vector r is received. The vector $e = r - c$ is called an *error vector*. A linear code is called a t-error-correcting code if it is capable of correcting any error e with $\mathrm{wt}(e) \leq t$. This happens exactly if the Hamming spheres of radius t centered at the codewords are disjoint.

In decoding, we have the received vector, and the goal is to decide which codeword was most likely transmitted. Suppose that $r \in \mathbb{F}_q^n$ and H is a parity check matrix for the code C. The vector $s = Hr^T$ is called the *syndrome* of r. The concept of syndrome is a common tool for the error correction and detection of linear codes. By the definition of parity check matrix, the received vector r is a codeword if and only if its syndrome is zero.

Next, we recall a decoding scheme called *nearest neighbour decoding* for the code C. We assume that the channel introduces errors uniformly at random and that the probability of an error in one coordinate is independent of errors in all other coordinates. Suppose that vector $r \in \mathbb{F}_q^n$ is received. Then r is decoded to the codeword $c \in C$ such that $d(r,c) < d(r,c')$ for each $c' \in C$ such that $c' \neq c$. If there is no such c, then the number of errors exceeds the error-correcting capacity of C. So the error cannot be corrected. Let $u \in \mathbb{F}_q^n$ and $0 \leq \ell \leq n$. The (Hamming) *sphere* of radius ℓ centered at u is defined by

$$S_\ell(u) = \{x \in \mathbb{F}_q^n : d(x,u) \leq \ell\}.$$

If $t = \lfloor \frac{d-1}{2} \rfloor$, then the spheres of radius t centered at distinct codewords of C are disjoint. Thus a received vector r with t or fewer errors is uniquely decoded to the correct codeword using the nearest neighbour decoding.

Since the errors are introduced uniformly at random, we give a justification for the nearest neighbour decoding using another scheme called *maximum likelihood decoding.* We assume that all codewords have the same probability of being sent. This will happen for example when the messages are ciphertexts produced by encryption because ciphertexts look like random strings. Let the probability that an error occurs on a symbol be p. In practice, p is a positive real number and $p \ll \frac{q-1}{q}$. We also assume that in case of an error, each of the $q-1$ symbols aside from the correct symbol is equally likely to be received with the probability $\frac{p}{q-1}$. This type of channel is called *q-ary symmetric.*

In the maximum likelihood decoding scheme the goal is to decode the received vector r to the codeword c such that the conditional probability $P(r|c)$ (the probability r is received, given that c is sent) is maximized over all codewords of C. An easy computation shows that for each codeword $c_1 \in C$ such that $d = (c_1, r)$, we have

$$P(r|c_1) = (1-p)^{n-d}(\frac{p}{q-1})^d.$$

Hence if the spheres of radius t at distinct codewords of C are disjoint and c is the result of nearest neighbour decoding, then for each codeword $c' \in C$ we have $P(r|c') < P(r|c)$. Thus the nearest neighbour decoding and maximum likelihood decoding are equivalent under the assumption that all codewords have the same probability of being sent. The next three theorems give the error detection and error correction capacity of linear codes. All of these results hold also for non-linear codes.

Theorem 1.2.3 *[103, Theorem 1.2] Let C be an $[n,k,d]$ linear code over $\mathbb{F}_q$. Then C can detect any $d-1$ errors and can correct any $\lfloor \frac{d-1}{2} \rfloor$ errors.*

For instance, the code C of Example 1.2.2 can detect any 2 errors and correct any single error. In general, the algorithms for carrying out the decoding methods for linear codes have a high complexity. However, for certain families of linear codes there are fast decoding algorithms (polynomial time), which are essentially based on solving algebraic equations over finite fields. One of the aims of coding theory is to construct families of linear codes which have efficient decoding algorithms. This is because decoding of a random linear code is NP hard [10].

In this thesis, we mainly concentrate on constructing good codes and we use the following connection between the decoding and the minimum distance computation. Let C be a linear code and assume that $r = c + e$ is a received vector, where $c \in C$ and e is the error pattern. Assuming $\mathrm{wt}(e) < d(C)/2$ implies that e is the lowest weight non-zero codeword in the linear code spanned by $C \cup \{r\}$.

Another well-known type of noise corruption is an *erasure*, which happens when in one of the coordinates of the received vector, a symbol is unreadable. A linear code is said to *correct ℓ erasures* if any vector containing ℓ or fewer erasures is correctable.

Theorem 1.2.4 *[103, Theorem 7.4] Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. Then C can correct any $d - 1$ erasures.*

In some communication channels, both errors and erasures can happen. Fortunately, there exist algorithms that correct errors and resolve the erasures simultaneously for such channels.

Theorem 1.2.5 *[103, Theorem 7.5] Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. If $d = 2t + u + 1$, then C is capable of correcting any t errors and u erasures.*

For example, a linear code with minimum distance 5 can correct either

i. 1 error and 2 erasures,

ii. 2 errors and no erasure,

iii. or no error and 4 erasures.

All the above results directly depend on the minimum distance of the code C. One of the major tasks in coding theory is to design codes with good parameters. In other words, the main task is either

1. to find codes with the largest possible minimum distance if the length and the number of codewords of the code are fixed, or

2. to find codes with the largest possible number of codewords if the minimum distance and length of the code are fixed.

Codes satisfying the above conditions are called *optimal*. This thesis proposes new constructions and many examples of record-breaking additive, quantum, and linear codes.

Many interesting and important codes arise by modifying or combining existing codes. Such constructions are usually called *secondary*. Next, we briefly recall a few well-known secondary constructions of linear codes. Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$. We can *puncture* the code C, by deleting a fixed coordinate of each codeword. The resulting punctured code is linear and has length $n-1$, dimension at least $k-1$, and minimum distance at least $d-1$.

Instead of removing a coordinate, we can add new coordinates to make a longer linear code. There are many ways to do that; the most common approach is called the *extended code*. The extended code of C is defined by

$$\hat{C} = \{(x_1, x_2, \ldots, x_n, x_{n+1}) \in \mathbb{F}_q^{n+1} : (x_1, x_2, \ldots, x_n) \in C \text{ and } x_{n+1} = -(x_1 + x_2 + \cdots + x_n)\}.$$

The extended code $\hat{C}$ is again a linear code with length $n+1$, dimension k, and minimum distance d or $d+1$. An interesting application of the extended code happens when C is binary. In this case, the extended code has only even-weight vectors. Therefore, the extended code of a binary code with an odd minimum distance d_o has minimum distance $d_o + 1$.

Let T be a set of $t \leq k$ coordinates, and $C(T)$ be the set of codewords of C taking the value 0 at each coordinate of T. The set $C(T)$ is a linear code. The punctured code of $C(T)$ after deleting the coordinates in T is called the *shortened code*. The shortened code of C has parameters $[n-t, k-t, d_1]$, where $d_1 \geq d$.

Let D be an $[n', k', d']$ linear code. The *direct sum* code of C and D is defined by

$$C \oplus D = \{(c_1, c_2) : c_1 \in C \text{ and } c_2 \in D\}.$$

The direct sum code obviously is linear and has parameters $[n+n', k+k', \min\{d, d'\}]$.

1.3 Linear cyclic codes

Many important families of linear codes, such as Reed-Solomon, Hamming, BCH, etc., are cyclic codes. Linear cyclic codes have rich algebraic properties that make them ideal for practical implementations. For instance, there are many computationally efficient encoding and decoding algorithms for linear cyclic codes.

In some communication channels, such as data storage devices, the Internet, and compact discs the error structure is not very random and errors occur within small intervals of the codeword. Such errors are called *burst errors*, and linear cyclic codes are used to correct these types of errors. We label the coordinate positions of length n vector in $\mathbb{F}_q^n$ by elements of $\mathbb{Z}/n\mathbb{Z}$ which is the set of integers modulo n. This will facilitate the representation and computations of codewords in linear cyclic codes.

Definition 1.3.1 A linear code $C \subseteq \mathbb{F}_q^n$ is called a *cyclic code* over $\mathbb{F}_q$ if for every $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, the vector $(c_{n-1}, c_0, \ldots, c_{n-2})$ obtained from a cyclic shift of the coordinates of c is also in C.

In studying linear cyclic codes, we often use the polynomial representation for each vector. The map $\phi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/\langle x^n - 1\rangle$ defined by

$$\phi((a_0, a_1, \ldots, a_{n-1})) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$$

is an $\mathbb{F}_q$-linear isomorphism of finite groups i.e. of vector spaces. Therefore, each vector in $\mathbb{F}_q^n$ can be uniquely represented by a polynomial in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Hence each length n linear code over $\mathbb{F}_q$ can alternatively be considered as a subspace of polynomials of degree less than n over $\mathbb{F}_q$. For simplicity, it is customary to identify the codewords with the polynomial representing it. The following statements are equivalent for a linear code C.

1. The code C is invariant under the cyclic shifts.

2. For each $c(x) \in \phi(C)$, the polynomial $xc(x) \bmod x^n - 1$ is also an element of $\phi(C)$.

Thus the map ϕ gives a one-to-one correspondence between length n linear cyclic codes over $\mathbb{F}_q$ and ideals of the ring $\mathbb{F}_q[x]/\langle x^n-1\rangle$. The ring $\mathbb{F}_q[x]/\langle x^n-1\rangle$ is a principal ideal ring, and therefore each ideal (or equivalently linear cyclic code) can be generated by a unique monic polynomial called the *generator polynomial.* This implies that all codewords of a linear cyclic code are multiples of the generator polynomial. Since all generator polynomials are factors of $x^n - 1$, the factorization of $x^n - 1$ over $\mathbb{F}_q$ is used to classify all linear cyclic codes of length n over $\mathbb{F}_q$. To get only distinct factors in the factorization of $x^n - 1$, for the rest of this thesis, we assume throughout that $\gcd(n, q) = 1$. This is a very common assumption in both theory and practice. In general, linear cyclic codes are mainly studied assuming this gcd condition.

For each $a \in \mathbb{Z}/n\mathbb{Z}$, the set $Z(a) = \{(aq^j) \bmod n : 0 \leq j \leq m-1\}$, where m is the smallest positive integer such that $aq^m = a \pmod{n}$, is called the *q-cyclotomic coset* of a modulo n. The smallest member of a q-cyclotomic coset is called the *coset leader*. All different q-cyclotomic cosets modulo n partition $\mathbb{Z}/n\mathbb{Z}$. Let $r = |Z(1)|$ or equivalently r be the smallest positive integer such that $n \mid q^r - 1$. Then the finite field $\mathbb{F}_{q^r}$ is the splitting field of $x^n - 1$. The next theorem presents the connection between factors of $x^n - 1$ and cyclotomic cosets modulo n.

Theorem 1.3.2 *[55, Theorem 4.1.1] Let n be a positive integer such that $\gcd(n, q) = 1$ and α be a primitive n-th root of unity in a finite field extension of $\mathbb{F}_q$. Then*

1. *For each $0 \leq s \leq n-1$, the minimal polynomial of α^s over $\mathbb{F}_q$ is given by*

$$M_{\alpha^s} = \prod_{i \in Z(s)} (x - \alpha^i).$$

2. *Let $Z(i_1), Z(i_2), \ldots, Z(i_r)$ be all the different q-cyclotomic cosets modulo n. Then the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$ is given by*

$$x^n - 1 = \prod_{j=1}^{r} M_{\alpha^{i_j}}.$$

Let α be a fixed primitive n-th root of unity in a finite field extension of $\mathbb{F}_q$. If $g(x)$ is the generator polynomial of a length n linear cyclic code C over $\mathbb{F}_q$, then the roots of $g(x)$ are in the form $\{\alpha^t : t \in A\}$, where A is a unique union of q-cyclotomic cosets modulo n. The set A with this property is called the *defining set* of the code C. The set $\{\alpha^t : t \in A\}$ is also referred to as the *zero set* of the cyclic code C. This is because, by Theorem 4.4.2 of [55], we have $c(x)$ is a codeword of C if and only if $c(\alpha^t) = 0$ for each $t \in A$.

Remark 1.3.3 In the numerical examples of cyclic, constacyclic, and twisted codes throughout this thesis, the primitive n-th root of unity α is fixed as follows. Let $n \mid q^r - 1$ for the smallest positive integer r with this property, and γ be the primitive element in $\mathbb{F}_{q^r}$ chosen by the `PrimitiveElement` function in Magma [17], then set $\alpha = \gamma^{(q^r-1)/n}$. Let us note all major computer algebra systems such as GAP, Macaulay2, Magma, and SageMath use the same primitive polynomial (so-called Conway polynomial) to construct $\mathbb{F}_{q^r}$ as an algebraic extension of $\mathbb{F}_q$. Therefore all our examples can exactly be reproduced in all other systems as well.

Next, we recall some properties of linear cyclic codes.

Theorem 1.3.4 *[55, Theorem 4.2.1] Let C be a length n linear cyclic code over $\mathbb{F}_q$ with the generator polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$, where $g_{n-k} \neq 0$. Then*

1. *the code C has dimension $k = n - \deg(g(x))$,*

2. *the matrix*

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \tag{1.3.1}$$

   is a generator matrix for the linear cyclic code C.

Example 1.3.5 The 2-cyclotomic cosets modulo 9 are $Z_0 = \{0\}$, $Z_1 = \{1, 2, 4, 8, 7, 5\}$, and $Z_3 = \{3, 6\}$. Thus $x^9 - 1$ over $\mathbb{F}_2$ has three irreducible factors. Moreover, $9 \mid 2^6 - 1$ and therefore $\mathbb{F}_{2^6}$ contains all the 9-th roots of unity. Let $\alpha \in \mathbb{F}_{2^6}$ be a primitive 9-th root of unity. Then, by Theorem 1.3.2, we can factorize $x^9 - 1$ into the product of monic irreducible factors over $\mathbb{F}_2$ as

$$x^9 - 1 = (x + 1)(x^6 + x^3 + 1)(x^2 + x + 1),$$

where $x+1$, $(x-\alpha^3)(x-\alpha^6)=x^2+x+1$, and

$$(x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^7)(x-\alpha^5)=x^6+x^3+1$$

are the minimal polynomials of 1, α, and α^3 over $\mathbb{F}_2$, respectively. The combination of these irreducible polynomials gives eight different factors of x^9-1. Thus there are eight different binary cyclic codes of length 9. As we will see in Section 1.6 and Chapter 4, some of these codes are equivalent and have the same parameters (dimension and minimum distance). Let $g(x)=(x+1)(x^2+x+1)$ be the generator polynomial of a linear cyclic code C. Then C has the defining set $A=\{0,3,6\}$ and has dimension $n-\deg(g(x))=9-3=6$ over $\mathbb{F}_2$.

Let $f(x)=\sum_{i=0}^{s}a_ix^i$ be a polynomial of degree s in $\mathbb{F}_q[x]$. The *reciprocal polynomial* of $f(x)$ is defined by

$$f^*(x)=x^sf(x^{-1})=\sum_{i=0}^{s}a_{s-i}x^i. \tag{1.3.2}$$

The reciprocal polynomial allows us to easily check the Euclidean and Hermitian orthogonality of vectors in linear cyclic codes. Let $a=(a_0,a_1,\ldots,a_{n-1})$ and $b=(b_0,b_1,\ldots,b_{n-1})$ be two vectors with the polynomial representations $a(x)$ and $b(x)$, respectively. Then a is orthogonal to b and all of its cyclic shifts with respect to the Euclidean inner product if and only if $a(x)b^*(x)\equiv 0 \pmod{x^n-1}$.

Theorem 1.3.6 *[55, Theorem 4.4.9] Let C be a linear cyclic code with the generator polynomial $g(x)$ and the defining set A. Let $h(x)=(x^n-1)/g(x)$. Then $C^\perp$ is a linear cyclic code and*

1. *the polynomial $h^*(x)/h(0)$ is the generator polynomial of the code $C^\perp$,*
2. *the set $\mathbb{Z}/n\mathbb{Z}\setminus((-A) \bmod n)$ is the defining set of $C^\perp$.*

Example 1.3.7 Let $n=7$. The 2-cyclotomic cosets modulo 7 are $\{0\}$, $\{1,2,4\}$, and $\{3,5,6\}$. Using Theorem 1.3.2, the irreducible polynomials corresponding to such cyclotomic cosets are $x+1$, x^3+x+1, and x^3+x^2+1, respectively. Let C be a length 7 binary cyclic code with the generator polynomial $g(x)=(x+1)(x^3+x+1)$. Then C has the defining set $\{0,1,2,4\}$. By Theorem 1.3.6, the Euclidean dual of C has the generator polynomial and the defining set $f(x)=x^3+x+1$ and $\{1,2,4\}$, respectively. This shows that the code C is a Euclidean self-orthogonal cyclic code. This is because $f(x)\mid g(x)$ which implies that $C\subseteq C^\perp$.

Let $f(x)=\sum_{i=0}^{s}a_ix^i$ be a polynomial of degree s in $\mathbb{F}_4[x]$. The *conjugate polynomial* of $f(x)$ is defined by

$$\overline{f}(x)=\sum_{i=0}^{s}\overline{a_i}x^i. \tag{1.3.3}$$

Next, we provide an analogous result for the Hermitian dual of linear cyclic codes over $\mathbb{F}_4$.

Theorem 1.3.8 *[55, Theorem 4.4.15] Let C be a linear cyclic code over $\mathbb{F}_4$ with the generator polynomial $g(x)$ and the defining set A. Let $h(x) = (x^n - 1)/g(x)$. Then*

1. *the conjugate polynomial of $h^*(x)/h(0)$ is the generator polynomial of the code $C^{\perp_h}$,*
2. *the set $\mathbb{Z}/n\mathbb{Z} \setminus ((-2A) \bmod n)$ is the defining set of $C^{\perp_h}$.*

Let C be a linear cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$. The polynomial $h(x) = (x^n - 1)/g(x)$ is called the *parity check polynomial* of the code C. This is because for each $r(x) \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$, we have $c(x) \in C$ if and only if $r(x)h(x) \equiv 0 \pmod{x^n - 1}$. Thus the parity check polynomial gives us a scheme to check whether the polynomial $r(x)$ is a codeword of C. Similar to linear codes, we can define the syndrome of vectors for linear cyclic codes. There are two customary ways to define the syndrome of a polynomial for linear cyclic codes. First, we define the syndrome of $r(x)$ using the parity check polynomial to be $s(x) = \big(r(x)h(x)\big) \bmod x^n - 1$. Alternatively, the syndrome of $r(x)$ can be defined using the generator polynomial $g(x)$ of C by $s(x)$ which is the remainder of the division $r(x) = q(x)g(x) + s(x)$. In both cases, we can conclude that $r(x)$ is a codeword if and only if $s(x) = 0$.

In certain channels, errors are introduced in short intervals rather than completely at random. For instance, in storage devices, physical irregularities or structural alteration can cause errors to be less independent and occur in consecutive locations. Similarly, interference over short time intervals in serially transmitted radio signals causes errors to occur in bursts. In general, suppose that a codeword $c \in C$ is transmitted, and it is received as $c + e$. The error vector e is called a burst error of length ℓ if the nonzero components of e all appear in an interval of size ℓ, and ℓ is the smallest such number. The majority of the tools developed for burst error correction rely on cyclic codes. So we briefly review the burst error detection process for linear cyclic codes. A *cyclic burst error* of length $\ell \leq n$ is a vector in $\mathbb{F}_q^n$ whose non-zero coordinates are within a cycle of length ℓ, and ℓ is the smallest number with this property. For example,

1. $e_1 = (0, 0, 1, 1, 0, 1, 0, 0, 0)$ is a cyclic burst error of length 4 in $\mathbb{F}_2^9$.
2. $e_2 = (0, 1, 1, 0, 1, 0, 0, 1, 0)$ is a cyclic burst error of length 7 in $\mathbb{F}_2^9$.
3. $e_3 = (0, 1, 0, 0, 0, 0, 0, 0, 1)$ is a cyclic burst error of length 3 in $\mathbb{F}_2^9$.

Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$ with the generator polynomial $g(x) = g_0 + g_1x + \cdots + g_{n-k-1}x^{n-k-1} + x^{n-k}$. It is easy to see that each polynomial $r(x) \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ which is a length $n - k$ burst error can be represented as

$$r(x) = x^i(r_0 + r_1x + r_2x^2 + \cdots + r_{n-k-2}x^{n-k-2} + r_{n-k-1}x^{n-k-1})$$

for some $0 \leq i \leq k$. Since $\gcd(x^i, g(x)) = 1$ and $\deg(g(x)) = n - k$, the polynomial $r(x)$ has a non-zero syndrome. This implies that the code C can detect all burst errors of length $t \leq n - k$.

The *cyclic redundancy check*, or CRC, is a technique used in digital networks as an error-detection scheme. It is applied to detect accidental changes to raw data and, in the case of error, data retransmission is requested. The error-detection protocol in CRC is based on the syndrome computation of linear cyclic codes. In practice, CRC is popular since it is simple to implement, easy to analyze mathematically, and particularly good at detecting many common errors caused by noise in transmission channels. The next example which is taken from [74, Example 4.26] provides an application of certain CRC in detecting errors.

Example 1.3.9 Let $g(x) = x^{16} + x^{15} + x^2 + 1 = (1 + x)(1 + x + x^{15})$. The smallest integer n such that $g(x) \mid x^n - 1$ is 32767. Hence $g(x)$ is the generator polynomial of a length 32767 binary cyclic code. The polynomial $g(x)$ is also called the generator polynomial of CRC-16-IBM (sometimes CRC-16-ANSI or simply as CRC-16). The main uses of CRC-16-IBM are in USB hardware, American National Standards Institute (ANSI), and Binary Synchronous Communications (BSC). For each received polynomial of degree less than 32767, the syndrome error-detection for $g(x)$ can detect

a. any odd number of errors

b. any pattern of two errors

c. all cyclic burst errors of length 16 or less

d. all cyclic burst errors of length 17 with probability 0.99997

e. all cyclic burst errors of length 18 or larger with probability 0.99998.

Some other CRC generator polynomials with various applications in digital communication are provided in [22, 56, 78, 88].

1.4 Minimum distance bounds for linear cyclic codes

As we mentioned previously, i.e., Theorems 1.2.3, 1.2.4, and 1.2.5, we need the minimum distance to determine the error-correcting and error-detecting capability of a linear code. Also, recall that computing the exact minimum distance for a general linear code is NP-hard [104]. Therefore, it is important to have upper or lower bounds for the minimum distance of certain linear codes. In this section, we discuss several well-known minimum distance bounds for linear cyclic codes, namely the Bose-Chaudhuri-Hocquenghem (BCH), Hartmann-Tzeng (HT), Roos, and a distance lower bound of van Lint and Wilson.

We first recall the result of Proposition 1.2.1 as it will be used very frequently in this section. A linear code C over $\mathbb{F}_q$ with a parity check matrix H has minimum distance d if and only if the set of each $d-1$ columns of H is linearly independent over $\mathbb{F}_q$ and there exists a set of d linearly dependent columns of H over $\mathbb{F}_q$. In general, applying this result directly still is computationally very inefficient. In this section, we use the structure of Vandermonde matrices and provide (minimum distance) lower bounds for the minimum distance of linear cyclic codes. Let $\beta_1, \beta_2, \ldots, \beta_s \in \mathbb{F}_q$. The $s \times s$ matrix

$$V = \begin{bmatrix} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{s-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{s-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_s & \beta_s^2 & \cdots & \beta_s^{s-1} \end{bmatrix} \tag{1.4.1}$$

with entries from $\mathbb{F}_q$ is called a *Vandermonde matrix.* The determinant of a Vandermonde matrix can be computed easily using the formula $\prod\limits_{1 \le i < j \le s} (\beta_j - \beta_i)$, see for example [55, Lemma 4.5.1]. In particular, the matrix V is nonsingular if and only if $\beta_1, \beta_2, \ldots, \beta_s$ are distinct elements of $\mathbb{F}_q$.

Throughout the rest of this section, C is a linear cyclic code over $\mathbb{F}_q$ of length n such that $\gcd(n, q) = 1$. Note that the theory of cyclic codes is insensitive to the selection of a primitive n-th root of unity in the following sense. As we will see in Theorem 1.6.4, changing the primitive n-th root of unity in the construction of cyclic codes results in a permutation equivalent linear cyclic code. From now on, we fix α to be a primitive n-th root of unity in a finite field extension of $\mathbb{F}_q$ using the convention of Remark 1.3.3. Let $A = \{i_1, i_2, \ldots, i_k\}$ be the defining set of the code C. The code C has dimension $n-k$, and the matrix

$$H = \begin{bmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \cdots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \cdots & \alpha^{(n-1)i_2} \\ & \vdots & & \vdots & \\ 1 & \alpha^{i_k} & \alpha^{2i_k} & \cdots & \alpha^{(n-1)i_k} \end{bmatrix} \tag{1.4.2}$$

is a generalized parity check matrix for C. This is because first, the matrix H has the rank k as the first k columns of H form a nonsingular Vandermonde matrix. Second, if $c = (c_0, c_1, \ldots, c_{n-1})$ is the vector representation of an arbitrary polynomial $c(x) \in \mathbb{F}_q[x]$, then the j-th coordinate of Hc^T is $c(\alpha^{i_j})$ for each $1 \le j \le k$. Since it is well-known that $c(x)$ is in correpondence to a codeword of C exactly when it is a multiple of the generator polynomial $g(x)$ of C, we have $Hc^T = 0$ if and only if $g(x) \mid c(x)$.

Definition 1.4.1 A set $\{i_1, i_2, \ldots, i_s\} \subseteq \mathbb{Z}/n\mathbb{Z}$ is called a *consecutive set* of length s if there exists an integer c with $\gcd(c, n) = 1$ such that

$$\{(ci_t) \bmod n : 1 \le t \le s\} = \{(j+t) \bmod n : 0 \le t \le s-1\}$$

for some $j \in \mathbb{Z}/n\mathbb{Z}$.

We now provide the BCH minimum distance bound, which is the oldest and the most well-known minimum distance lower bound for linear cyclic codes. It was discovered by Bose and Ray-Chaudhuri (1960) and independently by Hocquenghem (1959). This discovery also resulted in a new class of linear cyclic codes called BCH codes. In particular, BCH codes allow us to design the minimum distance of a cyclic code to be at least d by selecting $d-1$ consecutive elements to be in the defining set.

Theorem 1.4.2 (BCH bound) *[16, 52] Let C be a linear cyclic code of length n over $\mathbb{F}_q$ with the defining set A. If A contains a consecutive subset of length $\delta - 1$, then the code C has minimum distance $d(C) \geq \delta$.*

By the BCH bound, we can simply find a lower bound for the minimum distance of a linear cyclic code by finding the length of the longest consecutive set inside the defining set. Let A and B be two subsets of $\mathbb{Z}/n\mathbb{Z}$. We define the sum $A+B = \{(a+b) \bmod n : a \in A$ and $b \in B\}$. Hartmann and Tzeng, in 1972, provided a generalization of the BCH bound [51]. They showed that if the defining set of a linear cyclic code contains sum of more than one consecutive set, then the BCH bound can be improved.

Theorem 1.4.3 (Hartmann-Tzeng bound) *[51] Let C be a linear cyclic code of length n over $\mathbb{F}_q$ with the defining set A. If A contains a subset in the form*

$$\{(l+i_1c_1+i_2c_2) \bmod n :\ 0 \leq i_1 \leq t-2,\ 0 \leq i_2 \leq m,\ \gcd(c_1,n) = \gcd(c_2,n) = 1\}, \quad (1.4.3)$$

where $l, c_1, c_2 \in \mathbb{Z}$, $t \geq 2$, and m is a non-negative integer, then $d(C) \geq t+m$.

The set in (1.4.3) can also be expressed as the sum of two consecutive sets $M+N$, where $M = \{(l+i_1c_1) \bmod n :\ 0 \leq i_1 \leq t-2$ and $\gcd(c_1,n) = 1\}$ and $N = \{(i_2c_2) \bmod n :$ $0 \leq i_2 \leq m$ and $\gcd(c_2,n) = 1\}$.

Example 1.4.4 Let C be a linear cyclic code of length 17 over $\mathbb{F}_2$ with the defining set $A = \{1,2,4,8,9,13,15,16\}$. The set $\{1,2\}$ is a consecutive subset of A. Thus by the BCH bound $d(C) \geq 3$. Moreover, $\{(1+i_1+7i_2) \bmod 17 :\ 0 \leq i_1 \leq 1$ and $0 \leq i_2 \leq 2\} = \{1,2,8,9,15,16\} \subseteq A$. Therefore the code C has minimum distance $d(C) \geq 5$ by the HT bound. By applying the `MinimumDistance` function in Magma [17], we get $d(C) = 5$ and thus C is a $[17,9,5]$ binary cyclic code.

Hartmann and Tzeng also provided some other generalizations of their main minimum distance bound. First, they showed that the result of the HT bound remains valid if the defining set contains more than two consecutive sets. Second, they proved that the gcd condition in the HT bound could be relaxed to some extent.

Theorem 1.4.5 *[51] Let C be a linear cyclic code of length n over $\mathbb{F}_q$ with the defining set A. If A contains a subset in the form*

$$\{(l+i_1c_1+i_2c_2+\cdots+i_mc_m) \bmod n :\ 0 \leq i_j \leq s_j,\ \gcd(c_j,n) = 1\},$$

where $l, c_j \in \mathbb{Z}$ and s_j is a non-negative integer for each $1 \leq j \leq m$, then $d(C) \geq (\sum_{j=1}^{m} s_j)+2$.

Theorem 1.4.6 *[51] Let C be a linear cyclic code of length n over $\mathbb{F}_q$ with the defining set A. If A contains a subset in the form*

$$\{(l + i_i c_1 + i_2 c_2) \bmod n : \ 0 \leq i_1 \leq t-2, \ 0 \leq i_2 \leq m, \ \gcd(c_1, n) = 1, \ \gcd(c_2, n) \leq t-1\},$$

where $l, c_1, c_2 \in \mathbb{Z}$, $t \geq 2$, and m is a non-negative integer, then $d(C) \geq t + m$.

The Roos bound is another well-known lower bound for the minimum distance of linear cyclic codes. It bounds the minimum distance of a cyclic code when its defining set contains a subset in the form $M + N$, where N is a consecutive set, but M is not necessarily a consecutive set.

Theorem 1.4.7 (Roos bound) *[89] Let C be a length n linear cyclic code over $\mathbb{F}_q$ with the defining set A. Let M and N be non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$ such that N is consecutive and $M + N \subseteq A$. If there exists a consecutive set $\overline{M} \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $M \subseteq \overline{M}$ and $|\overline{M}| \leq |M| + |N| - 1$, then $d(C) \geq |M| + |N|$.*

If the sets M and N in Theorem 1.4.7 are both consecutive, then Roos bound and the HT bound are the same. Next, we provide an example from [89], where the Roos bound beats the HT and BCH bounds.

Example 1.4.8 [89, Example 1] The 2-cyclotomic cosets modulo 21 are $Z(0) = \{0\}$, $Z(1) = \{1, 2, 4, 8, 16, 11\}$, $Z(3) = \{3, 6, 12\}$, $Z(5) = \{5, 10, 20, 19, 17, 13\}$, $Z(7) = \{7, 14\}$, and $Z(9) = \{9, 18, 15\}$. Let C be a binary cyclic code of length 21 with the defining set $A = Z(1) \cup Z(3) \cup Z(7) \cup Z(9)$. Then $\{1, 2, 3, 4\} \subset A$ and by the BCH bound, minimum distance of C is at least 5. Also, $\{1, 2, 3, 4\} + \{0, 5\}$ is a subset of A. Thus the HT bound implies that $d(C) \geq 6$. Finally, let $N = \{2, 3, 4\}$ and $M = \{0, 4, 12, 20\}$. One can easily see that $M + N \subset A$ and M is a subset of the consecutive set $\overline{M} = \{0, 4, 8, 12, 16, 20\}$. Moreover, $|\overline{M}| = 6 \leq |M| + |N| - 1 = 6$ and thus the Roos bound implies that $d(C) \geq 7$.

Let $N = \{s_1, s_2, \ldots, s_t\}$ be a subset of $\mathbb{Z}/n\mathbb{Z}$ and D_N, in the form of (1.4.2), be a generalized parity check matrix for the linear cyclic code of length n over $\mathbb{F}_q$ with the defining set N. Let M be a matrix with n columns and $J \subseteq \mathbb{Z}/n\mathbb{Z}$. We denote by M^J the submatrix of M consisting of columns of M with indices from the set J. The last minimum distance lower bound that we mention here is due to a work by van Lint and Wilson in 1986 [102]. This distance bound is a generalization of the Roos bound.

Theorem 1.4.9 *[102] Let M and N be non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$. Suppose C is a length n linear cyclic code over $\mathbb{F}_q$ with the defining set A such that $M + N \subseteq A$. If for every $I \subseteq \mathbb{Z}/n\mathbb{Z}$ with $|I| < s$ the inequality $rank({D_N}^I) + rank({D_M}^I) > |I|$ holds, then $d(C) \geq s$.*

Another well-known technique to produce lower bounds on the minimum distance of linear cyclic codes is van Lint-Wilson shifting bound. The shifting bound is an algorithmic method and is more suitable for computational examples. We refer to [102, Section 5] for more information about the shifting bound.

1.5 Linear constacyclic codes over $\mathbb{F}_4$

Constacyclic codes are one of the well-known generalizations of linear cyclic codes. They were first introduced in [9] with many similar properties as linear cyclic codes. In this thesis, we only consider constacyclic codes over $\mathbb{F}_4$ due to their application in construction of binary quantum codes. Because of the similarity between the linear cyclic and constacyclic codes, in this section, we mainly concentrate on the construction and algebraic properties of constacyclic codes. Throughout this section, n is a positive odd integer and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ is the field of four elements, where $\omega^2 = \omega + 1$.

Definition 1.5.1 For each $0 \neq \eta \in \mathbb{F}_4$, a linear code $C \subseteq \mathbb{F}_4^n$ is called *η-constacyclic*, if for each codeword $(a_0, a_1, \dots, a_{n-1}) \in C$, the vector $(\eta a_{n-1}, a_0, \dots, a_{n-2})$ is also in C.

When $\eta = 1$, η-constacyclic codes are linear cyclic codes. In this thesis, we only consider η-constacyclic codes over $\mathbb{F}_4$, where $\eta \in \{\omega, \omega^2\}$. Recall that the length n vector $(a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_4^n$ can alternatively be represented using its polynomial form which is $\sum_{i=0}^{n-1} a_i x^i$. Similar to linear cyclic codes, there is a one-to-one correspondence between η-constacyclic codes and ideals of the ring $\mathbb{F}_4[x]/\langle x^n - \eta\rangle$. The ring $\mathbb{F}_4[x]/\langle x^n - \eta\rangle$ is a principal ideal ring and hence each ideal (or equivalently η-constacyclic code) is generated by a unique monic polynomial $g(x)$ over $\mathbb{F}_4$ such that $g(x) \mid x^n - \eta$. The polynomial $g(x)$ with this property is called the *generator polynomial* of the corresponding constacyclic code. Thus we use the factorization of $x^n - \eta$ to find all the different η-constacyclic codes. There are no repeated factors in the factorization of $x^n - \eta$ because we assumed that $\gcd(n, 2) = 1$.

Since $\eta \in \{\omega, \omega^2\}$, the multiplicative order of η is 3. Let δ be a fixed primitive $3n$-th root of unity in a finite field extension of $\mathbb{F}_4$ such that

$$\delta^n = \eta.$$

Let also $\Omega = \{1 + 3j : 0 \leq j \leq n-1\}$. Then the roots of $x^n - \eta$ are in the form δ^{1+3a} for each $1 + 3a \in \Omega$. For each $1 + 3a \in \Omega$, the 4-cyclotomic coset $Z(1 + 3a)$ is a subset of Ω. This is because $4(1 + 3a) = 1 + 3(4a + 1) \equiv 1 + 3a' \pmod{3n}$ for some integer a'. Therefore the 4-cyclotomic cosets partition the set Ω. Let $Z(a_1), Z(a_2), \dots, Z(a_t)$ be all the different 4-cyclotomic cosets modulo $3n$ such that $\Omega = \bigcup_{i=1}^{t} Z(a_i)$. Then similar to the result of Theorem 1.3.2 for linear cyclic codes, we can factorize $x^n - \eta$ as

$$x^n - \eta = \prod_{j=1}^{t} M_j, \tag{1.5.1}$$

where $M_j = \prod_{i \in Z(a_j)} (x - \delta^i)$ for each $1 \leq j \leq t$ is a monic irreducible factor over $\mathbb{F}_4$. Hence if $g(x)$ is the generator polynomial of an η-constacyclic code over $\mathbb{F}_4$ of length n, then the roots of $g(x)$ are $\{\delta^a : a \in A\}$, where A is a unique union of 4-cyclotomic cosets modulo $3n$. The set A is called the *defining set* of the η-constacyclic code generated by $g(x)$. Moreover, the set $\{\delta^a : g(\delta^a) = 0\}$ is referred to as the *zero set* of the η-constacyclic code generated by $g(x)$.

Let C be an η-constacyclic code over $\mathbb{F}_4$ of length n with the generator polynomial $g(x) = \sum_{i=0}^{n-k} g_i x^i$, where $g_{n-k} \neq 0$. Similar to the linear cyclic codes, the code C has dimension $k = n - \deg\big(g(x)\big)$ and the matrix

$$G = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \tag{1.5.2}$$

is a generator matrix of the code C.

Example 1.5.2 We find all the ω-constacyclic codes of length 7 over $\mathbb{F}_4$. First note that $\Omega = \{1, 4, 7, 10, 13, 16, 19\}$ and all the roots of $x^7 - \omega$ are in the form δ^i, where $i \in \Omega$ and δ is a fixed primitive 21-th root of unity in $\mathbb{F}_{4^3}$ such that $\delta^7 = \omega$. Moreover, $\Omega = Z(1) \cup Z(7) \cup Z(10)$. Using (1.5.1), we can decompose $x^7 - \omega$ into the product of irreducible factors as

$$x^7 - \omega = (x - \omega)(x^3 + \omega^2 x + 1)(x^3 + \omega x^2 + 1).$$

There are 8 different combinations of these irreducible factors which give the generator polynomials of all the ω-constacyclic codes of length 7 over $\mathbb{F}_4$. For instance, the ω-constacyclic code C with the generator polynomial $g(x) = (x^3 + \omega^2 x + 1)(x^3 + \omega x^2 + 1) = x^6 + \omega x^5 + \omega^2 x^4 + x^3 + \omega x^2 + \omega^2 x + 1$ is one of such codes. The code C has the defining set $\{1, 4, 10, 13, 16, 19\}$ and is a one-dimensional subspace of $\mathbb{F}_4$. In particular, the set $\{(1, \omega, \omega^2, 1, \omega, \omega^2, 1)\}$ forms a basis for C.

Next we give the generator polynomial and the defining set of the Euclidean and the Hermitian duals of a given η-constacyclic code over $\mathbb{F}_4$. Let $f(x) \in \mathbb{F}_4[x]$. We recall that the reciprocal polynomial of $f(x) = \sum_{i=0}^{k} a_i x^i$ is defined by $f^*(x) = x^k f(x^{-1}) = \sum_{i=0}^{k} a_{k-i} x^i$, and the conjugate polynomial of $f(x)$ is $\overline{f}(x) = \sum_{i=0}^{k} \overline{a_i} x^i$. Recall that $\eta \in \{\omega, \omega^2\}$.

Theorem 1.5.3 *[59, Section II] [105, Lemma 2.1] Let C be an η-constacyclic code of length n over $\mathbb{F}_4$ with the generator polynomial $g(x)$ and the defining set A. Let $h(x) = (x^n - \eta)/g(x)$. Then the following statements hold.*

1. *The Euclidean dual of C is an η^2-constacyclic code of length n over $\mathbb{F}_4$ with the generator polynomial $h^*(x)/h(0)$. Moreover, the set*

$$A^{\perp} = \Omega' \setminus ((-A) \bmod 3n)$$

is the defining set for $C^{\perp}$, where $\Omega' = \{(3k+2) \bmod 3n : 0 \leq k \leq n-1\}$.

2. *The Hermitian dual of C is an η-constacyclic code of length n over $\mathbb{F}_4$ with the generator polynomial $\overline{h^*(x)/h(0)}$ and the defining set*

$$A^{\perp_h} = \Omega \setminus ((-2A) \bmod 3n).$$

Similar to the linear cyclic codes, there are various upper and lower bounds for the minimum distance of constacyclic codes. Let C be an η-constacyclic code over $\mathbb{F}_4$ of length n with the defining set $A = \{i_1, i_2, \ldots, i_{n-k}\}$. The matrix

$$H = \begin{bmatrix} 1 & \delta^{i_1} & \delta^{2i_1} & \ldots & \delta^{(n-1)i_1} \\ 1 & \delta^{i_2} & \delta^{2i_2} & \ldots & \delta^{(n-1)i_2} \\ & & & \vdots & \\ 1 & \delta^{i_{n-k}} & \delta^{2i_{n-k}} & \ldots & \delta^{(n-1)i_{n-k}} \end{bmatrix} \tag{1.5.3}$$

is a generalized parity check matrix for the code C. We only state the BCH minimum distance lower bound for constacyclic codes.

Theorem 1.5.4 *[62, Lemma 4] Let C be an η-constacyclic code over $\mathbb{F}_4$ of length n. Let α be a primitive n-th root of unity in a finite field extension of $\mathbb{F}_4$ and $B = \{\eta\alpha^i : i \in A\}$, where $A \subseteq \mathbb{Z}/3n\mathbb{Z}$ is a consecutive set of size $t-1$. If B is a subset of the zero set of C, then $d(C) \geq t$.*

Many other minimum distance bounds for the constacyclic codes are discussed in [85].

1.6 Equivalence of linear codes

Suppose that C is a linear code over $\mathbb{F}_q$. Let A_i be the number of codewords of weight i in C. The list $[A_i : 0 \leq i \leq n]$ is called the weight distribution of C. In general, computing the weight distribution of specific codes or families of codes is an active research area.

There are different notions of equivalence for linear codes over $\mathbb{F}_q$. In this section, we present several such equivalence concepts that preserve the weight distribution when passing from one linear code to another. We also recall some results on equivalence of linear cyclic and constacyclic codes.

In general, finding linear codes with good parameters is one of the most challenging tasks in algebraic coding theory. Several attempts have been made in the literature to make the computer search for linear codes with good parameters more systematic. However, the computationally challenging obstacles such as minimum distance computation, which requires a considerable amount of time, have hindered the search process. One way to speed up the process of finding good codes is to design more efficient search algorithms using the properties such as equivalence of codes. For instance, recently, several new linear codes were discovered by using the equivalence of linear cyclic and constacyclic codes, and designing efficient algorithms to search for new linear codes, see for example [2, 5–7].

The results of this section are stated for linear codes over finite fields. However, almost all of them remain valid for non-linear codes and codes over rings. We begin with the simplest concept of equivalence on codes which is called permutation equivalence of codes.

Definition 1.6.1 [55, Section 1.6] Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$. Then C_1 and C_2 are called *permutation equivalent* if there exists a permutation of coordinates which sends C_1 to C_2.

An $n \times n$ matrix P is called a *permutation matrix* if it has exactly one 1 in each row and each column, and the other entries are zero. Let C_1 and C_2 be two length n linear codes over $\mathbb{F}_q$ and G be a generator matrix of C_1. Then C_1 and C_2 are permutation equivalent if there exists an $n \times n$ permutation matrix P such that GP is a generator matrix for C_2.

Let S be a $k \times n$ generator matrix for a linear code C over $\mathbb{F}_q$ and M be a $k \times k$ invertible matrix over $\mathbb{F}_q$. It is easy to see that the linear codes generated by MS and S are the same and the matrix MS is also a generator matrix for the code C. Therefore, if P is an $n \times n$ permutation matrix, then the codes generated by MSP and S are equivalent. We use this to find a generator matrix in standard form. A generator matrix S of an $[n, k]$ linear code is said to be in *standard form* if

$$S = \begin{bmatrix} I_k & A \end{bmatrix},$$

where I_k is the $k \times k$ identity matrix and A is a $k \times (n-k)$ matrix. A generator matrix in standard form is very useful for data transmission. For instance, if we can find a generator matrix in the form of S, then the information symbols (messages) will occur in the first k positions of a codeword.

Another application of permutation equivalence of linear codes is in the security of the McEliece cryptosystem. Let G be a generator matrix of a binary linear $[n,k,d]$ code C with $n = 2^m$, $k = n - mr$, and $d = 2r+1$ for some positive integer r. We also assume that there exists a fast decoding algorithm for the code C. Let S be a non-singular binary $k \times k$ matrix, P be an $n \times n$ binary permutation matrix, and $G' = SGP$. Then the McEliece cryptosystem is designed using such a binary code and has the following properties. *Public key* is the matrix $G' = SGP$ which is a generator matrix of an equivalent code to C. The *encryption* map $E : \mathbb{F}_2^k \to \mathbb{F}_2^n$ is defined by $E(x) = xG' + e$, where e is a random error vector of Hamming weight r. The *decryption* is done by the following steps. First, $y' = yP^{-1}$ is computed from the ciphertext $y = E(x)$. Note that $y' = (xSGP + e)P^{-1} = xSG + e'$, where e' is of Hamming weight at most r. Next, we apply a decoding algorithm on y' to obtain the vector xS. Finally, the plaintext is recovered after multiplying by S^{-1}.

A generalization of permutation equivalence of linear codes is given by both permuting the coordinates and scaling each coordinate by a non-zero value. An $n \times n$ matrix M is called a *monomial matrix* over $\mathbb{F}_q$ if M has exactly one non-zero entry from $\mathbb{F}_q$ in each row and each column. It is easy to see that each monomial matrix M can be decomposed as $M = PD$, where P is a permutation matrix and D is a non-singular diagonal matrix over $\mathbb{F}_q$.

Definition 1.6.2 [55, Section 1.7] Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$ and G be a generator matrix for C_1. Linear codes C_1 and C_2 are called *monomially equivalent* provided that there exists an $n \times n$ monomial matrix M over $\mathbb{F}_q$ such that GM is a generator matrix for C_2.

In the binary case, permutation and monomial equivalence of linear codes are the same. The monomial equivalence of codes can be generalized one more step. If ϕ is a field automorphism of $\mathbb{F}_q$, then we can apply the following process to get a linear code with the same weight distribution:

1. permute the coordinates,

2. scale each coordinate by a non-zero factor,

3. apply the map ϕ to all the coordinates.

This process is usually denoted by $M\phi$, where M is the monomial matrix corresponding to the first two steps. This thesis only deals with the permutation and monomial equivalence of linear codes.

Let C and C' be two length n linear codes over $\mathbb{F}_q$ and ϕ be an $\mathbb{F}_q$-linear bijection from C to C' preserving the Hamming weight. Then ϕ is an isometry of the spaces C

and C' equipped with the Hamming distance function $d(x,y)$ as the metric. This is because for each x and $y \in C$ we have

$$d(x,y) = wt(x-y) = wt(\phi(x-y)) = wt(\phi(x)-\phi(y)) = d(\phi(x),\phi(y)).$$

We call such mapping *isometry of linear codes* and the codes C and C' *isometric equivalent.* Although the isometry of linear codes looks different from the previous notions of equivalence for linear codes, it was proved by MacWilliams in [71] that the isometry and the monomial equivalence of binary linear codes are identical concepts in the sense of the next theorem. A generalization of MacWilliams' result over a general finite field is quoted below.

Theorem 1.6.3 *[15, Corollary 1] Let C and C' be two linear codes over a finite field. Then C and C' are isometric equivalent if and only if these codes are monomial equivalent.*

In spite of the above connection between monomial equivalence and isometry of linear codes, occasionally using one of these two definitions can be easier than the other. Therefore, we use both notions in the future sections and keep in mind that they are equivalent definitions.

1.6.1 Equivalence of linear cyclic codes

In this section, we give restriction of the mentioned equivalence definitions to the family of linear cyclic codes over $\mathbb{F}_q$ and provide several known results from the literature. Throughout this section, n always is a positive integer such that $\gcd(n,q)=1$. Let α denote a fixed primitive n-th root of unity in K which is a finite field extension of $\mathbb{F}_q$.

For each integer a such that $\gcd(n,a)=1$, the function μ_a defined on $\mathbb{Z}/n\mathbb{Z}$ by $\mu_a(x) = (ax) \bmod n$ is called a *multiplier.* Clearly, multipliers are permutations of $\mathbb{Z}/n\mathbb{Z}$. Let μ_a be a multiplier for some integer a. If $Z(b) = \{(bq^i) \bmod n : 0 \le i \le m-1\}$ is a q-cyclotomic coset modulo n containing b for some $b \in \mathbb{Z}/n\mathbb{Z}$, then $\mu_a(Z(b)) = Z(ab)$. Therefore multipliers act on the set of all cyclotomic cosets. Moreover, multipliers preserve the size of cyclotomic cosets. Note also that μ_{q^i} acts trivially on the cyclotomic cosets. Hence if A is the defining set of a length n linear cyclic code and μ_a is a multiplier on $\mathbb{Z}/n\mathbb{Z}$, then $\mu_a(A)$ is also the defining set for a length n linear cyclic code. The next result shows that multipliers map the defining set of a linear cyclic code to the defining set of a permutation equivalent cyclic code.

Theorem 1.6.4 *[72, Section 8.5] Let c be an integer such that $\gcd(c,n)=1$ and A_1 and A_2 be defining sets of two linear cyclic codes of length n over $\mathbb{F}_q$. If $\mu_c(A_1) = A_2$, then linear cyclic codes with the defining sets A_1 and A_2 are permutation equivalent.*

As an application of the previous theorem, we can easily see that each two linear cyclic codes with the defining sets A and $\mu_{-1}(A) = -A$ are permutation equivalent. Let

$\gcd(n,\phi(n))=1$, where ϕ is Euler's totient function, and let C be a length n linear cyclic code over $\mathbb{F}_q$. Palfy, in 1987, characterized all length n linear cyclic codes over $\mathbb{F}_q$ that are permutation equivalent to C using the action of multipliers on the defining set of C [77].

Theorem 1.6.5 *[54, Theorem 1.1] Let C and C' be two linear cyclic codes of length n over $\mathbb{F}_q$ with defining sets A_1 and A_2, respectively and $\gcd(n,\phi(n))=1$. The codes C and C' are permutation equivalent if and only if there exists a multiplier μ_a such that $\mu_a(A_1)=A_2$.*

This result helps us to find all permutation equivalent linear cyclic codes of certain lengths.

Example 1.6.6 Let $q=2$ and $n=15$. Then the 2-cyclotomic cosets modulo n are $A_0=\{0\}$, $A_1=\{1,2,4,8\}$, $A_3=\{3,6,9,12\}$, $A_5=\{5,10\}$, and $A_7=\{7,11,13,14\}$. Since $\gcd(15,\phi(15))=\gcd(15,8)=1$, by Theorem 1.6.5, all the permutation equivalent codes can be determined by multipliers. For example, $7A_1=A_7$ and therefore the linear cyclic codes with the defining sets A_1 and A_7 are permutation equivalent. Moreover, $(\mathbb{Z}/n\mathbb{Z})^*=\{1,2,4,7,8,11,13,14\}$ and all these values map A_3 to A_3. This implies that the linear cyclic code with the defining set A_3 is not permutation equivalent to the linear cyclic codes with the defining sets A_1 and A_7.

Furthermore, let $B\subseteq A_0\cup A_3\cup A_5$ be a union of cyclotomic cosets. The sets $A_1\cup B$ and $A_7\cup B$ are again the defining sets of two permutation equivalent linear cyclic codes since $7(A_1\cup B)=A_7\cup B$.

There are other permutations of $\mathbb{Z}/n\mathbb{Z}$ called generalized multipliers for investigating permutation equivalent cyclic codes [54]. In particular, there exist examples of permutation equivalent linear cyclic codes given by the generalized multipliers. Sometimes such permutation equivalent linear cyclic codes are not permutation equivalent by the action of multipliers, see for example [54, Examples 3.1-3.3].

Definition 1.6.7 Let $n=p^m$ and $k\leq m$, where p is an odd prime and k and $m\geq 2$ are positive integers. For each $1\leq d<p^k$ such that $\gcd(d,p)=1$, the map $M_d:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ defined by $M_d(i+jp^k)=(id \bmod p^k)+jp^k$ is called a *generalized multiplier* of $\mathbb{Z}/n\mathbb{Z}$.

Let μ and M be a multiplier and a generalized multiplier defined on $\mathbb{Z}/n\mathbb{Z}$, respectively. The composition map $M\mu$ on $\mathbb{Z}/n\mathbb{Z}$ is defined by $M\mu(x)=\mu(M(x))$ for each $x\in\mathbb{Z}/n\mathbb{Z}$. Let π be a permutation of $\mathbb{Z}/n\mathbb{Z}$ and $v=(v_0,\dots,v_{n-1})\in\mathbb{F}_q^n$. Define πv to be $(v_{\pi^{-1}(0)},\dots,v_{\pi^{-1}(n-1)})\in\mathbb{F}_q^n$. The map $v\mapsto\pi v$ is linear over $\mathbb{F}_q$. The matrix M such that $\pi v=vM$ for each v is called the *permutation matrix corresponding to π*.

Theorem 1.6.8 *[54, Theorem 3.1] Let C and C' be two linear cyclic codes of length p^2 over $\mathbb{F}_q$, where p is an odd prime and $\gcd(q,p)=1$. If C and C' are permutation equivalent, then they are equivalent by the action of permutation matrices corresponding to μ or $M\mu$, where μ is a multiplier and M is a generalized multiplier.*

We call the map ψ_b on $\mathbb{Z}/n\mathbb{Z}$ defined by $\psi_b(x) = (x+b) \bmod n$ a *shift map*. The next theorem shows that certain shift maps send the defining set of a linear cyclic code to the defining set of a monomially equivalent linear cyclic code.

Theorem 1.6.9 *[6] Let n be a positive integer such that $\gcd(n,q) = 1$ and A_1 and A_2 be defining sets of two length n linear cyclic codes C_1 and C_2 over $\mathbb{F}_q$, respectively. If b is a positive integer such that n divides $b|A_1|(q-1)$ and $\psi_b(A_1) = A_2$, where $\psi_b(x) = (x+b) \bmod n$, then the codes C_1 and C_2 are monomially equivalent.*

The results of Theorems 1.6.4 and 1.6.9 can be combined to state a more general condition for monomial equivalence of linear cyclic codes.

Corollary 1.6.10 *[6] Let A_1 and A_2 be defining sets of two linear cyclic codes of length n over $\mathbb{F}_q$. Let $\theta(x) = (ex+b) \bmod n$, where $\gcd(e,n) = 1$ and $n \mid b|A_1|(q-1)$. If $\theta(A_1) = A_2$, then linear cyclic codes with the defining sets A_1 and A_2 are monomially equivalent.*

Two equivalent linear cyclic codes under the action of an affine map θ defined above will be called *affine equivalent.* Let m and n be two positive integers such that $\gcd(nm, q) = 1$. If $g(x) \in \mathbb{F}_q[x]$ and $g(x) \mid x^n - 1$, then $g(x) \mid x^{nm} - 1$. Thus generator polynomials of length n linear cyclic codes remain generator polynomials for linear cyclic codes of length nm. The following theorem shows that if two cyclic codes of length n are affine equivalent, then the linear cyclic codes of length nm with the same generator polynomials are affine equivalent.

Theorem 1.6.11 *[6] Let n and m be positive integers such that $\gcd(nm,q) = 1$ and $g(x)$ and $h(x)$ be generator polynomials of two linear cyclic codes of length n over $\mathbb{F}_q$. If the cyclic codes generated by $g(x)$ and $h(x)$ are affine equivalent, then $g(x)$ and $h(x)$ generate affine equivalent cyclic codes of length nm.*

Note that, in the above theorem, the cyclic codes of length nm generated by $g(x)$ and $h(x)$ have minimum distance of at most two since $g(x), h(x) \mid x^n - 1$ and thus $x^n - 1$ is in correspondence with a weight two codeword.

1.6.2 Equivalence of linear constacyclic codes

This section briefly recalls recent results on isometric, monomial, and permutation equivalence of constacyclic codes. To keep the statements simple and also apply the same results to prune the search algorithm for binary quantum codes, we restrict our attention to constacyclic codes over $\mathbb{F}_4$. Recall that $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ is the field of four elements, where $\omega^2 = \omega + 1$. Throughout this section, we assume that n is a positive odd integer.

Recall that for each $a \in \mathbb{F}_4$, the conjugate of a is defined by $\overline{a} = a^2$. By [105, Theorem 3.2], the conjugation map

$$\Theta : \mathbb{F}_4[x]/\langle x^n - \omega\rangle \to \mathbb{F}_4[x]/\langle x^n - \omega^2\rangle \qquad (1.6.1)$$

defined by $\Theta(\sum_{i=0}^{n-1} a_i x^i) = \sum_{i=0}^{n-1} \overline{a_i} x^i$ is an isometry of linear codes between ω- and ω^2-constacyclic codes over $\mathbb{F}_4$. Therefore, Θ gives a one-to-one correspondence between the set of all ω-constacyclic codes of length n and all ω^2-constacyclic codes of length n over $\mathbb{F}_4$. Hence, from now on, we restrict our attention only to ω-constacyclic codes over $\mathbb{F}_4$. An isometry between cyclic codes and ω-constacyclic codes of certain lengths over $\mathbb{F}_4$ is given below.

Theorem 1.6.12 *[11, Theorem 15] Let n be a positive odd integer. There exists a one-to-one correspondence, given by an isometry of linear codes, between ω-constacyclic codes and linear cyclic codes of length n over $\mathbb{F}_4$ if and only if $\gcd(3, n) = 1$. In particular,*

1. *If $n \equiv 1 \pmod 3$, then the map $\Theta_1 : \mathbb{F}_4[x]/\langle x^n - \omega\rangle \to \mathbb{F}_4[x]/\langle x^n - 1\rangle$ defined by $\Theta_1(p(x)) = p(\omega x) \bmod (x^n - 1)$ is an isometry of linear codes.*
2. *If $n \equiv 2 \pmod 3$, then the map $\Theta_2 : \mathbb{F}_4[x]/\langle x^n - \omega\rangle \to \mathbb{F}_4[x]/\langle x^n - 1\rangle$ defined by $\Theta_2(p(x)) = p(\omega^2 x) \bmod (x^n - 1)$ is an isometry of ω-constacyclic codes.*

Thus only when $3 \mid n$, we have that ω-constacyclic codes and cyclic codes of length n over $\mathbb{F}_4$ can have different parameters. The following lemma states another useful isometry of ω-constacyclic codes.

Lemma 1.6.13 *[5, Lemma 2.4] Let n and $e = 3k + 1$ be positive integers such that n is odd and $\gcd(n, e) = 1$. Then the map $\psi : \mathbb{F}_4[x]/\langle x^n - \omega\rangle \to \mathbb{F}_4[x]/\langle x^n - \omega\rangle$ defined by $\psi(f(x)) = f(x^e) \bmod (x^n - \omega)$ is an isometry of ω-constacyclic codes.*

It is not difficult to see that the isometry ψ defined above permutes the coordinates. Let A_1 and A_2 be defining sets of two ω-constacyclic codes of length n over $\mathbb{F}_4$. By Lemma 1.6.13, if there exists a multiplier μ_e defined on $\mathbb{Z}/3n\mathbb{Z}$ such that $\mu_e(A_1) = A_2$, then the ω-constacyclic codes with the defining sets A_1 and A_2 are isometrically equivalent.

Example 1.6.14 Let $n = 15$ and δ be a primitive 45-th root of unity in a finite field extension of $\mathbb{F}_4$ such that $\delta^n = \omega$. Then $Z(1) = \{1, 4, 16, 19, 31, 34\}$, $Z(7) = \{7, 28, 22, 43, 37, 13\}$, and $Z(10) = \{10, 40, 25\}$. The multiplier μ_7 gives a bijection between $Z(1)$ and $Z(7)$. Therefore, the ω-constacyclic codes with the defining sets $Z(1)$ and $Z(7)$ are isometrically equivalent by Theorem 1.6.13.

Moreover, $\mu_7(Z(10)) = Z(10)$. Therefore, the ω-constacyclic codes with the defining sets $Z(1) \cup Z(10)$ and $Z(7) \cup Z(10)$ are also isometrically equivalent.

The next result discusses the affine equivalence of constacyclic codes over $\mathbb{F}_4$. This is analogous to the result of Corollary 1.6.10 for cyclic codes. We denote the defining set of an ω-constacyclic code with the generator polynomial $g(x)$ by A_g.

Theorem 1.6.15 *[2] Let n be a positive odd integer and C_1 and C_2 be two ω-constacyclic codes over $\mathbb{F}_4$ of length n with the generator polynomials $g(x)$ and $h(x)$, respectively. Let $e = 3k + 1$ such that $\gcd(3n, e) = 1$. If there exists a map $\theta(x) = (ex + 3j) \bmod (3n)$ on $\mathbb{Z}/3n\mathbb{Z}$ such that n divides $3j \deg(g(x))$ and $\theta(A_g) = A_h$, then C_1 and C_2 are monomially equivalent.*

Proof. This is the $q = 4$ instance of Theorem 3 of [2]. □

1.7 Quantum error-control codes

Similar to the classical linear codes, *quantum error-control codes* (QECCs) are used to protect quantum information against noise. In general, quantum particles are very fragile and they are easily impacted by noise, waves, and other particles. These unwanted interactions with the environment show up as noise in quantum information processing systems. Therefore performing large-scale quantum computations is practically impossible unless error correction and detection methods are applied to protect quantum information from errors. The most famous quantum algorithm is Shor's algorithm [93] for integer factorization, which is exponentially faster than the most efficient known classical integer factoring algorithm. If a quantum computer with a sufficient number of qubits (quantum bits) could gain resistance against quantum noise and other quantum decoherences, then Shor's algorithm could be used to break some public-key cryptography schemes, such as the widely used RSA (Rivest–Shamir–Adleman) scheme. Another impact of quantum computing is on analyzing massive amounts of data. Quantum computing can process large data sets at much faster speeds than classical computers and also analyze data at a more granular level to identify patterns and anomalies.

For a long time, it was unknown whether it would be possible to protect quantum information against noise. The first quantum error-correcting code was discovered by Shor [94]. This code, which is known as *Shor's 9-qubit-code*, encodes one qubit into nine qubits in such a way that the resulting state can be protected against arbitrary single-qubit error on each of these nine qubits. The QECCs are mostly developed based on similar principles as the classical error-control codes. However, there are three main differences between classical and quantum information which have hindered the adaptation of classical ideas for quantum information. These challenges are:

1. no-cloning theorem, which states that quantum information cannot be duplicated,
2. errors are continuous, which potentially may require infinite resources to correct a random error, and
3. the fact that measurement destroys quantum information.

The second item above can be overcome by choosing a suitable error model. An important family of QECCs is the class of *quantum stabilizer codes.* These codes were first discovered independently by Gottesman [41], and Calderbank, Rains, Shor, and Sloane [20]. The theory of quantum stabilizer codes builds a connection between classical and quantum codes, allowing us to import certain classical codes for use as quantum codes. This thesis deals only with quantum stabilizer codes. Shor's 9-qubit-code, which was mentioned above, is an example of a quantum stabilizer code.

In the rest of this section, we give the connection between classical and quantum codes. Moreover, we recall several well-known constructions of quantum codes from binary and quaternary codes. In the next section, we will provide a brief overview of quantum stabilizer codes that is sufficient for understanding our new results. For interested readers, a more detailed description of stabilizer codes from a quantum mechanical point of view is provided in Appendix A.

1.7.1 Mathematical formalism of stabilizer codes

Recall that $\mathbb{F}_4 = \{0, 1, w, w^2\}$ is the field of four elements, where $w^2 = w + 1$. An additive subgroup $C \subseteq \mathbb{F}_4^n$ is called an *additive quaternary code.* We skip the adjective "quaternary" throughout and abbreviate the name to "additive code." An additive code $C \subseteq \mathbb{F}_4^n$ with an $\mathbb{F}_2$-dimension k will be denoted by $(n, 2^k)$. Similar to linear codes, the minimum weight among all non-zero codewords of an additive code C is called the *minimum distance* of C, and it will be represented by $d(C)$.

Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_4^n$. The trace map $\mathrm{Tr} : \mathbb{F}_4 \to \mathbb{F}_2$ is defined by $\mathrm{Tr}(x) = x + \overline{x}$, where $\overline{x} = x^2$. We define conjugate of the vector u by $\overline{u} = (\overline{u_1}, \overline{u_2}, \ldots, \overline{u_n})$. The *trace inner product* of u and v is defined by

$$u * v = \mathrm{Tr}(u \cdot \overline{v}) = (u \cdot \overline{v}) + \overline{(u \cdot \overline{v})} = \sum_{i=1}^{n} (u_i \overline{v_i} + \overline{u_i} v_i). \tag{1.7.1}$$

If C is an $(n, 2^k)$ additive code, its *dual* with respect to the trace inner product is defined by

$$C^{\perp_t} = \{u \in \mathbb{F}_4^n : u * v = 0 \text{ for all } v \in C\}.$$

Here we use the notation $*$ for the trace inner product following the approach of [20]. Note that the inner product $*$ can be equivalently defined using a symplectic inner product (see (A.1.6) for more details). It is easy to see that $*$ is non-degenerate and $C^{\perp_t}$ is an $(n, 2^{2n-k})$ additive code. The code C is called *self-orthogonal* (respectively *self-dual*) with respect to the trace inner product if $C \subseteq C^{\perp_t}$ (respectively if $C = C^{\perp_t}$). Moreover, we call an additive code C a *dual-containing* code with respect to the trace inner product if $C^{\perp_t} \subseteq C$. Let C be an $(n, 2^k)$ additive code. A $k \times n$ matrix M is called a *generator matrix* for C, if the rows of M form a basis for C over $\mathbb{F}_2$.

We are now coming to the mathematical formalism of binary quantum stabilizer codes. The parameters of a *binary* quantum stabilizer code that encodes k logical qubits into n physical qubits and has minimum distance d are denoted by $[\![n, k, d]\!]$. In particular, an $[\![n, k, d]\!]$ quantum code consists of 2^k quantum states, and it is capable of correcting each error of weight at most $\lfloor \frac{d-1}{2} \rfloor$. Quantum codes can similarly be defined over larger alphabets; however, in this thesis, we only deal with binary quantum codes. The mathematical formalism of the quantum stabilizer code, as described in the next theorem, provides a sufficient condition for constructing binary quantum codes from additive codes over $\mathbb{F}_4$.

Theorem 1.7.1 *[20] Let $C \subseteq \mathbb{F}_4^n$ be an $(n, 2^{n+k}, d)$ additive code such that $C^{\perp_t} \subseteq C$. Then an $[\![n, k, d']\!]$ binary quantum stabilizer code can be constructed, where d' is the minimum weight in $C \setminus C^{\perp_t}$ if $k > 0$ and $d' = d$ otherwise.*

Proof. The proof follows from [20, Theorem 2]. □

From now on, we call a quantum stabilizer code simply a quantum code. If the quantum code of Theorem 1.7.1 has minimum distance $d' = d$, then the code is called a *pure* quantum code. Otherwise, it is called *impure.* Throughout this thesis, we never deal with the actual states of a binary quantum code (given in Theorem A.1.1), and we mainly apply the sufficient condition of Theorem 1.7.1 to construct a binary quantum code. The next example deals with the smallest length binary quantum code that is capable of correcting any arbitrary error of weight one.

Example 1.7.2 Let $n = 5$ and C be the trace dual of the additive code generated by

$$M = \begin{bmatrix} 1 & 0 & 1 & \omega & \omega \\ \omega & 0 & \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega & \omega & 1 \\ 0 & \omega & \omega^2 & \omega^2 & \omega \end{bmatrix}.$$

An easy computation shows that $C^{\perp_t} \subseteq C$. Hence by Theorem 1.7.1, we can construct a quantum code using the code C. Moreover, $d(C \setminus C^{\perp_t}) = 3$, which implies that such a quantum code has parameters $[\![5, 1, 3]\!]$. Later, in Example A.1.2, we compute the actual states of such quantum code.

In general, the stabilizer formalism of quantum codes allows many classical codes to be reused to construct binary quantum codes. In fact many of the best known binary quantum codes are stabilizer codes. We only consider stabilizer codes in this thesis and, in the following chapters, we design new constructions and infinite families of good quantum stabilizer codes from various families of classical codes. We also give many examples of record-breaking binary quantum codes.

1.7.2 Constructions of binary quantum codes

Similar to linear codes, we can modify given quantum codes to construct a new quantum code. Using (known) quantum codes to find new ones can simplify the task of finding good quantum codes, which can otherwise be quite a difficult problem. Let C and C' be $[\![n, k, d]\!]$ and $[\![n', k', d']\!]$ quantum codes, respectively. Then the *direct sum code*, which is denoted by $C \oplus C'$, is a quantum code with parameters $[\![n + n', k + k', \min\{d, d'\}]\!]$. A list of other important secondary constructions of quantum codes is provided below. These constructions are based on lengthening, puncturing, or selecting a subcode of the original code.

Theorem 1.7.3 *[20, Theorem 6] Let C be an $[\![n, k, d]\!]$ binary quantum code.*

1. *If $k > 0$, then there exists an $[\![n + 1, k, d]\!]$ binary quantum code.*

2. *If $k > 1$, or if $k \geq 1$ and the code C is pure, then there exists an $[\![n, k - 1, d]\!]$ binary quantum code.*

3. *If $n \geq 2$ and C is pure, then there exists an $[\![n - 1, k + 1, d - 1]\!]$ binary quantum code.*

4. *If $n \geq 2$, then there exists an $[\![n - 1, k, d - 1]\!]$ binary quantum code.*

Example 1.7.4 Let

$$G = \begin{bmatrix} 1 & 0 & \omega^2 & \omega & 1 & 0 & 0 & 0 \\ \omega & 0 & 1 & \omega^2 & \omega & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & \omega & \omega & \omega & \omega & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

be a generator matrix of an additive code over $\mathbb{F}_4$. One can easily see that every two rows of G are orthogonal with respect to the trace inner product. Let C be the trace dual of the code generated by G. Then C is an $(8, 2^9)$ additive code over $\mathbb{F}_4$ and $C^{\perp_t} \subseteq C$. Therefore Theorem 1.7.3 implies the existence of a quantum code Q.

Moreover, $d(C) = 1$ and $\min\{\mathrm{wt}(u) : u \in C \setminus C^{\perp_t}\} = 3$ which implies that Q is impure. Therefore, Q is an $[\![8, 1, 3]\!]$ binary quantum code. In fact, Q is the best-known quantum code with the length 8 and dimension 1 as presented in [43]. Now by applying the secondary constructions given in Theorem 1.7.3 parts (1) and (4) to Q, we get $[\![9, 1, 3]\!]$ and $[\![7, 1, 2]\!]$ quantum codes.

The Calderbank–Shor–Steane (CSS) construction is one of the first and simplest constructions of quantum codes in the literature. This construction combines two binary linear codes to construct a quantum code.

Theorem 1.7.5 *[20, Theorem 9] Let C_1 and C_2 be two binary linear codes with parameters $[n, k_1]$ and $[n, k_2]$ such that $C_1 \subseteq C_2$. Then there exists a quantum code with parameters $[\![n, k_2 - k_1, d]\!]$, where $d = \min\{d(C_2 \setminus C_1), d(C_1^{\perp} \setminus C_2^{\perp})\}$.*

Note that the CSS construction is a special case of stabilizer formalism. In particular, the quantum code of the CSS construction is formed by putting $C = \omega^2 C_1^{\perp} + \omega C_2$. Then $C^{\perp_t} = \omega C_1 + \omega^2 C_2^{\perp}$. An easy observation shows that $C^{\perp_t} \subseteq C$. Thus C is in correspondence to a binary quantum code by Theorem 1.7.1.

Another important construction of quantum codes is by shortening of the additive codes [86]. Let $C \subseteq \mathbb{F}_4^n$ be an additive code. For each $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n) \in C$, we define

$$\{u, v\}_S = (u_1\overline{v_1} + \overline{u_1}v_1, u_2\overline{v_2} + \overline{u_2}v_2, \ldots, u_n\overline{v_n} + \overline{u_n}v_n). \tag{1.7.2}$$

The *puncture code* of C, which is a binary linear code of length n, is defined by

$$P(C) = (span_{\mathbb{F}_2}\{\{u, v\}_S : u, v \in C\})^{\perp}. \tag{1.7.3}$$

The next result gives a shortening construction of quantum codes.

Theorem 1.7.6 *[45, Theorem 11] [86, Theorem 3] Let C be an additive code, not necessarily trace dual-containing, with parameters $(n, 2^{2n-k}, d)$. If there exists a codeword of weight r in $P(C^{\perp_t})$, then there exists a pure $[\![r, r-k', d']\!]$ binary quantum code for some $k' \le k$ and $d' \ge d$.*

The next theorem provides a useful connection between the Hermitian inner product and the trace inner product for linear codes over $\mathbb{F}_4$. Since Hermitian dual-containing codes have been extensively studied in the literature, the following theorem allows us to characterize all the dual-containing linear codes over $\mathbb{F}_4$ with respect to the trace inner product.

Theorem 1.7.7 *[20, Theorem 3] A linear code $C \subseteq \mathbb{F}_4^n$ is dual-containing with respect to the trace inner product if and only if it is dual-containing with respect to the Hermitian inner product.*

We now rephrase the result of Theorem 1.7.1 for the special case when C is a linear code over $\mathbb{F}_4$ and dual-containing with respect to the Hermitian inner product. The next theorem is a straightforward consequence of Theorems 1.7.1 and 1.7.7.

Theorem 1.7.8 *Let C be a linear $[n, k, d]$ code over $\mathbb{F}_4$ such that $C^{\perp_h} \subseteq C$. Then we can construct an $[\![n, 2k-n, d']\!]$ binary quantum code, where d' is the minimum weight in $C \setminus C^{\perp_h}$. If $C = C^{\perp_h}$ then $d' = d$.*

The next construction extends a linear code, which is not necessarily Hermitian dual-containing, to a Hermitian dual-containing linear code of a larger length over $\mathbb{F}_4$. It also bounds the minimum distance of the constructed quantum codes using the minimum distance of certain linear codes.

Theorem 1.7.9 *[68]. Let C be an $[n,k]$ linear code over $\mathbb{F}_4$ and $e = n-k-\dim(C\cap C^{\perp_h})$. Then there exists a quantum code with parameters $[\![n+e, 2k-n+e, d]\!]$, where*

$$d \geq \min\{d(C), d(C+C^{\perp_h})+1\}.$$

In Section 3.2, we will generalize the above construction by allowing its ingredient to be any additive code over $\mathbb{F}_4$.

1.8 Summary of our new techniques and results

The most successful and common technique to date for constructing binary quantum codes is the additive or stabilizer construction, which was introduced in the previous section. One appealing aspect of this construction is its links to classical coding theory, which facilitate the construction of good codes. For example, see Theorems 1.7.1 and 1.7.5. In particular, many of the currently best-known binary quantum codes are constructed using the link to classical codes [20, 43, 60]. This thesis exclusively relies on the connections to classical codes for constructing good quantum codes.

In this thesis, we chose to present our new results in Chapters 2, 3, and 4 in a way that mostly separates them from the foundational background. These chapters were developed in parallel with each of them also becoming a basis for a separate journal paper. Two of the papers are already accepted for publication (results of Chapters 2 and 4) [26, 30] and we plan to submit the last paper after the defence. This section briefly reviews the main results obtained, and techniques used, in Chapters 2, 3, and 4.

Techniques. The concept of additive twisted codes was introduced about 25 years ago. While they have been widely referenced in literature, they have not been developed much since their invention. We introduce a new perspective on twisted codes by viewing each code as a subgroup (additive subcode) of a particular linear cyclic code. This new approach provides a stronger connection between twisted codes and linear cyclic codes, enabling us to give novel minimum distance lower and upper bounds for twisted codes and show new similarities between twisted codes and linear cyclic codes.

In particular, we prove that the Hartmann-Tzeng (HT) bound holds for twisted codes. Our results revitalize the use of the HT bound and reveal new applications of twisted codes. Specifically, we demonstrate that the HT bound is well-suited for twisted codes. A strategic utilization of the concept of unsaturated intersection led us to the construction of families of record-breaking, and sometimes optimal, twisted codes.

The γ value is one of the main ingredients in the construction of twisted codes, yet its impact on code parameters has not been discussed in literature. We show that different γ

values can lead to twisted codes with distinct minimum distances, highlighting the need to examine the conditions for which two γ values yield the same code parameters. To address this issue, we show that all γ values within the same orbit of certain group action generate twisted codes with the same parameters.

The literature has placed great emphasis on the importance of the dual-containment condition in the construction of stabilizer codes, while essentially no attention has been given to codes that fail this condition. In reality, there exist many classical codes with good parameters that are not dual-containing but are nearly dual-containing, meaning they contain a large subset of their dual. We quantify this by proving formulas for dual-containment deficiency of a code. Using this formula, we give a novel construction of binary stabilizer quantum codes that makes it possible to also use the nearly dual-containing codes as its ingredients. In particular, we revive interest in duadic codes by demonstrating that adjustments to nearly dual-containing constructions are especially suitable for certain duadic codes and they led us to discovering many record-breaking codes.

We find new sufficient conditions on equivalence of cyclic codes beyond affine equivalence. Our results can be used to classify all equivalent cyclic codes of specific lengths.

Results. In Chapter 2, the focus is on duadic codes (Definition 2.2.2). These are linear cyclic codes such that there exists a multiplier that takes the defining set to its complement (with the exception of 0). As the multiplier -2 also ensures that we get a binary quantum code, we identified this family as a potentially good source of quantum codes. Indeed we succeeded in both theoretical and computational aspects (Theorem 2.3.6 and Corollaries 2.3.7 and 2.4.4). Additionally, we give new minimum distance bounds for linear cyclic codes (Proposition 2.5.2). We applied our constructions in a numerical search for good binary quantum codes using linear cyclic and duadic codes of length up to 241 over $\mathbb{F}_4$. This led to the discovery of many new record-breaking binary quantum codes, as shown in Table 2.1.

In Chapter 3, we turn attention to additive codes. We present our new nearly dual-containing construction of binary quantum stabilizer codes (Theorem 3.2.3). We provide new lower and upper bounds on minimum distance for twisted codes (Theorems 3.6.3, 3.7.2 and Corollaries 3.6.5, 3.6.6). We also give new infinite families of twisted codes with minimum distance at least five (Theorem 3.7.5). These families are further developed in Theorem 3.8.5. In Section 3.8, we present a secondary construction of quantum codes and give five infinite families of good quantum codes, including record-breaking codes (Theorems 3.8.4, 3.8.5, 3.8.11). We develop computational methods to search for new twisted codes with good parameters. Many record-breaking binary quantum codes are produced by these computations. In Section 3.9 we prove that ten of our quantum codes are optimal (have the highest possible minimum distance). In Section 3.10, we give new algebraic criteria for twisted codes to have the same parameters (Theorem 3.10.14 and Corollaries 3.10.15 and 3.10.16).

In Chapter 4, we first present new sufficient conditions for the equivalence of linear cyclic codes (Theorems 4.2.5, 4.2.11, and 4.2.16). Then we resolve two conjectures regarding the monomial equivalence of linear cyclic codes (Theorem 4.3.1 and Proposition 4.3.2). A necessary and sufficient condition for permutation equivalence of constacyclic codes of certain lengths over $\mathbb{F}_4$ is proved (Theorem 4.4.4). We list examples of record-breaking binary quantum codes and linear codes over $\mathbb{F}_4$ after pruning the search for new codes using the equivalence results. These codes are not of the type discussed in the other chapters.

Chapter 2

New quantum codes from self-dual linear codes over $\mathbb{F}_4$

In this chapter, we present a construction of binary quantum codes from Hermitian self-dual quaternary linear codes. Our main ingredients for such construction of quantum codes are nearly dual-containing cyclic and duadic codes over $\mathbb{F}_4$. In particular, we present an infinite family of 0-dimensional binary quantum codes that is constructed using odd-like duadic codes over $\mathbb{F}_4$. The minimum distance of our quantum codes is lower bounded using the minimum distance of their ingredient linear codes. We also present new results on the minimum distance and weights of vectors in linear cyclic codes using their fixed subcodes by the action of multipliers. Finally, we list many new record-breaking quantum codes that are obtained from our construction. Our numerical results extend the table of good duadic codes to much larger lengths.

This chapter is organized as follows. We survey our main contributions of this chapter in Section 2.1. The required background material is presented in Section 2.2. In Section 2.3, we provide our new constructions of quantum codes using the structure of duadic codes. In Section 2.4, we generalize our quantum constructions by considering more general linear codes over $\mathbb{F}_4$. In Section 2.5, we provide new minimum distance bounds for cyclic codes using their fixed subcodes. In Section 2.6, we present our numerical results that include many new record breaking 0-dimensional binary quantum codes. Many other record breaking quantum codes will be derived after applying the secondary constructions to our new codes.

The material in this chapter is a joint work with my senior supervisor Dr. Lisoněk and a version of it has been accepted for publication in the Springer journal Designs, Codes and Cryptography (special issue for the 12-th International Workshop on Coding and Cryptography), subject to minor revisions [30]. A portion of material in this section was accepted as a 10-page extended abstract and presented at the 12-th International Workshop on Coding and Cryptography (WCC 2022, Rostock, Germany) [29].

2.1 Our main contributions

To differentiate our new results from works in the literature, we summarize our main contributions of this chapter here. In Section 2.3, we first show that if the splitting of a duadic code over $\mathbb{F}_4$ is given by μ_{-2}, then the vectors of corresponding even-like duadic code always have even weights and the rest of vectors in the odd-like duadic code always have odd weights (Theorem 2.3.3). Next we present a construction for 0-dimensional quantum codes using certain odd-like duadic codes. We also give lower bounds for the minimum distance of such quantum codes (Theorem 2.3.6). This construction leads to an infinite family of quantum codes with lengths $p+1$, where $p \equiv -1$ or $-3 \pmod 8$ (Corollary 2.3.7).

In Section 2.4, we first give a generalization of our quantum construction of the previous section, which is also a construction for self-dual linear codes over $\mathbb{F}_4$ (Theorem 2.4.1). A secondary construction of binary quantum code is also provided (Corollary 2.4.2).

In Section 2.5, we give a lower bound for the minimum distance of linear cyclic codes over $\mathbb{F}_4$ using their fixed subcode by the action of multipliers (Proposition 2.5.2). Next we prove that many of such fixed subcodes are the same, and also give other complementary results about the weights of codewords in linear cyclic codes over $\mathbb{F}_4$.

In Section 2.6, we support our constructions by providing many record-breaking binary quantum codes. In particular, we provide a table of 0-dimensional quantum codes with lengths $n \leq 242$ that are obtained from our construction.

2.2 Duadic codes

Duadic codes are regarded as an important family of linear cyclic codes and were extensively discussed in [55, Chapter 6] and [33, Section 2.7]. This section briefly recalls duadic codes and important properties of them.

Definition 2.2.1 [33, Section 2.7] Let S_1 and S_2 be unions of non-zero q-cyclotomic cosets modulo n such that

1. $0 \notin S_1 \cup S_2$
2. $S_1 \cup S_2 \cup \{0\} = \mathbb{Z}/n\mathbb{Z}$ and $S_1 \cap S_2 = \emptyset$,
3. there is a multiplier μ_b such that $\mu_b S_1 = S_2$ and $\mu_b S_2 = S_1$.

Then the pair $\{S_1, S_2\}$ is called a splitting of $\mathbb{Z}/n\mathbb{Z}$ given by μ_b over $\mathbb{F}_q$.

A vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ is called *even-like* provided that

$$\sum_{i=1}^{n} x_i = 0$$

and it is called *odd-like* otherwise. A linear code is called *even-like* if it has only even-like codewords; a linear code is called *odd-like* if it is not even-like. In the binary case an even-like code has only even weights.

Binary duadic codes were first introduced by Leon et al. [65], and later they were generalized to larger fields by Pless [79, 80].

Definition 2.2.2 (Duadic codes) [55, Theorem 6.1.5] [33, Section 2.7] Let $\{S_1, S_2\}$ be a splitting of $\mathbb{Z}/n\mathbb{Z}$ over $\mathbb{F}_q$. Then the linear cyclic codes with the defining sets $S_1 \cup \{0\}$ and $S_2 \cup \{0\}$ are called a pair of even-like duadic codes. The linear cyclic codes with the defining sets S_1 and S_2 are called a pair of odd-like duadic codes.

Let (S_1, S_2) be a *splitting* of $\mathbb{Z}/n\mathbb{Z}$ given by μ_b over $\mathbb{F}_q$ and (C_1, C_2) and (D_1, D_2) be pairs of even-like and odd-like duadic codes with the defining sets $(S_1 \cup \{0\}, S_2 \cup \{0\})$ and (S_1, S_2), respectively. Then $C_1 \subset D_1$ and $C_2 \subset D_2$. Also, one can easily see that $x-1$ divides the generator polynomials of C_1 and C_2. Thus if $a(x)$ is the polynomial representation of a vector $a \in C_1$ or $\mathcal{C}_2$, then $a(1)$, which is the sum of the coordinates of a, is zero. This explains why the codes C_1 and C_2 are even-like. A similar argument shows that the codes D_1 and D_2 are odd-like codes as $x-1$ does not divide the generator polynomials of these codes.

A comprehensive list of important properties of duadic codes is provided below.

Theorem 2.2.3 *[90, Theorem 3.1] [55, Theorems 4.3.17, 6.1.3, 6.4.2, 6.4.3] Let (C_1, C_2) and (D_1, D_2) be pairs of even-like and odd-like duadic codes of length n over $\mathbb{F}_q$, respectively, such that $C_1 \subseteq D_1$ and $C_2 \subseteq D_2$. Then*

1. *C_1 and C_2 (respectively D_1 and D_2) are permutation equivalent codes by Theorem* 1.6.4.

2. *$C_1 \cap C_2 = \{0\}$ and $C_1 + C_2$ is the cyclic code generated by $x - 1$.*

3. *$D_1 \cap D_2 = H$ and $D_1 + D_2 = \mathbb{F}_q^n$, where H is the subspace of $\mathbb{F}_q^n$ with all ones vector as a basis.*

4. $\dim C_1 = \dim C_2 = (n-1)/2$ *and* $\dim D_1 = \dim D_2 = (n+1)/2$.

5. *C_1 is the subcode of D_1 consisting of its even-like vectors. The same holds for C_2 as the subcode of D_2.*

6. *$D_1 = C_1 \oplus H$ and $D_2 = C_2 \oplus H$.*

7. *If C_1 is Hermitian self-orthogonal, then $C_1^{\perp_h} = D_1$ and $C_2^{\perp_h} = D_2$. Otherwise, $C_1^{\perp_h} = D_2$ and $C_2^{\perp_h} = D_1$.*

8. *If C_1 is Euclidean self-orthogonal, then $C_1^{\perp} = D_1$ and $C_2^{\perp} = D_2$. Otherwise, $C_1^{\perp} = D_2$ and $C_2^{\perp} = D_1$.*

The next natural question arising in this context is to see for what values of n duadic codes exist over $\mathbb{F}_q$. The answer to this problem, which depends on both n and q, is provided below.

Theorem 2.2.4 *[55, Theorem 6.3.2] The duadic codes of length n over $\mathbb{F}_q$ exist if and only if q is a square modulo n.*

Next, we present some results about self-orthogonal duadic codes with respect to both Euclidean and Hermitian inner products. Both proofs use the fact that if A is the defining set of a (Euclidean or Hermitian) self-orthogonal code, then $0 \in A$. The rest is applying Theorem 1.3.6 for the Euclidean inner product and Theorem 1.3.8 for the Hermitian inner product.

Theorem 2.2.5 *[55, Theorem 6.4.1] Let C be a linear cyclic code over $\mathbb{F}_q$ with parameters $[n, \frac{n-1}{2}]$. Then C is Euclidean self-orthogonal if and only if C is an even-like duadic code with the multiplier μ_{-1}.*

We deal only with Hermitian self-orthogonal duadic codes over $\mathbb{F}_4$ in this chapter. The Hermitian self-orthogonality condition for duadic codes over $\mathbb{F}_4$ is given below. A generalization of this result over an arbitrary field can be seen in [90, Theorem 4.4].

Theorem 2.2.6 *[55, Theorem 6.4.4] Let C be a linear cyclic code over $\mathbb{F}_4$ with parameters $[n, \frac{n-1}{2}]$. Then C is Hermitian self-orthogonal if and only if C is an even-like duadic code with the multiplier μ_{-2}.*

Example 2.2.7 Let $n = 9$. The 4-cyclotomic cosets modulo 9 are $\{0\}$, $\{1, 4, 7\}$, $\{2, 5, 8\}$, $\{3\}$, and $\{6\}$. One can easily verify that the pair (S_1, S_2), where $S_1 = \{1, 3, 4, 7\}$ and $S_2 = \{2, 5, 6, 8\}$ is a splitting of $\mathbb{Z}/9\mathbb{Z}$ given by μ_{-1}. Let D_1 and D_2 be odd-like duadic codes with the defining sets S_1 and S_2, respectively, and C_1 and C_2 with the defining sets $S_1' = \{0, 1, 3, 4, 7\}$ and $S_2' = \{0, 2, 5, 6, 8\}$, respectively, be even-like duadic codes. The pairs (C_1, C_2) and (D_1, D_2) are permutation equivalent by Theorem 2.2.3 part 1.

By Theorems 2.2.5 and 2.2.6, C_1 and C_2 are Euclidean self-orthogonal but not Hermitian self-orthogonal, and have parameters $[9, 4]$. Moreover, by Theorem 2.2.3, we have the following properties.

- $C_1^{\perp} = D_1$ and $C_2^{\perp} = D_2$.
- $C_1^{\perp_h} = D_2$ and $C_2^{\perp_h} = D_1$.

Now we briefly recall the class of quadratic residue codes which are special cases of duadic codes. Let p be an odd prime number. Let Q_p be the set of non-zero squares (quadratic residues) modulo p and N_p be the set of nonsquares (quadratic nonresidues) modulo p. The sets Q_p and N_p satisfy the following properties:

1. $|Q_p| = |N_p| = \frac{p-1}{2}$.

2. $aQ_p = Q_p$ and $aN_p = N_p$ for each $a \in Q_p$. Also, $bQ_p = N_p$ and $bN_p = Q_p$ for each $b \in N_p$.

If $q \in Q_p$ then each q-cyclotomic coset modulo p different from $\{0\}$ either is a subset of Q_p or is a subset of N_p. Thus Q_p and N_p give a splitting of $\mathbb{Z}/p\mathbb{Z}$ given by μ_b for each $b \in N_p$. The duadic codes corresponding to such a splitting are called *quadratic residue codes,* abbreviated *QR codes,* of length p over $\mathbb{F}_q$.

The following theorem discusses the existence and orthogonality conditions for the binary and quaternary QR codes.

Theorem 2.2.8 *[55, Theorem 6.6.6 and Exercise 365] Let p be a prime number. Then*

1. *Binary QR codes of length p exist if and only if $p \equiv \pm 1 \pmod 8$.*

2. *QR codes of length p over $\mathbb{F}_4$ exist for any p.*

3. *If $p \equiv 1 \pmod 8$, then the QR codes of length p over $\mathbb{F}_4$ and $\mathbb{F}_2$ have the same parameters.*

4. *Even-like QR codes of length p over $\mathbb{F}_4$ are Hermitian self-orthogonal if and only if $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$.*

Let $p \equiv \pm 1 \pmod 8$ and (C_1, C_2) and (D_1, D_2) be pairs of binary even-like and odd-like QR codes of length p, respectively, such that $C_1 \subseteq D_1$ and $C_2 \subseteq D_2$.

a. *If $p \equiv -1 \pmod 8$, then $C_1^{\perp} = D_1$ and $C_2^{\perp} = D_2$.*

b. *If $p \equiv 1 \pmod 8$, then $C_1^{\perp} = D_2$ and $C_2^{\perp} = D_1$.*

Other useful information about the QR codes is provided in Section 6.6 of [55].

Let D be an odd-like duadic code with the even-like subcode C over $\mathbb{F}_q$. The *minimum odd-like weight* of D is defined by

$$d_o = \min\{\mathrm{wt}(v) : v \in D \setminus C\}.$$

Several minimum distance conditions for duadic and QR codes are provided below. Let $d(C)$ denote the minimum distance of a code C.

Theorem 2.2.9 *[55, Theorems 6.5.2 and 6.6.22] Let D be an odd-like duadic code of length n over $\mathbb{F}_q$. Let d_o be the minimum odd-like weight of D. Then*

1. *$d_o^2 \geq n$.*

2. *If the splitting is given by μ_{-1}, then $d_o^2 - d_o + 1 \geq n$.*

3. *Furthermore, if n is a prime number and D is a QR code, then*

   a. $d(D) = d_o$.

   b. *If $q = 2$ and $n \equiv -1 \pmod 8$, then $d(D) \equiv 3 \pmod 4$.*

An extended version of this result is provided in [55, Theorems 6.5.2, 6.6.22]. In general, although the square root bound is a nice theoretical result, our computations given in Table 2.1 show that it does not provide a tight bound for the minimum distance.

We conclude this section with some useful information regarding when a splitting over $\mathbb{F}_4$ is given by μ_{-2}, or in other words when a duadic code over $\mathbb{F}_4$ is Hermitian self-orthogonal by Theorem 2.2.6.

Theorem 2.2.10 *[55, Theorems 6.4.9 and 6.4.10] Let p be an odd prime number.*

1. *If $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$, then every splitting of $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_4$ is given by μ_{-2}.*

2. *If $p \equiv 3 \pmod 8$, then there is no splitting of $\mathbb{Z}/p\mathbb{Z}$ given by μ_{-2} over $\mathbb{F}_4$.*

3. *If $p \equiv 1 \pmod 8$, then μ_{-2} may or may not give a splitting of $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_4$,*

Moreover, if μ_{-2} and μ_{-1} give the same splitting of $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_4$, then $p \equiv \pm 1 \pmod 8$. If $p \equiv -1 \pmod 8$, then μ_{-2} and μ_{-1} give the same splitting of $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{F}_4$.

2.3 A new class of 0-dimensional binary quantum codes

A 0-dimensional quantum code with length n has parameters $[\![n, 0, d]\!]$. Such a quantum code represents a single quantum state capable of correcting any $(d-1)/2$ errors. In practice, 0-dimensional quantum codes can be useful for example in testing whether certain storage locations for qubits are decohering faster than they should [20]. Moreover, higher-dimensional quantum codes can be constructed by applying Theorem 1.7.3 part 1 to a 0-dimensional quantum code.

Hermitian self-dual codes over $\mathbb{F}_4$ can be viewed as a family of 0-dimensional binary quantum codes. In general, self-dual codes are an important subclass of codes, both for practical purposes (some best-known codes are of this type), and theoretically, in view of their connections with other mathematical objects [4, 24, 76]. Classical self-dual codes have been studied a lot in the literature [18, 53, 83, 87]. Among all linear cyclic codes, quadratic residue (QR) codes have received the most attention for constructing self-dual codes. In this chapter, we go beyond only QR codes and systematically construct Hermitian self-dual codes from cyclic and duadic codes over $\mathbb{F}_4$ by adding certain coordinates to create longer codes. This observation opens up new applications for duadic codes, as they can be utilized to construct good Hermitian self-dual codes. Our novel constructions are likely to be of interest to classical coding theorists.

In this section, we provide a new infinite family of 0-dimensional quantum codes, which are also Hermitian self-dual linear codes over $\mathbb{F}_4$, using duadic codes over $\mathbb{F}_4$. Our construction targets nearly dual-containing duadic codes and also bounds the minimum distance of the constructed quantum code using minimum distances of an odd-like and an even-like duadic code. Throughout this section, n always is a positive odd integer. For each integer a such that $\gcd(a, n) = 1$, we denote the multiplicative order of a modulo n by $\mathrm{ord}_n(a)$.

Constructions of 1-dimensional quantum codes from duadic codes can be found in the literature. One such construction is provided below which is obtained by applying the CSS construction to binary duadic codes.

Theorem 2.3.1 *[3, Theorems 4 and 10] Let n be a positive odd integer. Then there exists a quantum code with parameters $[\![n, 1, d]\!]$, where $d^2 \geq n$. If $\mathrm{ord}_n(2)$ is odd, then $d^2 - d + 1 \geq n$.*

Moreover, Guenda in [46] proved that the distance bound $d^2 - d + 1 \geq n$ in Theorem 2.3.1 is still valid when $\mathrm{ord}_n(4)$ is odd. She also found the following new family of quantum codes when $\mathrm{ord}_n(4)$ is even.

Theorem 2.3.2 *[46, Theorem 16] Let $n = p^m$ be an odd prime power and $\mathrm{ord}_n(4)$ be even. Then there exists an $[\![n, 1, d]\!]$ quantum code with $d^2 \geq n$.*

For $u, v \in \mathbb{F}_4^n$ let $\langle u, v\rangle_h$ denote their Hermitian inner product. Let also $\|u\| = \langle u, u\rangle_h$. One can easily see that $\|u\| \equiv \mathrm{wt}(u) \pmod 2$. The next theorem gives some useful information about the weights in certain even-like and odd-like quaternary duadic codes.

Lemma 2.3.3 *Let n be a positive odd integer and C_o be an odd-like duadic code of length n with a multiplier μ_{-2} over $\mathbb{F}_4$. Let C_e be the Hermitian dual of the code C_o. Then all vectors in C_e have even weights and all vectors in $C_o \setminus C_e$ have odd weights.*

Proof. First note that since the multiplier is μ_{-2}, we have $C_e \subseteq C_o$. So C_e is Hermitian self-orthogonal and for each $v \in C_e$, we have $\|v\| = 0$. This proves the first part.

Let j be the all-ones vector of length n and H be the subspace spanned by j over $\mathbb{F}_4$. By Theorem 2.2.3 part 6, $C_o = C_e \oplus H$. Let $u + \alpha j$ be an arbitrary element of $C_o \setminus C_e$, where $u \in C_e$ and $0 \neq \alpha \in \mathbb{F}_4$. Then

$$\|u + \alpha j\| = \|u\| + \|\alpha j\| + \langle u, \alpha j\rangle_h + \langle \alpha j, u\rangle_h = 1.$$

Hence $u + \alpha j$ has an odd weight. □

Motivated by the construction of binary quantum codes given in Theorem 1.7.9, we define the dual-containment deficiency of linear codes below.

Definition 2.3.4 The *dual-containment deficiency* of a linear code C with respect to the Hermitian inner product is defined by $e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h})$.

In particular, we have $C^{\perp_h} \subseteq C$ if and only if $e = 0$. Next, we classify all the odd-like duadic codes having the dual-containment deficiency $e = 1$ with respect to the Hermitian inner product.

Theorem 2.3.5 *Let C be an odd-like duadic code. Then $C^{\perp_h}$ has the dual-containment deficiency $e = 1$ if and only if C has multiplier μ_{-2}.*

Proof. First suppose that μ_{-2} is a multiplier of C. Thus there exists a splitting of $\mathbb{Z}/n\mathbb{Z}$ given by μ_{-2} in the form (S_1, S_2) such that S_1 is the defining set of C. The code $C^{\perp_h}$ has the defining set $\mathbb{Z}/n\mathbb{Z} \setminus (-2S_1) = \mathbb{Z}/n\mathbb{Z} \setminus S_2 = S_1 \cup \{0\}$. Hence $C^{\perp_h}$ is the even-like duadic subcode of C. Moreover, $C^{\perp_h}$ has the dual-containment deficiency

$$e = \dim(C) - \dim(C \cap C^{\perp_h}) = 1.$$

Conversely let (S'_1, S'_2) be a splitting of $\mathbb{Z}/n\mathbb{Z}$ given by μ_a and C be an odd-like duadic code with the defining set S'_1. Assume that $C^{\perp_h}$ has the dual-containment deficiency $e = 1$. Then

$$\begin{aligned} e = \dim(C) - \dim(C \cap C^{\perp_h}) &= n - |S'_1| - \Big(n - |S'_1 \cup (\mathbb{Z}/n\mathbb{Z} \setminus (-2S'_1))|\Big) \\ &= |S'_1 \cup (\mathbb{Z}/n\mathbb{Z} \setminus (-2S'_1))| - |S'_1| = 1. \end{aligned} \tag{2.3.1}$$

Now if $-2S'_1 \neq S'_2$, then $\{0, s\} \subseteq \mathbb{Z}/n\mathbb{Z} \setminus (-2S'_1)$ for some $s \in S'_2$. Thus (2.3.1) implies that $e \geq 2$ which is a contradiction. Therefore, $-2S'_1 = S'_2$ and μ_{-2} is a multiplier of C. □

Next, we use the quantum code construction stated in Theorem 1.7.9 to construct a new family of 0-dimensional quantum codes. In particular, the quantum codes that we are constructing in this section are extended odd-like duadic codes. Later, in Section 2.4, we provide a generalization of our construction to each linear codes over $\mathbb{F}_4$. In spite of the known theoretical results on duadic codes and their extended codes, they are not computationally discussed much in the literature. For instance, in [55], the parameters of length n duadic codes over $\mathbb{F}_4$ are only stated for $n \leq 41$. Hence we take advantage of this opportunity and compute the parameters of good extended duadic codes for much larger lengths ($n \leq 241$).

Now, we state our main result of this section.

Theorem 2.3.6 *Let n be a positive odd integer and C_o be an odd-like duadic code of length n with the multiplier μ_{-2} over $\mathbb{F}_4$. Then there exists a binary quantum code with parameters $[\![n + 1, 0, d]\!]$, where*

1. *$d \geq \min\{d(C_e), d(C_o) + 1\}$, where C_e is the even-like subcode of C_o.*

2. *d is even.*

3. *If $d(C_o)$ is odd, then $d \geq \sqrt{n}+1$. Moreover, if also μ_{-1} is a multiplier for C_o, then $d^2 - 3(d-1) \geq n$.*

Proof. Let (S_1, S_2) be a splitting of $\mathbb{Z}/n\mathbb{Z}$ given by μ_{-2} over $\mathbb{F}_4$ and C_o and C_e be the odd-like and even-like duadic code with the defining sets S_1 and $S_1 \cup \{0\}$, respectively. By Theorem 2.3.5, the code C_e has the dual-containment deficiency $e = 1$.

The code C_e has parameters $[n, n - \frac{n+1}{2}]$. Now applying the quantum construction given in Theorem 1.7.9 to C_e results in an Hermitian self-dual linear code Q over $\mathbb{F}_4$ which is also a quantum code with parameters $[\![n+1, 0, d]\!]$, where $d \geq \min\{d(C_e), d(C_o)+1\}$. The facts that Q is linear and Hermitian self-dual imply that all weights in Q are even, as was shown in the proof of Lemma 2.3.3.

Note that Lemma 2.3.3 implies that if $d(C_o) = d_o$ is odd, then $d_o < d(C_e)$. Thus d_o satisfies the square root bound provided in Theorem 2.2.9. The facts that $d \geq d_o + 1$ and $d_o \geq \sqrt{n}$ show that $d \geq \sqrt{n} + 1$.

Finally, if the same splitting is given by μ_{-1} and $d(C_o) = d_o$ is odd, then by Theorem 2.2.9, $d_o^2 - d_o + 1 \geq n$. Now combining $d - 1 \geq d_o$ with the previous inequality gives the result. □

The lower bound that we provided in Part (1) of Theorem 2.3.6 appears to be very good and almost all of our computational results rely on this lower bound. Restricting the code lengths to prime numbers in the form $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$ leads to an infinite family of 0-dimensional quantum codes of length $p+1$.

Corollary 2.3.7 *Let p be a prime number such that $p \equiv -1 \pmod 8$ or $p \equiv -3 \pmod 8$. Then there exists a $[\![p+1, 0, d]\!]$ quantum code with an even minimum distance d and*

$$d \geq \min\{d(C_e), d(C_o)+1\},$$

where C_o is an odd-like duadic code of length p and C_e is the even-like subcode of C_o. If C_o is a QR code then $d \geq d(C_o)+1$. Finally, if C_o is a QR code, $p \equiv -1 \pmod 8$, and $d = d(C_o)+1$, then $d \equiv 0 \pmod 4$.

Proof. The first part follows from Theorems 2.3.6 and Theorem 2.2.10 part 1. If C_o is a QR code, then Theorem 2.2.9 part 3a implies that $d(C_o) = d_o$. Moreover, Theorem 2.3.3 implies that $d(C_o)$ is odd and $d(C_e)$ is even. Thus $d_o < d(C_e)$ and $d \geq \min\{d(C_e), d(C_o)+1\}$. This implies that $d \geq d_o + 1$. The last fact about the minimum distance follows from Theorem 2.2.9 part 3b which implies that $d(C_o) \equiv 3 \pmod 4$. □

Some of our record-breaking quantum codes presented in Table 2.1 are computed using the above construction.

Recall that the multiplicative order of a modulo n is denoted by $\mathrm{ord}_n(a)$. For each positive odd integer n, we have $\mathrm{ord}_n(4) \mid \mathrm{ord}_n(2)$ and if $\mathrm{ord}_n(2)$ is odd, then $\mathrm{ord}_n(4) =$

$\mathrm{ord}_n(2)$. In the latter case, the binary and quaternary cyclotomic cosets modulo n are the same. Thus the binary and quaternary duadic codes have the same defining sets. In this special case, the following result helps compute the minimum distance of quaternary duadic codes much faster by only using the binary duadic code with the same defining set.

Theorem 2.3.8 *[79, Theorem 4] Let C be a quaternary linear code of minimum distance d which is generated by a set of binary vectors. Then the binary linear code generated by the same set of generators has minimum distance d.*

Although Theorem 2.3.8 is stated for linear codes over $\mathbb{F}_4$, in general it holds for linear codes over each finite field extension of the binary field; see Theorem 3.8.8 of [55]. Next, we give a restriction of Theorem 1.7.9 to binary cyclic codes that satisfy Theorem 2.3.8. We denote the Euclidean dual of a binary code C by $C^{\perp}$.

Corollary 2.3.9 *Let n be a positive odd integer such that $\mathrm{ord}_n(4) = \mathrm{ord}_n(2)$. If C is an $[n, k]$ binary cyclic code and e is the dual-containment deficiency of C, then there exists a binary quantum code with parameters $[\![n + e, 2k - n + e, d]\!]$, where $d \geq min\{d(C), d(C + C^{\perp}) + 1\}$.*

Proof. First note that $e = n - k - \dim(C \cap C^{\perp})$. Moreover, since $\mathrm{ord}_n(4) = \mathrm{ord}_n(2)$, the 2-cyclotomic and 4-cyclotomic cosets are the same modulo n. Hence binary and quaternary cyclic codes of length n with a fixed defining set have the same dimension over $\mathbb{F}_2$ and $\mathbb{F}_4$, respectively. Let A be the defining set of C, and D be the linear cyclic code over $\mathbb{F}_4$ with the defining set A. Thus D is an $[n, k]$ linear code over $\mathbb{F}_4$. The defining set of $D^{\perp_h}$ is $\mathbb{Z}/n\mathbb{Z} \setminus ((-2A) \bmod n) = \mathbb{Z}/n\mathbb{Z} \setminus ((-A) \bmod n)$, where the last equality follows from the fact that $2A \equiv A \pmod{n}$. Hence $D^{\perp_h}$ and $C^{\perp}$ have the same defining sets. A similar argument shows that $C \cap C^{\perp}$ (respectively $C + C^{\perp}$) and $D \cap D^{\perp_h}$ (respectively $D + D^{\perp_h}$) have the same defining sets. Therefore, $\dim(C \cap C^{\perp}) = \dim(D \cap D^{\perp_h})$ as linear codes over $\mathbb{F}_2$ and $\mathbb{F}_4$, respectively. Finally, Theorem 2.3.8 implies that $d(C^{\perp}) = d(D^{\perp_h})$ and $d(C + C^{\perp}) = d(D + D^{\perp_h})$. Now the result follows by applying Theorem 1.7.9 to the code D. □

Another advantage of the above result is that binary duadic codes have been studied extensively in the literature. For instance, the exact or probable minimum distance of all binary duadic codes of length $n \leq 241$ is determined in [81, 95], and [55, Section 6.5].

2.4 A more general family of 0-dimensional quantum codes

In this section, we present a construction of binary quantum codes which is also a method of constructing Hermitian self-dual codes over $\mathbb{F}_4$. Our construction mainly targets linear codes C such that $C \subsetneq C^{\perp_h}$ as the main ingredients for the construction of Theorem 1.7.9. Note that duadic codes are a special class of algebraic codes that satisfy the previous condition. Therefore, the results regarding the minimum distance in Theorem 2.3.6 are stronger than those in the next theorem. We will provide three examples of record-breaking quantum codes obtained from nearly dual-containing linear codes over $\mathbb{F}_4$ with $e = 3$.

Theorem 2.4.1 *Let C be an $[n, k]$ linear code over $\mathbb{F}_4$ such that $C \subseteq C^{\perp_h}$. Then there exists a quantum code with parameters $[\![2(n-k), 0, d]\!]$, where d is even and $d \geq \min\{d(C), d(C^{\perp_h})+1\}$.*

Proof. We apply the result of Theorem 1.7.9 to the code C. First note that the code C has the dual-containment deficiency $e = n - k - \dim(C \cap C^{\perp_h}) = n - 2k$. Now, Theorem 1.7.9 implies the existence of $[\![2(n-k), 0, d]\!]$ quantum code which satisfies $d \geq \min\{d(C), d(C^{\perp_h})+1\}$. Such quantum code is also a Hermitian self-dual code over $\mathbb{F}_4$. Since Hermitian self-dual codes over $\mathbb{F}_4$ only have even weights, d is even. □

Note that although we only stated the result of Theorem 2.4.1 for quantum codes, this result also gives a construction for Hermitian self-dual codes over $\mathbb{F}_4$. In particular, the quantum code of Theorem 2.4.1 is also a $[2(n-k), n-k, d]$ Hermitian self-dual code over $\mathbb{F}_4$, where d is even and $d \geq \min\{d(C), d(C^{\perp_h})+1\}$. Theorem 2.4.1 implies the following secondary construction of quantum codes.

Corollary 2.4.2 *Let C be a linear code over $\mathbb{F}_4$ that gives rise to an $[\![n, 2k-n]\!]$ quantum code, where $2k > n$. Then there exists a quantum code with parameters $[\![2k, 0, d]\!]$, where d is even and $d \geq \min\{d(C^{\perp_h}), d(C)+1\}$.*

Proof. First note that by Theorem 1.7.1 C is an $[n, k]$ linear code over $\mathbb{F}_4$ and $C^{\perp_h} \subsetneq C$. Now applying Theorem 2.4.1 to the code $C^{\perp_h}$ implies the existence of a $[\![2k, 0, d]\!]$ quantum code such that d is even and $d \geq \min\{d(C^{\perp_h}), d(C)+1\}$. □

Example 2.4.3 The best-known quantum code with parameters $[\![93, 3, 21]\!]$ is in correspondence with a Hermitian dual-containing linear code C over $\mathbb{F}_4$. Then Corollary 2.4.2 implies the existence of a $[\![96, 0]\!]$ quantum code. Moreover, $d(C) = 21 < d(C^{\perp_h})$ since $C^{\perp_h} \subsetneq C$, and $C^{\perp_h}$ has an even weight. Hence there exists a *new quantum code* with parameters $[\![96, 0, 22]\!]$. The previous quantum codes with the same length and dimension had minimum distance 20.

Next, we apply Theorem 2.4.1 to the family of linear cyclic codes over $\mathbb{F}_4$.

Corollary 2.4.4 *Let n be a positive odd integer and C be a length n linear cyclic code over $\mathbb{F}_4$ with the defining set A. If $A \cap -2A = \emptyset$, then there exists a $[\![2(n-|A|), 0, d]\!]$ quantum code (respectively a $[2(n-|A|), n-|A|, d]$ Hermitian self-dual linear code over $\mathbb{F}_4$) such that d is even and $d \geq \min\{d(C^{\perp_h}), d(C)+1\}$.*

Proof. The condition $A \cap -2A = \emptyset$ implies that $C^{\perp_h} \subseteq C$. Moreover, $\dim(C^{\perp_h}) = |A|$. Now the result follows from applying Theorem 2.4.1 to the code $C^{\perp_h}$. □

Next, we provide two new binary quantum codes that were obtained from two linear cyclic codes with $e = 3$.

Example 2.4.5 Let $n = 141$ and $A = Z(2) \cup Z(3) \cup Z(10)$. Note that $-2A = Z(1) \cup Z(5) \cup Z(15)$ and therefore $A \cap -2A = \emptyset$. Moreover, $|A| = 69$. Thus Corollary 2.4.4 implies the existence of a quantum code with parameters $[\![144, 0, d]\!]$, where d is even and $d \geq \min\{d(C^{\perp_h}), d(C) + 1\}$. Moreover, the minimum distance computation in Magma [17] shows that $d(C^{\perp_h}) \geq 20$ and $d(C) + 1 \geq 19$. Hence there exists a *new quantum code* with parameters $[\![144, 0, d \geq 20]\!]$. The previous best binary quantum code with the same parameters had minimum distance 18.

Example 2.4.6 Let $n = 123$ and $A = Z(1) \cup Z(2) \cup Z(6) \cup Z(7) \cup Z(9) \cup Z(11)$. Note that $-2A = Z(43) \cup Z(23) \cup Z(3) \cup Z(19) \cup Z(18) \cup Z(14)$ and $A \cap -2A = \emptyset$. Moreover, $|A| = 60$. Thus by Corollary 2.4.4 there exists a quantum code with parameters $[\![126, 0, d]\!]$, where d is even and $d \geq \min\{d(C^{\perp_h}), d(C) + 1\}$. Moreover, our Magma [17] computation shows that $d(C^{\perp_h}) \geq 22$ and $d(C) + 1 \geq 21$. The fact that d is even and $d \geq 21$ implies that this quantum code has parameters $[\![126, 0, d \geq 22]\!]$ which is a *new quantum code*. The previous best quantum code with the same parameters had minimum distance 21.

2.5 Minimum distance bounds for cyclic codes using their fixed subcodes

In general, computing the true minimum distance for linear codes is NP-hard [104] and very difficult for linear codes with large lengths and dimensions. In [58], the authors used fixed subcode by the action of multipliers to find an upper bound (or even the exact value) for the minimum distance of certain linear cyclic codes. In this section, we develop the theory of fixed subcodes by the action of multipliers and determine a new minimum distance lower bound for linear cyclic codes over $\mathbb{F}_4$. Almost all the results of this section remain valid for linear cyclic codes over an arbitrary finite field. However, as our main goal is to construct new binary quantum codes in the next sections, we only state our results for linear cyclic codes over $\mathbb{F}_4$.

In the rest of this section, we assume that n is a positive odd integer. Let a be a positive integer such that $\gcd(n, a) = 1$. Then the multiplier μ_a acts naturally as a permutation on $\mathbb{F}_4^n$. In particular, let $\{e_i : 0 \leq i \leq n-1\}$ be the standard basis of $\mathbb{F}_4^n$. Then $\mu_a(e_i) = e_{ai}$ for each $0 \leq i \leq n-1$, where ai is computed modulo n. For each $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_4^n$, we define $\mu_a(x)$ accordingly as $\mu_a(x) = (y_0, y_1, \ldots, y_{n-1})$, where $y_i = x_{a^{-1}i}$ for each $0 \leq i \leq n-1$. We denote the matrix representation of μ_a by T_a. Let C be a length n linear cyclic code over $\mathbb{F}_4$ with the defining set A. The code $\mu_a(C)$ is also a linear cyclic code over $\mathbb{F}_4$ and it has defining set $a^{-1}A$.

Now we formally define fixed subcodes by the action of multipliers.

Definition 2.5.1 Let C be a length n linear cyclic code over $\mathbb{F}_4$. The space of all vectors $v \in C$ such that $\mu_a(v) = v$ is called the fixed subcode of C under the action of μ_a.

We denote the fixed subcode of a linear cyclic code C under the action of μ_a by C_a. The code C_a is a subcode of $C \cap \mu_a(C)$ and can be easily computed as

$$C_a = C \cap \{x \in \mathbb{F}_4^n : (T_a - I)x^T = 0\}.$$

Fixed subcodes of linear cyclic codes under the action of multipliers are especially important to bound the minimum distance of cyclic codes. First note that for each integer a such that $\gcd(n, a) = 1$, we have $C_a \subseteq C$. Therefore, $d(C) \leq d(C_a)$ which gives an upper bound for $d(C)$. Several of our minimum distance upper bounds in Table 2.1 are obtained using the minimum distance of fixed subcodes. Moreover, in the next proposition, we provide a lower bound for the minimum distance of linear cyclic codes over $\mathbb{F}_4$ using their fixed subcodes. A modification of this proof technique can be employed to demonstrate that the minimum distance bounds also hold for additive cyclic codes. Note also that in the reformulation for additive cyclic codes the assumptions have to change as there is no defining set for them.

Proposition 2.5.2 *Let $C \subseteq \mathbb{F}_4^n$ be a linear cyclic code of length n with the defining set A and a be a positive integer such that $aA = A$.*

1. *If $\operatorname{ord}_n(a) = 2$, then $d(C_a)/2 + 1 \leq d(C)$.*

2. *If $\operatorname{ord}_n(a) = i$, where $i > 1$ is an odd integer, then $(d(C_a) - 1)/i + 1 \leq d(C)$.*

Proof. Let $v = (v_0, v_1, \dots, v_{n-1})$ be a minimum weight vector in C. Since C is cyclic, without loss of generality, we assume that v_0 is non-zero. If $\mu_a(v) = v$, then $d(C) = d(C_a)$ which completes the proof.

1. Suppose that $\operatorname{ord}_n(a) = 2$ and $v + \mu_a(v) \neq 0$. From $aA = A$, we get that $\mu_a(C) = C$. Then $\mu_a(v + \mu_a(v)) = v + \mu_a(v)$ which implies that $v + \mu_a(v)$ is a non-zero element of C_a. Since both v and $\mu_a(v)$ have the same coordinates in the 0-th position we have $d(C_a) \leq \operatorname{wt}(v + \mu_a(v)) \leq 2d(C) - 2$. Hence $d(C_a)/2 + 1 \leq d(C)$.

2. Let $\operatorname{ord}_n(a) = i$, where $i > 1$ is an odd integer and $w = \sum_{j=0}^{i-1} \mu_{a^j}(v)$. Since i is odd, w is a non-zero vector (we have $w_0 = v_0 \neq 0$). Then $\mu_a(w) = w$ and therefore $w \in C_a$. Note also that $\operatorname{wt}(w) \leq i\operatorname{wt}(v) - (i-1) = i(\operatorname{wt}(v) - 1) + 1$ since each $\mu_{a^j}(v)$ has v_0 in the 0-th position. Thus, $d(C_a) \leq \operatorname{wt}(w) \leq i(d(C) - 1) + 1$ which implies that $(d(C_a) - 1)/i + 1 \leq d(C)$. □

Our computations in Magma [17] show that many linear cyclic codes satisfying the conditions of Proposition 2.5.2 part 1 have the same minimum distance as their fixed subcode by an order two multiplier. In particular, for each $a \in \mathbb{Z}/n\mathbb{Z}$ such that $\operatorname{ord}_n(a) = 2$, we computed the minimum distance of all non-trivial length n linear cyclic codes with $9 < n < 85$ over $\mathbb{F}_4$ satisfying the conditions of Proposition 2.5.2 part 1. Among 72417 non-trivial such linear cyclic codes, 70256 of them had the same minimum distance as their corresponding fixed subcode by the action of μ_a. The equality rate is about 97% for all these codes. In general, determining when a linear cyclic code and its fixed subcode by μ_{-1} have the same minimum distance looks an interesting and presumably a difficult question.

One application of Proposition 2.5.2 part 1 is provided below. In both of the following examples, the minimum distance of the fixed subcode was computed much faster, while the minimum distance computation for the original code required a much longer time. In particular, we found two new quantum codes after applying the minimum distance lower bound of Proposition 2.5.2. These codes will be explained in detail below.

Example 2.5.3 Let $n = 157$ and C_o be the odd-like QR code over $\mathbb{F}_4$ with the defining set $Z(1) \cup Z(3) \cup Z(9)$. By Corollary 2.3.7 there exists a quantum code Q with parameters $[\![158, 0, d]\!]$, where d is even and $d \geq d(C_o) + 1$.

The BCH and square root bounds give 7 and 12 as the minimum distance lower bounds for C_o. Next we use the result of Proposition 2.5.2 to find a sharper lower bound for $d(C_o)$. Note that $\mathrm{ord}_n(4) = 26$ and $4^{13} \equiv -1 \pmod{157}$, and we use the inequality $d((C_o)_{-1})/2 + 1 \leq d(C_o)$, where $(C_o)_{-1}$ is the fixed subcode of C_o by the action of multiplier μ_{-1}. Our computation done in Magma [17] shows that $d((C_o)_{-1}) = 36$. Hence $d(C_o) \geq 19$ and the fact that d is even shows that Q has parameters $[\![158, 0, d \geq 20]\!]$. Thus Q is a *new quantum code* with a better minimum distance in comparison with the previous best-known code with the same length and dimension in [43] which had minimum distance 19.

Example 2.5.4 Let $n = 181$ and C_o be the odd-like QR code of length n over $\mathbb{F}_4$ with the defining set $Z(1)$. Corollary 2.3.7 implies the existence of a quantum code Q with parameters $[\![182, 0, d]\!]$, where d is even and $d \geq d(C_o) + 1$.

The BCH and square root bounds give 7 and 14 as the minimum distance lower bounds for C_o. Note that $\mu_{-1}(C_o) = C_o$ and our computations in Magma [17] shows that the fixed subcode of C_o under the action of multiplier μ_{-1} has the minimum distance 37. Hence $d(C_o) \geq 19.5$ by Proposition 2.5.2 and the inequality $d \geq d(C_o) + 1$ implies that $d \geq 20.5$. The fact that d is even shows that Q has parameters $[\![182, 0, d \geq 22]\!]$. Thus Q is a *new quantum code* with a better minimum distance in comparison with the previous best-known code, which had minimum distance 21 in the code table [43].

Next we provide a connection between different fixed subcodes which also helps to relate the number of certain weight codewords in the original code and its fixed subcode.

Theorem 2.5.5 *Let $C \subseteq \mathbb{F}_4^n$ be a linear cyclic code of length n and a be a positive integer such that $\mathrm{ord}_n(a) = p$ is prime. Let A_t be the number of weight t codewords in C for each $0 \leq t \leq n$. Then the following statements hold.*

1. *$C_a = C_{a^j}$ for each $1 \leq j \leq p - 1$.*

2. *Assume $\mu_a(C) = C$ and $0 \leq t \leq n$. Then either C_a has a weight t codeword or $p \mid A_t$. In particular, either $d(C) = d(C_a)$ or $p \mid A_{d(C)}$.*

Proof. 1. Let $1 \leq j \leq p-1$. First note that if $v \in C_a$ then $\mu_{a^j}(v) = v$ and therefore $v \in C_{a^j}$. Hence $C_a \subseteq C_{a^j}$. Next since $\gcd(p, j) = 1$, we can find integers b and c such that $bp + cj = 1$. If $u \in C_{a^j}$, then

$$\mu_a(u) = (\mu_a)^{bp+cj}(u) = (\mu_a)^{bp}(\mu_a)^{cj}(u) = (\mu_{a^j})^c(u) = u.$$

Thus $C_{a^j} \subseteq C_a$ which implies that $C_a = C_{a^j}$ for each $1 \leq j \leq p-1$.

2. If $A_t = 0$ then the conclusion holds trivially. Otherwise, let v be a weight t vector in C. Then

- either $\mu_{a^j}(v) = v$ for all $1 \leq j \leq p-1$
- or $v, \mu_a(v), \ldots, \mu_{a^{p-1}}(v)$ are all different weight t codewords of C.

If the former happens for a weight t codeword of C, then C_a also has a weight t vector. Otherwise, we can partition all the weight t codewords of C into sets of size p in the form $\{v, \mu_a(v), \ldots, \mu_{a^{p-1}}(v)\}$. Thus $p \mid A_t$.

The last part follows by choosing $t = d(C)$. □

This result allows us to compute only certain fixed subcodes in order to find a tighter bound for the minimum distance of linear cyclic codes over $\mathbb{F}_4$. Next, we give a generalization of the result of Theorem 2.5.5 part 1.

Proposition 2.5.6 *Let C be a linear cyclic code of length n over $\mathbb{F}_4$ and $a \in \mathbb{Z}/n\mathbb{Z}$ such that $\gcd(n, a) = 1$ and $\text{ord}_n(a) = t$. Then for each $1 \leq s \leq t-1$ such that $\gcd(s, t) = 1$ we have $C_a = C_{a^s}$.*

Proof. Assume $x \in C_a$. Then $\mu_{a^s}(x) = (\mu_a)^s(x) = x$. Thus $C_a \subseteq C_{a^s}$. Conversely, let $x \in C_{a^s}$. Since $\gcd(s, t) = 1$, we can find an integer s' such that $ss' \equiv 1 \pmod{t}$. Hence

$$\mu_a(x) = \mu_{a^{ss'}} = (\mu_{a^s})^{s'}(x) = x.$$

This implies that $C_{a^s} \subseteq C_a$. Therefore $C_a = C_{a^s}$. □

Let C be a linear cyclic code of length n over $\mathbb{F}_4$. In general, if the group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic and $p \mid |(\mathbb{Z}/n\mathbb{Z})^*|$, then the code C_a for each order p element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is the same. Otherwise, there may exist $a, b \in \mathbb{Z}_n^*$ of the same order such that $C_a \neq C_b$.

Example 2.5.7 Let $n = 35$ and C be a length 35 cyclic code over $\mathbb{F}_4$ with the defining set $Z(0) \cup Z(6)$. Then

- $\mathrm{ord}_{35}(6) = \mathrm{ord}_{35}(29) = \mathrm{ord}_{35}(34) = 2$ and C_6, C_{29}, and C_{34} are pairwise different codes.
- $\mathrm{ord}_{35}(4) = \mathrm{ord}_{35}(19) = \mathrm{ord}_{35}(26) = 6$ and C_4, C_{19}, and C_{26} are pairwise different codes.

The following proposition gives a decomposition for certain fixed subcodes.

Proposition 2.5.8 *Let C be a linear cyclic code of length n over $\mathbb{F}_4$ and $a_i \in \mathbb{Z}/n\mathbb{Z}$ for $1 \leq i \leq r$ such that $\gcd(\mathrm{ord}_n(a_i), \mathrm{ord}_n(a_j)) = 1$ for each $1 \leq i \neq j \leq r$. Let $a = \prod_{i=1}^{r} a_i \bmod n$. Then $C_a = \bigcap_{i=1}^{r} C_{a_i}$.*

Proof. For each i let $\mathrm{ord}_n(a_i) = \alpha_i$. Assume that $x \in C_a$ and $1 \leq l \leq r$. By the definition of a, we can find an integer $1 \leq s \leq \prod_{i=1}^{r} \alpha_i$ such that $a^s \equiv a_l \pmod{n}$. Hence we have

$$x = \mu_a(x) = (\mu_a)^s(x) = \mu_{a^s}(x) = \mu_{a_l}(x) \in C_{a_l}.$$

This implies that $C_a \subseteq \bigcap_{i=1}^{r} C_{a_i}$. Conversely, let $x \in \bigcap_{i=1}^{r} C_{a_i}$. Then we have

$$\mu_a(x) = \mu_{\prod_{i=1}^{r} a_i}(x) = \mu_{a_r}\mu_{a_{r-1}} \cdots \mu_{a_2}\mu_{a_1}(x) = x.$$

Therefore, we have $\bigcap_{i=1}^{r} C_{a_i} \subseteq C_a$. This completes the proof. □

Next we provide another result that gives information about the possible weights of codewords in the fixed subcodes by the action of multipliers.

Proposition 2.5.9 *Let C be a linear cyclic code of length n over $\mathbb{F}_4$ and a be a positive integer such that $\gcd(n, a) = 1$. Let $\mu_a = \sigma_1\sigma_2 \cdots \sigma_r$ be the decomposition of μ_a as a product of disjoint cycles. Then for each $v \in C_a$, $\mathrm{wt}(v) = \sum_{j=1}^{r} a_j|\sigma_j|$, where $a_j \in \{0, 1\}$ for $1 \leq j \leq r$.*

Proof. Let $1 \leq j \leq r$ and $\sigma_j = (t_1 t_2 \cdots t_m)$. Then for each $v = (v_0, v_1, \ldots, v_{n-1}) \in C_a$, we have $v_{t_1} = v_{t_2} = \cdots = v_{t_m}$. Thus $\mathrm{wt}(v) = \sum_{j=1}^{r} a_j|\sigma_j|$, where $a_j \in \{0, 1\}$. □

For instance, let $n = 13$ and C be a cyclic code of length n over $\mathbb{F}_4$. Then

$$\mu_4 = (0)(1\ 4\ 3\ 12\ 9\ 10)(2\ 8\ 6\ 11\ 5\ 7)$$

and therefore the possible non-zero weights for codewords of C_4 are $\{1, 6, 7, 12, 13\}$.

2.6 Numerical results

The constructions given in Sections 2.3 and 2.4 lead to many new quantum codes with minimum distances much higher than the previously best-known codes. In some cases the increase is by as much as 10. Overall, the computation is easiest when the dual-containment deficiency parameter is $e = 1$. In fact, in this case we arrive at the extended duadic codes. However, we also get three record-breaking quantum codes when $e = 3$. So our construction goes beyond only the extended duadic codes.

Table 2.1 shows parameters of some good quantum codes. In the table, the first two columns show the length and the coset leaders (minimum elements of cyclotomic cosets contained in the defining set) of the cyclic code. The convention for the choice of the primitive n-th root of unity for construction of cyclic codes was explained in Remark 1.3.3. The third column records whether the original code is a QR code, duadic code, or some general cyclic code. This is indicated with QR, D, and C respectively.

In Table 2.1, we included the probable minimum distances (computed using probabilistic methods) provided in [55, Section 6.5] for duadic codes of lengths 217, 233, and 239. Note that the binary and quaternary generator polynomials remain the same for all these three codes. The probable minimum distance d for each of these values is denoted by d^{ap} in the table. All the other minimum distances given in the table are the true minimum distance obtained from the minimum distance lower bound of the related construction. Moreover, such minimum distances are either computed by the built-in minimum distance function in computer algebra system Magma [17] or a reference for them is provided in the source column.

When the exact value of the minimum distance is not known, its lower and upper bounds are separated by a dash. Some of the minimum distance upper bounds presented in Table 2.1 are computed using Magma [17] functions for attacking the McEliece cryptosystem. While these functions have not been widely utilized in the literature for this purpose, our example in Appendix B demonstrates their effectiveness in computation. Specifically, our computations indicate that these Magma functions can significantly reduce the computation of minimum distance upper bounds.

The "source" column in the table provides information about the result used to construct such a quantum code. We denote theorems, propositions, and corollaries by their first letter in this column.

Finally, the PMD column shows the minimum distance of previous best known quantum code of the same length and dimension as shown in [43]. In cases where our code listed in Table 2.1 has a strictly higher minimum distance than the previous best known quantum code, we list the distance of our code in boldface in the parameters column.

It should be noted that we can apply the secondary construction given in Theorem 1.7.3 part 3 to the codes listed in Table 2.1 and produce many more record-breaking codes. For instance:

- the quantum code $[\![224, 0, 32]\!]$ generates 9 new quantum codes with parameters $[\![224 - i, 0, 32 - i]\!]$ for each $1 \leq i \leq 9$.
- the quantum code $[\![200, 0, 32]\!]$ generates 7 new quantum codes with parameters $[\![200 - i, 0, 32 - i]\!]$ for each $1 \leq i \leq 7$.
- the quantum code $[\![240, 0, 32]\!]$ generates 6 new quantum codes with parameters $[\![240 - i, 0, 32 - i]\!]$ for each $1 \leq i \leq 6$.
- the quantum code $[\![192, 0, 28]\!]$ generates 5 new quantum codes with parameters $[\![192 - i, 0, 28 - i]\!]$ for each $1 \leq i \leq 5$.

The codes obtained from secondary constructions are not listed in Table 2.1.

Length	Coset Leaders	Type	Parameters	Source	PMD
$n = 5$	1	QR	$[\![6, 0, 4]\!]$	T2.3.8	4
$n = 7$	1	QR	$[\![8, 0, 4]\!]$	T2.3.8	4
$n = 13$	1	QR	$[\![14, 0, 6]\!]$	T2.3.8	6
$n = 17$	$1, 3$	D	$[\![18, 0, 8]\!]$	T2.3.8	8
$n = 23$	1	QR	$[\![24, 0, 8]\!]$	T2.3.8	8
$n = 29$	1	QR	$[\![30, 0, 12]\!]$	T2.3.8	12
$n = 31$	$1, 5, 7$	QR	$[\![32, 0, 8]\!]$	T2.3.8	10
$n = 37$	1	QR	$[\![38, 0, 12]\!]$	T2.3.8	12
$n = 41$	$1, 3$	D	$[\![42, 0, 12]\!]$	T2.3.8	12
$n = 47$	1	QR	$[\![48, 0, 12]\!]$	T2.3.8	14
$n = 53$	1	QR	$[\![54, 0, 16]\!]$	T2.3.8	16
$n = 61$	1	QR	$[\![62, 0, 18]\!]$	T2.3.8	18
$n = 71$	1	QR	$[\![72, 0, 12]\!]$	T2.3.8	18
$n = 79$	1	QR	$[\![80, 0, 16]\!]$	T2.3.8	20
$n = 89$	$1, 3, 5, 13$	D	$[\![90, 0, 12]\!]$	T2.3.8	20
$n = 93$	$1, 5, 9, 13, 17, 23,$ 33, 34, 45	C	$[\![96, 0, \mathbf{22}]\!]$	C2.4.4 (e=3)	20
$n = 97$	$1, 5$	D	$[\![98, 0, 18]\!]$	T2.3.8	22
$n = 101$	1	QR	$[\![102, 0, 22]\!]$	T2.3.8	22
$n = 103$	1	QR	$[\![104, 0, 20]\!]$	[55] & T2.3.8	20
$n = 109$	$1, 3, 9$	QR	$[\![110, 0, 22]\!]$	T2.3.8	26
$n = 113$	$1, 3, 9, 10$	D	$[\![114, 0, \mathbf{24}]\!]$	T2.3.8	18
$n = 119$	$1, 2, 3, 6, 7, 21, 51$	D	$[\![120, 0, \mathbf{20}]\!]$	T2.3.8	18
$n = 123$	$1, 2, 6, 7, 9, 11$	C	$[\![126, 0, \mathbf{22} - 24]\!]$	C2.4.4 (e=3)	21
$n = 127$	$1, 9, 11, 13, 15,$ 19, 21, 31, 47	QR	$[\![128, 0, 20]\!]$	[95] & T2.3.8	22
$n = 137$	$1, 3$	D	$[\![138, 0, \mathbf{20} - 32]\!]$	T2.3.8	18
$n = 141$	$2, 3, 10$	C	$[\![144, 0, \mathbf{20}]\!]$	C2.4.4 (e=3)	18
$n = 145$	$1, 3, 5, 7, 11, 29$	D	$[\![146, 0, 18 - 32]\!]$	T2.3.8	18
$n = 149$	1	QR	$[\![150, 0, 18 - 30]\!]$	T2.3.8	18
$n = 151$	$1, 3, 7, 11, 15$	D	$[\![152, 0, \mathbf{24}]\!]$	[38] & T2.3.8	18
$n = 155$	$1, 2, 3, 5, 6, 9, 11,$ $15, 25, 31$	D	$[\![156, 0, 18 - 20]\!]$	T2.3.8	18
$n = 157$	$1, 3, 9$	QR	$[\![158, 0, \mathbf{20} - 36]\!]$	T2.3.8 & P2.5.2	19
$n = 161$	$5, 11, 35, 69$	D	$[\![162, 0, 16]\!]$	T2.3.8	20
$n = 167$	1	QR	$[\![168, 0, \mathbf{24}]\!]$	[101] & T2.3.8	20
$n = 173$	1	QR	$[\![174, 0, 20 - 36]\!]$	T2.3.8 & P2.5.2	21
$n = 181$	1	QR	$[\![182, 0, \mathbf{22} - 38]\!]$	T2.3.8 & P2.5.2	21
$n = 185$	$2, 6, 10, 17, 19, 74$	D	$[\![186, 0, 18 - 26]\!]$	T2.3.8	22
$n = 191$	1	QR	$[\![192, 0, \mathbf{28}]\!]$	[97] & T2.3.8	22
$n = 193$	$1, 5$	D	$[\![194, 0, 20 - 42]\!]$	T2.3.8	22
$n = 197$	1	QR	$[\![198, 0, 22 - 40]\!]$	T2.3.8 & P2.5.2	22
$n = 199$	1	QR	$[\![200, 0, \mathbf{32}]\!]$	[97] & T2.3.8	22
$n = 203$	$2, 3, 7, 29$	D	$[\![204, 0, 14 - 24]\!]$	T2.3.8	22
$n = 205$	$1, 3, 5, 7, 9, 11, 15,$ $17, 21, 31, 41$	D	$[\![206, 0, 20 - 36]\!]$	T2.3.8 & P2.5.2	20
$n = 217$	Many codes	D	$[\![218, 0, \mathbf{24}^{\mathbf{ap}}]\!]$	[55] & T2.3.8	21
$n = 221$	$1, 2, 3, 5, 6, 9, 10,$ $13, 17, 18, 39$	D	$[\![222, 0, 14 - 36]\!]$	T2.3.8	20
$n = 223$	$1, 9, 19$	QR	$[\![224, 0, \mathbf{32}]\!]$	[57] & T2.3.8	21
$n = 229$	$1, 3, 5$	QR	$[\![230, 0, 14 - 48]\!]$	T2.3.8	22
$n = 233$	$1, 3, 7, 27$	D	$[\![234, 0, \mathbf{30}^{\mathbf{ap}}]\!]$	[55] & T 2.3.8	20
$n = 235$	$1, 2, 5, 47$	D	$[\![236, 0, 14 - 24]\!]$	T2.3.8	20
$n = 239$	1	QR	$[\![240, 0, \mathbf{32}^{\mathbf{ap}}]\!]$	[55] & T2.3.8	20
$n = 241$	$1, 3, 5, 7, 9, 11,$ $13, 21, 25, 35$	D	$[\![242, 0, 14 - 56]\!]$	T2.3.8	20

Table 2.1: Parameters of good 0-dimensional quantum codes.

Chapter 3

Additive twisted codes and new families of quantum codes

Let $\mathbb{F}_4$ be the finite field of four elements. Recall that each $\mathbb{F}_2$-linear subspace $C \subseteq \mathbb{F}_4^n$ is called an *additive* code over $\mathbb{F}_4$. Additive codes over $\mathbb{F}_4$ are especially important due to their application in the construction of quantum codes. The class of additive twisted codes is possibly the most developed family of additive codes. Many algebraic characteristics of twisted codes are analogous to those of linear cyclic codes. They were first introduced as a subclass of additive cyclic codes by Jürgen Bierbrauer and Yves Edel [36]. Twisted codes, like linear cyclic codes, are defined and constructed using (unique) defining sets, and the BCH minimum distance bound holds for them [36]. Moreover, several families and examples of good quantum codes are constructed using dual-containing twisted codes [13].

In spite of the mentioned remarkable properties of twisted codes, several questions regarding the structure of twisted codes still need to be answered. Let n be a positive integer such that $n \mid 2^r - 1$ for some positive integer r, and $\mathbb{F}_{2^r}$ be the field of 2^r elements. We define the surjective $\mathbb{F}_2$-linear map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2 \times \mathbb{F}_2$ by

$$\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)),$$

where $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Twisted codes are constructed by applying the projection map ϕ_γ to linear cyclic codes over $\mathbb{F}_{2^r}$. In this chapter, we greatly improve the theory of twisted codes and construct new families and many examples of record-breaking, and sometimes optimal, binary quantum codes. We provide new theoretical results regarding the minimum distance and equivalence of twisted codes. We also study twisted codes constructed using different values of γ by changing the projection map ϕ_γ. In particular, we show that changing the value of γ may produce twisted codes with better minimum distance.

The main condition of stabilizer formalism (Theorem 1.7.1) to constructing a binary quantum code is its dual-containing condition. In this chapter, we also give a novel construction of binary quantum codes by relaxing the dual-containing condition of stabilizer formalism. This approach expands the scope of available classical codes for constructing good quantum codes and demonstrates the value of considering codes beyond those that meet the dual-containment condition. This generalizes the quantum construction of Theorem 1.7.9 by allowing additive codes over $\mathbb{F}_4$ to be used in order to construct quantum codes. We also provide a lower bound for the minimum distance of a binary quantum code constructed using this new approach. Many of our new quantum codes rely on this construction.

This chapter is organized as follows. Section 3.1 summarizes our main contributions in this chapter. In Section 3.2, we give our new construction of binary quantum codes. Section 3.3 recalls a method of presenting linear cyclic codes, called the trace representation, which is different from the approach used in Section 1.3. Twisted codes and their properties are recalled in Section 3.4. In Section 3.5, by viewing each twisted code as a subgroup of a linear cyclic code, we present a novel perspective on twisted codes. We also introduce the dual-containment deficiency of twisted codes and give a construction of binary quantum codes using the family of nearly dual-containing twisted codes. New minimum distance bounds for twisted codes are provided in Section 3.6. Next, in Section 3.7, we construct infinite families of twisted codes with minimum distance at least five. In Section 3.8, we give new infinite families and several examples of record-breaking binary quantum codes. In Section 3.9, we prove that ten of our quantum codes are optimal. In Section 3.10, we give new results on twisted codes constructed using different γ values.

The material in this chapter is a joint work with my senior supervisor Dr. Lisoněk. A portion of materials in this section was also presented at the Mathematical Congress of the Americas (MCA 2021, Buenos Aires, Argentina) [28], and at the 3rd International Workshop on Boolean Functions and their Applications (BFA 2018, Loen, Norway) [67].

3.1 Our main contributions

To distinguish our novel results from the earlier works in the literature, we briefly outline our major contributions in this section. In Section 3.2, we give a new construction of binary quantum codes from an arbitrary given additive code over $\mathbb{F}_4$. Our construction (Theorem 3.2.3) relaxes the dual-containment condition required in stabilizer construction of quantum codes. Throughout this chapter, this construction will be applied to produce many record-breaking binary quantum codes.

In Section 3.5, we provide sufficient conditions for a twisted code to be a linear cyclic code over $\mathbb{F}_4$ (Theorem 3.5.1). We give a connection between codewords of a twisted code and vectors in a certain linear cyclic code (Theorem 3.5.3). This new approach provides a stronger connection between twisted codes and linear cyclic codes, enabling us to show that the sum and intersection of twisted codes follow the same rule as cyclic codes (Proposition 3.5.4). For each twisted code, we compute its dual-containment deficiency (Theorem 3.5.5).

As a result, we generate binary quantum codes from nearly dual-containing twisted codes (Theorem 3.5.7).

In Section 3.6, we provide a general minimum distance lower bound for twisted codes using minimum distance of linear cyclic codes (Corollary 3.6.3). We show that the well-known minimum distance lower bounds for linear cyclic codes such as Hartmann-Tzeng and Roos bound remain valid for twisted codes (Corollaries 3.6.5 and 3.6.6).

In Section 3.7, we first give a new sufficient condition for twisted codes to have minimum distance at least five (Theorem 3.7.2). The proof strategy for this result is independent of the conventional methods for the minimum distance bounds, such as the result presented in Section 3.6. Next, we construct two infinite families of additive twisted codes with minimum distance at least five.

In Section 3.8, we introduce a secondary construction of quantum codes (new code from a given quantum code) using the structure of twisted codes (Theorem 3.8.2). Five new infinite families of quantum codes are given (Theorems 3.8.4, 3.8.5, 3.8.9, and 3.8.11). We show that our constructions are capable of generating record-breaking and ten optimal binary quantum codes.

Surprisingly, the influence of γ value on the parameters of twisted codes has not been discussed in the literature. In Section 3.10, we first provide necessary and sufficient conditions for two values of γ to form twisted codes with the same length and dimension (Theorem 3.10.2). Next, we give a necessary condition for two values of γ to construct twisted codes with the same parameters (Theorem 3.10.5). We show that each twisted code has the same parameters as at least five other twisted codes by changing the value of γ (Theorem 3.10.6). Finally, through an example, we show that the minimum distance of twisted codes can be improved by varying the value of γ (Example 3.10.9).

In Section 3.10.1, we give a sufficient condition for two twisted codes with different values of γ and different complete defining sets to have the same parameters (Theorem 3.10.14). Combining this result with a result of Section 3.10 significantly decreases the bound on the number of twisted codes constructed using different values of γ (Corollary 3.10.16). Finally, a search algorithm for binary quantum codes from nearly dual-containing twisted codes is outlined.

3.2 New construction of binary quantum codes from nearly dual-containing additive codes over $\mathbb{F}_4$

Throughout this section, to avoid confusion, we denote the dimension of an additive code $C \subseteq \mathbb{F}_4^n$ by $\dim_{\mathbb{F}_2}(C)$. Recall that the trace inner product of u and $v \in \mathbb{F}_4^n$ is defined by

$$u * v = \operatorname{Tr}(u \cdot \overline{v}) = (u \cdot \overline{v}) + \overline{(u \cdot \overline{v})} = \sum_{i=1}^{n} (u_i \overline{v_i} + \overline{u_i} v_i),$$

where $\overline{a}$ is the conjugate of a. The dual of C with respect to the trace inner product is defined by

$$C^{\perp_t} = \{u \in \mathbb{F}_4^n : u * v = 0 \text{ for all } v \in C\}.$$

The dual-containment deficiency of additive code C is defined by

$$\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}).$$

It measures how close additive code C is from being dual-containing with respect to the trace inner product. For instance, we have $C^{\perp_t} \subseteq C$ if and only if the dual-containment deficiency of C is zero. Recall that, as we mentioned in Theorem 1.7.1, a binary quantum code can be constructed if there exists an additive code C over $\mathbb{F}_4$ such that $C^{\perp_t} \subseteq C$.

In this section, we propose a new method of constructing binary quantum codes from an arbitrary given additive code. Our construction targets additive codes which are not necessarily dual-containing with respect to the trace inner product. This allows a greater number of classical codes to be incorporated into the mathematical formalism of stabilizer codes. The length and dimension of the resulting binary quantum code are computed exactly in terms of the length and dimension of the initial additive code. Another interesting advantage of our construction is that it provides a minimum distance lower bound for the output quantum code using the minimum distances of the input additive code and a modified code of it. Theorem 1.7.9 outlines a technique for constructing quantum codes from linear codes over $\mathbb{F}_4$, which is similar to our approach. However, our method extends beyond this class of codes. As we will see in the rest of this chapter, our construction is capable of constructing many new record-breaking quantum codes from additive codes over $\mathbb{F}_4$.

Let $C \subseteq \mathbb{F}_4^n$ be an additive code and $\dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = r$. In the next theorem, we show that the dual-containment deficiency of C is always an even number. Furthermore, we find a basis for $C^{\perp_t}$ such that the first r vectors form a basis for $C \cap C^{\perp_t}$ and the rest of the vectors are paired in a way that non-orthogonal vectors occur only as the elements of a pair. The following lemma and its proof follow from the properties of symplectic bilinear forms. For more information about symplectic bilinear forms, one can see, for example, [12, pp. 284–285].

Lemma 3.2.1 *Let $C \subseteq \mathbb{F}_4^n$ be an additive code. Then $s = \dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t})$ is even. Moreover, if $\dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = r$ and $s = 2e$, then we can find a basis for $C^{\perp_t}$ in the form $\{V_1, V_2, \ldots, V_r, M_1, M_2, \ldots, M_{2e}\}$ such that*

1. *The set $\{V_1, V_2, \ldots, V_r\}$ forms a basis for $C \cap C^{\perp_t}$.*
2. *For all $1 \leq i, j \leq 2e$ we have $M_i * M_j = 1$ if and only if $(i, j) = (2t-1, 2t)$ for some $1 \leq t \leq e$.*

Proof. First note that for each vector $v \in \mathbb{F}_4^n$ we have $v * v = 0$. Let $\dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = r$, $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = s$, and $\{V_1, V_2, \ldots, V_r\}$ be a basis for $C \cap C^{\perp_t}$. We can extend this to a basis for $C^{\perp_t}$ over $\mathbb{F}_2$ in the form

$$B = \{V_1, V_2, \ldots, V_r, m_1, m_2, \ldots, m_s\},$$

where $m_1, m_2, \ldots, m_s$ are in $C^{\perp_t} \setminus C \cap C^{\perp_t}$. Since $m_1 \notin C \cap C^{\perp_t}$, there exists a vector m_i for some $2 \leq i \leq s$ such that $m_1 * m_i = 1$. Without loss of generality, we assume that $m_1 * m_2 = 1$. If there exists another m_j, where $3 \leq j \leq s$ and $m_1 * m_j = 1$, then we replace m_j with $m_j + m_2$. Also, if there exists a vector m_z for some $3 \leq z \leq s$ such that $m_2 * m_z = 1$, then we replace m_z with $m_z + m_1$. Now, after considering these changes, we replace the vectors $m_3, m_4, \ldots, m_s$ with $m'_3, m'_4, \ldots, m'_s$, where for each $3 \leq j \leq s$ we have

$$m'_j = \begin{cases} m_j & \text{if } m_j * m_1 = 0 \text{ and } m_j * m_2 = 0 \\ m_j + m_1 & \text{if } m_j * m_1 = 0 \text{ and } m_j * m_2 = 1 \\ m_j + m_2 & \text{if } m_j * m_1 = 1 \text{ and } m_j * m_2 = 0 \\ m_j + m_1 + m_2 & \text{if } m_j * m_1 = 1 \text{ and } m_j * m_2 = 1. \end{cases}$$

The new vectors have the property that $m_1 * m_2 = 1$, m_1 and m_2 are orthogonal to any other vector m'_j for each $3 \leq j \leq s$, and the set $\{V_1, V_2, \ldots, V_r, m_1, m_2, m'_3, \ldots, m'_s\}$ forms a basis for $C^{\perp_t}$. Next, we apply the same procedure to the vectors $m'_3, m'_4, \ldots, m'_s$. By repeating this process, we find vectors $M_1, M_2, \ldots, M_s$, where for each $1 \leq i \leq s/2$

a. $M_{2i-1} * M_{2i} = 1$

b. M_{2i-1} and M_{2i} are orthogonal to each other vector of $M_1, M_2, \ldots, M_s$, and

c. $\{V_1, V_2, \ldots, V_r, M_1, M_2, \ldots, M_s\}$ is a basis for $C^{\perp_t}$.

Now, toward a contradiction, let s be an odd integer. Then, according to the conditions (a) and (b) above, we have $M_s * M_i = 0$ for each $1 \leq i \leq s-1$. This implies that $M_s \in C \cap C^{\perp_t}$, which is a contradiction. Therefore, s is an even integer, say $s = 2e$ for some positive integer e. Finally, one can easily see that the set $\{V_1, V_2, \ldots, V_r, M_1, M_2, \ldots, M_{2e}\}$ forms a basis for $C^{\perp_t}$ and satisfies the conditions (1) and (2) of this lemma. □

We present our quantum construction in two steps. We first apply a lengthening method to transform a given additive code into a trace self-orthogonal additive code. Then, in the following theorem, we explain more details of our construction and compute the parameters of the output quantum code. The proofs provide an explicit construction for such quantum codes.

Lemma 3.2.2 *Let C be an additive code of length n over $\mathbb{F}_4$ such that $\dim_{\mathbb{F}_2}(C^{\perp_t}) = k$ and $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = 2e$. Then there exists an additive code D such that $D^{\perp_t} \subseteq D$ and $D^{\perp_t}$ has parameters $(n + e, 2^k)$.*

Proof. Let S be a generator matrix for $C^{\perp_t}$. We choose the rows of S to be the vectors $V_1, V_2, \ldots, V_r, M_1, M_2, \ldots, M_{2e}$, where they satisfy the conditions of Lemma 3.2.1. Let T be a $2e \times e$ matrix with the entries $T_{2j-1,j} = 1$, $T_{2j,j} = \omega$ for $1 \leq j \leq e$, and the other entries of T be all zero. Let G be a $k \times (n + e)$ matrix defined by

$$G = \begin{bmatrix} V_{r\times n} & 0_{r\times e} \\ M_{2e\times n} & T_{2e\times e} \end{bmatrix},$$

where the matrix V has the rows $V_1, V_2, \ldots, V_r$, the rows of M are $M_1, M_2, \ldots, M_{2e}$, and 0 is the zero matrix. Since rows of the matrix V form a basis for $C \cap C^{\perp_t}$, one can easily verify that each of the first r rows of G is orthogonal to all rows of G.

Moreover, both of the matrices M and T have the property that all pairs of rows in each of these matrices are orthogonal except pairs consisting of two consecutive rows in the positions $2i - 1$ and $2i$ for each $1 \leq i \leq e$. This implies that each two rows from the last $2e$ rows of the matrix G are orthogonal. Therefore, the matrix G is a generator matrix for an $(n + e, 2^k)$ trace self-orthogonal additive code. In particular, if D is the additive code that is trace orthogonal to the code generated by G, then we have $D^{\perp_t} \subseteq D$. □

In Lemma 3.2.2, we constructed a quantum code by lengthening a given additive code. The next theorem, which is our main result of this section, states the parameters of such binary quantum code using the initial additive code. For a given matrix M, we denote the rows of M by $r(M)$.

Theorem 3.2.3 *Let C be an $(n, 2^{n+k})$ additive code over $\mathbb{F}_4$ and $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = 2e$. Then we can construct an $[\![n + e, k + e, d]\!]$ binary quantum code, where*

$$d \geq \min\{d(C), d(C + C^{\perp_t}) + 1\}.$$

Moreover, if $d = \min\{d(C), d(C + C^{\perp_t}) + 1\}$, then the quantum code is pure.

Proof. Let C be an $(n, 2^{n+k})$ additive code and $\dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = r$. Then an easy computation shows that $2e = n - k - r$. Consider the matrix

$$G = \begin{bmatrix} V_{r\times n} & 0_{r\times e} \\ M_{2e\times n} & T_{2e\times e} \\ A_{n+k-r\times n} & 0_{n+k-r\times e} \end{bmatrix},$$

where $r(V)$ is a basis for $C \cap C^{\perp_t}$, $r(M) \cup r(V)$ is a basis for $C^{\perp_t}$, and $r(A) \cup r(V)$ is a basis for C. The matrix T has entries $T_{2j-1,j} = 1$, $T_{2j,j} = \omega$ for $1 \leq j \leq e$, and the other entries of T are zero. By Lemma 3.2.1, we can assume that rows of M are vectors $M_1, M_2, \ldots, M_{2e}$ such that the only non-orthogonal pairs of vectors of M are in the from (M_{2i-1}, M_{2i}) for each $1 \leq i \leq e$. Let E be the additive code generated by the matrix

$$S = \begin{bmatrix} V_{r\times n} & 0_{r\times e} \\ M_{2e\times n} & T_{2e\times e} \end{bmatrix}.$$

By the proof of Lemma 3.2.2, the additive code E is self-orthogonal. Also, it is easy to see that each row of S is orthogonal to each row of G. Moreover, $\dim_{\mathbb{F}_2}(E) = (n+e)-(k+e)$ and the row space of G has dimension $(n+e)+(k+e)$. Therefore G is a generator matrix for the code $E^{\perp_t}$ and $E \subseteq E^{\perp_t}$. Hence $E^{\perp_t}$ is an $(n+e, 2^{(n+e)+(k+e)})$ trace dual-containing code. According to Theorem 1.7.1, it follows that $E^{\perp_t}$ can be extended to form an $[\![n+e, k+e]\!]$ binary quantum code.

It only remains to prove the minimum distance bound for the quantum code $E^{\perp_t}$. Let $x = (x_1, x_2) \in E^{\perp_t}$ be an $\mathbb{F}_2$-linear combination of the rows of G, where $x_1 \in \mathbb{F}_4^n$ and $x_2 \in \mathbb{F}_4^e$. If no rows of M appear in the combination, then $\mathrm{wt}(x) \geq d(C)$. If some of the rows of M join the linear combination, then $\mathrm{wt}(x) \geq d(C + C^{\perp_t}) + 1$. Hence, the quantum code $E^{\perp_t}$ has minimum distance $d \geq d(E^{\perp_t}) \geq \min\{d(C), d(C + C^{\perp_t}) + 1\}$. Finally, if $d = d(E^{\perp_t}) = \min\{d(C), d(C + C^{\perp_t}) + 1\}$, then $E^{\perp_t}$ is a pure quantum code by the definition of purity. □

If an additive code C has the dual-containment deficiency $2e = 0$, then the above construction reproduces the result of Theorem 1.7.1. Our construction will be used frequently in the next sections, and many new record-breaking quantum codes will be provided as its application. The next example shows how to use this result.

Example 3.2.4 Let C be an $(5, 2^7)$ additive code over $\mathbb{F}_4$ for which

$$G = \begin{bmatrix} \omega & 0 & \omega & \omega & 0 \\ 1 & \omega & \omega & \omega^2 & 0 \\ 0 & 1 & \omega^2 & 1 & \omega^2 \end{bmatrix}$$

is a generator matrix for $C^{\perp_t}$. Our computation shows that the first row forms a basis for the code $C \cap C^{\perp_t}$. Hence $\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t}) = 2e = 2$. By the construction explained in the proof of Theorem 3.2.3, if we add the new column vector $[0, 1, \omega]^T$ to G, then the new matrix, namely

$$G' = \begin{bmatrix} \omega & 0 & \omega & \omega & 0 & 0 \\ 1 & \omega & \omega & \omega^2 & 0 & 1 \\ 0 & 1 & \omega^2 & 1 & \omega^2 & \omega \end{bmatrix},$$

is a generator matrix of a trace self-orthogonal additive code E. Then $E^{\perp_t}$ is a quantum code with parameters $[\![6, 3]\!]$. Moreover, our computation shows that $d(C) = 3$ and $d(C + C^{\perp_t}) = 1$. Therefore, $E^{\perp_t}$ is a $[\![6, 3, 2]\!]$ quantum code.

3.3 Trace representation of linear cyclic codes

In this section, we briefly recall a different method for the presentation of linear cyclic codes. This construction, which is known as the trace representation of linear cyclic codes in the literature, will help us to

- describe the construction of twisted codes in a very similar fashion, and
- depict the similarities between the twisted codes and linear cyclic codes.

Throughout this section, q is a prime power. Let $\mathbb{F}_{q^r}$ be the field of q^r elements for some positive integer r, and $s \mid r$. Then $\mathbb{F}_{q^s} \subseteq \mathbb{F}_{q^r}$. The map $\mathrm{Tr}^r_s : \mathbb{F}_{q^r} \to \mathbb{F}_{q^s}$ defined by $\mathrm{Tr}^r_s(x) = \sum_{i=0}^{\frac{r}{s}-1} x^{q^{is}}$ is called the *trace map* to the intermediate field $\mathbb{F}_{q^s}$. In Section 1.2, we recalled several secondary constructions of linear codes. The subfield code and trace code are two other secondary constructions of linear codes.

Definition 3.3.1 [12, Definition 12.10] Let C be a length n linear code over $\mathbb{F}_{q^r}$. The set

$$\mathrm{Tr}^r_1(C) = \{(\mathrm{Tr}^r_1(x_1), \mathrm{Tr}^r_1(x_2), \ldots, \mathrm{Tr}^r_1(x_n)) : (x_1, x_2, \ldots, x_n) \in C\}$$

is called the *trace code* of C which is a length n linear code over $\mathbb{F}_q$.

Definition 3.3.2 [12, Definition 12.12] Let C be a length n linear code over $\mathbb{F}_{q^r}$. The *subfield code* of C over $\mathbb{F}_q$, denoted by $C_{\mathbb{F}_q}$, is the length n linear code over $\mathbb{F}_q$ defined by

$$C_{\mathbb{F}_q} = \{(x_1, x_2, \ldots, x_n) \in C : x_i \in \mathbb{F}_q \text{ for all } 1 \leq i \leq n\}.$$

The following theorem of Delsarte [32] gives a dual relation between subfield subcodes and trace codes. This connection is independent of the choice of the inner product; however, to achieve our purpose, which is the construction of linear cyclic codes using the trace representation, we state this result using the Euclidean inner product. Recall that $C^{\perp}$ is the Euclidean dual of the linear code C.

Theorem 3.3.3 *[32] Let C be a length n linear code over $\mathbb{F}_{q^r}$. Then*

$$\left(\mathrm{Tr}^r_1(C)\right)^{\perp} = (C^{\perp})_{\mathbb{F}_q}.$$

In other words, if A and B are the families of linear codes over $\mathbb{F}_{q^r}$ and over $\mathbb{F}_q$, respectively, then the following diagram commutes

$$\begin{tikzcd} A \arrow[r, "\perp"] \arrow[d, "\mathrm{Tr}^r_1"] & A \arrow[d, "()_{\mathbb{F}_q}"] \\ B \arrow[r, "\perp"] & B \end{tikzcd}, \qquad (3.3.1)$$

where Tr_1^r, $(\,)_{\mathbb{F}_q}$, and $\perp$ are the trace, subfield, and dual operations on linear codes, respectively.

Another important family of linear codes, which plays a central role in this presentation of linear cyclic codes, is the family of Galois closed codes. Recall that the map $\sigma_q : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ defined by $\sigma_q(x) = x^q$ is a field automorphism of $\mathbb{F}_{q^r}$ known as the *Frobenius automorphism* of $\mathbb{F}_{q^r}$. It is well-known that the *Galois group* of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ is the cyclic group generated by σ_q, for example see [12, Definition 12.6]. For a length n linear code C over $\mathbb{F}_{q^r}$, we define

$$\sigma_q(C) = \{(\sigma_q(x_1), \sigma_q(x_2), \ldots, \sigma_q(x_n)) : (x_1, x_2, \ldots, x_n) \in C\}.$$

It is not difficult to see that the codes C and $\sigma_q(C)$ are both linear codes with the same length, dimension, and minimum distance.

Definition 3.3.4 [12, Definition 12.15] Let C be a linear code of length n over $\mathbb{F}_{q^r}$. The code C is called *Galois closed* over $\mathbb{F}_q$ if $C = \sigma_q(C)$.

Note that if C is a linear code defined over $\mathbb{F}_{q^r}$, which is Galois closed over $\mathbb{F}_q$, then $C^\perp$ is also Galois closed over $\mathbb{F}_q$. In general, Galois closed codes are very useful in the design and analysis of linear codes. The $\mathbb{F}_q$-*Galois closure* of linear code C, denoted by $\overline{C}$, is the smallest linear code containing C that is Galois closed over $\mathbb{F}_q$. The $\mathbb{F}_q$-Galois closure of C can be constructed using the vector space sum $\overline{C} = \sum_{i=0}^{r-1} \sigma_q^i(C)$. A short list of properties of Galois closed codes is presented below.

Theorem 3.3.5 *[12, Theorem 12.17] Let C be a linear code over $\mathbb{F}_{q^r}$ of length n that is Galois closed over $\mathbb{F}_q$. Then the following statements hold.*

1. $\mathrm{Tr}_1^r(C) = C_{\mathbb{F}_q}$.

2. *The codes C and $\mathrm{Tr}_1^r(C)$ have the same dimension (as codes over $\mathbb{F}_{q^r}$ and $\mathbb{F}_q$, respectively).*

3. *The codes C and $\mathrm{Tr}_1^r(C)$ have the same minimum distance.*

For the rest of this section, we assume that n is a positive integer such that $n \mid q^r - 1$. In other words, $\mathbb{F}_{q^r}$ contains all the n-th roots of unity. Hence the set of all the q^r-cyclotomic cosets modulo n is in the form of

$$\{\{a\} : a \in \mathbb{Z}/n\mathbb{Z}\}.$$

This implies that each subset of $\mathbb{Z}/n\mathbb{Z}$ is in fact the defining set for a length n linear cyclic code over $\mathbb{F}_{q^r}$. The latter does not necessarily hold for the length n linear cyclic code over $\mathbb{F}_q$ as the defining sets of such codes are unions of q-cyclotomic cosets modulo n.

Definition 3.3.6 Let $\alpha \in \mathbb{F}_{q^r}$ be a primitive n-th root of unity and $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We define $B(A)$ to be a matrix over $\mathbb{F}_{q^r}$ such that for each $i \in A$ and $0 \leq j \leq n-1$ the entry in the row i and column j is defined by α^{ij}.

For instance, if $A = \{i_1, i_2, \ldots, i_k\} \subseteq \mathbb{Z}/n\mathbb{Z}$, then

$$B(A) = \begin{bmatrix} 1 & \alpha^{i_1} & \alpha^{2i_1} & \cdots & \alpha^{(n-1)i_1} \\ 1 & \alpha^{i_2} & \alpha^{2i_2} & \cdots & \alpha^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{i_k} & \alpha^{2i_k} & \cdots & \alpha^{(n-1)i_k} \end{bmatrix}. \tag{3.3.2}$$

One can easily see that the matrix $B(A)$ has rank equal to $|A|$. Recall that, as we stated in (1.4.2), matrices of this type are (generalized) parity check matrices for linear cyclic codes. In particular, the matrix $B(A)$ is a parity check matrix for the length n linear cyclic code over $\mathbb{F}_{q^r}$ with the defining set A. Next, we need the following definition to connect the linear cyclic codes over $\mathbb{F}_{q^r}$ that are Galois closed over $\mathbb{F}_q$ and linear cyclic codes over $\mathbb{F}_q$.

Definition 3.3.7 [12, Definition 13.2] Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. The $\mathbb{F}_q$-*Galois closure* of the set A is defined to be the union of all the q-cyclotomic cosets modulo n that intersect A nontrivially.

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We denote the $\mathbb{F}_q$-Galois closure of A by $\tilde{A}$. Recall that G is the Galois group of $\mathbb{F}_{q^r}/\mathbb{F}_q$, and σ_q is a generator of G. Next, we briefly justify the above definition using the action of G on $\mathbb{Z}/n\mathbb{Z}$. The group G acts on $\mathbb{Z}/n\mathbb{Z}$ naturally by mapping (σ_q^i, a) to $aq^i \bmod n$. One can easily see that under this action $\mathrm{Orb}(a) = Z(a)$ (the q-cyclotomic coset of a modulo n) and $\tilde{A} = \bigcup\limits_{a \in A} \mathrm{Orb}(a)$.

In the rest of this chapter, we denote the linear cyclic code of length n over $\mathbb{F}_{q^r}$ with the defining set A by $C(A)$. The definition of $B(A)$ implies that $C(A)^\perp$ is the linear cyclic code generated by the matrix $B(A)$. Next, we show that $C(\tilde{A})^\perp$ is the $\mathbb{F}_q$-Galois closure of the code $C(A)^\perp$. For each $a \in A$, we define $v^a = (1, \alpha^a, \alpha^{2a}, \ldots, \alpha^{(n-1)a})$. Then

$$\sigma_q(v^a) = (\sigma_q(1), \sigma_q(\alpha^a), \sigma_q(\alpha^{2a}), \ldots, \sigma_q(\alpha^{(n-1)a})) = v^{aq}.$$

This implies that $C(A)^\perp \subseteq C(\tilde{A})^\perp \subseteq \overline{C(A)^\perp}$. Next, we show that $C(\tilde{A})^\perp$ is Galois closed over $\mathbb{F}_q$. Let $c = \sum\limits_{a \in \tilde{A}} c_a v^a \in C(\tilde{A})^\perp$, where $c_a \in \mathbb{F}_{q^r}$. Then

$$\sigma_q(c) = \sum_{a \in \tilde{A}} \sigma_q(c_a)\sigma_q(v^a) = \sum_{a \in \tilde{A}} c_a^q v^{qa} \in C(\tilde{A})^\perp.$$

Hence $C(\tilde{A})^\perp$ is Galois closed over $\mathbb{F}_q$. This shows that $C(\tilde{A})^\perp$ is the $\mathbb{F}_q$-Galois closure of the code $C(A)^\perp$.

Now we have all the necessary information to recall the trace representation of linear cyclic codes over $\mathbb{F}_q$. The following theorem and its proof are taken from Chapters 12 and 13 of [12], and we just summarize the important parts here.

Theorem 3.3.8 *[12] Let $n \mid q^r - 1$, $A \subseteq \mathbb{Z}/n\mathbb{Z}$, and C be linear cyclic code of length n over $\mathbb{F}_q$ with the defining set $\tilde{A}$. Then $C = \big(\mathrm{Tr}_1^r(C(\tilde{A})^\perp)\big)^\perp = \big(C(\tilde{A})\big)_{\mathbb{F}_q}$.*

Proof. As we mentioned in (1.4.2), the matrix $B(\tilde{A})$ is a generalized parity check matrix for C. Moreover, $B(\tilde{A})$ is also a generator matrix of $C(\tilde{A})^\perp$, which is a Galois closed code over $\mathbb{F}_q$. Hence the following diagram of Theorem 3.3.3 commutes.

$$\begin{tikzcd}
C(\tilde{A})^\perp \arrow[r, "\perp"] \arrow[d, "\mathrm{Tr}_1^r"] & C(\tilde{A}) \arrow[d, "(\ )_{\mathbb{F}_q}"] \\
\mathrm{Tr}_1^r(C(\tilde{A})^\perp) \arrow[r, "\perp"] & \big(C(\tilde{A})\big)_{\mathbb{F}_q}
\end{tikzcd} \quad . \tag{3.3.3}$$

Finally, the definition of generalized parity check matrices and the fact that $C(\tilde{A})$ is Galois closed over $\mathbb{F}_q$ imply that $C = \big(C(\tilde{A})\big)_{\mathbb{F}_q}$. □

Example 3.3.9 Let $n = 15$. Then $\mathbb{F}_{2^4}$ contains α, which is a primitive 15-th root of unity. Let $A = \{0, 1\} \subset \mathbb{Z}/15\mathbb{Z}$. The 2-cyclotomic cosets modulo 15 are $\{0\}$, $\{1, 2, 4, 8\}$, $\{3, 6, 9, 12\}$, $\{5, 10\}$, and $\{7, 11, 13, 14\}$. The $\mathbb{F}_q$-Galois closure of A is $\widetilde{A} = \{0, 1, 2, 4, 8\}$ and

$$B(\widetilde{A}) = \begin{bmatrix} 1 & \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ 1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{13} \\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{11} \\ 1 & \alpha^8 & \alpha & \cdots & \alpha^7 \end{bmatrix}$$

is the generator matrix of $C(\tilde{A})^\perp$. By Theorem 3.3.8, $\big(\mathrm{Tr}_1^r(C(\tilde{A})^\perp)\big)^\perp$ is the length 15 binary linear cyclic code with the defining set $\widetilde{A}$.

3.4 Additive twisted codes

This section recalls the construction and several properties of additive twisted codes. In this section, we mostly follow the approach developed in [13] and [12, Section 17.2]. Both of the mentioned references have a very dense representation of the results. Therefore, in the following pages, we add extra details by expanding the explanations. Another aim of this section is to separate the background from our new results about twisted codes that will appear in Sections 3.5–3.10. For the rest of this chapter, as our main objective is to construct good binary quantum codes, we only consider twisted codes over $\mathbb{F}_2 \times \mathbb{F}_2$. Almost all the results of this chapter remain valid for additive twisted codes over a more general finite field. At the end of this section, in Table 3.1, we give a list of notations that are used to describe the family of twisted codes. Understanding the table makes it easier to understand the results provided in the following sections.

Let n be a positive integer such that $n \mid 2^r - 1$ for some positive integer r, and $\mathbb{F}_{2^r}$ be the field of 2^r elements. Recall that the surjective $\mathbb{F}_2$-linear map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2 \times \mathbb{F}_2$ is defined by

$$\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)), \tag{3.4.1}$$

where $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Since $n \mid 2^r - 1$, the multiplicative group $\mathbb{F}_{2^r}^*$ contains all the n-th roots of unity, namely $W = \{1, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\}$, where α is a primitive n-th root of unity in $\mathbb{F}_{2^r}^*$. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Similar as previous section, we define $B(A)$ to be a matrix over $\mathbb{F}_{2^r}$, where its rows and columns are labelled by elements of A and W, respectively. In other words, the entry in the row j and the column α^i is defined by α^{ij}. Let $C(A)$ be the length n linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A. Then $B(A)$ is a generator matrix for the code $C(A)^\perp$. We define $\phi_\gamma(C(A)^\perp)$ to be the additive code

$$\phi_\gamma(C(A)^\perp) = \{\phi_\gamma(c) : c \in C(A)^\perp\}.$$

Let $v = (v_1, v_2, \ldots, v_n)$ be a vector in $C(A)^\perp$. We denote $\phi_\gamma(v) = ((v_{11}, v_{12}), \ldots, (v_{n1}, v_{n2}))$, where $v_{i1} = \mathrm{Tr}_1^r(v_i)$ and $v_{i2} = \mathrm{Tr}_1^r(\gamma v_i)$ for each $1 \leq i \leq n$.

Definition 3.4.1 Let $\langle , \rangle_s : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{F}_2$ be the nondegenerate symplectic $\mathbb{F}_2$-bilinear form defined by

$$\langle \Big((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2}) \Big), \Big((b_{11}, b_{12}), \ldots, (b_{n1}, b_{n2}) \Big) \rangle_s = \sum_{i=1}^{n} a_{i1} b_{i2} - a_{i2} b_{i1}. \tag{3.4.2}$$

Later, in Remark 3.4.3, we show that the above symplectic inner product is equivalent to the trace inner product defined in (1.7.1). Now we formally define twisted codes.

Definition 3.4.2 Let $n \mid 2^r - 1$ for some integer r and A be a subset of $\mathbb{Z}/n\mathbb{Z}$. The dual of the code $\phi_\gamma(C(A)^\perp)$ with respect to the symplectic inner product $\langle , \rangle_s$ is called a *twisted code* of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Such a twisted code will be denoted by $\mathscr{C}_\gamma(A)$. In other words,

$$\mathscr{C}_\gamma(A) = \big(\phi_\gamma(C(A)^\perp)\big)^{\perp_s}.$$

We will be able to simplify the above representation of $\mathscr{C}_\gamma(A)$ later in (3.4.8). In general, the set A in the above definition is not unique, that is, a twisted code can be constructed using different subsets of $\mathbb{Z}/n\mathbb{Z}$. We call the set A an *incomplete defining set* of $\mathscr{C}_\gamma(A)$, if there exists $A' \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $\mathscr{C}_\gamma(A) = \mathscr{C}_\gamma(A')$ and $A \subsetneq A'$. On the other hand, if for each $A' \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $\mathscr{C}_\gamma(A) = \mathscr{C}_\gamma(A')$ we have $A' \subseteq A$, then the set A will be called the *complete defining set* of $\mathscr{C}_\gamma(A)$. Later, in Definition 3.4.7, we give a unique complete defining set for each twisted code. In general, a linear cyclic code can be completely determined and also constructed only by knowing its defining set based on a fixed primitive root of unity. To construct a twisted code, beside fixing a primitive n-th root of unity, we need to know an (incomplete) defining set and also the value of γ. Hence to avoid representing different twisted codes by the same notation, we use both the set A and the value of γ in the notation of twisted codes.

In the literature, only twisted codes with various (incomplete) defining sets were investigated, and the fact that various values of γ can yield twisted codes with different minimum distances was disregarded. This was because the previous research was mainly based on lower bounds on the code's distance which are insensitive to the selection of γ. In Section 3.10, we study twisted codes constructed using various values of γ. We find example of twisted codes which are highly sensitive to the selection of γ.

In the next remark, we connect the twisted codes with additive code over $\mathbb{F}_4$.

Remark 3.4.3 Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the field of four elements and $\mathscr{C}_\gamma(A)$ be a length n twisted code over $\mathbb{F}_4$. The $\mathbb{F}_2$-linear map $\psi : \mathbb{F}_2^{2n} \to \mathbb{F}_4^n$ defined by

$$\psi((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})) = (a_{11}\omega + a_{12}\omega^2, a_{21}\omega + a_{22}\omega^2, \ldots, a_{n1}\omega + a_{n2}\omega^2) \qquad (3.4.3)$$

is a vector space isomorphism. So we can consider each twisted code of length n over $\mathbb{F}_4$ as an $\mathbb{F}_2$-linear subspace of $\mathbb{F}_4^n$ (an additive code over $\mathbb{F}_4$). Moreover, one can easily verify that for each $u = ((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2}))$ and $v = ((b_{11}, b_{12}), \ldots, (b_{n1}, b_{n2})) \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$, we have

$$\langle u, v\rangle_s = \sum_{i=1}^{n} a_{i1}b_{i2} - a_{i2}b_{i1} = \psi(u) * \psi(v), \qquad (3.4.4)$$

where $*$ is the trace inner product defined in (1.7.1). Therefore, there is an $\mathbb{F}_2$-linear isomorphism between $\mathbb{F}_2^{2n}$ and $\mathbb{F}_4^n$ that preserves the mentioned inner products. Hence the construction of quantum codes provided in Theorem 3.2.3 remains valid for twisted codes.

Hence twisted codes can be viewed as $\mathbb{F}_2$-linear codes over $\mathbb{F}_4$ using the above connection. However, we mostly consider them as additive codes over $\mathbb{F}_2 \times \mathbb{F}_2$. Both of the inner products $*$ and $\langle , \rangle_s$ are used in the literature for the construction of quantum codes, and the above remark explains the explicit relation between them.

Unlike in the case of linear cyclic codes, the ordering of the 2-cyclotomic cosets modulo n is important in the construction of twisted codes. As we will see, the definition of saturated and unsaturated intersections is sensitive to the ordering of cyclotomic cosets. Moreover, many of our theoretical results and key properties of twisted codes rely on these two concepts. Throughout this chapter, we always consider the 2-cyclotomic cosets of a modulo n with the following ordering

$$Z(a) = \{a, (2a) \bmod n, (2^2a) \bmod n, \ldots, (2^{s-1}a) \bmod n\},$$

for each $0 \le a \le n-1$, where s is the smallest positive integer such that $2^s a \equiv a \pmod{n}$. Recall that $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ is a fixed value. We denote $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$, which is an integer larger than one.

Definition 3.4.4 Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $a \in A$. If $\kappa \mid |Z(a)|$ and $\kappa \mid i-j$ for each $2^i a, 2^j a \in Z(a) \cap A$, then $Z(a) \cap A$ is called *unsaturated*. Otherwise, $Z(a) \cap A$ is called *saturated*.

Note that in the above definition, we do not compute the actual intersection $Z(a) \cap A$, and we just use it as a notation for saturated and unsaturated intersections. As we will see in the following example, $Z(a) \cap A$ can be both saturated and unsaturated depending on the value of κ.

Example 3.4.5 Let $n = 15$. The 2-cyclotomic cosets modulo 15 are $Z(0) = \{0\}$, $Z(1) = \{1, 2, 4, 8\}$, $Z(3) = \{3, 6, 12, 9\}$, $Z(5) = \{5, 10\}$, and $Z(7) = \{7, 14, 13, 11\}$. Note that $\gamma \in \mathbb{F}_{16} \setminus \mathbb{F}_2$. Hence, $\kappa \in \{2, 4\}$.

- Let $A = \{5\}$ and $\kappa = 4$. Then $Z(5) \cap A$ is saturated.
- Let $A = \{5\}$ and $\kappa = 2$. Then $Z(5) \cap A$ is unsaturated.
- Let $A = \{1, 4\}$ and $\kappa = 4$. Then $Z(1) \cap A$ is saturated.
- Let $A = \{1, 4\}$ and $\kappa = 2$. Then $Z(1) \cap A$ is unsaturated.

The intersection of the defining set of a binary linear cyclic code of length n with a 2-cyclotomic coset Z modulo n is either $\emptyset$ or Z. However, in the case of twisted codes, there is a third option, namely unsaturated intersection. Later, in Theorem 3.5.1, we will see that $\mathscr{C}_\gamma(A)$ is a linear cyclic code over $\mathbb{F}_4$ if there is no unsaturated intersection of cyclotomic cosets with A. Another important fact to remember is that the saturated and unsaturated intersections both depend on the value of κ, and therefore changing γ can turn an unsaturated intersection into a saturated intersection and vice versa.

3.4.1 Quantum codes from twisted codes

In the previous section, we introduced the family of twisted codes as images of certain linear cyclic codes under the map ϕ_γ. In this subsection, we give more information about the structure of twisted codes. In particular, we find the complete defining set for a twisted code and its symplectic dual. Then a formula for computing the dimension of twisted codes is provided. We also will see the application of twisted codes in the construction of binary quantum codes.

First, we discuss how to find the complete defining set of a twisted code and its symplectic dual. Recall that $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ is a fixed value, $\mathbb{F}_2 \subsetneq \mathbb{F}_2(\gamma) \subseteq \mathbb{F}_{2^r}$, and $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. Moreover, after Definition 3.3.7, we defined the action of G, the Galois group of $\mathbb{F}_{2^r}/\mathbb{F}_2$, on $\mathbb{Z}/n\mathbb{Z}$ by

$$(\sigma_2^i, a) \to aq^i \bmod n$$

for each $a \in \mathbb{Z}/n\mathbb{Z}$, where σ_2 is the Frobenius automorphism of $\mathbb{F}_{2^r}/\mathbb{F}_2$. Let H be the subgroup of G generated by σ_2^{κ} and δ be the restriction of the above action to the subgroup H. We denote the orbit of $a \in \mathbb{Z}/n\mathbb{Z}$ under the action δ by $\mathrm{Orb}_{\delta}(a)$. An easy computation shows that $\mathrm{Orb}_{\delta}(a) = \{a2^{\kappa i} : 0 \leq i \leq \frac{r}{\kappa} - 1\}$ if $\kappa \mid \mathbb{Z}(a)$, which is an unsaturated intersection. The intersection $\mathrm{Orb}_{\delta}(a) \cap Z(a)$ is maximal among unsaturated intersections as the value of κ is fixed. This implies that if $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and Z is a 2-cyclotomic coset modulo n such that $Z \cap A$ is unsaturated and $a \in Z \cap A$, then $A \subseteq \mathrm{Orb}_{\delta}(a)$. In this case, we define

$$(Z \cap A)^H = \mathrm{Orb}_{\delta}(a)$$

and we call it the H-orbit of $Z \cap A$. A natural generalization of this observation can be applied to maximize an incomplete defining set of a twisted code. In particular, for an arbitrary $A \subseteq \mathbb{Z}/n\mathbb{Z}$, we define

$$\tilde{A} = \bigcup_{Z\cap A\ \ sat} Z \quad \bigcup_{Z\cap A\ \ unsat} (Z \cap A)^H, \tag{3.4.5}$$

where the unions run over all different 2-cyclotomic cosets modulo n, and sat and unsat stand for saturated and unsaturated intersection, respectively. It is consistent with the notation used after Definition 3.3.7 for the linear cyclic codes. The next lemma shows that the set $\tilde{A}$ is the maximum cardinality (complete) defining set of a twisted code with an incomplete defining set A. This lemma also gives the complete defining set of $\phi_{\gamma}(C(A)^{\perp})$ which is the symplectic dual of $\mathscr{C}_{\gamma}(A)$.

Lemma 3.4.6 *[13] Let $n \mid 2^r - 1$ be a positive integer and $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Then $\mathscr{C}_{\gamma}(A) = \mathscr{C}_{\gamma}(\tilde{A})$. Moreover,*

$$\mathscr{C}_{\gamma}(A)^{\perp_s} = \phi_{\gamma}(C(A)^{\perp}) = \mathscr{C}_{\gamma}(A_d),$$

where

$$A_d = \bigcup_{Z\cap A=\emptyset} -Z \quad \bigcup_{Z\cap A\ \ unsat} -((Z \cap A)^H). \tag{3.4.6}$$

Finally, the set $\tilde{A}$ is the maximal cardinality subset of $\mathbb{Z}/n\mathbb{Z}$ such that $\mathscr{C}_{\gamma}(A) = \mathscr{C}_{\gamma}(\tilde{A})$.

Proof. The result follows from Lemma 3 of [13]. □

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. The above result implies that the following diagram commutes:

$$\begin{tikzcd}
C(A)^{\perp} \arrow[r, leftrightarrow, "(\,)_d"] \arrow[d, "\phi_{\gamma}"] & C(A_d)^{\perp} \arrow[d, "\phi_{\gamma}"] \\
\mathscr{C}_{\gamma}(A_d) \arrow[r, leftrightarrow, "\perp_s"] & \mathscr{C}_{\gamma}(A)
\end{tikzcd} . \tag{3.4.7}$$

This result, specifically the equality

$$\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp), \tag{3.4.8}$$

will be used very frequently in the rest of this chapter because it is simpler than the form provided in its original definition (Definition 3.4.2). The uniqueness of $\tilde{A}$ in the above lemma motivates us to define the complete defining set of a twisted code as follows.

Definition 3.4.7 Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. The set $\tilde{A}$ defined in (3.4.5) is called the *complete defining set* of twisted code $\mathscr{C}_\gamma(A)$.

The set A_d defined above is also the complete defining set of the code $\mathscr{C}_\gamma(A)^{\perp_s}$. From now on, we reserve the symbol A_d for the complete defining set of $\mathscr{C}_\gamma(A)^{\perp_s}$. By Lemma 3.4.6, the twisted code $\mathscr{C}_\gamma(A)$ has the complete defining set $\tilde{A}$, and its symplectic dual is the code $\mathscr{C}_\gamma(A_d)$. The following theorem computes the dimension of twisted codes.

Theorem 3.4.8 *[13, Theorem 5] Let $n \mid 2^r - 1$ be a positive integer and $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Then the $\mathbb{F}_2$-dimension of $\mathscr{C}_\gamma(A)$ is $\sum_Z c_Z(A)$, where the sum runs over all 2-cyclotomic cosets modulo n and*

$$c_Z(A) = \begin{cases} 2|Z| & \text{if } Z \cap A = \emptyset \\ |Z| & \text{if } Z \cap A \text{ is unsaturated} \\ 0 & \text{if } Z \cap A \text{ is saturated.} \end{cases}$$

So far, we have discussed many similarities between twisted codes and linear cyclic codes. Next, we show that twisted codes are closed under cyclic shifts. Let $\mathscr{C}_\gamma(A)$ be a twisted code with the complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$. By (3.4.7), we have

$$\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp) = \{(\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)) : x \in C(A_d)^\perp\}. \tag{3.4.9}$$

Recall that $C(A_d)^\perp$ is a linear cyclic code over $\mathbb{F}_{2^r}$. Thus (3.4.9) implies that that $\mathscr{C}_\gamma(A)$ is a cyclic code.

Next, we discuss a necessary and sufficient condition for the dual-containment of twisted codes. Here we first introduce a concept that improves the representation of dual-containing twisted codes.

Definition 3.4.9 Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a length n twisted code. For each 2-cyclotomic coset Z modulo n, we call the intersection $Z \cap A$ *purely unsaturated* if $(-Z) \cap A$ and $Z \cap A$ are both unsaturated and $Z \cap A = -((-Z) \cap A)$.

Note that if $Z \cap A$ is purely unsaturated, then $(-Z) \cap A$ is also purely unsaturated.

Example 3.4.10 Let $n = 63$ and $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 2$. The ordered 2-cyclotomic cosets of 1 and -1 modulo 63 are $Z(1) = \{1, 2, 4, 8, 16, 32\}$ and $Z(-1) = \{62, 61, 59, 55, 47, 31\}$, respectively.

1. Let $A = \{1, 4, 16, 47, 59, 62\}$. Obviously, A is a complete defining set and

   $$Z(1) \cap A = \{1, 4, 16\} = -\{62, 59, 47\} = -(-Z(1) \cap A).$$

   Therefore, $Z(1) \cap A$ is purely unsaturated.

2. Let $B = \{1, 4, 16, 61, 55, 31\}$, which is the complete defining set of a twisted code. Then $Z(1) \cap B$ and $-Z(1) \cap B$ are both unsaturated. However,

   $$\{1, 4, 16\} = Z(1) \cap B \neq -(-Z(1) \cap B) = \emptyset.$$

   Thus $Z(1) \cap B$ is not purely unsaturated.

The next theorem gives a necessary and sufficient condition for the dual-containment of twisted codes using purely unsaturated intersections.

Theorem 3.4.11 *[13] Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then $\mathscr{C}_\gamma(A)^{\perp_s} \subseteq \mathscr{C}_\gamma(A)$ if and only if every 2-cyclotomic coset Z modulo n such that $A \cap Z \neq \emptyset$ satisfies exactly one of the following conditions.*

i. $Z \cap A$ *is purely unsaturated.*

ii. $(-Z) \cap A = \emptyset$.

Proof. The proof follows from [13, Theorem 6]. □

The above result was first stated in Theorem 6 of [13] with a small error in its reformulation, which was acknowledged in the pdf file provided at Yves Edel's home page [35]. The error caused certain dual-containing twisted codes to not be detected by the given criteria. In particular, the last line of Theorem 6 of [13] should be: (equivalently: $(-Z) \cap A = \emptyset$ or $(Z \cap A)^H = -(((-Z) \cap A)^H)$).

Let A_1 and A_2 be the complete defining sets of two additive twisted codes. Then the definition of twisted codes, Definition 3.4.2, implies that $\mathscr{C}_\gamma(A_2) \subseteq \mathscr{C}_\gamma(A_1)$ if and only if $A_1 \subseteq A_2$. This observation now implies that $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$ if and only if $A \subseteq A_d$. The following theorem gives the connection between binary quantum codes and dual-containing twisted codes.

Theorem 3.4.12 *Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that $A \subseteq A_d$. Then there exists a binary quantum code with parameters $[\![n, k, d]\!]$, where $\dim(\mathscr{C}_\gamma(A)) = n + k$ and $d(\mathscr{C}_\gamma(A)) = d$.*

Proof. First note that the condition $A \subseteq A_d$ implies that $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$. Now the proof follows from applying Theorem 1.7.1 to the code $\mathscr{C}_\gamma(A)$. □

We finish this section by giving a connection between twisted codes and certain Galois closed codes. Many of our results in Section 3.5 rely on the details provided below. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Recall that $C(A)$ is the linear cyclic code of length n over $\mathbb{F}_{2^r}$ with the defining set A.

Definition 3.4.13 Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We define $D(A) \subseteq \mathbb{F}_{2^r}^{2n}$ to be the $\mathbb{F}_2$-Galois closure of the $\mathbb{F}_{2^r}$-linear code

$$(C(A)^{\perp}, \gamma C(A)^{\perp}) = \{((x_1, \gamma x_1), (x_2, \gamma x_2), \ldots, (x_n, \gamma x_n)) : (x_1, x_2, \ldots, x_n) \in C(A)^{\perp}\}. \tag{3.4.10}$$

The fact that $D(A)$ is Galois closed over $\mathbb{F}_2$ implies that

$$\mathscr{C}_\gamma(A_d) = \mathscr{C}_\gamma(A)^{\perp_s} = \phi_\gamma(C(A)^{\perp}) = \mathrm{Tr}_1^r((C(A)^{\perp}, \gamma C(A)^{\perp})) = \mathrm{Tr}_1^r(D(A)). \tag{3.4.11}$$

Let $P_n = \mathbb{F}_{2^r}[x]/\langle x^n - 1\rangle$. For each 2-cyclotomic coset Z modulo n, we define

$$\rho(Z) = \{\sum_{i \in Z} a_i x^i : a_i \in \mathbb{F}_{2^r}\}.$$

The $\mathbb{F}_{2^r}$-linear vector space $P_n \times P_n$ can be decomposed as

$$P_n \times P_n = \bigoplus_Z (P_n \times P_n)_Z, \tag{3.4.12}$$

where the direct sum runs over all different 2-cyclotomic cosets modulo n and

$$(P_n \times P_n)_Z = \{(p(x), q(x)) : p(x), q(x) \in \rho(Z)\}. \tag{3.4.13}$$

The set $(P_n \times P_n)_Z$ is a subspace of $P_n \times P_n$ and has dimension $2|Z|$ over $\mathbb{F}_{2^r}$. Recall that α is a primitive n-th root of unity in $\mathbb{F}_{2^r}$. The map $\theta : P_n \to \mathbb{F}_{2^r}^n$ defined by $\theta(p(x)) = (p(\alpha^0), p(\alpha^1), \ldots, p(\alpha^{n-1}))$ is an $\mathbb{F}_{2^r}$-linear isomorphism. Hence the map $\theta' : P_n \times P_n \to \mathbb{F}_{2^r}^n \times \mathbb{F}_{2^r}^n$ defined by $\theta'(p(x), q(x)) = \big(\theta(p(x)), \theta(q(x))\big)$ is also an $\mathbb{F}_{2^r}$-linear isomorphism. Let

$$D_Z(A) = \theta'^{-1}(D(A)) \cap (P_n \times P_n)_Z. \tag{3.4.14}$$

The set $D_Z(A)$ gives the polynomial representation of vectors of a twisted code inside each $(P_n \times P_n)_Z$. One can obtain the polynomial representation of a twisted code by computing

$$\bigoplus_Z D_Z(A),$$

where the sum runs over all the cyclotomic cosets. The next proposition computes $D_Z(A)$ for each cyclotomic coset Z. This result will be applied later in Section 3.5 to classify nearly dual-containing twisted codes. The reason for stating this result early is to separate our new results in the upcoming sections from the works done in the literature.

Proposition 3.4.14 *[13] Let n be a positive integer such that $n \mid 2^r - 1$, and $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Let Z be a 2-cyclotomic coset modulo n and $|Z| = s$. Then the following results hold.*

i. $Z \cap A = \emptyset$ if and only if $D_Z(A) = \{(0,0)\}$.

ii. $Z \cap A$ is saturated if and only if $D_Z(A) = (P_n \times P_n)_Z$.

iii. $Z \cap A$ is unsaturated and $a \in Z \cap A$ if and only if $\{(x^{2^i a}, \gamma^{2^i} x^{2^i a}) : i = 0, 1, \ldots, s-1\}$ forms a basis for $D_Z(A)$ over $\mathbb{F}_{2^r}$.

Proof. The result follows from the proof of Lemma 1 and 2 of [13], and we only give the main idea below. Let $a \in Z \cap A$. Then $(x^a, \gamma x^a) \in D_Z(A)$. Since $D_Z(A)$ is Galois closed over $\mathbb{F}_2$, $D_Z(A)$ contains all the vectors in the form $(x^a, \gamma x^a)^{2^i} = (x^{2^i a}, \gamma^{2^i} x^{2^i a})$ for $i = 0, 1, \ldots, s-1$. Finding all such vectors allows us to form a basis for $D_Z(A)$ over $\mathbb{F}_{2^r}$. For instance, if $\kappa \nmid s$, then $(x^a, \gamma x^a)^{2^s} = (x^a, \gamma^{2^s} x^a)$ and $(x^a, \gamma x^a) \in D_Z(A)$. Since $\gamma \neq \gamma^{2^s}$, we have $(x^a, 0)$ and $(0, x^a)$ are two linear combination of the mentioned vectors. Now, it is easy to see that $D_Z(A) = (P_n \times P_n)_Z$. The proof for the other cases follows similarly. □

In summary, $D(A)$ is a Galois closed code over $\mathbb{F}_2$ such that $\mathrm{Tr}_1^r(D(A)) = \mathscr{C}_\gamma(A)^{\perp_s}$. A basis for the code $D(A)$ can be computed using the Proposition 3.4.14 and the fact that $D(A) = \bigoplus_Z \theta'(D_Z(A))$. One application of the above information about the code $D(A)$ is that it helps to compute the dual-containment deficiency of twisted codes, which is discussed in Proposition 3.5.5.

In this section, we used various notations to introduce the twisted codes and their properties. Table 3.1 below summarizes the important notations that will be used frequently in the rest of this chapter. Understanding the table facilitates the understanding of our upcoming results.

3.5 Nearly dual-containing twisted codes

In the previous section, we recalled the preliminary results about twisted codes. Throughout the remaining sections of this chapter, we present our new results on twisted codes. In this section, we identify nearly dual-containing twisted codes, which are the main ingredients for applying the quantum construction of Theorem 3.2.3. In Theorem 3.5.3, we give a connection between the weight of vectors in the codes $\mathscr{C}_\gamma(A)$ and $C(A)$. By employing this new approach, we establish a more powerful connection between twisted codes and linear cyclic codes. This allows us to compute the complete defining set of the sum and intersection of two twisted codes. We also give sufficient conditions for a twisted code to be linear over $\mathbb{F}_4$.

Indices	Description
$\mathbb{F}_{2^r}$	finite field of 2^r elements
n	a positive integer such that $n \mid 2^r - 1$
α	a primitive n-th root of unity in $\mathbb{F}_{2^r}$
γ	$\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$
κ	degree of the field extension $[\mathbb{F}_2(\gamma) : \mathbb{F}_2]$
ϕ_γ	$\mathbb{F}_2$-linear map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2 \times \mathbb{F}_2$ is defined by $\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x))$
$C(A)$	linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A
$\mathscr{C}_\gamma(A)$	twisted code over $\mathbb{F}_2 \times \mathbb{F}_2$ with an (incomplete) defining set A defined by $\mathscr{C}_\gamma(A) = \left(\phi_\gamma(C(A)^\perp)\right)^{\perp_s} = \phi_\gamma(C(A_d)^\perp)$
$\tilde{A}$	the complete defining set of twisted code $\mathscr{C}_\gamma(A)$ over $\mathbb{F}_2 \times \mathbb{F}_2$ (see (3.4.5))
A_d	the complete defining set of twisted code $\mathscr{C}_\gamma(A)^{\perp_s}$ over $\mathbb{F}_2 \times \mathbb{F}_2$ (see (3.4.6))
P_n	$P_n = \mathbb{F}_{2^r}[x]/\langle x^n - 1\rangle$
$\rho(Z)$	$\rho(Z) = \{\sum\limits_{i \in Z} a_i x^i : a_i \in \mathbb{F}_{2^r}\}$ for each 2-cyclotomic coset Z modulo n
θ	$\theta : P_n \to \mathbb{F}_{2^r}^n$ is defined by $\theta(p(x)) = (p(\alpha^0), p(\alpha^1), \ldots, p(\alpha^{n-1}))$
θ'	$\theta' : P_n \times P_n \to \mathbb{F}_{2^r}^n \times \mathbb{F}_{2^r}^n$ defined by $\theta'(p(x), q(x)) = (\theta(p(x)), \theta(q(x)))$
$D(A)$	$\mathbb{F}_2$-Galois closure of the $\mathbb{F}_{2^r}$-linear code $(C(A)^\perp, \gamma C(A)^\perp)$ (see (3.4.10))
$(P_n \times P_n)_Z$	$(P_n \times P_n)_Z = \{(p(x), q(x)) : p(x), q(x) \in \rho(Z)\}$
$D_Z(A)$	$D_Z(A) = \theta'^{-1}(D(A)) \cap (P_n \times P_n)_Z$ for each cyclotomic coset Z

Table 3.1: Notations of twisted codes.

Throughout this section, n is a positive integer such that $n \mid 2^r - 1$ for some positive integer r and $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Recall that the $\mathbb{F}_2$-linear map $\psi : \mathbb{F}_2^{2n} \to \mathbb{F}_4^n$ defined by

$$\psi((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})) = (a_{11}\omega + a_{12}\omega^2, a_{21}\omega + a_{22}\omega^2, \ldots, a_{n1}\omega + a_{n2}\omega^2)$$

is a vector space isomorphism. Using the map ψ, one can see that a twisted code $\mathscr{C}_\gamma(A)$ is linear over $\mathbb{F}_4$, if for each vector $a = \big((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})\big) \in \mathscr{C}_\gamma(A)$, the vector $a' = \big((a_{12}, a_{11} + a_{12}), \ldots, (a_{n2}, a_{n1} + a_{n2})\big) \in \mathscr{C}_\gamma(A)$. This is because $\psi(a') = \omega\psi(a)$. Next, we use this property and identify some twisted codes that are also linear cyclic codes over $\mathbb{F}_4$. This allows us to discard twisted codes that are linear cyclic codes in our search for good codes, as linear cyclic codes over $\mathbb{F}_4$ have been extensively studied in the literature.

Theorem 3.5.1 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. If for each 2-cyclotomic coset Z modulo n either $A \cap Z = \emptyset$ or $Z \subseteq A$, then $\mathscr{C}_\gamma(A)$ is a linear cyclic code over $\mathbb{F}_4$.*

Proof. As we mentioned earlier, twisted codes are cyclic. So we only show that $\mathscr{C}_\gamma(A)$ is a linear code over $\mathbb{F}_4$ assuming that either $A \cap Z = \emptyset$ or $Z \subseteq A$ for each cyclotomic coset Z. Recall that the set A_d defined in (3.4.6) is the complete defining set of $\mathscr{C}_\gamma(A)^{\perp_s}$. Let Z

be a 2-cyclotomic coset modulo n. Clearly, $A_d \cap Z = \emptyset$ or $Z \subseteq A_d$. By (3.4.11), we have $\mathscr{C}_\gamma(A) = \mathrm{Tr}_1^r(D(A_d))$. Moreover, using Corollary 3.4.14 part (ii), we get

$$D(A_d) = \bigoplus_Z \theta'(D_Z(A_d)) = \bigoplus_Z \theta'((P_n \times P_n)_Z),$$

where the direct sum runs over all different 2-cyclotomic cosets such that $A_d \cap Z$ is saturated. So it is enough to show that $\mathrm{Tr}_1^r\Big(\theta'((P_n \times P_n)_Z)\Big)$ is $\mathbb{F}_4$-linear for each such cyclotomic coset Z. Let $(p(x), q(x)) \in (P_n \times P_n)_Z$, where $Z \cap A_d$ is saturated. Then

$$u = \mathrm{Tr}_1^r\Big(((p(1), q(1)), (p(\alpha), q(\alpha)), \ldots, (p(\alpha^{n-1}), q(\alpha^{n-1})))\Big) \in \mathscr{C}_\gamma(A).$$

Since $(q(x), p(x) + q(x)) \in (P_n \times P_n)_Z$, we have

$$v = \mathrm{Tr}_1^r\Big(((q(1), p(1)+q(1)), (q(\alpha), p(\alpha)+q(\alpha)), \ldots, (q(\alpha^{n-1}), p(\alpha^{n-1})+q(\alpha^{n-1})))\Big) \in \mathscr{C}_\gamma(A).$$

Now u and v satisfy the linearity test mentioned above this theorem. Hence $\mathscr{C}_\gamma(A)$ is a linear subspace of $\mathbb{F}_4^n$. □

Example 3.5.2 In this example, we show that the unsaturated intersection of the defining set of a twisted code with cyclotomic cosets can result in linear and non-linear twisted codes over $\mathbb{F}_4$.

(1) Let $\kappa = 2$ ($\kappa \mid r = 8$) and $A = \{1, 4, 16, 13\}$ be the complete defining set of a twisted code of length 17 over $\mathbb{F}_4$. Then $A \subsetneq Z(1)$ and our computation in Magma [17] shows that $\mathscr{C}_\gamma(A)$ is a linear code over $\mathbb{F}_4$.

(2) Let $\kappa = 11$ ($\kappa \mid r = 11$) and $A = \{1\}$ be the complete defining set of a twisted code of length 23 over $\mathbb{F}_4$. Then $A \subsetneq Z(1)$ and our computation in Magma [17] shows that $\mathscr{C}_\gamma(A)$ is a non-linear code over $\mathbb{F}_4$.

Recall that the Euclidean inner product of two vectors x and $y \in \mathbb{F}_{2^r}^n$ is denoted by $x \cdot y$. Now, we give a connection between the structure of vectors in $\mathscr{C}_\gamma(A)$ and $C(A)$. This connection allows us to compute the defining set of the sum and intersection of twisted codes. As we will see in Corollary 3.6.3, this result also enables us to give a general minimum distance lower bound for twisted codes using the minimum distance of linear cyclic codes.

Theorem 3.5.3 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then the following statements are equivalent.*

1. *The vector $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathscr{C}_\gamma(A)$.*

2. *The vector $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2}) \in C(A)$.*

Proof. Let $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2}))$ and $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2})$ for arbitrary b_{i1} and $b_{i2} \in \mathbb{F}_2$, where $1 \leq i \leq n$. Let $z = (z_1, z_2, \ldots, z_n)$ be an arbitrary element of $C(A)^\perp$. Since Tr_1^r is linear over $\mathbb{F}_2$, one can easily verify that

$$\langle \phi_\gamma(z), y \rangle_s = \sum_{i=1}^{n} (b_{i1} \mathrm{Tr}_1^r(\gamma z_i) + b_{i2} \mathrm{Tr}_1^r(z_i)) = \mathrm{Tr}_1^r(\sum_{i=1}^{n} z_i(\gamma b_{i1} + b_{i2})) = \mathrm{Tr}_1^r(z \cdot x). \quad (3.5.1)$$

$1 \Rightarrow 2$: Suppose that $y \in \mathscr{C}_\gamma(A)$. Equation (3.5.1) implies that $\langle \phi_\gamma(z), y \rangle_s = \mathrm{Tr}_1^r(z \cdot x) = 0$ holds for any arbitrary z in $C(A)^\perp$. Hence $z \cdot x = 0$ as otherwise we can find $z' \in C(A)^\perp$ such that $0 = \langle \phi_\gamma(z'), y \rangle_s = \mathrm{Tr}_1^r(z' \cdot x) = 1$, which is a contradiction. Hence $x \in C(A)$.

$2 \Rightarrow 1$: Suppose that $x \in C(A)$. Then for each z in $C(A)^\perp$, we have $z \cdot x = 0$. Now, equation (3.5.1) implies that $\langle \phi_\gamma(z), y \rangle_s = \mathrm{Tr}_1^r(z \cdot x) = 0$ for each z in $C(A)^\perp$. Hence $y \in \mathscr{C}_\gamma(A)$. □

Recall that if $C(A)$ and $C(A')$ are two linear cyclic codes over $\mathbb{F}_{2^r}$ with the defining sets A and A', respectively, then $C(A) \cap C(A') = C(A \cup A')$ and $C(A) + C(A') = C(A \cap A')$. Next, we show that the complete defining sets of the sum and intersection of two twisted codes follow the same rule.

Proposition 3.5.4 *Let $A, A' \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining sets of two twisted codes of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then*

1. $\mathscr{C}_\gamma(A) \cap \mathscr{C}_\gamma(A') = \mathscr{C}_\gamma(A \cup A')$.
2. $\mathscr{C}_\gamma(A) + \mathscr{C}_\gamma(A') = \mathscr{C}_\gamma(A \cap A')$.

Proof. (1): Let $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathbb{F}_2^{2n}$ and $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2})$. Using the result of Theorem 3.5.3, we have $y \in \mathscr{C}_\gamma(A) \cap \mathscr{C}_\gamma(A')$ if and only if $x \in C(A) \cap C(A')$ if and only if $x \in C(A \cup A')$ if and only if $y \in \mathscr{C}_\gamma(A \cup A')$.

(2): Let

$$y_1 = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2}))$$

and

$$y_2 = ((b'_{11}, b'_{12}), (b'_{21}, b'_{22}), \ldots, (b'_{n1}, b'_{n2}))$$

be elements of $\mathbb{F}_2^{2n}$. Moreover, suppose that

$$x_1 = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2})$$

and

$$x_2 = (\gamma b'_{11} + b'_{12}, \gamma b'_{21} + b'_{22}, \ldots, \gamma b'_{n1} + b'_{n2}).$$

Then, by Theorem 3.5.3, we have if $y_1 + y_2 \in \mathscr{C}_\gamma(A) + \mathscr{C}_\gamma(A')$, then $x_1 + x_2 \in C(A) + C(A') = C(A \cap A')$. This implies that $y_1 + y_2 \in \mathscr{C}_\gamma(A \cap A')$. Thus $\mathscr{C}_\gamma(A) + \mathscr{C}_\gamma(A') \subseteq \mathscr{C}_\gamma(A \cap A')$.

Next we show that $\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A\cap A')) = \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)+\mathscr{C}_\gamma(A'))$, which proves that $\mathscr{C}_\gamma(A)+\mathscr{C}_\gamma(A') = \mathscr{C}_\gamma(A\cap A')$. By Theorem 3.4.8, we have $\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A\cap A')) = \sum_Z c_Z(A\cap A')$, where the sum runs over all different cyclotomic cosets. Using a similar argument we get

$$\begin{aligned}\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)+\mathscr{C}_\gamma(A')) &= \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)) + \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A')) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)\cap\mathscr{C}_\gamma(A'))\\ &= \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)) + \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A')) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A\cup A'))\\ &= \sum_Z (c_Z(A)+c_Z(A')-c_Z(A\cup A')).\end{aligned}$$

Let Z be a 2-cyclotomic coset modulo n. To prove that $\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A\cap A')) = \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A)+\mathscr{C}_\gamma(A'))$, it is sufficient to show that

$$k_Z = c_Z(A)+c_Z(A')-c_Z(A\cup A')-c_Z(A\cap A') = 0.$$

This is true because

$$k_Z = \begin{cases} c_Z(A)+c_Z(A')-c_Z(A)-c_Z(A')=0 & \text{if } A=Z \text{ or } A'=\emptyset\\ c_Z(A)+c_Z(A')-c_Z(A')-c_Z(A)=0 & \text{if } A'=Z \text{ or } A=\emptyset\\ c_Z(A)+c_Z(A)-c_Z(A)-c_Z(A)=0 & \text{if } A'=A\\ |Z|+|Z|-0-2|Z|=0 & \text{if } A\neq A' \text{ and } A\cap Z, A'\cap Z \text{ are unsaturated.}\end{cases}$$

□

3.5.1 Quantum codes from nearly dual-containing twisted codes

Let $A\subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$. Recall that, by Theorem 1.7.1, one can construct a quantum code from the twisted code $\mathscr{C}_\gamma(A)$, if $\mathscr{C}_\gamma(A_d)\subseteq\mathscr{C}_\gamma(A)$ or equivalently when $\mathscr{C}_\gamma(A)$ is symplectic dual-containing. A criterion for self-orthogonality, or equivalently dual-containment, of twisted codes was provided in Theorem 3.4.11. Next, we define the dual-containment deficiency of $\mathscr{C}_\gamma(A)$ by

$$e = \frac{\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d)) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d)\cap\mathscr{C}_\gamma(A))}{2} = \frac{\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d)) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A\cup A_d))}{2}.$$

This helps to apply the quantum construction of Theorem 3.2.3 to additive twisted codes which are not necessarily symplectic dual-containing. Note that $\mathscr{C}_\gamma(A)$ has the dual-containment deficiency $e=0$ if and only if $\mathscr{C}_\gamma(A_d)\subseteq\mathscr{C}_\gamma(A)$. In general, we target twisted codes with a small value of e, since the result of Theorem 3.2.3 is more likely to produce a good quantum code for such e values. This is because dimension of the code $\mathscr{C}_\gamma(A)+\mathscr{C}_\gamma(A_d)$ is large (hence it probably has a small minimum distance) when the value of e is closer to $\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d))$.

Let $Z_1, Z_2, \ldots, Z_r, {Z_1}', -{Z_1}', {Z_2}', -{Z_2}', \ldots, {Z_t}', -{Z_t}'$ be all the different 2-cyclotomic cosets modulo n, where $Z_i = -Z_i$ for all $1 \le i \le r$.

Theorem 3.5.5 *Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then*

$$\begin{aligned} 2e = \dim_{\mathbb{F}_2}\left(\mathscr{C}_\gamma(A_d)\right) - \dim_{\mathbb{F}_2}\left(\mathscr{C}_\gamma(A \cup A_d)\right) = \sum_{Z \cap A \ sat} 2|Z| \ + \sum_{\substack{Z \cap A \ unsat \\ (Z\cap A)^H \neq -((Z\cap A)^H)}} |Z| \\ + \sum_{\substack{Z' \cap A \ sat \\ -Z' \cap A \ sat}} 4|Z'| \ + \sum_{\substack{Z' \cap A \ sat \\ -Z' \cap A \ unsat}} 2|Z'| \ + \sum_{\substack{Z' \cap A \ unsat \\ -Z' \cap A \ unsat \\ (Z'\cap A)^H \neq -((-Z'\cap A)^H)}} 2|Z'| \end{aligned} \tag{3.5.2}$$

where the first two sums run over all cyclotomic cosets Z with $Z = -Z$ and the other sums run over all the cyclotomic cosets pairs $(Z', -Z')$ with $Z' \neq -Z'$. Also, in the above notation, sat and unsat stand for saturated and unsaturated, respectively.

Proof. First note that by (3.4.11), we have $\mathscr{C}_\gamma(A_d) = \mathrm{Tr}_1^r(D(A))$ and since $D(A)$ is Galois close over $\mathbb{F}_2$

$$\dim_{\mathbb{F}_2}\left(\mathscr{C}_\gamma(A_d)\right) = \dim_{\mathbb{F}_{2^r}}(D(A)) = \sum_Z \dim_{\mathbb{F}_{2^r}}(D_Z(A)),$$

where the sums run over all different 2-cyclotomic cosets modulo n. Moreover, the fact that

$$\left(\mathscr{C}_\gamma(A) \cap \mathscr{C}_\gamma(A_d)\right)^{\perp_s} = \mathscr{C}_\gamma(A \cup A_d)^{\perp_s} = \mathscr{C}_\gamma(A) + \mathscr{C}_\gamma(A_d) = \mathscr{C}_\gamma(A \cap A_d)$$

implies that

$$\dim_{\mathbb{F}_2}\left(\mathscr{C}_\gamma(A_d)\right) - \dim_{\mathbb{F}_2}\left(\mathscr{C}_\gamma(A \cup A_d)\right) = \sum_Z \left(\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(A \cap A_d))\right).$$

Let $N = A \cap A_d$. Next we compute $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N))$ for each cyclotomic coset Z using the result of Proposition 3.4.14.

Case (I): Let $Z = Z_i$ for some $1 \le i \le r$.

1. If $Z \cap A = \emptyset$, then $Z \cap N = \emptyset$. Thus $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
2. If $Z \cap A$ is saturated, then $Z \cap A_d = \emptyset$. Thus $Z \cap N = \emptyset$ and $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 2|Z|$.
3. Let $Z \cap A$ be unsaturated.
    (a) If $Z \cap A$ is purely unsaturated, then $Z \cap N = Z \cap A$ and $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
    (b) If $Z \cap A$ is not purely unsaturated, then $Z \cap N = \emptyset$ and $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = |Z|$.

Case (II): Let $Z = Z_i{}'$ for some $1 \leq i \leq t$.

1. If $Z \cap A = -Z \cap A = \emptyset$. Thus $Z \cap N = \emptyset$ and $-Z \cap N = \emptyset$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
2. If $Z \cap A = \emptyset$ and $-Z \cap A$ is saturated, then $Z \cap A_d = \emptyset$ and $-Z \cap A_d = -Z$. Thus $Z \cap N = \emptyset$ and $-Z \cap N = -Z$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
3. If $Z \cap A = \emptyset$ and $-Z \cap A$ is unsaturated, then $Z \cap A_d$ is unsaturated and $-Z \cap A_d = -Z$. Thus $Z \cap N = \emptyset$ and $-Z \cap N = -Z \cap A$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
4. If $Z \cap A$ and $-Z \cap A$ are both saturated, then $Z \cap A_d = \emptyset$ and $-Z \cap A_d = \emptyset$. Thus $Z \cap N = \emptyset$ and $-Z \cap N = \emptyset$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 4|Z|$.
5. If $Z \cap A$ is saturated and $-Z \cap A$ is unsaturated, then $Z \cap A_d$ is unsaturated and $-Z \cap A_d = \emptyset$. Thus $Z \cap N = Z \cap A_d$ and $-Z \cap N = \emptyset$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 2|Z|$.
6. Let $Z \cap A$ and $-Z \cap A$ be unsaturated.
   (a) If $(Z \cap A)^H = -((-Z \cap A)^H)$, then $Z \cap A_d = Z \cap A$ and $-Z \cap A_d = -Z \cap A$. Thus $Z \cap N = Z \cap A$ and $-Z \cap N = -Z \cap A$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 0$.
   (b) Otherwise, $Z \cap A_d \neq Z \cap A$ and $-Z \cap A_d \neq -Z \cap A$. Thus $Z \cap N = \emptyset$ and $-Z \cap N = \emptyset$. Hence $\dim_{\mathbb{F}_{2^r}}(D_Z(A)) - \dim_{\mathbb{F}_{2^r}}(D_Z(N)) = 2|Z|$.

Now (3.5.2) follows from putting the above cases together. □

The formula given in (3.5.2) provides a practical approach for designing twisted codes with a small value of e more systematically. For instance, when $Z = -Z$, the saturated intersection $Z \cap A$ implies a larger e value than an unsaturated intersection of $Z \cap A$. Moreover, when $Z' \neq -Z'$, the e value is non-decreasing when there are more saturated intersections between $Z' \cap A$ and $-Z' \cap A$. Hence having smaller numbers of saturated intersections of the complete defining set with Z' and $-Z'$ can produce twisted codes with a smaller value of e. Motivated by this observation, some of our record-breaking quantum codes are obtained from twisted codes with the complete defining set A such that $A = -A$ and $A \cap Z$ is either empty or unsaturated for each cyclotomic coset Z. Next, we characterize all the twisted codes with the dual-containment deficiency $e = 1$.

Corollary 3.5.6 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. The code $\mathscr{C}_\gamma(A)$ has the dual-containment deficiency $e = 1$ if and only if all the cyclotomic cosets intersecting A satisfy the condition (i) or (ii) of Theorem* 3.4.11 *except one cyclotomic coset, which is in the form*

1. $Z = \{0\}$,

2. or $Z = \{\frac{n}{3}, \frac{2n}{3}\}$, *when* $3 \mid n$, $\kappa = 2$, *and* $|Z \cap A| = 1$.

Proof. First, note that the only singleton 2-cyclotomic coset modulo n is $\{0\}$ as n is an odd integer. Moreover, one can easily verify that 2-cyclotomic cosets of size 2 exist only when $3 \mid n$ and are in the form of $Z = \{\frac{n}{3}, \frac{2n}{3}\}$.

$\Rightarrow$: If all the 2-cyclotomic cosets modulo n satisfy condition (i) or (ii) of Theorem 3.4.11, then the code $\mathscr{C}_\gamma(A_d)$ is self-orthogonal and $e = 0$. So there is at least one 2-cyclotomic coset Z such that $Z \cap A \neq \emptyset$ and Z does not satisfy the conditions of Theorem 3.4.11. Moreover, the formula provided in Theorem 3.5.5 verifies that Cases (1) and (2) above give $e = 1$. Next, if Z is not in the form of Case (1) or Case (2) above, then $|Z| > 2$ or Z has size two and $Z \cap A = Z$. Therefore, the dual-containment deficiency formula of Theorem 3.5.5 implies that $e > 1$.

$\Leftarrow$: It follows immediately from Theorem 3.5.5. □

Now we present a restriction of quantum construction of Theorem 3.2.3 to nearly dual-containing twisted codes. This result is very important as it allows us to construct quantum codes from the twisted codes which are not symplectic dual-containing.

Theorem 3.5.7 *Let* $\mathscr{C}_\gamma(A)$ *be an* $(n, 2^{n+k})$ *twisted code over* $\mathbb{F}_2 \times \mathbb{F}_2$ *with the defining set* $A \subseteq \mathbb{Z}/n\mathbb{Z}$ *and* e *be the dual-containment deficiency of the code* $\mathscr{C}_\gamma(A)$*. Then there exists a binary quantum code with parameters* $[\![n+e, k+e, d]\!]$*, where*

$$d \geq \min\{d(\mathscr{C}_\gamma(A)), d(\mathscr{C}_\gamma(A \cap A_d)) + 1\}.$$

Proof. First note that $\mathscr{C}_\gamma(A) + \mathscr{C}_\gamma(A_d) = \mathscr{C}_\gamma(A \cap A_d)$. Now, the proof follows by applying Theorem 3.2.3 to the twisted code $\mathscr{C}_\gamma(A)$ considered as an additive code over $\mathbb{F}_4$. □

Many new record-breaking binary quantum codes were obtained after applying the above theorem to nearly dual-containing twisted codes. The parameters of such codes are presented in Section 3.8.

3.6 New minimum distance bounds for twisted codes

Similar to linear cyclic codes, the minimum distance of twisted codes can be bounded using the BCH bound [13]. This is because twisted codes are constructed by applying the map ϕ_γ to linear cyclic codes. Currently, this is the only known minimum distance bound for the entire family of additive cyclic codes. Recall that n is a positive integer such that $n \mid 2^r - 1$ for some positive integer r and $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Recall that $C(A)$ is the length n linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A. In this section, we provide a minimum distance lower bound for twisted code using the minimum distance of the code $C(A)$. We show that the other well-known minimum distance lower bounds, such as Hartmann-Tzeng and Roos bounds, introduced in Section 1.4, remain valid for twisted codes. Moreover, we prove that any minimum distance lower bound for $C(A)$ is also a minimum distance lower bound for the twisted code $\mathscr{C}_\gamma(A)$.

Recall that $L \subseteq \mathbb{Z}/n\mathbb{Z}$ is called a consecutive set of length s if there exists an integer c with $\gcd(c, n) = 1$ such that

$$\{(cl) \bmod n : l \in L\} = \{(j+t) \bmod n : 0 \leq j \leq s-1\}$$

for some $t \in \mathbb{Z}/n\mathbb{Z}$. The next proposition gives the BCH minimum distance bound for twisted codes. This result was proved using a technical argument on the structure of Vandermonde matrices and then applying a modification of Theorem 1.2.1.

Proposition 3.6.1 *[13] Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ such that A contains a consecutive set of size $t-1$. Then $d(\mathscr{C}_\gamma(A)) \geq t$.*

Recall that $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code. The definition of the complete defining set, given in Definition 3.4.7, implies that for each $a \in A$, the value $2^\kappa a \in A$. The result of Theorem 3.3.8 and the discussion right before it imply that the codes $\left(C(A)\right)_{\mathbb{F}_{2^\kappa}}$, which is the linear cyclic code of length n over $\mathbb{F}_{2^\kappa}$ with the defining set A , and $C(A)$ are both Galois closed over $\mathbb{F}_{2^\kappa}$. Hence Theorem 3.3.5 implies that the codes $\left(C(A)\right)_{\mathbb{F}_{2^\kappa}}$ and $C(A)$ both have the same parameters (length, dimension, and minimum distance). This motivates us to state the following remark.

Remark 3.6.2 In this section and Section 3.7, we provide minimum distance bounds for the minimum distance of twisted codes using the linear cyclic codes $C(A)$. Moreover, as we showed above, the codes $C(A)$ and the linear cyclic code $\left(C(A)\right)_{\mathbb{F}_{2^\kappa}}$ both have the same parameters. Hence it will be more efficient to compute the minimum distance of $\left(C(A)\right)_{\mathbb{F}_{2^\kappa}}$ instead of $C(A)$. However, to avoid using many different notations and linear cyclic codes in our statements, we only state our minimum distance computations using the code $C(A)$. In other words, all of the results of this section remain valid if we replace $C(A)$ with the code $\left(C(A)\right)_{\mathbb{F}_{2^\kappa}}$.

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. In Theorem 3.5.3, we showed that the vector $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathscr{C}_\gamma(A)$ if and only if the vector $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2}) \in C(A)$. This connection allows us to provide a general minimum distance lower bound for twisted codes using the minimum distance of linear cyclic codes. Our proof here is shorter than that of the BCH bound for the twisted codes. Moreover, it provides a better insight about the structure of vectors in a twisted code.

Corollary 3.6.3 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. If $\mathscr{C}_\gamma(A)$ has a weight t vector, then $C(A)$ also has a weight t vector. In particular, $d(\mathscr{C}_\gamma(A)) \geq d(C(A))$.*

Proof. Note that the vectors x and y in the statement of Theorem 3.5.3 have the same weight. Let $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathscr{C}_\gamma(A)$. Then $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2}) \in C(A)$ which proves the first part of the statement. Moreover, assume that $\mathrm{wt}(y) = d(\mathscr{C}_\gamma(A))$. Then

$$d(\mathscr{C}_\gamma(A)) = \mathrm{wt}(y) = \mathrm{wt}(x) \geq d(C(A)).$$

□

In other words, any minimum distance lower bound for the minimum distance of linear cyclic code $C(A)$ remains a minimum distance lower bound for the code $\mathscr{C}_\gamma(A)$. Note that the converse of the above corollary is not necessarily true. In other words, the code $C(A)$ can contain vectors which are not of the form $(\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2})$ for arbitrary b_{i1} and $b_{i2} \in \mathbb{F}_2$, where $1 \leq i \leq n$. The following example shows that minimum weight vectors in a linear cyclic code $C(A)$ are not of the above form. Later, in Section 3.7, we develop this example into an infinite family of twisted codes with minimum distance at least five.

Example 3.6.4 Let $n = 73$ and $r = 9$. Then $73 \mid 2^9 - 1$ and $\mathbb{F}_{2^9}$ contains all the 73-rd roots of unity. Let $\kappa = 3$, $\gamma \in \mathbb{F}_8 \setminus \mathbb{F}_2$, and $A = \{1, 8, 9, 64, 65, 72\}$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Our computation in Magma [17] shows that $d(C(A)) = 4$ and all such weight four vectors have pairwise different non-zero coordinates. Hence, these weight four vectors are not of type $x = (\gamma b_{11} + b_{12}, \gamma b_{21} + b_{22}, \ldots, \gamma b_{n1} + b_{n2})$ with b_{i1} and $b_{i2} \in \mathbb{F}_2$, where $1 \leq i \leq n$. This is because every four non-zero coordinates of x must have an identical pair. So by Theorem 3.5.3, we have $d(\mathscr{C}_\gamma(A)) \geq 5$. Indeed our minimum distance computation in Magma verifies that $d(\mathscr{C}_\gamma(A)) = 5$.

Next, we provide minimum distance bounds for twisted codes analogous to the known bounds for linear cyclic codes provided in Section 1.4. We first state a minimum distance bound for twisted codes analogous to the Hartmann-Tzeng minimum distance lower bound of Theorem 1.4.5 for cyclic codes.

Corollary 3.6.5 *Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that A contains a subset in the form*

$$B = \{(l + i_1 c_1 + i_2 c_2 + \cdots + i_k c_k) \bmod n : \ 0 \leq i_j \leq s_j, \ \gcd(c_j, n) = 1\},$$

where $l, c_j \in \mathbb{Z}/n\mathbb{Z}$ and s_j is a non-negative integer for $1 \leq j \leq k$. Then $d(\mathscr{C}_\gamma(A)) \geq (\sum_{j=1}^{k} s_j) + 2$.

Proof. By the generalized Hartmann-Tzeng bound for linear cyclic codes, Theorem 1.4.5, we have $d(C(A)) \geq (\sum_{j=1}^{k} s_j) + 2$. Now, the result follows from Corollary 3.6.3. □

The next corollary is another lower bound for twisted codes analogous to the Roos bound for linear cyclic code provided in Theorem 1.4.7. This bound relaxes the consecutive condition in the original Hartmann-Tzeng bound and allows one of the two consecutive sets in the Hartmann-Tzeng bound to be non-consecutive.

Corollary 3.6.6 *Let M and N be non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$ such that N is consecutive and $M + N \subseteq A$. If there exists a consecutive set $\bar{M} \subseteq \mathbb{Z}/n\mathbb{Z}$ such that $M \subseteq \bar{M}$ and $|\bar{M}| \leq |M| + |N| - 1$, then $d(\mathscr{C}_\gamma(M + N)) \geq |M| + |N|$.*

Proof. By the Roos bound for linear cyclic codes, Theorem 1.4.7, we have $d(C(A)) \geq |M| + |N|$. Now, the result follows from Corollary 3.6.3. □

3.7 New infinite families of twisted codes with minimum distance at least five

Linear and additive codes with the minimum distance three and five are single and double error-correcting codes. These codes can only detect and correct errors when the error rate is low. In particular, single and double error-correcting codes are widely used in computer memory (usually RAM), where bit errors are extremely rare. Most of the double error correcting codes have complicated decoding procedures that can result in a significant increase in power and delay [69]. This motivates us to design a class of double error-correcting codes from twisted codes. Twisted codes, and more generally additive cyclic codes, can be viewed as quasi-cyclic codes [48]. Many efficient encoding and decoding algorithms for quasi-cyclic codes have been designed in the literature [1, 23, 39, 49, 106]. Hence our new double error-correcting twisted codes, along with other good twisted codes discovered in this thesis, can be useful for practical applications.

Recall that in Corollary 3.6.3, we proved that for each complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$, the inequality $d(\mathscr{C}_\gamma(A)) \geq d(C(A))$ holds, where $C(A)$ is the linear cyclic code of length n with the defining set A over $\mathbb{F}_{2^r}$. Moreover, in Example 3.6.4, we showed that this inequality can be strict. In this section, we develop this example into an infinite family of twisted codes. In particular, we first provide a sufficient condition for twisted codes to have minimum distance at least five. Our sufficient condition does not rely on conventional methods for bounding the minimum distance of linear cyclic codes, such as the structure of the Vandermonde matrix. Next, we apply this result to identify a general class and two infinite families of twisted codes with minimum distance at least five. These infinite families will be used later in Section 3.8 to construct infinite classes of record-breaking binary quantum codes. Moreover, applying the secondary constructions provided at the end of Section 1.2 results in more additive codes with minimum distance five.

For $A \subseteq \mathbb{Z}/n\mathbb{Z}$, we define $A_0 = A \cup \{0\}$. Recall that using the properties of linear cyclic codes, we have

$$\begin{aligned} C(A)^\perp + C(\{0\})^\perp &= C(\mathbb{Z}/n\mathbb{Z} \setminus -A) + C(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}) = C((\mathbb{Z}/n\mathbb{Z} \setminus -A) \cap (\mathbb{Z}/n\mathbb{Z} \setminus \{0\})) \\ &= C(\mathbb{Z}/n\mathbb{Z} \setminus -(A \cup \{0\})) = C(A_0)^\perp. \end{aligned}$$

Thus each vector $x \in C(A_0)^\perp$ can be written as $x = x_1 + x_2$, where $x_1 \in C(A)^\perp$ and $x_2 = (c, c, \ldots, c) \in C(\{0\})^\perp$ for some constant $c \in \mathbb{F}_{2^r}$. The next lemma gives a connection between the twisted codes $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A_0)$.

Lemma 3.7.1 *Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that $0 \notin A$. If $d(\mathscr{C}_\gamma(A_0)) \geq k$, then there is no codeword in the form $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathscr{C}_\gamma(A)$ such that $wt(y) < k$ and $\sum_{i=1}^{n}(b_{i1}, b_{i2}) = (0, 0)$.*

Proof. Toward a contradiction, let $y = ((b_{11}, b_{12}), (b_{21}, b_{22}), \ldots, (b_{n1}, b_{n2})) \in \mathscr{C}_\gamma(A)$ such that $wt(y) < k$ and $\sum_{i=1}^{n}(b_{i1}, b_{i2}) = (0, 0)$. Thus $y \notin \mathscr{C}(A_0)$ and there exists $x \in C(A_0)^\perp$ such that $\langle \phi_\gamma(x), y \rangle_s \neq 0$. As we mentioned above, we can write $x = x_1 + x_2$, where $x_1 \in C(A)^\perp$ and $x_2 = (c, c, \ldots, c)$ for some $c \in \mathbb{F}_{2^r}$. Since $y \in \mathscr{C}_\gamma(A)$ and $x_1 \in C(A)^\perp$, we conclude that

$$\langle \phi_\gamma(x), y \rangle_s = \langle \phi_\gamma(x_1), y \rangle_s + \langle \phi_\gamma(x_2), y \rangle_s = \langle \phi_\gamma(x_2), y \rangle_s.$$

Moreover, by using the equation provided in (3.5.1), we have

$$\langle \phi_\gamma(x), y \rangle_s = \langle \phi_\gamma(x_2), y \rangle_s = \mathrm{Tr}_1^r(c \sum_{i=1}^{n}(\gamma b_{i1} + b_{i2})) = 0,$$

where the last equality follows from the fact that $\sum_{i=1}^{n}(b_{i1}, b_{i2}) = (0, 0)$. However, this is a contradiction with the fact that $\langle \phi_\gamma(x), y \rangle_s \neq 0$. □

We call a non-empty defining set A of a twisted code *symmetric* if $A = -A$. The next theorem provides a sufficient condition for the twisted code $\mathscr{C}_\gamma(A)$ to have minimum distance at least five.

Theorem 3.7.2 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a symmetric complete defining set of a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ such that $0 \notin A$. If $d(\mathscr{C}_\gamma(A_0)) \geq 5$, then $\mathscr{C}_\gamma(A)$ has no codeword of weight 4. If in addition* $\gcd(n, 3) = 1$, *then $d(\mathscr{C}_\gamma(A)) \geq 5$.*

Proof. Since A is non-empty, by Proposition 3.6.1, the code $\mathscr{C}_\gamma(A)$ has minimum distance at least two. We prove the result in two steps. First, we show that there is no codeword of weight four in $\mathscr{C}_\gamma(A)$. Second, we prove that if $\gcd(n,3)=1$, then there is no vector with weight two or three in $\mathscr{C}_\gamma(A)$.

Step 1: Toward a contradiction, assume that $y \in \mathscr{C}_\gamma(A)$ is a weight four codeword. Since $\mathscr{C}_\gamma(A)$ is a cyclic code, without loss of generality, we can assume that the first coordinate of y is non-zero. Each non-zero coordinate of y has only one of the forms $(1,1)$, $(1,0)$, or $(0,1)$, which implies that at least two of the non-zero coordinates of y are equal. So, we assume that

1. the four non-zero coordinates of y have indices $0 \le 0, i, j, k \le n-1$ and, for simplicity, we discard the zero coordinates of y in its representation and also in all computations,

2. y has the same non-zero values in the positions 0 and i.

In other words, $y = ((b_{01}, b_{02}), (b_{01}, b_{02}), (b_{j1}, b_{j2}), (b_{k1}, b_{k2}))$. Moreover, Lemma 3.7.1 implies that $(b_{j1}, b_{j2}) \ne (b_{k1}, b_{k2})$. By Theorem 3.5.3, there exists a weight four vector $x = (x_0, x_0, x_j, x_k) = (\gamma b_{01} + b_{02}, \gamma b_{01} + b_{02}, \gamma b_{j1} + b_{j2}, \gamma b_{k1} + b_{k2}) \in C(A)$. Let t be an arbitrary element of A and $\alpha \in \mathbb{F}_{2^r}$ be a primitive n-th root of unity. Since A is symmetric, we have

$$x \cdot (1, \alpha^{it}, \alpha^{jt}, \alpha^{kt}) = x \cdot (1, \alpha^{-it}, \alpha^{-jt}, \alpha^{-kt}) = 0.$$

This implies

$$x_0 + x_0\alpha^{it} + x_j\alpha^{jt} + x_k\alpha^{kt} = 0 \tag{3.7.1}$$

and

$$x_0 + x_0\alpha^{-it} + x_j\alpha^{-jt} + x_k\alpha^{-kt} = 0. \tag{3.7.2}$$

Multiplying (3.7.1) by α^{-it} and adding it to (3.7.2) gives

$$x_j\alpha^{(j-i)t} + x_k\alpha^{(k-i)t} + x_j\alpha^{-jt} + x_k\alpha^{-kt} = (x_j, x_k, x_j, x_k) \cdot (\alpha^{(j-i)t}, \alpha^{(k-i)t}, \alpha^{-jt}, \alpha^{-kt}) = 0. \tag{3.7.3}$$

Let $x' = (x_j, x_k, x_j, x_k)$, where x' has values x_j, x_k, x_j, and x_k in the positions $j-i$, $k-i$, $-j$, and $-k$, respectively, and the other coordinates of x' are zero. If any of these indices is negative, we substitute it with its corresponding non-negative value modulo n. Note also that some of the indices may overlap ($\mathrm{wt}(x') \le 4$). Since (3.7.3) is valid for each $t \in A$, we have x' in $C(A)$. Also, the fact that $x_j \ne x_k$ implies that x' is not identically zero ($x' = 0$ implies that $2j \equiv 2k \equiv i \bmod n$ or equivalently $j \equiv k \bmod n$). So x' is a non-zero vector with a weight of at most four (some of the indices may overlap), and the sum of the coordinates is equal to zero. Thus, by Lemma 3.5.3, $\mathscr{C}_\gamma(A)$ has a codeword with weight at most four and the sum of the coordinates equal to $(0,0)$. However, by Lemma 3.7.1, $\mathscr{C}_\gamma(A)$ cannot have such a codeword. This contradiction completes the proof of Step 1.

Step 2: Toward a contradiction, let $y \in \mathscr{C}_\gamma(A)$ be a weight three codeword. By Lemma 3.7.1, all there coordinates of y cannot be different. So, without loss of generality, let $y = ((b_{01}, b_{02}), (b_{i1}, b_{i2}), (b_{j1}, b_{j2}))$ and $(b_{01}, b_{02}) = (b_{i1}, b_{i2})$. Similar to the previous step, there exists a weight three vector $x = (x_0, x_0, x_j) = (\gamma b_{01} + b_{02}, \gamma b_{01} + b_{02}, \gamma b_{j1} + b_{j2}) \in C(A)$ such that for each $t \in A$,

$$x_0 + x_0 \alpha^{it} + x_j \alpha^{jt} = 0 \text{ and } x_0 + x_0 \alpha^{-it} + x_j \alpha^{-jt} = 0. \tag{3.7.4}$$

If $j - i \not\equiv -j \pmod{n}$, then by multiplying the first equation of (3.7.4) by α^{-it} and adding it to the other equation we get

$$x_j \alpha^{(j-i)t} + x_j \alpha^{-jt} = (x_j, x_j) \cdot (\alpha^{(j-i)t}, \alpha^{-jt}) = 0.$$

This implies the existence of a weight two vector in $C(A)$ containing x_j in the positions $j - i$ and $-j$ (since $j - i \not\equiv -j \pmod{n}$, this codeword is non-zero and has weight two).

In the case $j - i \equiv -j \pmod{n}$, by adding both equations of (3.7.4), we get

$$x_i \alpha^{it} + x_j \alpha^{jt} + x_i \alpha^{-it} + x_j \alpha^{-jt} = (x_i, x_j, x_i, x_j) \cdot (\alpha^{it}, \alpha^{jt}, \alpha^{-it}, \alpha^{-jt}) = 0.$$

Note that $-j \not\equiv i \pmod{n}$ as otherwise $3 \mid n$, which is a contradiction. So there exists a weight four vector in $C(A)$ with non-zero values x_i, x_j, x_i, and x_j in the positions i, j, $-i$, and $-j$ (all indices are different), respectively.

So, in any case, after applying Theorem 3.5.3, we obtain a non-zero codeword of $\mathscr{C}_\gamma(A)$ with weight less than five and the sum of its coordinates is equal to zero. However, this contradicts Lemma 3.7.1. Thus, there is no weight three codeword in $\mathscr{C}_\gamma(A)$.

Finally, if $\mathscr{C}_\gamma(A)$ has a weight two codeword $y = ((b_{01}, b_{02}), (b_{i1}, b_{i2}))$, then there exists $x = (x_0, x_i) \in C(A)$. Thus for each $t \in A$, we have $x_0 + x_i \alpha^{it} = 0$ and $x_0 + x_i \alpha^{-it} = 0$. Now adding these two equations implies the existence of a weight two vector in $\mathscr{C}_\gamma(A)$ with the sum of the coordinates zero. However, this contradicts Lemma 3.7.1. Therefore, $\mathscr{C}_\gamma(A)$ has no codeword of weighs two, three, and four. □

Note that if we drop the condition $\gcd(n, 3) = 1$ in Theorem 3.7.2, then its result does not necessarily hold. We show this fact in the next example.

Example 3.7.3 Let $n = 15$ and $A = \{1, 2, 4, 7, 8, 11, 13, 14\}$ be a symmetric subset of $\mathbb{Z}/n\mathbb{Z}$. Our computation in Magma [17] shows that $d(\mathscr{C}_\gamma(A_0)) = 6$ and $d(\mathscr{C}_\gamma(A)) = 3$, where $\mathscr{C}_\gamma(A_0)$ and $\mathscr{C}_\gamma(A)$ are the twisted codes of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ with the complete defining set A_0 and A, respectively. Thus the result of Theorem 3.7.2 does not hold for $\mathscr{C}_\gamma(A)$.

The HT bound has not been used much in the literature to design codes with good properties. An interesting feature of twisted codes is the unsaturated intersection with the cyclotomic cosets, which allows us to select a portion of a cyclotomic coset in the defining set of a twisted code. This property makes the HT bound well-suited for twisted codes, and smart selection of the defining set can result in codes with good parameters. In fact we revive the HT bound by showing that proper selection of the defining set using the HT bound leads to the construction of new infinite families of twisted and quantum codes.

For an integer t, the notation $\pm t$ is used to present t and $-t$, and a set consisting of $\pm t$ contains both t and $-t$.

Corollary 3.7.4 *Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$, where $\gcd(n, 3) = 1$. If $\{\pm 1, \pm k, \pm(k+1)\} \subseteq A$ for some integer $1 \leq k \leq n-2$ and $\gcd(n, k) = \gcd(n, k+1) = 1$, then $\mathscr{C}_\gamma(A)$ has minimum distance at least five.*

Proof. Let $P = \{\pm 1, \pm k, \pm(k+1)\}$. First note that $\mathscr{C}_\gamma(A) \subseteq \mathscr{C}_\gamma(P)$ and $\mathscr{C}_\gamma(A_0) \subseteq \mathscr{C}(P_0)$. Moreover, $P_0 = \{0 + i_1 + ki_2 - (k+1)i_3 : 0 \leq i_1, i_2, i_3 \leq 1\}$. If $\gcd(n, k) = \gcd(n, k+1) = 1$, then the Hartmann-Tzeng bound given in Corollary 3.6.5 implies that $\mathscr{C}_\gamma(P_0)$ has minimum distance at least five. Thus Theorem 3.7.2 implies that $\mathscr{C}_\gamma(P)$ has minimum distance at least five. Since $\mathscr{C}_\gamma(A) \subseteq \mathscr{C}_\gamma(P)$ the code $\mathscr{C}_\gamma(A)$ has minimum distance at least five too. □

Table 3.2 represents the parameters of twisted codes obtained from the above corollary. We present parameters of such additive codes by $(n, 2^k, d)$, where n, k, d denote the length, dimension, and minimum distance of the code, respectively. In the table, for each length, among the codes with the same dimension, we only present the code with the largest minimum distance. Similarly, among the codes with the same length and minimum distance, we only give the code with the maximum dimension. Recall that we only consider the values of n such that $\gcd(n, 6) = 1$, and $17 \leq n \leq 89$.

In the following theorem, as an application of Corollary 3.7.4, we present two new infinite families of twisted codes with minimum distance at least five. These families will be used later in Theorem 3.8.5 to construct two new infinite families of binary quantum codes.

Theorem 3.7.5 *The following statements hold.*

1. *Let $t = 2^{2k+1}$ and $n = t^2 + t + 1$ for each $k \geq 1$. Then there exists a twisted code with parameters $(n, 2^{2n-6(2k+1)}, d \geq 5)$.*
2. *Let $t = 2^{2k}$ and $n = t^2 - t + 1$ for each $k \geq 1$. Then there exists a twisted code with parameters $(n, 2^{2n-12k}, d \geq 5)$.*

Proof. (1) First we show that the cyclotomic coset of 1 has size $|Z(1)| = 3(2k+1)$. Note that $2^{3(2k+1)} = t^3 \equiv -t^2 - t \equiv 1 \pmod{n}$. If $2^s \equiv 1 \pmod{n}$ for some $0 < s < 3(2k+1)$, then $s \leq 2k+1$ and thus $2^s \leq t < n$ which is impossible. Hence $|Z(1)| = 3(2k+1)$. This implies that $r = 3(2k+1)$ and $n \mid 2^r - 1$.

Let $\kappa = 2k+1$ and $A = \{\pm 1, \pm t, \pm(t+1)\}$. The fact that $|Z(1)|$ is an odd number implies that $Z(1) \neq Z(-1)$. Note that $1 = 2^0$, $t = 2^{(2k+1)}$, and $-(t+1) = 2^{2(2k+1)}$ which shows that $A \cap Z(1)$ is unsaturated and $-(A \cap Z(1)) = A \cap Z(-1)$. Hence both $A \cap Z(1)$ and $A \cap Z(-1)$ are unsaturated, and, by Theorem 3.4.8, the code $\mathscr{C}_\gamma(A)$ has dimension $2n - (|Z(1)| + |Z(-1)|) = 2n - 6(2k+1)$.

n	k	κ	parameters	n	k	κ	parameters
17	2	2	$(17, 2^{18}, 5)$	47	1	23	$(47, 2^2, 47)$
17	3	2	$(17, 2^{10}, 9)$	49	18	7	$(49, 2^{56}, 7)$
17	3	8	$(17, 2^2, 17)$	53	1	2	$(53, 2^2, 53)$
19	2	3	$(19, 2^2, 19)$	53	6	2	$(53, 2^{54}, 15)$
19	8	3	$(19, 2^{20}, 7)$	55	1	2	$(55, 2^{30}, 5)$
23	1	11	$(23, 2^2, 23)$	59	1	2	$(59, 2^2, 59)$
25	1	2	$(25, 2^{10}, 5)$	61	1	2	$(61, 2^2, 61)$
29	1	2	$(29, 2^2, 29)$	61	3	2	$(61, 2^{62}, 17)$
29	4	2	$(29, 2^{30}, 11)$	65	1	2	$(65, 2^{106}, 5)$
31	1	5	$(31, 2^{42}, 5)$	67	1	2	$(67, 2^2, 67)$
31	2	5	$(31, 2^{32}, 9)$	67	8	3	$(67, 2^{68}, 17)$
35	1	2	$(35, 2^{22}, 5)$	71	1	5	$(71, 2^2, 71)$
37	1	2	$(37, 2^2, 37)$	73	2	3	$(73, 2^{92}, 12)$
37	3	2	$(37, 2^{38}, 11)$	73	7	3	$(73, 2^{110}, 7)$
41	2	2	$(41, 2^{22}, 20)$	73	8	3	$(73, 2^{128}, 5)$
41	3	2	$(41, 2^{42}, 11)$	77	9	2	$(77, 2^{94}, 7)$
41	2	4	$(41, 2^2, 41)$	79	1	3	$(79, 2^2, 79)$
43	1	2	$(43, 2^{58}, 6)$	79	23	13	$(79, 2^{80}, 17)$
43	2	2	$(43, 2^{30}, 13)$	83	1	2	$(83, 2^2, 83)$
43	6	2	$(43, 2^2, 43)$	85	1	2	$(85, 2^{138}, 5)$
43	6	7	$(43, 2^{44}, 11)$	89	3	11	$(89, 2^{106}, 14)$

Table 3.2: Twisted codes satisfying Corollary 3.7.4.

One can easily see that $\gcd(n, t) = 1$ and $\gcd(n, t+1) = \gcd(n, t^2) = 1$. Moreover, $t \equiv 2 \pmod 3$, which implies that $\gcd(n, 3) = 1$. So the code $\mathscr{C}_\gamma(A)$ satisfies the conditions of Corollary 3.7.4 and we have $d(\mathscr{C}_\gamma(A)) \geq 5$. Therefore, the code $\mathscr{C}_\gamma(A)$ has parameters $\left(n, 2^{2n-6(2k+1)}, d \geq 5\right)$.

(2) We first show that $Z(1) = Z(-1)$ and $|Z(1)| = 12k$. Note that $2^{3(2k)} = t^3 \equiv -1 \pmod n$. Thus $-1 \in Z(1)$ which implies that $|Z(1)|$ is an even number and $|Z(1)| \mid 12k$. If $|Z(1)| = 2s < 12k$, then $2^s \equiv -1 \pmod n$. But we have $2^s \leq 2^{3k} < n - 1$, which is a contradiction. Hence $|Z(1)| = 12k$. This implies that $r = 12k$ and $n \mid 2^r - 1$.

Let $\kappa = 2k$ and $A = \{\pm 1, \pm(t-1), \pm t\} = \{2^{\kappa i} : 0 \leq i \leq 5\}$. This shows that $A \cap Z(1)$ is unsaturated and $-(A \cap Z(1)) = A \cap Z(-1)$. Thus, the intersection $A \cap Z(1)$ is unsaturated and, by Theorem 3.4.8, the code $\mathscr{C}_\gamma(A)$ has dimension $2n - |Z(1)| = 2n - 12k$.

It is easy to see that $\gcd(n, t) = 1$ and $\gcd(n, t-1) = \gcd(n, t^2) = 1$. Moreover, $t \equiv 1 \pmod 3$, which implies that $\gcd(n, 3) = 1$. So Corollary 3.7.4 implies that the code $d(\mathscr{C}_\gamma(A)) \geq 5$. Therefore, the code $\mathscr{C}_\gamma(A)$ has parameters $\left(n, 2^{2n-12k}, d \geq 5\right)$. □

Note that in the proof of Case (2), the selections $\kappa = 2$ and $\kappa = k$ both imply the same result. Choosing $k = 1$ in Cases (1) and (2) of Theorem 3.7.5 gives additive codes with parameters $(73, 2^{128}, 5)$ and $(13, 2^{14}, 5)$, respectively.

We finish this section by presenting a general upper bound for the minimum distance of twisted codes. Such minimum distance upper bound is useful for computational purposes. Recall that by (3.4.7), we have $\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp)$, where A_d is the complete defining set of the twisted code $\mathscr{C}_\gamma(A)^{\perp_s}$.

Theorem 3.7.6 *Let A and A_d be the complete defining sets of non-zero twisted codes $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A_d)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$, respectively. Then $d\big(C(A_d)^\perp\big) \geq d\big(\mathscr{C}_\gamma(A)\big)$.*

Proof. By the definition of twisted codes, we have $\mathscr{C}_\gamma(A) = \{(\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)) : x \in C(A_d)^\perp\}$. Let $x = (x_0, x_1, \ldots, x_{n-1}) \in C(A_d)^\perp$ be a minimum weight vector with $\mathrm{wt}(x) = s$. Without loss of generality, we can assume that $y = \big(\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)\big)$ is not zero, as otherwise, we can find a non-zero scalar $a \in \mathbb{F}_{2^r}$ such that $\big(\mathrm{Tr}_1^r(ax), \mathrm{Tr}_1^r(\gamma a x)\big)$ is not the zero vector. The vector x has exactly $n - s$ coordinates with entry zero. Since the trace map preserves the zero coordinates, y is non-zero and has at least $n-s$ zero coordinates. Hence, $d\big(C(A_d)^\perp\big) = \mathrm{wt}(x) \geq \mathrm{wt}(y) \geq d\big(\mathscr{C}_\gamma(A)\big)$. □

Next, we squeeze the minimum distance of a twisted code between the minimum distances of two linear cyclic codes over $\mathbb{F}_{2^r}$.

Corollary 3.7.7 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining set of a twisted code. Then*

$$d\big(C(A_d)^\perp\big) \geq d\big(\mathscr{C}_\gamma(A)\big) \geq d\big(C(A)\big). \tag{3.7.5}$$

Proof. The upper and lower distance bounds on $\mathscr{C}_\gamma(A)$ follow from Theorem 3.7.6 and Corollary 3.6.3, respectively. □

3.8 New infinite families of quantum codes

In this section, we first provide a secondary construction for binary quantum codes that are also dual-containing twisted codes. In particular, this construction produces a quantum code with a larger length and an improved minimum distance provided certain conditions are satisfied. Next, we give several new infinite families of binary quantum codes. One of the main features of these new families is that they can be constructed easily and their parameters can be computed computer-free. For each of these families, we provide a numerical example of a good (optimal or record-breaking) binary quantum code. Moreover, we present more record-breaking quantum codes after applying secondary constructions of Theorems 1.7.3 and 1.7.6 to our new binary quantum codes.

Recall that n is a positive integer such that $n \mid 2^r - 1$ for some positive integer r and $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Moreover, $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. We first state a result from the literature, which is a secondary construction for binary quantum code constructed using twisted codes. Let A be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Recall that, as we stated in Theorem 3.4.12, if $\mathscr{C}_\gamma(A)^{\perp_s} \subseteq \mathscr{C}_\gamma(A)$, then there exists a binary quantum code with parameters $[\![n,k,d]\!]$, where $\dim(\mathscr{C}_\gamma(A)) = n+k$ and $d(\mathscr{C}_\gamma(A)) = d$. In this section, the code $\mathscr{C}_\gamma(A)$, with the above properties, will be called an $[\![n,k,d]\!]$ quantum code.

Theorem 3.8.1 *[13, Theorem 8] Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\mathscr{C}_\gamma(A)$ be a binary quantum code with parameters $[\![n,k,t]\!]$. If A contains the interval $[1, t-1]$, then the extended code of $\mathscr{C}_\gamma(A \cup \{0\})$ is a binary quantum code with parameters $[\![n+1, k-1, t+1]\!]$.*

In the next theorem, we give another secondary construction for the binary quantum codes that are constructed from twisted codes. It also generalizes the result of Theorem 3.8.1 above. In general, the lengthening construction of the above theorem only relies on the BCH bound. However, our construction considers the general case even if the BCH bound does not provide a minimum distance improvement. As we will see in Example 3.8.3, our secondary construction goes beyond the result of Theorem 3.8.1. Moreover, Case (ii) of our construction has another potential for one unit lengthening of quantum codes.

Theorem 3.8.2 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\mathscr{C}_\gamma(A)$ be a pure binary quantum code with parameters $[\![n,k,t]\!]$. Then the following results hold.*

(i) If $d(\mathscr{C}_\gamma(\bar{A})) = t+1$, where $\bar{A} = A \cup \{0\}$, then there exists an $[\![n+1, k-1, t+1]\!]$ quantum code.

(ii) If $\kappa = 2$ and $\{a, n-a\}$ is a 2-cyclotomic coset such that $d(\mathscr{C}_\gamma(\bar{A})) = t+1$ for $\bar{A} = A \cup \{a\}$, then there exists an $[\![n+1, k-1, t+1]\!]$ quantum code.

Proof. We prove both cases simultaneously. Since $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$, Corollary 3.5.6 implies that code $\mathscr{C}_\gamma(\bar{A})$ has the dual-containment deficiency $e = 1$ in both Case (i) and (ii). Moreover, $\dim(\mathscr{C}_\gamma(A)) = n+k$ and $\dim(\mathscr{C}_\gamma(\bar{A})) = n+k-2$. Next by applying the quantum construction given in Theorem 3.5.7 to $\mathscr{C}_\gamma(\bar{A})$, we obtain a quantum code with parameters $[\![n+1, k-1, d]\!]$, where $d \geq \min\{d(\mathscr{C}_\gamma(\bar{A})), d(\mathscr{C}_\gamma(\bar{A}) + \mathscr{C}_\gamma(\bar{A}_d)) + 1\}$. Next Proposition 3.5.4 implies that

$$\mathscr{C}_\gamma(\bar{A}) + \mathscr{C}_\gamma(\bar{A}_d) = \mathscr{C}_\gamma(\bar{A} \cap \bar{A}_d) = \mathscr{C}_\gamma(A).$$

By the assumption $d(\mathscr{C}_\gamma(\bar{A})) = t+1$ and $d(\mathscr{C}_\gamma(A)) = t$. Therefore, $d \geq t+1$ and this completes the proof. □

In the next example, we construct a new binary quantum code using the above result.

Example 3.8.3 Let $n = 63$, $\kappa = 3$, and $A = \{27, 38, 52\}$ be the complete defining set of the length n twisted code $\mathscr{C}_\gamma(A)$. The 2-cyclotomic cosets modulo 63 which intersect A are $Z(13) = \{13, 26, 52, 41, 19, 38\}$ and $Z(27) = \{27, 54, 45\}$. One can easily see that the intersections $A \cap Z(13)$ and $A \cap Z(27)$ are both unsaturated and $A \cap Z(-13) = A \cap Z(-27) = \emptyset$. Thus by Theorem 3.4.11, $\mathscr{C}_\gamma(A)$ is dual-containing and has dimension $126 - (|Z(13)| + |Z(27)|) = 117$ over $\mathbb{F}_2$. Since $\gcd(63, 11) = 1$, the set $\{27, 38\} = \{27 + 11i : 0 \leq i \leq$

$1\} \subset A$ is a consecutive set. Hence Theorem 3.6.1 implies that $d(\mathscr{C}_\gamma(A)) \geq 3$. Therefore, Theorem 3.5.7 implies that $\mathscr{C}_\gamma(A)$ is a $[\![63, 54, 3]\!]$ binary quantum code.

Let $\bar{A} = A \cup \{0\} = \{27 + 25i_1 + 11i_2 :\ 0 \leq i_1, i_2 \leq 1\}$. By Corollary 3.6.5, $d(\mathscr{C}(\bar{A})) \geq 4$. Thus, part (i) of Theorem 3.8.2 implies a *new quantum code* with parameters $[\![64, 53, 4]\!]$. This code is pure and has minimum distance better than the previously best-known quantum code with the same length and dimension. Note that by applying the BCH bound to the code $\mathscr{C}_\gamma(\bar{A})$, we get the minimum distance lower bound of three. Hence the argument given in Theorem 3.8.1 cannot directly produce a distance four binary quantum code.

Recall that we defined the shortening construction of quantum codes as in Theorem 1.7.6. Let C be the $[\![64, 53, 4]\!]$ binary quantum code of Example 3.8.3. After applying Theorem 1.7.6 to the code C, we get the following *new pure quantum codes*

$$[\![38, 27, 4]\!], [\![44, 33, 4]\!], [\![46, 35, 4]\!], [\![48, 37, 4]\!], [\![50, 39, 4]\!], [\![56, 45, 4]\!], \tag{3.8.1}$$

where all have better minimum distance than the previously best-known quantum codes with the same length and dimension. In the next section, we show that all these codes are optimal. Next, we construct an infinite family of quantum codes with minimum distance at least four.

Theorem 3.8.4 *Let $r > 5$ be an even integer. Then there exists a binary quantum code with parameters*

$$[\![2^r, 2^r - \frac{3}{2}r - 2, d \geq 4]\!].$$

Proof. Let $n = 2^r - 1$, $\kappa = \frac{r}{2}$, and $A = \{1, a, b\}$, where $a = 2^{\frac{r}{2}} + 1$ and $b = 2^{\frac{r}{2}}$. Note that $Z(1) = \{1, 2, 2^2, \dots, 2^{r-1}\}$ is a size r cyclotomic coset and $Z(1) \neq Z(-1)$ since $-1 \equiv 2^r - 2 \pmod{n}$ and $2^r - 2 \notin Z(1)$ $(2^{r-1} < 2^r - 2)$. Also, $Z(a) = \{2^{\frac{r}{2}} + 1, 2(2^{\frac{r}{2}} + 1), \dots, 2^{\frac{r}{2}-1}(2^{\frac{r}{2}} + 1)\}$ and therefore $|Z(a)| = \frac{r}{2}$.

The intersections $Z(1) \cap A$ and $Z(a) \cap A$ are both unsaturated and Theorem 3.4.11 implies that the twisted code $\mathscr{C}_\gamma(A)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ is dual-containing with dimension $2n - (|Z(1)| + |Z(a)|) = 2^{r+1} - \frac{3r}{2} - 2$ over $\mathbb{F}_2$. Moreover, $\{a, b\} = \{2^{\frac{r}{2}} + i : 0 \leq i \leq 1\} \subset A$ is a consecutive set. Thus $d(\mathscr{C}_\gamma(A)) \geq 3$ and the quantum construction given in Theorem 3.5.7 implies that $\mathscr{C}_\gamma(A)$ is a $[\![2^r - 1, 2^r - \frac{3}{2}r - 1, 3]\!]$ pure quantum code. Let $\bar{A} = \{0, 1, a, b\} = \{0, 1\} + \{0, b\}$. Corollary 3.6.6 implies that $d(\mathscr{C}_\gamma(A)) \geq 4$ and therefore Theorem 3.8.2 gives a $[\![2^r, 2^r - \frac{3}{2}r - 2, d \geq 4]\!]$ quantum code. □

For instance, if $r = 6$, the above construction gives a $[\![64, 53, 4]\!]$ quantum code which has the same parameters as the result of Example 3.8.3 and is a new quantum code. Next, we present two new infinite families of quantum codes with minimum distance at least five.

Theorem 3.8.5 (i) *Let $t = 2^{2k+1}$ for some integer $k \geq 1$ and $n = t^2 + t + 1$. Then there exists an $[\![n, n - 12k - 6, d \geq 5]\!]$ binary quantum code.*

(ii) Let $t = 2^{2k}$ for some integer $k \geq 1$ and $n = t^2 - t + 1$. Then there exists an $[\![n, n - 12k, d \geq 5]\!]$ binary quantum code.

Proof. Let $\kappa = 2k + 1$ and $A = \{\pm 1, \pm t, \pm(t + 1)\}$. As we showed in the proof of Theorem 3.7.5 part (1), we have $r = 3(2k + 1)$ which implies that $\kappa \mid r$. Moreover, the code $\mathscr{C}_\gamma(A)$ has parameters $(n, 2^{2n-6(2k+1)}, d \geq 5)$ and the intersection $A \cap Z(1)$ is purely unsaturated. So by Theorem 3.4.11 the code $\mathscr{C}_\gamma(A)$ is dual-containing. Now the quantum construction given in Theorem 3.5.7 implies a binary quantum code with parameters $[\![n, n - 12k - 6, d \geq 5]\!]$.

(ii) : Let $\kappa = 2k$ and $A = \{\pm 1, \pm t, \pm(t - 1)\} = \{2^{\kappa i} : 0 \leq i \leq 5\}$. As we showed in the proof of Theorem 3.7.5 part (2), we have $r = 12k$ which implies that $\kappa \mid r$. Moreover, the code $\mathscr{C}_\gamma(A)$ has parameters $(n, 2^{2n-12k}, d \geq 5)$ and the intersection $A \cap Z(1)$ is purely unsaturated. So by Theorem 3.4.11 the code $\mathscr{C}_\gamma(A)$ is dual-containing. Now the quantum construction given in Theorem 3.5.7 gives a quantum code with parameters $[\![n, n - 12k, d \geq 5]\!]$. □

This construction can be used to produce good binary quantum codes. For instance, we construct two new record-breaking quantum codes with minimum distance of five using this result.

Example 3.8.6 *(i)* Let $t = 2^3$, $n = t^2 + t + 1 = 73$, and $A = \{\pm 1, \pm 8, \pm 9\}$. Then Theorem 3.8.5 part *(i)* gives a quantum code with parameters $[\![73, 55, 5]\!]$. This code is a *record-breaking quantum code.*

(ii) Let $t = 2^4$, $n = t^2 - t + 1 = 241$, and $A = \{\pm 1 \pm 15, \pm 16\}$. The construction given in part *(ii)* of Theorem 3.8.5 implies a *record-breaking quantum code* with parameters $[\![241, 217, 5]\!]$.

Note that modifying the codes provided in parts *(i)* and *(ii)* of the above example can produce more record-breaking quantum codes. One example of such new codes is provided below.

Example 3.8.7 (i) Let $n = 73$, $\kappa = 3$, and $A = \{\pm 1, \pm 8, \pm 9, 20, 14, 39\}$. Then one can easily verify that $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$. Moreover, the code $\mathscr{C}_\gamma(A)$ has dimension 119 and minimum distance 7. Hence the quantum construction given in Theorem 3.5.7 implies a binary quantum code with parameters $[\![73, 46, 7]\!]$. This is a new quantum code with *better minimum distance* than the previous best quantum codes with the same length and dimension.

(ii) Let $n = 241$, $\kappa = 2$, and $A = \{\pm 1, \pm 3, \pm 4, \pm 12, \pm 15, \pm 16, \pm 45, \pm 48, \pm 49, \pm 60, \pm 61, \pm 64\}$. An easy computation shows that $A \cap Z(1)$ and $A \cap Z(3)$ are purely unsaturated. Thus $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$. Moreover, $|Z(1)| = |Z(3)| = 24$. Thus the code $\mathscr{C}_\gamma(A)$ has dimension 434 and minimum distance 8. Now, the quantum construction given in Theorem 3.5.7 implies a binary quantum code with parameters $[\![241, 193, 8]\!]$. This is a new binary quantum code with *better minimum distance* than the previous best quantum codes with the same length and dimension. Applying the secondary constructions given in Theorem 1.7.3 gives 27 other record-breaking binary quantum codes. Moreover, this codes can be used to reconstruct 58 other binary quantum code with missing constructions (represented in red in [43]).

In Definition 2.2.1, we recalled the concept of splitting of $\mathbb{Z}/n\mathbb{Z}$ given by certain multipliers. This identified the class of duadic linear codes. Moreover, as we showed in Chapter 2, many new record-breaking quantum codes were constructed using duadic codes. A generalization of duadic codes, called polyadic or m-adic codes, is defined similarly by considering a splitting of $\mathbb{Z}/n\mathbb{Z}$ that consists of more than two disjoint subsets of $\mathbb{Z}/n\mathbb{Z}$ [19, 66, 82]. Analogously, we define the m-splitting for twisted codes.

Definition 3.8.8 Let $m \geq 2$ be a positive integer and $X_\infty \subseteq \mathbb{Z}/n\mathbb{Z}$ be a non-empty subset. An *m-splitting* of $\mathbb{Z}/n\mathbb{Z}$ is the $m+1$-tuple $(X_\infty, X_0, \ldots, X_{m-1})$ such that

- $\emptyset \neq X_i \subseteq \mathbb{Z}/n\mathbb{Z}$ for $0 \leq i \leq m-1$,
- $(X_\infty, X_0, \ldots, X_{m-1})$ is a partition of $\mathbb{Z}/n\mathbb{Z}$,
- all the elements of $(X_\infty, X_0, \ldots, X_{m-1})$ are complete defining sets,
- there exists a multiplier μ_b such that $\mu_b(X_\infty) = X_\infty$ and $\mu_b(X_j) = X_{j+1}$ for $0 \leq j \leq m-1$, where the subscripts are taken modulo m.

Recall that $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ and $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. Let Z be a 2-cyclotomic coset modulo n with the coset leader a and $|Z| = s$. Recall that if $\kappa \mid s$, then there are κ different possible unsaturated intersections with the set Z. Such unsaturated intersections can be represented explicitly as

$$Z^{(j)} = \{(2^{\kappa i + j}a) \bmod n : 0 \leq i \leq \frac{s}{\kappa} - 1\}$$

for all $0 \leq j \leq \kappa - 1$. In the next theorem, we provide an m-splitting for twisted codes, which leads to a class of good binary quantum codes. As we will see later, this class is capable of producing record-breaking binary quantum codes.

Theorem 3.8.9 *Let n be a positive integer such that $n \mid 2^{\kappa s} + 1$ for some positive integer s. Then the tuple $(X_\infty, X_0, \ldots, X_{\kappa-1})$ is a twisted κ-splitting of $\mathbb{Z}/n\mathbb{Z}$, where*

- $X_\infty = \bigcup_{\kappa \nmid |Z|} Z,$
- $X_j = \bigcup_{\kappa || Z|} Z^{(j)}$*, for* $0 \leq j \leq \kappa - 1,$

and the unions run over all 2-cyclotomic cosets modulo n satisfying the given condition. Moreover, the twisted code $\mathscr{C}_\gamma(X_j)$ of length n over $\mathbb{F}_2 \times \mathbb{F}_2$ is a binary quantum code with parameters $[\![n, |X_\infty|, d(\mathscr{C}_\gamma(X_j))]\!]$ for each $0 \leq j \leq \kappa - 1$.

Proof. Obviously, all the elements of the tuple $(X_\infty, X_0, \ldots, X_{\kappa-1})$ are complete defining sets, disjoint, and $\mathbb{Z}/n\mathbb{Z} = X_\infty \cup \bigcup_{i=0}^{\kappa-1} X_i$. Moreover, $\mu_2(X_\infty) = X_\infty$ and $\mu_2(X_j) = X_{j+1}$ for all $0 \leq j \leq m-1$. Hence $(X_\infty, X_0, \ldots, X_{\kappa-1})$ is a κ-splitting of $\mathbb{Z}/n\mathbb{Z}$.

Next, we show that $\mathscr{C}_\gamma(X_0)$ is a binary quantum code with the mentioned parameters. The proof for any other X_j follows similarly. First, note that $2^{\kappa s} \equiv -1 \pmod n$ and therefore we have $a \in X_0$ if and only if $-a \in X_0$. Thus, by Definition 3.4.9, we have

$$X_0 \cap Z = \begin{cases} \text{purely unsaturated} & \text{if } \kappa \mid |Z| \\ \emptyset & \text{otherwise} \end{cases}$$

for all different 2-cyclotomic cosets Z modulo n. Thus Theorem 3.4.11 implies that $\mathscr{C}_\gamma(X_0)$ is symplectic dual-containing. Moreover,

$$\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(X_0)) = \sum_{\kappa \mid |Z|} |Z| + \sum_{\kappa \nmid |Z|} 2|Z| = n + |X_\infty|.$$

Now Theorem 3.5.7 implies that $\mathscr{C}_\gamma(X_0)$ is a binary quantum code and it has the parameters $[\![n, |X_\infty|, d(\mathscr{C}_\gamma(X_0))]\!]$. □

Note that, as we will show in Corollary 3.10.15, all the quantum codes $\mathscr{C}_\gamma(X_j)$ are permutation equivalent for each $0 \leq j \leq \kappa - 1$. Hence it is sufficient to consider only one of them in our computations. Next, we give an application of this result by producing a record-breaking binary quantum code.

Example 3.8.10 Let $n = 57$ and $\gamma \in \mathbb{F}_8 \setminus \mathbb{F}_2$. An easy computation shows that $n \mid 2^9 + 1$. Since $\kappa = 3 \mid 9$, all the requirements of Theorem 3.8.9 are satisfied. The following are different 2-cyclotomic cosets modulo n

$$Z(1) = \{1, 2, 4, 8, 16, 32, 7, 14, 28, 56, 55, 53, 49, 41, 25, 50, 43, 29\},$$

$$Z(6) = \{6, 12, 24, 48, 39, 21, 42, 27, 54, 51, 45, 33, 9, 18, 36, 15, 30, 3\},$$

$$Z(11) = \{11, 22, 44, 31, 5, 10, 20, 40, 23, 46, 35, 13, 26, 52, 47, 37, 17, 34\},$$

$$Z(19) = \{19, 38\}, Z(0) = \{0\}.$$

Since κ only does not divide $|Z(0)|$ and $|Z(19)|$, after applying Theorem 3.8.9, we get $X_\infty = Z(0) \cup Z(19)$ and $X_i = Z(1)^{(i)} \cup Z(6)^{(i)} \cup Z(11)^{(i)}$ for $0 \leq i \leq 2$. Hence $(X_\infty, X_0, X_1, X_2)$ forms a twisted 3-splitting of $\mathbb{Z}/n\mathbb{Z}$. Moreover, our minimum distance computation in Magma [17] gives $d(\mathscr{C}_\gamma(X_0)) = 14$. Hence $\mathscr{C}_\gamma(X_0)$ is a binary quantum code with the parameters $[\![57, 3, 14]\!]$. This code is a *record-breaking* binary quantum code with a better minimum distance than the previously best-known quantum code, namely $[\![57, 3, 13]\!]$.

Next, we determine two other classes of quantum codes. These classes are capable of producing quantum codes that have the same minimum distance as the currently best-known quantum codes with the same length and dimension. As we mentioned at the beginning of Section 3.7, the algebraic structure of such twisted codes could be extremely beneficial for the practical implementation of such quantum codes.

Theorem 3.8.11 *(i) Let $t \geq 4$ be an even integer and $n = 2^t + 1$. Then there exists a pure quantum code with parameters*

$$[\![2^t + 1, 2^t - 2t + 1, d \geq 4]\!].$$

(ii) Let $t \geq 3$ be an odd integer and $n = 2^t + 1$. Then there exists a pure quantum code with parameters

$$[\![2^t + 2, 2^t - 2t, d \geq 4]\!].$$

Proof. In both cases (i) and (ii), the cyclotomic coset of 1 modulo n is

$$Z(1) = \{1, 2, 2^2, \ldots, 2^{t-1}, -1, -2, \ldots, -2^{t-1}\} = Z(-1).$$

Thus $|Z(1)| = 2t$.

(i) Let $A = \{1, 2^{\frac{t}{2}}, -1, -2^{\frac{t}{2}}\}$ and $\kappa = \frac{t}{2}$ $(\kappa \mid r = 2t)$. Then $Z(1) \cap A$ is purely unsaturated. So by Theorem 3.4.11, we have $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$. Hence the quantum construction given in Theorem 3.5.7 implies a binary quantum code with parameters $[\![2^t+1, 2^t+1-2t]\!]$. Also, we can write A as $A = \{1, -2^{\frac{t}{2}}\} + \{0, 2^{\frac{t}{2}} - 1\}$. Hence by Theorem 3.6.5, we have $d(\mathscr{C}_\gamma(A)) \geq 4$. Therefore, there exists a $[\![2^t + 1, 2^t + 1 - 2t, d \geq 4]\!]$ pure quantum code.

(ii) Let $A = \{-1, 1\}$ and $\kappa = t$ $(\kappa \mid r)$. Then $Z(1) \cap A$ is purely unsaturated. So by Theorem 3.4.11, we have $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$. Since $\{-1, 1\}$ is consecutive, the quantum construction given in Theorem 3.5.7 implies a binary pure quantum code with parameters $[\![2^t + 1, 2^t - 2t + 1, 3]\!]$. Let $A' = A \cup \{0\}$. Then A' is a consecutive set of length 3, so by the Theorem 3.8.2 part (i), we obtain a pure quantum code with the parameters $[\![2^t + 2, 2^t - 2t, d \geq 4]\!]$. □

The following codes are all obtained from the above construction, and all have the same minimum distance as the currently best-known binary quantum codes with the same length and dimension:

$$[\![10, 2, 4]\!], [\![17, 9, 4]\!], [\![34, 22, 4]\!], [\![65, 53, 4]\!], [\![130, 114, 4]\!]. \tag{3.8.2}$$

3.9 Quantum bounds and optimal codes

In this section, we recall the Singleton and Hamming bounds for quantum codes and show that ten of our binary quantum codes in the previous section are optimal. The *quantum*

Singleton bound, which was first given in [61], states that an $[\![n,k,d]\!]$ binary quantum code with $k > 0$ satisfies

$$n - k \geq 2(d-1).$$

Another simple bound relating the length, dimension, and minimum distance of a quantum code is the *quantum Hamming bound*, which is also known as the Sphere-packing bound [42]. This bound states that a pure $[\![n,k,d]\!]$ binary quantum code with $e = \lfloor \frac{d-1}{2} \rfloor$ satisfies

$$\sum_{j=0}^{e} \binom{n}{j} 3^j \leq 2^{n-k}. \tag{3.9.1}$$

Let Q be an $[\![n,k,d]\!]$ binary pure quantum code. Then Q will be called an *optimal pure* code, if there is no $[\![n,k,d']\!]$ binary pure quantum code, where $d' > d$. Next, we prove that ten of our quantum codes are optimal pure.

Theorem 3.9.1 *The quantum code* $[\![130,114,4]\!]$ *in (3.8.2) is not optimal pure and all the other quantum codes in Example 3.8.3 and lists (3.8.1) and (3.8.2) are optimal pure quantum codes.*

Proof. We only give a proof for one of these codes, and a similar argument shows that the other codes are optimal. In Example 3.8.3, we showed the existence of a $[\![64,53,4]\!]$ binary pure quantum code. Now we prove that this code is optimal. It is enough to show that there is no pure binary quantum code Q with parameters $[\![64,53,d \geq 5]\!]$. Let $e = \lfloor \frac{d-1}{2} \rfloor$. Then $e \geq 2$ and applying the Hamming bound to Q gives

$$\sum_{j=0}^{e} \binom{n}{j} 3^j \geq \sum_{j=0}^{2} \binom{n}{j} 3^j = 18337 > 2^{64-53} = 2048.$$

Hence there is no binary pure quantum code with parameters $[\![64,53,d \geq 5]\!]$. This proves that the quantum code of Example 3.8.3 is an optimal pure quantum code. □

3.10 Selection of γ value in twisted codes

Throughout this section, n is a positive integer such that $n \mid 2^r - 1$ for some positive integer r. As we mentioned in Definition 3.4.2, the main ingredients in the construction of a length n twisted code over $\mathbb{F}_2 \times \mathbb{F}_2$ are $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ and the complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$. Moreover, by Definition 3.4.7, the complete defining set of a twisted code is influenced using the degree of the field extension $[\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. Therefore, the choice of γ is a critical factor in the construction of twisted codes. Interestingly, the literature appears to have ignored the impacts of γ on the parameters of twisted codes.

In this section, we introduce various new insights into how the parameters of twisted codes are influenced by the selection of γ. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a defining set, not necessarily complete, of a length n twisted code over $\mathbb{F}_2 \times \mathbb{F}_2$ and let γ_1 and $\gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. We first show that if $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$, then the twisted codes constructed using γ_1 and γ_2 always have the same complete defining set and hence the same dimension. Next, we show that if $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2] \leq 3$, then the parameters of twisted codes are independent of the choice of γ_1 and γ_2. We also prove that for every $\kappa > 3$ if

$$s_\kappa = |\{\gamma \in \mathbb{F}_{2^r} : [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = \kappa\}|,$$

then there are at most $s_\kappa/6$ many different twisted codes constructed using different values of γ and the same complete defining set. Finally, through an example, we show the existence of A, γ_1, and γ_2 satisfying $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$ such that the twisted codes with the complete defining set A constructed using γ_1 and γ_2 have different minimum distances. Hence the choice of γ can change the parameters of twisted codes.

The next example shows that if we start with an incomplete defining set A, then different selections of γ values imply twisted codes with different complete defining sets and dimensions.

Example 3.10.1 Let $n = 15$. Note that $n \mid 2^4 - 1$ and therefore γ can be any element of $\mathbb{F}_{16} \setminus \mathbb{F}_2$. The 2-cyclotomic coset of 1 modulo 15 is $Z(1) = \{1, 2, 4, 8\}$.

Case 1: Let $\gamma_1 \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and $A = \{1, 4\}$. Since $\kappa_1 = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = 2$, the set A is the complete defining set and $A \cap Z(1)$ is unsaturated. Therefore the twisted code $\mathscr{C}_{\gamma_1}(A)$ has dimension 26 over $\mathbb{F}_2$.

Case 2: Let $\gamma_2 \in \mathbb{F}_{16} \setminus \mathbb{F}_4$ and $A = \{1, 4\}$. Then $\kappa_2 = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2] = 4$. In this case, A is an incomplete defining set, and we apply Definition 3.4.7 to form the complete defining set of A. Since $1, 4 \in A$, it follows that $A \cap Z(1)$ is saturated. Thus the complete defining set containing A is $\tilde{A} = Z(1)$. The twisted code $\mathscr{C}_{\gamma_2}(A)$ has dimension 22 over $\mathbb{F}_2$.

In the above cases, we started with the same (incomplete) defining set A and found different complete defining sets. Moreover, we obtained different dimensions for the corresponding twisted codes.

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. In the rest of this section, to avoid confusion, we denote the complete defining sets corresponding to the set A and the values γ_1 and γ_2 by A_{γ_1} and A_{γ_2}, respectively. The next theorem provides necessary and sufficient conditions for the values γ_1 and γ_2 to have the same complete defining sets, i.e., $A_{\gamma_1} = A_{\gamma_2}$.

Theorem 3.10.2 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. Then $A_{\gamma_1} = A_{\gamma_2}$ if and only if at least one of the following conditions hold:*

1. *The elements γ_1 and γ_2 satisfy $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$.*

2. *For each 2-cyclotomic coset Z modulo n that intersects A, the intersections $A_{\gamma_1} \cap Z$ and $A_{\gamma_2} \cap Z$ are both saturated.*

Proof. We first show that each of conditions (1) and (2) above implies $A_{\gamma_1} = A_{\gamma_2}$. Let γ_1 and $\gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ such that $\kappa = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$. By Definition 3.4.4, the saturated and unsaturated intersections both only depend on the set A and the value of κ. Thus for each 2-cyclotomic coset Z modulo n intersecting A, we have $A_{\gamma_1} \cap Z$ and $A_{\gamma_2} \cap Z$ both are saturated or both are unsaturated. This implies $A_{\gamma_1} = A_{\gamma_2}$. If $A_{\gamma_1} \cap Z$ and $A_{\gamma_2} \cap Z$ are saturated for each 2-cyclotomic coset Z that intersects A, then obviously $A_{\gamma_1} = A_{\gamma_2}$.

Now we show that if both of the conditions (1) and (2) are not satisfied, then $A_{\gamma_1} \neq A_{\gamma_2}$. Let $\kappa_1 = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] \neq [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2] = \kappa_2$, and $Z = \{a, 2a, \cdots, 2^{s-1}a\}$ be an ordered 2-cyclotomic coset modulo n of size s such that $a \in A \cap Z$ and $A_{\gamma_1} \cap Z$ is unsaturated. If $A_{\gamma_2} \cap Z$ is saturated, then obviously $A_{\gamma_1} \neq A_{\gamma_2}$. So we assume that $A_{\gamma_2} \cap Z$ is also unsaturated. If $\kappa_1 < \kappa_2$, then $a2^{\kappa_1} \in A_{\gamma_1}$ and $a2^{\kappa_1} \notin A_{\gamma_2}$. If $\kappa_1 > \kappa_2$, then $a2^{\kappa_2} \in A_{\gamma_2}$ and $a2^{\kappa_2} \notin A_{\gamma_1}$. So, in any case, $A_{\gamma_1} \neq A_{\gamma_2}$. □

Next, we give a consequence of this result on the dimension of twisted codes constructed using different values of γ.

Corollary 3.10.3 *Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ and $\gamma_1, \gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$. If the condition* (1) *or* (2) *of Theorem* 3.10.2 *is satisfied, then the twisted codes $\mathscr{C}_{\gamma_1}(A_{\gamma_1})$ and $\mathscr{C}_{\gamma_2}(A_{\gamma_2})$ have the same dimension over $\mathbb{F}_2$.*

Proof. Theorem 3.10.2 implies that $A_{\gamma_1} = A_{\gamma_2}$. Thus for each 2-cyclotomic coset Z modulo n we have $A_{\gamma_1} \cap Z = A_{\gamma_2} \cap Z$. Hence $A_{\gamma_1} \cap Z = A_{\gamma_2} \cap Z$ have the same status as empty, saturated, or unsaturated. Hence, by Theorem 3.4.8, the codes $\mathscr{C}_{\gamma_1}(A_{\gamma_1})$ and $\mathscr{C}_{\gamma_2}(A_{\gamma_2})$ have the same dimension. □

Recall that, as we mentioned in Theorem 3.5.1, the twisted codes satisfying part (2) of Theorem 3.10.2 are linear cyclic codes over $\mathbb{F}_4$. Since, in this chapter, we are more interested in twisted codes that are different from linear cyclic codes, from now on, we only consider the twisted codes that satisfy part (1) of Theorem 3.10.2. In particular, we are interested to see when two such values of γ_1 and γ_2 generate twisted codes with the same minimum distance. Recall that for each $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$, the map $\phi_\gamma : \mathbb{F}_{2^r} \to \mathbb{F}_2^2$ is the $\mathbb{F}_2$-linear transformation defined by $\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x))$.

Definition 3.10.4 For each $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ with $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$, we denote kernel of the map ϕ_γ restricted to the field $\mathbb{F}_{2^\kappa}$ by Φ_γ.

Let $\gamma \in \mathbb{F}_{2^s}$ such that $\mathbb{F}_2 \subsetneq \mathbb{F}_{2^s} \subseteq \mathbb{F}_{2^r}$. For each $x \in \mathbb{F}_{2^r}$, the following equality holds:

$$\phi_\gamma(x) = (\mathrm{Tr}_1^r(x), \mathrm{Tr}_1^r(\gamma x)) = \mathrm{Tr}_1^s(\mathrm{Tr}_s^r(x), \mathrm{Tr}_s^r(\gamma x)) = \mathrm{Tr}_1^s(\mathrm{Tr}_s^r(x), \gamma \mathrm{Tr}_s^r(x)) = \phi_\gamma(\mathrm{Tr}_s^r(x)). \tag{3.10.1}$$

This property will be used in the proof of the following theorem. Next, we give a sufficient condition for two twisted codes constructed using different values of γ to have the same parameters (length, dimension, and minimum distance). Recall that, as we mentioned in (3.4.7), the equality $\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp)$ holds for any twisted code, where $C(A_d)$ is the linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A_d.

Theorem 3.10.5 *Let $\gamma_1, \gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ such that $\kappa = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$ and $n \mid 2^r - 1$. If there exists a bijective map from Φ_{γ_1} to Φ_{γ_2} in the form $f(x) = \beta x$ for some $\beta \in \mathbb{F}_{2^\kappa}^*$, then the twisted codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ of length n have the same parameters for any complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$.*

Proof. As we showed in Corollary 3.10.3, the twisted codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same dimension over $\mathbb{F}_2$. Since $\mathscr{C}_{\gamma_1}(A) = \phi_{\gamma_1}(C(A_d)^\perp)$ and $\mathscr{C}_{\gamma_2}(A) = \phi_{\gamma_2}(C(A_d)^\perp)$, it only remains to show that $\phi_{\gamma_1}(C(A_d)^\perp)$ and $\phi_{\gamma_2}(C(A_d)^\perp)$ have the same minimum distances.

Let $\mathbb{F}_{2^\kappa} = \{0, 1, \alpha, \ldots, \alpha^{2^\kappa - 2}\}$, where α is a primitive element of the field $\mathbb{F}_{2^\kappa}$. Let $a = (a_1, a_2, \ldots, a_n) \in C(A_d)^\perp$. By (3.10.1), we have $\phi_{\gamma_1}(a) = \phi_{\gamma_1}(b)$, where $b = \mathrm{Tr}^r_\kappa(a) = (b_1, b_2, \ldots, b_n)$. The definition of Φ_{γ_1} implies that

$$\mathrm{wt}(\phi_{\gamma_1}(a)) = \mathrm{wt}(\phi_{\gamma_1}(b)) = \mathrm{wt}(b) - \#\text{ of non-zero coordinates of } b \text{ with elements in } \Phi_{\gamma_1}.$$

Since $\beta \in \mathbb{F}_{2^r}$, we have $\beta a \in C(A_d)^\perp$. Now $\phi_{\gamma_2}(\beta a) = \phi_{\gamma_2}(\beta b)$ and we have

$$\begin{aligned}\mathrm{wt}(\phi_{\gamma_2}(\beta a)) = \mathrm{wt}(\phi_{\gamma_2}(\beta b)) = \mathrm{wt}(\beta b) - \#\text{ of non-zero coordinates of } \beta b \text{ with}\\ \text{elements in } \Phi_{\gamma_2} = \mathrm{wt}(b) - \#\text{ of non-zero coordinates of } b \text{ with elements in } \Phi_{\gamma_1},\end{aligned}$$

where the last equality follows from the fact that $f(x)$ is a bijection. This relation implies that $d(\phi_{\gamma_2}(C(A_d)^\perp)) \leq d(\phi_{\gamma_1}(C(A_d)^\perp))$. Since $f^{-1}(x) = \beta^{-1}x$, the other inequality, namely $d(\phi_{\gamma_2}(C(A_d)^\perp)) \geq d(\phi_{\gamma_1}(C(A_d)^\perp))$, follows very similarly. Thus, the codes $\phi_{\gamma_1}(C(A_d)^\perp)$ and $\phi_{\gamma_2}(C(A_d)^\perp)$ have the same minimum distance. □

Let γ_1 and $\gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ such that $\kappa = [\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$. Next we use the above result and show that if $\kappa \leq 3$ then $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same parameters for any complete defining set A. Moreover, we show that for every $\kappa > 3$ if

$$s_\kappa = |\{\gamma \in \mathbb{F}_{2^r} : [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = \kappa\}|,$$

then there are at most $s_\kappa/6$ different twisted codes constructed using different values of γ and the same complete defining set. Before stating our results, we need the following observation. Let $f_1(x) = x + 1$ and $f_2(x) = \frac{1}{x}$ be two rational functions on $\mathbb{F}_{2^r} \setminus \mathbb{F}_2$. These functions generate the following group under the composition of functions

$$S_3 = \{f_0(x) = x, f_1(x) = x + 1, f_2(x) = \frac{1}{x}, f_3(x) = \frac{1}{x+1}, f_4(x) = \frac{x}{x+1}, f_5(x) = \frac{x+1}{x}\}. \tag{3.10.2}$$

The reason we represent this group by S_3 is that it is isomorphic to the symmetric group of degree 3. One can easily verify that the group S_3 acts naturally on the set $\mathbb{F}_{2^r} \setminus \mathbb{F}_2$. For each $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$, the orbit of γ under this action is defined by

$$\mathrm{Orb}(\gamma) = \{f(\gamma) : f \in S_3\}.$$

Note that an easy arithmetic computation shows that for each $\gamma_1, \gamma_2 \in \mathrm{Orb}(\gamma)$, we have $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$. Moreover, we have $|\mathrm{Orb}(\gamma)| < 6$ if and only if $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 2$. In the next theorem, we show that for any two such values of γ_1 and γ_2 and any complete defining set A, the codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same parameters.

Theorem 3.10.6 *Let $\gamma_1 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ and $\gamma_2 \in \mathrm{Orb}(\gamma_1)$. Then the twisted codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ of length n have the same parameters for any complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$.*

Proof. One can easily show that the following maps are bijections

1. $g_1(x) = x$ from Φ_{γ_1} to Φ_{γ_1+1}
2. $g_2(x) = \gamma_1 x$ from Φ_{γ_1} to $\Phi_{\frac{1}{\gamma_1}}$
3. $g_3(x) = (\gamma_1 + 1)x$ from Φ_{γ_1} to $\Phi_{\frac{1}{\gamma_1+1}}$
4. $g_4(x) = (\gamma_1 + 1)x$ from Φ_{γ_1} to $\Phi_{\frac{\gamma_1}{\gamma_1+1}}$
5. $g_5(x) = \gamma_1 x$ from Φ_{γ_1} to $\Phi_{\frac{\gamma_1+1}{\gamma_1}}$.

Hence the result follows from Theorem 3.10.5. We only show the bijection of Case (3) above as a sample. Suppose that $a \in \Phi_{\gamma_1}$. Then $\mathrm{Tr}_1^r(a) = \mathrm{Tr}_1^r(\gamma_1 a) = 0$. Next we show that $(\gamma_1+1)a \in \Phi_{\frac{1}{\gamma_1+1}}$. In other words, we need to show that $\mathrm{Tr}_1^r((\gamma_1+1)a) = \mathrm{Tr}_1^r((\gamma_1+1)\frac{a}{\gamma_1+1}) = 0$. This is trivial as

$$\mathrm{Tr}_1^r((\gamma_1 + 1)a) = \mathrm{Tr}_1^r(a) + \mathrm{Tr}_1^r(\gamma_1 a) = 0$$

and

$$\mathrm{Tr}_1^r((\gamma_1 + 1)\frac{a}{\gamma_1 + 1}) = \mathrm{Tr}_1^r(a) = 0.$$

Next let $b \in \Phi_{\frac{1}{\gamma_1+1}}$. This implies that $\mathrm{Tr}_1^r(b) = \mathrm{Tr}_1^r(\frac{b}{\gamma_1+1}) = 0$. Note that $g_3(\frac{b}{\gamma_1+1}) = b$. Hence it is sufficient to show that $\frac{b}{\gamma_1+1} \in \Phi_{\gamma_1}$. This holds since

$$\mathrm{Tr}_1^r(\frac{b}{\gamma_1 + 1}) = 0$$

and

$$\mathrm{Tr}_1^r(\frac{\gamma_1 b}{\gamma_1 + 1}) = \mathrm{Tr}_1^r(\frac{b}{\gamma_1 + 1} + b) = \mathrm{Tr}_1^r(\frac{b}{\gamma_1 + 1}) + \mathrm{Tr}_1^r(b) = 0.$$

□

In general, the result of Theorem 3.10.6 reduces the computation time of parameters of twisted codes by a factor of 6. As the computation of minimum distance can be time-consuming, this result improves the efficiency of such computations. In fact, even identifying a single code with the same parameters can save months of computation time. The next example shows that when $\kappa = 2, 3$, for each complete defining set $A \subseteq \mathbb{Z}/n\mathbb{Z}$, the parameters of twisted codes are independent of the choice of γ.

Example 3.10.7 (1) Let $\kappa = 2$ and $\mathbb{F}_4 = \{0, 1, \omega, \omega+1\}$, where ω is a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Then $\mathrm{Orb}(\omega) = \{\omega, \omega + 1\}$. Now Theorem 3.10.6 implies that $\mathscr{C}_\omega(A)$ and $\mathscr{C}_{\omega+1}(A)$ have the same parameters for any complete defining set A.

(2) Let $\kappa = 3$ and $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$, where α is a root of the irreducible polynomial $x^3 + x + 1$ over $\mathbb{F}_2$. Then

$$\mathrm{Orb}(\alpha) = \{\alpha, \alpha^2, \ldots, \alpha^6\}.$$

Now Theorem 3.10.6 implies that $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same parameters for any complete defining set A and each $\gamma_1, \gamma_2 \in \mathbb{F}_8 \setminus \mathbb{F}_2$.

Next, we show that when $\kappa = 4$, then there are exactly two different orbits and possibly two non-isomorphic twisted codes by selecting different values of γ. Later, in Corollary 3.10.16, we show that these two orbits always generate twisted codes with the same parameters.

Example 3.10.8 In this example, we provide more details and compute the sets Φ_γ for all the values $\gamma \in \mathbb{F}_{16} \setminus \mathbb{F}_4$. Let $\kappa = 4$ and $\mathbb{F}_{16} = \{0, 1, \alpha, \ldots, \alpha^{14}\}$, where α is a root of the irreducible polynomial $x^4 + x + 1$ over $\mathbb{F}_2$. Then

$$\mathbb{F}_{16} \setminus \mathbb{F}_4 = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}.$$

An easy computation shows that $\Phi_\alpha = \Phi_{\alpha^4} = \{0, 1, \alpha, \alpha^4\}$, $\Phi_{\alpha^2} = \Phi_{\alpha^8} = \{0, 1, \alpha^2, \alpha^8\}$, $\Phi_{\alpha^3} = \Phi_{\alpha^{14}} = \{0, \alpha, \alpha^2, \alpha^5\}$, $\Phi_{\alpha^6} = \Phi_{\alpha^{13}} = \{0, \alpha^2, \alpha^4, \alpha^{10}\}$, $\Phi_{\alpha^7} = \Phi_{\alpha^9} = \{0, \alpha, \alpha^8, \alpha^{10}\}$, and $\Phi_{\alpha^{11}} = \Phi_{\alpha^{12}} = \{0, \alpha^4, \alpha^5, \alpha^8\}$. The following results hold.

- The map $f_1(x)$ defined by $f_1(x) = x$ gives the trivial bijections of (3.10.3) and (3.10.4).
- The map $f_2 : \Phi_\alpha \to \Phi_{\alpha^3}$ defined by $f_2(x) = \alpha x$ is a bijection.
- The map $f_3 : \Phi_\alpha \to \Phi_{\alpha^{11}}$ defined by $f_3(x) = \alpha^4 x$ is a bijection.
- The map $f_4 : \Phi_{\alpha^2} \to \Phi_{\alpha^7}$ defined by $f_4(x) = \alpha^8 x$ is a bijection.
- The map $f_5 : \Phi_{\alpha^2} \to \Phi_{\alpha^6}$ defined by $f_5(x) = \alpha^2 x$ is a bijection.

In other words, the following diagrams of bijections exist.

$$\begin{tikzcd}
\Phi_{\alpha} = \Phi_{\alpha^4} \arrow[loop left, "f_1"] \arrow[r, "f_3"] \arrow[dr, "f_2"] & \Phi_{\alpha^{11}} = \Phi_{\alpha^{12}} \arrow[loop right, "f_1"] \\
 & \Phi_{\alpha^3} = \Phi_{\alpha^{14}} \arrow[loop right, "f_1"]
\end{tikzcd} \tag{3.10.3}$$

$$\begin{tikzcd}
\Phi_{\alpha^2} = \Phi_{\alpha^8} \arrow[loop left, "f_1"] \arrow[r, "f_5"] \arrow[dr, "f_4"] & \Phi_{\alpha^{6}} = \Phi_{\alpha^{13}} \arrow[loop right, "f_1"] \\
 & \Phi_{\alpha^7} = \Phi_{\alpha^{9}} \arrow[loop right, "f_1"]
\end{tikzcd} \tag{3.10.4}$$

Moreover, note that

$$\mathrm{Orb}(\alpha) = \{\alpha, \alpha^3, \alpha^4, \alpha^{11}, \alpha^{12}, \alpha^{14}\}$$

and

$$\mathrm{Orb}(\alpha^2) = \{\alpha^2, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{13}\}.$$

Hence the result of Theorem 3.10.6 implies that there are at most two non-isomorphic twisted codes for a fixed complete defining set and different selections of γ.

In the next section, we will use the permutation equivalence of twisted codes and provide more complementary results about twisted codes with the same parameters that are constructed using different values of γ.

So far, we have talked about when the values γ_1 and $\gamma_2 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ satisfying $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2]$ produce twisted codes with the same parameters. In the next example, we provide an example of two such gamma values such that the corresponding twisted codes have different minimum distances. In particular, one of the twisted codes produces a record-breaking binary quantum code, while the other has the same parameters as a currently best-known binary quantum code.

Example 3.10.9 Let $n = 69$ and $\kappa = 22$. The ordered 2-cyclotomic cosets modulo 69 are

$$Z(0) = \{0\}$$
$$Z(1) = \{1, 2, 4, 8, 16, 32, 64, 59, 49, 29, 58, 47, 25, 50, 31, 62, 55, 41, 13, 26, 52, 35\}$$
$$Z(68) = \{68, 67, 65, 61, 53, 37, 5, 10, 20, 40, 11, 22, 44, 19, 38, 7, 14, 28, 56, 43, 17, 34\}$$
$$Z(3) = \{3, 6, 12, 24, 48, 27, 54, 39, 9, 18, 36\}$$
$$Z(66) = \{66, 63, 57, 45, 21, 42, 15, 30, 60, 51, 33\}.$$

Let $A = \{1, -1\} \cup Z(-3)$. We first construct the field $\mathbb{F}_{2^{22}}$ by using the command `GF(2,22)` in Magma [17] and select the elements $\gamma_1 = \alpha$ and $\gamma_2 = \alpha^{89}$, where α is a primitive element of $\mathbb{F}_{2^{22}}$ defined by the `PrimitiveElement` function in Magma (hence also in GAP, Macaulay2 and SageMath by Remark 1.3.3). Note that $\mathbb{F}_2(\gamma_1) = \mathbb{F}_2(\gamma_2) = \mathbb{F}_{2^{22}}$. Because 89 divides $2^{22} - 1$, γ_2 is not a primitive element of $\mathbb{F}_{2^{22}}$. By Theorem 3.4.11, both $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ are dual-containing twisted codes with dimension 72 over $\mathbb{F}_2$. Thus by Theorem 3.5.7, both of these codes are $[\![69, 3]\!]$ binary quantum codes. Moreover, by computing their minimum distance using `MinimumDistance` function in Magma, we see that $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the minimum distances 15 and 16, respectively. Thus the code $\mathscr{C}_{\gamma_2}(A)$ is a new *record-breaking* binary quantum code with parameters $[\![69, 3, 16]\!]$ and the code $\mathscr{C}_{\gamma_1}(A)$ has the same parameters as a previously best-known quantum code.

By doing more computations, we find that the observation from the previous paragraph generalizes as follows. The minimum distance 16 is attainable by some elements γ with the algebraic degree 22 over $\mathbb{F}_2$ (both primitive and non-primitive). On the other hand, if the algebraic degree of γ is 11 over $\mathbb{F}_2$, then the minimum distance appears to be at most 11 with sporadically reaching 12. When $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$, then the minimum distance is 11.

3.10.1 Selection of γ value and equivalence of twisted codes

In general, determining when two twisted codes have the same parameters is an interesting task, and it was partially discussed in the previous section. In this section, we provide more complementary results by considering the permutation equivalence and equality of twisted codes. Note that, in general, the numeric search for twisted codes with good parameters is computationally very expensive in terms of both time and memory. This is because (1) the γ value in the construction of twisted codes can change, and (2) the defining set of a twisted code can contain unsaturated intersections of cyclotomic cosets. These possibilities hold only for the twisted codes and do not occur in the case of linear cyclic codes. Hence the results of this section, along with Section 3.10, will help to reduce the time complexity of the search algorithm for twisted codes with good parameters. At the end of this section, we also briefly describe a search algorithm for new binary quantum codes. Our algorithm targets only dual-containing and nearly dual-containing twisted codes.

Recall that in Section 1.6, we formally defined that two codes C_1 and C_2 are permutation equivalent if there exists a permutation matrix P such that $C_2 = C_1 P$. Throughout this section, n is a positive integer such that $n \mid 2^r - 1$ for some positive integer r and $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$.

Definition 3.10.10 Let $\mathscr{C}_\gamma(A_1)$ and $\mathscr{C}_\gamma(A_2)$ be two twisted codes of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. The codes $\mathscr{C}_\gamma(A_1)$ and $\mathscr{C}_\gamma(A_2)$ are called permutation equivalent if there exists a permutation of coordinates which maps $\mathscr{C}_\gamma(A_1)$ to $\mathscr{C}_\gamma(A_2)$.

Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$. We denote the group of all permutations of $\mathbb{Z}/n\mathbb{Z}$ by S_n. Recall that, as we mentioned in (3.4.9), the equality $\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp)$ holds for any twisted code, where $C(A_d)$ is the linear cyclic code over $\mathbb{F}_{2^r}$ with the defining set A_d. The following result is an easy consequence of Proposition 9.4.16 of [14]. Since in [14] the general family of additive cyclic codes is studied using a slightly different notation, here we provide a short proof for this result using the theory of additive twisted codes developed in this thesis.

Theorem 3.10.11 *[14] Let $A, A' \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining sets of two twisted codes of length n. If there exists $\sigma \in S_n$ such that $\sigma(C(A_d)^\perp) = C(A'_d)^\perp$, then the twisted codes $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A')$ are permutation equivalent.*

Proof. We show that $\sigma(\mathscr{C}_\gamma(A)) = \mathscr{C}_\gamma(A')$. The fact that $\phi_\gamma(\sigma(C(A_d)^\perp)) = \sigma(\phi_\gamma(C(A_d)^\perp))$ implies

$$\sigma(\mathscr{C}_\gamma(A)) = \sigma(\phi_\gamma(C(A_d)^\perp)) = \phi_\gamma(\sigma(C(A_d)^\perp)) = \phi_\gamma(C(A'_d)^\perp) = \mathscr{C}_\gamma(A').$$

□

The above theorem allows us to apply the results on permutation equivalence of linear cyclic codes and determine permutation equivalent twisted codes. Recall that the map $\mu_e : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\mu_e(x) = ex \bmod n$ is called a multiplier, where e is a positive integer such that $\gcd(n, e) = 1$. The next theorem allows us to check the equivalence of twisted codes using the multipliers.

Corollary 3.10.12 *Let $A, A' \subseteq \mathbb{Z}/n\mathbb{Z}$ be the complete defining sets of two length n twisted codes, and e be a positive integer such that $\gcd(e, n) = 1$. If $\mu_e(A) = A'$, then the twisted codes $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A')$ are permutation equivalent.*

Proof. First, note that by Theorem 1.6.4, the codes $C(A)$ and $C(A')$ are permutation equivalent. Hence the codes $C(A)^\perp$ and $C(A')^\perp$ are permutation equivalent. Now Theorem 3.10.11 implies that $\mathscr{C}_\gamma(A_d) = \mathscr{C}_\gamma(A)^{\perp_s}$ and $\mathscr{C}_\gamma(A'_d) = \mathscr{C}_\gamma(A')^{\perp_s}$ are permutation equivalent. Hence their symplectic duals, namely $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A')$, are permutation equivalent. □

Recall that, so far, we have discussed two scenarios under which two twisted codes have the same parameters. First, in Theorem 3.10.5, we showed that twisted codes with the same complete defining sets but different values of γ have the same parameters under certain conditions. Second, in Theorem 3.10.11, we provided sufficient conditions for two twisted codes with different complete defining sets but the same value of γ to have the same parameters. Next, we combine these results and provide sufficient conditions for two twisted codes with different complete defining sets and different γ values to have the same parameters. Let A be the complete defining set of a length n twisted code. For each $0 \le i \le \operatorname{ord}_n(2) - 1$, we define

$$2^i A = \{(2^i a) \bmod n : a \in A\}.$$

Example 3.10.13 Let $n = 21$. The ordered 2-cyclotomic cosets modulo 21 are $Z(0) = \{0\}$, $Z(1) = \{1, 2, 4, 8, 16, 11\}$, $Z(3) = \{3, 6, 12\}$, $Z(5) = \{5, 10, 20, 19, 17, 13\}$, $Z(7) = \{7, 14\}$, and $Z(9) = \{9, 18, 15\}$.

(1) Let $A = \{1, 8\}$ and $\kappa = 3$. Note that $A \cap Z(1)$ is unsaturated and $2A = \{2, 16\}$. In other words, there are three possible unsaturated intersections with $Z(1)$, namely $\{1, 8\}$, $\{2, 16\}$, and $\{4, 11\}$. Moreover, $2^i A$ for $0 \leq i \leq 2$ give all the possible unsaturated intersections with $Z(1)$.

(2) Let $A = \{3, 6, 12\}$. In this case, $A \cap Z(3)$ is saturated. It is easy to see that $2^i A = A$ for each $i \geq 0$.

The above example shows that for any complete defining set A, the set $2^i A$ remains a complete defining set of a twisted code for each $i \geq 0$. The next result shows that certain twisted codes with complete defining sets and different γ values are the same. Recall that $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$.

Theorem 3.10.14 *Let A be the complete defining set of a twisted code of length n over $\mathbb{F}_2 \times \mathbb{F}_2$. Then the twisted codes $\mathscr{C}_{\gamma^{2^i}}(2^i A)$ are the same for all $0 \leq i \leq \kappa - 1$.*

Proof. Recall from (3.4.7) that $\mathscr{C}_\gamma(A) = \phi_\gamma(C(A_d)^\perp)$. Let $\alpha \in \mathbb{F}_{2^r}$ be a primitive n-th root of unity and $a \in C(A_d)^\perp$. Recall that the vector $v^s \in \mathbb{F}_{2^r}^n$ is defined by $v^s = (1 \ \alpha^s \alpha^{2s} \ \cdots \ \alpha^{(n-1)s})$ for each $0 \leq s \leq n-1$. The matrix $B(A_d)$ defined in (3.3.2) is a generator matrix for the code $C(A_d)^\perp$. Then $a = \sum_{t \in A_d} b_t v^t$ for some $b_t \in \mathbb{F}_{2^r}$. Next we show that for each $0 \leq i \leq \kappa - 1$, the codes $\phi_\gamma(C(A_d)^\perp)$ and $\phi_{\gamma^{2^i}}(C(2^i A_d)^\perp)$ are the same. First, note that

$$\mathrm{Tr}_1^r((a, \gamma a)) = \mathrm{Tr}_1^r((a^{2^i}, \gamma^{2^i} a^{2^i})) \in \phi_{\gamma^{2^i}}(C(2^i A_d)^\perp), \tag{3.10.5}$$

where $a^{2^i} = \sum_{t \in A_d} b_t^{2^i} v^{2^i t} = \sum_{t \in 2^i A_d} b_t^{2^i} v^t \in C(2^i A_d)^\perp$. Therefore, the equation (3.10.5) implies that $\phi_\gamma(C(A_d)^\perp) \subseteq \phi_{\gamma^{2^i}}(C(2^i A_d)^\perp)$. Now we prove the other inclusion. Let $c = \sum_{t \in 2^i A_d} d_t v^t$ for some $d_t \in \mathbb{F}_{2^r}$. Then

$$\mathrm{Tr}_1^r((c, \gamma^{2^i} c)) = \mathrm{Tr}_1^r((c^{2^{\kappa-i}}, \gamma c^{2^{\kappa-i}})) \in \phi_\gamma(C(A_d)^\perp), \tag{3.10.6}$$

where $c^{2^{\kappa-i}} = \sum_{t \in 2^i A_d} d_t^{2^{\kappa-i}} v^{2^{\kappa-i} t} = \sum_{t \in A_d} d_t^{2^{\kappa-i}} v^t \in C(A_d)^\perp$. Thus the equation (3.10.6) implies that $\phi_{\gamma^{2^i}}(C(2^i A_d)^\perp) \subseteq \phi_\gamma(C(A_d)^\perp)$, and consequently $\mathscr{C}_\gamma(A) = \mathscr{C}_{\gamma^{2^i}}(2^i A)$. Since $0 \leq i \leq \kappa - 1$ was arbitrary, we conclude that the twisted codes $\mathscr{C}_{\gamma^{2^i}}(2^i A)$ are the same for all $0 \leq i \leq \kappa - 1$. □

The next result is a direct consequence of the above theorem.

Corollary 3.10.15 *Let A be the complete defining set of a twisted code of length n. Then the twisted codes $\mathscr{C}_{\gamma^{2^i}}(2^j A)$ all are permutation equivalent for each $0 \leq i, j \leq \kappa - 1$.*

Proof. We show that for each $0 \leq i, j \leq \kappa - 1$, the two twisted codes $\phi_\gamma(C(A_d)^\perp)$ and $\phi_{\gamma^{2^i}}(C(2^j A_d)^\perp)$ are permutation equivalent. By Theorem 3.10.14, the codes $\phi_\gamma(C(A_d)^\perp)$

and $\phi_{\gamma^{2^i}}(C(2^i A_d)^\perp)$ are the same. Moreover, since $\gcd(2,n)=1$, Corollary 3.10.12 implies that $\phi_\gamma(C(A_d)^\perp)$ and $\phi_{\gamma^{2^i}}(C(2^j A_d)^\perp)$ are permutation equivalent. Therefore, the codes $\phi_\gamma(C_{B(A)})$ and $\phi_{\gamma^{2^i}}(C_{B(2^j A)})$ are permutation equivalent. □

Next, we use the result of Theorem 3.10.6 and give a generalization of the above result. Recall that for each $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$, we have $\mathrm{Orb}(\gamma) = \{f(\gamma) : f \in S_3\}$, where S_3 is the group of rational functions defined in (3.10.2).

Corollary 3.10.16 *Let A be the complete defining set of a twisted code of length n, $\gamma_1 \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$, and $\gamma_2 \in \mathrm{Orb}(\gamma_1)$. Then the twisted codes $\mathscr{C}_{\gamma_1^{2^i}}(2^j A)$ and $\mathscr{C}_{\gamma_2^{2^{i'}}}(2^{j'} A)$ have the same parameters for each $0 \le i, j, i', j' \le \kappa - 1$.*

Proof. By Corollary 3.10.15, the twisted codes $\mathscr{C}_{\gamma_1^{2^i}}(2^j A)$ are permutation equivalent for all $0 \le i, j \le \kappa - 1$. The same holds for the twisted codes $\mathscr{C}_{\gamma_2^{2^{i'}}}(2^{j'} A)$ for all $0 \le i', j' \le \kappa - 1$. Moreover, Theorem 3.10.6 implies that the codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same parameters. This completes the proof. □

Next, we provide an application for the above corollary. Recall that in Theorem 3.10.6 we showed that the twisted codes $\mathscr{C}_{\gamma_1}(A)$ and $\mathscr{C}_{\gamma_2}(A)$ have the same parameters when $[\mathbb{F}_2(\gamma_1) : \mathbb{F}_2] = [\mathbb{F}_2(\gamma_2) : \mathbb{F}_2] \le 3$. Moreover, in Example 3.10.8, we showed that different selections of γ values in $\mathbb{F}_{16} \setminus \mathbb{F}_4$ may result in at most two twisted codes with different parameters. Next, we improve this result and show that different selections of γ values do not change the parameters of twisted codes when $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 4$.

Example 3.10.17 Let $\kappa = 4$ and $\mathbb{F}_{16} = \{0, 1, \beta, \ldots, \beta^{14}\}$, where β is a root of the irreducible polynomial $x^4 + x + 1$ over $\mathbb{F}_2$. As we showed in Example 3.10.8, for each $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$, the code $\mathscr{C}_\gamma(A)$ has the same parameters as either $\mathscr{C}_\beta(A)$ or $\mathscr{C}_{\beta^2}(A)$. Moreover, the codes $\mathscr{C}_\beta(A)$ and $\mathscr{C}_{\beta^2}(A)$ have the same parameters by Corollary 3.10.16. Therefore, for all $\gamma \in \mathbb{F}_4 \setminus \mathbb{F}_2$, the codes $\mathscr{C}_\gamma(A)$ all have the same parameters.

The criteria developed in this section help to identify many twisted codes with the same parameters. In the next example, we identify many twisted codes with the same parameters constructed using different complete defining sets.

Example 3.10.18 Let $n = 15$ and $\kappa = 4$. The ordered 2-cyclotomic cosets modulo 15 are $Z(0) = \{0\}$, $Z(1) = \{1, 2, 4, 8\}$, $Z(3) = \{3, 6, 12, 9\}$, $Z(5) = \{5, 10\}$, and $Z(7) = \{7, 14, 13, 11\}$. Let $A = \{0, 1, 3\}$. There are 12 different elements $\gamma \in \mathbb{F}_{16} \setminus \mathbb{F}_4$, and by the above example, the parameters of the twisted codes $\mathscr{C}_\gamma(A)$ are independent of the choice of γ. Moreover, Corollary 3.10.12 gives many more twisted codes which are permutation equivalent. For instance, the twisted codes $\mathscr{C}_\gamma(A)$ and $\mathscr{C}_\gamma(A')$ are permutation equivalent for each

$$A' \in \{\{0, 2, 6\}, \{0, 4, 12\}, \{0, 8, 9\}, \{0, 7, 6\}, \{0, 11, 3\}, \{0, 13, 9\}, \{0, 14, 12\}\}.$$

Next, we take advantage of the result of Corollary 3.10.16 and list all the values of γ in different field extensions of $\mathbb{F}_2$ that may produce twisted codes with different parameters. This restricts the search for good twisted codes to only a small number of γ values. Table 3.3 presents all such gamma values. In the table, α is the primitive element of the corresponding finite field constructed using the `PrimitiveElement` function in Magma [17]. The third column of the table gives the total number of $\gamma \in \mathbb{F}_{2^r}$ such that $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = \kappa$. Finally, the last column of Table 3.3 presents all the possible candidates for γ that may produce twisted codes with different parameters. Clearly, as it is evident from the values in the third and fourth columns of the table, the result of Corollary 3.10.16 significantly reduces the computational time to search for good twisted codes. This is particularly valuable considering that the minimum distance computation is a time-consuming process, and even saving a single computation can be highly beneficial. For instance, in the case where $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 9$, the result from Table 3.3 shows a significant time reduction by a factor of 50.4.

Field Extension	κ	# of all γ values	γ candidates
$\mathbb{F}_{2^2}$	2	2	α
$\mathbb{F}_{2^3}$	3	6	α
$\mathbb{F}_{2^4}$	4	12	α
$\mathbb{F}_{2^5}$	5	30	α
$\mathbb{F}_{2^6}$	6	54	α, α^3
$\mathbb{F}_{2^7}$	7	126	$\alpha, \alpha^5, \alpha^9$
$\mathbb{F}_{2^8}$	8	240	$\alpha, \alpha^5, \alpha^7, \alpha^9, \alpha^{13}, \alpha^{23}$
$\mathbb{F}_{2^9}$	9	504	$\alpha, \alpha^3, \alpha^7, \alpha^{13}, \alpha^{17}, \alpha^{19}, \alpha^{21}, \alpha^{23}, \alpha^{27}, \alpha^{35}$

Table 3.3: The values of γ that may produce twisted codes with different parameters.

We finish this section by briefly describing a search algorithm for new quantum codes that targets dual-containing and nearly dual-containing twisted codes with a small dual-containment deficiency value. Recall that for a complete defining set A, the dual-containment deficiency of the code $\mathscr{C}_\gamma(A)$ is defined by

$$e_A = \frac{\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d)) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d) \cap \mathscr{C}_\gamma(A))}{2} = \frac{\dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A_d)) - \dim_{\mathbb{F}_2}(\mathscr{C}_\gamma(A \cup A_d))}{2}.$$

In particular, we have $\mathscr{C}_\gamma(A_d) \subseteq \mathscr{C}_\gamma(A)$ if and only if $e_A = 0$.

Search algorithm. Step 1. Let n be a positive odd integer. Then we can find a positive integer r such that $n \mid 2^r - 1$ and r is the smallest with this property. Hence the 2-cyclotomic coset of 1 modulo n has size r. This allows us to find all the possible values of κ simply by finding all the factors of r.

Step 2. We fix one value of κ and partition each cyclotomic coset into unsaturated subsets. In other words, for each 2-cyclotomic coset $Z = \{a2^i : 0 \leq i \leq \kappa m - 1\}$ with the coset leader a modulo n, there are κ unsaturated subsets in the forms

$$Z^{(j)} = \{a2^{\kappa i+j} : 0 \leq i \leq m-1\}, \tag{3.10.7}$$

where $0 \leq j \leq \kappa - 1$. Therefore, the complete defining set of a twisted code intersects Z in only one of the following forms:

- The intersection is empty.
- The intersection is Z.
- The intersection is $Z^{(j)}$ for some $0 \leq j \leq \kappa - 1$.

If $\kappa \nmid |Z|$, then the third case above cannot happen.

Step 3. We select a $\gamma \in \mathbb{F}_{2^r} \setminus \mathbb{F}_2$ such that $\kappa = [\mathbb{F}_2(\gamma) : \mathbb{F}_2]$. In particular, we only choose the values from Table 3.3 when $\kappa < 10$, and use the result of Corollary 3.10.16 for $\kappa \geq 10$. This allows us to consider only a small number of γ values in our computations, and reduces the computation time.

Step 4. The defining set of a twisted code is defined to be a unique union of the intersections defined in Step 2. Let A_1 and A_2 be the complete defining sets of two additive twisted codes. An easy observation on the dual-containment deficiency formula of Theorem 3.5.5 shows that if $(A_1)_d \subseteq (A_2)_d$, then $e_{A_1} \leq e_{A_2}$. Therefore, we can design a *backtracking algorithm* to enumerate all twisted codes of length n with a given upper bound on the e_A value.

Step 5. For each complete defining set A satisfying Step 3, we apply the quantum construction of Theorem 3.5.7 to $\mathscr{C}_\gamma(A)$ and compute the parameters of the corresponding quantum code.

Note that, as previously explained before Table 3.3, the results presented in this section help to eliminate the need for redundant consideration of different twisted codes with the same parameters in the search algorithm. This pruning of the search algorithm leads to a significant improvement in its efficiency for finding codes with good parameters.

Chapter 4

Equivalence of codes and applications

Despite the long history and extensive study of linear cyclic codes, several questions regarding their equivalence remain unsolved and presumably are very difficult [54]. There have been several works toward the classification of equivalent cyclic and constacyclic codes using algebraic properties of these codes; for examples see [5–7, 11, 34, 46, 54].

We skip the adjective "linear" throughout this chapter and abbreviate the names of linear cyclic and linear constacyclic codes to "cyclic" and "constacyclic" codes, respectively. In this chapter, we develop new tools for permutation and monomial equivalence of linear cyclic and constacyclic codes. Our new results help to determine permutation or monomially equivalent cyclic codes, which are not necessarily detectable using the previous methods, such as the action of affine maps on defining sets or the generalized multipliers. We also resolve two questions raised in the literature regarding the isometric equivalence of cyclic codes induced by the action of affine maps on their defining sets. Recall that ϕ is Euler's totient function. Moreover, we prove that two constacyclic codes over $\mathbb{F}_4$ of an odd length n such that $\gcd(3n, \phi(3n)) = 1$ are permutation equivalent if and only if there exists a multiplier that maps the defining set of one code to the defining set of the other.

In general, finding linear codes with good parameters is one of the most challenging tasks in algebraic coding theory. A lot of work has been done in the literature to make the computer search for linear codes with good parameters more systematic. However, the computationally challenging obstacles, such as minimum distance computation, which requires a considerable amount of time, have slowed down the search process considerably. Recently, several new linear codes were discovered by designing a more efficient search algorithm for new linear codes using equivalence of cyclic and constacyclic codes, see for example [2, 5, 6].

The results of this chapter can be applied to make the search for new linear codes and also binary quantum codes with good parameters more systematic. In particular, we discuss the nearly dual-containment of cyclic and constacyclic codes with respect to the Hermitian inner product. This helps to find suitable ingredients for the quantum construction of Theorem 1.7.9. Moreover, we outline a search algorithm for new quantum codes from nearly dual-containing cyclic and constacyclic codes. Finally, we present examples of record-breaking binary quantum codes and linear codes. These codes were obtained after pruning the search algorithm for new linear and quantum codes using the results of this chapter and Section 1.6.

This chapter is organized as follows. Our main contributions are discussed in Section 4.1. In Section 4.2, we introduce novel sufficient conditions for permutation and monomial equivalence of cyclic codes over various finite fields. Next, in Section 4.3, we resolve two conjectures of Aydin, Lambrinos, and VandenBerg proposed in [6]. In Section 4.4, we present new results on the equivalence of constacyclic codes over $\mathbb{F}_4$. Finally, Section 4.5 outlines a search algorithm for good quantum codes from nearly dual-containing cyclic and constacyclic codes. We also present record-breaking binary quantum codes and linear codes over $\mathbb{F}_4$. Applying secondary constructions to our new codes produces many more record-breaking codes.

The material in this chapter is a joint work with my senior supervisor Dr. Lisoněk, and it has been published in Discrete Mathematics journal [26]. A portion of materials in this section was presented at the 25th International Conference on Applications of Computer Algebra (ACA 2019, Montreal, Canada) [27] and the 2022 Joint Mathematics Meetings (JMM 2022, Seattle, USA) [31].

4.1 Our main contributions

Significant literature exists on the equivalence of linear codes, particularly cyclic codes and their generalizations. Therefore, in order to separate the previous results from our new results in this chapter, we take the liberty to briefly summarize our new results in this section.

In Section 4.2, we introduce novel sufficient conditions for the permutation and monomial equivalence of cyclic codes (Theorems 4.2.5, 4.2.11, and 4.2.16). We also provide a list of code lengths and finite fields containing at least a pair of cyclic codes which are monomially equivalent but not affine equivalent. Many such pairs can be explained using our new results.

Throughout this chapter, the "defining set" of a cyclic or constacyclic code is a unique union of cyclotomic cosets. In Section 4.3, Theorem 4.3.1 resolves two conjectures and strengthens a result of [6]. Let C_1 and C_2 be two cyclic codes of length n over $\mathbb{F}_q$ with the defining sets A and B, and $\psi_b(x) = (x + b) \bmod n$ be the shift map on $\mathbb{Z}/n\mathbb{Z}$. We prove that C_1 and C_2 are monomially equivalent through the shift map ψ_b if and only if $\psi_b(A) = B$ and n divides $|A|b(q-1)$. Next, we prove that the generator polynomials of two monomially equivalent cyclic codes of length n over $\mathbb{F}_q$ generate monomially equivalent cyclic codes of lengths nm, where $\gcd(m, q) = 1$.

Recall that Theorem 1.6.5 states that for a positive integer n such that $\gcd(n, \phi(n)) = 1$, two cyclic codes of length n with the defining sets A_1 and A_2 are permutation equivalent if and only if there exists a multiplier μ_a such that $\mu_a(A_1) = A_2$. In Section 4.4, we give a result analogous to the result of Theorem 1.6.5 for constacyclic codes. In particular, we prove that two constacyclic codes of length n over $\mathbb{F}_4$ such that $\gcd(3n, \phi(3n)) = 1$ are permutation equivalent if and only if they are permutation equivalent by the action of multipliers on their defining sets.

In Section 4.5.1, we first compute the dual-containment deficiency of constacyclic code over $\mathbb{F}_4$ (Theorem 4.5.4 and Corollary 4.5.5). Next, we classify constacyclic codes with the dual-containment deficiency $e = 1$ and $e = 2$ (Theorem 4.5.7). Finally, we present a search algorithm for binary quantum codes with good parameters from nearly dual-containing constacyclic codes over $\mathbb{F}_4$, and give new record-breaking binary quantum codes and linear codes over $\mathbb{F}_4$.

4.2 Novel sufficient conditions for equivalence of cyclic codes

This section studies sufficient conditions for monomial and permutation equivalence of cyclic codes over various finite fields. Our conditions are easy to check, and they help to classify all monomially equivalent cyclic codes of certain lengths. Moreover, our new conditions enable us to prove monomial or permutation equivalence of pairs of codes in some cases that can not be resolved by previously known results.

In this chapter, vectors are indexed starting at zero. Throughout this chapter, we fix α to be a primitive n-th root of unity in the field $K = \mathbb{F}_q(\alpha)$. For $v = (1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$, we define the vector $v^s \in K^n$ to be $v^s = (1, \alpha^s, \alpha^{2s}, \ldots, \alpha^{(n-1)s})$ for each $0 \leq s \leq n-1$. Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ and H be an $(n-k) \times n$ matrix defined over a field extension of $\mathbb{F}_q$. Recall that the matrix H is called a generalized parity check matrix for the code C if for each $c \in \mathbb{F}_q^n$ we have $Hc^T = 0$ if and only if $c \in C$.

The monomial and permutation equivalence of linear codes can also be defined in terms of the generalized parity check matrices. The following lemma is elementary but we record it for further use in this chapter.

Lemma 4.2.1 *Let C_1 and C_2 be two linear codes of length n over $\mathbb{F}_q$, and H be a generalized parity check matrix for C_1. Let P be a permutation matrix and D be a non-singular diagonal matrix defined over $\mathbb{F}_q$. Then $C_2 = C_1PD$ if and only if HPD^{-1} is a generalized parity check matrix for C_2.*

Remark 4.2.2 In Sections 4.2.1, 4.2.2, and 4.2.3, we provide some intermediate lemmas before stating our main result. There might be easier proofs for the equivalence of codes in these lemmas by applying the results of Section 1.6.1. However, our main goal is to prove these lemmas using the action of specific permutation or monomial matrices. After proving our main results, namely Theorems 4.2.5, 4.2.11, and 4.2.16, we provide evidence showing that they are not of the types of results discussed in Section 1.6.1.

Before stating our new results, we first recall affine equivalence and permutation equivalence under the action of generalized multipliers for cyclic codes introduced in Corollary 1.6.10 and Definition 1.6.7, respectively. Let A_1 and A_2 be defining sets of two linear cyclic codes of length n over $\mathbb{F}_q$, and $\theta(x) = (ex + b) \bmod n$, where $\gcd(e, n) = 1$. Later we show that the condition $n \mid b|A_1|(q-1)$ is required for the existence of such affine maps. Recall that if $\theta(A_1) = A_2$, then cyclic codes with the defining sets A_1 and A_2 are called affine equivalent. In the following three sections we give monomially equivalent cyclic codes which are not, in general, affine equivalent.

Let $n = p^m$ and $k \leq m$ be positive integers, where p is an odd prime and $m \geq 2$. Recall that for $1 \leq d < p^k$ such that $\gcd(d, p^k) = 1$, the map $M_d : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $M_d(i + jp^k) = (id \bmod p^k) + jp^k$ is called a generalized multiplier of $\mathbb{Z}/n\mathbb{Z}$. Two codes that are monomially equivalent, as implied by our new results in the next three sections, are not necessarily permutation equivalent under the action of generalized multipliers.

4.2.1 New sufficient condition for monomial equivalence of cyclic codes

Let n be a positive integer divisible by 8 and $\mathbb{F}_q$ be a finite field of odd characteristic. We define the permutation σ on $\mathbb{Z}/n\mathbb{Z}$ by

$$\sigma(i) = \begin{cases} i & \text{if } i \equiv 0 \text{ or } 1 \pmod 4 \\ (i + \frac{n}{2}) \bmod n & \text{otherwise.} \end{cases}$$

Let P_σ be the permutation matrix corresponding to the action of σ and D be the diagonal matrix defined by

$$D_{ii} = \begin{cases} -1 & \text{if } i \equiv 1 \text{ or } 2 \pmod 4 \\ 1 & \text{otherwise} \end{cases}$$

for each $0 \leq i \leq n-1$. Let $\{s_i : 0 \leq i \leq n-1\}$ be the standard basis of $\mathbb{F}_q^n$. Then

$$s_i(P_\sigma D) = \begin{cases} s_i & \text{if } i \equiv 0 \pmod 4 \\ -s_i & \text{if } i \equiv 1 \pmod 4 \\ -s_{i+\frac{n}{2}} & \text{if } i \equiv 2 \pmod 4 \\ s_{i+\frac{n}{2}} & \text{if } i \equiv 3 \pmod 4. \end{cases}$$

Since the generalized multipliers are not defined over $\mathbb{Z}/n\mathbb{Z}$ for an even integer n, the action of $P_\sigma D$ cannot be of a generalized multiplier type. Later we also show that if two cyclic codes are monomially equivalent under the action of $P_\sigma D$, then they are not necessarily affine equivalent. Before stating our main result, we have two intermediate lemmas. Recall that $Z(a)$ denotes the q-cyclotomic coset modulo n containing a.

Lemma 4.2.3 *Suppose that q is odd. Let $n = 8k$ for some positive integer k and $0 < a \leq n-1$ be an odd integer. Then cyclic codes over $\mathbb{F}_q$ of length n with the defining sets $Z(a)$ and $Z(\frac{n}{2}+a)$ are monomially equivalent under the action of $P_\sigma D$.*

Proof. Let C_1 and C_2 be the cyclic codes of length n over $\mathbb{F}_q$ with the defining sets $Z(a)$ and $Z(\frac{n}{2}+a)$, respectively. First, note that since q is odd, we have $q(\frac{n}{2}+a) \equiv \frac{n}{2}+qa \pmod{n}$. Thus there is a one-to-one correspondence between the elements of $Z(a)$ and $Z(\frac{n}{2}+a)$ given by the shift map $\psi_{\frac{n}{2}}$. Moreover, both $Z(a)$ and $Z(\frac{n}{2}+a)$ consist of only odd values.

Let H_1 be a generalized parity check matrix for C_1 in the form of (1.4.2) and b be an arbitrary element of $Z(a)$. The vector v^b is a row of H_1 and we show that $v^b P_\sigma D = v^{b'}$, where $b' = (\frac{n}{2}+b) \bmod n$ is an element of $Z(\frac{n}{2}+a)$. Since both H_1 and $H_1 P_\sigma D$ are generalized parity check matrices of linear codes over $\mathbb{F}_q$ with the same dimension, showing that $v^b P_\sigma D = v^{b'}$ implies that $H_1 P_\sigma D$ is a generalized parity check matrix for C_2. In our computations, we use the fact that $\alpha^{\frac{n}{2}} = -1$.

Let $0 \leq i \leq n-1$. If $i \equiv 1 \pmod{4}$, then $(v^b P_\sigma D)_i = \alpha^{ib+\frac{n}{2}} = \alpha^{i(\frac{n}{2}+b)} = \alpha^{ib'}$. If $i \equiv 3 \pmod{4}$, then $(v^b P_\sigma D)_i = \alpha^{(i+\frac{n}{2})b} = \alpha^{i(\frac{n}{2}+b)} = \alpha^{ib'}$. If $i \equiv 0 \pmod{4}$, then $(v^b P_\sigma D)_i = \alpha^{ib} = \alpha^{i(\frac{n}{2}+b)} = \alpha^{ib'}$. If $i \equiv 2 \pmod{4}$, then $(v^b P_\sigma D)_i = \alpha^{(i+\frac{n}{2})b+\frac{n}{2}} = \alpha^{ib} = \alpha^{i(\frac{n}{2}+b)} = \alpha^{ib'}$. Hence, for each i, we get $(v^b P_\sigma D)_i = (v^{b'})_i$.

Thus $H_1 P_\sigma D$ is a generalized parity check matrix for C_2. Therefore, by Lemma 4.2.1, the codes C_1 and C_2 are monomially equivalent under the action of $P_\sigma D$. □

The above result can be easily extended to monomially equivalent cyclic codes with union of more than one cyclotomic coset as their defining set. Since $8 \mid n$, the q-cyclotomic cosets of 0 and $\frac{n}{2}$ are both singletons. Let $q \equiv 1 \pmod{4}$. Then the sets $\{\frac{n}{4}\}$ and $\{\frac{3n}{4}\}$ are two other singleton q-cyclotomic cosets. If $q \equiv 3 \pmod{4}$, then the set $\{\frac{n}{4}, \frac{3n}{4}\}$ is a q-cyclotomic coset.

Lemma 4.2.4 *Let $n = 8k$ for some positive integer k and $A_1 = \{0, \frac{n}{2}\}$ and $A_2 = \{\frac{n}{4}, \frac{3n}{4}\}$ be the defining sets of C_1 and C_2, which are cyclic codes of length n over $\mathbb{F}_q$, respectively. Then C_1 and C_2 are monomially equivalent under the action of $P_\sigma D$.*

Proof. Since $\alpha^{\frac{n}{2}} = -1$, the code C_1 has a parity check matrix in the form

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & -1 & 1 & -1 & \cdots & -1 \end{bmatrix}.$$

Let

$$H_2 = \begin{bmatrix} 1 & \alpha^{\frac{n}{4}} & \alpha^{\frac{2n}{4}} & \alpha^{\frac{3n}{4}} & 1 & \cdots & \alpha^{\frac{3n}{4}} \\ 1 & \alpha^{\frac{3n}{4}} & \alpha^{\frac{2n}{4}} & \alpha^{\frac{n}{4}} & 1 & \cdots & \alpha^{\frac{n}{4}} \end{bmatrix}$$

be a generalized parity check matrix of C_2. Next we show that $H_2P_\sigma D$ and H_1 generate the same row space over K. First, a straightforward computation shows that

$$H_2P_\sigma D = \begin{bmatrix} 1 & \alpha^{\frac{3n}{4}} & 1 & \alpha^{\frac{3n}{4}} & 1 & \cdots & \alpha^{\frac{3n}{4}} \\ 1 & \alpha^{\frac{n}{4}} & 1 & \alpha^{\frac{n}{4}} & 1 & \cdots & \alpha^{\frac{n}{4}} \end{bmatrix} = \begin{bmatrix} 1 & -\alpha^{\frac{n}{4}} & 1 & -\alpha^{\frac{n}{4}} & 1 & \cdots & -\alpha^{\frac{n}{4}} \\ 1 & \alpha^{\frac{n}{4}} & 1 & \alpha^{\frac{n}{4}} & 1 & \cdots & \alpha^{\frac{n}{4}} \end{bmatrix}.$$

Next by adding and subtracting the rows of $H_2P_\sigma D$ we find a basis for the row space of $H_2P_\sigma D$ in the form $B = \{(1,0,1,0,\ldots,0),(0,1,0,1,\ldots,1)\}$. One can easily see that the set B is also a basis for the row space of H_1. Thus $H_2P_\sigma D$ is also a generalized parity check matrix for C_1. Now Lemma 4.2.1 implies that the codes C_1 and C_2 are monomially equivalent under the action of $P_\sigma D$. □

Next, we combine the results of Lemmas 4.2.3 and 4.2.4 and state the main result of Section 4.2.1.

Theorem 4.2.5 *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $n = 8k$ for some positive integer k such that $\gcd(k,q) = 1$. Let A be a union of q-cyclotomic cosets modulo n with odd coset leaders. Then the cyclic codes of length n with the defining sets $A_1 = A \cup \{\frac{n}{4}, \frac{3n}{4}\}$ and $A_2 = \{(a + \frac{n}{2}) \bmod n : a \in A\} \cup \{0, \frac{n}{2}\}$ over $\mathbb{F}_q$ are monomially equivalent under the action of $P_\sigma D$.*

Proof. Let C_1 and C_2 be the cyclic codes of length n with the defining set A_1 and A_2 over $\mathbb{F}_q$, respectively. Let H_1 be a generalized parity check matrix for C_1, in the form of (1.4.2). Then Lemmas 4.2.3 and 4.2.4 imply that $H_1P_\sigma D$ is a generalized parity check matrix for C_2. Thus by Lemma 4.2.1 the codes C_1 and C_2 are monomially equivalent. □

Now we present some applications of Theorem 4.2.5. First let us note that if two cyclic codes are monomially equivalent by Theorem 4.2.5, then they are not necessarily affine equivalent or permutation equivalent by the action of a generalized multiplier.

Example 4.2.6 Let $A_1 = \{0,1,3,4\}$ and $A_2 = \{2,5,6,7\}$ be the defining sets of cyclic codes C_1 and C_2 over $\mathbb{F}_3$ of length 8. One can easily verify that there is no bijective affine map between A_1 and A_2. Hence C_1 and C_2 are not affine equivalent. Note also that $A_1 = \{1,3\} \cup \{0,4\}$ and $A_2 = \{5,7\} \cup \{2,6\}$ satisfy the conditions of Theorem 4.2.5 and therefore C_1 and C_2 are monomially equivalent over $\mathbb{F}_3$. Moreover, generalized multipliers are only defined on integers modulo an odd prime power. Hence C_1 and C_2 are not permutation equivalent by the action of generalized multipliers.

Example 4.2.7 Our computation in Magma [17] shows that all the monomially equivalent cyclic codes of length 8 over $\mathbb{F}_3$, $\mathbb{F}_7$, and $\mathbb{F}_{11}$ are either affine equivalent, monomially equivalent by the action of $P_\sigma D$, or a combination of both. Overall, there are 32 different cyclic codes of length 8 over any of these fields, many of which are monomially equivalent.

In order to keep this example reasonably concise, we only show the equivalence of cyclic codes over $\mathbb{F}_3$ with dimension four, and the monomial equivalence of the remaining codes can be proved similarly. An easy computation shows that a cyclic code of length 8 over $\mathbb{F}_3$ with dimension four has one of the following defining sets:

$$A_1 = \{0,1,3,4\},\ A_2 = \{0,2,4,6\}, A_3 = \{0,4,5,7\}, A_4 = \{1,2,3,6\},$$
$$A_5 = \{1,3,5,7\}, A_6 = \{2,5,6,7\}.$$

Let $C_1, \ldots, C_6$ be cyclic codes of length 8 over $\mathbb{F}_3$ with the defining sets $A_1, \ldots, A_6$, respectively. Our Magma computation shows that C_1, C_3, C_4, and C_6 are all monomially equivalent. The same holds for the codes C_2 and C_5. Moreover, C_1 and C_2 are not monomially equivalent as $d(C_1) = 4$ and $d(C_2) = 2$, where d denotes the minimum distance. Then

$$\begin{tikzcd} C_1 \arrow[r, leftrightarrow, "P_\sigma D"] \arrow[d, leftrightarrow, "\psi_4"] & C_6 \arrow[d, leftrightarrow, "\psi_4"] \\ C_3 & C_4 \end{tikzcd} \tag{4.2.1}$$

and

$$\begin{tikzcd} C_2 \arrow[r, "\psi_1"] & C_5 \end{tikzcd}\ , \tag{4.2.2}$$

where the arrows describe the actions under which the corresponding cyclic codes are monomially equivalent. In particular, in (4.2.1), the map ψ_4 is the shift by 4, and $P_\sigma D$ is the monomial action of Theorem 4.2.5. Moreover, in (4.2.2), the map ψ_1 is the shift by 1. Since ψ_4 and $P_\sigma D$ are involutions, two-sided arrows show their actions. Now the monomial equivalence of the mentioned cyclic codes can easily be verified using Theorems 4.2.5, 1.6.9, and 1.6.10.

Another application of Theorem 4.2.5 is to check whether two cyclic codes are isodual. A linear code is called *isodual* if it is monomially equivalent to its Euclidean dual. Isodual codes could also be defined similarly in terms of other inner products; however, in this thesis, we only consider Euclidean isodual codes. Next, by applying the result of Theorem 4.2.5, we show the existence of isodual cyclic codes of length 8 over $\mathbb{F}_3$.

Example 4.2.8 The 3-cyclotomic cosets modulo 8 are $\{0\}$, $\{1,3\}$, $\{2,6\}$, $\{4\}$, and $\{5,7\}$. Let C be a cyclic code over $\mathbb{F}_3$ of length 8 with the defining set $A = \{0,1,3,4\}$. Its Euclidean dual $C^\perp$ has the defining set $A' = (\mathbb{Z}/n\mathbb{Z}) \backslash (-A) = \{1,2,3,6\}$. Let $b = 4$. Then b satisfies the conditions of Theorem 1.6.9 and $\psi_4(A') = \{2,5,6,7\}$. Thus $C^\perp$ is isometrically equivalent to the cyclic code D with the defining set $\{2,5,6,7\}$ over $\mathbb{F}_3$. Moreover, as we showed in Example 4.2.6, the cyclic codes C and D are monomially equivalent. Therefore, C and $C^\perp$ are monomially equivalent. This makes C and $C^\perp$ a pair of isodual codes over $\mathbb{F}_3$ of length 8.

4.2.2 Permutation equivalence of cyclic codes over fields of odd characteristic

Let n be a positive integer divisible by 8. We define the permutation γ on $\mathbb{Z}/n\mathbb{Z}$ by

$$\gamma(i) = \begin{cases} i & \text{if } i \text{ is even} \\ (i-2) \bmod n & \text{if } i \text{ is odd.} \end{cases}$$

We denote the permutation matrix corresponding to γ by P_γ. Let $\{s_i : 0 \leq i \leq n-1\}$ be the standard basis of $\mathbb{F}_q^n$. Then

$$s_i P_\gamma = \begin{cases} s_i & \text{if } i \text{ is even} \\ s_{i-2} & \text{if } i \text{ is odd.} \end{cases}$$

Since the generalized multipliers are not defined over $\mathbb{Z}/n\mathbb{Z}$ for an even integer n, the action of P_γ cannot be of a generalized multiplier type. Our main result of this section relies on the following intermediate lemmas.

Lemma 4.2.9 *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $n = 8k$ for some positive integer k such that* $\gcd(k, q) = 1$.

1. *Let $A = \{0\}$ or $A = \{\frac{n}{2}\}$ and C be the cyclic code of length n over $\mathbb{F}_q$ with the defining set A. Then $C = CP_\gamma$.*

2. *Let* $q \equiv 1 \pmod 4$ *and C_1 and C_2 be the cyclic codes of length n over $\mathbb{F}_q$ with the defining sets $\{\frac{n}{4}\}$ and $\{\frac{3n}{4}\}$, respectively. Then $C_2 = C_1 P_\gamma$.*

Proof. If $A = \{0\}$, then the all-ones vector $v^0 = (1, 1, \dots, 1)$ is a parity check matrix for C. If $A = \{\frac{n}{2}\}$, then $v^{\frac{n}{2}} = (1, -1, 1, -1, \dots, -1)$ is a parity check matrix for C. A straightforward computation shows that $v^0 P_\gamma = v^0$ and $v^{\frac{n}{2}} P_\gamma = v^{\frac{n}{2}}$. Hence $C = CP_\gamma$.

If $q \equiv 1 \pmod 4$, then $\{\frac{n}{4}\}$ and $\{\frac{3n}{4}\}$ are singleton q-cyclotomic cosets modulo n. The code C_1 has a parity check matrix in the form $v^{\frac{n}{4}} = (1, \alpha^{\frac{n}{4}}, \alpha^{\frac{n}{2}}, \alpha^{\frac{3n}{4}}, 1, \alpha^{\frac{n}{4}}, \dots, \alpha^{\frac{3n}{4}})$. Moreover, $v^{\frac{n}{4}} P_\gamma = v^{\frac{3n}{4}}$. Therefore, by Lemma 4.2.1, we have $C_2 = C_1 P_\gamma$. □

Lemma 4.2.10 *Let $\mathbb{F}_q$ be a finite field of odd characteristic and $n = 8k$ for some positive integer k such that* $\gcd(k, q) = 1$. *Let C be a cyclic code of length n over $\mathbb{F}_q$ with the defining set $A = Z(a) \cup Z(a + \frac{n}{2})$ for some $a \in \mathbb{Z}/n\mathbb{Z}$. Then $C = CP_\gamma$.*

Proof. If $a = 0$ or $a = \frac{n}{2}$, then the proof follows from Lemma 4.2.9. So we assume that $a \neq 0, \frac{n}{2}$. Note also that since q is odd we have $\psi_{\frac{n}{2}}(Z(a)) = Z(a + \frac{n}{2})$. So $Z(a)$ and $Z(a + \frac{n}{2})$ have the same size. Let $Z(a) = \{a_1, a_2, \dots, a_r\}$. Next we show that the sets $\{v^{a_i}, v^{(a_i + \frac{n}{2})}\}$ and $\{v^{a_i} P_\gamma, v^{(a_i + \frac{n}{2})} P_\gamma\}$ generate the same vector space over K for each $1 \leq i \leq r$. This shows that if H is a generalized parity check matrix for C, in the form of (1.4.2), then HP_γ

and H generate the same row space over K. Hence Lemma 4.2.1 implies that $C = CP_\gamma$. Note that $\alpha^{\frac{n}{2}} = -1$, and

$$v^{a_i} = (1, \alpha^{a_i}, \alpha^{2a_i}, \alpha^{3a_i}, \dots, \alpha^{(n-1)a_i})$$

and

$$v^{(a_i+\frac{n}{2})} = (1, \alpha^{a_i+\frac{n}{2}}, \alpha^{2a_i}, \alpha^{3a_i+\frac{n}{2}}, \dots, \alpha^{(n-1)a_i+\frac{n}{2}}).$$

By adding and subtracting the vectors v^{a_i} and $v^{(a_i+\frac{n}{2})}$ we get

$$v^{a_i} + v^{(a_i+\frac{n}{2})} = (2, 0, 2\alpha^{2a_i}, 0, 2\alpha^{4a_i}, \dots, 0)$$

and

$$v^{a_i} - v^{(a_i+\frac{n}{2})} = (0, 2\alpha^{a_i}, 0, 2\alpha^{3a_i}, 0, 2\alpha^{5a_i}, \dots, 2\alpha^{(n-1)a_i}).$$

Clearly the vectors $v^{a_i}+v^{(a_i+\frac{n}{2})}$ and $v^{a_i}-v^{(a_i+\frac{n}{2})}$ are linearly independent over K. Moreover,

$$v^{a_i}P_\gamma = (1, \alpha^{3a_i}, \alpha^{2a_i}, \alpha^{5a_i}, \dots, \alpha^{a_i})$$

and

$$v^{(a_i+\frac{n}{2})}P_\gamma = (1, \alpha^{3a_i+\frac{n}{2}}, \alpha^{2a_i}, \alpha^{5a_i+\frac{n}{2}}, \dots\ \alpha^{a_i+\frac{n}{2}}).$$

Since P_γ does not change the entries in even number columns, $v^{a_i} + v^{(a_i+\frac{n}{2})} = v^{a_i}P_\gamma + v^{(a_i+\frac{n}{2})}P_\gamma$. Moreover,

$$v^{a_i}P_\gamma - v^{(a_i+\frac{n}{2})}P_\gamma = (0, 2\alpha^{3a_i}, 0, 2\alpha^{5a_i}, 0, 2\alpha^{7a_i}, \dots\ 2\alpha^{a_i}) = \alpha^{2a_i}(v^{a_i} - v_{(a_i+\frac{n}{2})}).$$

This completes the proof by showing that $\{v^{a_i}, v^{(a_i+\frac{n}{2})}\}$ and $\{v^{a_i}P_\gamma, v^{(a_i+\frac{n}{2})}P_\gamma\}$ generate the same vector space over K for each $1 \leq i \leq r$. □

Next, we combine the results of the above lemmas and state a sufficient condition for permutation equivalence of cyclic codes. This is the main result of this section.

Theorem 4.2.11 *Let n be a positive integer divisible by 8 and q be a prime power such that $q \equiv 1 \pmod 4$ and $\gcd(n, q) = 1$. Let $A \subseteq \mathbb{Z}/n\mathbb{Z}$ be a union of q-cyclotomic cosets modulo n such that for each $a \in A$ either $a \in \{0, \frac{n}{2}\}$, or $(a + \frac{n}{2}) \bmod n$ is also an element of A. Then cyclic codes of length n over $\mathbb{F}_q$ with the defining sets $A \cup \{\frac{n}{4}\}$ and $A \cup \{\frac{3n}{4}\}$ are permutation equivalent under the action of P_γ.*

Proof. Let C_1 and C_2 be cyclic codes of length n over $\mathbb{F}_q$ with the defining sets $A \cup \{\frac{n}{4}\}$ and $A \cup \{\frac{3n}{4}\}$, respectively. Suppose that the matrix H is a generalized parity check matrix for C_1, in the form of (1.4.2). The proof follows from Lemmas 4.2.9 and 4.2.10 as the matrix HP_γ is a generalized parity check matrix of C_2. Therefore, by Lemma 4.2.1, C_1 and C_2 are permutation equivalent under the action of P_γ. □

The next example shows that permutation equivalent cyclic codes of Theorem 4.2.11 are not necessarily affine equivalent. Moreover, as we mentioned earlier, P_γ is not of a generalized multiplier type.

Example 4.2.12 Let $n = 8$ and $A = \{0, 1, 5\}$. By Theorem 4.2.11, cyclic codes of length 8 with the defining sets $A_1 = A \cup \{2\}$ and $A_2 = A \cup \{6\}$ over $\mathbb{F}_5$ are permutation equivalent. One can easily verify that there is no affine map between the sets A_1 and A_2. Moreover, our computation in Magma [17] shows that all monomially equivalent cyclic codes of length 8 over $\mathbb{F}_5$ are either affine equivalent, permutation equivalent under the action of P_γ, or a combination of both. A similar process as in Example 4.2.7 can justify such monomial equivalences. This classifies all the monomially equivalent cyclic codes of length 8 over $\mathbb{F}_5$.

4.2.3 New conditions for permutation equivalence of cyclic codes over $\mathbb{F}_4$

Let n be a positive odd integer divisible by 27 and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the field of four elements, where $\omega^2 = \omega + 1$. For the rest of this section, α denotes a fixed primitive n-th root of unity in $\mathbb{F}_4(\alpha)$, such that $\alpha^{\frac{n}{3}} = \omega$. We define the permutation χ on $\mathbb{Z}/n\mathbb{Z}$ by

$$\chi(i) = \begin{cases} i + 3 & \text{if } i \equiv 0 \text{ or } 4 \text{ or } 5 \pmod 9 \\ i - 3 & \text{if } i \equiv 3 \text{ or } 7 \text{ or } 8 \pmod 9 \\ i & \text{otherwise.} \end{cases} \tag{4.2.3}$$

Note that since $\chi(0) \neq 0$ the permutation χ is not of multiplier or generalized multiplier type. We denote the permutation matrix corresponding to χ by P_χ. Let $\{s_i : 0 \leq i \leq n-1\}$ be the standard basis of $\mathbb{F}_4^n$. Then

$$s_i P_\chi = \begin{cases} s_{i+3} & \text{if } i \equiv 0 \text{ or } 4 \text{ or } 5 \pmod 9 \\ s_{i-3} & \text{if } i \equiv 3 \text{ or } 7 \text{ or } 8 \pmod 9 \\ i & \text{otherwise.} \end{cases}$$

Since $3 \mid n$ there are always three singleton 4-cyclotomic cosets modulo n namely $\{0\}$, $\{\frac{n}{3}\}$, and $\{\frac{2n}{3}\}$. Before stating our main result of Section 4.2.3, we have three intermediate lemmas.

Lemma 4.2.13 *Let n be a positive odd integer divisible by 27 and C be a cyclic code of length n over $\mathbb{F}_4$ with the defining set $\{a\}$, where $a \in \{0, \frac{n}{3}, \frac{2n}{3}\}$. Then $C = CP_\chi$.*

Proof. Note that $v^a = (1, \alpha^a, \alpha^{2a}, \ldots, \alpha^{(n-1)a})$ is a parity check matrix for C. Moreover, the entry in j-th column of v^a is

$$(v^a)_j = \begin{cases} 1 & \text{if } a = 0 \\ \omega^j & \text{if } a = \frac{n}{3} \\ \omega^{2j} & \text{if } a = \frac{2n}{3}. \end{cases}$$

One can easily see that the j-th column of v^a remains unchanged under the action of P_χ. Thus $v^a = v^a P_\chi$. Therefore, by Lemma 4.2.1, we have $C = CP_\chi$. □

Lemma 4.2.14 *Let n be a positive odd integer divisible by 27, and C_1 and C_2 be cyclic codes of length n over $\mathbb{F}_4$ with defining sets $Z(\frac{n}{9})$ and $Z(\frac{2n}{9})$, respectively. Then $C_2 = C_1 P_\chi$.*

Proof. First, note that $Z(\frac{n}{9}) = \{\frac{n}{9}, \frac{4n}{9}, \frac{7n}{9}\}$ and $Z(\frac{2n}{9}) = \{\frac{2n}{9}, \frac{5n}{9}, \frac{8n}{9}\}$. Let $u = v^{\frac{n}{9}} + v^{\frac{4n}{9}} + v^{\frac{7n}{9}}$. Then for each $0 \leq j \leq n-1$, we have

$$u_j = \alpha^{j\frac{n}{9}} + \alpha^{j\frac{4n}{9}} + \alpha^{j\frac{7n}{9}} = \alpha^{j\frac{n}{9}}(1 + \alpha^{j\frac{n}{3}} + \alpha^{j\frac{2n}{3}}).$$

Thus

$$u_j = \begin{cases} \alpha^{j\frac{n}{9}} & \text{if } 3 \mid j \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 1 & \text{if } j \equiv 0 \pmod 9 \\ \omega & \text{if } j \equiv 3 \pmod 9 \\ \omega^2 & \text{if } j \equiv 6 \pmod 9 \\ 0 & \text{otherwise} \end{cases}$$

for each $0 \leq j \leq n-1$. A similar computation shows that if $x = v^{\frac{2n}{9}} + v^{\frac{5n}{9}} + v^{\frac{8n}{9}}$, then

$$x_j = \begin{cases} 1 & \text{if } j \equiv 0 \pmod 9 \\ \omega^2 & \text{if } j \equiv 3 \pmod 9 \\ \omega & \text{if } j \equiv 6 \pmod 9 \\ 0 & \text{otherwise} \end{cases}$$

for each $0 \leq j \leq n-1$. Let u' and u'' be the cyclic shifts of u by one and two positions to the right, respectively. The set $S = \{u, u', u''\}$ is linearly independent over K and matrix H consisting of elements of S as its rows is a parity check matrix for C_1. Next, we show that if x' and x'' are the cyclic shifts of x by one and two positions to the right, respectively, then $\{uP_\chi, u'P_\chi, u''P_\chi\} = \{\omega x, \omega x', \omega x''\}$. Since H and HP_γ are parity check matrices of linear codes with the same dimension, this implies that HP_γ is a parity check matrix for C_2. A straightforward computation shows that

$$(uP_\chi)_j = \begin{cases} \omega & \text{if } j \equiv 0 \pmod 9 \\ 1 & \text{if } j \equiv 3 \pmod 9 \\ \omega^2 & \text{if } j \equiv 6 \pmod 9 \\ 0 & \text{otherwise} \end{cases}$$

for each $0 \le j \le n-1$. Thus $uP_\chi = \omega x$. The equalities $u'P_\chi = \omega x'$ and $u''P_\chi = \omega x''$ follow accordingly. Hence, HP_γ is a parity check matrix for C_2 and by Lemma 4.2.1, and we have $C_2 = C_1 P_\chi$. □

Lemma 4.2.15 *Let $n = 3^t k$, where k and $t \ge 3$ are positive integers such that $\gcd(k,3) = 1$. Let $1 \le e \le n-1$. Then the following statements hold.*

1. *The set $A_e = \{(ek + i\frac{n}{3^{t-1}}) \bmod n : 0 \le i \le 3^{t-1}-1\}$ is a union of 4-cyclotomic cosets modulo n.*
2. *Suppose that C is the cyclic code of length n over $\mathbb{F}_4$ with defining set A_e. Then $C = CP_\chi$.*

Proof. To prove (1) we show that $A_e = \bigcup_{i=0}^{3^{t-1}-1} Z(ek + i\dfrac{n}{3^{t-1}})$, where some of the cyclotomic cosets are repeating in the union. Obviously, $A_e \subseteq \bigcup_{i=0}^{3^{t-1}-1} Z(ek + i\dfrac{n}{3^{t-1}})$. Let $0 \le s \le 3^{t-1}-1$ and $j \ge 0$ be an arbitrary integer. We have $4^j = 3l + 1$ for some positive integer l and

$$4^j(ek + s\frac{n}{3^{t-1}}) = ek + s\frac{n}{3^{t-1}} + 3lek + 3ls\frac{n}{3^{t-1}} = ek + (s + le + 3ls)\frac{n}{3^{t-1}} \in A_e,$$

where the last equality follows from the fact that $3k = \frac{n}{3^{t-1}}$. Hence $Z(ek + s\frac{n}{3^{t-1}}) \subseteq A_e$ for each $0 \le s \le 3^{t-1}-1$. This implies that $A_e = \bigcup_{i=0}^{3^{t-1}-1} Z(ek + i\dfrac{n}{3^{t-1}})$.

Now we prove (2). Let H be a generalized parity check matrix for C consisting of the row vectors

$$v^{(ek+i\frac{n}{3^{t-1}})} = (1, \alpha^{ek+i\frac{n}{3^{t-1}}}, \alpha^{2(ek+i\frac{n}{3^{t-1}})}, \ldots, \alpha^{(n-1)(ek+i\frac{n}{3^{t-1}})})$$

for $0 \le i \le 3^{t-1}-1$. Next, we produce a new generalized parity check matrix H' for C using linear combinations of rows of H. We also show that the rows of $H'P_\chi$ are the same as the rows of H'. This implies that $C = CP_\chi$.

Let $u = \sum_{i=0}^{3^{t-1}-1} v^{(ek+i\frac{n}{3^{t-1}})}$ be the sum of all rows of H. For each $0 \leq l \leq n-1$, we can compute the entry of the l-th column of u as

$$u_l = \sum_{i=0}^{3^{t-1}-1} \alpha^{l(ek+i\frac{n}{3^{t-1}})} = \alpha^{ekl}(\sum_{i=0}^{3^{t-1}-1} \alpha^{\frac{iln}{3^{t-1}}}) = \begin{cases} \alpha^{ekl} & \text{if } 3^{t-1} \mid l \\ 0 & \text{otherwise.} \end{cases} \tag{4.2.4}$$

Let $u^{[m]}$ be cyclic shift of the vector u by m positions to the right for each $0 \leq m \leq 3^{t-1}-1$. Then (4.2.4) implies that the set $B = \{u^{[m]} : 0 \leq m \leq 3^{t-1}-1\}$ is linearly independent over K. Let H' be a $3^{t-1} \times n$ matrix over K consisting of elements of B as its rows. Then H' is a generalized parity check matrix for C. Moreover, for each $0 \leq m \leq 3^{t-1}-1$ and $0 \leq l \leq n-1$ we have

$$(u^{[m]})_l = \begin{cases} \alpha^{ekl} & \text{if } 3^{t-1} \mid l-m \\ 0 & \text{otherwise.} \end{cases}$$

Since $9 \mid 3^{t-1}$,

$$u^{[m]}P_\chi = \begin{cases} u^{[m+3]} & \text{if } m \equiv 0 \text{ or } 4 \text{ or } 5 \pmod 9 \\ u^{[m-3]} & \text{if } m \equiv 3 \text{ or } 7 \text{ or } 8 \pmod 9 \\ u^{[m]} & \text{otherwise.} \end{cases}$$

Hence $H'P_\chi$ and H' have the same set of rows. Therefore $C = CP_\chi$. □

Now we combine all the above results and state a sufficient condition for the permutation equivalence of cyclic codes over $\mathbb{F}_4$. Let $n = 3^t k$, where k and $t \geq 3$ are positive integers such that $\gcd(k, 3) = 1$. The next theorem is the main result of this section.

Theorem 4.2.16 *Let $n = 3^t k$, where k and $t \geq 3$ are positive integers such that $\gcd(k,3) = 1$. Suppose that $B \subseteq \{0, \frac{n}{3}, \frac{2n}{3}\}$ and $1 \leq e_j \leq n-1$ for $1 \leq j \leq r$, where r is a positive integer. Then cyclic codes of length n with the defining sets $T_1 = Z(\frac{n}{9}) \cup B \cup \bigcup_{j=1}^{r} A_{e_j}$ and $T_2 = Z(\frac{2n}{9}) \cup B \cup \bigcup_{j=1}^{r} A_{e_j}$ are permutation equivalent over $\mathbb{F}_4$ under the action of P_χ, where A_e is defined as in part (1) of Lemma 4.2.15 for each $1 \leq e \leq n-1$.*

Proof. Let C_1 and C_2 be cyclic codes of length n over $\mathbb{F}_4$ with the defining sets T_1 and T_2, respectively. By Lemmas 4.2.13, 4.2.14, and 4.2.15 the matrix P_χ maps a generalized parity check matrix of C_1 to a generalized parity check matrix of C_2. Therefore, the result follows from Lemma 4.2.1. □

Next, we present an application of the above result.

Example 4.2.17 Let $n = 27$. An easy computation shows that $Z(1) = \{1+3i : 0 \leq i \leq 8\}$ and $Z(2) = \{2+3i : 0 \leq i \leq 8\}$. Now by Theorem 4.2.16, the cyclic codes of length 27 over $\mathbb{F}_4$ with the following pairs of defining sets are permutation equivalent:

- $Z(0) \cup Z(1) \cup Z(3)$ and $Z(0) \cup Z(1) \cup Z(6)$.
- $Z(0) \cup Z(2) \cup Z(3)$ and $Z(0) \cup Z(2) \cup Z(6)$.
- $Z(0) \cup Z(1) \cup Z(3) \cup Z(9)$ and $Z(0) \cup Z(1) \cup Z(6) \cup Z(9)$.
- $Z(0) \cup Z(1) \cup Z(3) \cup Z(9) \cup Z(18)$ and $Z(0) \cup Z(1) \cup Z(6) \cup Z(9) \cup Z(18)$.

Our computation in Magma [17] shows that the above pairs of codes are not permutation equivalent under the action of multipliers, generalized multipliers, or a combination of both. This is because multipliers and generalized multipliers always map 0 to 0. However, by (4.2.3), we have $\chi(0) = 3$. Moreover, the above pairs of codes are not affine equivalent. There are many more such pairs of permutation equivalent cyclic codes over $\mathbb{F}_4$ of length 27. To the best of our knowledge, the permutation equivalence of the above pairs of codes can not be proved by earlier results in the literature.

Example 4.2.18 This example presents some other values of n and q such that there exist at least a pair of monomially equivalent cyclic codes over $\mathbb{F}_q$ of length n which are not affine equivalent.

- For $q = 2$, lengths $n = 45, 49$.
- For $q = 3$, lengths $n = 8^*, 16^{**}, 32^{**}, 40^*, 48^{**}, 56^*$.
- For $q = 4$, lengths $n = 25, 27^{\diamond}, 49$.
- For $q = 5$, lengths $n = \underline{8}, \underline{16}, \underline{24}^*$.
- For $q = 7$, lengths $n = 8^*, 16^*, 18, 24^*, 32^{**}, 40^*$.
- For $q = 11$, lengths $n = 8^*, 16^{**}, 24^*$.

In the above list:

- The symbol $*$ shows the code lengths for which there exists a pair of monomially equivalent codes obtained by Theorem 4.2.5.
- The underline shows the code lengths for which there exists a pair of permutation equivalent codes obtained by Theorem 4.2.11.
- The symbol $\diamond$ shows the code lengths for which there exists a pair of permutation equivalent codes obtained by Theorem 4.2.16.

- The symbol $**$ shows the code lengths for which there exists a pair of monomially equivalent codes obtained by the action of the monomial matrix

$$\begin{bmatrix} P_\sigma D & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & P_\sigma D \end{bmatrix}$$

  consisting of more than one block of the matrix $P_\sigma D$ of Theorem 4.2.5 on the main diagonal.

The sufficient conditions of Theorems 4.2.5, 4.2.11, and 4.2.16 along with the monomial and permutation equivalence criteria given in Section 1.6 detect many monomially equivalent cyclic codes over various finite fields. Therefore, it is extremely beneficial and computationally inexpensive to use such conditions, and make the search for new cyclic codes with good parameters faster.

4.3 More results on the equivalence of cyclic codes

Let n be a positive integer such that $\gcd(n, q) = 1$ and A_1 and A_2 be defining sets of two length n linear cyclic codes C_1 and C_2 over $\mathbb{F}_q$, respectively. Recall from Theorem 1.6.9 that if b is a positive integer such that $n \mid |A_1|(q-1)b$ and $\psi_b(A_1) = A_2$, where $\psi_b(x) = (x + b) \bmod n$, then the codes C_1 and C_2 are isometrically equivalent. Conjecture 2 of [6] proposes that the condition "n divides $|A_1|(q-1)b$" is a necessary condition for the isometric equivalence of cyclic codes by a shift map. The next theorem proves this fact and also strengthens the result of Theorem 1.6.9. Recall that α is a fixed primitive n-th root of unity in the field $K = \mathbb{F}_q(\alpha)$.

Theorem 4.3.1 *Let C_1 and C_2 be two cyclic codes over $\mathbb{F}_q$ of length n with defining sets A_1 and A_2, respectively, and b be a positive integer. The codes C_1 and C_2 are isometrically equivalent through the shift map ψ_b on their defining sets if and only if ψ_b is a bijection between A_1 and A_2 and n divides $|A_1|(q-1)b$.*

Proof. Without loss of generality assume $\psi_b(A_1) = A_2$. We only prove the forward direction as the reverse direction follows from Theorem 1.6.9. Let $g_1(x)$ and $g_2(x)$ be the generator polynomials of C_1 and C_2, respectively. Then $g_1(x) = \prod_{i \in A_1} (x - \alpha^i)$ and

$$g_2(x) = \prod_{i \in A_2} (x - \alpha^i) = \prod_{i \in A_1} (x - \alpha^{i+b}) = \alpha^{b|A_1|} \prod_{i \in A_1} (\alpha^{-b}x - \alpha^i) = \alpha^{b|A_1|} g_1(\alpha^{-b}x). \quad (4.3.1)$$

Since $g_2(x)$ is defined over $\mathbb{F}_q$, the equality $\left(g_2(0)\right)^q = g_2(0)$ holds. By combining this fact with (4.3.1), we get

$$0 = \left(g_2(0)\right)^q - g_2(0) = \alpha^{b|A_1|q}\left(g_1(0)\right)^q - \alpha^{b|A_1|}g_1(0). \tag{4.3.2}$$

The generator polynomial of a non-empty cyclic code always has a non-zero constant term. Let the non-zero constant term of $g_1(x)$ be $g_1(0) = c \in \mathbb{F}_q$. Now (4.3.2) implies that

$$\alpha^{b|A_1|q}c^q - \alpha^{b|A_1|}c = c\alpha^{b|A_1|}(\alpha^{b|A_1|(q-1)} - 1) = 0. \tag{4.3.3}$$

Since c and $\alpha^{b|A_1|}$ are both non-zero, (4.3.3) implies that $\alpha^{b|A_1|(q-1)} = 1$ or equivalently $n \mid b|A_1|(q-1)$. □

Let $g_1(x)$ and $g_2(x)$ be generator polynomials of two monomially equivalent cyclic codes of length n over $\mathbb{F}_q$. Conjecture 1 of [6] proposes that for each integer $m \geq 1$ coprime to q, the length nm cyclic codes generated by $g_1(x)$ and $g_2(x)$ are monomially equivalent. Next we prove this statement. Note also that the cyclic codes of length nm generated by $g_1(x), g_2(x)$ have minimum distance of at most two since $x^n - 1$ is in correspondence with a weight two codeword.

Proposition 4.3.2 *Let $g_1(x)$ and $g_2(x)$ be generator polynomials of two monomially (respectively permutation) equivalent cyclic codes over $\mathbb{F}_q$ of length n. For each integer $m \geq 1$ coprime to q, the cyclic codes of length nm over $\mathbb{F}_q$ generated by $g_1(x)$ and $g_2(x)$ are also monomially (respectively permutation) equivalent.*

Proof. Let C_1 and C_2 be the cyclic codes of length n generated by $g_1(x)$ and $g_2(x)$, respectively. First we assume that C_1 and C_2 are monomially equivalent.

Let β be a primitive nm-th root of unity in a finite field extension of $\mathbb{F}_q$. Then $\alpha = \beta^m$ is a primitive n-th root of unity. Let $A_{g_1} = \{t : 0 \leq t \leq n-1 \text{ and } g_1(\alpha^t) = 0\} = \{a_1, a_2, \ldots, a_k\}$ be the defining set of C_1. By (1.4.2), the matrix

$$H_1 = \begin{bmatrix} 1 & \alpha^{a_1} & \alpha^{2a_1} & \cdots & \alpha^{a_1(n-1)} \\ 1 & \alpha^{a_2} & \alpha^{2a_2} & \cdots & \alpha^{a_2(n-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{a_k} & \alpha^{2a_k} & \cdots & \alpha^{a_k(n-1)} \end{bmatrix}$$

is a generalized parity check matrix for the code C_1. Since the cyclic codes C_1 and C_2 are monomial equivalent, by Lemma 4.2.1 there exists a monomial matrix M such that H_1M is a generalized parity check matrix for the code C_2. The length nm cyclic code generated by $g_1(x)$ has defining set $A'_{g_1} = \{ma_1, ma_2, \ldots, ma_k\}$. Therefore, the cyclic code of length

nm generated by $g_1(x)$ has a generalized parity check matrix in the form

$$H = \begin{bmatrix} 1 & \beta^{ma_1} & \beta^{2ma_1} & \dots & \beta^{(nm-1)ma_1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \beta^{ma_k} & \beta^{2ma_k} & \dots & \beta^{(nm-1)ma_k} \end{bmatrix} = \begin{bmatrix} H_1 & H_1 & \cdots & H_1 \end{bmatrix},$$

where the right side matrix contains m blocks of H_1, and the last equality is due to the fact that $\beta^m = \alpha$. Let

$$M' = \begin{bmatrix} M & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & M \end{bmatrix} \tag{4.3.4}$$

be the $nm \times nm$ monomial matrix over $\mathbb{F}_q$ containing m copies of M on the main diagonal. Next, we show that HM' is a generalized parity check matrix for the cyclic code of length nm generated by $g_2(x)$.

To avoid confusion, we show the length n and nm column vectors corresponding to a polynomial $f(x) \in \mathbb{F}_q[x]$ by $[f(x)]_n$ and $[f(x)]_{nm}$, respectively. Since M' is a monomial matrix over $\mathbb{F}_q$, the linear codes over $\mathbb{F}_q$ with the generalized parity check matrices H and HM' are monomially equivalent by Lemma 4.2.1. Therefore, it is enough to show

$$(HM') \left[x^i g_2(x)\right]_{nm} = 0$$

for each $0 \leq i \leq nm - 1$ and this implies that HM' is a generalized parity check matrix for the cyclic code of length nm generated by $g_2(x)$. Note that

$$H(M') = \begin{bmatrix} H_1M & H_1M & \cdots & H_1M \end{bmatrix},$$

where the right hand side matrix contains m blocks of H_1M. Let $g_2(x) = \sum_{i=0}^{k} b_i x^i$. The vector $\left[x^i g_2(x)\right]_{nm}$ has at most n non-zero coordinates for each $0 \leq i \leq nm - 1$ and

$$\begin{aligned} HM' \left[x^i g_2(x)\right]_{nm} &= \begin{bmatrix} H_1M & H_1M & \cdots & H_1M \end{bmatrix} \left[x^i g_2(x)\right]_{nm} \\ &= H_1M \left[x^{(i \bmod n)} g_2(x)\right]_n = 0. \end{aligned} \tag{4.3.5}$$

The last equality of (4.3.5) follows from the fact that H_1M is a generalized parity check matrix for C_2. This proves that $g_1(x)$ and $g_2(x)$ generate monomial equivalent cyclic codes of length nm.

Note that if C_1 and C_2 are permutation equivalent, then the matrix M' defined in (4.3.4) is a permutation matrix and therefore $g_1(x)$ and $g_2(x)$ generate permutation equivalent cyclic codes of length nm over $\mathbb{F}_q$. □

4.4 New results on equivalence of constacyclic codes over $\mathbb{F}_4$

Recall that $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ is the field of four elements, where $\omega^2 = \omega + 1$. Throughout this section, we assume that n is a positive odd integer and $L = \mathbb{F}_4(\delta)$, where δ is a primitive $3n$-th root of unity such that $\delta^n = \omega$. Let $r = [L : \mathbb{F}_4]$ and

$$\Omega = \{1 + 3j : 0 \leq j \leq n - 1\}.$$

Then the roots of $x^n - \omega$ are in the form δ^a for each $a \in \Omega$. Let C_1 and C_2 be two ω-constacyclic codes over $\mathbb{F}_4$ of length n with the defining sets A_1 and A_2, respectively. Recall that if there exists a map $\psi_{3j}(x) = (x + 3j) \bmod (3n)$ on $\mathbb{Z}/3n\mathbb{Z}$ such that n divides $3j \deg(g(x))$, and $\psi_{3j}(A_1) = A_2$, then C_1 and C_2 are monomially equivalent. Next we show that the condition "n divides $3j \deg(g(x))$" is a necessary condition for the existence of a shift bijection between the defining sets of two ω-constacyclic codes over $\mathbb{F}_4$.

Theorem 4.4.1 *Let A_1 and A_2 be defining sets of two ω-constacyclic codes of length n over $\mathbb{F}_4$ and b be a positive integer. If the shift map $\psi_b(x)$ defined on $\mathbb{Z}/3n\mathbb{Z}$ satisfies $\psi_b(A_1) = A_2$, then 3 divides b and n divides $b|A_1|$.*

Proof. As we mentioned earlier, roots of $x^n - \omega$ are δ^{3k+1} for $0 \leq k \leq n-1$. Thus, 3 divides b as otherwise for each $s \in \psi_b(A_1)$, δ^s is not a root of $x^n - \omega$. Moreover, $x^n - \omega \mid x^{3n} - 1$ and therefore defining set of each ω-constacyclic code over $\mathbb{F}_4$ of length n is also defining set of a cyclic code of length $3n$ over $\mathbb{F}_4$. Now Theorem 4.3.1 implies that $3n \mid 3b|A_1|$ which is equivalent to $n \mid b|A_1|$. □

The next example presents several pairs of monomially equivalent constacyclic code obtained by the action of affine maps on their defining sets. After this example, we give an infinite family of pairs of monomially equivalent constacyclic codes using the observation of this example.

Example 4.4.2 Let $n = 21$. The defining set of an ω-constacyclic code of length n over $\mathbb{F}_4$ is a union of the following 4-cyclotomic cosets modulo $3n$: $Z(1) = \{1, 4, 16\}$, $Z(7) = \{7, 28, 49\}$, $Z(10) = \{10, 34, 40\}$, $Z(13) = \{13, 19, 52\}$, $Z(22) = \{22, 25, 37\}$, $Z(31) = \{31, 55, 61\}$, and $Z(43) = \{43, 46, 58\}$. We show that all the ω-constacyclic codes with a single cyclotomic coset as its defining set are monomially equivalent. We first use the shift map $\psi_{21}(x) = (x + 21) \bmod 63$ which satisfies the conditions of Theorem 1.6.15 (affine equivalence for constacyclic codes). Note that the map ψ_{21} gives the following bijections

$$Z(1) \to Z(22),\ Z(22) \to Z(43),\ Z(13) \to Z(10),\ \text{and } Z(10) \to Z(31). \tag{4.4.1}$$

Therefore, each pair of the ω-constacyclic codes with the defining sets $Z(1), Z(22), Z(43)$, or with the defining sets $Z(13), Z(10), Z(31)$ are monomially equivalent by Theorem 1.6.15.

Moreover, the multipliers $\mu_{13} : Z(1) \to Z(13)$ and $\mu_7 : Z(1) \to Z(7)$ are both bijections. Therefore, by Theorem 1.6.13, the constacyclic codes with the defining sets $Z(1), Z(7)$, and $Z(13)$ are permutation equivalent. Now, by combining these results, we see that each pair of ω-constacyclic codes of length n over $\mathbb{F}_4$ with the defining sets $Z(i)$ and $Z(j)$, where $i, j \in \{1, 7, 10, 13, 22, 31, 43\}$ are monomially equivalent. There are many more monomially equivalent ω-constacyclic codes of length 21 over $\mathbb{F}_4$.

Example 4.4.3 Let $n = 3(2k+1)$ for some integer $k > 1$. We show that each pair of ω-constacyclic codes of length n over $\mathbb{F}_4$ with the defining sets $Z(i)$ and $Z(j)$, where $i, j \in \{1, n+1, 2n+1\}$ are monomially equivalent. To prove this fact we show that the shift maps $\psi_n(x) = (x+n) \bmod 3n$ and $\psi_{2n}(x) = (x+2n) \bmod 3n$ are bijection from $Z(1)$ to $Z(n+1)$ and from $Z(1)$ to $Z(2n+1)$, respectively. Since both these maps satisfy the conditions of Theorem 1.6.15, ω-constacyclic codes with the defining sets in $\{Z(1), Z(n+1), Z(2n+1)\}$ are monomially equivalent.

First note that $4^i(n+1) \equiv n + 4^i \pmod{3n}$ and $4^i(2n+1) \equiv 2n + 4^i \pmod{3n}$ for each integer i. Therefore, the 4-cyclotomic cosets $Z(1)$, $Z(n+1)$, and $Z(2n+1)$ all have the same size. Moreover, let $Z(1) = \{4^i : 0 \le i \le r-1\}$, where $r = [\mathbb{F}_4(\delta) : \mathbb{F}_4]$. Then $Z(n+1) = \{n + 4^i : 0 \le i \le r-1\}$ and $Z(2n+1) = \{2n + 4^i : 0 \le i \le r-1\}$. Now, one can easily verify that the maps $\psi_n(x)$ and $\psi_{2n}(x)$ are bijections.

Recall that ϕ is the Euler's totient function. Our next goal of this section is to show that all permutation equivalent ω-constacyclic codes of length n over $\mathbb{F}_4$ such that $\gcd(3n, \phi(3n)) = 1$ are given by the action of multipliers on their defining sets. This result is analogous to the result of Theorem 1.6.5 for cyclic codes.

Theorem 4.4.4 *Let C_1 and C_2 be two non-trivial ω-constacyclic codes over $\mathbb{F}_4$ of length n with defining sets A_1 and A_2 such that $\gcd(3n, \phi(3n)) = 1$. Then C_1 and C_2 are permutation equivalent if and only if there exists a multiplier μ_e defined on $\mathbb{Z}/3n\mathbb{Z}$ such that $\mu_e(A_1) = A_2$ for some positive integer $e \equiv 1 \pmod 3$.*

Proof. We only prove the forward direction as the reverse follows from Lemma 1.6.13. Since $x^n - \omega \mid x^{3n} - 1$, the sets A_1 and A_2 are also defining sets of two cyclic codes D_1 and D_2 of length $3n$ over $\mathbb{F}_4$, respectively. It is enough to show that D_1 and D_2 are permutation equivalent, and since $\gcd(3n, \phi(3n)) = 1$, Theorem 1.6.5 implies the existence of a multiplier μ_e defined on $\mathbb{Z}/3n\mathbb{Z}$ such that $\mu_e(A_1) = A_2$. Moreover, the fact that $A_1, A_2 \subset \{3\ell + 1 : 0 \le \ell \le n-1\}$ implies $e \equiv 1 \pmod 3$.

Let $A_1 = \{a_1, a_2, \ldots, a_k\}$ and the matrix

$$H_1 = \begin{bmatrix} 1 & \delta^{a_1} & \cdots & \delta^{a_1(n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \delta^{a_k} & \cdots & \delta^{a_k(n-1)} \end{bmatrix}$$

be a generalized parity check matrix for the code C_1. Since $\delta^n = \omega$ the matrix

$$H = \begin{bmatrix} 1 & \delta^{a_1} & \dots & \delta^{a_1(3n-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \delta^{a_k} & \dots & \delta^{a_k(3n-1)} \end{bmatrix} = \begin{bmatrix} H_1 & \omega H_1 & \omega^2 H_1 \end{bmatrix} \tag{4.4.2}$$

is a generalized parity check matrix for D_1. The rest of the proof follows from the proof of Proposition 4.3.2 by choosing the matrices H_1 and H as above, and M' to be the permutation matrix

$$M' = \begin{bmatrix} P & 0 & 0 \\ 0 & P & 0 \\ 0 & 0 & P \end{bmatrix},$$

where P is a permutation matrix and H_1P is a generalized parity check matrix for C_2. □

The above result helps to classify all permutation equivalent ω-constacyclic codes of certain lengths.

4.5 Nearly dual-containing cyclic and constacyclic codes and new quantum codes

In this section, we only consider cyclic and constacyclic codes over $\mathbb{F}_4$. The family of nearly dual-containing cyclic codes over $\mathbb{F}_4$ with respect to the Hermitian inner product was studied in [68]. We first recall some known results about nearly dual-containing cyclic codes. Then we extend the idea to the family of constacyclic codes over $\mathbb{F}_4$. We also briefly describe search algorithms for new binary quantum codes from nearly dual-containing cyclic and constacyclic codes over $\mathbb{F}_4$. Throughout the rest of this section, n is a positive odd integer.

Let C be a cyclic code of length n over $\mathbb{F}_4$ with the defining set A. The Hermitian dual of C has the defining set $\mathbb{Z}/n\mathbb{Z} \setminus (-2A \bmod n)$. The next proposition determines when a cyclic code is dual-containing over $\mathbb{F}_4$ with respect to the Hermitian inner product.

Proposition 4.5.1 *[55, Theorem 4.4.16] Let n be a positive odd integer, and C be a cyclic code of length n over $\mathbb{F}_4$ with the defining set A. Then $C^{\perp_h} \subseteq C$ if and only if $A \cap -2A = \emptyset$.*

Recall that, as we defined in Definition 2.3.4, for each linear code C the value $e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h})$ is called the dual-containment deficiency of C. The following proposition calculates the dual-containment deficiency of a cyclic code.

Proposition 4.5.2 *[68] Let $C \subseteq \mathbb{F}_4^n$ be a cyclic code with the defining set A. Then*

$$e = \dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h}) = |A \cap -2A|.$$

To apply the quantum construction of Theorem 1.7.9 to a cyclic code, it is more reasonable to only target a code with a small e value. This is because dimension of the code $C+C^{\perp_h}$ is large (hence it probably has a small minimum distance) when the value of e is closer to $\dim(C^{\perp_h})$. Thus we only target cyclic codes over $\mathbb{F}_4$ with the dual-containment deficiency $e \leq 3$. We consider the following observations in our search algorithm for new binary quantum codes from nearly dual-containing cyclic codes.

Search algorithm. Step 1. Fix n to be a given positive odd integer. If $\gcd(n,3)=1$, then, by Theorem 1.6.12, cyclic and ω-constacyclic codes of length n over $\mathbb{F}_4$ are monomially equivalent. We store this information to avoid duplicating the computation of such codes.

Step 2. We design a *backtracking algorithm* to enumerate all cyclic codes of length n with a small value of e. Note that Proposition 4.5.2 allows us to fix an upper bound for the dual-containment deficiency e in the backtracking algorithm. In particular, we start with the defining set $A=\emptyset$ and add a 4-cyclotomic coset to A at each step. An easy observation on the definition of the dual-containment deficiency parameter shows that for the defining sets $A_1 \subseteq A_2$, $e_{A_1} \leq e_{A_2}$, where e_{A_1} and e_{A_2} are the corresponding dual-containment deficiency parameters. Therefore this allows us to enforce an upper bound on the dual-containment deficiency parameter e in the backtracking algorithm.

Step 3. We apply the results of Sections 1.6.1, 4.2, and 4.3 to consider only one of each two monomially equivalent cyclic codes.

Step 4. Finally, we apply the quantum construction of Theorem 1.7.9 to the codes satisfying the above steps. Note that we bound the minimum distance d using the lower bound $d \geq \min\{d(C), d(C+C^{\perp_h})+1\}$ with the aid of Magma computer algebra system [17].

In Section 4.5.2, we present new record-breaking binary quantum and linear codes that were obtained from our search.

4.5.1 Nearly dual-containing constacyclic codes over $\mathbb{F}_4$

In this section, we target nearly dual-containing constacyclic codes with respect to the Hermitian inner product to construct new binary quantum codes. We first give a formula that computes the dual-containment deficiency of each constacyclic code. Next, we classify all the constacyclic codes with small dual-containment deficiency values. Finally, we briefly describe our search algorithm for new binary quantum codes from nearly dual-containing constacyclic codes.

As we mentioned in (1.6.1), there exists an isometry between ω- and ω^2-constacyclic codes of length n over $\mathbb{F}_4$. So it is sufficient to study one of these two families, and our results remain valid for the other family. The following theorem gives a criterion for dual-containment of constacyclic codes over $\mathbb{F}_4$.

Theorem 4.5.3 *[59] Let $C \subseteq \mathbb{F}_4^n$ be an ω-constacyclic code with the defining set A. Then $C^{\perp_h} \subseteq C$ if and only if $A \cap -2A = \emptyset$.*

Proof. This is the case $q=4$ of [59, Lemma 2.2]. □

In practice, there are many ω-constacyclic codes which are not Hermitian dual-containing but are nearly dual-containing. The next theorem computes the dual-containment deficiency parameter using the defining sets of a given ω-constacyclic code. This result and its proof are similar to those of Proposition 4.5.2. Recall that $\Omega = \{1+3j : 0 \leq j \leq n-1\}$ for each positive odd integer n.

Theorem 4.5.4 *Let C be an ω-constacyclic code of length n over $\mathbb{F}_4$ with the defining set A. Then $e = |A \cap -2A|$.*

Proof. In this proof, the arithmetics of defining sets are done modulo $3n$. Let δ be a primitive $3n$-th root of unity in a finite field extension of $\mathbb{F}_4$ such that $\delta^n = \omega$. Then the generator polynomials of $C^{\perp_h}$ and $C \cap C^{\perp_h}$ are, respectively,

$$\prod_{k \in \Omega \setminus -2A} (x - \delta^k) \quad \text{and} \quad \prod_{k \in A \cup (\Omega \setminus -2A)} (x - \delta^k).$$

So $\dim(C^{\perp_h}) - \dim(C \cap C^{\perp_h})$ can be computed as

$$e = n - |\Omega \setminus -2A| - (n - |A \cup (\Omega \setminus -2A)|) = |A \cup (\Omega \setminus -2A)| - |\Omega \setminus -2A| = |A \cap -2A|. \tag{4.5.1}$$

□

The set $\Omega = \{1+3j : 0 \leq j \leq n-1\}$ can be partitioned using 4-cyclotomic cosets modulo $3n$ in the form $Z_1, \ldots, Z_r, Z'_1, -2Z'_1, \ldots, Z'_s, -2Z'_s$, where $-2Z_i = Z_i$ for each $1 \leq i \leq r$ and $Z'_j \neq -2Z'_j$ for all $1 \leq j \leq s$.

Corollary 4.5.5 *Let C be an ω-constacyclic code of length n over $\mathbb{F}_4$ with the defining set A. Then*

1. *C is Hermitian dual-containing if and only if $Z_i \not\subseteq A$ for all $1 \leq i \leq r$ and A contains at most one of Z'_j and $-2Z'_j$ for each $1 \leq j \leq s$.*

2. *C has the dual-containment deficiency parameters*

$$e = \sum_{i=1}^{r} |A \cap Z_i| + \sum_{j=1}^{s} 2\sqrt{|A \cap Z'_j||A \cap -2Z'_j|}. \tag{4.5.2}$$

Proof. The proof of part 1 follows immediately from part 2 since C is Hermitian dual-containing if and only if $e = 0$. Note that by Theorem 4.5.4 we have $e = |A \cap -2A| = \sum_{Z} |(A \cap -2A) \cap Z|$, where the sum runs over all the different 4-cyclotomic cosets Z such that $Z \subseteq \Omega$. For each $1 \leq i \leq r$, if $Z_i \subseteq A$, then $Z_i \subseteq -2A$. Therefore $Z_i \subseteq A \cap -2A$. Hence, $|(A \cap -2A) \cap Z_i| = |A \cap Z_i|$.

For each $1 \leq j \leq s$, the j-th term of the second sum in (4.5.2) is non-zero if and only if $Z'_j, -2Z'_j \subseteq A$. Moreover, $Z'_j, -2Z'_j \subseteq A$ is equivalent to $Z'_j, -2Z'_j \subseteq -2A$. Therefore, the j-th term of the second sum is $2|Z'_j|$ if and only if $Z'_j, -2Z'_j \subseteq (A \cap -2A)$ or equivalently $(Z'_j \cup -2Z'_j) \subseteq A \cap -2A$. □

Example 4.5.6 Let $n = 7$. Then $\Omega = \{1, 4, 7, 10, 13, 16, 19\}$ and all the ordered 4-cyclotomic cosets modulo 21 intersecting Ω are $Z(1) = \{1, 4, 16\}$, $Z(7) = \{7\}$, and $Z(10) = \{10, 19, 13\}$. Note also that $-2Z(1) = Z(10)$ and $-2Z(7) = Z(7)$. Therefore, if $Z(1)$ is the defining set of an ω-constacyclic code C of length n over $\mathbb{F}_4$, then the code C is Hermitian dual-containing by Corollary 4.5.5 part 1.

Moreover, if $Z(1) \cup Z(10)$ is the defining set for an ω-constacyclic code C' of length n over $\mathbb{F}_4$, then the code C' is not Hermitian dual-containing by Corollary 4.5.5. This constacyclic code has $e = 2|Z(1)| = 6$ by the formula (4.5.2).

Now, we classify all the nearly dual-containing constacyclic codes with $e = 1$ and $e = 2$.

Theorem 4.5.7 *Let C be an ω-constacyclic code of an odd length n over $\mathbb{F}_4$ and the defining set $A \subseteq \Omega$. Then*

I. The code C has the dual-containment deficiency parameter $e = 1$ if and only if one of the following happens.

(a) $n \equiv 1 \pmod 3$, the set A contains the singleton cyclotomic coset $\{n\}$, and the other cyclotomic cosets intersecting A satisfy the orthogonality conditions given in Corollary 4.5.5 part 1.

(b) $n \equiv 2 \pmod 3$, the set A contains the singleton cyclotomic coset $\{2n\}$, and the other cyclotomic cosets intersecting A satisfy the orthogonality conditions given in Corollary 4.5.5 part 1.

II. The case $e = 2$ never happens for C.

Proof. I. By the dual-containment deficiency formula given in (4.5.2), we have $e = 1$ if and only if A contains a singleton 4-cyclotomic coset modulo $3n$ in the form $\{1 + 3j\}$, where $4(1+3j) \equiv 1+3j \pmod{3n}$ for some $0 \leq j \leq n-1$ and other 4-cyclotomic cosets modulo $3n$ intersecting A satisfy the condition (1) of Corollary 4.5.5. This implies that

$$3(1 + 3j) \equiv 0 \pmod{3n} \tag{4.5.3}$$

and therefore $n \mid 1+3j$. If $n \equiv 1 \pmod 3$, the only cyclotomic coset satisfying the previous equation is $\{n\}$ and the case (a) happens. If $n \equiv 2 \pmod 3$, the cyclotomic coset $\{2n\}$ satisfies the equation (4.5.3) and therefore the case (b) above happens. Finally, for the values of n in the form $n \equiv 0 \pmod 3$, there is no singleton cyclotomic coset.

II. Since there is at most one singleton cyclotomic coset for each value of n, the formula (4.5.2) implies that the case $e = 2$ happens if and only if there exists a size two 4-cyclotomic coset modulo $3n$ in the form $Z = \{(1+3j), 4(1+3j)\} \subseteq A$ for some $0 \leq j \leq n-1$ such that $-2Z = Z$. Next, we show that there is no such cyclotomic coset. The condition $-2Z = Z$ implies that $3(1+3j) \equiv 0 \pmod{3n}$ or $6(1+3j) \equiv 0 \pmod{3n}$. Since $\gcd(n, 2) = 1$, these equations are the same. However, as we discussed in the previous case, the condition $3(1+3j) \equiv 0 \pmod{3n}$ implies that Z is a singleton cyclotomic coset. Therefore, there is no cyclotomic coset Z in the above form, and the case $e = 2$ never happens. □

Next, we briefly sketch the main observations in our search algorithm for new binary quantum codes from nearly dual-containing constacyclic codes.

Search algorithm. Step 1. Let n be a given positive odd integer. As we mentioned earlier, we only consider ω-constacyclic codes in our search for new quantum codes. This is because ω- and ω^2-constacyclic codes are monomially equivalent.

Step 2. If $\gcd(n, 3) = 1$, then, by Theorem 1.6.12, cyclic codes and ω-constacyclic codes of length n over $\mathbb{F}_4$ are monomially equivalent. So we do not duplicate the computation for cyclic and ω-constacyclic codes of such lengths.

Step 3. We design a *backtracking algorithm* to enumerate all ω-constacyclic codes of length n with a small value of e similar to that of cyclic codes introduced earlier on page 128.

Step 4. We apply the results of Sections 1.6.2 and 4.4 to only consider inequivalent ω-constacyclic codes in our search.

Step 5. Finally, we apply the quantum construction of Theorem 1.7.9.

4.5.2 Numerical results

This section presents new record-breaking binary quantum codes and linear codes over $\mathbb{F}_4$ that were obtained from our search for new codes. Results about equivalence of linear codes can be used to prune branches of the search algorithms for new codes with good properties. In practice, the parameters of quantum codes are known much less than classical linear codes in the literature, as can be seen in the code tables [43]. In the following examples, we give new record-breaking linear and quantum codes that were obtained from cyclic and constacyclic codes over $\mathbb{F}_4$. Applying the secondary construction to our new codes produces many more record-breaking linear codes and binary quantum codes. The validity of our new codes is already verified in the "Updates" section of [45].

Example 4.5.8 Let $n = 51$ and A be the defining set of a cyclic code C of length n over $\mathbb{F}_4$ with the coset leaders $\{0, 2, 7, 17, 34\}$. The code C is affine equivalent to 24 cyclic codes of the same length over $\mathbb{F}_4$, of which only one needs to be considered, thus reducing the running time by a factor of 24. Moreover, C is a $[51, 40]$ cyclic code and $\min\{d(C), d(C + C^{\perp_h}) + 1\} = 4$. After applying the construction of Theorem 1.7.9, we get $e = 3$ which implies the existence of a $[\![54, 32]\!]$ binary quantum code D. Note that the dual-containing code D was constructed using the proof of Theorem 1.7.9 provided in [68]. The minimum weight in $D \setminus D^{\perp_h}$ is 6. Hence we get a $[\![54, 32, 6]\!]$ code which has a *better minimum distance* than the currently best-known binary quantum code with the same length and dimension.

Example 4.5.9 Let $n = 111$ and A be the defining set of an ω-constacyclic code C of length n over $\mathbb{F}_4$ with the coset leaders $\{19, 37\}$. The code C has the same parameters as five other ω-constacyclic codes of the same length over $\mathbb{F}_4$ through an affine bijection on their defining sets. The code C is a $[111, 90]$ linear code, $e = 3$, and $\min\{d(C), d(C+C^{\perp_h})+1\} = 9$. After applying the construction of Theorem 1.7.9 to the code C, we constructed a new binary quantum code with parameters $[\![114, 72, 9]\!]$ which has a *better minimum distance* than the current best known binary quantum code. Moreover, the linear code C is a $[111, 90, 9]$ linear code over $\mathbb{F}_4$, which has a *better minimum distance* than the currently best-known linear code over $\mathbb{F}_4$ with the same length and dimension.

In a private communication with Markus Grassl, it was brought to our attention that the code C has a supercode C' with parameters $[111, 91, 9]$. Applying secondary constructions to C' produces 38 other record-breaking linear codes over $\mathbb{F}_4$. Moreover, applying the quantum construction of Theorem 1.7.9 to C' produces another record-breaking binary quantum code with parameters $[\![113, 73, 9]\!]$. The latter quantum code produces 35 other new record-breaking binary quantum codes after applying the secondary constructions to it.

The results on equivalence of codes allowed us to compute parameters of cyclic and constacyclic codes of certain lengths very fast. In particular, we first reduced the total number of cyclic and constacyclic codes to a smaller number of codes that contain no pairs of monomially equivalent codes under the results presented in this thesis. Then we computed the parameters of these remaining codes. This helped us to examine the parameters of cyclic and constacyclic codes of various lengths. Note also that determining even a small number of equivalent codes can significantly reduce the computation time of code parameters. The following example shows an instance of this observation.

Example 4.5.10 Let $n = 111$ and A be the defining set of an ω-constacyclic code C of length n over $\mathbb{F}_4$ with the coset leaders $\{19, 37, 49\}$. Our computation in Magma [17] shows that the code C has parameters $[111, 72, 16]$. The minimum distance computation time of C in Magma was about 53 days (1290 hours). The code C is permutation equivalent to two other ω-constacyclic codes of length n over $\mathbb{F}_4$ with the coset leaders $\{1, 13, 37\}$ and $\{7, 31, 37\}$. Hence, in this case, the computation time reduction given by the permutation equivalence of constacyclic codes is about 106 days. The time reduction can be even more significant when the code's length is larger, or its dimension is closer to $n/2$. The previously best-known linear code over $\mathbb{F}_4$ with the length 111 and dimension 72 had the minimum distance 15. Hence C is a new *record-breaking* linear code over $\mathbb{F}_4$. Shortening of the code C

produces five other record-breaking linear codes over $\mathbb{F}_4$ with the parameters $[111-i, 72-i, 16]$ for each $1 \leq i \leq 5$.

Chapter 5

Future directions

In this thesis, we developed new methods of constructing binary quantum stabilizer codes using classical linear and additive codes. This led to the discovery of many record-breaking and optimal binary quantum codes. New theoretical results for the equivalence of additive and linear codes were provided. Moreover, we gave several new minimum distance bounds. More details about our main contributions of this thesis were given in Section 1.8.

In the final chapter we discuss several questions and potential lines of work opened up by this thesis. These research problems are directly related to classical algebraic codes and can be applied to generate good quantum stabilizer codes more systematically.

5.1 Linear cyclic, constacyclic, and duadic codes

The quantum constructions presented in Chapter 2 were designed mainly based on the structure of duadic, QR, and linear cyclic codes over $\mathbb{F}_4$. One of our future plans is to apply the CSS construction (Theorem 1.7.5) to the binary duadic, QR, and linear cyclic codes and give other constructions for 0-dimensional quantum codes. The quantum CSS construction builds binary quantum codes by only considering linear binary codes satisfying an inclusion condition. In general, applying the CSS construction to linear binary codes C_1 and C_2 such that $C_1 \nsubseteq C_2$ produces nearly dual-containing additive codes over $\mathbb{F}_4$. Such nearly dual-containing codes could be good ingredients for the quantum construction of Theorem 3.2.3. In particular, my computations suggest that record-breaking binary quantum codes can be constructed this way.

In this thesis, we classified all nearly dual-containing linear cyclic and constacyclic codes with respect to the Hermitian inner product. The family of quasi-cyclic (QC) codes, which is a generalization of linear cyclic codes, could be another promising candidate for applying the quantum construction of Theorem 1.7.9. In the literature, there are numeric examples of good quantum codes from Hermitian dual-containing QC codes that are obtained from an exhaustive search [37]. Therefore, another research idea is to classify nearly dual-containing QC codes.

In Section 2.5 (Proposition 2.5.2) we provided bounds for the minimum distance of linear cyclic codes. Our distance bounds were designed using the action of multipliers on cyclic codes. The following are some remaining questions to be answered.

1. Our numeric computation showed that about 97% of cyclic codes with length $9 \leq n \leq 85$ have the same minimum distance as their fixed subcode by the action of a multiplier. An interesting question is to classify linear cyclic codes that have the same minimum distance as their fixed subcodes.
2. Is it possible to make the minimum distance lower bound of Proposition 2.5.2 tighter? One idea for this problem is to obtain more information about the minimum distance of the original linear cyclic code by examining the weight distribution of its fixed subcode.
3. To provide a similar lower bound for the minimum distance of other families of linear or additive codes such as linear constacyclic codes.

Another interesting problem is designing families of constacyclic BCH codes with good properties. In general, constacyclic BCH codes have been studied relatively less than other families of BCH codes, and good classes of linear codes have been constructed this way [98]. Constacyclic BCH codes can also be used to produce quantum codes with good parameters [70].

5.2 Modifications of our quantum code construction

In Section 3.2, we gave a construction for binary quantum codes from given additive codes over $\mathbb{F}_4$ (Theorem 3.2.3). In particular, we showed that if C is an $(n, 2^{n+k})$ additive code over $\mathbb{F}_4$ and

$$e = \frac{\dim_{\mathbb{F}_2}(C^{\perp_t}) - \dim_{\mathbb{F}_2}(C \cap C^{\perp_t})}{2},$$

then there exists a binary quantum code with parameters $[\![n+e, k+e, d]\!]$, where

$$d \geq \min\{d(C^{\perp_t}), d(C + C^{\perp_t}) + 1\}. \tag{5.2.1}$$

We propose two ideas that could be applied to improve the minimum distance bound of (5.2.1). First, in the proof of this result, we used a fixed $2e \times e$ matrix T to construct a dual-containing additive code. The matrix T generates an additive code with the minimum distance of one over $\mathbb{F}_4$. That is the reason we have $d(C + C^{\perp_t}) + 1$ in the above bound. In general, there are many alternatives for the matrix T above, and different selections of such a matrix could improve the minimum distance lower bound of (5.2.1). This improvement can happen when $e \geq 4$.

Second, in Example 4.5.8, we constructed a quantum code with the minimum distance of 6. In the same example, we showed that the lower bound in (5.2.1) gives $d \geq 4$. The next natural question is to see under what condition such minimum distance improvement happens and systematically attack such cases. This question was raised in a private communication with Markus Grassl.

5.3 Additive twisted codes

We studied additive twisted codes in Chapter 3. Although we answered several questions about the structure of twisted codes, there are still some remaining questions. Answering such questions would help the development of this family as one of the most structured classes of additive codes as suggested below.

In general, twisted codes form only a strict subclass of additive cyclic codes. Perhaps the first interesting problem is to modify the construction of twisted codes in order to produce all additive cyclic codes in a similar fashion. Such approach possibly provides a more detailed connection between additive cyclic codes and linear cyclic codes. This could help to compute the dimension and bound the minimum distance of additive cyclic codes more easily. An idea for this generalization is to apply different projection maps ϕ_γ to $\theta'(D_Z(A))$ in the composition (3.4.14) for different cyclotomic cosets.

In Theorem 3.6.3, we gave a minimum distance lower bound for twisted codes using the minimum distance of corresponding linear cyclic code over a larger alphabet. Moreover, in Example 3.6.4, we showed that for certain twisted codes, this lower bound is not tight. Hence one can design twisted codes with a better minimum distance than their corresponding linear cyclic codes. The next natural question is to see under what conditions such minimum distance improvement happens and form infinite classes of such codes.

Let $\emptyset \subsetneq A \subsetneq Z$ be the complete defining set of a twisted code $\mathscr{C}_\gamma(A)$ of length n for some 2-cyclotmic coset Z modulo n. In Example 3.5.2, we showed that different choices of A can result in linear and non-linear $\mathscr{C}_\gamma(A)$ over $\mathbb{F}_4$. Thus an interesting question is to classify all defining sets A such that $\mathscr{C}_\gamma(A)$ is a linear code over $\mathbb{F}_4$.

Recently, a family of Galois closed linear codes was introduced to construct new linear codes with good parameters [47]. The family of twisted codes was also constructed by applying the map ϕ_γ to linear cyclic codes that are Galois closed. Applying the map ϕ_γ to the family of Galois closed codes introduced in [47] could also produce additive codes with good properties. Record-breaking binary quantum codes also could be constructed this way.

The *covering radius* of a code C of length n over $\mathbb{F}_q$ is the smallest integer r such that the Hamming balls of radius r centered at the codewords of C cover $\mathbb{F}_q^n$. A code with minimum distance d and covering radius r such that $r = \lfloor \frac{d-1}{2} \rfloor$ is called *perfect*. Moreover, if the covering radius satisfies $r = \lfloor \frac{d-1}{2} \rfloor + 1$, then the code is called *quasi-perfect* [72, Section

1.5]. A complete classification of the parameters for which perfect codes over Galois fields exist was completed in the early 1970s [99, 100, 107]. However, the classification of the sets of possible parameters for quasi-perfect codes is much more complicated [25], and research on computing the covering radius of a code and constructing quasi-perfect codes is ongoing [8, 40, 92]. In Section 3.8, we presented some families of additive codes over $\mathbb{F}_4$ with minimum distances of four and five. As another line of work, we would like to compute the covering radius of such codes as they can potentially be quasi-perfect additive codes.

Bibliography

[1] C. Aguilar-Melchor, O. Blazy, J.-C. Deneuville, P. Gaborit, and G. Zémor. Efficient encryption from random quasi-cyclic codes. *IEEE Transactions on Information Theory*, 64(5):3927–3943, 2018.

[2] D. Akre, N. Aydin, M. Harrington, and S. Pandey. A generalization of cyclic code equivalence algorithm to constacyclic codes. *Designs, Codes and Cryptography*, pages 1–15, 2022.

[3] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. In *2006 IEEE International Symposium on Information Theory*, pages 1105–1108. IEEE, 2006.

[4] E. F. Assmus, Jr. and H. F. Mattson. Perfect codes and the Mathieu groups. *Arch. Math. (Basel)*, 17:121–135, 1966.

[5] N. Aydin, N. Connolly, and M. Grassl. Some results on the structure of constacyclic codes and new linear codes over $GF(7)$ from quasi-twisted codes. *Adv. Math. Commun.*, 11(1):245–258, 2017.

[6] N. Aydin, J. Lambrinos, and O. VandenBerg. On equivalence of cyclic codes, generalization of a quasi-twisted search algorithm, and new linear codes. *Des. Codes Cryptogr.*, 87(10):2199–2212, 2019.

[7] N. Aydin and R. O. VandenBerg. A new algorithm for equivalence of cyclic codes and its applications. *Applicable Algebra in Engineering, Communication and Computing*, 2021. https://doi.org/10.1007/s00200-021-00525-4.

[8] T. Baicheva, I. Bouyukliev, S. Dodunekov, and V. Fack. Binary and ternary linear quasi-perfect codes with small dimensions. *IEEE transactions on information theory*, 54(9):4335–4339, 2008.

[9] E. Berlekamp. *Algebraic coding theory.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, revised edition, 2015.

[10] E. Berlekamp, R. McEliece, and H. Van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[11] J. Bierbrauer. The theory of cyclic codes and a generalization to additive codes. *Des. Codes Cryptogr.*, 25(2):189–206, 2002.

[12] J. Bierbrauer. *Introduction to coding theory.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[13] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Combin. Des.*, 8(3):174–188, 2000.

[14] J. Bierbrauer, S. Marcugini, and F. Pambianco. Additive cyclic codes. In W. C. Huffman, J.-L. Kim, and P. Solé, editors, *Concise encyclopedia of coding theory, Chapter 9.* Chapman and Hall/CRC, 2021.

[15] K. Bogart, D. Goldberg, and J. Gordon. An elementary proof of the MacWilliams theorem on equivalence of codes. *Information and Control*, 37(1):19–22, 1978.

[16] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.

[17] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[18] S. Bouyuklieva. Self-dual codes. In W. C. Huffman, J.-L. Kim, and P. Solé, editors, *Concise encyclopedia of coding theory, Chapter 4.* Chapman and Hall/CRC, 2021.

[19] R. A. Brualdi and V. S. Pless. Polyadic codes. *Discrete Appl. Math.*, 25(1-2):3–17, 1989. Combinatorics and complexity (Chicago, IL, 1987).

[20] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.

[21] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Trans. Inform. Theory*, 44(1):367–378, 1998.

[22] T. Chakravarty and P. Koopman. Performance of cyclic redundancy codes for embedded networks. Master's thesis, Carnegie Mellon University, 2001.

[23] Y. Chen and K. K. Parhi. Overlapped message passing for quasi-cyclic low-density parity check codes. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 51(6):1106–1113, 2004.

[24] J. Conway and N. Sloane. Three lectures on exceptional groups. *Sphere Packings, Lattices and Groups*, pages 267–298, 1999.

[25] D. Danev, S. Dodunekov, and D. Radkova. A family of constacyclic ternary quasi-perfect codes with covering radius 3. *Designs, Codes and Cryptography*, 59:111–118, 2011.

[26] R. Dastbasteh and P. Lisoněk. On the equivalence of linear cyclic and constacyclic codes. *Discrete Mathematics*, 346(9):113489, 2023.

[27] R. Dastbasteh and P. Lisoněk. Constructions of quantum codes. Talk at the Special Session on Algebra and Application to Combinatorics, Coding Theory and Cryptography conducted at the Applications of Computer Algebra, Montréal, Canada, 2019.

[28] R. Dastbasteh and P. Lisoněk. Additive twisted codes and new infinite families of binary quantum codes. Talk at the Special Session on Theory and Applications of Coding Theory conducted at the Mathematical Congress of the Americas, Buenos Aires, Argentina, 2021 (online).

[29] R. Dastbasteh and P. Lisoněk. A new family of quantum codes from duadic codes. Talk at the Twelfth International Workshop on Coding and Cryptography, Rostock, Germany, 2022.

[30] R. Dastbasteh and P. Lisoněk. New quantum codes from self-dual codes over $\mathbb{F}_4$ (accepted by Designs, Codes and Cryptography, subject to minor revisions). *arXiv preprint arXiv:2211.00891*, 2022.

[31] R. Dastbasteh and P. Lisoněk. On the equivalence of linear cyclic and constacyclic codes and applications in quantum codes. Talk at the AMS Special Session on Advances in Coding Theory, II conducted at the Joint Mathematics Meetings, Seattle, USA, 2022.

[32] P. Delsarte. On subfield subcodes of modified Reed-Solomon codes. *IEEE Trans. Inform. Theory*, IT-21(5):575–576, 1975.

[33] C. Ding. Cyclic codes over finite fields. In W. C. Huffman, J.-L. Kim, and P. Solé, editors, *Concise encyclopedia of coding theory, Chapter 2*. Chapman and Hall/CRC, 2021.

[34] E. Dobson. Monomial isomorphisms of cyclic codes. *Des. Codes Cryptogr.*, 76(2):257–267, 2015.

[35] Y. Edel. Quantum twisted codes (revised version) `https://www.mathi.uni-heidelberg.de/~yves/Papers/QTBCH.html`, 2022.

[36] Y. Edel and J. Bierbrauer. Twisted BCH-codes. *J. Combin. Des.*, 5(5):377–389, 1997.

[37] M. F. Ezerman, S. Ling, B. Özkaya, and P. Solé. Good stabilizer codes from quasi-cyclic codes over $\mathbb{F}_4$ and $\mathbb{F}_9$. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2898–2902. IEEE, 2019.

[38] P. Gaborit, C.-S. Nedeloaia, and A. Wassermann. On the weight enumerators of duadic and quadratic residue codes. *IEEE Trans. Inform. Theory*, 51(1):402–407, 2005.

[39] M. Geiselhart, M. Ebada, A. Elkelesh, J. Clausius, and S. ten Brink. Automorphism ensemble decoding of quasi-cyclic LDPC codes by breaking graph symmetries. *IEEE Communications Letters*, 26(8):1705–1709, 2022.

[40] M. Giulietti and F. Pasticci. Quasi-perfect linear codes with minimum distance 4. *IEEE transactions on information theory*, 53(5):1928–1935, 2007.

[41] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A (3)*, 54(3):1862–1868, 1996.

[42] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Physical Review A*, 54(3):1862, 1996.

[43] M. Grassl. Code Tables: Bounds on the parameters of various types of codes. `http://www.codetables.de/`.

[44] M. Grassl. Algebraic quantum codes: linking quantum mechanics and discrete mathematics. *Int. J. Comput. Math. Comput. Syst. Theory*, 6(4):243–259, 2021.

[45] M. Grassl, T. Beth, and M. Rötteler. On optimal quantum codes. *International Journal of Quantum Information*, 2(01):55–64, 2004.

[46] K. Guenda. Quantum duadic and affine-invariant codes. *International Journal of Quantum Information*, 7(01):373–384, 2009.

[47] C. Güneri, F. Özbudak, and S. Sayıcı. On subfield subcodes obtained from restricted evaluation codes. *In: WCC 2022: The Twelfth International Workshop on Coding and Cryptography, Rostock (2022)*, 2022.

[48] C. Güneri, F. Özdemir, and P. Solé. On the additive cyclic structure of quasi-cyclic codes. *Discrete Mathematics*, 341(10):2735–2741, 2018.

[49] K. K. Gunnam, G. S. Choi, W. Wang, E. Kim, and M. B. Yeary. Decoding of quasi-cyclic LDPC codes using an on-the-fly computation. In *2006 Fortieth Asilomar Conference on Signals, Systems and Computers*, pages 1192–1199. IEEE, 2006.

[50] R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 29:147–160, 1950.

[51] C. R. P. Hartmann and K. K. Tzeng. Generalizations of the BCH bound. *Information and Control*, 20:489–498, 1972.

[52] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres*, 2:147–156, 1959.

[53] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11(3):451–490, 2005.

[54] W. C. Huffman, V. Job, and V. Pless. Multipliers and generalized multipliers of cyclic objects and cyclic codes. *J. Combin. Theory Ser. A*, 62(2):183–215, 1993.

[55] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes.* Cambridge University Press, Cambridge, 2003.

[56] D. T. Jones. An improved 64-bit cyclic redundancy check for protein sequences. *University College London*, 2009.

[57] A. Joundan, S. Nouh, and A. Namir. New efficient techniques to catch lowest weights in large quadratic residue codes. In *Proc. of the 5th International Conference on Advances in Computing, Electronics and Communication*, 2017.

[58] I. A. Joundan, S. Nouh, M. Azouazi, and A. Namir. A new efficient way based on special stabilizer multiplier permutations to attack the hardness of the minimum weight search problem for large BCH codes. *International Journal of Electrical and Computer Engineering*, 9(2):1232, 2019.

[59] X. Kai, S. Zhu, and P. Li. Constacyclic codes and some new quantum MDS codes. *IEEE Trans. Inform. Theory*, 60(4):2080–2086, 2014.

[60] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inform. Theory*, 52(11):4892–4914, 2006.

[61] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Physical Review A*, 55(2):900, 1997.

[62] A. Krishna and D. V. Sarwate. Pseudocyclic maximum-distance-separable codes. *IEEE Trans. Inform. Theory*, 36(4):880–884, 1990.

[63] P. J. Lee and E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In *Advances in Cryptology—EUROCRYPT'88: Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, May 25–27, 1988 Proceedings 7*, pages 275–280. Springer, 1988.

[64] J. S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes. *IEEE Transactions on Information Theory*, 34(5):1354–1359, 1988.

[65] J. S. Leon, J. M. Masley, and V. Pless. Duadic codes. *IEEE Trans. Inform. Theory*, 30(5):709–714, 1984.

[66] S. Ling and C. Xing. Polyadic codes revisited. *IEEE Trans. Inform. Theory*, 50(1):200–207, 2004.

[67] P. Lisoněk and R. Dastbasteh. Constructions of quantum codes. Talk at the 3rd International Workshop on Boolean Functions and their Applications, Loen, Norway, 2018.

[68] P. Lisoněk and V. Singh. Quantum codes from nearly self-orthogonal quaternary linear codes. *Des. Codes Cryptogr.*, 73(2):417–424, 2014.

[69] S. Liu, J. Li, P. Reviriego, M. Ottavi, and L. Xiao. A double error correction code for 32-bit data words with efficient decoding. *IEEE Transactions on Device and Materials Reliability*, 18(1):125–127, 2018.

[70] Y. Liu, R. Li, L. Lv, and Y. Ma. A class of constacyclic BCH codes and new quantum codes. *Quantum Information Processing*, 16:1–16, 2017.

[71] F. J. MacWilliams. *Combinatorial problems of elementary Abelian groups*. ProQuest LLC, Ann Arbor, MI, 1962. Thesis (Ph.D.)–Radcliffe College.

[72] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[73] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *The Deep Space Network Progress Report*, DSN PR 42-44. NASA:114–116, 1978.

[74] T. K. Moon. *Error correction coding: mathematical methods and algorithms*. John Wiley & Sons, 2020.

[75] D. E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the IRE Professional Group on Electronic Computers*, (3):6–12, 1954.

[76] H.-V. Niemeier. Definite quadratische Formen der Dimension 24 und Diskriminante 1. *J. Number Theory*, 5:142–178, 1973.

[77] P. P. Pálfy. Isomorphism problem for relational structures with a cyclic automorphism. *European J. Combin.*, 8(1):35–43, 1987.

[78] A. Perez. Byte-wise CRC calculations. *IEEE Micro*, 3(03):40–50, 1983.

[79] V. Pless. Q-codes. *Journal of Combinatorial Theory, Series A*, 43(2):258–276, 1986.

[80] V. Pless. Duadic codes and generalizations. In *Eurocode '92 (Udine, 1992)*, volume 339 of *CISM Courses and Lect.*, pages 3–15. Springer, Vienna, 1993.

[81] V. Pless, J. M. Masley, and J. S. Leon. On weights in duadic codes. *J. Combin. Theory Ser. A*, 44(1):6–21, 1987.

[82] V. Pless and J. J. Rushanan. Triadic codes. *Linear Algebra Appl.*, 98:415–433, 1988.

[83] V. Pless and N. J. A. Sloane. On the classification and enumeration of self-dual codes. *J. Combinatorial Theory Ser. A*, 18:313–335, 1975.

[84] E. Prange. *Cyclic error-correcting codes in two symbols.* Air Force Cambridge Research Center, 1957.

[85] D. Radkova and A. van Zanten. Bounds for the minimum distance in constacyclic codes. In *Proceedings Eleventh International Workshop on Algebraic and Combinatorial Coding Theory*, pages 236–242, 2008.

[86] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45(6):1827–1832, 1999.

[87] E. M. Rains and N. J. A. Sloane. Self-dual codes. In V. Pless, R. A. Brualdi, and W. C. Huffman, editors, *Handbook of coding theory*, pages 177–294. North-Holland, Amsterdam, 1998.

[88] T. V. Ramabadran and S. S. Gaitonde. A tutorial on CRC computations. *IEEE micro*, 8(4):62–75, 1988.

[89] C. Roos. A new lower bound for the minimum distance of a cyclic code. *IEEE Trans. Inform. Theory*, 29(3):330–332, 1983.

[90] J. J. Rushanan. *Topics in integral matrices and abelian group codes.* ProQuest LLC, Ann Arbor, MI, 1986. Thesis (Ph.D.)–California Institute of Technology.

[91] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

[92] M. Shi, T. Helleseth, F. Özbudak, and P. Solé. Covering radius of Melas codes. *IEEE Transactions on Information Theory*, 68(7):4354–4364, 2022.

[93] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994)*, pages 124–134. IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[94] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493, 1995.

[95] M. H. M. Smid. Duadic codes. *IEEE Trans. Inform. Theory*, 33(3):432–433, 1987.

[96] J. Stern. A method for finding codewords of small weight. *Coding theory and applications*, 388:106–113, 1989.

[97] W.-K. Su, P.-Y. Shih, T.-C. Lin, and T.-K. Truong. On the minimum weights of binary extended quadratic residue codes. In *2009 11th International Conference on Advanced Communication Technology*, volume 3, pages 1912–1913. IEEE, 2009.

[98] Z. Sun, S. Zhu, and L. Wang. A class of constacyclic BCH codes. *Cryptography and Communications*, 12(2):265–284, 2020.

[99] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM J. Appl. Math.*, 24:88–96, 1973.

[100] A. Tietäväinen. A short proof for the nonexistence of unknown perfect codes over GF(q), $q > 2$. *Ann. Acad. Sci. Fenn. Ser. A. I.*, (580):6, 1974.

[101] T.-K. Truong, C.-D. Lee, Y. Chang, and W.-K. Su. A new scheme to determine the weight distributions of binary extended quadratic residue codes. *IEEE Transactions on Communications*, 57(5):1221–1224, 2009.

[102] J. H. van Lint and R. M. Wilson. On the minimum distance of cyclic codes. *IEEE Trans. Inform. Theory*, 32(1):23–40, 1986.

[103] S. A. Vanstone and P. C. Van Oorschot. *An introduction to error correcting codes with applications*, volume 71. Springer Science & Business Media, 2013.

[104] A. Vardy. The intractability of computing the minimum distance of a code. *IEEE Trans. Inform. Theory*, 43(6):1757–1766, 1997.

[105] Y. Yang and W. Cai. On self-dual constacyclic codes over finite fields. *Des. Codes Cryptogr.*, 74(2):355–364, 2015.

[106] A. Zeh and S. Ling. Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance. In *2014 IEEE International Symposium on Information Theory*, pages 2584–2588. IEEE, 2014.

[107] V. Zinoviev and V. Leontiev. The nonexistence of perfect codes over Galois fields. *Probl. Control and Inform. Theory*, 2(2):123–132, 1973.

Appendix A

Quantum stabilizer codes

A.1 Stabilizer formalism of binary quantum codes

This section describes quantum stabilizer codes from a quantum mechanical point of view. In a classical computer, the *bit*, which is the contraction of "binary digit", is the basic unit of information. The bit represents a state using the binary values. A general state of a classical computer is represented using a binary vector. Similarly, the basic unit of quantum information is called *qubit*, which is the contraction of "quantum bit". In quantum mechanics, it is customary to use *Dirac notation*, sometimes called bra-ket notation, to present row and column vectors. A *bra* is denoted by $\langle v|$, where v is a row vector. Similarly, a *ket* is denoted by $|u\rangle$, where u is a column vector. A complex Hilbert space $\mathcal{H}$ is associated to every quantum mechanical system. In this section, $\mathcal{H} = \mathbb{C}$ is the complex Hilbert space with the inner product

$$\langle u, v\rangle = \sum_{i=1}^{n} \overline{u_i} v_i,$$

where $v, u \in \mathcal{H}^n$ and $\overline{u_i}$ is the complex conjugate. Let $\{|0\rangle, |1\rangle\}$ be a basis for $\mathcal{H}^2$ (they are usually selected as $|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$). An arbitrary state of a closed 1-qubit quantum system is defined by

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $\alpha, \beta \in \mathcal{H}$ and $|\alpha|^2 + |\beta|^2 = 1$. The main difference between a qubit and a classical bit is that a qubit can be in a *superposition* of the states. This happens when α and β are both non-zero. Hence there are infinitely many different quantum states for a qubit, whereas in the classic case, the states of a single bit can only be zero or one. In general, the state of a closed n-qubit quantum system can be described as

$$|\phi\rangle = \sum_{i \in \mathbb{F}_2^n} \alpha_i\,|i\rangle\,,$$

where $\alpha_i \in \mathcal{H}$, $\sum\limits_{i \in \mathbb{F}_2^n} |\alpha_i|^2 = 1$ and the set of vectors $\{|i\rangle : \ i \in \mathbb{F}_2^n\}$ forms a basis for $\mathcal{H}^{2^n}$.

Let A be an $m \times n$ and B be a $p \times q$ matrix. We define the tensor product of A and B to be

$$A \otimes B = \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & \cdots & A_{2n}B \\ \vdots & \vdots & \cdots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{bmatrix}.$$

Let $|\phi\rangle$ and $|\psi\rangle$ be quantum states of an n-qubit and an m-qubit system, respectively. The *composition* of these systems is an nm-qubit system with the state $|\phi\rangle \otimes |\psi\rangle$. Any nm-qubit system can be represented as a sum of products of n-qubit and an m-qubit systems. For example, a two qubits system can be described as a linear combination of the composite states $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$, $|10\rangle = |1\rangle \otimes |0\rangle$, and $|11\rangle = |1\rangle \otimes |1\rangle$.

Note that if $|\phi_1\rangle$ and $|\phi_2\rangle$ are two states of an n-qubit and an m-qubit systems, respectively, then $|\phi_1\phi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ is a valid state for an nm-qubit system. However, a general state of an nm-qubit system cannot necessarily be described as a tensor product of an n-qubit and an m-qubit system. For instance, the two qubit state $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be decomposed into a tensor product of two one qubit states. A state of a composite system which cannot be decomposed as a tensor product of states of its component systems is called an *entangled* state. The entanglement phenomenon has various applications in quantum cryptography, superdense coding, and models of quantum teleportation.

The matrices defined by

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \text{ and } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

are called the *Pauli* matrices. It is not difficult to show that the Pauli matrices satisfy the following properties.

1. X, Y, and Z are all hermitian (self-adjoint) and unitary.
2. $X^2 = Y^2 = Z^2 = I$.
3. The eigenvalues of Pauli matrices are ±1.
4. $XZ = -iY$ and $X^aZ^b = (-1)^{(a\cdot b)}Z^bX^a$ for each $a, b \in \mathbb{F}_2$.
5. The set $P_1 = \{\pm I, \pm X, \pm Y, \pm Z, \pm iI, \pm iX, \pm iY, \pm iZ\}$ is a multiplicative group and is called a *1-dimensional Pauli group.*

Note also that by the first equation in Case (4) above, we can express $Y = iXZ$. Moreover, by the second equation of (4), we can write each operator in a normal form.

Next, we consider the actions of the Pauli matrices X and Z on a 1-qubit state. Let $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ be the quantum state of a 1-qubit system for some values α and $\beta \in \mathcal{H}$. Then $X|a\rangle = \beta|0\rangle + \alpha|1\rangle$ and thus X flips the coefficients of $|0\rangle$ and $|1\rangle$. The Pauli matrix X is usually referred to as the *bit flip* quantum operator on a single qubit state.

Let $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. It is easy to see that $|+\rangle$ and $|-\rangle$ form a basis for $\mathcal{H}^2$. For any state in the form $|b\rangle = \alpha' |+\rangle + \beta' |-\rangle$ where α' and $\beta' \in \mathcal{H}$, we have $Z |b\rangle = \beta' |+\rangle + \alpha' |-\rangle$. Therefore, Z flips the signs, and it is referred to as the *sign flip* quantum operator on a single qubit state. In this setting, when qubit $|\phi\rangle$ is sent and $XZ |\phi\rangle$ or $ZX |\phi\rangle$ is received, then both a bit flip and a sign flip error have occurred.

Recall that an $n \times n$ matrix U over $\mathcal{H}$ is called a *unitary matrix* if

$$U^*U = UU^* = I,$$

where U^* is the conjugate transpose of U. Suppose that the state $|\phi\rangle$ is transmitted over a quantum channel and the state $|\phi'\rangle$ is received. Then there exists a unitary matrix E such that $E|\phi\rangle = |\phi'\rangle$. In this case we say the error E has happened. The matrices I, X, Z, XZ form a basis for all 2×2 matrices over $\mathcal{H}$. Hence an arbitrary one qubit error operator (a 2×2 unitary matrix) can be represented as a linear combination of the mentioned matrices.

Next, we can consider the action of tensor products of the Pauli matrices on more than one qubit. An n-dimensional *generalized Pauli matrix* is represented by

$$X^u Z^v = X^{u_1} Z^{v_1} \otimes X^{u_2} Z^{v_2} \otimes \cdots \otimes X^{u_n} Z^{v_n},$$

where $u = (u_1, u_2, \dots, u_n), v = (v_1, v_2, \dots, v_n) \in \mathbb{F}_2^n$. In particular, the matrix $X^u Z^v$ acts on the i-th qubit as $X^{u_i} Z^{v_i}$ for each $1 \leq i \leq n$. For example, $X^{(1,0,1,0)} Z^{(0,0,1,1)}$ is equivalent to the generalized Pauli operator

$$X \otimes I \otimes XZ \otimes Z.$$

The generalized Pauli operators are the error models, for the error correction and error detection, of most n-qubit systems, and any error operator on an n-qubit system can be expressed as a linear combination of them. We define the *n-dimensional Pauli group* as $P_n = \bigotimes_{i=1}^{n} P_1$.

Now, we connect the length n generalized Pauli matrices and vectors over $\mathbb{F}_4$. For each $c = (c_1, c_2, \dots, c_n) \in \mathbb{F}_4^n$, we can alternatively represent c as $((c_{11}, c_{12}), (c_{21}, c_{22}), \dots, (c_{n1}, c_{n2}))$, where $c_{i1}, c_{i2} \in \mathbb{F}_2$ and

$$c_i = \omega c_{i1} + \omega^2 c_{i2} \tag{A.1.1}$$

for each $1 \leq i \leq n$. Let

$$\overline{P_n} = \{X^u Z^v : u, v \in \mathbb{F}_2^n\}$$

be the set of all n-dimensional generalized Pauli matrices. Then $\overline{P_n}$ consists of all different representatives of the group $P_n/\{\pm I, \pm iI\}$. Therefore, there is a group isomorphism Φ between $\mathbb{F}_4^n$ and $P_n/\{\pm I, \pm iI\}$ defined by

$$\begin{aligned}\Phi(((c_{11}, c_{12}), (c_{21}, c_{22}), \dots, (c_{n1}, c_{n2}))) &= X^{(c_{11}, c_{21}, \dots, c_{n1})} Z^{(c_{12}, c_{22}, \dots, c_{n2})} \\ &= X^{c_{11}} Z^{c_{12}} \otimes X^{c_{21}} Z^{c_{22}} \otimes \cdots \otimes X^{c_{n1}} Z^{c_{n2}}.\end{aligned}$$

For each $X^aZ^b \in \overline{P_n}$, we define

$$\text{wgt}(X^aZ^b) = |\{1 \leq i \leq n : (a_i, b_i) \neq (0,0)\}|. \tag{A.1.2}$$

This definition is consistent with the definition of weight for vectors over $\mathbb{F}_4$. In particular, for each $u \in \mathbb{F}_4^n$, we have $\text{wt}(u) = \text{wgt}(\Phi(u))$.

Let $E_1 = X^uZ^v$ and $E_2 = X^{u'}Z^{v'}$ be two elements of $\overline{P_n}$. Then E_1 and E_2 commute in P_n if and only if

$$E_1E_2 = X^uZ^vX^{u'}Z^{v'} = (-1)^{u'\cdot v}X^uX^{u'}Z^vZ^{v'} \tag{A.1.3}$$

and

$$E_2E_1 = X^{u'}Z^{v'}X^uZ^v = (-1)^{u.v'}X^{u'}X^uZ^{v'}Z^v \tag{A.1.4}$$

are the same. In other words, E_1 and E_2 commute in P_n if and only if $(-1)^{u\cdot v'-v\cdot u'} = 1$. Recall that $\langle , \rangle_s : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is the nondegenerate symplectic $\mathbb{F}_2$-bilinear form defined by

$$\langle\Big((a_{11}, a_{12}), \ldots, (a_{n1}, a_{n2})\Big), \Big((b_{11}, b_{12}), \ldots, (b_{n1}, b_{n2})\Big)\rangle_s = \sum_{i=1}^{n} a_{i1}b_{i2} - a_{i2}b_{i1}. \tag{A.1.5}$$

A straightforward computation shows that

$$(\omega u + \omega^2 v) * (\omega u' + \omega^2 v') = u \cdot v' - v \cdot u' = \langle (u, v), (u', v')\rangle. \tag{A.1.6}$$

This shows the connection between the symplectic inner product and the trace inner product. Both of the inner products $*$ and $\langle , \rangle_s$ are used in the literature for the construction of quantum codes. The definition of quantum codes provided in Theorem 1.7.1 is based on the trace inner product.

The computations of (A.1.3) and (A.1.4) show that E_1 and E_2 commute in P_n if and only if $(\omega u + \omega^2 v)$ and $(\omega u' + \omega^2 v')$ are trace orthogonal. This implies that if C is an additive code over $\mathbb{F}_4$ such that $C^{\perp_t} \subseteq C$, then the set

$$G_{C^{\perp_t}} = \{X^uZ^v : (\omega u + \omega^2 v) \in C^{\perp_t}\}$$

is a commutative subgroup of P_n. Let

$$N(G_{C^{\perp_t}}) = \{X^uZ^v : (\omega u + \omega^2 v) \in C\}.$$

Then, the normalizer of $G_{C^{\perp_t}}$ in P_n is

$$(\pm I)N(G_{C^{\perp_t}}) \cup (\pm iI)N(G_{C^{\perp_t}}).$$

This observation allows us to distinguish the error vectors in $\overline{P_n} \setminus N(G_{C^{\perp_t}})$ from the errors in $N(G_{C^{\perp_t}})$. In particular, for any operator $E_1 = X^uZ^v \notin N(G_{C^{\perp_t}})$ we can find another error operator $E_2 = X^{u'}Z^{v'} \in G_{C^{\perp_t}}$ such that E_1 and E_2 do not commute. The error correction and error detection schemes of quantum stabilizer codes are designed based on this property.

We are now coming to the definition of binary quantum stabilizer codes. We give the definition in two steps. First, we recall the sufficient condition of mathematical formalism of quantum stabilizer codes given in Theorem 1.7.1. Next, we explain how the states of a quantum stabilizer code are constructed. Recall that an $[\![n,k,d]\!]$ quantum code consists of 2^k number of n-qubit states, and it is capable of correcting each error $E \in \overline{P_n}$ if $\mathrm{wgt}(E) \leq \lfloor \frac{d-1}{2} \rfloor$. In Theorem 1.7.1, we showed that if $C \subseteq \mathbb{F}_4^n$ is an $(n, 2^{n+k}, d)$ additive code such that $C^{\perp_t} \subseteq C$, then an $[\![n,k,d']\!]$ binary quantum stabilizer code can be constructed, where d' is the minimum weight in $C \setminus C^{\perp_t}$ if $C \subsetneq C^{\perp_t}$, and $d' = d$ otherwise. The following theorem describes how the states of a quantum code can be constructed.

Theorem A.1.1 *Let $C \subseteq \mathbb{F}_4^n$ be an $(n, 2^{n+k}, d)$ additive code such that $C^{\perp_t} \subseteq C$. Then the common eigenspace with eigenvalue 1 of matrices in $G_{C^{\perp_t}}$ is an $[\![n,k,d']\!]$ binary quantum code, where d' is the minimum weight in $C \setminus C^{\perp_t}$ if $k > 0$ and $d' = d$ if $k = 0$.*

Proof. The proof follows from the discussion in Section 3 of [44]. □

Therefore each quantum code consists of precisely the states *stabilized* by each matrix from $G_{C^{\perp_t}}$. This gives the name stabilizer codes to this family of quantum codes. The next example constructs the smallest length binary quantum code that is capable of correcting any arbitrary error of weight one.

Example A.1.2 Let $n = 5$ and C be the trace dual of the additive code generated by

$$M = \begin{bmatrix} 1 & 0 & 1 & \omega & \omega \\ \omega & 0 & \omega & \omega^2 & \omega^2 \\ 0 & 1 & \omega & \omega & 1 \\ 0 & \omega & \omega^2 & \omega^2 & \omega \end{bmatrix}.$$

Recall that in Example 1.7.2, we showed that C is in correspondence to a $[\![5,1,3]\!]$ binary quantum code. Next, we use Theorem A.1.1 to construct this quantum code. Applying the map Φ to the rows of M gives the following error vectors in $\overline{P_5}$ which form a basis for $G_{C^{\perp_t}}$:

$$E_1 = XZ \otimes I \otimes XZ \otimes X \otimes X$$

$$E_2 = X \otimes I \otimes X \otimes Z \otimes Z$$

$$E_3 = I \otimes XZ \otimes X \otimes X \otimes XZ$$

$$E_4 = I \otimes X \otimes Z \otimes Z \otimes X.$$

The common eigenvectors with eigenvalue 1 of the errors E_1 to E_4 are

$$|c_1\rangle = \frac{1}{4}(|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle)$$

and

$$|c_2\rangle = \frac{1}{4}(|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle).$$

These states are stabilized by the matrix M' consisting of E_1 to E_4 as it rows. In other words, $M' \left|c_1\right\rangle = \left|c_1\right\rangle$ and $M' \left|c_2\right\rangle = \left|c_2\right\rangle$. Hence the corresponding quantum code is $Q = \{\left|c_1\right\rangle, \left|c_2\right\rangle\}$, which is capable of correcting an arbitrary error on one of the qubits.

Appendix B

Magma code for Chapter 2

The following Magma code produces a linear cyclic code over $\mathbb{F}_4$ with given odd length and coset leaders. As an example, we use the result of Corollary 2.3.7 and produce the best-known binary quantum code with parameters $[[38, 0, 12]]$.

```
> F4<z>:=GF(4);
> p<x>:=PolynomialRing(F4);
> n:=37;
> F<v>:=SplittingField(x^n-1);
> a:=PrimitiveElement(F);
> b:=(#F-1)/n;
> Z:=Integers();
> an:=a^(Z!b);
> Omega:={i: i in [0..n-1]};
> conjclass:=function(pa)
function> return { ((an^pa))^(4^i) : i in [ 0 .. n-1 ] };
function> end function;
> conjcla:=function(pa)
function> return { pa *(4^i) mod n : i in [ 0 .. n-1 ] };
function> end function;
> classes1:= SetToSequence( { conjcla(j) : j in Omega } );
> printf "conjugacy classes = %o\n",classes1;
conjugacy classes = [
{ 0 },
{ 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36 },
{ 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35 }
]
> printf "number of classes = %o\n",#classes1;
number of classes = 3
> printf "class sizes = %o\n",[ #c : c in classes1];
class sizes = [ 1, 18, 18 ]
> orderconjcla:=function(pa)
function> return [ pa *(4^i) mod n : i in [ 0 .. n-1 ] ];
function> end function;
> /////////////////// Cyclic Code Over F4 of lengh n./////////////
> R<XX>:=PolynomialRing(F,1);
> code:= function(class)
function> cs:=SetToSequence(class);
function> I:=&*[&*[XX-((SetToSequence(conjclass(cs[i]))[j])): j in
[1..#SetToSequence(conjclass(cs[i]))]] : i in [1..#class] ];
function> II:=p!I;
function> Code:=CyclicCode(n, II);
function> return(Code);
function> end function;
> Leaders:={1};
> C:=code(Leaders);
> printf "code parameters are %o\n",[Length(C),Dimension(C),
MinimumDistance(C)];
code parameters are [ 37, 19, 11 ]
```

Now applying the result of Corollary 2.3.7 to the code C above results a binary quantum code with parameters $[[38, 0, 12]]$. This is the currently best-known 0-dimensional binary quantum code of length 38.

For some of the codes in Table 2.1, the minimum distance upper bounds were computed using certain attacks on the McEliece cryptosystem [21, 63, 64, 73, 96]. This is based on the following observation. Let C be a linear code and $r = c + e$ where $c \in C$ and e is the error pattern. Assuming that $\mathrm{wt}(e) < \frac{d(C)}{2}$ implies that e is the lowest weight codeword in the linear code spanned by $C \cup \{r\}$. This observation connects decoding and computing the minimum weight. Several probabilistic algorithms for finding a fixed-weight vector in a coset of a general (random) linear code have been implemented in Magma. An example of one of such computation is provided below. In the example, the code C has length $n = 157$, coset leaders $\{1, 3, 9\}$, and it is constructed using the above Magma code. Moreover, we decompose C as $C = C_1 \oplus \mathrm{Span}\{r\}$, where r is a random vector in C and C_1 is constructed using `CodeComplement` function.

```
> F4<z>:=GF(4);
> p<x>:=PolynomialRing(F4);
> n:=157;
      ⋮
> Leaders:={1,3,9};
> C:=code(Leaders);
> r:=Random(C);
> E:=LinearCode<F4,n|r>;
> C1:=CodeComplement(C,E);
> w:=McEliecesAttack(C1,r,35);
> Weight(w);
35
> w in C;
true
```

The above computation shows that $d(C) \leq 35$. This computation was done in 4.67 seconds, however, the minimum distance upper bound of 35 was obtained, using `MinimumDistance` function, after 466.32 seconds.

Appendix C

Magma code for Chapter 3

The following is Magma code for Example 3.8.6 Part (i).

```
> F2:=GF(2);
> F4:=GF(4);
> w:=PrimitiveElement(F4);
> n:=73;
> r:=1;
> while (2^r mod n) ne 1 do r:=r+1; end while;
> printf "r is %o\n",r;
r is 9
> Allkappa:=[i: i in [2..r]| r mod i eq 0];
> printf "all possible kappa values are = %o\n",Allkappa;
all possible kappa values are = [ 3, 9 ]
> kappa:=Allkappa[1];
> printf "kappa is %o\n",kappa;
kappa is 3
> A:={1,-1,8,-8,9,-9};
> Acom:={ (a*2^(kappa*j)) mod n : j in [ 0 .. r-1 ], a in A };
> printf "the complete defining set is %o\n",Acom;
the complete defining set is { 1, 8, 9, 64, 65, 72 }
> F:=GF(2,r);
> eta:=PrimitiveElement(F);
> u:=eta^( Integers()!((2^r-1)/n) );
> gamma:=eta^( Integers()!((2^r-1)/(2^kappa -1)) );
> tF:=Generator(F);
> assert Order(u) eq n;
> Gbin:=Matrix(F2, r*(#A), 2*n, [
> &cat[ [Trace(tF^i*u^(m*j)) ,Trace(gamma*tF^i*u^(m*j)) ]
>        : j in [ 1 .. n ] ]
> : i in [ 0 .. r-1 ] , m in A ]);
> Cbin:=LinearCode(Gbin);
> dim:=Dimension(Cbin);
> GM:=GeneratorMatrix(Cbin);
> G:=Matrix(F4,dim,n,[]);
> for i:=1 to dim do
for> for j:=1 to n do
for|for> G[i,j]:=GM[i,2*j-1]*w+GM[i,2*j]*w^2;
for|for> end for;
for> end for;
> C := SymplecticDual(AdditiveCode(G));
> IsSymplecticSelfOrthogonal(AdditiveCode(G));
true
> d:=MinimumWeight(C);
> printf "quantum parameters = %o\n",
printf> [[Length(C),2*Dimension(C)-Length(C),d]];
quantum parameters = [[ 73, 55, 5 ]]
```

Appendix D

Magma code for Chapter 4

The following is the Magma code for Example 4.5.9.

```
> F4<z>:=GF(4);
> p<x>:=PolynomialRing(F4);
> n:=111;
> L:=Factorization(x^n-z);
> F<v>:=SplittingField(x^n-z);
> a:=PrimitiveElement(F);
> b:=(#F-1)/(3*n);
> Z:=Integers();
> an:=a^(Z! b);
> Omega:={(3*i+1) mod (3*n): i in [0..n-1]};
> conjclass:=function(pa)
function> return { ((an^pa))^(4^i) : i in [ 0 .. n-1 ] };
function> end function;
> R<XX>:=PolynomialRing(F,1);
> code:= function(class)
function> cs:=SetToSequence(class);
function> I:=&*[&*[XX-((SetToSequence(conjclass(cs[i]))[j])): j in
[1..#SetToSequence(conjclass(cs[i]))]] : i in [1..#class] ];
function> II:=p!I;
function> Code:=ConstaCyclicCode(n, II,z);
function> return(Code);
function> end function;
> Leaders:={19,37};
> C:=code(Leaders);
> K:=Dimension(C);
> [n,Dimension(C)];
> e:=n-K-Dimension(C meet LinearCode(SymplecticDual(C)));
> printf "e=%o\n",e;
e=3
> d:=Minimum({MinimumDistance(C+LinearCode(SymplecticDual(C)))+1,
MinimumDistance(C)});
> printf "Quantum parameters are %o\n",[[n+e,2*K-n+e,d]];
Quantum parameters are [[ 114, 72, 9 ]]
```