QUANTUM ERROR CONTROL CODES

A Dissertation

by

SALAH ABDELHAMID AWAD ALY AHMED

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2008

Major Subject: Computer Science

QUANTUM ERROR CONTROL CODES

A Dissertation

by

SALAH ABDELHAMID AWAD ALY AHMED

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

Chair of Committee,	Andreas Klappenecker
Committee Members,	Mahmoud M. El-Halwagi
	Anxiao (Andrew) Jiang
	Rabi N. Mahapatra
Head of Department,	Valerie Taylor

May 2008

Major Subject: Computer Science

ABSTRACT

Quantum Error Control Codes. (May 2008)

Salah Abdelhamid Awad Aly Ahmed,

B.Sc., Mansoura University;

M.Sc., Cairo University;

M.Sc., DePaul University

Chair of Advisory Committee: Dr. Andreas Klappenecker

It is conjectured that quantum computers are able to solve certain problems more quickly than any deterministic or probabilistic computer. For instance, Shor's algorithm is able to factor large integers in polynomial time on a quantum computer. A quantum computer exploits the rules of quantum mechanics to speed up computations. However, it is a formidable task to build a quantum computer, since the quantum mechanical systems storing the information unavoidably interact with their environment. Therefore, one has to mitigate the resulting noise and decoherence effects to avoid computational errors.

In this dissertation, I study various aspects of quantum error control codes – the key component of fault-tolerant quantum information processing. I present the fundamental theory and necessary background of quantum codes and construct many families of quantum block and convolutional codes over finite fields, in addition to families of subsystem codes. This dissertation is organized into three parts:

Quantum Block Codes. After introducing the theory of quantum block codes, I establish conditions when BCH codes are self-orthogonal (or dual-containing) with respect to Euclidean and Hermitian inner products. In particular, I derive two families of nonbinary quantum BCH codes using the stabilizer formalism. I

study duadic codes and establish the existence of families of degenerate quantum codes, as well as families of quantum codes derived from projective geometries.

Subsystem Codes. Subsystem codes form a new class of quantum codes in which the underlying classical codes do not need to be self-orthogonal. I give an introduction to subsystem codes and present several methods for subsystem code constructions. I derive families of subsystem codes from classical BCH and RS codes and establish a family of optimal MDS subsystem codes. I establish propagation rules of subsystem codes and construct tables of upper and lower bounds on subsystem code parameters.

Quantum Convolutional Codes. Quantum convolutional codes are particularly well-suited for communication applications. I develop the theory of quantum convolutional codes and give families of quantum convolutional codes based on RS codes. Furthermore, I establish a bound on the code parameters of quantum convolutional codes – the generalized Singleton bound. I develop a general framework for deriving convolutional codes from block codes and use it to derive families of non-catastrophic quantum convolutional codes from BCH codes.

The dissertation concludes with a discussion of some open problems.

.

Dedicated to my family and teachers.

Dedicated to every child, who was

born of ignorant or poor parents.

Ph.D. defended on

October 09, 2007

Ramadan 27, 1428.

ACKNOWLEDGMENTS

I believe that *"Knowledge comes by learning, whoever seeks goodness will be given it."* For me, learning is a journey, not a destination. It is a lifetime process until death. This dissertation would not be a reality without the kind people whom I met during my graduate studies.

I thank my dissertation advisor Dr. Andreas Klappenecker for his support, guidance, and patience. He kindly introduced me to this pioneering research. I learned greatly during the short valuable time he gave me. Andreas taught me how to write high quality research papers. Throughout countless emails, I cannot remember how many times I thought my code constructions and paper drafts were good enough, and he kindly challenged me to make them correct and outstanding. Andreas was a reason to channel my life towards becoming a researcher and an independent thinker.

I thank all my committee members: Dr. M. Suhail Zubairy, Dr. Mahmoud El-Halwagi, Dr. Rabi Mahapatra, and Dr. Andrew Jiang. They were all supportive and kind. A special gratefulness goes to my mentor Dr. El-Halwagi for his encouragement, whenever I could not find anyone to talk to at TAMU. I would like to thank Henry Pfister, Amr Sabry, Hani Abu-Salem, Mary Knight, and many others. I thank the thesis office staff members at TAMU for their assistance and patience.

I thank Ahmad El-Guindy, Pradeep K. Sarvepalli, Zhenning Kong, Salim El-Rouayheb, Jason Lee, Sherif Hassan, and Robert Jacobson. I thank Martin Roetteler and Marcus Grassl for their collaboration. I would like to thank Emina Soljanin and the Mathematical Science Research Group at Bell Labs & Alcatel-Lucent. I had a great opportunity to collaborate with her and Zhenning throughout an internship research program.

In a weighty remarkable document like this where the precision of every word counts with caution; remaining silent is too difficult. During the last five years of my life, I was undoubtedly isolated from people and life. Words cannot describe how I felt. I would like to thank my parents and extended family members for their patience while I was away from them for many unseen years. I hope my degree instills them with pride and proves that their eldest son can get this degree from an outstanding institution, even though he struggled and he never gave up. I also wish this dissertation will ignite a light for my nephews and all youth in my home city to encourage them to pursue graduate studies and to seek true knowledge. Finally, from infancy until now, I have always been blessed by the prayers of my relatives and elders; I can now be sure that my work is not based on my cleverness or intelligence. Through it all, God has been present at all times. He almightily has been the most merciful and most compassionate to hear my woe and sadness in many consecutive nights and days spent lonely in Texas. I owe all praise, gratitude, and everything to Him.

Salah A. Aly

December 1, 2007.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Quantum computing is a relatively new interdisciplinary field that has recently attracted many researchers from physics, mathematics, and computer science. The main idea of quantum computing is to utilize the laws of quantum physics to perform fast computations. Quantum information processing can be beneficial in numerous applications, such as secure key exchange or quick search. Arguably, one of the most attractive features is that quantum algorithms are conjectured to solve certain computational problems exponentially faster than any classical algorithm. For instance, Shor's quantum algorithm can factor integers faster than any known classical algorithm.

Quantum information is represented by the states of quantum mechanical systems. Since the information-carrying quantum systems will inevitably interact with their environment, one has to deal with decoherence effects that tend to destroy the stored information. Hence, it is infeasible to perform quantum computations without introducing techniques to remedy this dilemma. One method is to apply fault-tolerant operations that make the computations permissible under a certain threshold value. These fault-tolerant techniques employ quantum error control codes to protect quantum information.

The main contribution of this dissertation is the development of novel techniques for quantum error control, including the construction of numerous quantum error control codes to guard quantum information.

This dissertation follows the style of *IEEE Transactions on Information Theory.*

A. Background

The state space of a discrete quantum mechanical system is given by a finite-dimensional Hilbert space, namely by a finite-dimensional complex vector space that is equipped with the standard Hermitian inner product. The states of the quantum system are assumed to be vectors of unit length in the induced norm. Any quantum mechanical operation other than a measurement is given by a unitary linear operation.

For quantum information processing, one chooses a fixed orthonormal basis of the state space of the quantum mechanical system, called the computational basis. The basis vectors represent classical information that is processed by the quantum computer. To fix ideas, consider a quantum system with two-dimensional state space $\mathbb{C}^2$. The basis vectors

$$v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad v_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

can be used to represent the classical bits 0 and 1. As the indices of the basis vectors can be difficult to read, it is customary in quantum information processing to use Dirac's ket notation for the basis vectors; namely, the vector v_0 is denoted by $|0\rangle$ and the vector v_1 is denoted by $|1\rangle$. Therefore, any possible state of such a two-dimensional quantum system is given by a linear combination of the form

$$a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad \text{where } a, b \in \mathbb{C} \text{ and } |a|^2 + |b|^2 = 1,$$

as any vector of unit length is a possible state. One refers to the state vector of a two-dimensional quantum system as a quantum bit or qubit.

The superposition or linear combination of the basis vectors $|0\rangle$ and $|1\rangle$ of a quantum bit is one marked difference between classical and quantum information processing. One can measure a quantum bit in the computational basis. Such a measurement of a quantum bit in the state $a|0\rangle + b|1\rangle$ leaves the quantum bit with a probability of $|a|^2$ in state $|0\rangle$ and with probability $|b|^2$ in state $|1\rangle$. Furthermore, the outcome of this probabilistic operation is recorded as a measurement result.

In quantum information processing, the operations manipulating quantum bits follow the rules of quantum mechanics, that is, an operation that is not a measurement must be realized by a unitary operator. For example, a quantum bit can be flipped by a quantum NOT gate X that transfers the qubits $|0\rangle$ and $|1\rangle$ to $|1\rangle$ and $|0\rangle$, respectively. Thus, this operation acts on a general quantum state as follows.

$$X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle.$$

With respect to the computational basis, the quantum NOT gate X is represented by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Other popular operations include the phase flip Z, the combined bit and phase-flip Y, and the Hadamard gate H, which are represented with respect to the computational basis by the matrices

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The state space of a joint quantum system is described by the tensor product of the state spaces of its parts. Consequently, a quantum register of length n, which is by definition a combination of n qubits, can be represented by the normalized complex linear combination of the 2^n mutually orthogonal basis states in $\mathbb{C}^{2^n}$, namely as a linear combination of the vectors

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle = |\psi_1\psi_2...\psi_n\rangle \text{ where } |\psi_i\rangle \in \{|0\rangle, |1\rangle\}.$$

Operations acting on two (or more) quantum bits include the controlled not operation CNOT, which realizes the map

$$|00\rangle \mapsto |00\rangle\,, |01\rangle \mapsto |01\rangle\,, |10\rangle \mapsto |11\rangle\,, |11\rangle \mapsto |10\rangle\,.$$

In the computational basis, the CNOT operation is described by the matrix

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

B. Quantum Codes

Quantum error control codes like their classical counterparts are means to protect quantum information against noise and decoherence. Quantum codes can be classified into additive or nonadditive codes. If the code is defined based on an abelian subgroup (stabilizer), then it is called an additive (stabilizer) code. The structure and construction of additive codes are well-known. Additive codes are also defined over a vector space, therefore addition (or subtraction) of two codewords is also a valid codeword in the codespace [30].

Shor's demonstrated the first quantum error correcting code [137]. The code encodes one qubit into nine qubits, and is able to correct for one error and detect two errors. Shortly Gottesman [58], Steane [144], and Calderbank, Rains, Shor, Sloane [30] developed the stabilizer codes and the problem transferred to finding classical additive codes over the finite fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ that are self-orthogonal or dual-containing with respect to the Euclidean or Hermitian inner products, respectively. Since then, many families of quantum error-correcting codes have been constructed, also, bounds on the minimum distance and code parameters of quantum codes have been driven. In [30], a table of upper bounds on the minimum distance of binary quantum codes has been given. Moreover, propagation rules to drive new quantum codes from existing quantum codes have been shown.

Nonbinary quantum codes, inspired by their classical counterparts, might be useful for some applications. For example, in quantum concatenated codes, the underline finite field would be $\mathbb{F}_{2^m}$, which is useful for decoding operations [21]. In this dissertation I derive both binary and nonbinary quantum block and convolutional codes in addition to subsystem codes. The foundation materials that will be used in the next chapters are presented in Chapters I, II, and III.

In contrast, the nonadditive codes do not have uniform structure and are not equivalent to any nontrivial additive codes. Knill showed in [91] that nonadditive codes can give better performance. As far as I know, the literature lacks a comparative analytical study among these two classifications of codes. Roychowdhury and Vatan [130] established sufficient conditions on the existence of nonadditive codes, introduced strongly nonadditive codes, and proved Gilbert-Varshimov bounds for these codes. Furthermore, they also showed that the nonadditive codes that correct t errors satisfy asymptotically rate $R \geq 1 - 2H_2(2t/n)$. Arvind el al. developed the theory of non-stabilizer quantum codes from Abelian subgroup of the error group [14].

There is also a different approach, to design quantum codes, that is known as entangled-assisted quantum codes. Designing quantum codes by entanglement property assumes a shared entangled qubits between two parties (sender and receiver). Some progress in this theory and constructing quantum codes using entanglement are shown in [29, 74].

C. Problem Statement

In this section, I will state some of the open research problems that I have been investigating. My goal is to construct good families of quantum codes to protect quantum information against noise and decoherence. I will construct quantum block and convolutional codes in addition to subsystem codes.

Quantum Block Codes. A well-known method of constructing quantum error-correcting codes is by using the stabilizer formalism. Let S be a stabilizer abelian subgroup of an error group G, and $C(S)$ be a subgroup in G that contains all elements which commute with every element in S, ((i.e. $S \subseteq C(S)$, An expanded explanation is provided in Chapter III). If we also assume that S and $C(S)$ can be mapped to a classical code C and its dual $C^{\perp}$, respectively. Then a quantum code Q exists, stabilized by the subgroup S as shown by the independent work of Calderbank and Shor [31] and Steane [143]. The quantum code Q is a q^k dimensional subspace of the Hilbert space C^{q^n}, and it has parameters $[[n,k,d]]_q$ with k information logic qubits and n encoded qubits. The code Q is able to correct all errors up to $\lfloor (d-1)/2 \rfloor$, see Chapter III for more details. A quantum code is called impure if there is a vector in C with weight less than any vector in $(C^{\perp} \backslash C)$; otherwise it is called pure. Pure quantum codes have been constructed based on good classical codes (i.e. codes with high minimum distance). However, the construction of impure quantum codes from classical codes with poor distances has not been widely investigated. Surprisingly, one can construct good impure quantum codes based on bad classical codes (i.e. codes with low minimum distance).

Research Problems The goals of my research in quantum block codes are to:

a) Construct families of quantum block codes over finite fields based on self-orthogonal (or dual-containing) classical codes. Determine whether there are families of impure quantum codes such that the stabilizer has many vectors with small weights and these families are not extended codes.

b) Study the probability of undetected errors for some families of stabilizer codes and search for codes with undetected error probability that approaches zero.

c) Determine whether stabilizer codes be constructed from polynomial and Euclidean geometry codes since these codes have the feature of majority list decoding, and what are the conditions that will determine whether these codes will be self-orthogonal (or dual-containing)?

d) Analyze the method by which a family of stabilizer codes uses fault-tolerant quantum computing. What is its threshold value? Can it be improved? And if so, what assumptions must be made to improve it?

e) Determine whether quantum stabilizer codes, in which errors have some nice structure, can correct beyond the minimum distance, since we know that fire and burst-error classical codes can correct errors beyond half of their minimum distance.

Subsystem Codes. Subsystem codes are a relatively new construction of quantum codes based on isolating the active errors into two subsystems. Hence, a quantum code Q is a tensor product of two subsystems A and B, i.e. $Q = A \otimes B$. The dimension of the subsystem A is q^k while the dimension of the subsystem B is q^r; the code Q has parameters $[[n, k, r, d]]_q$. A special feature of subsystem codes is that any classical additive code C can be used to construct a subsystem code. One should contrast this with stabilizer codes, where the classical codes are required to satisfy self-orthogonality (or dual-containing) conditions. Many interesting problems have not yet been addressed on subsystem codes such as bounds, weight enumerators, encoding circuits and families of subsystem codes. Also, there are no tables of upper bounds, lower bounds, or best known subsystem codes.

Research Problems The goals of my research in subsystem codes are to:

a) Investigate properties of subsystem codes and find good subsystem codes with high rates and large minimum distances. How do stabilizer codes compare with subsystem codes with $r \geq 1$? How are families of subsystem codes constructed based on classical codes?

b) Analyze the conditions under which classical codes will give us subsystem codes with large gauge qubits $r \geq 1$. Assuming we have RS or BCH codes with length n and designed distance δ that can be used to construct subsystem codes. How much does the minimum distance for subsystem RS or BCH codes increase, if k and r are exchanged?

c) Implement the linear programming and Gilbert-Varshimov bounds, using Magma computer algebra, to derive tables of upper bounds, lower bounds, and best known codes of subsystem codes over finite fields.

d) Determine what the efficient encoding and decoding circuits look like for subsystem codes, and whether we can draw an encoding circuit for a subsystem code from a given encoding circuit of a stabilizer code.

Quantum Convolutional Codes. Quantum convolutional codes (QCC's) seem to be useful for quantum communication because they have online encoder and decoder algorithms (circuits). One main property of quantum convolutional codes is the delay operator where the encoder has some memory set. However, quantum convolutional codes still have not been studied extensively. Furthermore, many interesting and open questions remain regarding the properties and the usefulness of quantum convolutional codes. At this time, it is not known whether quantum convolutional codes offer a decisive advantage over quantum block codes, since we do not yet have a well-defined formalism of quantum convolutional codes. For example, the CSS construction, projectors, and non-catastrophic encoders are not clearly defined for quantum convolutional codes. In other words, except for the work by Ollivier [113], there are only some examples of quantum convolutional codes with 1/3, 1/4, and $1/n$ code rates.

Research Problems The goals of my research in quantum convolutional codes are to:

a) Formulate a stabilizer formalism for convolutional codes that is similar to the well-defined stabilizer formalism of quantum block codes, and to construct families of quantum convolutional codes based on classical convolutional codes.

b) Determine whether it is possible to construct quantum convolutional codes, given RS and BCH codes with length n and designed distance δ, and to determine under which conditions these codes can be mapped to self-orthogonal convolutional codes, what the restrictions are on δ, and whether parameters of quantum convolutional codes can be bounded using a generalized Singleton bound.

c) Design online efficient encoding and decoding circuits for quantum convolutional codes.

d) Establish whether a scenario for quantum convolutional codes, where the errors can be isolated into subsystems, exists that is similar to error avoiding codes (subsystem codes) that can be constructed from block codes.

D. Dissertation Outline

Some of the research problems stated in the previous subsection are completely solved up on my research, some are left as an extension work, and obviously some will take more than a decade before acceptable answers can be proposed. In this dissertation

I construct many families of quantum error control codes and study their properties. The dissertation is structured into three parts and the main results are stated as follows.

I) In part I, Chapters III IV V VI, I study families of quantum block codes constructed using the CSS construction. I establish conditions when nonbinary primitive BCH codes are dual-containing with respect to Euclidean and Hermitian products; consequently I derived families of quantum BCH codes. Also, I compute the dimension and bound the minimum distance of BCH codes under some restricted conditions. I derive impure quantum codes with remarkable minimum distance based on duadic codes. Also, I construct one family of quantum codes from project geometry codes.

II) In part II, Chapters VII VIII IX X, I study families of subsystem codes. I give various methods for subsystem code constructions, and, in addition, I derive families of subsystem codes based on BCH and RS codes. I generate tables of upper and lower bounds of subsystem code parameters. Finally, I trade the dimensions of subsystem code parameters and present a fair comparison between stabilizer and subsystem codes.

III) In part III, Chapters XI XII XIII, I study quantum convolutional codes. I establish the stabilizer formalism of quantum convolutional codes using the direct limit, and I derive the generalized Singleton bound for quantum convolutional codes. Finally, I demonstrate two families of quantum convolutional codes derived from RS and BCH codes.

CHAPTER II

BACKGROUND

In this chapter I will present background material and terminologies of classical coding theory and quantum error control codes that are necessary to assist the reader in understanding the families of quantum codes presented in the following chapters. I will also cite previous work on quantum error control codes that is relevant to my work in this dissertation.

The power of quantum computers comes from their ability to use quantum mechanical principles such as entanglement, interference, superposition, and measurement. These fascinating natural types of computers can solve certain problems exponentially faster than any known classical computers. Some well known examples of problems that can be solved are factorization of large primes and searching [111]. It was recently demonstrated that quantum key distribution schemes can be used to exchange private keys over public communication channels.

Finding problems that can be solved by quantum computers is an interesting research subject, yet a difficult task. With the exception of a few problems, it is not well-known what types of problems that quantum computers can solve exponentially fast. However, there is no doubt about the usefulness and powerfulness of quantum computers. The most difficult problem associated with building quantum computers is isolating the *noise*. The term *noise* can be defined as quantum errors that are caused by decoherence from an environment.

A. Classical Coding Theory

Let q be a power of a prime p. Let $\mathbb{F}_q$ denote a finite field with q elements. If $q = p^m$ then

$$\mathbb{F}_q^n[x] = \{f(x) \in \mathbb{F}_q[x] \mid deg f(x) < m\}, \tag{2.1}$$

where $f(x)$ is a polynomial of max degree m, and $\mathbb{F}_q[x]$ is a polynomial ring. If $q = p$, then the field has the integer elements $\{0, 1, ..., p-1\}$ with the normal addition and multiplication operations module p. The addition and multiplication of elements in $\mathbb{F}_q$, where $q = p^m$, are done by adding and multiplying in $\mathbb{F}_p[x]$ module a known irreducible polynomial $P_m(x)$ in $\mathbb{F}_p[x]$ of degree m. A detailed survey on finite fields is reported in [75]. Let β be an element in $\mathbb{F}_q$. The smallest positive integer ℓ such that $\beta^\ell = 1$ is called the order of β. The order of a finite field is the number of elements on it, i.e., the cardinality of the field. If $\alpha \in \mathbb{F}_q$ and the order of α is $q-1$, then α is called a primitive element in $\mathbb{F}_q$. In this case, all nonzero elements in $\mathbb{F}_q$ can be represented in $q-1$ consecutive powers of a primitive element $\{1, \alpha, \alpha^2, ..., \alpha^{q-1}, \alpha^q = \alpha, \alpha^\infty = 0\}$.

Linear Codes. Let $\mathbb{F}_q^n$ be a vector space with dimension n and size q^n. A code C is a subspace of the vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Every linear code is generated by a generator matrix G of size $k \times n$. Let u be a vector in $\mathbb{F}_q^k$, then

$$C = \{uG \mid \quad \forall \quad u \in \mathbb{F}_q^k\}, \tag{2.2}$$

where G is a generator matrix of size $k \times n$ over $\mathbb{F}_q$. The k basis vectors of G are the basis for the code C. The code C has q^k codewords, the size of C. We can also generate a dual matrix H of size $(n-k) \times n$ from the matrix G such that

$$GH^T = 0. \tag{2.3}$$

The $n-k$ rows of H are also linearly independent. H is called the parity check matrix of C. We say that v is a valid codeword in C, if and only if, $Hv^T = 0$. The parity check matrix H can also be used to define the C as

$$C = \{v \in \mathbb{F}_q^n \mid Hv^T = 0\}. \tag{2.4}$$

The dual of a code C is denoted by $C^\perp$ and is defined by

$$C^\perp = \{w \mid w \in \mathbb{F}_q^n, \quad w.v = 0 \ \ \forall \quad v \in C\}, \tag{2.5}$$

where $w.v$ is the Euclidean inner product between two vectors in $\mathbb{F}_q$. If we assume that $w = (w_1, w_2, \ldots, w_n)$ and $v = (v_1, v_2, \ldots, v_n)$ then $w.v = \sum_{i=1}^n w_i v_i$. We can say that w is orthogonal to v if their inner product vanishes, i.e., $w.v = 0$. If $C^\perp \subseteq C$, then the code is called dual-containing. It means that all codewords in $C^\perp$ lie in C as well. Also, if all codewords in C lie in $C^\perp$, then the code C is called self-orthogonal, i.e., $C \subseteq C^\perp$. Self-orthogonal or dual-containing codes are of particular interest to our work because they are used to derive quantum codes. If $C = C^\perp$, then the code is called self-dual. If $[n, k, d]_q$ are parameters of a code C, then $[n, n-k, d]_q$ are parameters of the dual code $C^\perp$.

Minimum Distance and Hamming Weight. Some important criteria's of a code are the weight and minimum distance among its codewords. The weight of a codeword v in a code C is the number of nonzero positions (coordinates) in v. Let w and v be two codewords in a code $C \subseteq \mathbb{F}_q^n$. The Hamming distance between w and v is given by the number of positions in which w and v differ. It is weight of the difference codeword.

$$d(w, v) = \mid \{i \mid 1 \le i \le n, w_i \neq v_i\} \mid = \mathrm{wt}(w - v). \tag{2.6}$$

The minimum distance of a code is the smallest distance between two different codewords in C. If $C \subseteq \mathbb{F}_q^n$, then the minimum distance d is the minimum weight of a nonzero codeword.

The code performance can be measured by its rate, decoding and encoding complexity, and minimum distance. If the minimum distance is large, the code has a better ability to correct errors. Given a minimum distance d of a code C, the maximum number of errors t that can be corrected by C is $t = \lfloor (d-1)/2 \rfloor$, where the errors are distributed in random positions. The rate of a a code C is given by the ratio of its dimension to its length, i.e., k/n. The linear code parameters are given by $[n, k, d]_q$ or $(n, q^k, d)_q$.

Let A_i and B_i be the number of codewords in C and $C^\perp$ of weight i, respectively. The list of codewords A_i and B_i are called the weight distributions of C and $C^\perp$, respectively. If C is a code with parameters $[n, k, d]$ over $\mathbb{F}_q$, then it is a well-known fact that $A_0+A_1+\ldots+A_n = q^k$. Furthermore, $A_0 = 1$ and $A_1 = A_2 = \ldots = A_{d-1} = 0$.

Error Corrections. Now assume a codeword $v \in C$ is sent over a noise communication channel. Let $r = v + e$ be the received vector where e is the added noise. Then one can use the matrix H to perform error correction and detection capabilities of the code C.

$$s = rH^T = (v + e)H^T = eH^T. \tag{2.7}$$

Based on the value of the syndrome s, one might be able to correct the received codeword r to the original codeword v, see [75, 107] for further details.

1. Bounds on the Code Parameters

The relationship between the code parameters n, k, d and q has been well studied in order to compare the performance of codes. The minimum distance d is used to measure the ability of a code to correct errors. Good error correcting codes are designed with a large minimum distance d and as large a number of codewords q^k as possible, for a given length n and alphabet size q. So, it is crucial to establish upper and lower bounds on the code parameters. There have been many upper bounds on the code parameters such as Singleton, Hamming and sphere packing, and linear programming bounds. Also, there have been some lower bounds such as Gilbert-Varshamov bound.

Singleton Bound and MDS Codes. Given a code C with parameters $[n, k, d]_q$ for $d \leq n$, the classical Singleton bound can be stated as

$$q^k \leq q^{n-d+1}. \tag{2.8}$$

If C is a linear code, then $k \leq n - d + 1$. Codes that attain the Singleton bound with equality are called Maximum Distance Separable (MDS) codes. MDS codes are also optimal codes. This class of codes is of particular interest because it has the maximum distance that can be achieved among all other codes with the same length, dimension, and alphabet size. No other codes of length n and size q^k have larger minimum distances than MDS codes, with the same parameters. Also, it is known that the dual of a classical MDS code is also an MDS code.

Hamming Bound and Perfect Codes. Given a code C with parameters $[n, k, d]_q$ for $d \leq n$, the classical Hamming bound can be stated as

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \leq q^{n-k}, \tag{2.9}$$

where $t = \lfloor (d-1)/2 \rfloor$. Codes that attain Hamming bound with equality are classified as perfect codes. Let every codeword be represented by a sphere of radius t. The interpretation of Hamming bound, or sometimes called sphere packing bound, is that all codewords or the q^k spheres are pairwise disjoint in the space $\mathbb{F}_q^n$. For further details on bound on the classical code parameters, see for example [75, 106, 107].

2. Families of Codes

There have been numerous families of classical codes. The most notable are the Bose-Chaudhuri-Hocquenghem (BCH), Reed-Solomon (RS), Reed-Muller (RM), algebraic and projective geometry, and LDPC codes, see [75, 106, 107]. In this dissertation I will describe some of these families. I will establish the conditions required for these codes to be self-orthogonal (or dual-containing) over finite fields, and, consequently, they can be used to derive quantum error control codes.

B. Quantum Error Control Codes

There has been a tremendous amount of research work in quantum error correcting codes during the last ten years. As such, the theory of stabilizer codes is well developed over binary and nonbinary fields. Many families of stabilizer codes are constructed based on BCH, RS, RM, finite geometry classical codes, where these families of codes are shown to be self-orthogonal (or dual-containing). Recently, the theory of stabilizer codes over finite fields has been extended to subsystem codes, where families of classical codes do not need to be self-orthogonal (or dual-containing). Also, new families and code constructions of subsystem codes have been investigated. I will summarize previous work related to my research in the following subsections.

1. Quantum Block Codes

The first quantum code was introduced by Shor as an impure quantum code with parameters $[[9,1,3]]_2$ in a landmark paper in 1995 [137]. The idea was to protect one qubit against bit flip and phase errors into nine qubits. Gottesman developed the theory and introduced quantum encoding circuits and fault-tolerant quantum computing [57, 58, 61]. Calderbank and Shor extended the theory to codes over $\mathbb{F}_4$ and introduced the CSS construction independently with Steane [30, 31, 144]. The quantum code Q can be defined as follows.

Definition 1. A q-ary quantum code Q, denoted by $[[n,k,d]]_q$, is a q^k dimensional subspace of the Hilbert space $\mathbb{C}^{q^n}$ and can correct all errors up to $\lfloor \frac{d-1}{2} \rfloor$.

The code Q is able to encode k logical qubits into n physical qubits with a minimum distance of at least d between any two codewords. The Q can be constructed based on two classical codes C_1 and C_2 such that $C_2^\perp \leq C_1$ as follows.

Fact 2 (CSS Code Construction)**.** *Let C_1 and C_2 denote two classical linear codes with parameters $[n,k_1,d_1]_q$ and $[n,k_2,d_2]_q$ such that $C_2^\perp \leq C_1$. Then there exists a $[[n,k_1+k_2-n,d]]_q$ stabilizer code with minimum distance $d = \min\{\mathrm{wt}(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\} \geq \min\{d_1,d_2\}$.*

Constructing a quantum code Q reduces to constructing a self-orthogonal (or dual-containing) classical code C defined over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ as follows.

Fact 3. *If there exists an $\mathbb{F}_q$-linear $[n,k,d]_q$ classical code C containing its dual, $C^\perp \subseteq C$, then there exists an $[[n,2k-n,\geq d]]_q$ quantum stabilizer code that is pure to d.*

Fact 4. *If there exists an $\mathbb{F}_{q^2}$-linear $[n,k,d]_{q^2}$ classical code C such that $C^{\perp_h} \subseteq C$, then there exists an $[[n,2k-n,\geq d]]_q$ quantum stabilizer code that is pure to d.*

There have been many families of quantum codes based on binary classical codes, see [63, 64, 66, 82, 145]. These classes of codes are derived from BCH, RS, algebraic geometry codes in addition to codes over graphs. The theory has been generalized to finite fields, see [16, 44, 45, 59, 83, 123, 129, 135]. Recently, new bounds, encoding circuits, and new families have been investigated, see [11, 12, 44, 46, 71, 104, 129].

We will describe foundations of quantum block codes, as well as bounds and families of such codes in Chapters III,IV,V, VI.

2. Subsystem Codes

Subsystem codes are a generalization of the theory of quantum error correction and decoherence free subspaces. Such codes are an extension of quantum codes that are constructed based on self-orthogonal(or dual-containing) classical codes. The assumption is that a quantum code Q can be decomposed as a tensor product of two subsystems A and B, i.e. $Q = A \otimes B$. The source qubits are stored in the subsystem A and gauge qubits are stored in subsystem B. Therefore, subsystem codes are quantum error control codes where errors can be avoided as well as corrected. One can correct only errors on the subsystem A and completely neglect the errors affecting the subsystem B [19, 95]; for a group representation of operator quantum codes, see [86, 89, 121].

It has been shown in [6, 9] that subsystem codes over $\mathbb{F}_q$ can be derived from classical additive codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ without the needed for self-orthogonal or dual-containing conditions. An approach for code construction and bounds on the code parameters is shown in [9]. It has been claimed that subsystem codes seem to offer some attractive features for protection of quantum information and fault-tolerant quantum computing. They can be self-correcting codes [19]. Let $\mathcal{H} = C^{q^n}$ be the Hilbert space such that $\mathcal{H} = Q \oplus Q^{\perp}$, where $Q^{\perp}$ is the orthogonal complement of Q. An $[[n,k,r,d]]_q$ subsystem code Q can be described as

Definition 5. An $[[n,k,r,d]]_q$ subsystem code is a decomposition of the subspace Q into a tensor product of two vector spaces A and B such that $Q = A \otimes B$. If $\dim A = k$ and $\dim B = r$, then the code Q is able to detect all errors of weight less than d on subsystem A.

Subsystem codes can be constructed from classical codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$.

Fact 6 (Euclidean Construction). *If C is a k'-dimensional $\mathbb{F}_q$-linear code of length n that has a k''-dimensional subcode $D = C \cap C^\perp$ and $k' + k'' < n$, then there exists an*

$$[[n, n-(k'+k''), k'-k'', \mathrm{wt}(D^\perp \setminus C)]]_q$$

subsystem code.

Fact 7 (Hermitian Construction). *Let $C \subseteq \mathbb{F}_{q^2}^n$ be an $\mathbb{F}_{q^2}$-linear $[n,k,d]_{q^2}$ code such that $D = C \cap C^{\perp_h}$ is of dimension $k' = \dim_{\mathbb{F}_{q^2}} D$. Then there exists an*

$$[[n, n-k-k', k-k', \mathrm{wt}(D^{\perp_h} \setminus C)]]_q$$

subsystem code.

We will describe foundations of subsystem codes; in addition to bounds and families of such codes in Chapters VII,VIII,IX, X.

3. Quantum Convolutional Codes

Quantum convolutional codes (QCC's) seem to be useful for quantum communication because they have online encoders and decoders. One main property of quantum convolutional codes is the delay operator where the encoder has some memory set. However, quantum convolutional codes still have not been studied extensively. As pointed out earlier by several authors [68], many interesting and unsolved questions remain regarding the properties and the usefulness of quantum convolutional codes. At this time, it is not known if quantum convolutional codes offer a decisive advantage over quantum block codes. We do not yet have a well-defined formalism of quantum convolutional codes. For example, the CSS construction, projector of a quantum convolutional code, and non-catastrophic encoders are not clearly defined for quantum convolutional codes. In other words, except for the work by Ollivier [113], there are only some examples of quantum convolutional codes with 1/3, 1/4, and $1/n$ code rates. There have been examples of quantum convolutional codes in the literature; the most notable being are the $((5, 1, 3))$ code of Ollivier and Tillich, the $((4, 1, 3))$ code of Almeida and Palazzo and the rate 1/3 codes of Forney and Guha. We present the most notable results as follows

- Ollivier and Tillich developed the stabilizer framework for quantum convolutional codes. They also addressed the encoding and decoding aspects of quantum convolutional codes (cf. [112, 113, 115, 115]). Furthermore, they provided a maximum likelihood error estimation algorithm. They showed, as an example, a quantum convolutional code of rate $k/n = 1/5$ that can correct only one error.

- Forney and Guha constructed quantum convolutional codes with rate 1/3 [50]. Also, together with Grassl, they derived rate $(n-2)/n$ quantum convolutional codes [49]. They gave tables of optimal rate 1/3 quantum convolutional codes and they also constructed good quantum block codes obtained by tail-biting convolutional codes.

- Grassl and Rötteler constructed quantum convolutional codes from product codes. They showed that starting with an arbitrary convolutional code and a self-orthogonal block code, a quantum convolutional code can be constructed. (cf. [68]). Recently, Grassl and Rötteler [70] stated a general algorithm to construct quantum circuits for non-catastrophic encoders and encoder inverses for channels with memories. Unfortunately, the encoder they derived is for a subcode of the original code.

Recall that one can construct convolutional stabilizer codes from self-orthogonal (or dual-containing) classical convolutional codes over $\mathbb{F}_q$ (cf. [10, Corollary 6]) and $\mathbb{F}_{q^2}$ (see [10, Theorem 5]) as stated in the following theorem.

Fact 8. *An* $[(n, k, nm; \nu, d_f)]_q$ *convolutional stabilizer code exists if and only if there exists an* $(n, (n-k)/2, m; \nu)_q$ *convolutional code such that* $C \leq C^\perp$ *where the dimension of* $C^\perp$ *is given by* $(n+k)/2$ *and* $d_f = \mathrm{wt}(C^\perp \backslash C)$.

We will describe foundations of quantum convolutional codes, as well as bounds and families of such codes in Chapters XI,XII,XIII.

C. Fault Tolerant Quantum Computing

The main purpose of fault tolerant quantum computing is to limit the number of errors that may happen in practical quantum computers. These errors may happen in the quantum error correcting operations or in the quantum circuits (i.e. gate operations). First, Shor presented the idea of applying fault tolerant quantum computations into quantum gates [138]. He applied it on controlled-not and phase gates, and showed how to perform fault tolerant operations even if an error happened in one single qubit. The most prominent work in fault tolerant quantum computing was conducted by Preskill [122], Gottesman [59], Steane [146], Knill [88]. Fault tolerant quantum computing seems to speed up the process of building quantum computers under a certain threshold value, known as threshold theorem [1, 88, 146].

CHAPTER III

FUNDAMENTALS OF QUANTUM BLOCK CODES

In this chapter I aim to provide an accessible introduction to the theory of quantum error-correcting codes over finite fields. Many definitions that are stated in this chapter will be also used through out the dissertation's parts. I will recall certain definitions concerning the error group and bounds of quantum code parameters from this chapter in the later chapters. Whenever, there is a definition or result that has not been mentioned in this chapter and will be used in the dissertation's chapters, I will state it accordingly if needed. I tried to keep the prerequisites to a minimum, though I assume that the reader has a minimal background in coding theory and quantum computing as introduced in the first two chapters or as shown in any introductory textbook such as [111]. Also, I recommend the introductory textbooks [75] and [107] as sources for the classical coding theory. I will cite most of the known previous work in quantum error control codes. Finally, part of this chapter has been done in a joint work with A. klappenecker and P. Sarvepalli and has been presented in [133].

This chapter focuses only on quantum block codes and it is organized as follows. Section A gives a brief overview of the main ideas of stabilizer codes while Section B reviews the relation between quantum stabilizer codes and classical codes. This connection makes it possible to reduce the study of quantum stabilizer codes to the study of self-orthogonal (or dual-containing) classical codes, though the definition of self-orthogonality is a little broader than the classical one. Further, it allows us to use all the tools of classical codes to derive bounds on the parameters of good quantum codes. Section C gives an overview of the important bounds for quantum codes. I will state quantum Singleton and Hamming bounds on quantum code parameters. I will prove quantum Hamming bound for impure quantum codes that can correct one or two errors. After that I will introduce many families of quantum error-correcting codes derived from self-orthogonal (or dual-containing) classical codes in the following chapters.

Notations. The finite field with q elements is denoted by $\mathbb{F}_q$, where $q = p^m$ and p is assumed to be a prime and m is an integer number. The trace function from $\mathbb{F}_{q^r}$ to $\mathbb{F}_q$ is defined as $\mathrm{tr}_{q^r/q}(x) = \sum_{i=0}^{r-1} x^{q^k}$, and we may omit the subscripts if $\mathbb{F}_q$ is the prime field. The center of a group G is denoted by $Z(G)$ and the centralizer of a subgroup S in G by $C_G(S)$. We denote by $H \leq G$ the fact that H is a subgroup of G. The trace $\mathrm{Tr}(M)$ of a square matrix $M = [m_{ij}]$ of size $n \times n$ is the sum of the diagonal elements of M, i.e., $\sum_{i=1}^{n} m_{ii} = \mathrm{Tr}(M)$.

A. Stabilizer Codes

In this chapter, we use q-ary quantum digits, shortly called qudits, as the basic unit of quantum information. The state of a qudit is a nonzero vector in the complex vector space $\mathbb{C}^q$. This vector space is equipped with an orthonormal basis whose elements are denoted by $|x\rangle$, where x is an element of the finite field $\mathbb{F}_q$. The state of a system of n qudits is then a nonzero vector in $\mathbb{C}^{q^n}$. In general, quantum codes are just nonzero subspaces of $\mathbb{C}^{q^n}$. A quantum code that encodes k logical qudits of information into n physical qudits is denoted by $[[n, k, d]]_q$, where the subscript q indicates that the code is q-ary and d is the minimum distance of this code. More generally, an $((n, K, d))_q$ quantum code is a K-dimensional subspace encoding $\log_q K$ qudits into n qudits and it can correct up to $t = \lfloor (d-1)/2 \rfloor$ errors.

The first quantum error-correcting code was introduced by Shor in 1995 as an impure quantum code with parameters $[[9, 1, 3]]_2$ [137]. The idea was to protect one qubit against bit flip and phase flip errors by encoding this qubit into nine qubits.

Calderbank and Shor extended the theory and formalized the CSS construction independently with Steane [30, 31, 144]. Shortly, Gottesman introduced stabilizer codes, quantum concatenated codes and quantum encoding circuits [57, 58, 60].

As the quantum codes are subspaces, it seems natural to describe them by giving a basis for the subspace. However, in case of quantum codes this turns out to be an inconvenient description. For instance, consider a $[[7, 1, 3]]_2$ Steane code that encodes one logical qubit into seven physical qubits with a minimum distance three among its codewords. We can describe a basis for this code as follows

$$\begin{aligned} |0_L\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |0111100\rangle + |1011010\rangle + |1101001\rangle , \\ |1_L\rangle &= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |0111100\rangle + |1011010\rangle + |1101001\rangle . \end{aligned}$$

An alternative description of the quantum error-correcting codes that will be discussed in this chapter relies on error operators that act on $\mathbb{C}^{q^n}$. Let E be an error operator. If we make the assumption that the errors are independent on each qudit, then each error operator E can be decomposed as $E = E_1 \otimes \cdots \otimes E_n$. Furthermore, linearity of quantum mechanics allows us to consider only a discrete set of errors. The quantum error-correcting codes that we consider here can be described as the joint eigenspace of an abelian subgroup of error operators. The subgroup of error operators is called the stabilizer of the code (because it leaves each state in the code unaffected) and the code is called a stabilizer code. In the next four subsections, we will describe the error group and stabilizer codes in details.

1. Error Bases

Let P be a set of Pauli matrices given by $\{I, X, Z, Y\}$. In general, we can regard any error as being composed of an amplitude error (qubit flip) and a phase error (qubit shift). Let a and b be elements in $\mathbb{F}_q$. We can define unitary operators $X(a)$ and $Z(b)$ on $\mathbb{C}^q$ that generalize the Pauli X and Z operators to the q-ary case; they are defined as

$$X(a)\,|x\rangle = |x + a\rangle\,, \qquad Z(b)\,|x\rangle = \omega^{\mathrm{tr}(bx)}\,|x\rangle\,, \tag{3.1}$$

where tr denotes the trace operation from $\mathbb{F}_q$ to $\mathbb{F}_p$, and $\omega = \exp(2\pi i/p)$ is a primitive pth root of unity.

Let $\mathcal{E} = \{X(a)Z(b)\,|\,a, b \in \mathbb{F}_q\}$ be the set of error operators. The error operators in $\mathcal{E}$ form a basis of the set of complex $q \times q$ matrices as the trace $\mathrm{Tr}(A^\dagger B) = 0$ for distinct elements A, B of $\mathcal{E}$. Further, we observe that

$$X(a)Z(b)\,X(a')Z(b') = \omega^{\mathrm{tr}(ba')}X(a + a')Z(b + b'). \tag{3.2}$$

The error basis for n q-ary quantum systems can be obtained by tensoring the error basis for each system. Let $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{F}_q^n$. Let us denote by $X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n)$ and $Z(\mathbf{a}) = Z(a_1) \otimes \cdots \otimes Z(a_n)$ for the tensor products of n error operators. Then we have the following result whose proof follows from the definitions of $X(\mathbf{a})$ and $Z(\mathbf{b})$.

Lemma 9. *The set* $\mathcal{E}_n = \{X(\mathbf{a})Z(\mathbf{b})\,|\,\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ *is an error basis on the complex vector space* $\mathbb{C}^{q^n}$.

2. Stabilizer Codes

We will describe the quantum codes using a set of error bases. Consider the error group G_n defined as

$$G_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \,|\, \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}. \tag{3.3}$$

G_n is simply a finite group of order pq^{2n} generated by the matrices in the error basis $\mathcal{E}_n$. Two elements E_1 and E_2 in G_n are abelian if $E_1E_2 = E_2E_1$.

Let S be the largest abelian subgroup of the error group G_n fixes every element in a quantum code Q. Then a *stabilizer code* Q is a non-zero subspace of $\mathbb{C}^{q^n}$ defined as

$$Q = \bigcap_{E\in S} \{|\psi\rangle \in \mathbb{C}^{q^n} \mid E\,|\psi\rangle = |\psi\rangle\}. \tag{3.4}$$

Alternatively, Q is the joint $+1$ eigenspace of the stabilizer subgroup S. The notation of eigenspace and eigen value are described for example in [38]. A stabilizer code contains *all* joint eigenvectors of S with eigenvalue 1, as equation (3.4) indicates. If the code is smaller and does not contain all the joint eigenvectors of S with eigenvalue 1, then it is not a stabilizer code for S. In other words, every error operator E in S fixes every codeword $|\psi\rangle$ in Q.

3. Stabilizer and Error Correction

Now, we define the quantum code via its stabilizer S, then we can be able to describe the performance of the code, that is, we should be able to tell how many errors it can error and how the error-correction is done, in addition to how many errors it can detect.

The central idea of error detection is that a detectable error acting on Q should either act as a scalar multiplication on the code space (in which case the error did not affect the encoded information) or it should map the encoded state to the orthogonal complement of Q (so that one can set up a measurement to detect the error). Specifically, we say that Q is able to detect an error E in the unitary group $U(q^n)$ if and only if the condition $\langle c_1|E|c_2\rangle = \lambda_E\langle c_1|c_2\rangle$ holds for all $c_1, c_2 \in Q$, see [90].

We can show that a stabilizer code Q with stabilizer S can detect all errors in G_n that are scalar multiples of elements in S or that do not commute with some element of S, see Lemma 10. In particular, an undetectable error in G_n has to commute with all elements of the stabilizer. Let $S \leq G_n$ and $C_{G_n}(S)$ denote the centralizer of S in G_n,

$$C_{G_n}(S) = \{E \in G_n \,|\, EE' = E'E \text{ for all } E' \in S\}. \tag{3.5}$$

Let $SZ(G_n)$ denote the group generated by S and the center $Z(G_n)$. We need the following characterization of detectable errors.

Lemma 10. *Suppose that $S \leq G_n$ is the stabilizer group of a stabilizer code Q of dimension $\dim Q > 1$. An error E in G_n is detectable by the quantum code Q if and only if either E is an element of $SZ(G_n)$ or E does not belong to the centralizer $C_{G_n}(S)$.*

Proof. See [16, 81]; the interested reader can find a more general approach in [85, 87]. □

Since detectability of errors is closely associated to commutativity of error operators, we will derive the following condition on commuting elements in G_n:

Lemma 11. *Two elements $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ and $E' = \omega^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ of the error group G_n satisfy the relation $EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})}E'E$. In particular, the elements E and E' commute if and only if the trace symplectic form $\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})$ vanishes.*

Proof. We can easily verify that $EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}')} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$ and $E'E = \omega^{\mathrm{tr}(\mathbf{b}'\cdot\mathbf{a})} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$ using equation (3.2). Therefore, $\omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})}E'E$ yields EE', as claimed. $\square$

Minimum Distance. We shall also define the minimum distance of a quantum code Q. In order to do so, we need to define the symplectic weight of a vector $(a|b)$ in $\mathbb{F}_q^{2n}$. The *symplectic weight* swt of a vector $(\mathbf{a}|\mathbf{b})$ in $\mathbb{F}_q^{2n}$ is defined as

$$\mathrm{swt}((\mathbf{a}|\mathbf{b})) = |\{\, k \mid (a_k, b_k) \neq (0,0)\}|. \tag{3.6}$$

The weight $\mathrm{wt}(E)$ of an element $E = \omega^c E_1 \otimes \cdots \otimes E_n = \omega^c X(\mathbf{a})Z(\mathbf{b})$ in the error group G_n is defined to be the number of nonidentity tensor components i.e., $\mathrm{wt}(E) = |\{E_i \neq I\}| = \mathrm{swt}((\mathbf{a}|\mathbf{b}))$.

A quantum code Q is said to have *minimum distance* d if and only if it can detect all errors in G_n of weight less than d, but cannot detect some error of weight d. We say that Q is an $((n,K,d))_q$ code if and only if Q is a K-dimensional subspace of $\mathbb{C}^{q^n}$ that has minimum distance d. An $((n,q^k,d))_q$ code is also called an $[[n,k,d]]_q$ code. One of these two notations will be used when needed.

Due to the linearity of quantum mechanics, a quantum error-correcting code that can detect a set $\mathcal{D}$ of errors, can also detect all errors in the linear span of $\mathcal{D}$. A code of minimum distance d can correct all errors of weight $t = \lfloor (d-1)/2 \rfloor$ or less.

Pure and Impure Codes. We say that a quantum code Q is *pure to* t if and only if its stabilizer group S does not contain non-scalar error operators of weight less than t. An $[[n,k,d]]_q$ quantum code is called pure if and only if it is pure to its minimum distance d. We will follow the same convention as in [30], that an $[[n,0,d]]_q$ code is pure. Impure codes are also referred to as degenerate codes. Degenerate codes are of interest because they have the potential for passive error-correction and they are

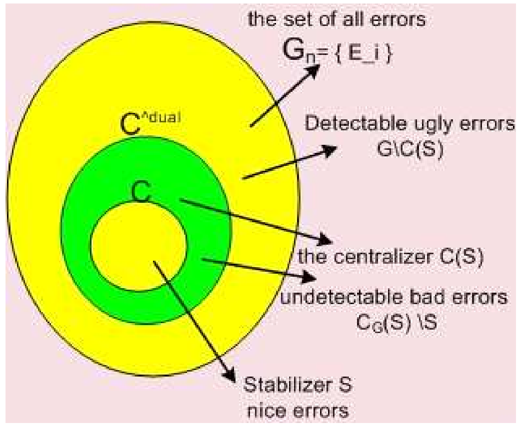


Fig. 1. The relationship between a quantum stabilizer code Q and a classical code C, where $C \subseteq C^{\perp}$.

difficult to construct as we will explain later.

4. Encoding Quantum Codes

The Stabilizer S of a quantum code Q provides also a means for encoding quantum codes. The essential idea is to encode the information into the code space through a projector. For an $((n, K, d))_q$ quantum code with stabilizer S, the projector P is defined as

$$P = \frac{1}{|S|} \sum_{E \in S} E. \tag{3.7}$$

It can be checked that P is an orthogonal projector onto a vector space Q. Further, we have

$$K = \dim Q = \operatorname{Tr} P = q^n/|S|. \tag{3.8}$$

The stabilizer allows us to derive encoded operators, so that we can operate directly on the encoded data instead of decoding and then operating on them. These operators are in $C_{G_n}(S)$. See [58] and [71] for more details.

B. Deriving Quantum Codes from Self-orthogonal Classical Codes

In this section we show how stabilizer codes are related to classical codes (additive codes over $\mathbb{F}_q$ or over $\mathbb{F}_{q^2}$). The central idea behind this relation is the fact insofar as the detectability of an error is concerned the phase information is irrelevant. This means we can factor out the phase defining a map from G_n onto $\mathbb{F}_q^{2n}$ and study the images of S and $C_{G_n}(S)$. We will denote a classical code $C \leq \mathbb{F}_q^n$ with K codewords and distance d by $(n, K, d)_q$. If it is linear then we will also denote it by $[n, k, d]_q$ where $k = \log_q K$. We define the Euclidean inner product of $x, y \in \mathbb{F}_q^n$ as $x \cdot y = \sum_{i=1}^n x_i y_i$. The dual code $C^\perp$ is the set of vectors in $\mathbb{F}_q^n$ orthogonal to C i.e., $C^\perp = \{x \in \mathbb{F}_q^n \mid x \cdot c = 0 \text{ for all } c \in C\}$. For more details on classical codes see [75] or [107].

Constructing a quantum code Q reduces to constructing a self-orthogonal classical code C over $\mathbb{F}_q$ and $\mathbb{F}_q^2$, see [30, 35, 36, 58, 62, 137, 144, 145]. This relationship is shown in Fig. 1.

Fact 12 (CSS Code Construction)**.** *Let C_1 and C_2 denote two classical linear codes with parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$ such that $C_2^\perp \leq C_1$. Then there exists a $[[n, k_1 + k_2 - n, d]]_q$ stabilizer code with minimum distance $d = \min\{\mathrm{wt}(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\} \geq \min\{d_1, d_2\}$.*

Also, we can construct quantum codes from classical codes that contain their duals or are self-orthogonal as follows:

Fact 13. *If C is a classical linear $[n, k, d]_q$ code containing its dual, $C^\perp \leq C$, then there exists a $[[n, 2k - n, d]]_q$ stabilizer code.*

Fact 13 is particularly interesting because it helps us to construct a quantum code from a classical code and its dual. There have been many families of quantum codes based on binary classical codes, see [63, 64, 66, 82]. The theory has been generalized to finite fields, see [16, 44, 45, 59, 83, 123, 129, 135]. Recently, new bounds, encoding circuits, and new families have been investigated, see [11, 12, 44, 46, 71, 104, 129].

1. Codes over $\mathbb{F}_q$.

If we associate with an element $\omega^c X(\mathbf{a})Z(\mathbf{b})$ of G_n an element $(\mathbf{a}|\mathbf{b})$ of $\mathbb{F}_q^{2n}$, then the group $SZ(G_n)$ is mapped to the additive code

$$C = \{(\mathbf{a}|\mathbf{b}) \,|\, \omega^c X(\mathbf{a})Z(\mathbf{b}) \in SZ(G_n)\} = SZ(G_n)/Z(G_n). \tag{3.9}$$

To relate the images of the stabilizer and its centralizer, we need the notion of a trace-symplectic form of two vectors $(\mathbf{a}|\mathbf{b})$ and $(\mathbf{a}'|\mathbf{b}')$ in $\mathbb{F}_q^{2n}$,

$$< (\mathbf{a}|\mathbf{b}) \,|\, (\mathbf{a}'|\mathbf{b}') >_s = \operatorname{tr}_{q/p}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a}). \tag{3.10}$$

Let $C^{\perp_s}$ be the trace-symplectic dual of C defined as

$$C^{\perp_s} = \{x \in \mathbb{F}_q^{2n} \,|< x|\, c >_s = 0 \text{ for all } c \in C\}. \tag{3.11}$$

The centralizer $C_{G_n}(S)$ contains all elements of G_n that commute with each element of S; thus, by Lemma 11, $C_{G_n}(S)$ is mapped onto the trace-symplectic dual code $C^{\perp_s}$ of the code C,

$$C^{\perp_s} = \{(\mathbf{a}|\mathbf{b}) \,|\, \omega^c X(\mathbf{a})Z(\mathbf{b}) \in C_{G_n}(S)\}. \tag{3.12}$$

The next theorem illustrates this connection between classical codes and stabilizer codes and generalizes the well-known connection to symplectic codes [30, 57] of the binary case.

Theorem 14. *An $((n,K,d))_q$ stabilizer code exists if and only if there exists an additive code $C \leq \mathbb{F}_q^{2n}$ of size $|C| = q^n/K$ such that $C \leq C^{\perp_s}$ and* $\operatorname{swt}(C^{\perp_s} \setminus C) = d$

if $K > 1$*(* *and* $\operatorname{swt}(C^{\perp_s}) = d$ *if* $K = 1$*).*

Proof. See [16, 81] for the proof. $\square$

In 1996, Calderbank and Shor [31] and Steane [144] introduced the following construction of quantum codes. It is perhaps the simplest method to build quantum codes via classical codes over $\mathbb{F}_q$.

Lemma 15 (CSS Code Construction)**.** *Let* C_1 *and* C_2 *denote two classical linear codes with parameters* $[n, k_1, d_1]_q$ *and* $[n, k_2, d_2]_q$ *such that* $C_2^\perp \leq C_1$*. Then there exists a* $[[n, k_1 + k_2 - n, d]]_q$ *stabilizer code with minimum distance* $d = \min\{\operatorname{wt}(c) \mid c \in (C_1 \setminus C_2^\perp) \cup (C_2 \setminus C_1^\perp)\}$ *that is pure to* $\min\{d_1, d_2\}$*.*

Proof. Let $C = C_1^\perp \times C_2^\perp \leq \mathbb{F}_q^{2n}$. Clearly $C \leq C_2 \times C_1$. If $(c_1 \mid c_2) \in C$ and $(c_1' \mid c_2') \in C_2 \times C_1$, then we observe that $\operatorname{tr}(c_2 \cdot c_1' - c_2' \cdot c_1) = \operatorname{tr}(0 - 0) = 0$. Therefore, $C \leq C_2 \times C_1 \leq C^{\perp_s}$. Since $|C| = q^{2n-k_1-k_2}$, $|C^{\perp_s}| = q^{2n}/|C| = q^{k_1+k_2} = |C_2 \times C_1|$. Therefore, $C^{\perp_s} = C_2 \times C_1$. By Theorem 14 there exists an $((n, K, d))_q$ quantum code with $K = q^n/|C| = q^{k_1+k_2-n}$. The claim about the minimum distance and purity of the code is obvious from the construction. $\square$

Corollary 16. *If* C *is a classical linear* $[n, k, d]_q$ *code containing its dual,* $C^\perp \leq C$*, then there exists an* $[[n, 2k - n, \geq d]]_q$ *stabilizer code that is pure to* d*.*

We will use Lemma 15 and Corollary 16 to derive many families of quantum error-correcting codes based on BCH, RS, duadic, and projective geometry codes as shown in the following sections.

2. Codes over $\mathbb{F}_{q^2}$.

We can also extend the connection of the quantum codes and classical codes that are defined over $\mathbb{F}_{q^2}$, especially as it allows us the use of codes over quadratic extension fields. The binary case was done in [30] and partial generalizations were done in [83, 109] and [123]. We provide a slightly alternative generalization using a trace-alternating form. Let (β, β^q) denote a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. We define a trace-alternating form of two vectors v and w in $\mathbb{F}_{q^2}^n$ by

$$(v|w)a = \mathrm{tr}_{q/p}\left(\frac{v \cdot w^q - v^q \cdot w}{\beta^{2q} - \beta^2}\right). \tag{3.13}$$

The argument of the trace is an element of $\mathbb{F}_q$ as it is invariant under the Galois automorphism $x \mapsto x^q$.

Let $\phi : \mathbb{F}_q^{2n} \longrightarrow \mathbb{F}_{q^2}^n$ take $(\mathbf{a}|\mathbf{b}) \mapsto \beta\mathbf{a}+\beta^q\mathbf{b}$. The map ϕ is isometric in the sense that the symplectic weight of $(\mathbf{a}|\mathbf{b})$ is equal to the Hamming weight of $\phi((\mathbf{a}|\mathbf{b}))$. This map allows us to transform the trace-symplectic duality into trace-alternating duality. In particular it can be easily verified that if $c, d \in \mathbb{F}_q^{2n}$, then $< c, | \, d > s = (\phi(c), |, \phi(d))a$. If $D \leq \mathbb{F}_{q^2}^n$, then we denote its trace-alternating dual by $D^{\perp_a} = \{v \in \mathbb{F}_{q^2}^n \mid (v|w)a = 0 \text{ for all } w \in D\}$. Now Theorem 14 can be reformulated as:

Theorem 17. *An $((n, K, d))_q$ stabilizer code exists if and only if there exists an additive subcode D of $\mathbb{F}_{q^2}^n$ of cardinality $|D| = q^n/K$ such that $D \leq D^{\perp_a}$ and $\mathrm{wt}(D^{\perp_a} \setminus D) = d$ if $K > 1$ (and $\mathrm{wt}(D^{\perp_a}) = d$ if $K = 1$).*

Proof. From Theorem 14 we know that an $((n, K, d))_q$ stabilizer code exists if and only if there exists a code $C \leq \mathbb{F}_q^{2n}$ such that $|C| = q^n/K$, $C \leq C^{\perp_s}$, and $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ if $K > 1$ (and $\mathrm{swt}(C^{\perp_s}) = d$ if $K = 1$). The theorem follows simply by applying the isometry ϕ. □

If we restrict our attention to linear codes over $\mathbb{F}_{q^2}$, then the hermitian form is more useful. The hermitian inner product of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_{q^2}^n$ is given by $\mathbf{x}^q \cdot \mathbf{y}$. From the definition of the trace-alternating form it is clear that if two vectors are orthogonal with respect to the hermitian form they are also orthogonal with respect to the trace-alternating form. Consequently, if $D \leq \mathbb{F}_{q^2}^n$, then $D^{\perp_h} \leq D^{\perp_a}$, where $D^{\perp_h} = \{v \in \mathbb{F}_{q^2}^n \mid v^q \cdot w = 0 \text{ for all } w \in D\}$.

Therefore, any self-orthogonal code with respect to the hermitian inner product is self-orthogonal with respect to the trace-alternating form. In general, the two dual spaces $D^{\perp_h}$ and $D^{\perp_a}$ are not the same. However, if D happens to be $\mathbb{F}_{q^2}$-linear, then the two dual spaces coincide.

Corollary 18. *If there exists an $\mathbb{F}_{q^2}$-linear $[n,k,d]_{q^2}$ code D such that $D^{\perp_h} \le D$, then there exists an $[[n, 2k-n, \ge d]]_q$ quantum code that is pure to d.*

Proof. Let $q = p^m$, p prime. If D is a k-dimensional subspace of $\mathbb{F}_{q^2}^n$, then $D^{\perp_h}$ is a $(n-k)$-dimensional subspace of $\mathbb{F}_{q^2}^n$. We can also view D as a $2mk$-dimensional subspace of $\mathbb{F}_p^{2mn}$, and $D^{\perp_a}$ as a $2m(n-k)$-dimensional subspace of $\mathbb{F}_p^{2mn}$. Since $D^{\perp_h} \subseteq D^{\perp_a}$ and the cardinalities of $D^{\perp_a}$ and $D^{\perp_h}$ are the same, we can conclude that $D^{\perp_a} = D^{\perp_h}$. The claim follows from Theorem 17. □

So it is sufficient to consider the hermitian form in case of $\mathbb{F}_{q^2}$-linear codes. For additive codes (that are not linear) over $\mathbb{F}_{q^2}$ we have to use the rather inconvenient trace-alternating form. Finally, using the hermitian construction, we will derive many families of quantum error-correcting codes in the following sections.

C. Bounds on Quantum Codes

We need some bounds on the achievable minimum distance of a quantum stabilizer code. Perhaps the simplest one is the Knill-LaFlamme bound, also called the quantum Singleton bound. The binary version of the quantum Singleton bound was first proved by Knill and Laflamme in [90], see also [15, 17], and later generalized by Rains using weight enumerators in [123].

Theorem 19 (Quantum Singleton Bound)**.** *An* $((n, K, d))_q$ *stabilizer code with* $K > 1$ *satisfies*

$$K \le q^{n-2d+2}. \tag{3.14}$$

All binary and nonbinary quantum codes obeys the quantum Singleton bound as shown in Theorem 19. In addition all pure and impure quantum codes satisfies this bound as well. Codes which meet the quantum Singleton bound are called quantum MDS codes. In [81], it was showed that these codes cannot be indefinitely long and the maximal length of a q-ary quantum MDS codes is upper bounded by $2q^2-2$. This could probably be tightened to q^2+2. It would be interesting to find quantum MDS codes of length greater than q^2+2 since it would disprove the MDS Conjecture for classical codes [75]. A related open question is regarding the construction of codes with lengths between q and q^2-1. At the moment there are no analytical methods for constructing a quantum MDS code of arbitrary length in this range (see [65] for some numerical results).

Another important bound for quantum codes is the quantum Hamming bound. The quantum Hamming bound states (see [46, 57]) that:

Theorem 20 (Quantum Hamming Bound)**.** *Any pure* $((n, K, d))_q$ *stabilizer code satisfies*

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q^2-1)^i \le q^n/K. \tag{3.15}$$

While the quantum Singleton bound holds for all quantum codes, it is not known if the quantum Hamming bound is of equal applicability. So far no degenerate quantum code has been found that beats this bound. Gottesman showed that impure binary quantum codes cannot beat the quantum Hamming bound [58].

In [17] Ashikhmin and Litsyn derived many bounds for quantum codes by extending a novel method originally introduced by Delsarte [41] for classical codes. Using this method they proved the binary versions of Theorem 20 and Theorem 19. We use this method to show that the Hamming bound holds for all double error-correcting quantum codes. See [81] for a similar result for single error-correcting codes. But first we need Theorem 21 and the Krawtchouk polynomial of degree j in the variable x,

$$K_j(x) = \sum_{s=0}^{j} (-1)^s (q^2-1)^{j-s} \binom{x}{s} \binom{n-x}{j-s}. \tag{3.16}$$

Theorem 21. *Let Q be an $((n,K,d))_q$ stabilizer code of dimension $K > 1$. Suppose that S is a nonempty subset of $\{0,\ldots,d-1\}$ and $N = \{0,\ldots,n\}$. Let*

$$f(x) = \sum_{i=0}^{n} f_i K_i(x) \tag{3.17}$$

be a polynomial satisfying the conditions

i) $f_x > 0$ for all x in S, and $f_x \geq 0$ otherwise;

ii) $f(x) \leq 0$ for all x in $N \setminus S$.

Then

$$K \leq \frac{1}{q^n} \max_{x \in S} \frac{f(x)}{f_x}. \tag{3.18}$$

Proof. See [81]. □

We demonstrate usefulness of the previous theorem by showing that the quantum Hamming bound holds for impure nonbinary codes when $d = 5$.

Lemma 22 (Quantum Hamming Bound)**.** *An $((n,K,5))_q$ stabilizer code with $K > 1$*

satisfies

$$K \leq q^n/(n(n-1)(q^2-1)^2/2 + n(q^2-1) + 1). \tag{3.19}$$

Proof. Let $f(x) = \sum_{j=0}^{n} f_j K_j(x)$, where $f_x = (\sum_{j=0}^{e} K_j(x))^2$, $S = \{0, 1, \ldots, 4\}$ and N={0,1,...,n}. Calculating $f(x)$ and f_x gives us

$$\begin{aligned}
f_0 &= (1 + n(q^2-1) + n(n-1)(q^2-1)^2/2)^2 \\
f_1 &= \frac{1}{4}(n-1)^2(n-2)^2(q^2-1)^4 \\
f_2 &= (\frac{1}{2}(n-3)(n-2)(q^2-1)^2 - (n-2)(q^2-1))^2 \\
f_3 &= (1 - 2(n-3)(q^2-1) + \frac{1}{2}(n-4)(n-3)(q^2-1)^2)^2 \\
f_4 &= (3 - 3(n-4)(q^2-1) + \frac{1}{2}(n-5)(n-4)(q^2-1)^2)^2
\end{aligned}$$

and,

$$\begin{aligned}
f(0) &= q^{2n}(1 + n(q^2-1) + \frac{1}{2}(n-1)n(q^2-1)^2) \\
f(1) &= q^{2n}(q^2 + 2(n-1)(q^2-1) + (n-1)(q^2-2)(q^2-1)) \\
f(2) &= q^{2n}(4 + 4(q^2-2) + (q^2-2)^2 + 2(n-2)(q^2-1)) \\
f(3) &= q^{2n}(6 + 6(q^2-2)) \\
f(4) &= 6q^{2n}.
\end{aligned}$$

Clearly $f_x > 0$ for all $x \in S$. Also, $f(x) \leq 0$ for all $x \in N \backslash S$ since the binomial coefficients for negative values are zero. The Hamming bound is given by

$$K \leq q^{-n} \max_{s \in S} \frac{f(x)}{f_x} \tag{3.20}$$

So, there are four different comparisons where $f(0)/f_0 \geq f(x)/f_x$, for $x = 1, 2, 3, 4$. We find a lower bound for n that holds for all values of q. For $n \geq 7$ it follows that

$$\max\{f(0)/f_0, f(1)/f_1, f(2)/f_2, f(3)/f_3, f(4)/f_4\} = f(0)/f_0 \tag{3.21}$$

$\square$

The detailed prove of Lemma 22 can be found in [2]. While the above method is a general method to prove Hamming bound for impure quantum codes, the number of terms increases with a large minimum distance. It becomes difficult to find the true bound using this method. However, one can derive more consequences from Theorem 21; see, for instance, [15, 17, 103, 110].

D. Perfect Quantum Codes

A quantum code that meets the quantum Hamming bound with equality is known as a perfect quantum code. In fact the famous $[[5,1,3]]_2$ code [99] is one such. We will show that there do not exist any pure perfect quantum codes other than the ones mentioned in the following theorem. It is actually a very easy result and follows from known results on classical perfect codes, but we had not seen this result earlier in the literature.

Theorem 23. *There do not exist any pure perfect quantum codes with distance greater than 3.*

Proof. Assume that Q is a pure perfect quantum code with the parameters $((n,K,d))_q$. Since it meets the quantum Hamming bound we have

$$\sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (q^2-1)^j = q^n/K. \tag{3.22}$$

By Theorem 17 the associated classical code C is such that $C^{\perp_a} \leq C \leq \mathbb{F}_{q^2}^n$ and has parameters $(n, q^nK, d)_{q^2}$. Its distance is d because the quantum code is pure. Now C obeys the classical Hamming bound (see [75, Theorem 1.12.1] or any textbook on classical codes). Hence

$$|C| = q^n K \leq \frac{q^{2n}}{\sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (q^2-1)^j}. \tag{3.23}$$

Substituting the value of K we see that this implies that C is a perfect classical code. But the only perfect classical codes with distance greater than 3 are the Golay codes and the repetition codes [75]. The perfect Golay codes are over $\mathbb{F}_2$ and $\mathbb{F}_3$ not over a quadratic extension field as C is required to be. The repetition codes are of dimension 1 and cannot contain their duals as C is required to contain. Hence C cannot be anyone of them. Therefore, there are no pure quantum codes of distance greater than 3 that meet the quantum Hamming bound. $\square$

Since it is not known if the quantum Hamming bound holds for nonbinary degenerate quantum codes with distance $d > 5$, it would be interesting to find degenerate quantum codes that either meet or beat the quantum Hamming bound [2]. This is obviously a challenging open research problem.

CHAPTER IV

QUANTUM BCH CODES

An attractive feature of BCH codes is that one can infer valuable information from their design parameters (length, size of the finite field, and designed distance), such as bounds on the minimum distance and dimension of the code. In this chapter, we show that one can also deduce from the design parameters whether or not a primitive, narrow-sense BCH contains its Euclidean or Hermitian dual code. This information is invaluable in the construction of quantum BCH codes. A new proof is provided for the dimension of BCH codes with small designed distance, and simple bounds on the minimum distance of such codes and their duals are derived as a consequence. These results allow us to derive the parameters of two families of primitive quantum BCH codes as a function of their design parameters. This chapter is based on a joint work with P.K. Sarvepalli and A. Klappenecker and it was presented in [8, 11].

A. BCH Codes

The Bose-Chaudhuri-Hocquenghem (BCH) codes [25, 26, 56, 72] are a well-studied class of cyclic codes that have found numerous applications in classical and more recently in quantum information processing. Recall that a cyclic code of length n over a finite field $\mathbb{F}_q$ with q elements, and $\gcd(n, q) = 1$, is called a *BCH code with designed distance* δ if its generator polynomial is of the form

$$g(x) = \prod_{z \in Z}(x - \alpha^z), \qquad Z = C_b \cup \cdots \cup C_{b+\delta-2},$$

where $C_x = \{xq^k \bmod n \,|\, k \in \mathbb{Z}, k \geq 0\}$ denotes the q-ary cyclotomic coset of x modulo n, α is a primitive element of $\mathbb{F}_{q^m}$, and $m = \mathrm{ord}_n(q)$ is the multiplicative order of q modulo n. Such a code is called primitive if $n = q^m - 1$, and narrow-sense if $b = 1$.

An attractive feature of a (narrow-sense) BCH code is that one can derive many structural properties of the code from the knowledge of the parameters n, q, and δ alone. Perhaps the most well-known facts are that such a code has minimum distance $d \geq \delta$ and dimension $k \geq n - (\delta - 1)\operatorname{ord}_n(q)$. In this chapter, we will show that a necessary condition for a narrow-sense BCH code which contains its Euclidean dual code is that its designed distance $\delta = O(qn^{1/2})$. We also derive a sufficient condition for dual containing BCH codes. Moreover, if the codes are primitive, these conditions are same. These results allow us to derive families of quantum stabilizer codes. Along the way, we find new results concerning the minimum distance and dimension of classical BCH codes.

To put our results into context, we give a brief overview of related work in quantum BCH codes. This chapter was motivated by problems concerning quantum BCH codes; specifically, our goal was to derive the parameters of the quantum codes as a function of the design parameters. Examples of certain binary quantum BCH codes have been given by many authors, see, for example, [30, 63, 64, 144]. Steane [145] gave a simple criterion to decide when a binary narrow-sense primitive BCH code contains its dual, given the design distance and the length of the code. We generalize Steane's result in various ways, in particular, to narrow-sense (not necessarily primitive) BCH codes over arbitrary finite fields with respect to Euclidean and Hermitian duality. These results allow one to derive quantum BCH codes; however, it remains to determine the dimension, purity, and minimum distance of such quantum codes.

The dimension of a classical BCH code can be bounded by many different standard methods, see [23, 75, 107] and the references therein. An upper bound on the dimension was given by Shparlinski [139], see also [94, Chapter 17]. More recently, the dimension of primitive narrow-sense BCH codes of designed distance $\delta < q^{\lceil m/2 \rceil} + 1$ was apparently determined by Yue and Hu [151], according to reference [150]. We generalize their result and determine the dimension of narrow-sense BCH codes for a certain range of designed distances. As desired, this result allows us to explicitly obtain the dimension of the quantum codes without computation of cyclotomic cosets.

The purity and minimum distance of a quantum BCH code depend on the minimum distance and dual distance of the associated classical code. In general, it is a difficult problem to determine the true minimum distance of BCH codes, see [32]. A lower bound on the dual distance can be given by the Carlitz-Uchiyama-type bounds when the number of field elements is prime, see, for example, [107, page 280] and [148]. Many authors have determined the true minimum distance of BCH codes in special cases, see, for instance, [116], [150].

We refer to such a code as a $\mathcal{BCH}(n, q; \delta)$ code, and call Z the defining set of the code. The basic properties of these classical codes are discussed, for example, in the books [75, 78, 107].

Given a classical BCH code, we can use one of the following well-known constructions to derive a quantum stabilizer code:

1. If there exists a classical linear $[n, k, d]_q$ code C such that $C^{\perp} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ stabilizer code that is pure to d. If the minimum distance of $C^{\perp}$ exceeds d, then the quantum code is pure and has minimum distance d.

2. If there exists a classical linear $[n, k, d]_{q^2}$ code D such that $D^{\perp_h} \subseteq D$, then there exists an $[[n, 2k-n, \geq d]]_q$ stabilizer code that is pure to d. If the minimum distance of $D^{\perp_h}$ exceeds d, then the quantum code is pure and has minimum distance d.

The orthogonality relations are defined in the *Notations* at the end of this section. Examples of certain binary quantum BCH codes have been given in [30, 64, 65, 144].

Our goal is to derive the parameters of the quantum stabilizer code as a function of their design parameters n, q, and δ of the associated primitive, narrow-sense BCH code C. This entails the following tasks:

a) Determine the design parameters for which $C^\perp \subseteq C$;

b) determine the dimension of C;

c) bound the minimum distance of C and $C^\perp$.

In case q is a perfect square, we would also like to answer the Hermitian versions of questions a) and c):

a') Determine the design parameters for which $C^{\perp_h} \subseteq C$;

c') bound the minimum distance of C and $C^{\perp_h}$.

To put our work into perspective, we sketch our results and give a brief overview of related work.

Let C be a primitive, narrow-sense BCH code C of length $n = q^m - 1$, $m \geq 2$, over $\mathbb{F}_q$ with designed distance δ.

To answer question a), we prove in Theorem 34 that $C^\perp \subseteq C$ holds if and only if $\delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$. The significance of this result is that allows one to identify all BCH codes that can be used in the quantum code construction 1). Fortunately, this question can be answered now without computations. Steane proved in [145] the special case $q = 2$, which is easier to show, since in this case there is no difference between even and odd m.

In Theorem 36, we answer question a') and show that $C^{\perp_h} \subseteq C$ if and only if $\delta \leq q^{(m+[m \text{ even}])/2} - 1 - (q-2)[m \text{ even}]$, where we assume that q is a perfect square. This result allows us to determine all primitive, narrow-sense BCH codes that can be used in construction 2). We are not aware of any prior work concerning the Hermitian case.

In the binary case, an answer to question b) was given by MacWilliams and Sloane [107, Chapter 9, Corollary 8]. Apparently, Yue and Hu answered question b) in the case of small designed distances [151]. We give a new proof of this result in Theorem 26 and show that the dimension $k = n - m\lceil(\delta-1)(1-1/q)\rceil$ for δ in the range $2 \leq \delta < q^{\lceil m/2 \rceil} + 1$. As a consequence of our answer to b), we obtain the dimensions of the quantum codes in constructions 1) and 2).

Finding the true minimum distance of BCH codes is an open problem for which a complete answer seems out of reach, see [32]. As a simple consequence of our answer to b), we obtain better bounds on the minimum distance for some BCH codes, and we derive simple bounds on the (Hermitian) dual distance of BCH codes with small designed distance, which partly answers c) and c').

In Section E, all these results are used to derive two families of quantum BCH codes. Impatient readers should now browse this section to get the bigger picture. Theorem 37 yields the result that one obtains using construction 1). Cohen, Encheva, and Litsyn derived in [37] the special case $q = 2$ of our theorem by combining the results of Steane, and MacWilliams and Sloane that we have mentioned already. The result of construction 2) is given in Theorem 38.

Notations. We denote the ring of integers by $\mathbf{Z}$ and a finite field with q elements by $\mathbf{F}_q$. We follow Knuth and attribute to $[P(k)]$ the value 1 if the property $P(k)$ of the integer k is true, and 0 otherwise. For instance, we have $[k \text{ even}] = k - 1 \bmod 2$, but the left hand side seems more readable. If x and y are vectors in $\mathbb{F}_q^n$, then we write $x \perp y$ if and only if $x \cdot y = 0$. Similarly, if x and y are vectors in $\mathbb{F}_{q^2}^n$, then we write $x \perp_h y$ if and only if $x^q \cdot y = 0$.

B. Dimension and Minimum Distance

In this section we determine the dimension of primitive, narrow-sense BCH codes of length n with small designed distance. Furthermore, we derive bounds on the minimum distance of such codes and their duals.

1. Dimension

First, we make some simple observations about cyclotomic cosets that are essential in our proof.

Lemma 24. *If q be a power of a prime, m a positive integer and $n = q^m - 1$, then all q-ary cyclotomic cosets $C_x = \{xq^\ell \bmod n \,|\, \ell \in \mathbb{Z}\}$ with x in the range $1 \le x < q^{\lceil m/2 \rceil} + 1$ have cardinality $|C_x| = m$.*

Proof. Seeking a contradiction, we assume that $|C_x| < m$. If $m = 1$, then C_x would have to be the empty set, which is impossible. If $m > 1$, then $|C_x| < m$ implies that there must exist an integer j in the range $1 \le j < m$ such that j divides m and $xq^j \equiv x \mod n$. In other words, $q^m - 1$ divides $x(q^j - 1)$; hence, $x \ge (q^m - 1)/(q^j - 1)$.

If m is even, then $j \le m/2$; thus, $x \ge q^{m/2} + 1$. If m is odd, then $j \le m/3$ and it follows that $x \ge (q^m - 1)/(q^{m/3} - 1)$, and it is easy to see that the latter term is larger than $q^{\lceil m/2 \rceil} + 1$. In both cases this contradicts our assumption that $1 \le x \le q^{\lceil m/2 \rceil}$; hence $|C_x| = m$. □

Lemma 25. *Let q be a power of a prime, m a positive integer, and $n = q^m - 1$. Let x and y be integers in the range $1 \le x, y < q^{\lceil m/2 \rceil} + 1$ such that $x, y \not\equiv 0 \bmod q$. If $x \ne y$, then the q-ary cosets of x and y modulo n are disjoint, i.e., $C_x \ne C_y$.*

Proof. Seeking a contradiction, we assume that $C_x = C_y$. This assumption implies that $y \equiv xq^\ell \bmod n$ for some integer ℓ in the range $1 \le \ell < m$.

If $xq^\ell < n$, then $xq^\ell \equiv 0 \bmod q$; this contradicts our assumption $y \not\equiv 0 \bmod q$, so we must have $xq^\ell \geq n$. It follows from the range of x that ℓ must be at least $\lfloor m/2 \rfloor$.

If $\ell = \lfloor m/2 \rfloor$, then we cannot find an admissible x within the given range such that $y \equiv xq^{\lfloor m/2 \rfloor} \bmod n$. Indeed, it follows from the inequality $xq^{\lfloor m/2 \rfloor} \geq n$ that $x \geq q^{\lceil m/2 \rceil}$, so x must equal $q^{\lceil m/2 \rceil}$, but that contradicts $x \not\equiv 0 \bmod q$. Therefore, ℓ must exceed $\lfloor m/2 \rfloor$.

Let us write x as a q-ary number $x = x_0 + x_1 q + \cdots + x_{m-1} q^{m-1}$, with $0 \leq x_i < q$. Note that $x_0 \neq 0$ because $x \not\equiv 0 \bmod q$. If $\lfloor m/2 \rfloor < \ell < m$, then xq^ℓ is congruent to $y_0 = x_{m-\ell} + \cdots + x_{m-1} q^{\ell-1} + x_0 q^\ell + \cdots + x_{m-\ell-1} q^{m-1}$ modulo n. We observe that $y_0 \geq x_0 q^\ell \geq q^{\lceil m/2 \rceil}$. Since $y \not\equiv 0 \bmod q$, it follows that $y = y_0 \geq q^{\lceil m/2 \rceil} + 1$, contradicting the assumed range of y. □

The previous two observations about cyclotomic cosets allow us to derive a closed form for the dimension of a primitive BCH code. This result generalizes binary case [107, Corollary 9.8, page 263]. See also [147] which gives estimates on the dimension of BCH codes among other things.

Theorem 26. *A primitive, narrow-sense BCH code of length $q^m - 1$ over $\mathbb{F}_q$ with designed distance δ in the range $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$ has dimension*

$$k = q^m - 1 - m\lceil (\delta - 1)(1 - 1/q) \rceil. \tag{4.1}$$

Proof. The defining set of the code is of the form $Z = C_1 \cup C_2 \cdots \cup C_{\delta-1}$, a union of at most $\delta - 1$ consecutive cyclotomic cosets. However, when $1 \leq x \leq \delta - 1$ is a multiple of q, then $C_{x/q} = C_x$. Therefore, the number of cosets is reduced by $\lfloor (\delta-1)/q \rfloor$. By Lemma 25, if $x, y \not\equiv 0 \bmod q$ and $x \neq y$, then the cosets C_x and C_y are disjoint. Thus, Z is the union of $(\delta - 1) - \lfloor (\delta-1)/q \rfloor = \lceil (\delta-1)(1-1/q) \rceil$ distinct cyclotomic cosets. By Lemma 24 all these cosets have cardinality m. Therefore, the degree of the generator polynomial is $m\lceil(\delta-1)(1-1/q)\rceil$, which proves our claim about the dimension of the code. □

If we exceed the range of the designed distance in the hypothesis of the previous theorem, then our dimension formula (4.1) is no longer valid, as our next example illustrates.

Example 27. *Consider a primitive, narrow-sense BCH code of length $n = 4^2-1 = 15$ over $\mathbb{F}_4$. If we choose the designed distance $\delta = 6 > 4^1+1$, then the resulting code has dimension $k = 8$, because the defining set Z is given by*

$$Z = C_1 \cup C_2 \cup \cdots \cup C_5 = \{1,4\} \cup \{2,8\} \cup \{3,12\} \cup \{5\}.$$

The dimension formula (4.1) yields $4^2-1-2\lceil(6-1)(1-1/4)\rceil = 7$, so the formula does not extend beyond the range of designed distances given in Theorem 26.

2. Distance Bounds

The true minimum distance d_{min} of a primitive BCH code over $\mathbb{F}_q$ with designed distance δ is bounded by $\delta \leq d_{min} \leq q\delta - 1$, see [107, p. 261]. If we apply the Farr bound (essentially the sphere packing bound) using the dimension given in Theorem 26, then we obtain:

Corollary 28. *If C is primitive, narrow-sense BCH code of length q^m-1 over $\mathbb{F}_q$ with designed distance δ in the range $2 \leq \delta \leq q^{\lceil m/2\rceil}+1$ such that*

$$\sum_{i=0}^{\lfloor(\delta+1)/2\rfloor} \binom{q^m-1}{i}(q-1)^i > q^{m\lceil(\delta-1)(1-1/q)\rceil}, \tag{4.2}$$

then C has minimum distance $d = \delta$ or $\delta+1$; if, furthermore, $\delta \equiv 0 \bmod q$, then $d = \delta+1$.

Proof. Seeking a contradiction, we assume that the minimum distance d of the code satisfies $d \geq \delta + 2$. We know from Theorem 26 that the dimension of the code is $k = q^m - 1 - m\lceil(\delta-1)(1-1/q)\rceil$. If we substitute this value of k into the sphere-packing bound

$$q^k \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{q^m-1}{i}(q-1)^i \leq q^n,$$

then we obtain

$$\begin{aligned} \sum_{i=0}^{\lfloor (\delta+1)/2 \rfloor} \binom{q^m-1}{i}(q-1)^i &\leq \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{q^m-1}{i}(q-1)^i \\ &\leq q^{m\lceil(\delta-1)(1-1/q)\rceil}, \end{aligned}$$

but this contradicts condition (4.2); hence, $\delta \leq d \leq \delta + 1$.

If $\delta \equiv 0 \bmod q$, then the cyclotomic coset C_δ is contained in the defining set Z of the code because $C_\delta = C_{\delta/q}$. Thus, the BCH bound implies that the minimum distance must be at least $\delta + 1$. □

Corollary 29. *A primitive, narrow sense BCH code of length $n = q^m - 1$ over $\mathbb{F}_q$ with designed distance δ in the range $2 \leq \delta \leq q^{\lceil m/2 \rceil} + 1$ that satisfies*

$$n < \sum_{i=0}^{k-1} \left\lceil \frac{\delta+1}{q^i} \right\rceil, \qquad \text{with} \qquad k = n - m\lceil(\delta-1)(1-1/q)\rceil, \tag{4.3}$$

has minimum distance δ.

Proof. This follows from Theorem 26 and the Griesmer bound. □

Remark. The two competing requirements on the designed distance in the hypothesis of this corollary limit its applicability. We can use the same proof technique for codes with larger minimum distance if we replace k in equation (4.3) by a suitable bound. Generalizing our observations about cyclotomic cosets in the previous section could improve the trivial bound $k \geq q^m - 1 - m(\delta - 1)$.

Example 30. *Consider a primitive, narrow-sense BCH code of length* $n = 3^2 - 1$ *over* F_3. *Let* $\delta = 4$, *it can be seen that* $\sum_{i=0}^{2} 2^i \begin{pmatrix} 8 \\ i \end{pmatrix} > 3^4$. *This means that condition (4.2) holds, then by Corollary 28, the code of length 8 and designed distance* $\delta = 4$ *has a minimum distance* $d_{min} = 4$. *To verify that, let us construct a primitive narrow-sense BCH code with length* $n = 8$ *and designed distance* $\delta = 4$. *We have* $k = q^m - 1 - m\lceil 2t(1-1/q)\rceil = 4$ *and the generator polynomial is* $g(x) = 2 + x + x^3 + x^4$ *and the parity check polynomial is* $h(x) = 1 + x + x^2 + 2x^3 + x^4$.

So, $h_R(x) = 1 + 2x + x^2 + x^3 + x^4$ *and the parity check matrix is*

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

by subtracting columns 4 and 5 then add the result to columns 1 and 2, we found that the min distance for this matrix H is 4 that verifies our claim in Corollary 28 where $2t + 1 \equiv 0 \bmod 3$.

Lemma 31. *Suppose that C is a primitive, narrow-sense BCH code of length* $n = q^m - 1$ *over* $\mathbb{F}_q$ *with designed distance* $2 \le \delta \le \delta_{\max} = q^{\lceil m/2\rceil} - 1 - (q-2)[m \text{ odd}])$, *then the dual distance* $d^{\perp} \ge \delta_{\max} + 1$.

Proof. Let $N = \{0, 1, \dots, n-1\}$ and Z_δ be the defining set of C. We know that $Z_{\delta_{\max}} \supseteq Z_\delta \supset \{1, \dots, \delta - 1\}$. Therefore $N \setminus Z_{\delta_{\max}} \subseteq N \setminus Z_\delta$. Further, we know that $Z \cap Z^{-1} = \emptyset$ if $2 \le \delta \le \delta_{\max}$ from Lemma 33 and Theorem 34. Therefore, $Z_{\delta_{\max}}^{-1} \subseteq N \setminus Z_{\delta_{\max}} \subseteq N \setminus Z_\delta$.

Let T_δ be the defining set of the dual code. Then $T_\delta = (N \setminus Z_\delta)^{-1} \supseteq Z_{\delta_{\max}}$. Moreover $\{0\} \in N \setminus Z_\delta$ and therefore T_δ. Thus there are at l east $\delta_{\max}$ consecutive roots in T_δ. Thus the dual distance $d^\perp \geq \delta_{\max}+1$. □

Lemma 32. *Suppose that C is a primitive, narrow-sense BCH code of length $n = q^{2m}-1$ over $\mathbb{F}_{q^2}$ with designed distance $2 \leq \delta \leq \delta_{\max} = q^{m+[m\ even]}-1-(q^2-2)[m \text{ even}])$, then the dual distance $d^\perp \geq \delta_{\max}+1$.*

Proof. The proof is analogous to the one of Lemma 31; just keep in mind that the defining set Z_δ is invariant under multiplication by q^2 modulo n. □

C. Euclidean Dual Codes

Recall that the Euclidean dual code $C^\perp$ of a code $C \subseteq \mathbb{F}_q^n$ is given by $C^\perp = \{y \in \mathbb{F}_q^n \,|\, x \cdot y = 0 \text{ for all } x \in C\}$. Steane showed in [145] that a primitive binary BCH code of length 2^m-1 contains its dual if and only if its designed distance δ satisfies $\delta \leq 2^{\lceil m/2 \rceil}-1$. In this section we derive a similar condition for nonbinary BCH codes.

Lemma 33. *Suppose that $\gcd(n,q)=1$. A cyclic code of length n over $\mathbb{F}_q$ with defining set Z contains its Euclidean dual code if and only if $Z \cap Z^{-1} = \emptyset$, where Z^{-1} denotes the set $Z^{-1} = \{-z \bmod n \mid z \in Z\}$.*

Proof. See, for instance, [75, Theorem 4.4.11]. □

Theorem 34. *A primitive, narrow-sense BCH code of length q^m-1, with $m \geq 2$, over the finite field $\mathbb{F}_q$ contains its dual code if and only if its designed distance δ satisfies*

$$\delta \leq \delta_{\max} = q^{\lceil m/2 \rceil}-1-(q-2)[m \text{ odd}].$$

Proof. Let $n = q^m-1$. The defining set Z of a primitive, narrow-sense BCH code C of designed distance δ is given by $Z = C_1 \cup C_2 \cdots \cup C_{\delta-1}$, where $C_x = \{xq^j \bmod n \mid j \in \mathbf{Z}\}$.

1. We will show that the code C cannot contain its dual code if the designed distance $\delta > \delta_{\max}$. Seeking a contradiction, we assume that the defining set Z contains the set $\{1, \ldots, s\}$, where $s = \delta_{\max}$. By Lemma 33, it suffices to show that $Z \cap Z^{-1}$ is not empty. If m is even, then $s = q^{m/2} - 1$, and Z^{-1} contains the element $-sq^{m/2} \equiv q^{m/2} - 1 \equiv s \bmod n$, which means that $Z \cap Z^{-1} \neq \emptyset$; contradiction. If m is odd, then $s = q^{(m+1)/2} - q + 1$, and the element given by $-sq^{(m-1)/2} \equiv q^{(m+1)/2} - q^{(m-1)/2} - 1 \bmod n$ is contained in Z^{-1}. Since this element is less than s for $m \geq 3$, it is contained in Z, so $Z \cap Z^{-1} \neq \emptyset$; contradiction. Combining these two cases, we can conclude that $\delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ is odd}]$ for $m \geq 2$.

2. For the converse, we prove that if $\delta \leq \delta_{\max}$, then $Z \cap Z^{-1} = \emptyset$, which implies $C^{\perp} \subseteq C$ by Lemma 33. It suffices to show that $\min C_{-x} \geq \delta_{\max}$ for any coset C_x in Z. Since $1 \leq x < \delta_{\max} \leq q^{\lceil m/2 \rceil} - 1$, we can write x as a q-ary integer of the form $x = x_0 + x_1 q + \cdots + x_{m-1} q^{m-1}$ with $0 \leq x_i < q$, and $x_i = 0$ for $i \geq \lceil m/2 \rceil$. If $\bar{y} = n - x$, then $\bar{y} = \bar{y}_0 + \bar{y}_1 q + \cdots + \bar{y}_{m-1} q^{m-1} = \sum_{i=0}^{m-1} (q - 1 - x_i) q^i$. Set $y = \min C_{-x}$. We note that y is a conjugate of $\bar{y}$. Thus, the digits of y are obtained by cyclically shifting the digits of $\bar{y}$.

3a) First we consider the case when m is even. Then the q-ary expansion of x has at least $m/2$ zero digits. Therefore, at least $m/2$ of the $\bar{y}_i$ are equal to $q - 1$. Thus, $y \geq \sum_{i=0}^{m/2-1} (q-1) q^i = q^{m/2} - 1 = \delta_{\max}$.

3b) If m is odd, then as $1 \leq x < q^{(m+1)/2} - q + 1$, we have $m > 1$ and $\bar{y} = \bar{y}_0 + \bar{y}_1 q + \cdots + (\bar{y}_{(m-1)/2}) q^{(m-1)/2} + (q-1) q^{(m+1)/2} + \cdots + (q-1) q^{m-1}$. For $0 \leq j \leq (m-1)/2$, we observe that $xq^j < n$, and since $\bar{y} q^j \equiv -xq^j \bmod n, \bar{y} q^j = n - xq^j \geq q^m - 1 - (q^{(m+1)/2} - q) q^{(m-1)/2} = q^{(m+1)/2} - 1 \geq \delta_{\max}$. For $(m+1)/2 \leq j \leq m - 1$, we find that

$$\begin{aligned}\bar{y}q^j \bmod n &= \bar{y}_{m-j} + \cdots + \bar{y}_{(m-1)/2}q^{j-(m+1)/2}\\ &+ (q-1)q^{j-(m-1)/2} + \cdots + (q-1)q^{j-1}\\ &+ \bar{y}_0 q^j + \cdots + \bar{y}_{m-j-1}q^{m-1},\\ &\geq (q^{(m-1)/2}-1)q^{j-(m-1)/2} + \bar{y}_0 + \cdots\\ &+ \bar{y}_{(m-1)/2},\\ &\geq q^{(m+1)/2} - q + 1 = \delta_{\max},\end{aligned}$$

where $\bar{y}_0 + \cdots + \bar{y}_{(m-1)/2} \geq 1$ because $x < q^{(m+1)/2} - q + 1$. Hence $y = \min\{\bar{y}q^j \mid j \in \mathbf{Z}\} \geq \delta_{\max}$ when m is odd.

Therefore a primitive BCH code contains its dual if and only if $\delta \leq \delta_{\max}$, for $m \geq 2$. □

D. Hermitian Dual Codes

If the cardinality of the field is a perfect square, then we can define another type of orthogonality relation for codes. Recall that if the code C is a subspace of the vector space $\mathbb{F}_{q^2}^n$, then its Hermitian dual code $C^{\perp_h}$ is given by $C^{\perp_h} = \{y \in \mathbb{F}_{q^2}^n \mid y^q \cdot x = 0 \text{ for all } x \in C\}$, where $y^q = (y_1^q, \ldots, y_n^q)$ denotes the conjugate of the vector $y = (y_1, \ldots, y_n)$. The goal of this section is to establish when a primitive, narrow-sense BCH code contains its Hermitian dual code.

Lemma 35. *Assume that* $\gcd(n,q) = 1$. *A cyclic code of length* n *over* $\mathbb{F}_{q^2}$ *with defining set* Z *contains its Hermitian dual code if and only if* $Z \cap Z^{-q} = \emptyset$, *where* $Z^{-q} = \{-qz \bmod n \mid z \in Z\}$.

Proof. Let $N = \{0, 1, \ldots, n-1\}$. If $g(z) = \prod_{x \in Z}(z - \alpha^x)$ is the generator polynomial of a cyclic code C, then $h^\dagger(z) = \prod_{x \in N \setminus Z}(z - \alpha^{-qx})$ is the generator polynomial of $C^{\perp_h}$.

Thus, $C^{\perp_h} \subseteq C$ if and only if $g(z)$ divides $h^\dagger(z)$. The latter condition is equivalent to $Z \subseteq \{-qx \mid x \in N \setminus Z\}$, which can also be expressed as $Z \cap Z^{-q} = \emptyset$. □

Theorem 36. *A primitive, narrow-sense BCH code of length $q^{2m}-1$ over $\mathbb{F}_{q^2}$, where $m \neq 2$, contains its Hermitian dual code if and only if its designed distance δ satisfies*

$$\delta \leq \delta_{\max} = q^{m+[m\ even]} - 1 - (q^2-2)[m\ even].$$

Proof. Let $n = q^{2m}-1$. Recall that the defining set Z of a primitive, narrow-sense BCH code C over the finite field $\mathbb{F}_{q^2}$ with designed distance δ is given by $Z = C_1 \cup \cdots \cup C_{\delta-1}$ with $C_x = \{xq^{2j} \bmod n \mid j \in \mathbb{Z}\}$.

1. We will show that the code C cannot contain its Hermitian dual code if the designed distance $\delta > \delta_{\max}$. Seeking a contradiction, we assume that the defining set Z contains $\{1, \ldots, s\}$, where $s = \delta_{\max}$. By Lemma 35, it suffices to show that $Z \cap Z^{-q}$ is not empty. If m is odd, then $s = q^m - 1$. Notice that $n - qsq^{2(m-1)/2} = q^m - 1 = s$, which means that $s \in Z \cap Z^{-q}$, and this contradicts our assumption that this set is empty. If m is even, then $s = q^{m+1} - q^2 + 1$. We note that $n - qsq^{m-2} = q^{m+1} - q^{m-1} - 1 < s = q^{m+1} - q^2 + 1$, for $m > 2$. It follows that $q^{m+1} - q^{m-1} - 1 \in Z \cap Z^{-q}$, contradicting our assumption that this set is empty. Combining the two cases, we can conclude that s must be smaller than the value $q^{m+[m \text{ even}]} - 1 - (q^2-2)[m \text{ even}]$.

2. For the converse, we show that if $\delta < \delta_{\max}$, then $Z \cap Z^{-q} = \emptyset$, which implies $C^{\perp_h} \subseteq C$ thanks to Lemma 35. It suffices to show that $\min\{n - qC_x\} \geq \delta_{\max}$ or, equivalently, that $\max qC_x \leq n - \delta_{\max}$ holds for $1 \leq x \leq \delta - 1$.

3. If m is odd, then the q-ary expansion of x is of the form $x = x_0 + x_1 q + \cdots + x_{m-1}q^{m-1}$, with $x_i = 0$, for $m \leq i \leq 2m-1$ as $x < q^m - 1$. So at least m of the x_i are equal to zero, which implies $\max qC_x < q^{2m} - 1 - (q^m - 1) = n - \delta_{\max}$.

4. Let m be even and qxq^{2j} be the q^2-ary conjugates of qx. Since $x < q^{m+1} - q^2 + 1$, $x = x_0 + x_1 q + \cdots + x_m q^m$ and at least one of the $x_i \leq q-2$. If $0 \leq 2j \leq m-2$, then $qxq^{2j} \leq q(q^{m+1} - q^2)q^{m-2} = q^{2m} - q^{m+1} = n - q^{m+1} + 1 < n - \delta_{\max}$. If $2j = m$, then $qxq^m = x_{m-1} + x_m q + 0.q^2 + \cdots + 0.q^m + x_0 q^{m+1} \cdots + x_{m-2} q^{2m-1}$. We note that there occurs a consecutive string of $m-1$ zeros and because one of the $x_i \leq q-2$, we have $qxq^{2j} < n - q^2(q^{m-1} - 1) - 1 \leq n - \delta_{\max}$. For $m + 2 \leq 2j \leq 2m - 2$, we see that $qxq^{2j} < n - q^4(q^{m-1} - 1) < n - \delta_{\max}$.

Thus we can conclude that the primitive BCH codes contain their Hermitian duals when $\delta \leq q^{m+[m \text{ even}]} - 1 - (q^2 - 2)[m \text{ even}]$. $\square$

E. Families of Quantum BCH Codes

We use the results of the previous sections to prove the existence of quantum stabilizer codes. We use the CSS construction as shown in the previous Chapter.

Theorem 37. *If q is a power of a prime, and m and δ are integers such that $m \geq 2$ and $2 \leq \delta \leq \delta_{\max} = q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$, then there exists a quantum stabilizer code Q with parameters*

$$[[q^m - 1, q^m - 1 - 2m\lceil(\delta - 1)(1 - 1/q)\rceil, d_Q \geq \delta]]_q$$

that is pure up to δ. If $\mathcal{BCH}(n, q; \delta)$ has true minimum distance d, and $d \leq \delta_{\max}$, then Q is a pure quantum code with minimum distance $d_Q = d$.

Proof. Theorem 26 and 34 imply that there exists a classical BCH code with parameters $[q^m - 1, q^m - 1 - m\lceil(\delta - 1)(1 - 1/q)\rceil, \geq \delta]_q$ which contains its dual code. An $[n, k, d]_q$ code that contains its dual code implies the existence of the quantum code with parameters $[[n, 2k - n, \geq d]]_q$ by the CSS construction, see [65], [64]. By

Lemma 31, the dual distance exceeds $\delta_{\max}$; the statement about the purity and minimum distance is an immediate consequence. □

Theorem 38. *If q is a power of a prime, m is a positive integer, and δ is an integer in the range $2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2-2)[m \text{ even}]$, then there exists a quantum code Q with parameters*

$$[[q^{2m}-1, q^{2m}-1-2m\lceil(\delta-1)(1-1/q^2)\rceil, d_Q \geq \delta]]_q$$

that is pure up to δ. If $\mathcal{BCH}(n,q^2;\delta)$ has true minimum distance d, with $d < \delta_{\max}$, then Q is a pure quantum code of minimum distance $d_Q = d$.

Proof. It follows from Theorems 26 and 36 that there exists a primitive, narrow-sense $[q^{2m}-1, q^{2m}-1-m\lceil(\delta-1)(1-1/q^2)\rceil, \geq \delta]_{q^2}$ BCH code that contains its Hermitian dual code. Recall that if a classical $[n,k,d]_{q^2}$ code C exists that contains its Hermitian dual code, then there exists an $[[n, 2k-n, \geq d]]_q$ quantum code that is pure up to d, see [16]; this proves our claim. By Lemma 32, the Hermitian dual distance exceeds $\delta_{\max}$, which implies the last statement of the claim. □

F. Quantum BCH from Self-orthogonal Product Codes

It has been shown that product codes have a special interest because they have simple decoding algorithms and high bit rates. Furthermore, the Quantum BCH codes have much higher rates than the corresponding classical product codes. We apply an important result by Grassl [68, Theorem 5-8] in quantum block codes.

Let $C_i = [n_i, k_i, d_i]_q$ be a linear code over finite field $\mathbb{F}_q$ with generator matrix G_i for $i \in \{1,2\}$. Then the linear code $C = [n_1n_2, k_1k_2, d_1d_2]_q$ is the product code of $C_1 \otimes C_2$ with generator matrix $G = G_1 \otimes G_2$, see [49, 68, 113].

Lemma 39. *Let* $C_E \subseteq C_E^{\perp}$ *and* $C_H \subseteq C_H^{\perp}$ *denote two codes which are self-orthogonal with respect to the Euclidean and Hermitian inner products, respectively. Also, Let* C *and* D *denote arbitrary linear codes over* $\mathbb{F}_q$ *and* $\mathbb{F}_{q^2}$*, respectively. Then* $C \otimes C_E$ *and* $D \otimes C_H$ *are Euclidean and Hermitian self-orthogonal codes, respectively. Furthermore, the minimum distance of the dual of the product code* $C \otimes C_E$ $(D \otimes C_H)$ *cannot exceed the minimum distance of the dual distance of* $C(D)$ *and the dual distance of* $C_E(C_H)$.

Proof. See [68, Theorem 7, Corollary 6]. □

We can explicitly determine dimension of the new self-orthogonal product code if we know dimension of the original two self-orthogonal codes. Therefore, we apply our previous result in dimension of BCH codes as shown in section 2 into Lemmas 40 and 41.

Lemma 40. *Let* C_i *be a primitive narrow-sense BCH code with length* $n_i = q^{m_i} - 1$ *and designed distance* $2 \leq \delta_i \leq q^{\lceil m_i/2 \rceil} - 1 - (q-2)[m_i \text{ odd}]$ *over finite field* $\mathbb{F}_q$ *for* $i \in \{1, 2\}$*. Then the product code*

$$C_1 \otimes C_2^{\perp} = [n_1 n_2, k_1(n_2 - k_2), \geq \delta_1 \operatorname{wt}(C_2^{\perp})]_q$$

is self-orthogonal and its Euclidean dual code is

$$(C_1 \otimes C_2^{\perp})^{\perp} = [n_1 n_2, n_1 n_2 - k_1(n_2 - k_2), \geq \min(\operatorname{wt}(C_1^{\perp}), \delta_2)]_q$$

where $k_i = q^{m_i} - 1 - m_i \lceil (\delta_i - 1)(1 - 1/q) \rceil$ *and* $\operatorname{wt}(C_i^{\perp}) \geq \delta_i$.

Proof. We know that if $2 \leq \delta_2 \leq q^{m/2} - 1$, then C_2 contains its Euclidean dual as shown in Theorem 34. From [68, Theorem 5] and Lemma 39, we conclude that the product code $C_1 \otimes C_2^{\perp}$ is Euclidean self-orthogonal. □

Lemma 41. *Let $C_1 = [n, k, d]$ be a primitive narrow-sense BCH code with length $n = q^m - 1$ and designed distance $2 \leq \delta \leq q^{m/2} - 1$ over $\mathbb{F}_q$. Furthermore, let $C_2 = [q-1, q-\delta_2, \delta_2]$ be a self-orthogonal Reed-Solomon code. Then the product code*

$$C_1 \otimes C_2 = [(q-1)n, k(q-\delta_2), \geq \delta_1\delta_2]_q$$

is self-orthogonal with parameters

$$(C_1 \otimes C_2)^\perp = [(q-1)n, (q-1)n - k(q-\delta_2),$$
$$\geq \min(\mathrm{wt}(C_1^\perp), q-\delta_2)]_q$$

where $k = q^m - 1 - m\lceil(\delta_1 - 1)(1 - 1/q)\rceil$ and $\mathrm{wt}(C_1^\perp) \geq \delta_1$.

Proof. Since C_2 is a self-orthogonal code, then the dual code $C_2^\perp$ has minimum distance $q - \delta_2$ and dimension $\delta_2 - 1$. From [68, Theorem 5] and Lemma 39, we conclude that $C_1 \otimes C_2$ is self-orthogonal. The dual distance of $(C_1 \otimes C_2)^\perp$ comes from lemma 39 such that the dual distance of $C_2^\perp$ is $\mathrm{wt}(C_2^\perp) = q - \delta_2$. □

Now, we generalize the previous two lemmas to any arbitrary primitive BCH codes.

Lemma 42. *Let C_i be a primitive BCH code with length $n_i = q^{m_i} - 1$ and designed distance $2 \leq \delta_i \leq q^{\lceil m_i/2 \rceil} - 1 - (q-2)[m_i \text{ odd}]$ over $\mathbb{F}_q$ for $i \in \{1, 2\}$. Then the product code*

$$C_1 \otimes C_2 = [n_1 n_2, k_1 k_2, \geq \delta_1\delta_2]_q$$

is self-orthogonal with parameters

$$C_1^\perp \otimes C_2^\perp = [n_1 n_2, n_1 n_2 - k_1 k_2, \geq min(\delta_1^\perp, \delta_2^\perp)]_q$$

where $k_i = q_i^m - 1 - m_i\lceil(\delta_i - 1)(1 - 1/q)\rceil$ and $\delta_i^\perp \geq \delta_i$.

Proof. Direct conclusion and similar proof as Lemma 40. □

Note: Lemmas 41 and 40 can be extended to Hermitian self-orthogonal codes. Finally, we can construct families of quantum error-correcting codes using Lemmas 40 and 41.

Lemma 43. *Let C_i be a primitive narrow-sense BCH code with length $n_i = q^{m_i} - 1$ and designed distance $2 \leq \delta_i \leq q^{\lceil m_i/2 \rceil} - 1 - (q-2)[m_i \text{ odd}]$ over $\mathbb{F}_q$ for $i \in \{1, 2\}$. Furthermore, the product code*

$$C_1 \otimes C_2^{\perp} = [n_1 n_2, k_1(n_2 - k_2), \geq \delta_1 \operatorname{wt}(C_2^{\perp})]_q$$

is self-orthogonal where $k_i = q^{m_i} - 1 - m_i \lceil (\delta_i - 1)(1 - 1/q) \rceil$ and $\operatorname{wt}(C_i^{\perp}) \geq \delta_i$. Then there exists a quantum error-correcting codes with parameters

$$[[n_1 n_2, n_1 n_2 - 2k_1(n_2 - k_2), d_{min}]]_q.$$

Proof. The proof is a direct consequence. □

G. Conclusions and Discussion

We have investigated primitive, narrow-sense BCH codes in this chapter. A careful analysis of the cyclotomic cosets in the defining set of the code allowed us to derive a formula for the dimension of the code when the designed distance is small. We were able to characterize when primitive, narrow-sense BCH codes contain their Euclidean and Hermitian dual codes, and this allowed us to derive two series of quantum stabilizer codes.

BCH are an interesting class of codes because on in advance can choose their design parameters. In the following chapters, we will show that BCH can be used to derived families of unit memory quantum convolutional codes as well as families of subsystem codes.

It remains open problem to establish conditions when nonprimitive non-narrow sense BCH codes contain their Euclidean and Hermitian duals. In general, we do not know the exact minimum distance of a BCH code with given parameters.

BCH codes can be used to derive LDPC codes. One can represent elements of the finite field as zero vectors of the code length except at positions of power of those elements. In [13] we derive LDPC codes derived from nonprimitive BCH codes. This construction can be used to derive families of quantum LDPC codes.

CHAPTER V

QUANTUM DUADIC CODES

Good quantum codes, such as quantum MDS codes, are typically nondegenerate (pure), meaning that errors of small weight require active error-correction, which is—paradoxically—itself prone to errors. Decoherence free subspaces, on the other hand, do not require active error correction, but perform poorly in terms of minimum distance. In this chapter, examples of degenerate (impure) quantum codes are constructed that have better minimum distance than decoherence free subspaces and allow some errors of small weight that do not require active error correction. In particular, two new families of $[[n, 1, \geq \sqrt{n}]]_q$ degenerate quantum codes are derived from classical duadic codes. This chapter is based on a joint work with A. Klappenecker and P.K. Sarvepalli, see [7, 12]. I aim to provide enough details in classical duadic codes and degenerate quantum codes, so my results on quantum duadic codes will be readable.

A. Introduction

Suppose that q is a power of a prime p. Recall that an $[[n, k, d]]_q$ quantum stabilizer code Q is a q^k-dimensional subspace of $\mathbb{C}^{q^n}$ such that $\langle u|E|u\rangle = \langle v|E|v\rangle$ holds for any error operator E of weight $\mathrm{wt}(E) < d$ and all $|u\rangle, |v\rangle \in Q$, see [16,81] for details. The stabilizer code Q is called nondegenerate (or pure) if and only if $\langle v|E|v\rangle = q^{-n} \operatorname{tr} E$ holds for all errors E of weight $\mathrm{wt}(E) < d$ where tr is the trace of E; otherwise, Q is called degenerate. Recall that purity and nondegeneracy are equivalent notions in the case of stabilizer codes, see [30, 58].

In spite of the negative connotations of the term "degenerate", we will argue that degeneracy is an interesting and in some sense useful quality of a quantum code. Let us call an error nice if and only if it acts by scalar multiplication on the stabilizer code. Nice errors do not require any correction, which is a nice feature considering the fact that operational imprecisions of a quantum computer can introduce errors in a correction step (which is the main reason why elaborate fault-tolerant implementations are needed).

If we assume a depolarizing channel, then errors of small weight are more likely to occur than errors of large weight. If the stabilizer code Q is nondegenerate, then all nice errors have weight d or larger, so the most probable errors *all* require (potentially hazardous) active error correction. On the other hand, if the stabilizer code is degenerate, then there exist nice errors of weight less than the minimum distance. Given these observations, it would be particularly interesting to find degenerate stabilizer codes with many nice errors of small weight.

Although the first quantum error-correcting code by Shor was a degenerate $[[9,1,3]]_2$ stabilizer code, it turns out that most known quantum stabilizer code families provide pure codes. If one insists on a large minimum distance, then nondegeneracy seems more or less unavoidable (for example, quantum MDS codes are necessarily nondegenerate, see [123]). However, the fact that most known stabilizer codes do not have nice errors of small weight is the result of more pragmatic considerations.

Let us illustrate this last remark with the CSS construction; similar points can be made for other stabilizer code constructions. Suppose we start with a classical self-orthogonal $[n,k,d]_q$ code C, i.e., $C \subseteq C^\perp$, then one can obtain with the CSS construction an $[[n,n-2k,\delta]]_q$ stabilizer code, where $\delta = \mathrm{wt}(C^\perp \setminus C)$. Since we often do not know the weight distribution of the code C, the easiest way to obtain a stabilizer code with minimum distance at least δ_0 is to choose C such that its dual distance $d^\perp \geq \delta_0$, as this ensures $\delta \geq d^\perp \geq \delta_0$. However, since $C \subseteq C^\perp$, the side effect is that all nonscalar nice errors have a weight of at least $d \geq d^\perp \geq \delta_0$.

Our considerations above suggest a different approach. Since we would like to have nice errors of small weight, we start with a classical self-orthogonal code C that has a small minimum distance, but is chosen such that the vector of smallest Hamming weight in the difference set $C^{\perp} \setminus C$ is large. In general, it is of course difficult to find a good lower bound for the weights in this difference set.

We illustrate this approach for degenerate quantum stabilizer codes that are derived from classical duadic codes. Recall that the duadic codes generalize the quadratic residue codes, see [102], [140], [141]. We show that one can still obtain a surprisingly large minimum distance, considering the fact we start with classical codes that are really bad.

The chapter is organized as follows. In Section B, we recall basic properties of duadic codes. In Section C, we construct degenerate quantum stabilizer codes using the CSS construction. Finally, in Section D, we obtain further quantum stabilizer codes using the Hermitian code construction.

Notation Throughout this chapter, n denotes a positive odd integer. If a is an integer coprime to n, then we denote by $\mathrm{ord}_n(a)$ the multiplicative order of a modulo n. We briefly write $q \equiv \Box \bmod n$ to express the fact that q is a quadratic residue modulo n. We write $p^{\alpha} \| n$ if and only if the integer n is divisible by p^{α} but not by $p^{\alpha+1}$. If $\gcd(a,n) = 1$, then the map $\mu_a : i \mapsto ai \bmod n$ denotes a permutation on the set $\{0, 1, \ldots, n-1\}$. An element $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ is said to be even-like if $\sum_i c_i = 0$, and odd-like otherwise. A code $C \subseteq \mathbb{F}_q^n$ is said to be even-like if every codeword in C is even-like, and odd-like otherwise.

B. Classical Duadic Codes

In this section, we recall the definition and basic properties of duadic codes of length n over a finite field $\mathbb{F}_q$ such that $\gcd(n, q) = 1$. For each choice, we will obtain a quartet of codes: two even-like cyclic codes and two odd-like cyclic codes.

Let S_0, S_1 be the defining sets of two cyclic codes of length n over $\mathbb{F}_q$ such that

1. $S_0 \cap S_1 = \emptyset$,
2. $S_0 \cup S_1 = S = \{1, 2, \ldots, n-1\}$, and
3. $aS_i \bmod n = S_{(i+1 \bmod 2)}$ for some a coprime to n.

In particular, each S_i is a union of q-ary cyclotomic cosets modulo n. Since condition 3) implies $|S_0| = |S_1|$, we have $|S_i| = (n-1)/2$, whence n must be odd. The tuple $\{S_0, S_1, a\}$ is called a *splitting* of n given by the permutation μ_a.

Let α be a primitive n-th root of unity over $\mathbb{F}_q$. For $i \in \{0, 1\}$, the odd-like duadic code D_i is a cyclic code of length n over $\mathbb{F}_q$ with defining set S_i and generator polynomial

$$g_i(x) = \prod_{j \in S_i} (x - \alpha^j). \tag{5.1}$$

The even-like duadic code C_i is defined as the even-like subcode of D_i; thus, it is a cyclic code with defining set $S_i \cup \{0\}$ and generator polynomial $(x-1)g_i(x)$. The dimension of a cyclic code D_i of length n and generator polynomial $g_i(x)$ is given by

$$k_i = n - deg(g_i(x)). \tag{5.2}$$

The dimension of D_i is $(n+1)/2$ and that of C_i is $(n-1)/2$ respectively. Obviously $C_i \subset D_i$. We have the following results on the classical duadic codes.

Theorem 44. *Duadic codes of length n over $\mathbb{F}_q$ exist if and only if q is a quadratic residue modulo n, i.e., $q \equiv \square \bmod n$.*

Proof. This is well-known, see for example, [141, Theorem 1] or [75, Theorem 6.3.2, pages 220-221]. □

It is natural to ask when duadic codes are self-orthogonal, so that the CSS construction [30] can be used.

Lemma 45. *Let C_i and D_i be the even-like and odd-like duadic codes of length n over $\mathbb{F}_q$, where $i \in \{0, 1\}$. Then*

i) $C_i^\perp = D_i$ *if and only if* $-S_i \equiv S_{(i+1 \bmod 2)} \bmod n$.

ii) $C_i^\perp = D_{(i+1 \bmod 2)}$ *if and only if* $-S_i \equiv S_i \bmod n$.

Proof. See [75, Theorems 6.4.2-3] □

In other words, if the splitting is given by μ_{-1}, then the even-like duadic codes C_i are self-orthogonal. If μ_{-1} fixes the set S_i, then $C_1 \subset C_0^\perp = D_1$ and $C_0 \subset C_1^\perp = D_0$. This naturally raises the question when μ_{-1} gives a splitting of n and when it only fixes the codes. For some special cases of n this is known. When all prime factors of $n = \prod p_i^{m_i}$ are such that $p_i \equiv -1 \mod 4$, then we have the following result.

Lemma 46. *Let $n = \prod p_i^{m_i}$ be the prime factorization of an odd integer n, where each $m_i > 0$ and q is a quadratic residue modulo n. If every $p_i \equiv -1 \mod 4$, then all the splitters of n are given by μ_{-1}. On the other hand if at least one $p_i \equiv 1 \mod 4$, then there exists a splitting given by μ_a where $a \neq -1$.*

Proof. See [141, Theorem 8]. □

Although the weight distribution of a duadic code is not known in general, the following well-known fact gives partial information about the weights of odd-like codewords.

Lemma 47 (Square Root Bound)**.** *Let D_0 and D_1 be a pair of odd-like duadic codes of length n over $\mathbb{F}_q$. Then their minimum odd-like weights in both codes are same, say d_o. We have*

1. $d_o^2 \geq n$,

2. $d_o^2 - d_o + 1 \geq n$ if the splitting is given by μ_{-1}.

Proof. See [75, Theorem 6.5.2]. □

C. Quantum Duadic Codes – Euclidean Case

In this section, we derive quantum stabilizer codes from classical duadic code using the well-known CSS construction. Recall that in the CSS construction, the existence of an $[n, k_1]_q$ code C and an $[n, k_2]_q$ code D such that $C \subset D$ guarantees the existence of an $[[n, k_2 - k_1, d]]_q$ quantum stabilizer code with minimum distance $d = \min \mathrm{wt}\{(D \setminus C) \cup (C^\perp \setminus D^\perp)\}$.

1. Basic Code Constructions

Recall that two $\mathbb{F}_q$-linear codes C_1 and C_2 are said to be equivalent if and only if there exists a monomial matrix M and automorphism γ of $\mathbb{F}_q$ such that $C_2 = C_1 M \gamma$, see [75, page 25]. We denote equivalence of codes by $C_1 \sim C_2$. For us it is relevant that equivalent codes have the same weight distribution, see [75, page 25].

The permutation map $\mu_a : i \mapsto ai \bmod n$ also defines an action on polynomials in $\mathbb{F}_q[x]$ by $f(x)\mu_a = f(x^a)$. This induces an action on a cyclic code C over $\mathbb{F}_q$ by

$$C\mu_a = \{c(x)\mu_a \mid c(x) \in C\} = \{c(x^a) \mid c(x) \in C\}.$$

Lemma 48. *Let C be a cyclic code of length n over $\mathbb{F}_q$ with defining set T. If* $\gcd(a, n) = 1$, *then the cyclic code $C\mu_a$ has the defining set $a^{-1}T$. Furthermore, we* *have $C\mu_a \sim C$.*

Proof. This follows from the definitions, see also [75, Corollary 4.4.5] and [75, page 141]. $\square$

Theorem 49. *Let n be a positive odd integer, and let $q \equiv \square \bmod n$. There exist quantum duadic codes with the parameters $[[n,1,d]]_q$, where $d^2 \geq n$. If $\operatorname{ord}_n(q)$ is odd, then there also exist quantum duadic codes with minimum distance $d^2 - d + 1 \geq n$.*

Proof. Let $N = \{0, 1, \ldots, n-1\}$. If $q \equiv \square \bmod n$, then there exist duadic codes $C_i \subset D_i$, for $i \in \{0, 1\}$. Suppose that the defining set of D_i is given by S_i; thus, the defining set of the even-like subcode C_i is given by $S_i \cup \{0\}$. It follows that $C_i^{\perp}$ has defining set $-(N \setminus (\{0\} \cup S_i)) = -S_{(i+1 \bmod 2)}$. Using Lemma 48, we obtain $C_i^{\perp} = D_{(i+1 \bmod 2)}\mu_{-1} \sim D_{(i+1 \bmod 2)}$ and $D_i^{\perp} = C_{(i+1 \bmod 2)}\mu_{-1} \sim C_{(i+1 \bmod 2)}$. By the CSS construction, there exists an $[[n, (n+1)/2 - (n-1)/2, d]]_q$ quantum stabilizer code with minimum distance $d = \min\{\operatorname{wt}((D_i \setminus C_i) \cup (C_i^{\perp} \setminus D_i^{\perp}))\}$. Since $C_i^{\perp} \sim D_{(i+1 \bmod 2)}$ and $D_i^{\perp} \sim C_{(i+1 \bmod 2)}$, the minimum distance $d = \min\{\operatorname{wt}((D_i \setminus C_i) \cup (D_{(i+1 \bmod 2)} \setminus C_{(i+1 \bmod 2)})\}$, which is nothing but the minimum odd-like weight of the duadic codes; hence $d^2 \geq n$. If $\operatorname{ord}_n(q)$ is odd, then μ_{-1} gives a splitting of n [131, Lemma 5]. In this case, Lemma 47 implies that the odd-like weight d satisfies $d^2 - d + 1 \geq n$. $\square$

In the binary case, it is possible to derive degenerate codes with similar parameters using topological constructions [28, 51, 84], but the codes do not appear to be equivalent to the construction given here.

2. Degenerate Codes

The next result proves the existence of degenerate duadic quantum stabilizer codes. This results shows that the classical duadic codes, such as $C_i \subseteq D_i$, contain codewords of very small weight but their set difference $D_i \setminus C_i$ (and $C_i^\perp \setminus D_i^\perp$) does not. First we need the following lemma, which shows the existence of duadic codes of low distance.

It is always possible to construct a degenerate code of distance d and pure to 1 by the method discussed in [30, Theorem 6]; see also [81, Lemma 69]. An alternative method to construct impure codes is to use concatenation [30, 58]. However such a construction assumes the existence of a pure code of distance d. The families we propose here are based on classical codes whose distance is low compared to their quantum distance.

Theorem 50. *Let p be an odd prime and $q \equiv \Box \bmod p$. Let $t = \mathrm{ord}_p(q)$, and let z be such that $p^z \| q^t - 1$. Then for $m > 2z$, there exist degenerate $[[p^m, 1, d]]_q$ quantum codes pure to $d' \leq p^z < d$ with $d^2 \geq p^m$ and $d^2 - d + 1 \geq p^m$ if $p \equiv -1 \bmod 4$.*

Proof. The existence of quantum stabilizer codes with these parameters follows from Theorems 49, which combined cover the two cases $p \equiv \pm 1 \bmod 4$.

But d', the minimum distance of the underlying classical even-like duadic codes, is upper bounded by p^z, see [141, Theorem 6]. For $m > 2z$, the minimum distance d of the quantum code satisfies $d \geq p^{m/2} > p^z \geq d'$; thus, we have a degenerate quantum code. $\Box$

Our next goal is to find a generalization of Theorem 50 to lengths that are not necessarily prime powers.

Lemma 51. *Let $n = \prod p_i^{m_i}$ be an odd integer and $q \equiv \Box \bmod p_i$. If $t_i = \mathrm{ord}_{p_i}(q)$ and $p_i^{z_i} \| q^{t_i} - 1$, and $m_i > 2z_i$, then there exists a duadic code of length n and (even-like) minimum distance $\leq \min\{p_i^{z_i}\} < \sqrt{n}$.*

Proof. By Theorem 44 there exist duadic codes of lengths $p_i^{m_i}$ and by [141, Theorem 6] their minimum distance, d_i' is less than $p_i^{z_i}$. Since we know that the odd-like distance is $\geq p_i^{m_i/2} > p_i^{z_i}$, the minimum distance must be even-like. By [141, Theorem 4], there exists duadic codes of length $n = \prod p_i^{m_i}$ whose minimum distance $d' \leq \min\{d'_i\} \leq \min\{p_i^{z_i}\} < \prod p_i^{m_i/2} = \sqrt{n}$. Since this is less than the minimum odd-like distance, the minimum distance is even-like. $\square$

Theorem 52. *Let $n = \prod p_i^{m_i}$ be an odd integer and $q \equiv \square \bmod p_i$. Let $t_i = \mathrm{ord}_{p_i}(q)$, and let z_i be such that $p_i^{z_i} \| q^{t_i} - 1$. Then for $m_i > 2z_i$, there exists a degenerate $[[n, 1, d]]_q$ quantum code pure to $d' \leq \min\{p_i^{z_i}\} < d$ with $d^2 \geq n$. If $p_i \equiv -1 \bmod 4$, then $d^2 - d + 1 \geq n$.*

Proof. From Lemma 51, we know that there exist duadic codes of length n and minimum (even-like) distance $d' \leq \min\{p_i^{z_i}\} < \sqrt{n}$. From Theorem 49, we know there exists a quantum duadic code with parameters $[[n, 1, d]]$, where $d \geq \sqrt{n} > d'$. Hence, the quantum code is degenerate.

If $p_i \equiv -1 \bmod 4$, then by [141, Theorem 8], the permutation μ_{-1} gives a splitting for this code. Hence the odd-like distance must satisfy $d^2 - d + 1$. $\square$

Note that the previous result does not specify whether these duadic codes have a splitting given by μ_{-1}. Next we consider duadic codes when μ_{-1} leaves them invariant.

Theorem 53. *Let $q \equiv \square \bmod n$ such $n|(q^b + 1)$ for some b. Let $t_i = \mathrm{ord}_{p_i}(q)$, and let z_i be such that $p_i^{z_i} \| q^{t_i} - 1$. Then for $m_i > 2z_i$, there exists a degenerate $[[n, 1, d]]_q$ quantum code pure to $d' \leq \min\{p_i^{z_i}\} < d$ with $d^2 \geq n$.*

Proof. By Lemma 51, there exists a duadic code with minimum even-like distance $d' \leq \min\{p^{z_i}\}$. But Theorem [141, Theorem 3.2.10] tells us that this code is fixed by μ_{-1}. Now Theorem 49 implies that we can construct a $[[n, 1, d \geq \sqrt{n}]]_q$ quantum code. As $d' \leq \min\{p_i^{z_i}\} < \sqrt{n} \leq d$, we conclude that the quantum code is degenerate. $\square$

Example 54. *Let us consider binary quantum duadic codes of length* 7^m*. Note that* 2 *is a quadratic residue modulo* 7 *as* $4^2 \equiv 2 \mod 7$*. Since* $\mathrm{ord}_7(2) = 3$ *and* $7 \| 2^3 - 1$*, we have* $z = 1$*. By Theorem 52 for* $m \geq 2$ *there exist quantum codes with the parameters* $[[7^m, 1, d]]_2$*. As* $p = 7 \equiv -1 \mod 4$ *we have with* $d^2 - d + 1 \geq 7^m$*. But,* d'*, the distance of the (even-like) duadic codes is upper bounded by* $p^z = 7$*. Hence these codes are pure to* $d' \leq 7$*. Actually, using the fact that the true distance of the even-like codes is* 4 *[141] we can show that the quantum codes are pure to* 4*.*

D. Quantum Duadic Codes – Hermitian Case

Recall that if there exists an $\mathbb{F}_{q^2}$-linear $[n, k, d]_{q^2}$ code C such that $C^{\perp_h} \subseteq C$, then there exists an $[[n, 2k - n, \geq d]]_q$ quantum stabilizer code that is pure to d. In this section, we construct duadic quantum codes using this construction. Since $q^2 \equiv \Box \mod n$, duadic codes exist over $\mathbb{F}_{q^2}$ for all n, when $\gcd(n, q^2) = 1$. In this case, the splitting μ_{-q} plays a role analogous to that of μ_{-1} in the previous section.

1. Basic Code Constructions

Lemma 55. *Let* C_i *and* D_i *respectively be the even-like and odd-like duadic codes over* $\mathbb{F}_{q^2}$*, where* $i \in \{0, 1\}$*. Then* $C_i^{\perp_h} = D_i$ *if and only if there is a* q^2*-splitting of* n *given by* μ_{-q}*, that is,* $-qS_i \equiv S_{(i+1 \bmod 2)} \mod n$*.*

Proof. See [131, Theorem 4.4]. □

Lemma 56. *Let* $n = \prod p_i^{m_i}$ *be an odd integer such that* $\mathrm{ord}_n(q)$ *is odd. Then* μ_{-q} *gives a splitting of* n *over* $\mathbb{F}_{q^2}$*. In fact* μ_{-1} *and* μ_{-q} *give the same splitting. Otherwise* μ_q *gives a splitting of* n*.*

Proof. Suppose that $\{S_0, S_1, a\}$ be a splitting. We know that each S_i is an union of some q^2-ary cyclotomic cosets, so $q^2 S_i \equiv S_i \mod n$. Now $q^{\mathrm{ord}_n(q)} S_i \equiv S_i \mod n$.

If $\mathrm{ord}_n(q) = 2k+1$, then $q^{2k+1}S_i \equiv qS_i \equiv S_i \bmod n$; hence, μ_q fixes each S_i if the multiplicative order of q modulo n is odd.

Notice that if $\mathrm{ord}_n(q)$ is odd, then $\mathrm{ord}_n(q^2)$ is also odd. By [132, Lemma 5], we know that there exists a q^2-splitting of n given by μ_{-1} if and only if $\mathrm{ord}_n(q^2)$ is odd. Hence $-S_i \equiv S_{(i+1 \bmod 2)} \bmod n$. Since μ_q fixes S_i we have $-qS_i \equiv S_{(i+1 \bmod 2)} \bmod n$; hence, μ_{-q} gives a q^2-splitting of n.

Conversely, if μ_{-q} gives a splitting of n, then $-qS_i \equiv S_{(i+1 \bmod 2)} \bmod n$. But as μ_q fixes S_i we have $-S_i \equiv S_{(i+1 \bmod 2)} \bmod n$. Therefore μ_{-1} gives the same splitting as μ_{-q}. If $\mathrm{ord}_n(q) = 2k$, then $q^k = -1$. Hence, $q^k S_i \bmod n = -S_i \bmod n = S_{(i+1 \bmod 2)}$ because μ_{-1} gives a splitting of n. Because $\mu_{q^{2r}}$ fixes S_i, $k = 2w+1$ for some w. And $q^{2w+1}S_i \bmod n = qS_i \bmod n = -S_i = S_{(i+1 \bmod 2)}$. Thus μ_q gives a splitting of n. □

Theorem 57. *Let n be an odd integer such that $\mathrm{ord}_n(q)$ is odd. Then there exists an $[[n,1,d]]_q$ quantum code with $d^2 - d + 1 \geq n$.*

Proof. By Lemma 56, there exist duadic codes $C_i \subset D_i$ with splitting given by μ_{-q} and μ_{-1}. This means that the $C_i \subseteq C_i^{\perp_h} = D_i$ by Lemma 55. Hence there exists an $[[n, n-(n-1), d]]_q$ quantum code with $d = \mathrm{wt}(D_i \setminus C_i)$. As μ_{-1} gives a splitting, we have $d^2 - d + 1 \geq n$ by Lemma 47. □

2. Degenerate Codes

We construct a family of degenerate quantum codes that has a large minimum distance.

Theorem 58. *Let $n = \prod p_i^{m_i}$ be an odd integer with $\mathrm{ord}_n(q)$ odd and every $p_i \equiv -1 \bmod 4$. Let $t_i = \mathrm{ord}_{p_i}(q^2)$, and $p_i^{z_i} \| q^{2t_i} - 1$. Then for $m_i > 2z_i$, there exist degenerate quantum codes with parameters $[[n,1,d]]_q$ pure to $d' \leq \min\{p_i^{z_i}\} < d$ with $d^2 - d + 1 \geq n$.*

Proof. From Lemma 51 we know that there exists an even-like duadic code with parameters $[n, (n-1)/2, d']_{q^2}$ and $d' \leq \min\{p_i^{z_i}\}$.

Then by [141, Theorem 8], we know that for this code μ_{-1} gives a splitting. By Lemma 56, μ_{-q} also gives a splitting for this code. Hence by Theorem 57 this duadic code gives a quantum duadic code $[[n, 1, d]]_q$, which is impure as $d' \leq \min\{p_i^{z_i}\} < \sqrt{n} < d$. □

Finally, one can construct more quantum codes, for instance when $\mathrm{ord}_n(q)$ is even, by finding the conditions under which μ_{-q} gives a splitting of n.

Lemma 59. *Let n be an odd integer such that $gcd(n, q^{2i-1} + 1) = 1$ for some integer $1 \leq i \leq ord_n(q)$. Then μ_{-q} gives a splitting of n over $\mathbb{F}_{q^2}$.*

Proof. Assume w.l.g. that there exists $C_x \in S_0$ such that $-qC_x \bmod n \equiv C_x$ with $x \neq 0$. The proof is by contraction. Let $C_x = \{x, xq^2, xq^4, ..., xq^{2i}\}$, so, $-qx \equiv xq^{2i} \bmod n$. Hence, $-qx - xq^{2i} \bmod n \equiv 0$ or $-xq(1 + q^{2i-1}) \bmod n \equiv 0$. Since $gcd(n, q^{2i-1} + 1) = 1 = gcd(n, q)$ and $x < n$, then there is no integer solution for the last equation unless $x = 0$ that contradicts out assumption. Therefore, $-qC_x \bmod n \equiv C_y$. consequently, the lemma holds. □

Lemma 60. *Let n be an odd integer such that $gcd(n, q^{2i-1} + 1) = 1$ for some integer $1 \leq i \leq ord_n(q)$. Then there exists an $[[n, 1, d]]_q$ quantum code with $d^2 - d + 1 \geq n$.*

Proof. Direct conclusion and similar proof as Lemma 57 by using Lemma 59 and Lemma 55. □

Now, we relax the condition in lemma 59 by studying the case where $ord_n(q)$ is even.

Lemma 61. *Let $n = \prod p_i^{m_i}$ be an odd integer such that every $p_i \equiv 1 \bmod 4$ or $\mathrm{ord}_n(q)$ is even. If $n|(q^{2b}+1)$ for some integer b, Then μ_{-q} gives a splitting of n over $\mathbb{F}_{q^2}$ if μ_{-1} fixes $S_i \bmod n$.*

Proof. Let w.l.g. $1 \in S_0$. We show that $-q \notin S_0$. Suppose $-q \in S_0$, then $-qS_0 \equiv -q^{2i+1}S_0 \bmod n = S_0 = -S_0$ because μ_{-1} fixes S_0 and $1 \in S_0$. So, $q^{2i+1}S_0 \bmod n = S_0$ but this is contradiction since $ord_n(q)$ is even. Now, we construct all elements of S_0 and S_1 such that $S_0 \cap S_1 = \phi$.

Assume w.l.g. that there exist $C_x \in S_0$ and $C_y \in S_1$ such that $-qC_x \bmod n \equiv C_y$. let $C_x = \{x, xq^2, xq^4, ..., xq^{2i}\}$, so, $-qxq^{2i} \bmod n \equiv y \bmod n$ or $-xq^{2i+1} \bmod n \equiv y \bmod n$. Since $x \in C_x \in S_0$ and $y \in C_y \in S_1$ and consequently $q^{2i} = -1 \bmod n$. Using Lemma [140, Lemma 3.2.6.] and the fact that $ord_n(q)$ is even then $n|(q^{2b}+1)$ for some integer b. Indeed, μ_{-q} gives a splitting of n over F_{q^2}. ☐

E. Conclusion

The motivation for this work was that many good quantum error-correcting codes, such as quantum MDS codes, are typically pure and thus require active corrective steps for all errors of small Hamming weight. At the other extreme are decoherence free subspaces (see [105, 152]) that do not require any active error correction at all, but perform poorly in terms of minimum distance. We pointed out that degenerate quantum codes can form a compromise, namely they can reach larger minimum distances while allowing at least some nice errors of low weight that do not require active error correction.

We have constructed two families of quantum duadic codes with the parameters $[[n, 1, \geq \sqrt{n}]]_q$ and have shown that they contain large subclasses of degenerate quantum codes. Though these codes encode only one qubit, they are interesting because they demonstrate that there exist families of classical codes which can give rise to remarkable degenerate quantum codes. Since these code are cyclic, we know that there exist several nice errors of small weight. A more detailed study of the weight distribution of classical duadic codes can reveal which code are particularly interesting for quantum error-correction. We note that generalizations of duadic codes, such as triadic and polyadic codes, can be used to obtain degenerate quantum codes with higher rates.

CHAPTER VI

QUANTUM PROJECTIVE GEOMETRY CODES

In this chapter I study projective geometry codes over finite fields. I settle down conditions when these codes contain their dual codes, $C^{\perp} \subseteq C$. Consequently, using the CSS construction, I construct families of quantum error-correcting codes based on projective geometry codes. For further details see [133].

Lachaud [96–98] introduced projective Reed-Muller codes (PRM) over finite fields in 1988. Projective Reed-Muller (PRM) codes are a well-known class of projective geometry codes. I establish conditions when Projective Reed-Muller codes are self-orthogonal, hence I construct their corresponding quantum PRM codes. In addition, I study puncturing of these quantum PRM codes.

Notation: Let us denote by $\mathbf{F}_q[X_0, X_1, ..., X_m]$ the polynomial ring in $X_0, X_1, ..., X_m$ with coefficients in $\mathbf{F}_q$. Furthermore, let $\mathbf{F}_q[X_0, X_1, ..., X_m]_h^{\nu} \cup \{0\}$ be the vector space of homogeneous polynomials in $X_0, X_1, ..., X_m$ with coefficients in $\mathbf{F}_q$ with degree ν (cf. [18], [97], [142]). Let $P^m(\mathbf{F}_q)$ be the m-dimensional projective space over $\mathbf{F}_q$. We evaluate the function $f(P_i)$ at the projective points $P_i \in P^m(\mathbf{F}_q)$.

A. Projective Reed-Muller Codes

A Generalized Reed-Muller code (GRM), $C_\nu(m, q)$ over $\mathbf{F}_q$ of order $1 \leq \nu \leq m(q-1)$ and length q^m is defined as

$$\begin{aligned} C_\nu(m, q) &= \{(f(0), f(p_1), ..., f(P_{q^m-1}) \,|\, f(X_1, ..., X_m) \\ &\quad \in \mathbf{F}_q[X_1, ..., X_m], deg(f) \leq \nu\}. \end{aligned} \tag{6.1}$$

Lemma 62. *Generalized Reed-Muller (GRM) codes $C_\nu(m,q)$ over $\boldsymbol{F}_q$ of order $1 \leq \nu \leq (q-1)m$ have length $n = q^m$, dimension*

$$k(\nu) = \sum_{t=0}^{\nu} \sum_{j=0}^{n} (-1)^j \left(\begin{array}{c} m \\ \\ j \end{array} \right) \left(\begin{array}{c} t+m-jq-1 \\ \\ t-jq \end{array} \right) \tag{6.2}$$

and minimum distance $d(\nu) = (q-s)q^{m-r-1}$, where $\nu = (q-1)r + s$, $0 \leq s < (q-1)$ and $0 \leq r \leq m-1$.

Proof. See for instance [142] and [18, chapter 16].

$\square$

The Projective Reed-Muller code (PRM) over $\mathbf{F}_q$ of integer order ν and length $n = (q^{m+1}-1)/(q-1)$ is denoted by $\mathcal{P}_q(\nu, m)$ and defined as

$$\begin{aligned} \mathcal{P}_q(\nu, m) \quad &= \quad \{(f(P_1), ..., f(P_n) \,|\, f(X_0, ..., X_m) \in \mathbf{F}_q[X_0, ..., X_m]_h^\nu \cup \{0\}\}, \\ &\quad\quad \text{and } P_i \in P^m(\mathbf{F}_q) \text{ for } 1 \leq i \leq n. \end{aligned} \tag{6.3}$$

Lemma 63. *The projective Reed-Muller code $\mathcal{P}_q(\nu, m)$, $1 \leq \nu \leq m(q-1)$, is an $[n,k,d]_q$ code with length $n = (q^{m+1}-1)/(q-1)$, dimension*

$$k(\nu) = \sum_{\substack{t=\nu \bmod (q-1) \\ t \leq \nu}} \sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \tag{6.4}$$

and minimum distance $d(\nu) = (q-s)q^{m-r-1}$ where $\nu = r(q-1)+s+1$, $0 \leq s < q-1$

Proof. See [142, Theorem 1]. $\square$

The duals of PRM codes are also known and under some conditions they are also PRM codes. The following result gives more precise details.

Lemma 64. *Let $\nu^{\perp} = m(q-1) - \nu$, then the dual of $\mathcal{P}_q(\nu, m)$ is given by*

$$\mathcal{P}_q(\nu, m)^{\perp} = \begin{cases} \mathcal{P}_q(\nu^{\perp}, m) & \nu \not\equiv 0 \bmod (q-1) \\ \mathrm{Span}_{\boldsymbol{F}_q}\{1, \mathcal{P}_q(\nu^{\perp}, m)\} & \nu \equiv 0 \bmod (q-1) \end{cases} \tag{6.5}$$

Proof. See [142, Theorem 2]. □

As mentioned earlier our main methods of constructing quantum codes are the CSS construction and the Hermitian construction. This requires us to identify nested families of codes and/or self-orthogonal codes. First we identify when the PRM codes are nested i.e., we find out when a PRM code contains other PRM codes as subcodes.

Lemma 65. *If $\nu_2 = \nu_1 + k(q-1)$, where $k > 0$, then $\mathcal{P}_q(\nu_1, m) \subseteq \mathcal{P}_q(\nu_2, m)$ and* $\mathrm{wt}(\mathcal{P}_q(\nu_2, m) \setminus \mathcal{P}_q(\nu_1, m)) = \mathrm{wt}(\mathcal{P}_q(\nu_2, m))$.

Proof. In the finite field $\mathbb{F}_q$, we can replace any variable x_i by x_i^q, hence every function in $\mathbb{F}_q[x_0, x_1, \ldots, x_m]_{\nu}^h$ is present in $\mathbb{F}_q[x_0, x_1, \ldots, x_m]_{\nu+k(q-1)}^h$. Hence $\mathcal{P}_q(\nu_1, m) \subseteq \mathcal{P}_q(\nu_2, m)$. Let $\nu_1 = r(q-1) + s + 1$, then $\nu_2 = (k+r)(q-1) + s + 1$. By Lemma 63, $d(\nu_1) = (q-s)q^{m-r-1} > (q-s)q^{m-r-k-1} = d(\nu_2)$. This implies that there exists a vector of weight $d(\nu_2)$ in $\mathcal{P}_q(\nu_2, m)$ and $\mathrm{wt}(\mathcal{P}_q(\nu_2, m) \setminus \mathcal{P}_q(\nu_1, m)) = \mathrm{wt}(\mathcal{P}_q(\nu_2, m))$. □

Example. Let $m = 1$, $q = 5$, so $n = (q^{m+1} - 1)/(q-1) = 6$. There are 6 points in this space $\{(0,1), (1,0), (1,1), (1,2), (1,3), (1,4)\}$. Therefore, in $\mathcal{P}_5(1,1)$, there are two codewords $\{(011111), (101234)\}$. Also, in $\mathcal{P}_5(5,1)$, there are 6 codewords

$$\{(011111), (001234), (001441), (001324), (001111), (101234)\},$$

Hence, the $\mathcal{P}_5(1,1) \subset \mathcal{P}_5(5,1)$ as shown in Lemma 65. Clearly, the code $\mathcal{P}_5(1,1)$ is not contained in $\mathcal{P}_5(2,1)$, $\mathcal{P}_5(3,1)$, or $\mathcal{P}_5(4,1)$.

B. Quantum Projective Reed-Muller Codes

We now construct stabilizer codes using the CSS and hermitian constructions.

Lemma 66. ***(CSS Construction)*** *Suppose given two classical linear codes* $C = [n, k_C, d_C]_q$ *and* $E = [n, k_E, d_E]_q$ *over* $\mathbf{F}_q$ *with* $C \subseteq E$*. Furthermore, let the minimum distance be* $d = \min wt\{(E \backslash C) \cup (C^\perp \backslash E^\perp)\}$ *if* $C \subset E$ *and* $d = \min wt\{C \cup C^\perp\}$ *if* $C = E$*, then there exists a* $[[n, k_E - k_C, d]]_q$ *quantum code.*

Proof. See for instance [134, Lemma 2].

□

Theorem 67. *Let* $n = (q^{m+1} - 1)/(q-1)$ *and* $1 \leq \nu_1 < \nu_2 \leq m(q-1)$ *such that* $\nu_2 = \nu_1 + l(q-1)$ *with* $\nu_1 \not\equiv 0 \bmod (q-1)$*. Then there exists an* $[[n, k(\nu_2) - k(\nu_1), \min\{d(\nu_2), d(\nu_1^\perp)\}]]_q$ *stabilizer code, where the parameters* $k(\nu)$ *and* $d(\nu)$ *are given in Theorem 63.*

Proof. A direct application of the CSS construction in conjunction with Lemma 65.

□

We do not need to use two pairs of codes as we had seen in the previous two cases, we could use a single self-orthogonal code for constructing a quantum code. We will illustrate this idea by finding self-orthogonal PRM codes.

Corollary 68. *Let* $0 \leq \nu \leq \lfloor m(q-1)/2 \rfloor$ *and* $2\nu \equiv 0 \bmod q-1$*, then* $\mathcal{P}_q(\nu, m) \subseteq \mathcal{P}_q(\nu, m)^\perp$*. If* $\nu \not\equiv 0 \bmod q-1$ *there exists an* $[[n, n-2k(\nu), d(\nu^\perp)]]_q$ *quantum code where* $n = (q^{m+1}-1)/(q-1)$*.*

Proof. We know that $\nu^\perp = m(q-1) - \nu$ and if $\mathcal{P}_q(\nu, m) \subseteq \mathcal{P}_q(\nu, m)^\perp$, then $\nu \leq \nu^\perp$ and by Lemma 65 $\nu^\perp = \nu + k(q-1)$ for some $k \geq 0$. It follows that $2\nu \leq \lfloor m(q-1)/2 \rfloor$ and $2\nu = (m-k)(q-1)$, i.e., $2\nu \equiv 0 \bmod q-1$. The quantum code then follows from Theorem 67. □

Hermitian Constructions. We can study Projective Reed-Muller codes generated over $\mathbf{F}_{q^2}$. We show that if a code is contained in its hermitian dual code, then there is a corresponding quantum PRM code. We define the hermitian inner product of two codewords c and c' as

$$\langle c \,|\, c' \rangle = X.\overline{Y} = \sum_{i=1}^{n} x_i \overline{y_i} = \sum_{i=1}^{n} x_i y_i^q \tag{6.6}$$

We say the code C is hermitian self-orthogonal if $C \subseteq C^{\perp_h}$ such that $\langle c \,|\, c' \rangle = 0$ for all codewords $c \in C$ and $c' \in C^{\perp_h}$.

Lemma 69. *Let $[n,k,d]_{q^2}$ be a linear PRM code such that $1 \leq \nu \leq m(q-1)$, then its contained in its hermitian dual (i.e. $PC_{q^2}(\nu,m) \subseteq PC_{q^2}(\nu,m)^{\perp_h}$).*

Lemma 70. *Given a PRM $PC_{q^2}(\nu,m)$ that is contained in its hermitian dual code $PC_{q^2}(\nu,m)^{\perp_h}$ with minimum distance $d = \min\{wt(C^{\perp_h} \backslash C)\}$, then there exists an $[[n, n-2k, d]]_q$ quantum stabilizer code.*

Proof. See for instance [65, Corollary 2] and [16, Corollary 1]. $\square$

Theorem 71. *Let $0 \leq \nu \leq m(q-1)$ and $\nu \not\equiv 0 \mod (q-1)$, there exist a quantum PRM code $[[n, n-2k(\nu), d(\nu^{\perp})]]_q$ with $n = (q^{2(m+1)}-1)/(q^2-1)$, where*

$$k(\nu) = \sum_{\substack{t = \nu \mod (q^2-1) \\ t \leq \nu}} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t+m-jq^2}{t-jq^2} \right) \tag{6.7}$$

and

$$d(\nu^{\perp}) = (q^2 - s) q^{2(m-r-1)} \tag{6.8}$$

such that $\nu - 1 = r(q^2-1) + s$, $0 \leq s < q^2 - 1$

Proof. We note that this code is constructed over $\mathbf{F}_{q^2}$, and $wt(PC_{q^2}(\nu, m)^\perp) = wt(PC_{q^2}(\nu, m)^{\perp_h}) = d(\nu^\perp)$. Applying Lemma 69 and Lemma 70, we construct a quantum code with parameters $[[n, n - 2k(\nu), d(\nu^\perp)]]_q$. □

C. Puncturing Quantum Codes

Finally we will briefly touch upon another important aspect of quantum code construction, which is the topic of shortening quantum codes. In the literature on quantum codes, there is not much distinction made between puncturing and shortening of quantum codes and often the two terms are used interchangeably. Obtaining a new quantum code from an existing one is more difficult task than in the classical case, the main reason being that the code must be so modified such that the resulting code is still self-orthogonal. Fortunately, however there exists a method due to Rains [123] that can solve this problem.

From Lemma 15 we know that with every quantum code constructed using the CSS construction, we can associate two classical codes, C_1 and C_2. Define C to be the direct product of $C_1^\perp$ and $C_2^\perp$ viz. $C = C_1^\perp \times C_2^\perp$. Then we can associate a puncture code $P(C)$ [71, Theorem 12] which is defined as

$$P(C) \quad = \quad \{(a_i b_i)_{i=1}^n \mid a \in C_1^\perp, b \in C_2^\perp\}^\perp. \tag{6.9}$$

Surprisingly, $P(C)$ provides information about the lengths to which we can puncture the quantum codes. If there exists a vector of nonzero weight r in $P(C)$, then the corresponding quantum code can be punctured to a length r and minimum distance greater than or equal to distance of the parent code.

Theorem 72. *Let* $0 \le \nu_1 < \nu_2 \le m(q-1) - 1$ *where* $\nu_2 \equiv \nu_1 \bmod q - 1$. *Also let* $0 \le \mu \le \nu_2 - \nu_1$ *and* $\mu \equiv 0 \bmod q - 1$. *If* $\mathcal{P}_q(\mu, m)$ *has codeword of weight*

r, then there exists an $[[r, \geq (k(\nu_2) - k(\nu_1) - n + r), \geq d]]_q$ quantum code, where $n = (q^m - 1)/(q - 1)$ $d = \min\{d(\nu_2), d(\nu_1^\perp)\}$. In particular, there exists a $[[d(\mu), \geq (k(\nu_2) - k(\nu_1) - n + d(\mu)), \geq d]]_q$ quantum code.

Proof. Let $C_i = \mathcal{P}_q(\nu_i, m)$ with ν_i as stated. Then by Theorem 67, an $[[n, k(\nu_2) - k(\nu_1), d]]_q$ quantum code Q exists where $d = \min\{d(\nu_2), d(\nu_1^\perp)\}$. From equation (6.9) we find that $P(C)^\perp = \mathcal{P}_q(\nu_1 + \nu_2^\perp, m)$, so

$$\begin{aligned} P(C) &= \mathcal{P}_q(m(q-1) - \nu_1 - \nu_2^\perp, m), \\ &= \mathcal{P}_q(\nu_2 - \nu_1, m). \end{aligned} \tag{6.10}$$

By [71, Theorem 11], if there exists a vector of weight r in $P(C)$, then there exists an $[[r, k', d']]_q$ quantum code, where $k' \geq (k(\nu_2) - k(\nu_1) - n + r)$ and distance $d' \geq d$. obtained by puncturing Q. Since $P(C) = \mathcal{P}_q(\nu_2 - \nu_1, m) \supseteq \mathcal{P}_q(\mu, m)$ for all $0 \leq \mu \leq \nu_2 - \nu_1$ and $\mu \equiv \nu_2 - \nu_1 \equiv 0 \bmod q-1$, the weight distributions of $\mathcal{P}_q(\mu, m)$ give all the lengths to which Q can be punctured. Moreover $P(C)$ will certainly contain vectors whose weight $r = d(\mu)$, that is the minimum weight of $PC(\mu, m)$. Thus there exist punctured quantum codes with the parameters $[[d(\mu), \geq (k(\nu_2) - k(\nu_1) - n + d(\mu)), \geq d]]_q$. □

D. Conclusion and Discussion

In this chapter, I drove families of quantum codes based on Projective Reed-Muller codes. In addition, I showed how to puncture the constructed quantum codes.

One can study similar classes of Euclidean geometry codes to derive new families of quantum error-correcting codes. For example, cyclic Reed-Muller [22], non-primitive Reed-Muller [24], Euclidean geometry codes [107, Chapter 13], [18] over finite fields are obvious extensions of the families given in this chapter. In addition one can investigate polynomial codes to derive a family of quantum codes based on polynomial codes [79].

CHAPTER VII

SUBSYSTEM CODES

Subsystem codes are a relatively new construction of quantum error control codes. Subsystem codes combine the features of decoherence free subspaces, noiseless subsystems, and quantum error-correcting codes. Such codes promise to offer appealing features, such as simple syndrome calculation and a wide variety of easily implementable fault-tolerant operations.

In this chapter I give an introduction to subsystem codes. I will show how to derive subsystem codes from classical codes that are not necessarily self-orthogonal (or dual-containing). I will establish the relationships between stabilizer and subsystem codes.

A. Introduction

Subsystem codes are a relatively new construction of quantum codes. Subsystem codes generalize the known constructions of active and passive quantum error control codes such as decoherence free subspaces, noiseless subsystems, and quantum stabilizer codes, see [80, 105, 136, 152]. The stabilizer formalism of subsystem codes can be found in [89, 95, 121]. Errors in subsystem codes not only can be corrected but also can be avoided. Subsystem codes promise to be useful for fault-tolerant quantum computation in comparison to stabilizer codes [1, 9].

The main purpose of subsystem codes is to simplify the known quantum codes specifically the stabilizer codes. The subsystem codes do not need the underlying classical codes to be self-orthogonal or dual containing as in the case of stabilizer codes. Furthermore, errors can be isolated into two subsystems. Therefore, they have less syndrome measurement and more efficient error corrections [19, 121]. We will show that many subsystem codes can be constructed easily from existing stabilizer codes that are available in [27, 30].

An $((n, K, R, d))_q$ subsystem code is a KR-dimensional subspace Q of $\mathbb{C}^{q^n}$ that is decomposed into a tensor product $Q = A \otimes B$ of a K-dimensional vector space A and an R-dimensional vector space B such that all errors of weight less than d can be detected by A. The vector spaces A and B are respectively called the subsystem A and the co-subsystem B. For some background on subsystem codes, see for instance [9, 86, 121].

Assume that we have a $[[n, k, r, d]]_q$ subsystem code Q that decomposes as $Q = A \otimes B$. In general Q is a subspace in the q^n-dimensional Hilbert space, $\mathbb{C}^{q^n}$, the information is stored on the correlations between all the n-qudits, and there is not necessarily a one to one correspondence between the logical qudits and the physical qudits. Similarly for the gauge qudits, i.e., co-subsystem B. But if there is a one to one correspondence between the physical qudits and the gauge qudits, say r' of them, then the subsystem A is essentially in the Hilbert space of $n - r'$ qudits, and we can discard the r' gauge qudits to obtain a $[[n - r', k, r - r', d]]_q$ subsystem code. We call those gauge qudits trivial gauge qudits. If all the gauge qudits can be identified with physical qudits, then we call such a subsystem code a *trivial subsystem code*. Such codes are no different from padding a stabilizer code with random qudits; nothing is to be gained from them. Further, we will assume that a nontrivial subsystem code has no trivial gauge qudits. We aim in this study to judge whether stabilizer codes are superior to subsystem codes.

There have been many families of stabilizer codes derived from classical self-orthogonal codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$, see for example [8, 30, 81]. But in the other hand, there are not many families of subsystem codes constructed yet, except [20]. This is because the theory is recently developed and it is a challenging task to find two

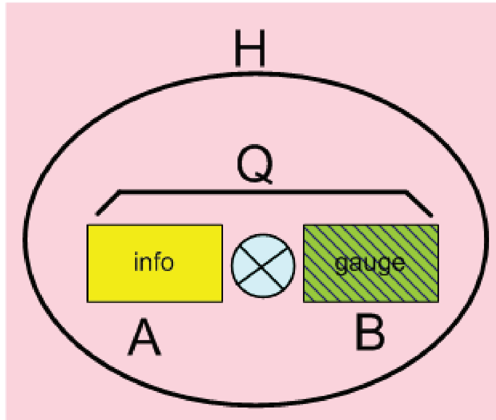


Fig. 2. A quantum code Q is decomposed into two subsystem A (info) and B (gauge)

classical codes such that dual of their intersection can lead to a subsystem code. Subsystem codes exist given particular stabilizer codes over $\mathbb{F}_q$.

Notation: Let q be a power of a prime integer p. For vectors x, y in $\mathbb{F}_q^n$, we define the Euclidean inner product $\langle x|y\rangle = \sum_{i=1}^{n} x_i y_i$ and the Euclidean dual of $C \subseteq \mathbb{F}_q^n$ as $C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x|y\rangle = 0 \text{ for all } y \in C\}$. We also define the hermitian inner product for vectors x, y in $\mathbb{F}_{q^2}^n$ as $\langle x|y\rangle_h = \sum_{i=1}^{n} x_i^q y_i$ and the hermitian dual of $C \subseteq \mathbb{F}_{q^2}^n$ as $C^{\perp_h} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}$. The trace-symplectic product of two elements $u = (a|b), v = (a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as $\langle u|v\rangle_s = \operatorname{tr}_{q/p}(a' \cdot b - a \cdot b')$, where $x \cdot y$ is the usual Euclidean inner product.The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as $C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w\rangle_s = 0 \text{ for all } w \in C\}$.

B. Subsystem Codes

Let $\mathcal{H}$ be the Hilbert space $\mathcal{H} = \mathbb{C}^{q^n} = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \ldots \otimes \mathbb{C}^q$. Let $|x\rangle$ be the vectors of orthonormal basis of $\mathbb{C}^q$, where the labels x are elements in the finite field $\mathbb{F}_q$. For

$a, b \in \mathbb{F}_q$, we define the unitary operators $X(a)$ and $Z(b)$ in $\mathbb{C}^q$ as follows:

$$X(a)\,|x\rangle = |x + a\rangle\,, \qquad Z(b)\,|x\rangle = \omega^{\mathrm{tr}(bx)}\,|x\rangle\,, \tag{7.1}$$

where $\omega = \exp(2\pi i/p)$ is a primitive pth root of unity and tr is the trace operation from $\mathbb{F}_q$ to $\mathbb{F}_p$

Now, we can define the set of error operators $E = \{X(a)Z(b)\,|\,a, b \in \mathbb{F}_q\}$ in an error group. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. Let us denote by

$$X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n) \text{ and },$$

$$Z(\mathbf{b}) = Z(b_1) \otimes \cdots \otimes Z(b_n)$$

the tensor products of n error operators. The set $\mathbf{E} = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ form an error basis on $\mathbb{C}^{q^n}$. We can define the error group $\mathbf{G}$ as follows

$$\mathbf{G} = \{\omega^c\mathbf{E} = \omega^c X(\mathbf{a})Z(\mathbf{b})\,|\,\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}. \tag{7.2}$$

Let Q be a quantum code such that $\mathcal{H} = Q \oplus Q^{\perp}$, where $Q^{\perp}$ is the orthogonal complement of Q. We can define the subsystem code $QA \otimes B$, see Fig.2, as follows

Definition 73. An $[[n, k, r, d]]_q$ subsystem code is a decomposition of the subspace Q into a tensor product of two vector spaces A and B such that $Q = A \otimes B$, where $\dim A = k$ and $\dim B = r$. The code Q is able to detect all errors of weight less than d on subsystem A.

Subsystem codes can be constructed from the classical codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. Such codes do not need the classical codes to be self-orthogonal (or dual-containing) as shown in the following theorem.

Theorem 74. *Let C be a classical additive subcode of $\mathbb{F}_q^{2n}$ such that $C \neq \{0\}$ and let D denote its subcode $D = C \cap C^{\perp_s}$. If $x = |C|$ and $y = |D|$, then there exists a* *subsystem code $Q = A \otimes B$ such that*

i) $\dim A = q^n/(xy)^{1/2}$,

ii) $\dim B = (x/y)^{1/2}$.

The minimum distance of subsystem A is given by

(a) $d = \mathrm{swt}((C + C^{\perp_s}) - C) = \mathrm{swt}(D^{\perp_s} - C)$ *if* $D^{\perp_s} \neq C$;

(b) $d = \mathrm{swt}(D^{\perp_s})$ *if* $D^{\perp_s} = C$.

Thus, the subsystem A can detect all errors in E of weight less than d, and can correct all errors in E of weight $\leq \lfloor (d-1)/2 \rfloor$.

Many subsystem codes can be derived based on the previous theorem as we will show in the next chapters.

C. Bounds on Pure Subsystem Code Parameters

We want to investigate some bounds and limitations on subsystem codes that can be constructed with the help of Theorem 74. It will be convenient to introduce first some standard notations for the parameters of the codes.

All stabilizer codes obey the quantum Singleton bound and all pure stabilizer codes also saturate the quantum Hamming bound. The conjecture where impure stabilizer codes obey or disobey quantum Hamming bound has been an open question. We will show that also pure subsystem codes obey Singleton and Hamming bounds.

Let X be an additive subcode of $\mathbb{F}_q^{2n}$ and $Y = X \cap X^{\perp_s}$. By Theorem 74, we can obtain an $((n, K, K', d))_q$ subsystem code Q from X that has minimum distance $d = \mathrm{swt}(Y^{\perp_s} - X)$. The set difference involved in the definition of the minimum distance make it harder to compute the minimum distance. Therefore, we introduce pure codes that are easier to analyze. Let d_p denote the minimum distance of the code X, that is, $d_p = \mathrm{swt}(X)$. Then we say that the associated subsystem code is *pure to*

d_p. Furthermore, we call Q a pure code if $d_p \geq d$, and an impure code otherwise.

Lemma 75. *If Theorem 74 allows one to construct a pure* $((n, K, K', d))_q$ *subsystem code* Q*, then there exists a pure* $((n, KK', d))_q$ *stabilizer code.*

Proof. Let X be a classical additive subcode of $\mathbb{F}_q^{2n}$ that defines Q, and let $Y = X \cap X^{\perp_s}$. Furthermore, Theorem 74 implies that $KK' = q^n/|Y|$. Since $Y \subseteq Y^{\perp_s}$, there exists an $((n, q^n/|Y|, d'))_q$ stabilizer code with minimum distance $d' = \mathrm{wt}(Y^{\perp_s} - Y)$. The purity of Q implies that $\mathrm{swt}(Y^{\perp_s} - X) = \mathrm{swt}(Y^{\perp_s}) = d$. As $Y \subseteq X$, it follows that $d' = \mathrm{swt}(Y^{\perp_s} - Y) = \mathrm{swt}(Y^{\perp_s}) = d$; hence, there exists a pure $((n, KK', d))_q$ stabilizer code. □

In Chapter VIII, we generalize Lemma 75 and also derive the converse.

1. Quantum Singleton Bound

The quantum Singleton bound for pure subsystem codes, not necessarily linear, can be stated as follows.

Theorem 76 (Singleton Bound.)**.** *Any pure* $((n, K, K', d))_q$ *subsystem code that is constructed using Theorem 74 satisfies the bound*

$$KK' \leq q^{n-2d+2}. \tag{7.3}$$

Proof. By Lemma 75, there exists a pure $((n, KK', d))_q$ stabilizer code. By the quantum Singleton bound, we have $KK' \leq q^{n-2d+2}$. □

Corollary 77. *A pure* $[[n, k, r, d]]_q$ *code satisfies* $k + r \leq n - 2d + 2$.

Our next goal is to show that in fact all $((n, q^{n-2d+2}, K', d))_q$ subsystem codes are pure. Note that $((n, q^{n-2d+2}, d))$ are the parameters of a quantum MDS code. An $[[n, k, r, d]]_q$ subsystem code derived from an $\mathbb{F}_q$-linear classical code $C \leq \mathbb{F}_q^{2n}$ satisfies the Singleton bound $k + r \leq n - 2d + 2$. A subsystem code attaining the Singleton bound with equality is called an MDS subsystem code.

An important consequence of the previous theorems is the following simple observation which yields an easy construction of subsystem codes that are optimal among the $\mathbb{F}_q$-linear Clifford subsystem codes.

Theorem 78. *Any* $[[n, n-2d+2, r, d]]_q$ *subsystem code is pure.*

Proof. Assume that there exists an $[[n, n-2d+2, r, d]]_q$ subsystem code that is impure. Then there exists an $(n, q^{n-k+r})_{q^2}$ classical code $X \subseteq \mathbb{F}_{q^2}^n$ and an $(n, q^{n-k-r})_{q^2}$ code $Y = X \cap X^{\perp_a}$ such that $k = n-2d+2 = \dim_{\mathbb{F}_{q^2}} Y^{\perp_a} - \dim_{\mathbb{F}_{q^2}} X$ and $\mathrm{wt}(Y^{\perp_a} \setminus X) = d$ and $\mathrm{wt}(X) = d' < d$. Then it is possible to construct a stabilizer code with distance $\geq d$ that is impure to d' by considering a self-orthogonal subcode $X \cap X^{\perp_a} \subseteq X' \subseteq X$ that includes a vector of weight d' such that $|X'| = q^{n-k}$. Such a subcode will always exist. Then the resulting stabilizer code is of parameters $[[n, n-2d+2, d]]_q$ and is impure. But we know that all quantum MDS codes are pure [123], see also [81, Corollary 60]. This implies that $d' \geq d$ contradicting that $d' < d$. Hence every $[[n, n-2d+2, r, d]]_q$ subsystem code is pure. □

A very straightforward consequence of Theorems 76 and 78 is the following corollary:

Lemma 79. *There exists no* $[[n, n-2d+2, r, d]]_q$ *subsystem code with* $r > 0$*.*

This still leaves a room for subsystem codes being superior to quantum block codes. For instance if a $[[11, 1, 8, 3]]_2$ code exists, then it is equivalent to a $[[3, 1, 3]]_2$ code which is superior to $[[5, 1, 3]]_2$ code. In addition, there does not exist an $[[11, 9, 3]]_2$ stabilizer code.

Theorem 80. *If there exists an $\mathbb{F}_q$-linear $[[n,k,d]]_q$ MDS stabilizer code, then there exists a pure $\mathbb{F}_q$-linear $[[n,k-r,r,d]]_q$ MDS subsystem code for all r in the range $0 \le r < k$.*

Proof. From Lemma 78, we know that the MDS stabilizer code with parameters $[[n,k,d]]_q$ exists and must be pure. Therefore it obey the quantum Singleton bound with equality. Therefore the pure subsystem code exists with parameters $[[n,k-r,r,d]]_q$ for $0 \le r < k$ and it must be an MDS code since it obeys the same bound with equality. □

2. Quantum Hamming Bound

We can also derive the quantum Hamming bound on subsystem code parameters. We can show that It is easy to derive a Hamming like bound for pure subsystem codes as stated in the following lemma.

Lemma 81 (Hamming Bound.)**.** *A pure $((n,K,K',d))_q$ code satisfies*

$$\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} (q^2-1)^j \le q^n/KK'. \tag{7.4}$$

Proof. By Lemma 75 a pure subsystem $((n,K,K',d))_q$ code implies the existence of a pure $((n,KK',d))_q$ code. But this obeys the quantum Hamming bound [46]. Therefore it follows that

$$\sum_{j=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} (q^2-1)^j \le q^n/KK'. \tag{7.5}$$

□

Recall that a pure subsystem code is called perfect if and only if it attains the Hamming bound with equality. We conclude this section with the following consequence lemma:

Lemma 82. *If there exists an $\mathbb{F}_q$-linear pure $[[n,k,d]]_q$ stabilizer code that is perfect, then there exists a pure $\mathbb{F}_q$-linear $[[n,k-r,r,d]]_q$ perfect subsystem code for all r in the range $0 \le r \le k$.*

Proof. Existence of an $\mathbb{F}_q$-linear pure stabilizer code with parameters $[[n,k,d]]_q$ implies existence of a subsystem code with parameters $[[n,k-r,r,d]]_q$ for $0 \le r < k$. But we know that the stabilizer code is perfect then

$$\sum_{j=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{j} (q^2-1)^j = q^{n-k} \tag{7.6}$$

By Lemma 81, it is a direct consequence that the subsystem code obeys this bound with equality. □

In the following chapters, we will give various methods to construct subsystem codes. In addition, we will derive many families of subsystem codes. We will give tables of upper and lower bounds on subsystem code parameters.

CHAPTER VIII

SUBSYSTEM CODE CONSTRUCTIONS

Subsystem codes are the most versatile class of quantum error-correcting codes known to date that combine the best features of all known passive and active error-control schemes. The subsystem code is a subspace of the quantum state space that is decomposed into a tensor product of two vector spaces: the subsystem and the co-subsystem. In this chapter, A generic method to derive subsystem codes from existing subsystem codes is given that allows one to trade the dimensions of subsystem and co-subsystem while maintaining or improving the minimum distance. As a consequence, it is shown that all pure MDS subsystem codes are derived from MDS stabilizer codes. The existence of numerous families of MDS subsystem codes is established.

A. Introduction

Subsystem codes are a relatively new construction of quantum codes that combine the features of decoherence free subspaces [105], noiseless subsystems [152], and quantum error-correcting codes [30, 57]. Such codes promise to offer appealing features, such as simplified syndrome calculation and a wide variety of easily implementable fault-tolerant operations, see [1, 9, 19, 95].

An $((n, K, R, d))_q$ subsystem code is a KR-dimensional subspace Q of $\mathbb{C}^{q^n}$ that is decomposed into a tensor product $Q = A \otimes B$ of a K-dimensional vector space A and an R-dimensional vector space B such that all errors of weight less than d can be detected by A. The vector spaces A and B are respectively called the subsystem A and the co-subsystem B. For some background on subsystem codes, see for instance [9, 86, 121].

A special feature of subsystem codes is that any classical additive code C can be used to construct a subsystem code. One should contrast this with stabilizer codes, where the classical codes are required to satisfy a self-orthogonality condition.

We assume that the reader is familiar with the relation between classical and quantum stabilizer codes, see [30, 123]. In [9, 86], the authors gave an introduction to subsystem codes, established upper and lower bounds on subsystem code parameters, and provided two methods for constructing subsystem codes. The main results on this paper are as follows:

i) If q is a power of a prime p, then we show that a subsystem code with parameters $((n, K/p, pR, \geq d))_q$ can be obtained from a subsystem code with parameters $((n, K, R, d))_q$. Furthermore, we show that the existence of a pure $((n, K, R, d))_q$ subsystem code implies the existence of a pure $((n, pK, R/p, d))_q$ code.

ii) We show that all pure MDS subsystem codes are derived from MDS stabilizer codes. We establish here for the first time the existence of numerous families of MDS subsystem codes.

B. Subsystem Code Constructions

First we recall the following fact that is key to most constructions of subsystem codes (see below for notations):

Theorem 83. *Let C be a classical additive subcode of $\mathbb{F}_q^{2n}$ such that $C \neq \{0\}$ and let D denote its subcode $D = C \cap C^{\perp_s}$. If $x = |C|$ and $y = |D|$, then there exists a subsystem code $Q = A \otimes B$ such that*

i) $\dim A = q^n/(xy)^{1/2}$,

ii) $\dim B = (x/y)^{1/2}$.

The minimum distance of subsystem A is given by

(a) $d = \mathrm{swt}((C + C^{\perp_s}) - C) = \mathrm{swt}(D^{\perp_s} - C)$ *if* $D^{\perp_s} \neq C$;

(b) $d = \mathrm{swt}(D^{\perp_s})$ *if* $D^{\perp_s} = C$.

Thus, the subsystem A *can detect all errors in* E *of weight less than* d*, and can correct all errors in* E *of weight* $\leq \lfloor (d-1)/2 \rfloor$.

A subsystem code that is derived with the help of the previous theorem is called a Clifford subsystem code. We will assume throughout this paper that all subsystem codes are Clifford subsystem codes. In particular, this means that the existence of an $((n, K, R, d))_q$ subsystem code implies the existence of an additive code $C \leq \mathbb{F}_q^{2n}$ with subcode $D = C \cap C^{\perp_s}$ such that $|C| = q^n R/K$, $|D| = q^n/(KR)$, and $d = \mathrm{swt}(D^{\perp_s} - C)$, see Fig. 3.

A subsystem code derived from an additive classical code C is called pure to d' if there is no element of symplectic weight less than d' in C. A subsystem code is called pure if it is pure to the minimum distance d. We require that an $((n, 1, R, d))_q$ subsystem code must be pure.

We also use the bracket notation $[[n, k, r, d]]_q$ to write the parameters of an $((n, q^k, q^r, d))_q$ subsystem code in simpler form. Some authors say that an $[[n, k, r, d]]_q$ subsystem code has r gauge qudits, but this terminology is slightly confusing, as the co-subsystem typically does not correspond to a state space of r qudits except perhaps in trivial cases. We will avoid this misleading terminology. An $((n, K, 1, d))_q$ subsystem code is also an $((n, K, d))_q$ stabilizer code and vice versa.

Notation. Let q be a power of a prime integer p. We denote by $\mathbb{F}_q$ the finite field with q elements. We use the notation $(x|y) = (x_1, \ldots, x_n|y_1, \ldots, y_n)$ to denote the concatenation of two vectors x and y in $\mathbb{F}_q^n$. The symplectic weight of $(x|y) \in \mathbb{F}_q^{2n}$ is defined as

$$\mathrm{swt}(x|y) = \{(x_i, y_i) \neq (0, 0) \,|\, 1 \leq i \leq n\}.$$

We define $\mathrm{swt}(X) = \min\{\mathrm{swt}(x) \,|\, x \in X, x \neq 0\}$ for any nonempty subset $X \neq \{0\}$

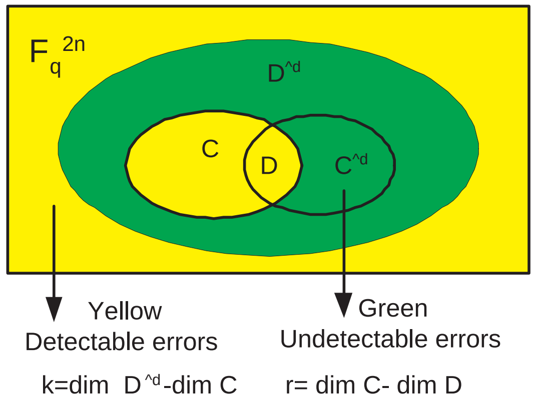


Fig. 3. Subsystem code parameters from classical codes

of $\mathbb{F}_q^{2n}$.

The trace-symplectic product of two vectors $u = (a|b)$ and $v = (a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as

$$\langle u|v\rangle_s = \mathrm{tr}_{q/p}(a' \cdot b - a \cdot b'),$$

where $x \cdot y$ denotes the dot product and $\mathrm{tr}_{q/p}$ denotes the trace from $\mathbb{F}_q$ to the subfield $\mathbb{F}_p$. The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as

$$C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w\rangle_s = 0 \text{ for all } w \in C\}.$$

We define the Euclidean inner product $\langle x|y\rangle = \sum_{i=1}^n x_i y_i$ and the Euclidean dual of $C \subseteq \mathbb{F}_q^n$ as

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x|y\rangle = 0 \text{ for all } y \in C\}.$$

We also define the Hermitian inner product for vectors x, y in $\mathbb{F}_{q^2}^n$ as $\langle x|y\rangle_h = \sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbb{F}_{q^2}^n$ as

$$C^{\perp_h} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}.$$

C. Trading Dimensions of Subsystem Codes

In this section we show how one can trade the dimensions of subsystem and co-subsystem to obtain new codes from a given subsystem or stabilizer code. The results are obtained by exploiting the symplectic geometry of the space. A remarkable consequence is that nearly any stabilizer code yields a series of subsystem codes.

Our first result shows that one can decrease the dimension of the subsystem and increase at the same time the dimension of the co-subsystem while keeping or increasing the minimum distance of the subsystem code.

Theorem 84. *Let q be a power of a prime p. If there exists an $((n,K,R,d))_q$ subsystem code with $K>p$ that is pure to d', then there exists an $((n,K/p,pR,\geq d))_q$ subsystem code that is pure to $\min\{d,d'\}$. If a pure $((n,p,R,d))_q$ subsystem code exists, then there exists a $((n,1,pR,d))_q$ subsystem code.*

Proof. By definition, an $((n,K,R,d))_q$ Clifford subsystem code is associated with a classical additive code $C\subseteq \mathbb{F}_q^{2n}$ and its subcode $D=C\cap C^{\perp_s}$ such that $x=|C|$, $y=|D|$, $K=q^n/(xy)^{1/2}$, $R=(x/y)^{1/2}$, and $d=\mathrm{swt}(D^{\perp_s}-C)$ if $C\neq D^{\perp_s}$, otherwise $d=\mathrm{swt}(D^{\perp_s})$ if $D^{\perp_s}=C$.

We have $q=p^m$ for some positive integer m. Since K and R are positive integers, we have $x=p^{s+2r}$ and $y=p^s$ for some integers $r\geq 1$, and $s\geq 0$. There exists an $\mathbb{F}_p$-basis of C of the form

$$C=\mathrm{span}_{\mathbb{F}_p}\{z_1,\dots,z_s,x_{s+1},z_{s+1},\dots,x_{s+r},z_{s+r}\}$$

that can be extended to a symplectic basis $\{x_1,z_1,\dots,x_{nm},z_{nm}\}$ of $\mathbb{F}_q^{2n}$, that is, $\langle x_k\,|\,x_\ell\rangle=0$, $\langle z_k\,|\,z_\ell\rangle=0$, $\langle x_k\,|\,z_\ell\rangle=\delta_{k,\ell}$ for all $1\leq k,\ell\leq nm$, see [38, Theorem 8.10.1].

Define an additive code

$$C_m = \mathrm{span}_{\mathbb{F}_p}\{z_1, \dots, z_s, x_{s+1}, z_{s+1}, \dots, x_{s+r+1}, z_{s+r+1}\}.$$

It follows that

$$C_m^{\perp_s} = \mathrm{span}_{\mathbb{F}_p}\{z_1, \dots, z_s, x_{s+r+2}, z_{s+r+2}, \dots, x_{nm}, z_{nm}\}$$

and

$$D = C_m \cap C_m^{\perp_s} = \mathrm{span}_{\mathbb{F}_p}\{z_1, \dots, z_s\}.$$

By definition, the code C is a subset of C_m.

The subsystem code defined by C_m has the parameters (n, K_m, R_m, d_m), where $K_m = q^n/(p^{s+2r+2}p^s)^{1/2} = K/p$ and $R_m = (p^{s+2r+2}/p^s)^{1/2} = pR$. For the claims concerning minimum distance and purity, we distinguish two cases:

(a) If $C_m \neq D^{\perp_s}$, then $K > p$ and $d_m = \mathrm{swt}(D^{\perp_s} - C_m) \geq \mathrm{swt}(D^{\perp_s} - C) = d$. Since by hypothesis $\mathrm{swt}(D^{\perp_s} - C) = d$ and $\mathrm{swt}(C) \geq d'$, and $D \subseteq C \subset C_m \subseteq D^{\perp_s}$ by construction, we have $\mathrm{swt}(C_m) \geq \min\{d, d'\}$; thus, the subsystem code is pure to $\min\{d, d'\}$.

(b) If $C_m = D^{\perp_s}$, then $K_m = 1 = K/p$, that is, $K = p$; it follows from the assumed purity that $d = \mathrm{swt}(D^{\perp_s} - C) = \mathrm{swt}(D^{\perp_s}) = d_m$.

This proves the claim. $\square$

For $\mathbb{F}_q$-linear subsystem codes there exists a variation of the previous theorem which asserts that one can construct the resulting subsystem code such that it is again $\mathbb{F}_q$-linear.

Theorem 85. *Let q be a power of a prime p. If there exists an $\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ subsystem code with $k > 1$ that is pure to d', then there exists an $\mathbb{F}_q$-linear $[[n, k-1, r+1, \geq d]]_q$ subsystem code that is pure to $\min\{d, d'\}$. If a pure $\mathbb{F}_q$-linear $[[n, 1, r, d]]_q$*

subsystem code exists, then there exists an $\mathbb{F}_q$-linear $[[n, 0, r+1, d]]_q$ subsystem code.

Proof. The proof is analogous to the proof of the previous theorem, except that $\mathbb{F}_q$-bases are used instead of $\mathbb{F}_p$-bases. □

There exists a partial converse of Theorem 84, namely if the subsystem code is pure, then it is possible to increase the dimension of the subsystem and decrease the dimension of the co-subsystem while maintaining the same minimum distance.

Theorem 86. *Let q be a power of a prime p. If there exists a pure $((n, K, R, d))_q$ subsystem code with $R > 1$, then there exists a pure $((n, pK, R/p, d))_q$ subsystem code.*

Proof. Suppose that the $((n, K, R, d))_q$ Clifford subsystem code is associated with a classical additive code

$$C_m = \operatorname{span}_{\mathbb{F}_p}\{z_1, \ldots, z_s, x_{s+1}, z_{s+1}, \ldots, x_{s+r+1}, z_{s+r+1}\}.$$

Let $D = C_m \cap C_m^{\perp_s}$. We have $x = |C_m| = p^{s+2r+2}$, $y = |D| = p^s$, hence $K = q^n/p^{r+s}$ and $R = p^{r+1}$. Furthermore, $d = \operatorname{swt}(D^{\perp_s})$.

The code

$$C = \operatorname{span}_{\mathbb{F}_p}\{z_1, \ldots, z_s, x_{s+1}, z_{s+1}, \ldots, x_{s+r}, z_{s+r}\}$$

has the subcode $D = C \cap C^{\perp_s}$. Since $|C| = |C_m|/p^2$, the parameters of the Clifford subsystem code associated with C are $((n, pK, R/p, d'))_q$. Since $C \subset C_m$, the minimum distance d' satisfies

$$d' = \operatorname{swt}(D^{\perp_s} - C) \leq \operatorname{swt}(D^{\perp_s} - C_m) = \operatorname{swt}(D^{\perp_s}) = d.$$

On the other hand, $d' = \operatorname{swt}(D^{\perp_s} - C) \geq \operatorname{swt}(D^{\perp_s}) = d$, whence $d = d'$. Furthermore, the resulting code is pure since $d = \operatorname{swt}(D^{\perp_s}) = \operatorname{swt}(D^{\perp_s} - C)$. □

Replacing $\mathbb{F}_p$-bases by $\mathbb{F}_q$-bases in the proof of the previous theorem yields the following variation of the previous theorem for $\mathbb{F}_q$-linear subsystem codes.

Theorem 87. *Let q be a power of a prime p. If there exists a pure $\mathbb{F}_q$-linear $[[n,k,r,d]]_q$ subsystem code with $r > 0$, then there exists a pure $\mathbb{F}_q$-linear $[[n,k+1,r-1,d]]_q$ subsystem code.*

The purity hypothesis in Theorems 86 and 87 is essential, as the next remark shows.

Remark 88. *The Bacon-Shor code is an impure $[[9,1,4,3]]_2$ subsystem code. However, there does not exist any $[[9,5,3]]_2$ stabilizer code. Thus, in general one cannot omit the purity assumption from Theorems 86 and 87, see also Fig. 4.*

An $[[n,k,d]]_q$ stabilizer code can also be regarded as an $[[n,k,0,d]]_q$ subsystem code. We record this important special case of the previous theorems in the next corollary.

Corollary 89. *If there exists an ($\mathbb{F}_q$-linear) $[[n,k,d]]_q$ stabilizer code that is pure to d', then there exists for all r in the range $0 \leq r < k$ an ($\mathbb{F}_q$-linear) $[[n,k-r,r,\geq d]]_q$ subsystem code that is pure to* $\min\{d,d'\}$ *. If a pure ($\mathbb{F}_q$-linear) $[[n,k,r,d]]_q$ subsystem code exists, then a pure ($\mathbb{F}_q$-linear) $[[n,k+r,d]]_q$ stabilizer code exists.*

This result makes it very easy to obtain subsystem codes from stabilizer codes. For example, if there is a stabilizer code with parameters $[[9,3,3]]_2$, then there are subsystem codes with parameters $[[9,1,2,3]]_2$ and $[[9,2,1,3]]_2$. The optimal stabilizer codes derived in [65,81] can all be converted to subsystem codes. These code families satisfy Singleton bound $k+2d = n+2$. An illustration of this corollary and families of subsystem codes based on RS codes are given in the next chapter.

From Subsystem to Stabilizer Codes. We have established a connection from stabilizer codes to subsystem codes as well as trading the dimensions between subsystem codes and co-subsystem codes. This result is applicable for both pure and impure stabilizer codes. Here we show that not all subsystem (co-subsystem) codes can be reduced to stabilizer codes. We gave a partial answer to this statement in [9]. We showed that pure subsystem codes can be converted to pure stabilizer codes as stated in Lemma 90.

Lemma 90. *If a pure $((n, K, R, d))_q$ subsystem code Q exists, then there exists a pure $((n, KR, d))_q$ stabilizer code.*

Proof. Let C be a classical additive subcode of $\mathbb{F}_q^{2n}$ that defines Q. The code

$$C = \operatorname{span}_{\mathbb{F}_p}\{z_1, \ldots, z_s, x_{s+1}, z_{s+1}, \ldots, x_{s+r}, z_{s+r}\}$$

has subcode $D = C \cap C^{\perp_s}$. We have $|C| = p^{s+2r}$ and $|D| = p^s$ for some integers $r \geq 1$, and $s \geq 0$. Furthermore, we know that $K = q^n/(|C||D|)^{1/2}$ and $R = \sqrt{|C|/|D|}$, then $KR = q^n/|D|$. Since $D \subseteq D^{\perp_s}$, there exists an $((n, q^n/|D|, d'))_q$ stabilizer code with minimum distance $d' = \operatorname{wt}(D^{\perp_s} - D)$. The purity of Q implies that $\operatorname{swt}(D^{\perp_s} - C) = \operatorname{swt}(D^{\perp_s}) = d$. As $D \subseteq C$, it follows that $d' = \operatorname{swt}(D^{\perp_s} - D) = \operatorname{swt}(D^{\perp_s}) = d$; hence, there exists a pure $((n, KR, d))_q$ stabilizer code. $\square$

Now, what we can say about the impure subsystem codes. It turns out that not every impure subsystem code can be transferred to a stabilizer code as shown in the following Lemma.

Lemma 91. *If an impure $((n, K, R, d))_q$ subsystem code Q exists, then there not necessarily exists an impure $((n, KR, d))_q$ stabilizer code.*

Proof. Let an impure $((n, K, R, d))_q$ subsystem code Q exists. We prove by contradiction that there is no impure $((n, KR, d))_q$ stabilizer code in general. The proof is shown by an example. We know that $[[9,1,4,3]]_2$ Becan-shor code is an impure code, which beats quantum Hamming bound for subsystem codes. If an $[[9,5,3]]_2$ stabilizer code exists, then it would not obey the quantum Hamming bound for quantum block codes. But, from the linear programming upper bound, there is no such $[[9,5,3]]$ over the binary field, see [30]. Therefore, not every impure subsystem code gives stabilizer code. $\square$

Subsystem versus Stabilizer Codes. There is a tradeoff between stabilizer and subsystem codes. We showed that one can reduce subsystem codes with parameters $[[n,k,r,d]]_q$ for $0 \leq r < k$ to stabilizer codes with parameters $[[n-r,k,d]]_q$. Also, pure subsystem codes with parameters $[[n,k,r,d]]_q$ give raise to stabilizer codes with parameters $[[n,k+r,d]]_q$. In the other hand, one can start with a stabilizer code with parameters $[[n,k,d]]_q$ and obtain a subsystem code with parameters $[[n,k-r,r,d]]_q$, for $0 \leq r < k$, see Corollary 89. The comparison between subsystem codes and stabilizer codes can be viewed as follows.

- Syndrome measurements. One way is to look at the number of syndrome measurements. Stabilizer codes need $n-k$ syndrome measurements while subsystem codes need $n-k-r$ for fixed n and d, as for example, the short subsystem code $[[8,2,1,3]]_2$ (or $[[8,1,2,3]]_2$).
- Subsystem codes may beat the Singleton and Hamming bound. There might exist subsystem codes that beat the quantum Singleton bound $k+r \leq n-2d+2$ and the quantum Hamming bound $\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i}(q^2-1)^i \leq q^n/KR$. We have not found any codes for small length $n \leq 50$, using MAGMA computer algebra, that beat the Singleton bound. Most likely there are no codes that beat this bound as we showed in case of linear pure subsystem codes in [9]. Pure subsystem codes obey the quantum Hamming bound. In the other hand, there are some impure subsystem

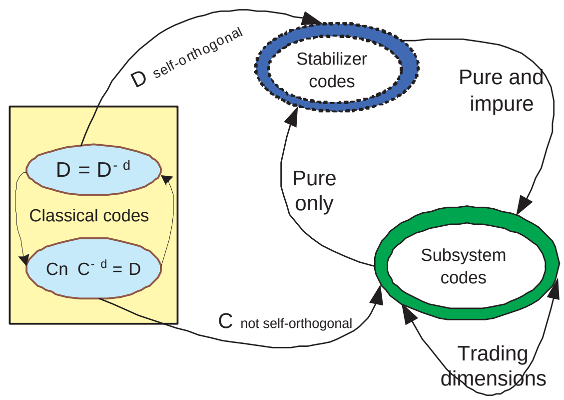


Fig. 4. Stabilizer and subsystem codes based on classical codes

codes that beat the quantum Hamming bound. For example, subsystem codes with parameters $[[9,1,4,3]]_2$, $[[25,1,16,5]]_2$, and $[[30,1,20,5]]_2$ do not obey the quantum Hamming bound. They are constructed using Bacon-Shor code constructions over $\mathbb{F}_2$. In fact, we found many subsystem codes that do not obey this bound and be easily derived from this construction.

- Encoding and decoding circuits. It has been shown that the encoding and decoding circuits of stabilizer codes can also be used in subsystem codes. The conjecture is that subsystem codes might have better efficient encoding and decoding circuits using benefit of the gauge qubits, see [20].
- Fault tolerant and subsystem codes. It has been shown recently that subsystem codes are suitable to protect quantum information since they have a good strategy of fault tolerant and high threshold values, see [1].

D. MDS Subsystem Codes

In this section we derive all MDS subsystem codes. Recall that an $[[n,k,r,d]]_q$ subsystem code derived from an $\mathbb{F}_q$-linear classical code $C \leq \mathbb{F}_q^{2n}$ satisfies the Singleton bound $k+r \leq n-2d+2$. A subsystem code attaining the Singleton bound with equality is called an MDS subsystem code. An important consequence is the following simple observation which yields an easy construction of subsystem codes that are optimal among the $\mathbb{F}_q$-linear Clifford subsystem codes.

Theorem 92. *If there exists an $\mathbb{F}_q$-linear $[[n,k,d]]_q$ MDS stabilizer code, then there exists a pure $\mathbb{F}_q$-linear $[[n,k-r,r,d]]_q$ MDS subsystem code for all r in the range $0 \leq r \leq k$.*

Proof. An MDS stabilizer code must be pure, see [123, Theorem 2] or [81, Corollary 60]. By Corollary 89, a pure $\mathbb{F}_q$-linear $[[n,k,d]]_q$ stabilizer code implies the existence of an $\mathbb{F}_q$-linear $[[n,k-r,r,d_r \geq d]]_q$ subsystem code that is pure to d for any r in the range $0 \leq r \leq k$. Since the stabilizer code is MDS, we have $k = n-2d+2$. By the Singleton bound, the parameters of the resulting $\mathbb{F}_q$-linear $[[n, n-2d+2-r, r, d_r]]_q$ subsystem codes must satisfy $(n-2d+2-r)+r \leq n-2d_r+2$, which shows that the minimum distance $d_r = d$, as claimed. $\square$

Remark 93. *We conjecture that $\mathbb{F}_q$-linear MDS subsystem codes are actually optimal among all subsystem codes, but a proof that the Singleton bound holds for general subsystem codes remains elusive.*

We recall that the Hermitian construction of stabilizer codes yields $\mathbb{F}_q$-linear stabilizer codes, as can be seen from our reformulation of [65, Corollary 2].

Lemma 94 ([65]). *If there exists an $\mathbb{F}_{q^2}$-linear code $X \subseteq \mathbb{F}_{q^2}^n$ such that $X \subseteq X^{\perp_h}$, then there exists an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^{2n}$ such that $C \subseteq C^{\perp_s}$, $|C| = |X|$, $\mathrm{swt}(C^{\perp_s} - C) = \mathrm{wt}(X^{\perp_h} - X)$ and $\mathrm{swt}(C) = \mathrm{wt}(X)$.*

Proof. Let $\{1, \beta\}$ be a basis of $\mathbb{F}_{q^2}/\mathbb{F}_q$. Then $\mathrm{tr}_{q^2/q}(\beta) = \beta + \beta^q$ is an element β_0 of $\mathbb{F}_q$; hence, $\beta^q = -\beta + \beta_0$. Let

$$C = \{(u|v) \,|\, u, v \in \mathbb{F}_q^n, u + \beta v \in X\}.$$

It follows from this definition that $|X| = |C|$ and that $\mathrm{wt}(X) = \mathrm{swt}(C)$. Furthermore, if $u + \beta v$ and $u' + \beta v'$ are elements of X with u, v, u', v' in $\mathbb{F}_q^n$, then

$$\begin{aligned} 0 &= (u + \beta v)^q \cdot (u' + \beta v') \\ &= u \cdot u' + \beta^{q+1} v \cdot v' + \beta_0 v \cdot u' + \beta(u \cdot v' - v \cdot u'). \end{aligned}$$

On the right hand side, all terms but the last are in $\mathbb{F}_q$; hence we must have $(u \cdot v' - v \cdot u') = 0$, which shows that $(u|v) \perp_s (u'|v')$, whence $C \subseteq C^{\perp_s}$. Expanding $X^{\perp_h}$ in the basis $\{1\,\beta\}$ yields a code $C' \subseteq C^{\perp_s}$, and we must have equality by a dimension argument. Since the basis expansion is isometric, it follows that

$$\mathrm{swt}(C^{\perp_s} - C) = \mathrm{wt}(X^{\perp_h} - X).$$

The $\mathbb{F}_q$-linearity of C is a direct consequence of the definition of C. $\square$

In corollary 95, we give a few examples of MDS subsystem codes that can be obtained from Theorem 92.

Corollary 95. *i) An $\mathbb{F}_q$-linear pure $[[n, n-2d+2-r, r, d]]_q$ MDS subsystem code exists for all n, d, and r such that $3 \leq n \leq q$, $1 \leq d \leq n/2+1$, and $0 \leq r \leq n-2d+1$.*

ii) An $\mathbb{F}_q$-linear pure $[[(\nu+1)q, (\nu+1)q-2\nu-2-r, r, \nu+2]]_q$ MDS subsystem code exists for all ν and r such that $0 \leq \nu \leq q-2$ and $0 \leq r \leq (\nu+1)q-2\nu-3$.

iii) An $\mathbb{F}_q$-linear pure $[[q-1, q-1-2\delta-r, r, \delta+1]]_q$ MDS subsystem code exists for all δ and r such that $0 \leq \delta < (q-1)/2$ and $0 \leq r \leq q-2\delta-1$.

iv) An $\mathbb{F}_q$*-linear pure* $[[q, q-2\delta-2-r', r', \delta+2]]_q$ *MDS subsystem code exists for all* $0 \le \delta < (q-1)/2$ *and* $0 \le r' < q-2\delta-2$.

v) An $\mathbb{F}_q$*-linear pure* $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ *MDS subsystem code exists for all* δ *and* r *in the range* $0 \le \delta < q-1$ *and* $0 \le r < q^2-2\delta-1$.

vi) An $\mathbb{F}_q$*-linear pure* $[[q^2, q^2-2\delta-2-r', r', \delta+2]]_q$ *MDS subsystem code exists for all* δ *and* r' *in the range* $0 \le \delta < q-1$ *and* $0 \le r' < q^2-2\delta-2$.

Proof. i) By [65, Theorem 14], there exist $\mathbb{F}_q$-linear $[[n, n-2d+2, d]]_q$ stabilizer codes for all n and d such that $3 \le n \le q$ and $1 \le d \le n/2+1$. The claim follows from Theorem 92.

ii) By [134, Theorem 5], there exist a $[[(\nu+1)q, (\nu+1)q-2\nu-2, \nu+2]]_q$ stabilizer code. In this case, the code is derived from an $\mathbb{F}_{q^2}$-linear code X of length n over $\mathbb{F}_{q^2}$ such that $X \subseteq X^{\perp_h}$. The claim follows from Lemma 94 and Theorem 92.

iii) , iv) There exist $\mathbb{F}_q$-linear stabilizer codes with parameters $[[q-1, q-2\delta-1, \delta+1]]_q$ and $[[q, q-2\delta-2, \delta+2]]_q$ for $0 \le \delta < (q-1)/2$, see [65, Theorem 9]. Theorem 92 yields the claim.

v) , vi) There exist $\mathbb{F}_q$-linear stabilizer codes with parameters $[[q^2-1, q^2-2\delta-1, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2, \delta+2]]_q$. for $0 \le \delta < q-1$ by [65, Theorem 10]. The claim follows from Theorem 92.

□

The existence of the codes in i) are merely established by a non-constructive Gilbert-Varshamov type counting argument. However, the result is interesting, as it asserts that there exist for example $[[6, 1, 1, 3]]_q$ subsystem codes for all prime powers $q \ge 7$, $[[7, 1, 2, 3]]_q$ subsystem codes for all prime powers $q \ge 7$, and other short subsystem codes that one should compare with a $[[5, 1, 3]]_q$ stabilizer code. If the syndrome calculation is simpler, then such subsystem codes could be of practical value.

The subsystem codes given in ii)-vi) of the previous corollary are constructively established. The subsystem codes in ii) are derived from Reed-Muller codes, and in iii)-vi) from Reed-Solomon codes. There exists an overlap between the parameters given in ii) and in iv), but we list here both, since each code construction has its own merits.

Remark 96. *By Theorem 87, pure MDS subsystem codes can always be derived from MDS stabilizer codes. Therefore, one can derive in fact all possible parameter sets of pure MDS subsystem codes with the help of Theorem 92.*

Remark 97. *In the case of stabilizer codes, all MDS codes must be pure. For subsystem codes this is not true, as the* $[[9, 1, 4, 3]]_2$ *subsystem code shows. Finding such impure* $[[n, k, r, d]]_q$ *MDS subsystem codes with* $k + r > n - 2d + 2$ *is a particularly interesting challenge.*

E. Conclusion and Discussion

Subsystem codes – or operator quantum error-correcting codes as some authors prefer to call them – are among the most versatile tools in quantum error-correction, since they allow one to combine the passive error-correction found in decoherence free subspaces and noiseless subsystems with the active error-control methods of quantum error-correcting codes. The subclass of Clifford subsystem codes that was studied in this chapter is of particular interest because of the close connection to classical error-correcting codes. As Proposition 122 shows, one can derive from each additive code over $\mathbb{F}_q$ an Clifford subsystem code. This offers more flexibility than the slightly rigid framework of stabilizer codes. However, there exist few systematic constructions of good families subsystem codes and much of the theory remains to be developed. For instance, more bounds are needed for the parameters of subsystem codes.

In this chapter, we showed that any $\mathbb{F}_q$-linear MDS stabilizer code yields a series of pure $\mathbb{F}_q$-linear MDS subsystem codes. These codes are known to be optimal among the $\mathbb{F}_q$-linear Clifford subsystem codes. We conjecture that the Singleton bound holds in general for subsystem codes. There is quite some evidence for this fact, as pure Clifford subsystem codes and $\mathbb{F}_q$-linear Clifford subsystem codes are known to obey this bound.

We used Reed-Muller and Reed-Solomon codes to derive pure $\mathbb{F}_q$-linear MDS subsystem codes. In a similar fashion, one can derive other interesting subsystem codes from BCH stabilizer codes, see for instance [8].

CHAPTER IX

FAMILIES OF SUBSYSTEM CODES

A. Introduction

In this chapter I construct families of subsystem codes. I will derive cyclic subsystem codes, as well as BCH and RS subsystem codes. I will present an optimal family of subsystem codes in a sense that this family obeys quantum Singleton bound with equality.

Let Q be a quantum code such that $\mathcal{H} = Q \oplus Q^{\perp}$, where $Q^{\perp}$ is the orthogonal complement of Q. Recall definition of the error model acting in qubits as shown in Chapter III. We can define the subsystem code Q as follows.

Definition 98. An $[[n,k,r,d]]_q$ subsystem code is a decomposition of the subspace Q into a tensor product of two vector spaces A and B such that $Q = A \otimes B$, where $\dim A = q^k$ and $\dim B = q^r$. The code Q is able to detect all errors of weight less than d on subsystem A.

Subsystem codes can be constructed from classical codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. We recall the Euclidean and Hermitian construction from [9].

Lemma 99 (Euclidean Construction)**.** *If C is a k'-dimensional $\mathbb{F}_q$-linear code of length n that has a k''-dimensional subcode $D = C \cap C^{\perp}$ and $k' + k'' < n$, then there exists an*

$$[[n, n-(k'+k''), k'-k'', \mathrm{wt}(D^{\perp} \setminus C)]]_q$$

subsystem code.

Proof. Let us define the code $X = C \times C \subseteq \mathbb{F}_q^{2n}$, therefore $X^{\perp_s} = (C \times C)^{\perp_s} = C^{\perp_s} \times C^{\perp_s}$. Hence $Y = X \cap X^{\perp_s} = (C \times C) \cap (C^{\perp_s} \times C^{\perp_s}) = C \cap C^{\perp_s}$. Let

$\dim_{\mathbb{F}_q} Y = k''$. Hence $|X||Y| = q^{k'+k''}$ and $|X|/|Y| = q^{k'-k''}$. By Theorem [9, Theorem 1], there exists a subsystem code $Q = A \otimes B$ with parameters $[[n, \dim A, \dim B, d]]_q$ such that

i) $\dim A = q^n/(|X||Y|) = q^{n-k'-k''}$.

ii) $\dim B = |X|/|Y| = q^{k'-k''}$.

iii) $d = swt(Y^{\perp_s} \backslash X) = \mathrm{wt}(D^{\perp} \setminus C)$.

□

Also, subsystem codes can be constructed from two classical codes using the Euclidean construction as shown in the following lemma.

Lemma 100 (Euclidean Construction). *Let $C_i \subseteq \mathbb{F}_q^n$, be $[n, k_i]_q$ linear codes where $i \in \{1, 2\}$. Then there exists an $[[n, k, r, d]]_q$ subsystem code with*

- $k = n - (k_1 + k_2 + k')/2$,
- $r = (k_1 + k_2 - k')/2$, *and*
- $d = \min\{\mathrm{wt}((C_1^{\perp} \cap C_2)^{\perp} \setminus C_1), \mathrm{wt}((C_2^{\perp} \cap C_1)^{\perp} \setminus C_2)\}$,

where $k' = \dim_{\mathbb{F}_q}(C_1 \cap C_2^{\perp}) \times (C_1^{\perp} \cap C_2)$.

Also, the subsystem codes can be derived from classical codes, that are defined over $\mathbb{F}_{q^2}$, using the Hermitian construction.

Lemma 101 (Hermitian Construction). *Let $C \subseteq \mathbb{F}_{q^2}^n$ be an $\mathbb{F}_{q^2}$-linear $[n, k, d]_{q^2}$ code such that $D = C \cap C^{\perp_h}$ is of dimension $k' = \dim_{\mathbb{F}_{q^2}} D$. Then there exists an*

$$[[n, n-k-k', k-k', \mathrm{wt}(D^{\perp_h} \setminus C)]]_q$$

subsystem code.

Notation. If S is a set, then $|S|$ denotes the cardinality of the set S. Let q be a power of a prime integer p. We denote by $\mathbb{F}_q$ the finite field with q elements. We use the notation $(x|y) = (x_1, \ldots, x_n|y_1, \ldots, y_n)$ to denote the concatenation of two vectors x and y in $\mathbb{F}_q^n$. The symplectic weight of $(x|y) \in \mathbb{F}_q^{2n}$ is defined as

$$\operatorname{swt}(x|y) = \{(x_i, y_i) \neq (0,0) \,|\, 1 \leq i \leq n\}.$$

We define $\operatorname{swt}(X) = \min\{\operatorname{swt}(x) \,|\, x \in X, x \neq 0\}$ for any nonempty subset $X \neq \{0\}$ of $\mathbb{F}_q^{2n}$. The trace-symplectic product of two vectors $u = (a|b)$ and $v = (a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as

$$\langle u|v\rangle_s = \operatorname{tr}_{q/p}(a' \cdot b - a \cdot b'),$$

where $x \cdot y$ denotes the dot product and $\operatorname{tr}_{q/p}$ denotes the trace from $\mathbb{F}_q$ to the subfield $\mathbb{F}_p$. The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as

$$C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w\rangle_s = 0 \text{ for all } w \in C\}.$$

We define the Euclidean inner product $\langle x|y\rangle = \sum_{i=1}^n x_i y_i$ and the Euclidean dual of $C \subseteq \mathbb{F}_q^n$ as

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x|y\rangle = 0 \text{ for all } y \in C\}.$$

We also define the Hermitian inner product for vectors x, y in $\mathbb{F}_{q^2}^n$ as $\langle x|y\rangle_h = \sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbb{F}_{q^2}^n$ as

$$C^{\perp_h} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}.$$

B. Cyclic Subsystem Codes

In this section we shall derive subsystem codes from classical cyclic codes. We first recall some definitions before embarking on the construction of subsystem codes. For further details concerning cyclic codes see for instance [75] and [107].

Let n be a positive integer and $\mathbb{F}_q$ a finite field with q elements such that

$\gcd(n,q) = 1$. Recall that a linear code $C \subseteq \mathbb{F}_q^n$ is called *cyclic* if and only if $(c_0,\ldots,c_{n-1})$ in C implies that $(c_{n-1},c_0,\ldots,c_{n-2})$ in C.

For $g(x)$ in $\mathbb{F}_q[x]$, we write $(g(x))$ to denote the principal ideal generated by $g(x)$ in $\mathbb{F}_q[x]$. Let π denote the vector space isomorphism $\pi\colon \mathbb{F}_q^n \to R_n = \mathbb{F}_q[x]/(x^n-1)$ given by

$$\pi((c_0,\ldots,c_{n-1})) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + (x^n-1).$$

A cyclic code $C \subseteq \mathbb{F}_q^n$ is mapped to a principal ideal $\pi(C)$ of the ring R_n. For a cyclic code C, the unique monic polynomial $g(x)$ in $\mathbb{F}_q[x]$ of the least degree such that $(g(x)) = \pi(C)$ is called the *generator polynomial* of C. If $C \subseteq \mathbb{F}_q^n$ is a cyclic code with generator polynomial $g(x)$, then

$$\dim_{\mathbb{F}_q} C = n - \deg g(x).$$

Since $\gcd(n,q) = 1$, there exists a primitive n^{th} root of unity α over $\mathbb{F}_q$; that is, $\mathbb{F}_q[\alpha]$ is the splitting field of the polynomial $x^n - 1$ over $\mathbb{F}_q$. Let us henceforth fix this primitive n^{th} primitive root of unity α. Since the generator polynomial $g(x)$ of a cyclic code $C \subseteq \mathbb{F}_q^n$ is of minimal degree, it follows that $g(x)$ divides the polynomial $x^n - 1$ in $\mathbb{F}_q[x]$. Therefore, the generator polynomial $g(x)$ of a cyclic code $C \subseteq \mathbb{F}_q^n$ can be uniquely specified in terms of a subset T of $\{0,\ldots,n-1\}$ such that

$$g(x) = \prod_{t\in T}(x - \alpha^t).$$

The set T is called the *defining set* of the cyclic code C (with respect to the primitive n^{th} root of unity α). A defining set is the union of cyclotomic cosets modulo n. The following lemma recalls some well-known and easily proved facts about defining sets (see e.g. [75]).

Lemma 102. *Let C_i be a cyclic code of length n over $\mathbb{F}_q$ with defining set a T_i for*

$i = 1, 2$. Let $N = \{0, 1, \ldots, n-1\}$ and $T_1^a = \{at \bmod n \,|\, t \in T\}$ for some integer a. Then

i) $C_1 \cap C_2$ has defining set $T_1 \cup T_2$.

ii) $C_1 + C_2$ has defining set $T_1 \cap T_2$.

iii) $C_1 \subseteq C_2$ if and only if $T_2 \subseteq T_1$.

iv) $C_1^{\perp}$ has defining set $N \setminus T_1^{-1}$.

v) $C_1^{\perp_h}$ has defining set $N \setminus T_1^{-r}$ provided that $q = r^2$ for some positive integer r.

Notation. If T is a defining set of a cyclic code of length n, then we denote henceforth by T^a the set

$$T^a = \{at \bmod n \,|\, t \in T\},$$

as in the previous lemma. We use a superscript, since this notation will be frequently used in set differences, and arguably $N \setminus T^{-q}$ is more readable than $N \setminus -qT$.

Now, we shall give a general construction for subsystem cyclic codes. We say that a code C is self-orthogonal if and only if $C \subseteq C^{\perp}$. We show that if a classical cyclic code is self-orthogonal, then one can easily construct cyclic subsystem codes.

Proposition 103. Let D be a self-orthogonal cyclic code of length n over $\mathbb{F}_q$ with defining set T_D. Let T_D and $T_{D^{\perp}}$ respectively denote the defining sets of D and $D^{\perp}$. If T is a subset of $T_D \setminus T_{D^{\perp}}$, then one can define a cyclic code C of length n over $\mathbb{F}_q$ by the defining set $T_C = T_D \setminus (T \cup T^{-1})$. If $n - k = |T_D|$, $r = |T \cup T^{-1}|$ with $0 \leq r < n - 2k$, and $d = \min \mathrm{wt}(D^{\perp} \setminus C)$, then there exists a subsystem code with parameters $[[n, n-2k-r, r, d]]_q$.

Proof. Since D is a self-orthogonal cyclic code, we have $D \subseteq D^{\perp}$, whence $T_{D^{\perp}} \subseteq T_D$ by Lemma 102 iii). Observe that if s is an element of the set $S = T_D \setminus T_{D^{\perp}} = T_D \setminus (N \setminus T_D^{-1})$, then $-s$ is an element of S as well. In particular, T^{-1} is a subset of $T_D \setminus T_{D^{\perp}}$.

By definition, the cyclic code C has the defining set $T_C = T_D \setminus (T \cup T^{-1})$; thus, the dual code $C^\perp$ has the defining set

$$T_{C^\perp} = N \setminus T_C^{-1} = T_{D^\perp} \cup (T \cup T^{-1}).$$

Furthermore, we have

$$T_C \cup T_{C^\perp} = (T_D \setminus (T \cup T^{-1})) \cup (T_{D^\perp} \cup T \cup T^{-1}) = T_D;$$

therefore, $C \cap C^\perp = D$ by Lemma 102 i).

Since $n - k = |T_D|$ and $r = |T \cup T^{-1}|$, we have $\dim_{\mathbb{F}_q} D = n - |T_D| = k$ and $\dim_{\mathbb{F}_q} C = n - |T_C| = k + r$. Thus, by Lemma 100 there exists an $\mathbb{F}_q$-linear subsystem code with parameters $[[n, \kappa, \rho, d]]_q$, where

i) $\kappa = \dim D^\perp - \dim C = n - k - (k + r) = n - 2k - r$,

ii) $\rho = \dim C - \dim D = k + r - k = r$,

iii) $d = \min \mathrm{wt}(D^\perp \setminus C)$,

as claimed. □

We notice that if $\mathrm{wt}(D) \leq \mathrm{wt}(D^\perp)$, then the constructed cyclic subsystem codes are impure. In addition, if $d = \mathrm{wt}(D^\perp) = \mathrm{wt}(D^\perp \backslash D)$, then the constructed codes are pure up to d.

We can also derive subsystem codes from cyclic codes over $\mathbb{F}_{q^2}$ by using cyclic codes that are self-orthogonal with respect to the Hermitian inner product.

Proposition 104. Let D be a cyclic code of length n over $\mathbb{F}_{q^2}$ such that $D \subseteq D^{\perp_h}$. Let T_D and $T_{D^{\perp_h}}$ respectively be the defining set of D and $D^{\perp_h}$. If T is a subset of $T_D \setminus T_{D^{\perp_h}}$, then one can define a cyclic code C of length n over $\mathbb{F}_{q^2}$ with defining set $T_C = T_D \setminus (T \cup T^{-q})$. If $n - k = |T_D|$ and $r = |T \cup T^{-q}|$ with $0 \leq r < n - 2k$, and $d = \mathrm{wt}(D^{\perp_h} \setminus C)$, then there exists an $[[n, n - 2k - r, r, d]]_q$ subsystem code.

Proof. Since $D \subseteq D^{\perp_h}$, their defining sets satisfy $T_{D^{\perp_h}} \subseteq T_D$ by Lemma 102 iii). If s is an element of $T_D \setminus T_{D^{\perp_h}}$, then one easily verifies that $-qs \pmod n$ is an element of $T_D \setminus T_{D^{\perp_h}}$.

Let $N = \{0, 1, \ldots, n-1\}$. Since the cyclic code C has the defining set $T_C = T_D \setminus (T \cup T^{-q})$, its dual code $C^{\perp_h}$ has the defining set $T_{C^{\perp_h}} = N \setminus T_C^{-q} = T_{D^{\perp_h}} \cup (T \cup T^{-q})$. We notice that

$$T_C \cup T_{C^{\perp_h}} = (T_D \setminus (T \cup T^{-q})) \cup (T_{D^{\perp_h}} \cup T \cup T^{-q}) = T_D;$$

thus, $C \cap C^{\perp_h} = D$ by Lemma 102 i).

Since $n - k = |T_D|$ and $r = |T \cup T^{-q}|$, we have $\dim D = n - |T_D| = k$ and $\dim C = n - |T_C| = k + r$. Thus, by Lemma 101 there exists an $[[n, \kappa, \rho, d]]_q$ subsystem code with

i) $\kappa = \dim D^{\perp_h} - \dim C = (n-k) - (k+r) = n - 2k - r$,

ii) $\rho = \dim C - \dim D = k + r - k = r$,

iii) $d = \min \operatorname{wt}(D^{\perp_h} \setminus C)$,

as claimed. □

We notice that if $\operatorname{wt}(D) \leq \operatorname{wt}(D^{\perp_h})$, then the constructed cyclic subsystem codes are impure. In addition, if $d = \operatorname{wt}(D^{\perp}) = \operatorname{wt}(D^{\perp_h} \setminus D)$, then the constructed codes are pure up to d.

The previous two propositions allow one to easily construct subsystem codes from classical cyclic codes. We will illustrate this fact by deriving cyclic subsystem codes from BCH and Reed-Solomon codes. Also, one can derive subsystem codes from classical cyclic codes if the generator polynomial is known.

C. Subsystem BCH Codes

In this section we consider an important class of cyclic codes that can be constructed with arbitrary designed distance δ. We will construct families of subsystem BCH codes.

Let n be a positive integer, $\mathbb{F}_q$ be a finite field with q elements, and α is a primitive nth root of unity. A primitive narrow-sense BCH code C of designed distance δ and length n is a cyclic code with generator monic polynomial $g(x)$ over $\mathbb{F}_q$ that has $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ as zeros. c is a codeword in C if and only if $c(\alpha) = c(\alpha^2) = \ldots = c(\alpha^{\delta-1}) = 0$. The parity check matrix of this code can be defined as

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-1} & \alpha^{2(\delta-1)} & \cdots & \alpha^{(\delta-1)(n-1)} \end{bmatrix} \tag{9.1}$$

We have shown in [8, 11] that narrow sense BCH codes, primitive and non-primitive, with length n and designed distance δ are Euclidean dual-containing codes if and only if $2 \leq \delta \leq \delta_{\max} = \frac{n}{q^m-1}(q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}])$. We use this result and [6, Theorem 2] to derive primitive subsystem BCH codes from classical BCH codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ [9, 11].

Lemma 105. *If q is a power of a prime, m is a positive integer, and $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$. Then there exists a subsystem BCH code with parameters $[[q^m-1, n-2m\lceil(\delta-1)(1-1/q)\rceil - r, r, \geq \delta]]_q$ where $0 \leq r < n-2m\lceil(\delta-1)(1-1/q)\rceil$.*

Proof. We know that if $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd}]$, then there exists a stabilizer code with parameters $[[q^m-1, n-2m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]]_q$. Let r be an integer in the range $0 \leq r < n-2m\lceil(\delta-1)(1-1/q)\rceil$. From [6, Theorem 2], then there must exist a subsystem BCH code with parameters $[[q^m-1, n-2m\lceil(\delta-1)(1-1/q)\rceil-r, r, \geq \delta]]_q$. $\square$

Lemma 106. *If q is a power of a prime, m is a positive integer, and δ is an integer in the range $2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2-2)[m \text{ even}]$, then there exists a subsystem code Q with parameters*

$$[[q^{2m}-1, q^{2m}-1-2m\lceil(\delta-1)(1-1/q^2)\rceil - r, r, d_Q \geq \delta]]_q$$

that is pure up to δ, where $0 \leq r < q^{2m}-1-2m\lceil(\delta-1)(1-1/q^2)\rceil$.

Proof. If $2 \leq \delta \leq \delta_{\max} = q^{m+[m \text{ even}]} - 1 - (q^2-2)[m \text{ even}]$, then exists a classical BCH code with parameters $[q^m-1, q^m-1-m\lceil(\delta-1)(1-1/q)\rceil, \geq \delta]_q$ which contains its dual code. From [6, Theorem 2], [5], then there must exist a subsystem code with the given parameters. $\square$

Instead of constructing subsystem codes from stabilizer BCH codes as shown in Lemmas 105, 106, we can also construct subsystem codes from classical BCH code over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ under some restrictions on the designed distance. Let C_i be a cyclotomic coset defined as $\{iq^j \mod n \mid j \in Z\}$.

Lemma 107. *If q is a power of a prime, m is a positive integer, and $2 \leq \delta \leq q^{\lceil m/2\rceil}-1-(q-2)[m \text{ odd}]$. Let D be a BCH code with length $n = q^m-1$ and defining set $T_D = \{C_0, C_1, \ldots, C_{n-\delta}\}$, such that $\gcd(n,q)=1$. Let $T \subseteq \{0\} \cup \{C_\delta, \ldots, C_{n-\delta}\}$ be a nonempty set. Assume $C \subseteq \mathbb{F}_q^n$ be a BCH code with the defining set $T_C = \{C_0, C_1, \ldots, C_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then there exists a subsystem BCH code with the parameters $[[n, n-2k-r, r, \geq \delta]]_q$, where $k = m\lceil(\delta-1)(1-1/q)\rceil$ and $r = |T \cup T^{-1}|$.*

Proof. The proof can be divide into the following parts:

i) We know that $T_D = \{C_0, C_1, \ldots, C_{n-\delta}\}$ and $T \subseteq \{0\} \cup \{C_\delta, \ldots, C_{n-\delta}\}$ be a nonempty set. Hence $T_D^\perp = \{C_1, \ldots, C_{\delta-1}\}$. Furthermore, if $2 \leq \delta \leq q^{\lceil m/2 \rceil} - 1 - (q-2)[m \text{ odd }]$, then $D \subseteq D^\perp$. Furthermore, let $k = m\lceil(\delta-1)(1-1/q)\rceil$, then $\dim D^\perp = n-k$ and $\dim D = k$.

ii) We know that $C \in \mathbb{F}_q^n$ is a BCH code with defining set $T_C = T_D \setminus (T \cup T^{-1}) = \{C_0, C_1, \ldots, C_{n-\delta}\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then the dual code $C^\perp$ has defining set $T_C^\perp = \{C_1, \ldots, C_{\delta-1}\} \cup T \cup T^{-1} = T_{D^\perp} \cup T \cup T^{-1}$. We can compute the union set T_D as $T_C \cup T_C^\perp = \{C_0, C_1, \ldots, C_{n-\delta}\} = T_D$. By Lemma 102, therefore, $C \cap C^\perp = D$. Furthermore, if $r = |T \cup T^{-1}|$, then $\dim C = k + r$.

iii) From step (i) and (ii), and for $0 \leq r < n - 2k$, and by Lemma 100, there exits a subsystem code with parameters $[[n, \dim D - \dim C, \dim C - \dim D, d]]_q = [[n, n-2k-r, r, d]]_q$, $d = \min wt(D^\perp - C) \geq \delta$.

□

Also, we can derive subsystem BCH codes from classical BCH codes over $\mathbb{F}_{q^2}$ as shown in the following Lemma, see [5, 8, 11].

Lemma 108. *If q is a power of a prime, n, m are positive integers, and* $\gcd(n, q) = 1$. *Let $n = (q^2)^m - 1$, $2 \leq \delta \leq q^m - 1 - (q-2)[m \text{ odd }]$ and $T \subseteq \{0\} \cup \{C_\delta, \ldots, C_{n-\delta}\}$. Let $C \subseteq \mathbb{F}_{q^2}^n$ be a cyclic code with the defining set $T_C = \{C_0, C_1, \ldots, C_{n-\delta}\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem code with the parameters $[[n, n-2k-r, r, \geq \delta]]_q$, where $k = m\lceil(\delta-1)(1-1/q^2)\rceil$ and $0 \leq r = |T \cup T^{-q}| < n - 2k$.*

Proof. The proof is very similar to the proof shown in Lemma 107 taking in consideration that the classical BCH codes are over $\mathbb{F}_{q^2}$.

i) We know that the BCH code contains its Hermitian dual code if $2 \leq \delta \leq q^m - 1 - (q-2)[m \text{ odd }]$. Let $n = (q^2)^m - 1$ and $D^{\perp_h} \subseteq \mathbb{F}_{q^2}^n$ be a BCH code defined with a designed distance δ. The dual code $D^{\perp_h}$ has defining set $T_{D^{\perp_h}} = \{C_1, \ldots, C_{\delta-1}\}$. Consequently, the code D has defining set $\{C_0, C_1, \ldots, C_{n-\delta}\}$ and it is self-orthogonal, i.e., $D \subseteq D^{\perp_h}$. Furthermore, if $k = m\lceil(\delta-1)(1-1/q^2)\rceil$, then $\dim D^{\perp_h} = n - k$ and $\dim = k$.

ii) We know that $C \subseteq \mathbb{F}_{q^2}^n$ is a BCH code with defining set $T_C = \{C_0, C_1, \ldots, C_{n-\delta}\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then the dual code $C^{\perp_h}$ has defining set $T_{C^{\perp_h}} = \{C_1, \ldots, C_{\delta-1}\} \cup T \cup T^{-q}$. We can compute the union set T_D as $T_C \cup T_{C^{\perp_h}} = \{C_0, C_1, \ldots, C_{n-\delta}\}$. Therefore, $C \cap C^{\perp_h} = D$. Assume $r = |T \cup T^{-q}|$, then $\dim C = k + r$

iii) From step (i) and (ii), and by Lemma 101 for $0 \leq r < n - 2k$, there exits a subsystem code with parameters $[[n, n-2k-r, r, d]]_q$, where $k = m\lceil(\delta-1)(1-1/q^2)\rceil$ and $0 \leq r = |T \cup T^{-q}| < n - 2k$, $d = \min wt(D^{\perp} - C) \geq \delta$.

$\square$

Tables I and IIshow some families of subsystem BCH codes derived from classical BCH codes. The subsystem code $[[21, 18, 1, 2]]_2$ constructed using BCH codes, but the stabilizer code $[[21, 19, 2]]_2$ does not exist using the linear programming bound [30].

It may be useful to end up this section with an example

Example 109. *Consider a BCH code $D^{\perp}$ with designed distance $d = 5$ and length $n = 2^5 - 1$ over $\mathbb{F}_4$. Then $C_1 = \{1, 2, 4, 8, 16\}$, $C_2 = \{3, 6, 12, 24, 17\}$, and $C_5 = \{5, 10, 20, 9, 18\}$. Then $T_{D^{\perp_h}} = C_1 \cup C_3$. Hence* $\dim D = 10$ *and* $\dim D^{\perp_h} = 21$. *Now, let $T = C_5$, so, $T^{-q} = C_{11} = \{11, 13, 21, 22, 26\}$ and $T_{C^{\perp_h}} = T_{D^{\perp_h}} \cup T \cup T^{-q}$. We have $|T_{C^{\perp_h}} = 20|$, therefore* $\dim C = 20$. *Conseqeuntly, there exists a subsystem BCH* *codes with parameters* $[[n, \dim D^{\perp_h} - \dim C, \dim C - \dim D, \geq \delta]]_q = [[31, 1, 10, \geq 5]]_2$. *Some subsystem BCH codes are shown in Tables I and II.*

D. Subsystem RS Codes

In this section we will derive cyclic subsystem codes based on Reed-Solomon codes. Also, we show that given optimal stabilizer codes, one can construct optimal subsystem codes. Recall that a Reed-Solomon code over $\mathbb{F}_q$ is a BCH code with length $n = q-1$ and minimum distance equals to its designed distance δ. Therefore, the RS code C with designed distance δ has defining set T with size $\delta - 1$. This can be seen as all roots lie in different cyclotomic cosets. The dimension of a RS code is given by $n - \delta + 1$. RS codes are an important class of optimal cyclic codes. They are MDS codes, in which Singleton bound is satisfied with equality.

Grassl *et al.* in [65] showed that optimal stabilizer codes with maximal minimum distance exist with parameters $[[n, n-2d+2, d]]_q$ over $\mathbb{F}_q$ for $3 \leq n \leq q$ and $1 \leq d \leq n/2+1$. Also, optimal stabilizer codes exist with parameters $[[q^2, q^2-2d+2, d]]_q$ for $1 \leq d \leq q$ over $\mathbb{F}_q$, see [65, Theorems 9, 10]. These codes satisfy the quantum Singleton bound $k + 2d = n + 2$. The following subsystem codes are optimal since they obey the singleton bound $k + r + 2d = n + 2$ as shown in [9, Theorem 21].

Lemma 110 (Reed-Solomon Subsystem codes)**.** *Let q be power of a prime.*

i) If $0 \leq \delta < (q-1)/2$ *there exist subsystem codes with parameters* $[[q-1, q-2\delta-1-r, r, \delta+1]]_q$ *and* $[[q, q-2\delta-2-r, r, \delta+2]]_q$.

ii) If $0 \leq \delta < q-1$ *there exist subsystem codes with parameters* $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ *and* $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$

Proof. i) We know that if $0 \leq \delta < (q-1)/2$, then there are stabilizer codes with parameters $[[q-1, q-2\delta-1, \delta+1]]_q$ and $[[q, q-2\delta-2, \delta+2]]_q$, see [65, Theorem 9].

Now, let $0 \leq r < q-2\delta-1$, then using [6, Corollary 6], there are subsystem codes with parameters $[[q-1, q-2\delta-1-r, r, \delta+1]]_q$ and $[[q, q-2\delta-2-r, r, \delta+2]]_q$.

ii) Similarly, if $0 \leq \delta < q-1$, then from [65, Theorem 10], there exist stabilizer codes with parameters $[[q^2-1, q^2-2\delta-1, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$. Assuming $0 \leq r < q^2-2\delta-1$, then from [6, Corollary 6], there exist subsystem codes with parameters $[[q^2-1, q^2-2\delta-1-r, r, \delta+1]]_q$ and $[[q^2, q^2-2\delta-2-r, r, \delta+2]]_q$.

□

Instead of extending the subsystem code that we constructed, one can start with a subsystem code with length $n = q$ and shorten it to a subsystem code with length $n = q-1$. These subsystem codes are all $\mathbb{F}_{q^2}$-linear. Therefore they satisfy $k+r = n-2d+2$. As a consequence the subsystem codes in Lemma 110 are optimal. The subsystem codes that we derive are not necessarily cyclic. In order to derive cyclic codes we need to make further restrictions on the codes. The following lemma gives an explicit construction for cyclic subsystem codes based on the Reed-Solomon codes over $\mathbb{F}_q$.

Lemma 111. *Let q be a prime power, and $n = q-1$, $2 \leq \delta < (q-1)/2$ and $T \subseteq \{0\} \cup \{\delta, \ldots, n-\delta\}$. Let $C \subseteq \mathbb{F}_q^n$ be a cyclic code with the defining set $T_C = \{0, 1, \ldots, n-\delta\} \setminus (T \cup T^{-1})$ where $T^{-1} = \{-t \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem RS code with the parameters $[[n, n-2\delta+2-r, r, \geq \delta]]_q$, where $0 \leq r = |T \cup T^{-1}| < n-2(\delta+1)$.*

Proof. We divide the proof to the following parts

i) We know that if $2 \leq \delta < (q-1)/2$, then there exists classical cyclic code $D^\perp$ that contains its dual code D, i.e., $D \subseteq D^\perp$. The code $D^\perp$ has defining set

$T_{D^\perp} = \{1, 2, ..., \delta - 1\}$. Therefore the defining set of D is given by $T_D = \{0\} \cup \{1, \cdots, n-\delta\}$ and $D = C \cap C^\perp$. Also, $\dim D^\perp = n - (\delta - 1)$ and $\dim D = \delta - 1$.

ii) Let $T \subseteq T_D$ be a nonempty set and $T^{-1} = \{-t \bmod n \mid t \in T\}$. Let $C \subseteq \mathbb{F}_q^n$ be a cyclic code with the defining set $T_C = T_D \setminus (T \cup T^{-1})$. We can actually compute the defining set of the dual code $C^\perp$ as $T_{C^\perp} = T_{D^\perp} \cup T \cup T^{-1}$. We notice that $T_C \cup T_{C^\perp} = \{1, 2, \cdots, n - \delta\} \cup \{0\} = T_D$. Let $k = \delta - 1$ and $0 \le r = |T \cup T^{-1}| < n - 2k$.

iii) From steps (i), (ii) and by using Lemma 100, there is a subsystem code with $[[n, k, r, \ge \delta]]_q$, where $k = n - 2\delta + 2 - r$ and $0 \le r = |T \cup T^{-1}| < n - 2(\delta - 1)$.

□

Also, cyclic subsystem codes, based on RS codes over $\mathbb{F}_{q^2}$, can be derived as shown in the following lemma. Some codes are shown in Table III.

Lemma 112. *Let q be a prime power, $n = q^2-1$, and $2 \le \delta < (q-1)$. Let $T \subseteq \{0\} \cup \{q\delta, \ldots, q(n-\delta)\}$ be a nonempty set. Let $C \subseteq \mathbb{F}_{q^2}^n$ be a cyclic code with the defining set $T_C = \{0, q, \ldots, q(n-\delta)\} \setminus (T \cup T^{-q})$ where $T^{-q} = \{-qt \bmod n \mid t \in T\}$. Then there exists a cyclic subsystem RS code with the parameters $[[n, n - 2(\delta - 1) - r, r, \ge \delta]]_q$, where $0 \le r = |T \cup T^{-q}| < n - 2(\delta - 1)$.*

Proof. The proof is a direct consequence as shown in the previous lemmas.

We know that if $2 \le \delta < (q - 1)$, then there exists a cyclic code $D^\perp$ over $\mathbb{F}_{q^2}$ that contains it is dual code D. The code $D^{\perp_h}$ has length n, and minimum distance δ. The defining set of the code D is given by $T_D = \{q, 2q, \cdots, q(n - \delta)\} \cup \{0\}$

We just notice that the defining set of the dual code $C^{\perp_h}$ is given by $T_{C^{\perp_h}} = \{q, 2q, ..., q(\delta-1)\} \cup T \cup T^{-q}$. Furthermore, $T_C \cup T_{C^{\perp_h}} = \{q, 2q, \cdots, q(n-\delta)\} \cup \{0\} = T_D$. Hence, $D \subseteq C$, $D \subseteq C^{\perp_h}$, and $D = C \cap C^{\perp_h}$. From Lemma 101, there must exist a cyclic subsystem RS code with parameters $[[n,k,r,\geq \delta]]_q$, where $k=n-2(\delta-1)-r$ and $0 \leq r = |T \cup T^{-q}| < n-2(\delta+1)$. $\square$

In table III we show various optimal subsystem codes derived from RS codes. Some of these codes have been derived by puncture existing subsystem codes. It is also possible to derive some optimal impure subsystem codes. For instance $[[9,1,4,3]]_2$ is an optimal impure subsystem codes.

Puncture Subsystem Codes The MDS subsystem codes constructed from RS codes can also be punctured to other subsystem codes. Recall that if there is a subsystem code with parameters $[[n,k,r,d]]_q$ then there is a subsystem code with parameters $[[n-1,k,r,\geq\ d-1]_q$. This is known as the propagation rules of quantum code constructions.

We end up this section by presenting two examples to illustrate the previous construction.

Example 113. *Let C be a RS code with length $n=q-1=6$ over $\mathbb{F}_q$. Define $N=\{0,1,2,3,4,5\}$. We can construct subsystem code from RS codes with parameters $[6,4,3]_7$. This code is a subcode-subfield in BCH codes with deigned distance $\delta=3$. So, $T_{D^\perp}=\{1,2\}$, $T_D=\{0,1,2,3\}$, $T_C=\{1,2,3\}$ and $T_{C^\perp}=\{0,1,2\}$. We notice that $T_D=T_C\cup T_{C^\perp}$ and $\dim C=3$, $\dim D=2$ and $\dim D^\perp=4$. So, we have k=4-3=1 and r=3-2=1. Consequently, there exists a subsystem code with parameters $[6,1,1,3]$ over $\mathbb{F}_7$*

The previous example shows the shortest subsystem codes with length $n=6$. However, it is not necessarily that this code exists only over $\mathbb{F}_7$. In fact, as we were able to show that there exists a subsystem code with length $n=6$ over $\mathbb{F}_3$.

Example 114. *Let F_{13} be the finite field with $q = 13$ elements. Let $D^\perp$ be the narrow-sense Reed-Solomon code of length $n = 12$ and designed distance $\delta = 5$ over F_{13}. So, $D^\perp$ has defining set $T_{D^\perp} = \{1, 2, 3, 4\}$. Therefore, $D^\perp$ is an MDS code with parameters $[12, 8, 5]$. The dual of $D^\perp$ is a RS code D with defining set $T_D = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Also, D is an MDS code with parameters $[12, 4, 9]$. Clearly, from our construction,*

$$D \subseteq D^\perp \iff T_{D^\perp} \subseteq T_D$$

Now, let us define the code C by choosing a defining set $T_C = \{1, 2, 3, 4, 7\}$. So, $D \subseteq C \iff T_C \subseteq T_D$. Also compute the defining set of $C^\perp$ as $T_{C^\perp} = \{0, 1, 2, 3, 4, 6, 7\}$. So, $D \subseteq C^\perp \iff T_{C^\perp} \subseteq T_D$. We see from our construction of these codes that

$$C \cap C^\perp = D \iff T_C \cup T_{C^\perp} = T_D.$$

Hence, we can compute the parameters of the subsystem code as follows. The minimum distance is given by $d_{min} = D^\perp \backslash C = 5$, dimension $k = \dim D^\perp - \dim C = 8 - 7 = 1$, and gauge qubits $r = \dim C - \dim D = 7 - 4 = 3$. Therefore, we have a subsystem code with parameters $[[12, 1, 3, 5]]$, which is also an MDS code obeying Singleton bound $k + r + 2d = n + 2$.

Actually, if we choose the defining set of C to be $T_C = \{1, 2, 3, 4, 6, 7\}$, then the defining set of $C^\perp$ is $T_{C^\perp} = \{0, 1, 2, 3, 4, 7\}$, then we get a subsystem code with parameters $d_{min} = D^\perp \backslash C = 5$, $k = \dim D^\perp - \dim C = 8-6 = 2$, $r = \dim C - \dim D = 6 - 4 = 2$. Therefore, we have a subsystem code with parameters $[[12, 2, 2, 5]]$, which is also an MDS code. Some of subsystem RS codes are listed in Table IV.

E. Short Subsystem Codes $[[8,1,2,3]]_2$ and $[[6,1,1,3]]_3$

In this section we present the shortest subsystem codes over $\mathbb{F}_2$ and $\mathbb{F}_3$ fields. Corollary 89 implies that a stabilizer code with parameters $[[n,k,d]]_q$ gives subsystem codes with parameters $[[n,k-r,r,d]]_q$, see Tables I, II, III, IV, V.

Consider a stabilizer code with parameters $[[8,3,3]]_2$. This code can be used to derive $[[8,2,1,3]]_2$ and $[[8,1,2,3]]_2$ subsystem codes. We give an explicit construction of these codes. Further, we claim that $[[8,1,2,3]]_2$ and $[[8,2,1,3]]_2$ are the shortest nontrivial binary subsystem codes. We obtain these codes using MAGMA computer algebra search . It remains to study properties of these codes and whether they have nice error correction capabilities. We show the stabilizer and normalizer matrices for these codes. Also, we prove their minimum distances using the weight enumeration of these codes. It was known that the $[[9,1,4,3]]_2$ Becan-Shor code is the shortest subsystem code constructed via graphs, in which it tolerates 4 gauge qubits. We present two codes with less length, however we can not tolerate more than 2 gauge qubits. The following example shows $[[8,1,2,3]]$ short subsystem code over $\mathbb{F}_2$.

Example 115.

$$D_S = \begin{bmatrix} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \end{bmatrix} \tag{9.2}$$

$$D_S^{\perp} = \begin{bmatrix} X & I & I & I & I & I & Z & Y \\ Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \\ I & Y & I & I & I & I & X & Z \\ I & I & X & I & I & Y & Z & I \\ I & I & Y & I & I & I & Z & X \\ I & I & I & X & I & Y & I & Z \\ I & I & I & Y & I & Y & Y & Y \\ I & I & I & I & X & I & Y & Z \\ I & I & I & I & Y & Y & Z & Z \\ I & I & I & I & I & Z & X & Y \end{bmatrix} \tag{9.3}$$

$$C_S = \left[\begin{array}{cccccccc} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline Y & I & I & I & I & Y & X & X \\ I & X & I & I & I & Y & Y & X \end{array}\right] \tag{9.4}$$

$$C_S^{\perp} = \left[\begin{array}{cccccccc} X & I & Y & I & Z & Y & X & Z \\ Y & I & Y & X & I & Z & Z & X \\ I & X & Y & Y & Z & X & Z & I \\ I & Y & I & Z & Y & X & X & Z \\ I & I & X & Z & X & Y & Z & Y \\ \hline X & I & I & I & I & I & Z & Y \\ I & I & I & Y & I & Y & Y & Y \end{array}\right] \tag{9.5}$$

We notice that the matrix D_S generates the code $D = C \cap C^{\perp_s}$. Furthermore, dimensions of the subsystems A and B are given by $k = \dim D^{\perp_s} - \dim C = (11 - 7)/2 = 2$ and $r = \dim C - \dim D = (7-5)/2 = 1$. Hence we have $[[8,2,1,3]]_2$ and $[[8,1,2,3]]_2$ subsystem codes.

We show that the subsystem codes $[[8,1,2,3]]_2$ is not better than the stabilizer code $[[8,3,3]]_2$ in terms of syndrome measurement. The reason is that the former needs $8-1-2=5$ syndrome measurements, while the later needs also $8-3=5$ measurements. This is an obvious example where subsystem codes have no superiority in terms of syndrome measurements.

We post an open question regarding the threshold value and fault tolerant gate operations for this code. We do not know at this time if the code $[[8,1,2,3]]_2$ has better threshold value and less fault-tolerant operations. Also, does the subsystem code with parameters $[[8,1,3,3]]_2$ exist?

No nontrivial $[[7,1,1,3]]_2$ exists. There exists a trivial $[[7,1,1,3]]_2$ code obtained by simply extending the $[[7,1,3]]_2$ code as the $[[5,1,3]]_2$ code. We show the smallest subsystem code with length 7 must have at most minimum weight equals to 2. Since $[[7,2,2]]_2$ exists, then we can construct the stabilizer and normalizer matrices as follows.

$$D_S = \begin{bmatrix} X & X & X & X & I & I & I \\ Y & Y & Y & Y & I & I & I \\ I & I & I & I & X & I & I \\ I & I & I & I & I & X & I \\ I & I & I & I & I & I & X \end{bmatrix} \tag{9.6}$$

$$D_S^{\perp} = \begin{bmatrix} X & I & I & X & I & I & I \\ Y & I & I & Y & I & I & I \\ I & X & I & X & I & I & I \\ I & Y & I & Y & I & I & I \\ I & I & X & X & I & I & I \\ I & I & Y & Y & I & I & I \\ I & I & I & I & X & I & I \\ I & I & I & I & I & X & I \\ I & I & I & I & I & I & X \end{bmatrix} \tag{9.7}$$

Clearly, from our construction and using Corollary 89, there must exist a subsystem code with parameters k and r given as follows. $\dim D^{\perp_s} = 9/2$ and $\dim C = 7/2$. Also, $\dim D = 5/2$ and $min(D^{\perp_s} \backslash C) = 2$. Therefore, , $k = (9-7)/2 = 1$ and $r = (7-5)/2 = 1$. Consequently, the parameters of the subsystem code are $[[7,1,1,2]]_2$.

This example shows $[[6,1,1,3]]$ short subsystem code over $\mathbb{F}_3$.

Example 116. *We give a nontrivial short subsystem code over* $\mathbb{F}_3$. *This is derived from the* $[[6,2,3]]_3$ *graph quantum code, see [44] for existence results and [67] for a method to construct the code. Also, we showed an example earlier for an* $[[6,1,1,3]]$

subsystem code over $\mathbb{F}_7$. *Consider the field* $\mathbb{F}_3$ *and let* $C \subseteq \mathbb{F}_3^{12}$ *be a linear code defined by the following generator matrix.*

$$C = \left[\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 2 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 2 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 2 & 2 & 0 & 2 & 0 & 2 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right] = \left[\begin{array}{c} S \\ \hline X_1 \\ Z_1 \end{array}\right].$$

Let the symplectic inner product $\langle (a|b)|(c|d)\rangle_s = a \cdot d - b \cdot c$. *Then the symplectic dual of* C *is generated by*

$$C^{\perp_s} = \left[\begin{array}{c} S \\ \hline X_2 \\ Z_2 \end{array}\right],$$

where $X_2 = \left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 2 & 0 & 0 & 0 \end{array}\right]$ *and* $Z_2 = \left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]$. *The matrix* S *generates the code* $D = C \cap C^{\perp_s}$. *Now* D *defines a* $[[6,2,3]]_3$ *stabilizer code [44, Theorem 3.1] and [67, Theorem 1 and Equation (15)]. Therefore,* $\operatorname{swt}(D^{\perp_s} \setminus D) = 3$. *It follows that* $\operatorname{swt}(D^{\perp_s} \setminus C) \geq \operatorname{swt}(D^{\perp_s}) = 3$. *By [9, Theorem 4], we have a* $[[6, (\dim D^{\perp_s} - \dim C)/2, (\dim C - \dim D)/2, 3]]_3$ *viz. a* $[[6,1,1,3]]_3$ *subsystem code.*

We can also have a trivial $[[6,1,1,3]]_2$ code. This trivial extension seems to argue against the usefulness of subsystem codes and if they will really lead to improvement in performance. An obvious open question is if there exist nontrivial $[[6,1,1,3]]_2$ or $[[7,1,1,3]]_2$ subsystem codes.

F. Conclusion and Discussion

We constructed cyclic subsystem codes by using the defining sets of classical cyclic codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. Also, we presented a simple method to obtain subsystem codes from stabilizer codes and derived optimal subsystem codes from RS codes. In addition, we drove families of subsystem BCH and RS codes. We introduced the short subsystem codes over binary and ternary fields. We leave it as open questions to realize performance and usefulness of these codes. Also, we pose the construction of a nontrivial $[[6,1,1,3]]_2$ code and compare its performance with the $[[5,1,3]]_2$ code as an open problem.

One can derive many other families of subsystem codes using the Euclidean and Hermitian construction of subsystem codes. In addition, one can design the encoding and decoding circuits of cyclic subsystem codes.

Table I. Subsystem BCH codes derived using the Euclidean construction

Subsystem Code	Parent BCH Code C	Designed distance
$[[15,4,3,3]]_2$	$[15,7,5]_2$	4
$[[15,6,1,3]]_2$	$[15,5,7]_2$	6
$[[31,10,1,5]]_2$	$[31,11,11]_2$	8
$[[31,20,1,3]]_2$	$[31,6,15]_2$	12
$[[63,6,21,7]]_2$	$[63,39,9]_2$	8
$[[63,6,15,7]]_2$	$[63,36,11]_2$	10
$[[63,6,3,7]]_2$	$[63,30,13]_2$	12
$[[63,18,3,7]]_2$	$[63,24,15]_2$	14
$[[63,30,3,5]]_2$	$[63,18,21]_2$	16
$[[63,32,1,5]]_2$	$[63,16,23]_2$	22
$[[63,44,1,3]]_2$	$[63,10,27]_2$	24
$[[63,50,1,3]]_2$	$[63,7,31]_2$	28
$[[15,2,5,3]]_4$	$[15,9,5]_4$	4
$[[15,2,3,3]]_4$	$[15,8,6]_4$	6
$[[15,4,1,3]]_4$	$[15,6,7]_4$	7
$[[15,8,1,3]]_4$	$[15,4,10]_4$	8
$[[31,10,1,5]]_4$	$[31,11,11]_4$	8
$[[31,20,1,3]]_4$	$[31,6,15]_4$	12
$[[63,12,9,7]]_4$	$[63,30,15]_4$	15
$[[63,18,9,7]]_4$	$[63,27,21]_4$	16
$[[63,18,7,7]]_4$	$[63,26,22]_4$	22

Table II. Subsystem BCH codes derived using the Hermitian construction

Subsystem Code	Parent BCH Code C	Designed distance
$[[14,1,3,4]]_2$	$[14,8,5]_{2^2}$	6^*
$[[15,1,2,5]]_2$	$[15,8,6]_{2^2}$	6
$[[15,5,2,3]]_2$	$[15,6,7]_{2^2}$	7
$[[16,5,2,3]]_2$	$[16,6,7]_{2^2}$	7^+
$[[17,8,1,4]]_2$	$[17,5,9]_{2^2}$	4
$[[21,6,3,3]]_2$	$[21,9,7]]_{2^2}$	6
$[[21,7,2,3]]_2$	$[21,8,9]_{2^2}$	8
$[[31,10,1,5]]_2$	$[31,11,11]_{2^2}$	8
$[[31,20,1,3]]_2$	$[31,6,15]_{2^2}$	12
$[[32,10,1,5]]_2$	$[32,11,11]_{2^2}$	8^+
$[[32,20,1,3]]_2$	$[32,6,15]_{2^2}$	12^+
$[[25,12,3,3]]_3$	$[25,8,12]_{3^2}$	9^*
$[[26,6,2,5]]_3$	$[26,11,8]_{3^2}$	8
$[[26,12,2,4]]_3$	$[26,8,13]_{3^2}$	9
$[[26,13,1,4]]_3$	$[26,7,14]_{3^2}$	14
$[[80,1,17,20]]_3$	$[80,48,21]_{3^2}$	21
$[[80,5,17,17]]_3$	$[80,46,22]_{3^2}$	22

$*$ punctured code

$+$ Extended code

Table III. Optimal pure subsystem codes

Subsystem Codes	Parent Code (RS Code)
$[[8,1,5,2]]_3$	$[8,6,3]_{3^2}$
$[[8,4,2,2]]_3$	$[8,3,6]_{3^2}$
$[[8,5,1,2]]_3$	$[8,2,7]_{3^2}$
$[[9,1,4,3]]_3$	$[9,6,4]^{\dagger}_{3^2}, \delta=3$
$[[9,4,1,3]]_3$	$[9,3,7]^{\dagger}_{3^2}, \delta=6$
$[[15,1,10,3]]_4$	$[15,12,4]_{4^2}$
$[[15,9,2,3]]_4$	$[15,4,12]_{4^2}$
$[[15,10,1,3]]_4$	$[15,3,13]_{4^2}$
$[[16,1,9,4]]_4$	$[16,12,5]^{\dagger}_{4^2}, \delta=4$
$[[24,1,17,4]]_5$	$[24,20,5]_{5^2}$
$[[24,16,2,4]]_5$	$[24,5,20]_{5^2}$
$[[24,17,1,4]]_5$	$[24,4,21]_{5^2}$
$[[24,19,1,3]]_5$	$[24,3,22]_{5^2}$
$[[24,21,1,2]]_5$	$[24,2,23]_{5^2}$
$[[23,1,18,3]]_5$	$[23,20,4]^{*}_{5^2}, \delta=5$
$[[23,16,3,3]]_5$	$[23,5,19]^{*}_{5^2}, \delta=20$
$[[48,1,37,6]]_7$	$[48,42,7]_{7^2}$

* Punctured code

† Extended code

Table IV. Reed-Solomon(RS) subsystem codes

Subsystem Codes	Parent RS Code
$[[15,1,10,3]]_4$	$[15,12,4]_{4^2}$
$[[15,1,8,3]]_4$	$[15,11,5]_{4^2}$
$[[15,1,6,3]]_4$	$[15,10,6]_{4^2}$
$[[15,2,5,3]]_4$	$[15,9,7]_{4^2}$
$[[24,1,17,4]]_5$	$[24,20,5]_{5^2}$
$[[24,2,10,4]]_5$	$[24,16,9]_{5^2}$
$[[24,4,10,4]]_5$	$[24,15,10]_{5^2}$
$[[24,16,2,4]]_5$	$[24,5,20]_{5^2}$
$[[24,17,1,4]]_5$	$[24,4,21]_{5^2}$
$[[24,19,1,3]]_5$	$[24,3,22]_{5^2}$
$[[48,1,37,6]]_7$	$[48,42,7]_{7^2}$
$[[48,2,26,6]]_7$	$[48,36,13]_{7^2}$

Table V. Families of subsystem codes from stabilizer codes

Family	Stabilizer $[[n,k,d]]_q$	Subsystem $[[n,k-r,r,d]]_q$, $k>r\geq 0$
Short MDS	$[[n,n-2d+2,d]]_q$	$[[n,n-2d+2-r,r,d]]_q$
Hermitian Hamming	$[[n,n-2m,3]]_q$	$m\geq 2$, $[[n,n-2m-r,r,3]]_q$
Euclidean Hamming	$[[n,n-2m,3]]_q$	$[[n,n-2m-r,r,3]]_q$
Melas	$[[n,n-2m,\geq 3]]_q$	$[[n,n-2m-r,r,\geq 3]]_q$
Euclidean BCH	$[[n,n-2m\lceil(\delta-1)(1-1/q)\rceil,\geq\delta]]_q$	$[[n,n-2m\lceil(\delta-1)(1-1/q)\rceil-r, r,\geq\delta]]_q$
Hermitian BCH	$[[n,n-2m\lceil(\delta-1)(1-1/q^2)\rceil,\geq\delta]]_q$	$[[n,n-2m\lceil(\delta-1)(1-1/q^2)\rceil-r, r,\geq\delta]]_q$
Punctured MDS	$[[q^2-q\alpha,q^2-q\alpha-2\nu-2,\nu+2]]_q$	$[[q^2-q\alpha,q^2-q\alpha-2\nu-2-r, r,\nu+2]]_q$
Euclidean MDS	$[[n,n-2d+2]]_q$	$[[n,n-2d+2-r,r]]_q$
Hermitian MDS	$[[q^2-s,q^2-s-2d+2,d]]_q$	$[[q^2-s,q^2-s-2d+2-r,r,d]]_q$
Twisted	$[[q^r,q^r-r-2,3]]_q$	$[[q^r,q^r-r-2-r,r,3]]_q$
Extended twisted	$[[q^2+1,q^2-3,3]]_q$	$[[q^2+1,q^2-3-r,r,3]]_q$
Perfect	$[[n,n-s-2,3]]_q$ $[[n,n-s-2,3]]_q$	$[[n,n-s-2-r,r,3]]_q$ $[[n,n-s-2-r,r,3]]_q$

CHAPTER X

PROPAGATION RULES AND TABLES OF SUBSYSTEM CODE CONSTRUCTIONS

In this chapter I present tables of upper and lower bounds on subsystem code parameters. I derive new subsystem codes from existing ones by extending and shortening the length of the codes. Also, I trade the dimension of subsystem A and co-subsystem B to obtain new subsystem codes from known codes with the same lengths.

A. Introduction

We investigate subsystem codes and study their properties. Given a subsystem code with parameters $[[n, k, r, d]]_q$, we establish propagation rules to derive new subsystem codes with possibly parameters $[[n+1, k, r, \geq d]]_q$, $[[n-1, k-1, \geq r, d]]_q$, etc. We construct tables of the upper bounds on the minimum distance and dimension of subsystem codes using linear programming bounds over $\mathbb{F}_2$ and $\mathbb{F}_3$. Also, we construct tables of lower bounds on subsystem code parameters using Gilbert-Varshamov (GV) bound. We show that our method gives all codes over $\mathbb{F}_2$ for small code length and one can generate more tables over higher fields with large alphabets. Our results provide us with better understanding of subsystem codes in terms of comparing these codes with stabilizer codes. Subsystem codes need $n-k-r$ syndrome measurements in comparison to stabilizer codes that need $n-k$ syndrome measurements. We show that some impure subsystem codes do not give raise to stabilizer codes. Also, such codes do not obey the quantum Hamming bound.

Notation: We assume that q is a power of prime p and $\mathbb{F}_q$ denotes a finite field with q elements. By qudit we mean a q-ary quantum bit. The symplectic weight of an element $w = (x_1, \dots, x_n, y_1, \dots, y_n)$ in $\mathbb{F}_q^{2n}$ is defined as $\text{swt}(w) = |\{(x_i, y_i) \neq$

$(0,0) \mid 1 \leq i \leq n\}|$. The trace-symplectic product of two elements $u = (a|b), v = (a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as $\langle u|v\rangle_s = \operatorname{tr}_{q/p}(a' \cdot b - a \cdot b')$, where $x \cdot y$ is the usual Euclidean inner product. The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as $C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w\rangle_s = 0 \text{ for all } w \in C\}$. For vectors x, y in $\mathbb{F}_{q^2}^n$, we define the Hermitian inner product $\langle x|y\rangle_h = \sum_{i=1}^n x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbb{F}_{q^2}^n$ as $C^{\perp_h} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}$. The trace alternating form of two vectors u, w in $\mathbb{F}_{q^2}^n$ is defined as $\langle u|v\rangle_a = \operatorname{tr}_{q/p}[(\langle u|v\rangle_h - \langle v|u\rangle_h)/(\beta^2 - \beta^{2q})]$, where $\{\beta, \beta^q\}$ is a normal basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. If $C \subseteq \mathbb{F}_{q^2}^n$, then the trace alternating dual of C is defined as $C^{\perp_a} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_a = 0 \text{ for all } y \in C\}$.

B. Upper and Lower Bounds on Subsystem Code Parameters

We want to investigate some limitations on subsystem codes that are constructed in the previous chapters. Bounds on code parameters are useful for many reasons such as the computer search can be minimized. To that end, we will investigate some upper and lower bounds on the parameters of subsystem codes.

Linear Programming Bounds. We will show the linear programming bound as an upper bound on subsystem code parameters. We ensure that one can not hope to obtain subsystem codes unless they obey this bound. This also means that if a subsystem code obeys this bound, it is not guaranteed that the code itself will exist unless it can be constructed. Assume we have the same notation as above.

Theorem 117. *If an $((n, K, R, d))_q$ Clifford subsystem code with $K > 1$ exists, then there exists a solution to the optimization problem: maximize $\sum_{j=1}^{d-1} A_j$ subject to the constraints*

1. $A_0 = B_0 = 1$ and $0 \leq B_j \leq A_j$ for all $1 \leq j \leq n$;

2. $\sum_{j=0}^{n} A_j = q^n R/K$; $\quad \sum_{j=0}^{n} B_j = q^n/KR$;

3. $A_j^{\perp_s} = \frac{K}{q^n R} \sum_{r=0}^{n} K_j(r) A_r$ *holds for all* j *in the range* $0 \le j \le n$;

4. $B_j^{\perp_s} = \frac{KR}{q^n} \sum_{r=0}^{n} K_j(r) B_r$ *holds for all* j *in the range* $0 \le j \le n$;

5. $A_j = B_j^{\perp_s}$ *for all* j *in* $0 \le j < d$ *and* $A_j \le B_j^{\perp_s}$ *for all* $d \le j \le n$;

6. $B_j = A_j^{\perp_s}$ *for all* j *in* $0 \le j < d$ *and* $B_j \le A_j^{\perp_s}$ *for all* $d \le j \le n$;

7. $(p-1)$ *divides* A_j, B_j, $A_j^{\perp_s}$, *and* $B_j^{\perp_s}$ *for all* j *in the range* $1 \le j \le n$;

where the coefficients A_j *and* B_j *assume only integer values, and* $K_j(r)$ *denotes the Krawtchouk polynomial*

$$K_j(r) = \sum_{s=0}^{j} (-1)^s (q^2-1)^{j-s} \binom{r}{s} \binom{n-r}{j-s}. \tag{10.1}$$

Proof. If an $((n, K, R, d))_q$ subsystem code exists, then the weight distribution A_j of the associated additive code C and the weight distribution B_j of its subcode $D = C \cap C^{\perp_s}$ obviously satisfy 1). By Lemma 100, we have $K = q^n/\sqrt{|C||D|}$ and $R = \sqrt{|C|/|D|}$, which implies $|C| = \sum A_j = q^n R/K$ and $|D| = \sum B_j = q^n/KR$, proving 2). Conditions 3) and 4) follow from the MacWilliams relation for symplectic weight distribution, see [81, Theorem 23]. As C is an $\mathbb{F}_p$-linear code, for each nonzero codeword c in C, αc is again in C for all α in $\mathbb{F}_p^\times$; thus, condition 7) must hold. Since the quantum code has minimum distance d, all vectors of symplectic weight less than d in $D^{\perp_s}$ must be in C, since $D^{\perp_s} - C$ has minimum distance d; this implies 5). Similarly, all vectors in $C^{\perp_s} \subseteq C + C^{\perp_s}$ of symplectic weight less than d must be contained in C, since $(C + C^{\perp_s}) - C$ has minimum distance d; this implies 6). $\square$

We can use the previous theorem to derive bounds on the dimension of the co-subsystem. If the optimization problem is not solvable, then we can immediately conclude that a code with the corresponding parameter settings cannot exist. We are able to solve this optimization problem and have constructed Table VII over $\mathbb{F}_2$. Also, Table VIII shows code parameters of subsystem codes over $\mathbb{F}_3$. It is not necessary that the short subsystem codes are binary. The linear programming indicates that there is no subsystem code with parameters $[[6, 1, 1, 3]]_2$. However, there is a subsystem code with parameters $[[6, 1, 1, 3]]_3$ constructed over graphs.

Impure Subsystem Codes and Hamming Bound. The following Lemma shows that there exist some families of subsystem codes that beat the quantum Hamming bound. For stabilizer Hamming codes see the tables given in [81].

Lemma 118. *If there exists an $[[n, k, d]]_q$ stabilizer perfect code and $d' \geq d+2$, then there must be an $[[n, k-r, r, d']]_q$ subsystem code that beats the Hamming bound.*

Proof. We know that the stabilizer code satisfies the Hamming bound

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q^2-1)^i \leq q^{n-k}, \tag{10.2}$$

But the given code is perfect, then the inequality holds. From our construction in Theorem 121, there must exist a subsystem code with the given parameters. Since $\lfloor (d'-1)/2 \rfloor \geq \lfloor (d-1)/2 \rfloor$ then the result is a direct consequence. □

One example to show this Theorem would be Hermitian stabilizer Hamming codes. These codes have parameters $[[n, n-2m, 3]]_q$, where $m \geq 2$, $gcd(m, q^2-1) = 1$ and $n = \frac{q^{2m}-1}{q^2-1}$. Let $q = 2$, and $m = 4$ such that $gcd(m, q^2-1) = 1$, then $n = (q^{2m}-1)/(q^2-1) = 85$. So, there exists a perfect stabilizer Hamming code with parameters $[[85, 77, 3]]_2$. Consequently, there must be a subsystem code with parameters $[[85, 77-r, r, \geq 5]]_2$ that beats Hamming bound. Also, the code $[[341, 331, 3]]_2$ gives us the same result.

The quantum Hamming bound for impure nonbinary stabilizer codes has not been proved for $d \geq 7$, see [2]. Of course if the underline stabilizer code beats Hamming bound, obviously, the subsystem codes would also beat the Hamming bound. The condition in the theorem can be relaxed. It is not necessarily needed the stabilizer code to be perfect but it seems to be hard to find a general theme in this case.

Lower Bounds for Subsystem Codes. We can also present a lower bound of subsystem code parameters known as the Gilbert-Varshamov bound. Our goal is to provide a table of a lower bound on subsystem code parameters, for more details see [9].

Theorem 119. *Let $\mathbb{F}_q$ be a finite field of characteristic p. If K and R are powers of p such that $1 < KR \leq q^n$ and d is a positive integer such that*

$$\sum_{j=1}^{d-1} \binom{n}{j} (q^2-1)^j (q^n KR - q^n R/K) < (p-1)(q^{2n}-1)$$

holds, then an $((n, K, R, \geq d))_q$ subsystem code exists.

Proof. See [9, Thoerem 7]. □

C. Pure Subsystem Code Constructions

Lemma 120. *If there exists a pure $((n, K, R, d))_q$ Clifford subsystem code, then there also exists an $((n, R, K, \geq d))_q$ Clifford subsystem code that is pure to d.*

Proof. By Theorem 122, there exist classical codes $D \subseteq C \subseteq \mathbb{F}_{q^2}^n$ with the parameters $(n, q^n R/K)_{q^2}$ and $(n, q^n/KR)_{q^2}$. Furthermore, since the subsystem code is pure, we have $\mathrm{wt}(D^{\perp_a} \setminus C) = \mathrm{wt}(D^{\perp_a}) = d$. Let us interchange the roles of C and $C^{\perp_a}$, that is, now we construct a subsystem code from $C^{\perp_a}$. The parameters of the resulting subsystem code are given by

$$((n, \sqrt{|D^{\perp_a}|/|C^{\perp_a}|}, \sqrt{|C^{\perp_a}|/|D|}, \mathrm{wt}(D^{\perp_a} \setminus C^{\perp_a})))_q. \tag{10.3}$$

We note that

- $\sqrt{|D^{\perp_a}|/|C^{\perp_a}|} = \sqrt{|C|/|D|} = R$ and
- $\sqrt{|C^{\perp_a}|/|D|} = \sqrt{|D^{\perp_a}|/|C|} = K$.

The minimum distance d' of the resulting code satisfies $d' = \mathrm{wt}(D^{\perp_a} \setminus C^{\perp_a}) \geq \mathrm{wt}(D^{\perp_a}) = d$; the claim about the purity follows from the fact that $\mathrm{wt}(D^{\perp_a}) = d$. $\square$

The following Theorem shows that given a stabilizer code, one can construct subsystem codes with the same length and distance. Various methods of subsystem code constructions have been shown in the previous two chapters.

Theorem 121. *Let q and R be powers of a prime p. If there exists an $((n, K, d))_q$ stabilizer code pure to d', then there exists an $((n, K/R, R, \geq d))_q$ subsystem code that is pure to d'.*

Proof. Let $D \subseteq D^{\perp_s} \subseteq \mathbb{F}_q^{2n}$ be a classical code generated by the $\mathbb{F}_p$-basis $\beta_D = \{z_1, z_2, ..., z_s\}$ where $d = \mathrm{swt}(D^{\perp_s} \backslash D)$. We know that there exists a stabilizer code Q with parameters $((n, K, d))_q$ that it is pure to $d' = \mathrm{swt}(D)$. $\dim Q = |D^{\perp_s}|/|D| = q^n/p^s = p^{nm-s}$, where $q = p^m$.

Let us construct the additive code $C \subseteq D^{\perp_s}$ by expanding the set β_D as follows

$$\begin{aligned} C &= span_{\mathbb{F}_p}(\beta_D, \{z_{s+1}, x_{s+1}, ..., z_{s+r}, x_{s+r}\}) \\ &= < z_1, ..., z_s; z_{s+1}, x_{s+1}, ..., z_{r+s}, x_{s+r} > . \end{aligned}$$

From Lemma [9, Lemma 10], $\langle x_k \,|\, x_\ell \rangle = 0 = \langle z_k \,|\, z_\ell \rangle$ and $\langle x_k \,|\, z_\ell \rangle = \delta_{k,\ell}$, therefore $D \subseteq C$. We notice that the code C does not contain its dual $C^{\perp_s}$ because the elements in C does not commute with each other. The dual code $C^{\perp_s}$ is generated by the set

$$C^{\perp_s} = span_{\mathbb{F}_p}(\beta_D, \{z_{r+s+1}, x_{r+s+1}, ..., z_n, x_n\})$$

The symplectic inner product between any two elements in C and $C^{\perp_s}$ vanishes. We see that $D = C \cap C^{\perp_s} =< z_1, z_2, ..., z_s >$. Therefore, using [9, Theorem 1], there exists a subsystem code $Q_s = A \otimes B$ such that $\dim A = q^n/(|C||D|)^{1/2} = q^n/(p^{2r+s}q^s)^{1/2} = p^{mn-r-s} = K/R$. Also, $\dim B = |C|/|D| = (p^{2r+s}/p^s)^{1/2} = p^r = R$.

If weight of a codeword c in $D^{\perp_s}$ is d, then either $c \in C$ or $c \in D^{\perp_s}\backslash C$. If $c \in D^{\perp_s}\backslash C$, then the subsystem code Q_s has minimum distance d. If $c \in C$ and no other codewords in $D^{\perp_s}\backslash C$ has weight d, then the subsystem code Q_s has minimum distance $\geq d$. Let $wt(D)$ be d', since $D \subseteq C$ then the subsystem code Q_s is pure to d'. □

D. Propagation Rules of Subsystem Codes

In this section we present propagation rules of subsystem code constructions similar to propagation rules of stabilizer code constructions. We show that given a subsystem code with parameters $[[n, k, r, d]]_q$, it is possible to construct new codes with either increase or decrease the length and dimension of the code by one. Also, we can construct new subsystem codes from known two subsystem codes.

Recall Lemmas 100 and 101, there exists a subsystem code Q with parameters $[[n, k, r, d]]_q$ using the Euclidean and Hermitian constructions. The code Q is decomposed into two sub-systems, $Q = A \otimes B$, where $|A| = q^k$ and $|B| = q^r$. From the previous section, if there is an $[[n, k, r, d]]_q$ subsystem code, then there are two classical codes $C, D \in F_{q^2}^n$ such that $D = C \cap C^{\perp_s}$, $X = |C| = q^{n-k+r}$ and $Y = |D| = q^{n-k-r}$. The minimum distance of Q is $d = \min \mathrm{swt}(D^{\perp_s}\backslash C)$. We use this note to show the following Lemmas.

Let $C_1 \leq \mathbb{F}_q^n$ and $C_2\mathbb{F}_q^n$ be two classical codes defined over F_q. The direct sum of C_1 and C_2 is a code $C \leq \mathbb{F}_q^{2n}$ defined as follows

$$C = C_1 \oplus C_2 = \{uv \mid u \in C_1, v \in C_2\}. \tag{10.4}$$

In a matrix form the code C can be described as

$$C = \begin{pmatrix} C_1 & 0 \\ 0 & C_2 \end{pmatrix}$$

An $[n, k_1, d_1]_q$ classical code C_1 is a subcode in an $[c, k_2, d_2]_q$ if every codeword v in C_1 is also a codeword in C_2, hence $k_1 \leq k_2$. We say that an $[[n, k_1, r_1, d_1]]_q$ subsystem code Q_1 is a subcode in an $[[n, k_2, r_2, d_2]]_q$ subsystem code Q_2 if every codeword $|v\rangle$ in Q_1 is also a codeword in Q_2 and $k_1 + r_1 \leq k_2 + r_1$.

Notation. Let q be a power of a prime integer p. We denote by $\mathbb{F}_q$ the finite field with q elements. We use the notation $(x|y) = (x_1, \ldots, x_n|y_1, \ldots, y_n)$ to denote the concatenation of two vectors x and y in $\mathbb{F}_q^n$. The symplectic weight of $(x|y) \in \mathbb{F}_q^{2n}$ is defined as

$$\mathrm{swt}(x|y) = \{(x_i, y_i) \neq (0,0) \,|\, 1 \leq i \leq n\}.$$

We define $\mathrm{swt}(X) = \min\{\mathrm{swt}(x) \,|\, x \in X, x \neq 0\}$ for any nonempty subset $X \neq \{0\}$ of $\mathbb{F}_q^{2n}$.

The trace-symplectic product of two vectors $u = (a|b)$ and $v = (a'|b')$ in $\mathbb{F}_q^{2n}$ is defined as

$$\langle u|v\rangle_s = \mathrm{tr}_{q/p}(a' \cdot b - a \cdot b'),$$

where $x \cdot y$ denotes the dot product and $\mathrm{tr}_{q/p}$ denotes the trace from $\mathbb{F}_q$ to the subfield

$\mathbb{F}_p$. The trace-symplectic dual of a code $C \subseteq \mathbb{F}_q^{2n}$ is defined as

$$C^{\perp_s} = \{v \in \mathbb{F}_q^{2n} \mid \langle v|w\rangle_s = 0 \text{ for all } w \in C\}.$$

We define the Euclidean inner product $\langle x|y\rangle = \sum_{i=1}^{n} x_i y_i$ and the Euclidean dual of $C \subseteq \mathbb{F}_q^n$ as

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x|y\rangle = 0 \text{ for all } y \in C\}.$$

We also define the Hermitian inner product for vectors x, y in $\mathbb{F}_{q^2}^n$ as $\langle x|y\rangle_h = \sum_{i=1}^{n} x_i^q y_i$ and the Hermitian dual of $C \subseteq \mathbb{F}_{q^2}^n$ as

$$C^{\perp_h} = \{x \in \mathbb{F}_{q^2}^n \mid \langle x|y\rangle_h = 0 \text{ for all } y \in C\}.$$

Theorem 122. *Let C be a classical additive subcode of $\mathbb{F}_q^{2n}$ such that $C \neq \{0\}$ and let D denote its subcode $D = C \cap C^{\perp_s}$. If $x = |C|$ and $y = |D|$, then there exists a subsystem code $Q = A \otimes B$ such that*

i) $\dim A = q^n/(xy)^{1/2}$,

ii) $\dim B = (x/y)^{1/2}$.

The minimum distance of subsystem A is given by

(a) $d = \mathrm{swt}((C + C^{\perp_s}) - C) = \mathrm{swt}(D^{\perp_s} - C)$ *if* $D^{\perp_s} \neq C$;

(b) $d = \mathrm{swt}(D^{\perp_s})$ *if* $D^{\perp_s} = C$.

Thus, the subsystem A can detect all errors in E of weight less than d, and can correct all errors in E of weight $\leq \lfloor (d-1)/2 \rfloor$.

Extending Subsystem Codes. We derive new subsystem codes from known ones by extending and shortening the length of the code.

Theorem 123. *If there exists an $((n, K, R, d))_q$ Clifford subsystem code with $K > 1$, then there exists an $((n+1, K, R, \geq d))_q$ subsystem code that is pure to 1.*

Proof. We first note that for any additive subcode $X \leq \mathbb{F}_q^{2n}$, we can define an additive code $X' \leq \mathbb{F}_q^{2n+2}$ by

$$X' = \{(a\alpha|b0) \,|\, (a|b) \in X, \alpha \in \mathbb{F}_q\}.$$

We have $|X'| = q|X|$. Furthermore, if $(c|e) \in X^{\perp_s}$, then $(c\alpha|e0)$ is contained in $(X')^{\perp_s}$ for all α in $\mathbb{F}_q$, whence $(X^{\perp_s})' \subseteq (X')^{\perp_s}$. By comparing cardinalities we find that equality must hold; in other words, we have

$$(X^{\perp_s})' = (X')^{\perp_s}.$$

By Theorem 122, there are two additive codes C and D associated with an $((n, K, R, d))_q$ Clifford subsystem code such that

$$|C| = q^n R/K$$

and

$$|D| = |C \cap C^{\perp_s}| = q^n/(KR).$$

We can derive from the code C two new additive codes of length $2n+2$ over $\mathbb{F}_q$, namely C' and $D' = C' \cap (C')^{\perp_s}$. The codes C' and D' determine a $((n+1, K', R', d'))_q$ Clifford subsystem code. Since

$$\begin{aligned} D' &= C' \cap (C')^{\perp_s} = C' \cap (C^{\perp_s})' \\ &= (C \cap C^{\perp_s})', \end{aligned}$$

we have $|D'| = q|D|$. Furthermore, we have $|C'| = q|C|$. It follows from Theorem 122 that

(i) $K' = q^{n+1}/\sqrt{|C'||D'|} = q^n/\sqrt{|C||D|} = K$,

(ii) $R' = (|C'|/|D'|)^{1/2} = (|C|/|D|)^{1/2} = R$,

(iii) $d' = \operatorname{swt}((D')^{\perp_s} \setminus C') \geq \operatorname{swt}((D^{\perp_s} \setminus C)') = d$.

Since C' contains a vector $(\mathbf{0}\alpha|\mathbf{0}0)$ of weight 1, the resulting subsystem code is pure to 1. $\square$

Corollary 124. *If there exists an $[[n,k,r,d]]_q$ subsystem code with $k > 0$ and $0 \leq r < k$, then there exists an $[[n+1,k,r,\geq d]]_q$ subsystem code that is pure to 1.*

Shortening Subsystem Codes. We can also shorten the length of a subsystem code and still trade the dimensions of the new subsystem code and its co-subsystem code as shown in the following Lemma.

Theorem 125. *If an $((n,K,R,d))_q$ pure subsystem code Q exists, then there is a pure subsystem code Q_p with parameters $((n-1,qK,R,\geq d-1))_q$.*

Proof. We know that existence of the pure subsystem code Q with parameters $((n,K,R,d))_q$ implies existence of a pure stabilizer code with parameters $((n,KR,\geq d))_q$ for $n \geq 2$ and $d \geq 2$ from [6, Theorem 2.]. By [81, Theorem 70], there exist a pure stabilizer code with parameters $((n-1,qKR,\geq d-1))_q$. This stabilizer code can be seen as $((n-1,qKR,0,\geq d-1))_q$ subsystem code. By using [6, Theorem 2.], there exists a pure $\mathbb{F}_q$-linear subsystem code with parameters $((n-1,qK,R,\geq d-1))_q$ that proves the claim. $\square$

Analog of the previous Theorem is the following Lemma.

Lemma 126. *If an $\mathbb{F}_q$-linear $[[n,k,r,d]]_q$ pure subsystem code Q exists, then there is a pure subsystem code Q_p with parameters $[[n-1,k+1,r,\geq d-1]]_q$.*

Proof. We know that existence of the pure subsystem code Q implies existence of a pure stabilizer code with parameters $[[n,k+r,\geq d]]_q$ for $n \geq 2$ and $d \geq 2$ by using [6, Theorem 2. and Theorem 5.]. By [81, Theorem 70], there exist a pure stabilizer code with parameters $[[n-1, k+r+1, \geq d-1]]_q$. This stabilizer code can be seen as an $[[n-1, k+r+1, 0, \geq d-1]]_q$ subsystem code. By using [6, Theorem 3.], there exists a pure $\mathbb{F}_q$-linear subsystem code with parameters $[[n-1, k+1, r, \geq d-1]]_q$ that proves the claim. $\square$

We can also prove the previous Theorem by defining a new code C_p from the code C as follows.

Theorem 127. *If there exists a pure subsystem code $Q = A \otimes B$ with parameters $((n, K, R, d))_q$ with $n \geq 2$ and $d \geq 2$, then there is a subsystem code Q_p with parameters $((n-1, K, qR, \geq d-1))_q$.*

Proof. By Theorem 122, if an $((n, K, R, d))_q$ subsystem code Q exists for $K > 1$ and $1 \leq R < K$, then there exists an additive code $C \in \mathbb{F}_q^{2n}$ and its subcode $D \leq \mathbb{F}_q^{2n}$ such that $|C| = q^n R/K$ and $|D| = |C \cap C^{\perp_s}| = q^n/KR$. Furthermore, $d = \min \operatorname{swt}(D^{\perp_s} \backslash C)$. Let $w = (w_1, w_2, \ldots, w_n)$ and $u = (u_1, u_2, \ldots, u_n)$ be two vectors in $\mathbb{F}_q^n$. W.l.g., we can assume that the code $D^{\perp_s}$ is defined as

$$D^{\perp_s} = \{(u|w) \in \mathbb{F}_q^{2n} \mid w, u \in \mathbb{F}_q^n\}.$$

Let $w_{-1} = (w_1, w_2, \ldots, w_{n-1})$ and $u_{-1} = (u_1, u_2, \ldots, u_{n-1})$ be two vectors in $\mathbb{F}_q^{n-1}$. Also, let $D_p^{\perp_s}$ be the code obtained by puncturing the first coordinate of $D^{\perp_s}$, hence

$$D_p^{\perp_s} = \{(u_{-1}|w_{-1}) \in \mathbb{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbb{F}_q^{n-1}\}.$$

since the minimum distance of $D^{\perp_s}$ is at least 2, it follows that $|D_p^{\perp_s}| = |D^{\perp_s}| = K^2|C| = K^2 q^n R/K = q^n RK$ and the minimum distance of $D_p^{\perp_s}$ is at least $d-1$.

Now, let us construct the dual code of $D_p^{\perp_s}$ as follows.

$$\begin{aligned}(D_p^{\perp_s})^{\perp_s} &= \{(u_{-1}|w_{-1}) \in \mathbb{F}_q^{2n-2} \mid \\ &\qquad (0u_{-1}|0w_{-1}) \in D, w_{-1}, u_{-1} \in \mathbb{F}_q^{n-1}\}.\end{aligned}$$

Furthermore, if $(u_{-1}|w_{-1}) \in D_p$, then $(0u_{-1}|0w_{-1}) \in D$. Therefore, D_p is a self-orthogonal code and it has size given by

$$|D_p| = q^{2n-2}/|D_p^{\perp_s}| = q^{n-2}/RK.$$

We can also puncture the code C to the code C_p at the first coordinate, hence

$$\begin{aligned}C_p &= \{(u_{-1}|w_{-1}) \in \mathbb{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbb{F}_q^{n-1}, \\ &\qquad (aw_{-1}|bu_{-1}) \in C, a, b \in F_q\}.\end{aligned}$$

Clearly, $D \subseteq C$ and if $a = b = 0$, then the vector $(0u_{-1}|0w_{-1}) \in D$, therefore, $(u_{-1}, w_{-1}) \in D_p$. This gives us that $D_p \subseteq C_p$. Furthermore, hence $|C| = |C_p|$. The dual code $C_p^{\perp_s}$ can be defined as

$$\begin{aligned}C_p^{\perp_s} &= \{(u_{-1}|w_{-1}) \in \mathbb{F}_q^{2n-2} \mid w_{-1}, u_{-1} \in \mathbb{F}_q^{n-1}, \\ &\qquad (ew_{-1}|fu_{-1}) \in C^{\perp_s}, e, f \in F_q\}.\end{aligned}$$

Also, if $e = f = 0$, then $D_p \subseteq C_p^{\perp_s}$, furthermore,

$$D_p^{\perp_s} = C_p \cup C_p^{\perp_s} = \{(u_{-1}|w_{-1}) \in \mathbb{F}_q^{2n-2} \mid \tag{10.5}$$

$$(0u_{-1}|0w_{-1}) \in D\} \tag{10.6}$$

Therefore there exists a subsystem code $Q_p = A_p \otimes B_p$. Also, the code $D_p^{\perp_s}$ is pure and has minimum distance at least $d - 1$. We can proceed and compute the dimension of subsystem A_p and co-subsystem B_p from Theorem 122 as follows.

(i) $K_p = q^{n-1}/\sqrt{|C_p||D_p|} = q^{n-1}/\sqrt{(q^nR/K)(q^{n-2}/RK)} = K$,

(ii) $R_p = (|C_p|/|D'_p|)^{1/2} = ((q^nR/K)/(q^{n-2}/RK))^{1/2} = qR$,

(iii) $d_p = \operatorname{swt}((D_p)^{\perp_s} \setminus C_p) = \operatorname{swt}((D^{\perp_s} \setminus C_p)) \geq d-1$.

Therefore, there exists a subsystem cod with parameters $((n-1, K, qR, \geq d-1))_q$.

The minimum distance condition follows since the code Q has $d = \min \operatorname{swt}(D^{\perp_s} \backslash C)$ and the code Q_p has minimum distance as Q reduced by one. So, the minimum weight of $D_p^{\perp_s} \backslash C_p$ is at least the minimum weight of $(D^{\perp_s} \backslash C) - 1$

$$\begin{aligned} d_p &= \min \operatorname{swt}({D_p}^{\perp_s} \backslash C_p) \\ &\geq \min \operatorname{swt}(D^{\perp_s} \backslash C) - 1 = d - 1 \end{aligned}$$

If the code Q is pure, then $\min \operatorname{swt}(D^{\perp_s}) = d$, therefore, the new code Q_p is pure since $d_p = \min \operatorname{swt}(D_p^{\perp_s}) \geq d$.

We conclude that if there is a subsystem code with parameters $((n-1, K, qR, \geq d-1))_q$, using [6, Theorem 2.], there exists a code with parameters $((n-1, qK, R, \geq d-1))_q$. $\square$

Reducing Dimension. We also can reduce dimension of the subsystem code for fixed length n and minimum distance d, and still obtain a new subsystem code with improved minimum distance as shown in the following results.

Theorem 128. *If a (pure)$\mathbb{F}_q$-linear $[[n, k, r, d]]_q$ subsystem code Q exists for $d \geq 2$, then there exists an $\mathbb{F}_q$-linear $[[n, k-1, r, d_e]]_q$ subsystem code Q_e (pure to d) such that $d_e \geq d$.*

Proof. Existence of the $[[n, k, r, d]]_q$ subsystem code Q, implies existence of two additive codes $C \leq \mathbb{F}_q^{2n}$ and $D \leq \mathbb{F}_q^{2n}$ such that $|C| = q^{n-k+r}$ and $|D| = |C \cap C^{\perp_s}| = q^{n-k-r}$. Furthermore, $d = \min \operatorname{swt}(D^{\perp_s} \backslash C)$ and $D \subseteq D^{\perp_s}$.

The idea of the proof comes by extending the code D by some vectors from $D^{\perp_s}\backslash(C \cup C^{\perp_s})$. Let us choose a code D_e of size $|q^{n+1-r-k}| = q|D|$. We also ensure that the code D_e is self-orthogonal. Clearly extending the code D to D_e will extend both the codes C and $C^{\perp_s}$ to C_e and $C_e^{\perp_s}$, respectively. Hence $C_e = q|C| = q^{n+1+r-k}$ and $D_e = C_e \cap C_e^{\perp_s}$.

There exists a subsystem code Q_e stabilized by the code C_e. The result follows by computing parameters of the subsystem code $Q_e = A_e \otimes B_e$.

(i) $K_e = q^n/\sqrt{|C_e||D_e|} = q^n/((q^{n+1+r-k})(q^{n+1-k-r}))^{1/2} = q^{k-1}$,

(ii) $R_e = (|C_e|/|D_e|)^{1/2} = ((q^{n+1}R/K)/(q^{n+1}/RK))^{1/2} = q^r$,

(iii) $d_e = \operatorname{swt}((D_e)^{\perp_s} \setminus C_e) \geq \operatorname{swt}((D^{\perp_s} \setminus C_e)) = d$. If the inequality holds, then the code is pure to d.

Arguably, It follows that the set $(D_e^{\perp_s}\backslash C_e)$ is a subset of the set $D^{\perp_s}\backslash C$ because $C \leq C_e$, hence the minimum weight d_e is at least d. □

Lemma 129. *Suppose an $[[n, k, r, d]]_q$ linear pure subsystem code Q exists generated by the two codes $C, D \leq \mathbb{F}_q^{2n}$. Then there exist linear $[[n-m, k', r', d']]_q$ and $[[n-m, k'+r'-r'', r'', d']]_q$ subsystem codes with $k' \geq k-m$, $r' \geq r$, $0 \leq r'' < k'+r'$, and $d' \geq d$ for any integer m such that there exists a codeword of weight m in $(D^{\perp_s}\backslash C)$.*

Proof. [Sketch] This lemma 129 can be proved easily by mapping the subsystem code Q into a stabilizer code. By using [30, Theorem 7.], and the new resulting stabilizer code can be mapped again to a subsystem code with the required parameters. □

Combining Subsystem Codes We can also construct new subsystem codes from given two subsystem codes. The following theorem shows that two subsystem codes can be merged together into one subsystem code with possibly improved distance or dimension.

Theorem 130. *Let Q_1 and Q_2 be two pure binary subsystem codes with parameters $[[n_1, k_1, r_1, d_1]]_2$ and $[[n_2, k_2, r_2, d_2]]_2$ for $k_2 + r_2 \leq n_1$, respectively. Then there exists a subsystem code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1 - r, r, d]]_2$, where $d \geq min\{d_1, d_1 + d_2 - k_2 - r_2\}$ and $0 \leq r < k_1 + r_1$.*

Proof. Existence of an $[[n_i, k_i, r_i, d_i]]_2$ pure subsystem code Q_i for $i \in \{1, 2\}$, implies existence of a pure stabilizer code S_i with parameters $[[n_i, k_i+r_i, d_i]]_2$ with $k_2+r_2 \leq n_1$, see [6]. Therefore, by [30, Theorem 8.], there exists a stabilizer code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1, d]]_2$, $d \geq \min\{d_1, d_1 + d_2 - k_2 - r_2\}$. But this code gives us a subsystem code with parameters $[[n_1 + n_2 - k_2 - r_2, k_1 + r_1 - r, r, \geq d]]_2$ with $k_2 + r_2 \leq n_1$ and $0 \leq r < k_1 + r_1$ that proves the claim. □

Theorem 131. *Let Q_1 and Q_2 be two pure subsystem codes with parameters $[[n, k_1, r_1, d_1]]_q$ and $[[n, k_2, r_2, d_2]]_q$, respectively. If $Q_2 \subseteq Q_1$, then there exists an $[[2n, k_1 + k_2 + r_1 + r_2 - r, r, d]]_q$ pure subsystem code with minimum distance $d \geq \min\{d_1, 2d_2\}$ and $0 \leq r < k_1 + k_2 + r_1 + r_2$.*

Proof. Existence of a pure subsystem code with parameters $[[n, k_i, r_i, d_i]]_q$ implies existence of a pure stabilizer code with parameters $[[n, k_i + r_i, d_i]]_q$ using [6, Theorem 4.]. But by using [81, Lemma 74.], there exists a pure stabilizer code with parameters $[[2n, k_1 + k_2 + r_1 + r_2, d]]_q$ with $d \geq \min\{2d_2, d_1\}$. By [6, Theorem 2., Corollary 6.], there must exist a pure subsystem code with parameters $[[2n, k_1+k_2+r_1+r_2-r, r, d]]_q$ where $d \geq \min\{2d_2, d_1\}$ and $0 \leq r < k_1 + k_2 + r_1 + r_2$, which proves the claim. □

We can recall the trace alternative product between two codewords of a classical code and the proof of Theorem 131 can be stated as follows.

Lemma 132. *Let Q_1 and Q_2 be two pure subsystem codes with parameters $[[n, k_1, r_1, d_1]]_q$ and $[[n, k_2, r_2, d_2]]_q$, respectively. If $Q_2 \subseteq Q_1$, then there exists an $[[2n, k_1 + k_2, r_1 + r_2, d]]_q$ pure subsystem code with minimum distance $d \geq \min\{d_1, 2d_2\}$.*

Proof. Existence of the code Q_i with parameters $[[n, K_i, R_i, d_i]]_q$ implies existence of two additive codes C_i and D_i for $i \in \{1, 2\}$ such that $|C_i| = q^n R_i/K_i$ and $|D_i| = |C \cup C^{\perp_s}| = q^n/R_i K_i$.

We know that there exist additive linear codes $D_i \subseteq D_i^{\perp_a}$, $D_i \subseteq C_i$, and $D_i \subseteq C_i^{\perp_a}$. Furthermore, $D_i = C_i \cap C_i^{\perp_a}$ and $d_i = wt(D_i^{\perp_a} \backslash C_i)$. Also, $C_i = q^{n+r_i-k_i}$ and $|D| = q^{n-r_i-k_i}$.

Using the direct sum definition between to linear codes, let us construct a code D based on D_1 and D_2 as

$$D = \{(u, u + v) \mid u \in D_1, v \in D_2\} \leq \mathbb{F}_{q^2}^{2n}.$$

The code D has size of $|D| = q^{2n-(r_1+r_2+k_1+k_2)=|D_1||D_2|}$. Also, we can define the code C based on the codes C_1 and C_2 as

$$C = \{(a, a + b) \mid a \in C_1, b \in C_2\} \leq \mathbb{F}_{q^2}^{2n}.$$

The code C is of size $|C| = |C_1||C_2| = q^{2n+r_1+r_2-k_1-k_2}$. But the trace-alternating dual of the code D is

$$D^{\perp_a} = \{(u' + v'|, v') \mid u' \in D_1^{\perp_a}, v' \in D_2^{\perp_a}\}.$$

We notice that $(u' + v', v')$ is orthogonal to $(u, u + v)$ because, from properties of the product,

$$\begin{aligned}\langle (u, u+v) \mid (u'+v', v')\rangle_a &= \langle u \mid u'+v'\rangle_a + \langle u+v \mid v'\rangle_a \\ &= 0\end{aligned}$$

holds for $u \in D_1, v \in D_2, u' \in D_1^{\perp_a}$, and $v' \in D_2^{\perp_a}$.

Therefore, $D \subseteq D^{\perp_a}$ is a self-orthogonal code with respect to the trace alternating product. Furthermore, $C^{\perp_a} = \{(a'+b', b') \mid a' \in C_1^{\perp_a}, b' \in C_2^{\perp_a}\}$. Hence, $C \cap C^{\perp_a} = \{(a, a+b) \cap (aa+b', b')\} = D$. Therefore, there exists an $\mathbb{F}_q$-linear subsystem code $Q = A \otimes B$ with the following parameters.

i)

$$\begin{aligned}K &= |A| = q^{2n}/(|C||D|)^{1/2} \\ &= \frac{q^{2n}}{\sqrt{(q^{2n}R_1R_2/K_1K_2)(q^{2n}/K_1K_2R_1R_2)}} \\ &= \frac{q^{2n}}{\sqrt{q^{2n+r_1+r_2-k_1-k_2}q^{2n-r_1-r_2-k_1-k_2}}} \\ &= q^{k_1k_2} = K_1K_2.\end{aligned}$$

ii) $R = (\frac{|C|}{|D|})^{1/2} = R_1R_2$.

iii) the minimum distance is a direct consequence.

□

Theorem 133. *If there exist two pure subsystem quantum codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively. Then there exists a pure subsystem code Q' with parameters $[[n_1+n_2, k_1+k_2+r_1+r_2-r, r, \geq \min(d_1, d_2)]]_q$.*

Proof. This Lemma can be proved easily from [6, Theorem 5.] and [81, Lemma 73.]. The idea is to map a pure subsystem code to a pure stabilizer code, and once again map the pure stabilizer code to a pure subsystem code. □

Theorem 134. *If there exist two pure subsystem quantum codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively. Then there exists a pure subsystem code Q' with parameters $[[n_1 + n_2, k_1 + k_2, r_1 + r_2, \geq \min(d_1, d_2)]]_q$.*

Proof. Existence of the code Q_i with parameters $[[n, K_i, R_i, d_i]]_q$ implies existence of two additive codes C_i and D_i for $i \in \{1, 2\}$ such that $|C_i| = q^n R_i/K_i$ and $|D_i| = |C \cup C^{\perp_s}| = q^n/R_iK_i$.

Let us choose the codes C and D as follows.

$$C = C_1 \oplus C_2 = \{uv \mid v \in C_1, v \in C_2\},$$

and

$$D = D_1 \oplus D_2 = \{ab \mid a \in D_1, b \in C_2\},$$

respectively. From this construction, and since D_1 and D_2 are self-orthogonal codes, it follows that D is also a self-orthogonal code. Furthermore, $D_1 \subseteq C_1$ and $D_2 \subseteq C_2$, then

$$D_1 \oplus D_2 \subseteq C_1 \oplus C_2,$$

hence $D \subseteq C$. The code C is of size

$$\begin{aligned} |C| &= |C_1||C_2| = q^{(n_1+n_2)-(k_1+k_2)+(r_1+r_2)} \\ &= q^{n_1}q^{n_2}R_1R_2/K_1K_2 \end{aligned}$$

and D is of size

$$\begin{aligned} |D| &= |D_1||D_2| = q^{(n_1+n_2)-(k_1+k_2)-(r_1+r_2)} \\ &= q^{n_1}q^{n_2}/R_1R_2K_1K_2. \end{aligned}$$

On the other hand,

$$C^{\perp_s} = (C_1 \oplus C_2)^{\perp_s} = C_2^{\perp_s} \oplus C_1^{\perp_s} \supseteq D_2 \oplus D_1.$$

Furthermore, $C \cap C^{\perp_s} = (C_1 \oplus C_2) \cap (C_2^{\perp_s} \cap C_1^{\perp_s}) = D$.

Therefore, there exists a subsystem code $Q = A \otimes B$ with the following parameters.

i)

$$\begin{aligned} K &= |A| = q^{n_1+n_2}/(|C||D|)^{1/2} \\ &= \frac{q^{n_1+n_2}}{\sqrt{(q^{n_1+n_2}R_1R_2/K_1K_2)(q^{n_1+n_2}/K_1K_2R_1R_2)}} \\ &= \frac{q^{n_1+n_2}}{\sqrt{q^{n_1+n_2+r_1+r_2-k_1-k_2}q^{n_1+n_2-r_1-r_2-k_1-k_2}}} \\ &= q^{k_1k_2} = K_1K_2 = |A_1||A_2|. \end{aligned}$$

ii)

$$\begin{aligned} R &= (\frac{|C|}{|D|})^{1/2} = \sqrt{\frac{q^{n_1}q^{n_2}R_1R_2/K_1K_2}{q^{n_1}q^{n_2}/R_1R_2K_1K_2}} \\ &= R_1R_2 = |B_1||B_2|. \end{aligned}$$

iii) the minimum weight of $D^{\perp_s} \backslash C$ is at least the minimum weight of $D_1^{\perp_s} \backslash C_1$ or $D_2^{\perp_s} \backslash C_2$.

$$\begin{aligned} d &= \min\{\mathrm{swt}(D_1^{\perp_s} \backslash C_1), (D_2^{\perp_s} \backslash C_2)\} \\ &\geq \min\{d_1, d_2\}. \end{aligned}$$

□

Theorem 135. *Given two pure subsystem codes Q_1 and Q_2 with parameters $[[n_1, k_1, r_1, d_1]]_q$ and $[[n_2, k_2, r_2, d_2]]_q$, respectively, with $k_2 \leq n_1$. An $[[n_1+n_2-k_2, k_1+r_1+r_2-r, r, d]]_q$*

Table VI. Existence of subsystem propagation rules

n \ k	k-1	k	k+1
n-1	$[r+2,d-1]_q$	$[\leq r+2,d]_q$, $[r+1,d-1]_q$	$[r,d-1]_q$
n	$[r+1,d]_q$, $[r+1,\geq d]_q$	$[r,d]_q \rightarrow [\leq r,\geq d]_q$ $\rightarrow [\geq r,\leq d]_q$	$[r-1,d]_q$
n+1	$[\geq r,\geq d]_q$	$[\geq r,d]_q$, $[r,\geq d]_q$	

subsystem code exists such that $d \geq \min\{d_1, d_1+d_2-k_2\}$ *and* $0 \leq r < k_1+r_1+r_2$.

Proof. The proof is a direct consequence as shown in the previous theorems. □

Theorem 136. *If an* $((n,K,R,d))_{q^m}$ *pure subsystem code exists, then there exists a pure subsystem code with parameters* $((nm,K,R,\geq d))_q$. *Consequently, if a pure subsystem code with parameters* $((nm,K,R,\geq d))_q$ *exists, then there exist a subsystem code with parameters* $((n,K,R,\geq \lfloor d/m \rfloor))_{q^m}$..

Proof. Existence of a pure subsystem code with parameters $((n,K,R,d))_{q^m}$ implies existence of a pure stabilizer code with parameters $((n,KR,d))_{q^m}$ using [6, Theorem 5.]. By [81, Lemma 76.], there exists a stabilizer code with parameters $((nm,KR,\geq d))_q$. From [6, Theorem 2,5.], there exists a pure subsystem code with parameters $((nm,K,R,\geq d))_q$ that proves the first claim. By [81, Lemma 76.] and [6, Theorem 2,5.], and repeating the same proof, the second claim is a consequence. □

Table VII. Upper bounds on subsystem code parameters using linear programming, $q = 2$

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=6	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),							
	(3,2),	(2,2),	(1,2),									
	(1,3),											
n=7	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),						
	(4,2),	(3,2),	(2,2),	(1,2),								
	(2,3),											
n=8	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),					
	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),							
	(3,3),	(2,3),										
n=9	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),				
	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),						
	(4,3),	(3,3),	(2,3),									
	(2,4),											
n=10	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),			
	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),					
	(5,3),	(4,3),	(3,3),	(1,3),								
	(3,4),	(2,4),										
n=11	(10,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),		
	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),				
	(6,3),	(5,3),	(4,3),	(3,3),	(1,3),							
	(4,4),	(3,4),	(2,4),									
	(2,5),											
n=12	(11,1),	(10,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),	
	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),			
	(7,3),	(6,3),	(5,3),	(4,3),	(3,3),	(1,3),						
	(5,4),	(4,4),	(3,4),	(1,4),								
	(3,5),	(1,5),										
n=13	(12,1),	(11,1),	(10,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),
	(9,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),		
	(8,3),	(7,3),	(6,3),	(5,3),	(4,3),	(3,3),						
	(6,4),	(5,4),	(4,4),	(3,4),	(1,4),							
	(4,5),	(3,5),										
	(1,6),											

Table VII. Continued

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=14	(13,1),	(12,1),	(11,1),	(10,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),
	(10,2),	(10,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),	
	(9,3),	(8,3),	(7,3),	(6,3),	(5,3),	(4,3),	(2,3),					
	(7,4),	(6,4),	(5,4),	(4,4),	(3,4),							
	(5,5),	(4,5),	(2,5),									
	(3,6),											
n=15	(14,1),	(13,1),	(12,1),	(11,1),	(10,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),
	(12,2),	(11,2),	(10,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),
	(10,3),	(9,3),	(8,3),	(7,3),	(6,3),	(5,3),	(4,3),	(2,3),				
	(8,4),	(7,4),	(6,4),	(5,4),	(4,4),	(2,4),						
	(6,5),	(5,5),	(4,5),	(2,5),								
	(4,6),	(3,6),										
n=16	(15,1),	(14,1),	(13,1),	(11,1),	(11,1),	(10,1),	(9,1),	(8,1),	(6,1),	(6,1),	(5,1),	(4,1),
	(13,2),	(12,2),	(11,2),	(10,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),
	(11,3),	(10,3),	(9,3),	(8,3),	(7,3),	(6,3),	(5,3),	(4,3),	(2,3),			
	(9,4),	(8,4),	(7,4),	(6,4),	(5,4),	(4,4),	(2,4),					
	(7,5),	(6,5),	(5,5),	(4,5),	(1,5),							
	(5,6),	(4,6),	(2,6),									
	(1,7),											
n=17	(14,1),	(15,1),	(14,1),	(13,1),	(11,1),	(10,1),	(10,1),	(9,1),	(8,1),	(7,1),	(5,1),	(4,1),
	(14,2),	(13,2),	(12,2),	(11,2),	(9,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),
	(12,3),	(11,3),	(10,3),	(9,3),	(8,3),	(7,3),	(6,3),	(5,3),	(4,3),	(1,3),		
	(9,4),	(9,4),	(8,4),	(7,4),	(6,4),	(5,4),	(4,4),	(2,4),				
	(8,5),	(7,5),	(6,5),	(5,5),	(3,5),							
	(6,6),	(5,6),	(4,6),	(1,6),								
	(4,7),	(1,7),										
n=18	(17,1),	(15,1),	(15,1),	(13,1),	(13,1),	(12,1),	(11,1),	(9,1),	(8,1),	(8,1),	(6,1),	(5,1),
	(13,2),	(14,2),	(12,2),	(11,2),	(11,2),	(10,2),	(9,2),	(8,2),	(7,2),	(6,2),	(5,2),	(4,2),
	(13,3),	(12,3),	(11,3),	(10,3),	(9,3),	(8,3),	(7,3),	(6,3),	(5,3),	(3,3),	(1,3),	
	(11,4),	(10,4),	(9,4),	(8,4),	(7,4),	(6,4),	(5,4),	(4,4),	(1,4),			
	(9,5),	(8,5),	(7,5),	(6,5),	(5,5),	(2,5),						
	(7,6),	(6,6),	(4,6),	(3,6),								
	(5,7),	(4,7),										

Table VIII. Upper bounds on subsystem code parameters using linear programming, $q = 3$

n/k	k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8	k=9	k=10	k=11	k=12
n=4	(3,1),	(2,1),	(1,1),									
	(1,2),											
n=5	(4,1),	(3,1),	(2,1),	(1,1),								
	(2,2),	(1,2),										
n=6	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),							
	(3,2),	(2,2),	(1,2),									
	(1,3),											
n=7	(4,1),	(4,1),	(4,1),	(3,1),	(2,1),	(1,1),						
	(4,2),	(3,2),	(2,2),	(1,2),								
	(2,3),	(1,3),										
n=8	(5,1),	(5,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),					
	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),							
	(3,3),	(2,3),	(1,3),									
	(1,4),											
n=9	(6,1),	(5,1),	(6,1),	(4,1),	(4,1),	(3,1),	(1,1),	(1,1),				
	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),						
	(3,3),	(3,3),	(2,3),	(1,3),								
	(2,4),	(1,4),										
n=10	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),	(2,1),	(1,1),			
	(7,2),	(6,2),	(5,2),	(4,2),	(3,2),	(2,2),	(1,2),					
	(5,3),	(4,3),	(3,3),	(2,3),	(1,3),							
	(3,4),	(2,4),	(1,4),									
	(1,5),											
n=11	(10,1),	(9,1),	(7,1),	(7,1),	(6,1),	(5,1),	(4,1),	(2,1),	(2,1),			
	(7,2),	(7,2),	(5,2),	(5,2),	(4,2),	(3,2),	(1,2),	(1,2),				
	(6,3),	(5,3),	(4,3),	(3,3),	(2,3),	(1,3),						
	(4,4),	(3,4),	(2,4),	(1,4),								
	(2,5),	(1,5),										
n=12	(10,1),	(9,1),	(9,1),	(8,1),	(7,1),	(6,1),	(5,1),	(4,1),	(3,1),			
	(8,2),	(6,2),	(4,2),	(4,2),	(3,2),	(2,2),	(2,2),	(2,2),	(1,2),			
	(6,3),	(6,3),	(5,3),	(4,3),	(3,3),	(2,3),						
	(5,4),	(4,4),	(3,4),	(2,4),	(1,4),							
	(3,5),	(2,5),	(1,5),									
	(1,6),											

E. Conclusion and Discussion

We have established a number of subsystem code constructions. In particular, we have shown how one can derive subsystem codes from stabilizer codes. In combination with the propagation rules that we have derived, one can easily create tables with the best known subsystem codes. Table VI. shows the propagation rules of subsystem code parameters and what the rules are to derive new subsystem codes from existing ones. We will construct tables of subsystem code parameters over binary and finite fields.

Tables VII and VIII present upper bounds on subsystem code parameters using the linear programming bound implemented using MAGMA [27] and Matlab 0.7 programs, for small code lengths. As a future research, designing the encoding and decoding circuits of subsystem codes will be conducted as well as deriving tables of upper bounds for large code lengths. Finally, it will be interesting to derive sharp upper and lower bounds on subsystem code parameters.

CHAPTER XI

QUANTUM CONVOLUTIONAL CODES

A. Introduction

Quantum information is sensitive to noise and needs error correction and recovery strategies. Quantum block error-correcting code (QBC) and quantum convolutional codes (QCC) are means to protect quantum information against noise. The theory of stabilizer block error-correcting codes is widely studied over binary and finite fields, see for example [16, 30, 81, 123] and references therein. Quantum convolutional codes (QCC) have not been studied well over binary and finite fields. There remain many interesting and open questions regarding the properties and the usefulness of quantum convolutional codes. At this point in time, it is not known if quantum convolutional codes offer a decisive advantage over quantum block codes. However, it appears that quantum convolutional codes are more suitable for quantum communications.

In this chapter, we extend the theory of quantum convolutional codes over finite fields generalizing some of the previously known results. After a brief review of previous work in quantum convolutional codes, we give the necessary background in classical and quantum convolutional codes in Sections C and D. We reformulate the necessary terminology of the theory of quantum convolutional codes. Then in the next two chapters, we construct families of quantum convolutional codes based on classical codes [10].

B. Previous Work on QCC

We review the previous work on quantum convolutional codes. There have been examples of quantum convolutional codes in literature; the most notable being the

$((5,1,3))$ code of Ollivier and Tillich, the $((4,1,3))$ code of Almeida and Palazzo and the rate 1/3 codes of Forney and Guha.

- Chau initiated the early work in quantum convolutional codes [33, 34]. However, there are negative arguments about his work [39] and many authors are divided whether his codes are truly quantum convolutional codes or not.

- Ollivier and Tillich developed the stabilizer framework for quantum convolutional codes. They also addressed the encoding and decoding aspects of quantum convolutional codes [112–115]. Furthermore, they provided a maximum likelihood error estimation algorithm. They showed, as an example, a code of rate $k/n = 1/5$ that can correct only one error.

- Almedia and Palazzo constructed a concatenated convolutional code of rate 1/4 with memory $m = 3$; i.e. a ((4,1,3)) code as shown in [40]. Their construction is valid only a specific code parameter. It would be interesting if their work can be generalized, if possible, to any two arbitrary concatenated codes.

- Kong and Parhi constructed quantum convolutional codes with rates $1/(n+1)$ and $1/n$ from a classical convolutional codes with rates $1/n$ and $1/(n-1)$, see [92, 93]. Their work was not a general approach for any quantum convolutional codes, with arbitrary rate k/n and $k > 1$.

- Forney and Guha constructed quantum convolutional codes with rate 1/3 [50]. Also, together with Grassl, they derived rate $(n-2)/n$ quantum convolutional codes [49]. They gave tables of optimal rate 1/3 quantum convolutional codes and they also constructed good quantum block codes obtained by tail-biting convolutional codes.

- Grassl and Rötteler constructed quantum convolutional codes from product codes. They showed that starting with an arbitrary convolutional code and a self-orthogonal block code, a quantum convolutional code can be constructed [68].

- Recently, Grassl and Rötteler [70] gave a general algorithm to construct quantum circuits for non-catastrophic encoders and encoder inverses for channels with memories. Unfortunately, the encoder they derived is for a subcode of the original code.

It is apparent from the discussion above that several issues need to be addressed regarding the efficiency of the decoding algorithms and encoding circuits for quantum convolutional codes. Somewhat surprisingly there has been no work done on the bounds of quantum convolutional codes. In this chapter we address this problem partially by giving a bound for a class of QCC. This bound is somewhat similar to the generalized Singleton bound for classical convolutional codes.

Motivation In this chapter we give a straightforward extension of the theory of quantum convolutional codes to nonbinary alphabets. We give analytical constructions for quantum convolutional codes unlike the previous work where most of the codes were constructed by either heuristics or computer search. In many cases, we give the exact free distance of the quantum convolutional codes. The main contributions of our work are that we:

- establish bounds on a class of quantum convolutional codes similar to generalized Singleton bound for classical convolutional codes.

- provide the necessary definitions and terminology of stabilizer formalization of convolutional codes, free distance, error bases.

- construct families of quantum convolutional codes based on classical block codes – such as Reed-Solomon (RS), BCH, and Reed-Muller codes.

C. Background on Convolutional Codes

1. Overview

Classical convolutional codes appeared in a series of seminal papers in the seventies of the last century. The algebraic structure of these codes was initiated by Forney [47,48] and Justesen [108]. Cyclic convolutional codes were first introduced by Piret [117–119] and generalized by Roos [125]. Using this construction, one family of cyclic convolutional codes based on Reed-Solomon codes was derived [119]. It was shown that any convolutional code has a canonical direct decomposition into subcodes; and hence it has a minimal encoder.

The subject became active, once again, by a series of recent papers by Gluesing-Luerssen al et. in [52–54] and by Rosenthal [128]. Cyclic convolutional codes are defined as left principle ideals in a skew-polynomial ring. Also, a subclass of cyclic convolutional codes is described where the units of the skew polynomial ring is used.

Unit memory convolutional codes are an important class of codes that is appeared in a paper by Lee [101]. He also showed that these codes have large free distance d_f among other codes (multi-memory) with the same rate. Upper and lower bounds on the free distance of unit memory codes were derived by Thommesen and Justesen [149], confirming superiority of these codes in comparison to other convolutional codes. Since then, there were some attempts to construct unit memory codes by using computer search and by puncturing existing convolutional codes. For an algebraic method to construct unit memory convolutional codes, classes of these codes were derived by Piret based on RS codes [119] and by Hole based on BCH codes [73].

Also, a class of unit memory codes defined using circulant sub-matrices was derived by Justesen et. al [77].

Bounds on convolutional codes have been studies as well. Rosenthal al et. showed a generalized Singleton bound and MDS convolutional codes [126–128].

2. Algebraic Structure of Convolutional Codes

We give some background concerning classical convolutional codes, following [75, Chapter 14] and [100].

Let $\mathbb{F}_q$ denote a finite field with q elements. An $(n,k,\delta)_q$ *convolutional code* C is a submodule of $\mathbb{F}_q[D]^n$ generated by a right-invertible matrix $G(D)=(g_{ij})\in\mathbb{F}_q[D]^{k\times n}$,

$$C=\{\mathbf{u}(D)G(D)\mid \mathbf{u}(D)\in\mathbb{F}_q[D]^k\}, \tag{11.1}$$

such that $\sum_{i=1}^k \nu_i=\max\{\deg\gamma\,|\,\gamma \text{ is a } k\text{-minor of } G(D)\}=:\delta$,
where $\nu_i=\max_{1\le j\le n}\{\deg g_{ij}\}$. We say δ is the *degree* of C. The *memory* μ of $G(D)$ is defined as $\mu=\max_{1\le i\le k}\nu_i$. The *weight* $\mathrm{wt}(v(D))$ of a polynomial $v(D)$ in $\mathbb{F}_q[D]$ is defined as the number of nonzero coefficients of $v(D)$, and the *weight* of an element $\mathbf{u}(D)\in\mathbb{F}_q[D]^n$ is defined as $\mathrm{wt}(\mathbf{u}(D))=\sum_{i=1}^n \mathrm{wt}(u_i(D))$. The *free distance* d_f of C is defined as $d_f=\mathrm{wt}(C)=\min\{\mathrm{wt}(u)\mid u\in C, u\neq 0\}$. We say that an $(n,k,\delta)_q$ convolutional code with memory μ and free distance d_f is an $(n,k,\delta;\mu,d_f)_q$ convolutional code.

Let $\mathbf{N}$ denote the set of nonnegative integers. Let

$$\Gamma_q=\{v\colon \mathbf{N}\to\mathbb{F}_q\,|\text{ all but finitely many coefficients of } v \text{ are } 0\}. \tag{11.2}$$

We can view $v\in\Gamma_q$ as a sequence $\{v_i=v(i)\}_{i\ge 0}$ of finite support. We define a vector space isomorphism $\sigma\colon\mathbb{F}_q[D]^n\to\Gamma_q$ that maps an element $\mathbf{u}(D)=(u_1(D),\dots,u_n(D))$ in $\mathbb{F}_q[D]^n$ to the coefficient sequence of the polynomial $\sum_{i=0}^{n-1} D^i u_i(D^n)$, that is, an element in $\mathbb{F}_q[D]^n$ is mapped to its interleaved coefficient sequence. Frequently, we will refer to the image $\sigma(C) = \{\sigma(c) \mid c \in C\}$ of a convolutional code (11.1) again as C, as it will be clear from the context whether we discuss the sequence or polynomial form of the code. Let $G(D) = G_0 + G_1 D + \cdots + G_\mu D^\mu$, where $G_i \in \mathbb{F}_q^{k\times n}$ for $0 \le i \le \mu$. We can associate to the generator matrix $G(D)$ its semi-infinite coefficient matrix

$$G = \begin{pmatrix} G_0 & G_1 & \cdots & G_\mu & & & \\ & G_0 & G_1 & \cdots & G_\mu & & \\ & & \ddots & \ddots & & & \ddots \end{pmatrix}. \tag{11.3}$$

If $G(D)$ is the generator matrix of a convolutional code C, then one easily checks that $\sigma(C) = \Gamma_q G$.

In the literature, convolutional codes are often defined in the form $\{p(D)G'(D) \mid p(D) \in \mathbb{F}_q(D)^k\}$, where $G'(D)$ is a matrix of full rank in $\mathbb{F}_q^{k\times n}[D]$. In this case, one can obtain a generator matrix $G(D)$ in our sense by multiplying $G'(D)$ from the left with a suitable invertible matrix $U(D)$ in $\mathbb{F}_q^{k\times k}(D)$, see [75].

Euclidean and Hermitian Inner Products. We define the *Euclidean inner product* of two sequences u and v in Γ_q by $\langle u \,|\, v\rangle = \sum_{i\in\mathbf{N}} u_i v_i$, and the Euclidean dual of a convolutional code $C \subseteq \Gamma_q$ by $C^\perp = \{u \in \Gamma_q \,|\, \langle u \,|\, v\rangle = 0 \text{ for all } v \in C\}$. A convolutional code C is called self-orthogonal if and only if $C \subseteq C^\perp$. It is easy to see that a convolutional code C is self-orthogonal if and only if $GG^T = 0$.

Consider the finite field $\mathbb{F}_{q^2}$. The *Hermitian inner product* of two sequences u and v in Γ_{q^2} is defined as $\langle u \,|\, v\rangle_h = \sum_{i\in\mathbf{N}} u_i\, v_i^q$. We have $C^{\perp_h} = \{u \in \Gamma_{q^2} \,|\, \langle u \,|\, v\rangle_h = 0 \text{ for all } v \in C\}$. Then, $C \subseteq C^{\perp_h}$ if and only if $GG^\dagger = 0$, where the Hermitian transpose $\dagger$ is defined as $(a_{ij})^\dagger = (a_{ji}^q)$.

Delay Operator. We can define the delay operator as a shift operator in the codeword to the left or right. Let $g_i(D)$ be a row in the infinite generator polynomial $G(D)$, the right $j-th$ shift is given by

$$D^j g_i(D) = g_{i+j}(D). \tag{11.4}$$

3. Duals of Convolutional Codes

The dual of a convolutional code plays an important role in constructing quantum convolutional codes. Therefore, we first introduce the dual of a convolutional code. We can define the inner product between two sequences $\mathbf{v}$ and $\mathbf{w}$ as

$$\langle \mathbf{v}|\mathbf{w}\rangle = \sum_{i\in\mathbb{Z}} \langle \mathbf{v}_i|\mathbf{w}_i\rangle. \tag{11.5}$$

Recall that every codeword in C is equivalent to a sequence. The dual convolutional code $C^\perp$ is the set of all sequences that are orthogonal to every sequence $\mathbf{v}$ in C.

Lemma 137 (Dual of Convolutional Code)**.** *Let k/n be the rate of a convolutional code C generated by a semi-infinite generator matrix G. Also, let $(n-k)/n$ be the rate of dual of a convolutional code $C^\perp$ generated by the semi-infinite generator matrix $G^\perp$, such that*

$$G = \begin{pmatrix} G_0 & G_1 & \cdots & G_m & & & \\ & G_0 & G_1 & \cdots & G_m & & \\ & & \ddots & \ddots & & & \ddots \end{pmatrix}$$

and

$$G^\perp = \begin{pmatrix} G_0^\perp & G_1^\perp & \cdots & G_{m^\perp}^\perp & & & \\ & G_0^\perp & G_1^\perp & \cdots & G_{m^\perp}^\perp & & \\ & & \ddots & \ddots & & & \ddots \end{pmatrix} \tag{11.6}$$

where G_i are $k \times n$ matrices, for all $0 \le i \le m$. Then $G(G^\perp)^T = 0$.

Proof. see [76, Theorem 2.63]. □

A convolutional code C is said to be self-orthogonal if $C \subseteq C^{\perp}$. Clearly, a convolutional code is self-orthogonal if and only if $GG^T = 0$. We can also define a relation between the polynomial generators matrices $G(D)$ and $G^{\perp}(D)$. If $G_r^{\perp}(D) = G_{m^{\perp}}^{\perp} + G_{m^{\perp}-1}^{\perp}D + \cdots + G_1^{\perp}D^{m^{\perp}-1} + G_0^{\perp}D^{m^{\perp}}$, then $G(D)(G_r^{\perp}(D))^T = 0$ (see [76, Theorem 2.64]). The following Lemma gives the relation between the total constraint lengths of a code and its dual code.

Lemma 138. *The convolutional code C is self-orthogonal if and only if*

$$G(D)G(D^{-1})^T = 0 \tag{11.7}$$

Proof. Let the polynomial $G(D) = G_0 + G_1D + \ldots + G_mD^m$ and its dual polynomial $G^{\perp}(D) = G_0^{\perp} + G_1^{\perp}D + \ldots + G_{m^{\perp}}^{\perp}D^{m^{\perp}}$ be the polynomial generator matrices of C and its dual, respectively. We know that $G(D)G_r^{\perp}(D)^T = 0$. But,

$$\begin{aligned} G_r^{\perp}(D) &= G_{m^{\perp}}^{\perp} + G_{m^{\perp}-1}^{\perp}D + \cdots + G_1^{\perp}D^{m^{\perp}-1} + G_0^{\perp}D^{m^{\perp}} \\ &= \left(G_{m^{\perp}}^{\perp}D^{-m^{\perp}} + G_{m^{\perp}-1}^{\perp}D^{1-m^{\perp}} + \cdots + G_1^{\perp}D^{-1} + G_0^{\perp}\right)D^{m^{\perp}} \\ &= G^{\perp}(D^{-1})D^{m^{\perp}}. \end{aligned} \tag{11.8}$$

Therefore, $G(D)G_r^{\perp}(D)^T = G(D)G^{\perp}(D^{-1})^T D^{m^{\perp}} = 0$. So, $G(D)G^{\perp}(D^{-1})^T = 0$. Let $C \leq C^{\perp}$ be a self-orthogonal convolutional code, we know that the elements of $G(D)$ can be generated from the elements of $G^{\perp}(D)$. Since, $G(D)G^{\perp}(D^{-1})^T = 0$, it follows that $G(D)G(D^{-1})^T = 0$.

Conversely, if $G(D)G(D^{-1})^T = 0$, then it implies that the convolutional code generated by $G(D)$ must be a subcode of $G^{\perp}(D)$. Therefore, C must be a self-orthogonal convolutional code. □

We can also formulate the above condition in a slightly different manner as follows. Let $G(D) = [g_{ij}(D)]$. Then $G(D)G(D^{-1})^T = \sum_{l=1}^{n} g_{il}(D)g_{jl}(D^{-1})$. So, for a self-orthogonal code $\sum_{l=1}^{n} g_{il}(D)g_{jl}(D^{-1}) = 0$, for all $1 \leq i, j \leq k$. Alternatively, if

$$G(D) = [\mathbf{g}_1(D), \mathbf{g}_2(D), \ldots, \mathbf{g}_k(D)]^T, \tag{11.9}$$

where $\mathbf{g}_i(D) = [g_{i1}(D), g_{i2}(D), \ldots, g_{in}(D)]$, then

$$G(D)G(D^{-1})^T = [g_i(D)g_j(D^{-1})^T] = 0, \tag{11.10}$$

i.e. $g_i(D)g_j(D^{-1})^T = 0$ **Cross-Correlation.** It is also possible to derive these conditions in terms of the cross-correlations between codewords of a convolutional code as in [49]. Let us define the Euclidean inner product between two (Laurent) series $g(D) = \sum_{i\in\mathbb{Z}} g_i D^i$ and $h(D) = \sum_{i\in\mathbb{Z}} h_i D^i$ for $g_i, h_i \in \mathbb{F}_q$ as

$$\langle g(D)|h(D)\rangle = \sum_{i\in\mathbb{Z}} g_i h_i. \tag{11.11}$$

If the series are over F_{q^2}, we can define their Hermitian inner product as

$$\langle g(D)|h(D)\rangle_h = \sum_{i\in\mathbb{Z}} g_i^q h_i. \tag{11.12}$$

If $\mathbf{v}(D)$ is equal to $[v_1(D), v_1(D), \ldots, v_n(D) \mid v_i(D) \in \mathbb{F}_q((D))]$ then we can define the Euclidean inner product with $\mathbf{w}(D) = [w_1(D), w_1(D), \ldots, w_n(D)]$ as

$$\langle \mathbf{v}(D)|\mathbf{w}(D)\rangle = \sum_{i=1}^{n} \langle v_i(D)|w_i(D)\rangle. \tag{11.13}$$

Let us define the conjugate of $g(D) \in \mathbb{F}_{q^2}((D))$ as $g^\dagger(D) = \sum_{i\in\mathbb{Z}} g_i^q D^i$. Then, we can also define the Hermitian inner product of $\mathbf{v}(D)$ and $\mathbf{w}(D)$ as

$$\langle \mathbf{v}(D)|\mathbf{w}(D)\rangle_h = \sum_{i=1}^{n} \langle v_i(D)|w_i(D)\rangle_h = \sum_{i=1}^{n} \langle v_i(D)|w_i^\dagger(D)\rangle. \tag{11.14}$$

Now, we define the cross-correlation between the sequences $\mathbf{v}(D)$ and $\mathbf{w}(D)$ as

$$R_{\mathbf{vw}}(D) = \sum_{i\in\mathbb{Z}}\langle \mathbf{v}(D)|D^i\mathbf{w}(D)\rangle D^i = \sum_{i\in\mathbb{Z}} R_{\mathbf{vw},i}D^i. \tag{11.15}$$

If C is self-orthogonal, then $R_{\mathbf{vw}}(D)=0$ for any $\mathbf{v}(D),\mathbf{w}(D)\in C$.

Lemma 139. $R_{\mathbf{vw}}(D)=\mathbf{v}(D)\mathbf{w}(D^{-1})^T$

Proof. The proof is a direct consequence from definition of $R_{\mathbf{vw}}(D)$, Equation (11.15).

$$\begin{aligned}
R_{\mathbf{vw}}(D) &= \sum_{i\in\mathbb{Z}}\langle \mathbf{v}(D)|D^i\mathbf{w}(D)\rangle D^i \\
&= \sum_{i\in\mathbb{Z}}\sum_{j=1}^{n}\langle \mathbf{v}_j(D)|D^i\mathbf{w}_j(D)\rangle D^i \\
&= \sum_{i\in\mathbb{Z}}\sum_{j=1}^{n}\mathbf{v}_j\mathbf{w}_{j-i}D^i = \sum_{i\in\mathbb{Z}}\sum_{j=1}^{n}\mathbf{v}_jD^jD^{-j}\mathbf{w}_{j-i}D^i \\
&= \sum_{j=1}^{n}\mathbf{v}_jD^j\sum_{i\in\mathbb{Z}}D^{-j}\mathbf{w}_{j-i}D^i = \sum_{j=1}^{n}\mathbf{v}_jD^j\sum_{i\in\mathbb{Z}}\mathbf{w}_{j-i}D^{-(j-i)} \\
&= \mathbf{v}(D)\mathbf{w}(D^{-1})^T
\end{aligned} \tag{11.16}$$

∎

If $\mathbf{v}(D)$ is orthogonal to $\mathbf{w}(D)$, then $R_{\mathbf{vw}}(D)=0$. We can also define the cross-correlation with respect to the Hermitian inner product as

$$\begin{aligned}
R^h_{\mathbf{vw}}(D) &= \sum_{i\in\mathbb{Z}}\langle \mathbf{v}(D)|D^i\mathbf{w}(D)\rangle_h D^i = \sum_{i\in\mathbb{Z}} R^h_{\mathbf{vw},i}D^i, \\
&= \mathbf{v}(D)\mathbf{w}^\dagger(D^{-1}).
\end{aligned} \tag{11.17}$$

If a code C is Hermitian self-orthogonal, then $R^h_{\mathbf{vw}}(D)=0$ for any $\mathbf{v}(D),\mathbf{w}(D)\in C$.

Lemma 140. *Let $G(D)$ be a minimal encoder of a convolutional code C with total* *constraint length δ. Then the dual encoder $G^{\perp}(D)$ of $C^{\perp}$ has also a total constraint equals to δ*

Proof. See for example [47, Theorem 7] $\square$

D. Quantum Convolutional Codes

The state space of a q-ary quantum digit is given by the complex vector space $\mathbb{C}^q$. Let $\{|x\rangle \mid x \in \mathbb{F}_q\}$ denote a fixed orthonormal basis of $\mathbb{C}^q$, called the computational basis. For $a, b \in \mathbb{F}_q$, we define the unitary operators

$$X(a)\,|x\rangle = |x+a\rangle \quad \text{and} \quad Z(b)\,|x\rangle = \exp(2\pi i\,\mathrm{tr}(bx)/p)\,|x\rangle\,, \tag{11.18}$$

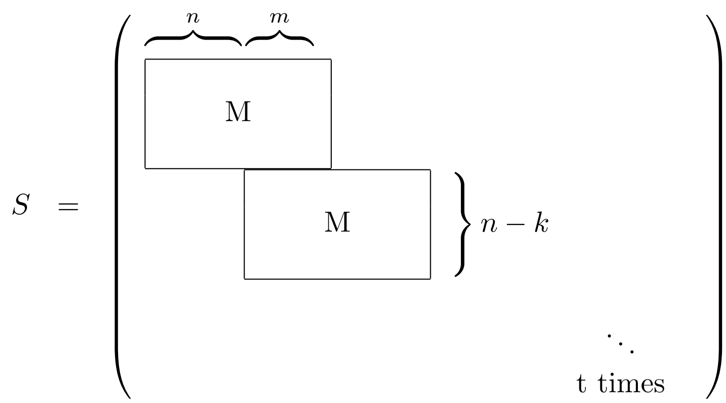
where the addition is in $\mathbb{F}_q$, p is the characteristic of $\mathbb{F}_q$, and $\mathrm{tr}(x) = x^p + x^{p^2} + \cdots + x^q$ is the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. The set $\mathcal{E} = \{X(a), Z(b) \mid a, b \in \mathbb{F}_q\}$ is a basis of the algebra of $q \times q$ matrices, called the *error basis*.

A quantum convolutional code encodes a stream of quantum digits. One does not know in advance how many qudits *i.e.*, quantum digits will be sent, so the idea is to impose structure on the code that simplifies online encoding and decoding. Let n, m be positive integers. We will process $n+m$ qudits at a time, m qudits will overlap from one step to the next, and n qudits will be output.

For each t in $\mathbf{N}$, we define the Pauli group $P_t = \langle M | M \in \mathcal{E}^{\otimes(t+1)n+m}\rangle$ as the group generated by the $(t+1)n+m$-fold tensor product of the error basis $\mathcal{E}$. Let $I = X(0)$ be the $q \times q$ identity matrix. For $i, j \in \mathbf{N}$ and $i \leq j$, we define the inclusion homomorphism $\iota_{ij}\colon P_i \to P_j$ by $\iota_{ij}(M) = M \otimes I^{\otimes n(j-i)}$. We have $\iota_{ii}(M) = M$ and $\iota_{ik} = \iota_{jk} \circ \iota_{ij}$ for $i \leq j \leq k$. Therefore, there exists a group

$$P_\infty = \varinjlim (P_i, \iota_{ij}), \tag{11.19}$$

called the direct limit of the groups P_i over the totally ordered set $(\mathbf{N}, \leq)$. For each nonnegative integer i, there exists a homomorphism $\iota_i\colon P_i \to P_\infty$ given by $\iota_i(M_i) = M_i \otimes I^{\otimes\infty}$ for $M_i \in P_i$, and $\iota_i = \iota_j \circ \iota_{ij}$ holds for all $i \leq j$. We have $P_\infty = \bigcup_{i=0}^{\infty} \iota_i(P_i)$; put differently, P_∞ consists of all infinite tensor products of matrices in $\langle M \,|\, M \in \mathcal{E}\rangle$ such that all but finitely many tensor components are equal to I. The direct limit structure that we introduce here provides the proper conceptual framework for the definition of convolutional stabilizer codes; see [124] for background on direct limits.



We will define the stabilizer of the quantum convolutional code also through a direct limit. Let S_0 be an abelian subgroup of P_0. For positive integers t, we recursively define a subgroup S_t of P_t by $S_t = \langle N \otimes I^{\otimes n}, I^{\otimes tn} \otimes M \,|\, N \in S_{t-1}, M \in S_0\rangle$. Let Z_t denote the center of the group P_t. We will assume that

S1) $I^{\otimes tn} \otimes M$ and $N \otimes I^{\otimes tn}$ commute for all $N, M \in S_0$ and all positive integers t.

S2) $S_t Z_t / Z_t$ is an $(t+1)(n-k)$-dimensional vector space over $\mathbb{F}_q$.

S3) $S_t \cap Z_t$ contains only the identity matrix.

Assumption **S1** ensures that S_t is an *abelian* subgroup of P_t, **S2** implies that S_t is generated by $t+1$ shifted versions of $n-k$ generators of S_0 and all these $(t+1)(n-k)$ generators are independent, and **S3** ensures that the stabilizer (or +1 eigenspace) of

S_t is nontrivial as long as $k < n$.

The abelian subgroups S_t of P_t define an abelian group

$$S = \varinjlim(S_i, \iota_{ij}) = \langle \iota_t(I^{\otimes tn} \otimes M) \,|\, t \geq 0, M \in S_0 \rangle \tag{11.20}$$

generated by shifted versions of elements in S_0.

Definition 141. Suppose that an abelian subgroup S_0 of P_0 is chosen such that **S1**, **S2**, and **S3** are satisfied. Then the +1-eigenspace of $S = \varinjlim(S_i, \iota_{ij})$ in $\bigotimes_{i=0}^{\infty} \mathbb{C}^q$ defines a convolutional stabilizer code with parameters $[(n, k, m)]_q$.

In practice, one works with a stabilizer S_t for some large (but previously unknown) t, rather than with S itself. We notice that the rate k/n of the quantum convolutional stabilizer code defined by S is approached by the rate of the stabilizer block code S_t for large t. Indeed, S_t defines a stabilizer code with parameters $[[(t + 1)n + m, (t + 1)k + m]]_q$; therefore, the rates of these stabilizer block codes approach

$$\lim_{t\to\infty} \frac{(t+1)k+m}{(t+1)n+m} = \lim_{t\to\infty} \frac{k+m/(t+1)}{n+m/(t+1)} = \frac{k}{n}. \tag{11.21}$$

We say that an error E in P_∞ is *detectable* by a convolutional stabilizer code with stabilizer S if and only if a scalar multiple of E is contained in S or if E does not commute with some element in S. The *weight* wt of an element in P_∞ is defined as its number of non-identity tensor components. A quantum convolutional stabilizer code is said to have *free distance* d_f if and only if it can detect all errors of weight less than d_f, but cannot detect some error of weight d_f. Denote by $Z(P_\infty)$ the center of P_∞ and by $C_{P_\infty}(S)$ the centralizer of S in P_∞. Then the free distance is given by $d_f = \min\{\mathrm{wt}(e) \mid e \in C_{P_\infty}(S) \setminus Z(P_\infty)S\}$.

Let (β, β^q) denote a normal basis of $\mathbb{F}_{q^2}/\mathbb{F}_q$. Define a map $\tau\colon P_\infty \to \Gamma_{q^2}$ by

$\tau(\omega^c X(a_0)Z(b_0) \otimes X(a_1)Z(b_1) \otimes \cdots) = (\beta a_0 + \beta^q b_0, \beta a_1 + \beta^q b_1, \dots)$. For sequences v and w in Γ_{q^2}, we define a trace-alternating form

$$\langle v \,|\, w \rangle_a = \mathrm{tr}_{q/p}\left(\frac{v \cdot w^q - v^q \cdot w}{\beta^{2q} - \beta^2}\right). \tag{11.22}$$

Lemma 142. *Let A and B be elements of P_∞. Then A and B commute if and only if $\langle \tau(A) \,|\, \tau(B) \rangle_a = 0$.*

Proof. This follows from [81] and the direct limit structure. □

Lemma 143. *Let Q be an $\mathbb{F}_{q^2}$-linear $[(n, k, m)]_q$ quantum convolutional code with stabilizer S, where $S = \varinjlim(S_i, \iota_{ij})$ and S_0 an abelian subgroup of P_0 such that **S1**, **S2**, and **S3** hold. Then $C = \sigma^{-1}\tau(S)$ is an $\mathbb{F}_{q^2}$-linear $(n, (n-k)/2; \mu \leq \lceil m/n \rceil)_{q^2}$ convolutional code generated by $\sigma^{-1}\tau(S_0)$. Further, $C \subseteq C^{\perp_h}$.*

Proof. Recall that $\sigma : \mathbb{F}_{q^2}[D]^n \to \Gamma_{q^2}$, maps $u(D)$ in $\mathbb{F}_{q^2}[D]^n$ to $\sum_{i=0}^{n-1} D^i u_i(D^n)$. It is invertible, thus $\sigma^{-1}\tau(e) = \sigma^{-1} \circ \tau(e)$ is well defined for any e in P_∞. Since S is generated by shifted versions of S_0, it follows that $C = \sigma^{-1}\tau(S)$ is generated as the $\mathbb{F}_{q^2}$ span of $\sigma^{-1}\tau(S_0)$ and its shifts, *i.e.*, $D^l\sigma^{-1}\tau(S_0)$, where $l \in \mathcal{N}$. Since Q is an $\mathbb{F}_{q^2}$-linear $[(n, k, m)]_q$ quantum convolutional code, S_0 defines an $[[n+m, k+m]]_q$ stabilizer code with $(n-k)/2$ $\mathbb{F}_{q^2}$-linear generators. Since the maps σ and τ are linear $\sigma^{-1}\tau(S_0)$ is also $\mathbb{F}_{q^2}$-linear. As $\sigma^{-1}\tau(e)$ is in $\mathbb{F}_{q^2}[D]^n$ we can define an $(n-k)/2 \times n$ polynomial generator matrix that generates C. This generator matrix need not be right invertible, but we know that there exists a right invertible polynomial generator matrix that generates this code. Thus C is an $(n, (n-k)/2; \mu)_{q^2}$ code. Since S is abelian, Lemma 142 and the $\mathbb{F}_{q^2}$-linearity of S imply that $C \subseteq C^{\perp_h}$. Finally, observe that maximum degree of an element in $\sigma^{-1}\tau(S_0)$ is $\lceil m/n \rceil$ owing to σ. Together with [75, Lemma 14.3.8] this implies that the memory of $\sigma^{-1}\tau(S)$ must be $\mu \leq \lceil m/n \rceil$. □

E. CSS Code Constructions

We define the degree of an $\mathbb{F}_{q^2}$-linear $[(n,k,m)]_q$ quantum convolutional code Q with stabilizer S as the degree of the classical convolutional code $\sigma^{-1}\tau(S)$. It is possible to define the degree of the quantum convolutional code purely in terms of the stabilizer too, but such a definition is somewhat convoluted. We denote an $[(n,k,m)]_q$ quantum convolutional code with free distance d_f and total constraint length δ as $[(n,k,m;\delta,d_f)]_q$. It must be pointed out this notation is at variance with the classical codes in not just the order but the meaning of the parameters.

Corollary 144. *An $\mathbb{F}_{q^2}$-linear $[(n,k,m;\delta,d_f)]_q$ convolutional stabilizer code implies the existence of an $(n,(n-k)/2;\delta)_{q^2}$ convolutional code C such that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$.*

Proof. As before let $C = \sigma^{-1}\tau(S)$, by Lemma 142 we can conclude that $\sigma^{-1}\tau(C_{P_\infty}(S)) \subseteq C^{\perp_h}$. Thus an undetectable error is mapped to an element in $C^{\perp_h}\setminus C$. While τ is injective on S it is not the case with $C_{P_\infty}(S)$. However we can see that if c is in $C^{\perp_h}\setminus C$, then surjectivity of τ (on $C_{P_\infty}(S)$) implies that there exists an error e in $C_{P_\infty}(S)\setminus Z(P_\infty)S$ such that $\tau(e)=\sigma(c)$. As τ and σ are isometric e is an undetectable error with $\mathrm{wt}(c)$. Hence, we can conclude that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$. Combining with Lemma 143 we have the claim stated. □

An $[(n,k,m;\delta,d_f)]_q$ code is said to be a *pure code* if there are no errors of weight less than d_f in the stabilizer of the code. Corollary 144 implies that $d_f = \mathrm{wt}(C^{\perp_h}\setminus C) = \mathrm{wt}(C^{\perp_h})$.

Theorem 145. *Let C be $(n,(n-k)/2,\delta;\mu)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n,k,n\mu;\delta,d_f)]_q$ convolutional stabilizer code, where $d_f = \mathrm{wt}(C^{\perp_h}\setminus C)$. The code is pure if $d_f = \mathrm{wt}(C^{\perp_h})$.*

Sketch. Let $G(D)$ be the polynomial generator matrix of C, with the semi-infinite generator matrix G defined as in equation (11.3). Let $C_t = \langle \sigma(G(D)), \ldots, \sigma(D^t G(D))\rangle = \langle C_{t-1}, \sigma(D^t G(D))\rangle$, where σ is applied to every row in $G(D)$. The self-orthogonality of C implies that C_t is also self-orthogonal. In particular C_0 defines an $[n+n\mu, (n-k)/2]_{q^2}$ self-orthogonal code. From the theory of stabilizer codes we know that there exists an abelian subgroup $S_0 \leq P_0$ such that $\tau(S_0) = C_0$, where P_t is the Pauli group over $(t+1)n+m$ qudits; in this case $m = n\mu$. This implies that $\tau(I^{\otimes nt} \otimes S_0) = \sigma(D^t G(D))$. Define $S_t = \langle S_{t-1}, I^{\otimes nt} \otimes S_0\rangle$, then $\tau(S_t) = \langle \tau(S_{t-1}, \sigma(D^t G(D))\rangle$. Proceeding recursively, we see that $\tau(S_t) = \langle \sigma(G(D)), \ldots, \sigma(D^t G(D))\rangle = C_t$. By Lemma 142, the self-orthogonality of C_t implies that S_t is abelian, thus **S1** holds. Note that $\tau(S_t Z_t/Z_t) = C_t$, where Z_t is the center of P_t. Combining this with $\mathbb{F}_{q^2}$-linearity of C_t implies that $S_t Z_t/Z_t$ is a $(t+1)(n-k)$ dimensional vector space over F_q; hence **S2** holds. For **S3**, assume that $z \neq \{1\}$ is in $S_t \cap Z_t$. Then z can be expressed as a linear combination of the generators of S_t. But $\tau(z) = 0$ implying that the generators of S_t are dependent. Thus $S_t \cap Z_t = \{1\}$ and **S3** also holds. Thus $S = \varinjlim(S_t, \iota_{tj})$ defines an $[(n, k, n\mu; \delta)]_q$ convolutional stabilizer code. By definition the degree of the quantum code is the degree of the underlying classical code. As $\sigma^{-1}\tau(S) = C$, arguing as in Corollary 144 we can show that $\sigma^{-1}\tau(C_{P_\infty}(S)) = C^{\perp_h}$ and $d_f = \mathrm{wt}(C^{\perp_h} \setminus C)$. □

Corollary 146. *Let C be an $(n, (n-k)/2, \delta; \mu)_q$ code such that $C \subseteq C^\perp$. Then there exists an $[(n, k, n\mu; \delta, d_f)]_q$ code with $d_f = \mathrm{wt}(C^\perp \setminus C)$. It is pure if $\mathrm{wt}(C^\perp \setminus C) = \mathrm{wt}(C^\perp)$.*

Proof. Since $C \subseteq C^\perp$, its generator matrix G as in equation (11.3) satisfies $GG^T = 0$. We can obtain an $\mathbb{F}_{q^2}$-linear $(n, (n-k)/2, \delta; \mu)_{q^2}$ code, C' from G as $C' = \Gamma_{q^2} G$. Since $G_i \in \mathbb{F}_q^{(n-k)/2 \times n}$ we have $GG^\dagger = GG^T = 0$. Thus $C' \subseteq C'^{\perp_h}$. Further, it can checked that $\mathrm{wt}(C'^{\perp_h} \setminus C') = \mathrm{wt}(C^{\perp} \setminus C)$. The claim follows from Theorem 145. □

F. QCC Singleton Bound

Three main properties to measure performance of a quantum convolutional stabilizer code are code rate, minimum free distance, and complexity of its encoders (decoders). We study bounds on the minimum free distance of QCC's. All quantum block codes whether they are pure or impure saturate the quantum Singleton bound. Also, classical convolutional codes obey modified Singleton bound. We recall generalized Singleton bound for convolutional codes as shown in the following Lemma.

Lemma 147 (Generalized Singleton Bound). *The free distance of a $(n, k, m; \delta, d_f)_q$ convolutional code is upper-bounded by*

$$d_f \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1 = \mathfrak{B}(n, k, m; \delta). \tag{11.23}$$

Proof. See [127, Theorem 2.4]. □

If the free distance of the QCC is same as the free distance of the dual code, i.e. $C^{\perp} \backslash C$, then QCC is called pure code. The following Lemma shows the generalized Singleton bound for pure QCC's.

Theorem 148 (Singleton bound). *The free distance of an $[(n, k, m; \delta, d_f)]_q$ $\mathbb{F}_{q^2}$-linear pure convolutional stabilizer code is bounded by*

$$d_f \quad \leq \quad \frac{n-k}{2}\left(\left\lfloor \frac{2\delta}{n+k} \right\rfloor + 1\right) + \delta + 1 \tag{11.24}$$

Proof. By Corollary 144, there exists an $(n, (n-k)/2, \delta)_{q^2}$ code C such that $\mathrm{wt}(C^{\perp_h} \setminus C) = d_f$, and the purity of the code implies that $\mathrm{wt}(C^{\perp_h}) = d_f$. The dual code $C^{\perp}$ or $C^{\perp_h}$ has the same degree as code [76, Theorem 2.66]. Thus, $C^{\perp_h}$ is an $(n, (n+k)/2, \delta)_{q^2}$

convolutional code with free distance d_f. By the generalized Singleton bound [127, Theorem 2.4] for classical convolutional codes, we have

$$d_f \leq (n-(n+k)/2)\left(\left\lfloor \frac{\delta}{(n+k)/2} \right\rfloor + 1\right) + \delta + 1,$$

which implies the claim. $\square$

G. QCC Example

Example 149 (QCC with rate 1/3 and single error correction)**.** *Consider the code C generated by*

$$g_1 = \begin{pmatrix} D & 1+D+D^2 & 1+D^2 \end{pmatrix}.$$

and the set of all generators can be given as $\{D^i g_1(D), i \in \mathbb{Z}\}$. So, the generator matrix of the code in the infinite form is

$$G = \begin{pmatrix} g_1(x) \\ Dg_1(x) \\ . \\ . \\ . \end{pmatrix} = \begin{pmatrix} 011 & 110 & 011 & & \\ & 011 & 110 & 011 & \\ & & \ddots & \ddots & \ddots \end{pmatrix} \qquad (11.25)$$

Now, we can map the generator G to a stabilizer subgroup S with two generators. The two generators of S have infinite length of Pauli matrices as

$$(\ldots, III, IXX, XXI, IXX, III, \ldots)$$

and

$$(\cdots, III, IZZ, ZZI, IZZ, III, \cdots).$$

It is straight forward to check that g_1 is orthogonal to itself using the cross correlated function. Also, row shifts of the matrix G are orthogonal to each other. Therefore, the code C is self-orthogonal, and the dual code $C^\perp$ has rate $2/3$ and generated by.

$$H = \begin{pmatrix} D & 1+D & 1+D \\ 1 & 1 & 1 \end{pmatrix}$$

Also, $C^\perp$ can be mapped to a centralizer subgroup $C(S) \in \mathcal{G}$. One can check that $C^\perp$ has minimum free distance $d_f = 3$. Clearly, the convolutional code has memory $v = 2$, i.e. the max degree of g_1.

CHAPTER XII

QUANTUM CONVOLUTIONAL CODES DERIVED FROM REED-SOLOMON CODES

In this chapter I construct quantum convolutional codes based on generalized Reed-Solomon and Reed-Muller codes. The quantum convolutional codes derived from the generalized Reed-Solomon codes are shown to be optimal in the sense that they attain the Singleton bound with equality, as shown in Chapter XI.

A. Convolutional GRS Stabilizer Codes

In this section we will use Piret's construction of Reed-Solomon convolutional codes [119] to derive quantum convolutional codes. Let $\alpha \in \mathbb{F}_{q^2}$ be a primitive nth root of unity, where $n|q^2-1$. Let $w = (w_0, \ldots, w_{n-1}), \gamma = (\gamma_0, \ldots, \gamma_{n-1})$ be in $\mathbb{F}_{q^2}^n$ where $w_i \neq 0$ and all $\gamma_i \neq 0$ are distinct. Then the generalized Reed-Solomon (GRS) code over $\mathbb{F}_{q^2}^n$ is the code with the parity check matrix, (cf. [75, pages 175–178])

$$H_{\gamma,w} = \begin{bmatrix} w_0 & w_1 & \cdots & w_{n-1} \\ w_0\gamma_0 & w_1\gamma_1 & \cdots & w_{n-1}\gamma_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_0\gamma_0^{t-1} & w_1\gamma_1^{2(t-1)} & \cdots & w_{n-1}\gamma_{n-1}^{(t-1)(n-1)} \end{bmatrix}. \tag{12.1}$$

The code is denoted by $\mathrm{GRS}_{n-t}(\gamma, v)$, as its generator matrix is of the form $H_{\gamma,v}$ for some $v \in \mathbb{F}_{q^2}^n$. It is an $[n, n-t, t+1]_{q^2}$ MDS code [75, Theorem 5.3.1]. If we choose $w_i = \alpha^i$, then $w_i \neq 0$. If $\gcd(n, 2) = 1$, then α^2 is also a primitive nth root of unity; thus $\gamma_i = \alpha^{2i}$ are all distinct and we have an $[n, n-t, t+1]_{q^2}$ GRS code with parity check matrix H_0, where

$$H_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \cdots & \alpha^{(2t-1)(n-1)} \end{bmatrix}. \tag{12.2}$$

Similarly if $w_i = \alpha^{-i}$ and $\gamma_i = \alpha^{-2i}$, then we have another $[n, n-t, t+1]_{q^2}$ GRS code with parity check matrix

$$H_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(n-1)} \\ 1 & \alpha^{-3} & \alpha^{-6} & \cdots & \alpha^{-3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(2t-1)} & \alpha^{-2(2t-1)} & \cdots & \alpha^{-(2t-1)(n-1)} \end{bmatrix}. \tag{12.3}$$

The $[n, n-2t, 2t+1]_{q^2}$ GRS code with $w_i = \alpha^{-i(2t-1)}$ and $\gamma_i = \alpha^{2i}$ has a parity check matrix H^* that is equivalent to $\left[\begin{smallmatrix} H_0 \\ H_1 \end{smallmatrix}\right]$ up to a permutation of rows. Let us consider the convolutional code generated by the generator polynomial matrix $H(D) = H_0 + DH_1$, see Equation 12.4. The polynomial generator matrix $H(D)$ can also be converted to a semi-infinite matrix H that defines the same code.

H(D) =

$$\begin{bmatrix} 1+D & \alpha+\alpha^{-1}D & \alpha^2+\alpha^{-2}D & \cdots & \alpha^{n-1}+\alpha^{(-n-1)}D \\ 1+D & \alpha^3+\alpha^{-3}D & \alpha^6+\alpha^{-6}D & \cdots & \alpha^{3(n-1)}+\alpha^{-3(n-1)}D \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1+D & \alpha^{\mu-1}+\alpha^{-(\mu-1)}D & \alpha^{2(\mu-1)}+\alpha^{-2(\mu-1)}D & \cdots & \alpha^{(\mu-1)(n-1)}+\alpha^{-(\mu-1)(n-1)}D \end{bmatrix} \tag{12.4}$$

Our goal is to show that under certain restrictions on n the following semi-infinite coefficient matrix H determines an $\mathbb{F}_{q^2}$-linear Hermitian self-orthogonal convolutional code

$$H = \begin{bmatrix} H_0 & H_1 & \mathbf{0} & \cdots & \cdots \\ \mathbf{0} & H_0 & H_1 & \mathbf{0} & \cdots \\ \vdots & \vdots & \vdots & \cdots & \ddots \end{bmatrix}. \tag{12.5}$$

To show that H is Hermitian self-orthogonal, it is sufficient to show that H_0, H_1 are both self-orthogonal and H_0 and H_1 are orthogonal to each other. A portion of this result is contained in [65, Lemma 8], *viz.*, $n = q^2 - 1$. We will prove a slightly stronger result. We will show that the matrices $\overline{H}_0, \overline{H}_1$ are self-orthogonal and mutually orthogonal, where

$$\overline{H}_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\mu-1} & \alpha^{2(\mu-1)} & \cdots & \alpha^{(\mu-1)(n-1)} \end{bmatrix} \text{ and} \tag{12.6}$$

$$\overline{H}_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{(-n-1)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{-(\mu-1)} & \alpha^{-2(\mu-1)} & \cdots & \alpha^{-(\mu-1)(n-1)} \end{bmatrix}. \tag{12.7}$$

Lemma 150. *Let $n|q^2-1$ such that $q+1 < n \leq q^2-1$ and $2 \leq \mu = 2t \leq \lfloor n/(q+1) \rfloor$, then*

$$\overline{H}_0 = (\alpha^{ij})_{1\leq i<\mu, 0\leq j<n} \quad \textit{and} \quad \overline{H}_1 = (\alpha^{-ij})_{1\leq i<\mu, 0\leq j<n} \tag{12.8}$$

are self-orthogonal with respect to the Hermitian inner product. Further, $\overline{H}_0$ is or-

thogonal to $\overline{H}_1$*.*

Proof. Denote by $\overline{H}_{0,j} = (1, \alpha^j, \alpha^{2j}, \cdots, \alpha^{j(n-1)})$ and $\overline{H}_{1,j} = (1, \alpha^{-j}, \alpha^{-2j}, \cdots, \alpha^{-j(n-1)})$, where $1 \leq j \leq \mu - 1$. The Hermitian inner product of $\overline{H}_{0,i}$ and $\overline{H}_{0,j}$ is given by

$$\langle \overline{H}_{0,i} | \overline{H}_{0,j} \rangle_h = \sum_{l=0}^{n-1} \alpha^{il} \alpha^{jql} = \frac{\alpha^{(i+jq)n} - 1}{\alpha^{i+jq} - 1}, \tag{12.9}$$

which vanishes if $i + jq \not\equiv 0 \mod n$. If $1 \leq i, j \leq \mu - 1 = \lfloor n/(q+1) \rfloor - 1$, then $q + 1 \leq i + jq \leq (q+1) \lfloor n/(q+1) \rfloor - (q+1) < n$; hence, $\langle \overline{H}_{0,i} | \overline{H}_{0,j} \rangle_h = 0$. Thus, $\overline{H}_0$ is self-orthogonal. Similarly, $\overline{H}_1$ is also self-orthogonal. Furthermore,

$$\langle \overline{H}_{0,i} | \overline{H}_{1,j} \rangle_h = \sum_{l=0}^{n-1} \alpha^{il} \alpha^{-jql} = \frac{\alpha^{(i-jq)n} - 1}{\alpha^{i-jq} - 1}. \tag{12.10}$$

This inner product vanishes if $\alpha^{i-jq} \neq 1$ or, equivalently, if $i - jq \not\equiv 0 \mod n$. Since $1 \leq i, j \leq \lfloor n/(q+1) \rfloor - 1 \leq q - 2$, we have $1 \leq i \leq \lfloor n/(q+1) \rfloor - 1 \leq q - 2$ while $q \leq jq \leq q \lfloor n/(q+1) \rfloor - q < n$. Thus $i \not\equiv jq \mod n$ and this inner product also vanishes, which proves the claim. □

Since H_i is contained in $\overline{H}_i$, we obtain the following:

Corollary 151. *Let* $2 \leq \mu = 2t \leq \lfloor n/(q+1) \rfloor$*, where* $n | q^2 - 1$ *and* $q + 1 < n \leq q^2 - 1$*. Then* H_0 *and* H_1 *are Hermitian self-orthogonal. Further,* H_0 *is orthogonal to* H_1 *with respect to the Hermitian inner product.*

The following example explains our construction.

Example 152. *Let* $q = 5$ *and* $t = 2$*, then* $n = 24$ *and* $2 \leq \mu = 4 \leq q - 1$*.*

$$H_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{22} & \alpha^{23} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \cdots & \alpha^{66} & \alpha^{69} \end{bmatrix} \quad \textit{and}$$

$$H_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \cdots & \alpha^{-22} & \alpha^{-23} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \cdots & \alpha^{-66} & \alpha^{-69} \end{bmatrix}$$

We notice that $H_0^q H_0 = 0$, $H_1^q H_1 = 0$, *and* $H_0^q H_1 = 0$. *Also if we extend* H_0 *by one row, we find that* $H_0^q H_0 \neq 0$.

Before we can construct quantum convolutional codes, we need to compute the free distances of C and $C^{\perp_h}$, where C is the convolutional code generated by H.

Lemma 153. *Let* $2 \leq 2t \leq \lfloor n/(q+1) \rfloor$, *where* $\gcd(n, 2) = 1$, $n | q^2 - 1$ *and* $q + 1 < n \leq q^2 - 1$. *Then the convolutional code* $C = \Gamma_{q^2} H$ *has free distance* $d_f \geq n - 2t + 1 > 2t + 1 = d_f^{\perp}$, *where* $d_f^{\perp} = \mathrm{wt}(C^{\perp_h})$ *is the free distance of* $C^{\perp_h}$.

Proof. Since $d_f^{\perp} = \mathrm{wt}(C^{\perp_h}) = \mathrm{wt}(C^{\perp})$, we compute the weight $\mathrm{wt}(C^{\perp})$. Let $c = (\dots, 0, c_0, \dots, c_l, 0, \dots)$ be a codeword in $C^{\perp}$ with $c_i \in \mathbb{F}_{q^2}^n$, $c_0 \neq 0$, and $c_l \neq 0$. It follows from the parity check equations $cH^T = 0$ that $c_0 H_1^T = 0 = c_l H_0^T$ holds. Thus, $\mathrm{wt}(c_0), \mathrm{wt}(c_l) \geq t+1$. If $l > 0$, then $\mathrm{wt}(c) \geq \mathrm{wt}(c_0) + \mathrm{wt}(c_l) \geq 2t+2$. If $l = 0$, then c_0 is in the dual of H^*, which is an $[n, n-2t, 2t+1]_{q^2}$ code. Thus $\mathrm{wt}(c) = \mathrm{wt}(c_0) \geq 2t+1$ and $d_f^{\perp} \geq 2t + 1$. But if c_x is in the dual of H^*, then $(\dots, 0, c_x, 0, \dots)$ is a codeword of C. Thus $d_f^{\perp} = 2t + 1$.

Let $(\dots, c_{i-1}, c_i, c_{i+1}, \dots)$ be a nonzero codeword in C. Observing the structure of C, we see that any nonzero c_i must be in the span of H^*. But H^* generates an $[n, 2t, n - 2t + 1]_{q^2}$ code. Hence $d_f \geq n - 2t + 1$. If $2t \leq \lfloor n/(q+1) \rfloor$, then $t \leq n/6$; thus $d_f \geq n - 2t + 1 > 2t + 1 = d_f^{\perp}$ holds. □

The preceding proof generalizes [119, Corollary 4] where the free distance of $C^{\perp}$ was computed for $q = 2^m$.

B. Quantum Convolutional Codes from RS Codes

We derive a family of quantum convolutional codes based on the previous construction of generalized Reed-Solomon Codes. Furthermore, we show the optimality of the derived quantum codes.

Theorem 154. *Let q be a power of a prime, n an odd divisor of q^2-1, such that $q+1<n\leq q^2-1$ and $2\leq \mu=2t\leq \lfloor n/(q+1)\rfloor$. Then there exists a pure quantum convolutional code with parameters $[(n,n-\mu,n;\mu/2,\mu+1)]_q$. This code is optimal, since it attains the Singleton bound with equality.*

Proof. The convolutional code generated by the coefficient matrix H in equation (12.5) has parameters $(n,\mu/2,\delta\leq\mu/2;1,d_f)_{q^2}$. Inspecting the corresponding polynomial generator matrix shows that $\delta\leq\mu/2$, since $\nu_i=1$ for $1\leq i\leq\mu/2$. By Corollary 151, this code is Hermitian self-orthogonal; moreover, Lemma 153 shows that the distance of its dual code is given by $d_f^\perp=\mu+1<d_f$. By Theorem 145, we can conclude that there exists a pure convolutional stabilizer code with parameters $[(n,n-\mu,n;\delta\leq\mu/2,\mu+1)]_q$. It follows from Theorem 148 that

$$\begin{aligned}\mu+1&\leq(\mu/2)\left(\lfloor 2\delta/(2n-\mu)\rfloor+1\right)+\delta+1\\&\leq(\mu/2)\left(\lfloor \mu/(2n-\mu)\rfloor+1\right)+\delta+1.\end{aligned}\tag{12.11}$$

Since $\lfloor\mu/(2n-\mu)\rfloor=0$, the right hand side equals $\mu/2+\delta+1$, which implies $\delta=\mu/2$ and the optimality of the quantum code. □

The following two examples explain our construction.

Example 155. *Let $q=4$ and $t=1$, then $n=15$ and $2\leq\mu=2\leq q-1$.*

$$H_0=\begin{bmatrix}1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{13} & \alpha^{14}\end{bmatrix}\tag{12.12}$$

and

$$H_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \cdots & \alpha^{-13} & \alpha^{-14} \end{bmatrix} \tag{12.13}$$

We notice that $H_0^q H_0 = 0$*,* $H_1^q H_1 = 0$*, and* $H_0^q H_1 = 0$*. Also if we extend* H_0 *by one row, we find that* $H_0^q H_0 \neq 0$*.*

Example 156. *Let* $q = 5$ *and* $t = 2$*, then* $n = 24$ *and* $2 \leq \mu = 4 \leq q - 1$*.*

$$H_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{22} & \alpha^{23} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \cdots & \alpha^3 & \alpha^{21} \end{bmatrix}$$

and

$$H_1 = \begin{bmatrix} 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \cdots & \alpha^{-22} & \alpha^{-23} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} & \alpha^{-12} & \cdots & \alpha^{-66} & \alpha^{-69} \end{bmatrix}$$

We notice that $H_0^q H_0 = 0$*,* $H_1^q H_1 = 0$*, and* $H_0^q H_1 = 0$*. Also if we extend* H_0 *by one row, we find that* $H_0^q H_0 \neq 0$*.*

C. Convolutional Codes from Quasi-Cyclic Subcodes of Reed-Muller Codes

An alternative method to construct convolutional codes from block codes is to use quasi-cyclic codes. We consider the Reed-Muller codes to construct a series quantum convolutional codes with varying memory. But first we review the necessary background on binary Reed-Muller codes. Furthermore, we use the framework developed by Esmaeili and Gulliver to construct quasi-cyclic subcodes RM codes from block RM codes over the binary field, see [43], [42] for more details.

Let $u, v \in \mathbb{F}_2^n$, where $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, u_2, \ldots, v_n)$. We define the boolean product

$$uv = (u_1v_1, u_2v_2, \ldots, u_nv_n). \tag{12.14}$$

The product of i such n-tuples is said to have a degree of i. Let $v_0 = (1, 1, \ldots, 1) \in \mathbb{F}_2^{2^m}$. For $m > 0$ and $1 \leq i \leq m$, define $b_i \in \mathbb{F}_2^{2^m}$ as concatenation of 2^{m-i} blocks of the form $\mathbf{01}$. Each block is of length 2^i and equal to $(\mathbf{01})$, where $\mathbf{0}, \mathbf{1} \in \mathbb{F}_2^{2^{i-1}}$.

Let $0 \leq r < m$ and $B = \{b_1, b_2, \ldots, b_m\} \subseteq \mathbb{F}_2^{2^m}$. Then the rth order Reed-Muller code is the span of v_0 and all products of elements in B upto and including the degree r and it is denoted by $\mathcal{R}(r, m)$. Let G_m^r denote the generator matrix of $\mathcal{R}(r, m)$. Let B_m^i denote all the products with exactly degree i. Then for $0 \leq i \leq r < m$ (see [42] for details)

$$G_m^r = \begin{bmatrix} B_m^r \\ B_m^{r-1} \\ \vdots \\ B_m^{i+1} \\ G_m^i \end{bmatrix}. \tag{12.15}$$

The dimension of $\mathcal{R}(r, m)$ is given by $k(r) = \sum_{i=0}^{r} \binom{m}{i}$ and its distance is given by 2^{m-r}. The dual of $\mathcal{R}(r, m)$ is given by $\mathcal{R}(r, m)^\perp = \mathcal{R}(m - 1 - r, m)$. The dual distance of $\mathcal{R}(r, m)$ is 2^{r+1} as can be easily verified. Further details on the properties of Reed-Muller codes can be found in [75].

Let $w_\mu = (110 \cdots 0) \in \mathbb{F}_2^{2^\mu}$. Let lw_μ denote the vector obtained by concatenating l copies of w_μ. For $0 \leq i \leq l - 1$, let $QM_{i,l} = (2^{l-i-1}w_{i+1}) \otimes B_{m-l}^{r-i}$ which is a matrix of size $\binom{m-l}{r-i} \times 2^m$ and for $i = l$ let $QM_{l,l} = \begin{bmatrix} G_{m-l}^{r-l} & \mathbf{0} & \cdots & \mathbf{0} \end{bmatrix}$. The convolutional code derived from the quasi-cyclic subcode of $\mathcal{R}(r, m)$ has the following generator matrix.

$$
\begin{aligned}
G &= \left[\begin{array}{c} QM_{0,l} \\ QM_{1,l} \\ \vdots \\ QM_{l-1,l} \\ QM_{l,l} \end{array}\right] \\
&= \left[\begin{array}{c|c|c|c|c|c|c} B^{r}_{m-l} & B^{r}_{m-l} & B^{r}_{m-l} & B^{r}_{m-l} & B^{r}_{m-l} & \cdots & B^{r}_{m-l} \\ B^{r-1}_{m-l} & B^{r-1}_{m-l} & \mathbf{0} & \mathbf{0} & B^{r-1}_{m-l} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \ddots \\ B^{r-l+1}_{m-l} & B^{r-l+1}_{m-l} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ G^{r-l}_{m-l} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{array}\right], \\
&= \left[\begin{array}{ccccc} G_0 & G_1 & \cdots & \cdots & G_{2^l-1} \end{array}\right]. \qquad (12.16)
\end{aligned}
$$

We note that $G_0 = G^{r}_{m-l}$ and for $1 \leq i \leq 2^l - 1$, the elements of G_i are a subset of the elements in G_0. The convolutional code generated by G has rate $\sum_{i=0}^{r} \binom{m-l}{i} / 2^{m-l}$ and free distance 2^{m-r} [42].

Lemma 157. *The free distance of the convolutional code orthogonal to G is 2^{r+1}.*

Proof. Assume that c is codeword in the space orthogonal to G. Without loss of generality we can take it to be of the form $c = (c_0, c_1, \ldots, c_i, \ldots)$, where all the $c_i = \mathbf{0}$, for $i < 0$. Since $cG^T = 0$, we have the following set of constraints for $t \geq 0$.

$$
\sum_{t-2^l-1}^{t} c_i G^{T}_{t-i} = 0. \qquad (12.17)
$$

Alternatively, we can write the above as a set of equations as

$$\begin{aligned} c_0 G_0^T &= 0, \\ c_1 G_0^T + c_0 G_1^T &= 0, \\ \vdots &= \vdots \\ c_i G_0^T + c_{i-1} G_1^T + \cdots + c_{i-2^l+1} G_{2^l-1}^T &= 0 \\ \vdots &= \vdots, \end{aligned} \tag{12.18}$$

□

If follows that $c_0 \in \mathcal{R}(r, m-l)^\perp$. Since the rowspace of G_i is a subset of the rowspace of G_0, it then follows that $c_0 G_1^T = 0$ giving $c_1 G_0^T = 0$. Thus c_1 is also in $\mathcal{R}(r, m-l)^\perp$. Proceeding like this we see that $c_i \in \mathcal{R}(r, m-l)^\perp$ for all $i \geq 0$. Thus the free distance of the code orthogonal to G is equal to the dual distance of $\mathcal{R}(r, m-l)$ which is 2^{r+1}.

Lemma 158. *Let $1 \leq l \leq m$ and $0 \leq r \leq \lfloor (m-l-1)/2 \rfloor$, then the convolutional code generated by G is self-orthogonal.*

Proof. It is sufficient to show that $G_i G_j^T = 0$ for $0 \leq i, j \leq 2^l - 1$. Since the rows of G_i are a subset of the rows of G_0 it suffices to show that G_0 is self-orthogonal. For G_0 to be self-orthogonal we require that $r \leq (m-l) - r - 1$ which holds. Hence, G generates a self-orthogonal convolutional code. □

D. Quantum Convolutional Codes from QC RM Codes

We can derive a family of QC RM codes as shown in the following Lemma.

Lemma 159. *Let $1 \leq l \leq m$ and $0 \leq r \leq \lfloor (m-l-1)/2 \rfloor$, then there exist pure linear quantum convolutional codes with the parameters $((2^{m-l}, 2^{m-l} - 2k, 2^l - 1))$ and* *free distance* 2^{r+1}*, where* $k = \sum_{i=0}^{r} \binom{m-l}{i}$.

Proof. Since G defines a linear self-orthogonal convolutional code with parameters $(2^{m-l}, k(r), 2^l - 1)$ and free distance 2^{m-r}, there exists a linear quantum convolutional code with the parameters $((2^{m-l}, 2^{m-l} - 2k(r), 2^l - 1))$. For $0 \leq r \leq \lfloor (m-l-1)/2 \rfloor$, the dual distance $2^{r+1} < 2^{m-r}$, hence the code is pure. □

It turns out that the convolutional codes in [42] that are used here have degree 0, hence, are a sequence of juxtaposed block codes disguised as convolutional codes. Consequently, the codes constructed in the previous theorem have parameters $[(2^{m-l}, 2^{m-l} - 2k(r), 0; 0, 2^{r+1})]_2$.

E. Conclusion and Discussion

We constructed two families of quantum convolutional codes based on RS and Reed-Muller codes. We showed that quantum convolutional codes derived from our constructions have better parameters in comparison to quantum block codes counterparts. We proved that the codes derived from RS codes are optimal in a sense that they it attains generalized Singleton bound with equality. One possible extension of this work is to construct other good families of quantum convolutional codes.

CHAPTER XIII

QUANTUM CONVOLUTIONAL CODES DERIVED FROM BCH CODES

Quantum convolutional codes can be used to protect a sequence of qubits of arbitrary length against decoherence. We introduce two new families of quantum convolutional codes. Our construction is based on an algebraic method which allows to construct classical convolutional codes from block codes, in particular BCH codes. These codes have the property that they contain their Euclidean, respectively Hermitian, dual codes. Hence, they can be used to define quantum convolutional codes by the stabilizer code construction. We compute BCH-like bounds on the free distances which can be controlled as in the case of block codes, and establish that the codes have non-catastrophic encoders. Some materials presented in this chapter are also published in [4,8] as a joint work with M. Grassl, A. Klappenecker, M. Rötteler, and P.K. Sarvepalli.

A. Introduction

Unit memory convolutional codes are an important class of codes that appeared in a paper by Lee [101]. He also showed that these codes have large free distance d_f among other codes (multi-memory) with the same rate. Convolutional codes are often designed heuristically. However, classes of unit memory codes were constructed algebraically by Piret based on Reed-Solomon codes [119] and by Hole based on BCH codes [73]. In a recent paper, doubly-cyclic convolutional codes are investigated which include codes derived from Reed-Solomon and BCH codes [55]. These codes are related, but not identical to the codes defined in this chapter.

A quantum convolutional codes encodes a sequence of quantum digits at a time. A stabilizer framework for quantum convolutional codes based on direct limits was developed in [10] including necessary and sufficient conditions for the existence of convolutional stabilizer codes. An $[(n, k, \mathrm{m}; \nu)]_q$ convolutional stabilizer code with free distance $d_f = \mathrm{wt}(C^\perp \backslash C)$ can also correct up to $\lfloor \frac{(d_f - 1)}{2} \rfloor$ errors. It is important to mention that the parameters of a quantum convolutional code Q are defined differently. The *memory* m is defined as the overlap length among any two infinite sequences of the code Q. Also, the *degree* ν is given by the degree of the classical convolutional code $C^\perp$. The code Q is *pure* if there are no errors less than d_f in the stabilizer of the code; $d_f = \mathrm{wt}(C^\perp \backslash C) = \mathrm{wt}(C^\perp)$.

Recall that one can construct convolutional stabilizer codes from self-orthogonal (or dual-containing) classical convolutional codes over $\mathbb{F}_q$ (cf. [10, Corollary 6]) and $\mathbb{F}_{q^2}$ (see [10, Theorem 5]) as stated in the following theorem.

Theorem 160. *An $[(n, k, nm; \nu, d_f)]_q$ convolutional stabilizer code exists if and only if there exists an $(n, (n-k)/2, m; \nu)_q$ convolutional code such that $C \leq C^\perp$ where the dimension of $C^\perp$ is given by $(n + k)/2$ and $d_f = \mathrm{wt}(C^\perp \backslash C)$.*

The main results of this chapter are: (a) a method to construct convolutional codes from block codes (b) a new class of convolutional stabilizer codes based on BCH codes. These codes have non-catastrophic dual encoders making it possible to derive non-catastrophic encoders for the quantum convolutional codes.

B. Construction of Convolutional Codes from Block Codes

In this section, we give a method to construct convolutional codes from block codes. This generalizes an earlier construction by Piret [120] to construct convolutional codes from block codes. One benefit of this method is that we can easily bound the free distance using the techniques for block codes. Another benefit is that we can give easily a non-catastrophic encoder.

Given an $[n, k, d]_q$ block code with parity check matrix H, it is possible to split the matrix H into $m+1$ disjoint submatrices H_i, each of length n such that

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_m \end{bmatrix}. \tag{13.1}$$

Then we can form the polynomial matrix

$$H(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \widetilde{H}_2 D^2 + \ldots + \widetilde{H}_m D^m, \tag{13.2}$$

where the number of rows of $H(D)$ equals the maximal number κ of rows among the matrices H_i. The matrices $\widetilde{H}_i$ are obtained from the matrices H_i by adding zero-rows such that the matrix $\widetilde{H}_i$ has κ rows in total. Then $H(D)$ generates a convolutional code. Of course, we already knew that H_i define block codes of length n, but taking the H_i from a single block code will allow us to characterize the parameters of the convolutional code and its dual using the techniques of block codes. Our first result concerns a non-catastrophic encoder for the code generated by $H(D)$.

Theorem 161. *Let $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$ linear code with parity check matrix H in $\mathbb{F}_q^{(n-k)\times n}$. Assume that H is partitioned into submatrices $H_0, H_1, \ldots, H_m$ as in equation (13.1) such that $\kappa = \operatorname{rk} H_0$ and $\operatorname{rk} H_i \leq \kappa$ for $1 \leq i \leq m$. Define the polynomial matrix*

$$H(D) = \widetilde{H}_0 + \widetilde{H}_1 D + \widetilde{H}_2 D^2 + \ldots + \widetilde{H}_m D^m, \tag{13.3}$$

where $\widetilde{H}_i$ are obtained from the matrices H_i by adding zero-rows such that the matrix $\widetilde{H}_i$ has a total of κ rows. Then we have:

(a) The matrix $H(D)$ is a reduced basic generator matrix.

(b) If the code C contains its Euclidean dual $C^\perp$ or its Hermitian dual $C^{\perp_h}$, then the convolutional code $U = \{\mathbf{v}(D)H(D) \,|\, \mathbf{v}(D) \in \mathbb{F}_q^{n-k}[D]\}$ is respectively contained in its dual code $U^\perp$ or $U^{\perp_h}$.

(c) Let d_f and $d_f^\perp$ respectively denote the free distances of U and $U^\perp$. Let d_i be the minimum distance of the code $C_i = \{v \in \mathbb{F}_q^n \,|\, v\widetilde{H}_i^t = 0\}$, and let $d^\perp$ denote the minimum distance of $C^\perp$. Then the free distances are bounded by $\min\{d_0 + d_m, d\} \leq d_f^\perp \leq d$ *and* $d_f \geq d^\perp$.

Proof. To prove the claim (a), it suffices to show that

i) $H(0)$ has full rank κ;

ii) $(\mathrm{coeff}(H(D)_{ij}, D^{\nu_i}))_{1\leq i\leq\kappa, 1\leq j\leq n}$ has full rank κ;

iii) $H(D)$ is non-catastrophic;

cf. [119, Theorem 2.16 and Theorem 2.24].

By definition, $H(0) = \widetilde{H}_0$ has rank κ, so i) is satisfied. Condition ii) is satisfied, since the rows of H are linearly independent; thus, the rows of the highest degree coefficient matrix are independent as well.

It remains to prove iii). Seeking a contradiction, we assume that the generator matrix $H(D)$ is catastrophic. Then there exists an input sequence $\mathbf{u}$ with infinite Hamming weight that is mapped to an output sequence $\mathbf{v}$ with finite Hamming weight, i. e. $v_i = 0$ for all $i \geq i_0$. We have

$$v_{i+m} = u_{i+m}\widetilde{H}_0 + u_{i+m-1}\widetilde{H}_1 + \ldots + u_i\widetilde{H}_m, \tag{13.4}$$

where $v_{i+m} \in \mathbb{F}_q^n$ and $u_j \in \mathbb{F}_q^\kappa$. By construction, the vector spaces generated by the rows of the matrices H_i intersect trivially. Hence $v_i = 0$ for $i \geq i_0$ implies that $u_{i-j}\widetilde{H}_j = 0$ for $j = 0, \ldots, m$. The matrix $\widetilde{H}_0$ has full rank. This implies that $u_i = 0$ for $i \geq i_0$, contradicting the fact that $\mathbf{u}$ has infinite Hamming weight; thus, the claim

(a) holds.

To prove the claim (b), let $\mathbf{v}(D)$, $\mathbf{w}(D)$ be any two codewords in U. Then from equation (13.4), we see that v_i and w_j are in the rowspan of H *i.e.* $C^\perp$, for any $i, j \in \mathbb{Z}$. Since $C^\perp \subseteq C$, it follows that $v_i \cdot w_j = 0$, for any $i, j \in \mathbb{Z}$ which implies that $\langle \mathbf{v}(D) \,|\, \mathbf{w}(D)\rangle = \sum_{i\in\mathbb{Z}} v_i \cdot w_i = 0$. Hence $U \subseteq U^\perp$. Similarly, we can show that if $C^{\perp_h} \subseteq C$, that $U \subseteq U^{\perp_h}$.

For the claim (c), without loss of generality assume that the codeword $\mathbf{c}(D) = \sum_{i=0}^{l} c_i D^i$ is in $U^\perp$, with $c_0 \neq 0 \neq c_l$. Then $\mathbf{c}(D)D^m$ and $\mathbf{c}(D)D^{-l}$ are orthogonal to every element in $H(D)$, from which we can conclude that $c_0 H_m^t = 0 = c_l H_0^t$. It follows that $c_0 \in C_0$ and $c_l \in C_l$. If $l > 0$, then $\mathrm{wt}(c_0) \geq d_m$ and $\mathrm{wt}(c_l) \geq d_0$ implying $\mathrm{wt}(\mathbf{c}(D)) \geq d_0 + d_m$. If $l = 0$, then $c_0 D^i$, where $0 \leq i \leq m$ is orthogonal to every element in $H(D)$, thus $c_0 H_i^t = 0$, whence $c_0 H^t = 0$ and $c_0 \in C$, implying that $\mathrm{wt}(c_0) \geq d$. It follows that $\mathrm{wt}(c) \geq \min\{d_0 + d_m, d\}$, giving the lower bound on $d_f^\perp$.

For the upper bound note that if c_0 is a codeword C, then $c_0 H_i^t = 0$. Therefore codeword $\mathbf{c}(D)$ and its shifts $\mathbf{c}(D)D^i$ for $0 \leq i \leq m$ are orthogonal to $H(D)$. Hence $\mathbf{c}(D) \in U^\perp$ and $d_f^\perp \leq d$.

Finally, let $\mathbf{c}(D)$ be a codeword in U. We saw earlier in the proof of (b) that that every c_i is in $C^\perp$. Thus $d_f \geq \min\{\mathrm{wt}(c_i)\} \geq d^\perp$. □

A special case of our claim (a) has been established by a different method in [73, Proposition 1].

C. Convolutional BCH Codes

One of the attractive features of BCH codes is that they allow us to design a code with desired distance. There have been prior approaches to construct convolutional BCH codes most notably [128] and [73], where one can control the free distance of the convolutional code. Here we focus on codes with unit memory. In the literature on convolutional codes there is a subtle distinction between unit memory and partial unit memory codes, however for our purposes, we will disregard such nuances. Our codes have better distance parameters as compared to Hole's construction and are easier to construct compared to [128].

1. Unit Memory Convolutional BCH Codes

Let $\mathbb{F}_q$ be a finite field with q elements, n be a positive integer such that $\gcd(n, q) = 1$. Let α be a primitive nth root of unity. A BCH code C of designed distance δ and length n is a cyclic code with generator polynomial $g(x)$ in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ whose defining set is given by $Z = C_b \cup C_{b+1} \cup \cdots \cup C_{b+\delta-2}$, where $C_x = \{xq^i \bmod n \mid i \in \mathbb{Z}, i \geq 0\}$. Let

$$H_{\delta,b} = \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{b(n-1)} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(b+1)(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{(b+\delta-2)} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(b+\delta-2)(n-1)} \end{bmatrix}.$$

Then $C = \{v \in \mathbb{F}_q^n \,|\, vH_{\delta,b}^t = 0\}$. If $r = \mathrm{ord}_n(q)$, then a parity check matrix, H for C is given by writing every entry in the matrix $H_{\delta,b}$ as a column vector over some $\mathbb{F}_q$-basis of $\mathbb{F}_{q^r}$, and removing any dependent rows. Let $B = \{b_1, \ldots, b_r\}$ denote a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Suppose that $w = (w_1, \ldots, w_n)$ is a vector in $\mathbb{F}_{q^r}^n$, then we can write $w_j = w_{j,1}b_1 + \cdots + w_{j,r}b_r$ for $1 \leq j \leq n$. Let $w^i = (w_{1,i}, \ldots, w_{n,i})$ be vectors in $\mathbb{F}_q^n$ with $1 \leq i \leq r$, For a vector v in $\mathbb{F}_q^n$, we have $v \cdot w = 0$ if and only if $v \cdot w^i = 0$ for all $1 \leq i \leq r$.

For a matrix M over $\mathbb{F}_{q^r}$, let $\mathrm{ex}_B(M)$ denote the matrix that is obtained by expanding each row into r rows over $\mathbb{F}_q$ with respect to the basis B, and deleting all but the first rows that generate the rowspan of the expanded matrix. Then $H = \mathrm{ex}_B(H_{\delta,b})$.

It is well known that the minimum distance of a BCH code is greater than or equal to its designed distance δ, which is very useful in constructing codes. Before we can construct convolutional BCH codes we need the following result on the distance of cyclic codes.

Lemma 162. *Let* $\gcd(n,q) = 1$ *and* $2 \leq \alpha \leq \beta < n$*. Let* $C \subseteq \mathbb{F}_q^n$ *be a cyclic code with defining set*

$$Z = \{z \mid z \in C_x, \alpha \leq x \leq \beta, x \not\equiv 0 \bmod q\}. \tag{13.5}$$

Then the minimum distance $\Delta(\alpha,\beta)$ *of* C *is lower bounded as*

$$\Delta(\alpha,\beta) \geq \begin{cases} q + \lfloor(\beta-\alpha+3)/q\rfloor - 2, & \text{if } \beta-\alpha \geq 2q-3; \\ \lfloor(\beta-\alpha+3)/2\rfloor, & \text{otherwise.} \end{cases} \tag{13.6}$$

Proof. Our goal is to bound the distance of C using the Hartmann-Tzeng bound (for instance, see [75]). Let $A = \{z, z+1, \ldots, z+a-2\} \subseteq Z$. Let $\gcd(b,q) < a$ and $A + jb = \{z+jb, z+1+jb, \ldots, z+a-2+jb\} \subseteq Z$ for all $0 \leq j \leq s$. Then by [75, Theorem 4.5.6], the minimum distance of C is $\Delta(\alpha,\beta) \geq a+s$.

We choose $b = q$, so that $\gcd(n,q) = 1 < a$ is satisfied for any $a > 1$. Next we choose $A \subseteq Z$ such that $|A| = q-1$ and $A + jb \subseteq Z$ for $0 \leq j \leq s$, with s as large as possible. Now two cases can arise. If $\beta - \alpha + 1 < 2q - 2$, then there *may not* always exist a set A such that $|A| = q-1$. In this case we relax the constraint that $|A| = q-1$ and choose A as the set of maximum number of consecutive elements. Then $|A| = a - 1 \geq \lfloor(\beta-\alpha+1)/2\rfloor$ and $s \geq 0$ giving the distance $\Delta(\alpha,\beta) \geq \lfloor(\beta-\alpha+1)/2\rfloor + 1 = \lfloor\beta-\alpha+3)/2\rfloor$.

If $(\beta - \alpha + 1) \geq 2q - 2$, then we can always choose a set $A \subseteq \{z \mid \alpha \leq z \leq \alpha + 2q - 3, z \not\equiv 0 \bmod q\}$ such that $|A| = q - 1$. Since we want to make s as large as possible, the worst case arises when $A = \{\alpha+q-1, \ldots, \alpha+2q-3\}$. Since $A + jb \subseteq Z$ holds for $0 \leq j \leq s$, it follows $\alpha + 2q - 3 + sq \leq \beta$. Thus $s \leq \lfloor(\beta - \alpha + 3)/q\rfloor - 2$. Thus the distance $\Delta(\alpha, \beta) \geq q + \lfloor(\alpha - \beta + 3)/q\rfloor - 2$. □

Theorem 163 (Convolutional BCH codes)**.** *Let n be a positive integer such that* $\gcd(n, q) = 1$*,* $r = \mathrm{ord}_n(q)$ *and* $2 \leq 2\delta < \delta_{\max}$*, where*

$$\delta_{\max} = \left\lfloor \frac{n}{q^r - 1}(q^{\lceil r/2\rceil} - 1 - (q-2)[r \text{ odd}]) \right\rfloor. \tag{13.7}$$

Then there exists a unit memory rate k/n convolutional BCH code with free distance $d_f \geq \delta + 1 + \Delta(\delta+1, 2\delta)$ and $k = n - \kappa$, where $\kappa = r\lceil \delta(1 - 1/q)\rceil$. The free distance of the dual is $\geq \delta_{\max} + 1$.

Proof. Let $C \subseteq \mathbb{F}_q^n$ be a narrow-sense BCH code of designed distance $2\delta + 1$ and B a basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Recall that a parity check matrix for C is given by $H = \mathrm{ex}_B(H_{2\delta+1,1})$. Further, let $H_0 = \mathrm{ex}_B(H_{\delta+1,1})$, then from

$$H_{2\delta+1,1} = \begin{bmatrix} H_{\delta+1,1} \\ H_{\delta+1,\delta+1} \end{bmatrix}, \tag{13.8}$$

it follows that $H = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$, where H_1 is the complement of H_0 in H. It is obtained from $\mathrm{ex}_B(H_{\delta+1,\delta+1})$ by removing all rows common to $\mathrm{ex}_B(H_{\delta+1,1})$. The code D_0 with parity check matrix $H_0 = \mathrm{ex}_B(H_{\delta+1,1})$ coincides with narrow-sense BCH code of length n and design distance $\delta + 1$.

By [8, Theorem 10], we have $\dim C = n - r\lceil 2\delta(1 - 1/q)\rceil$ and $\dim D_0 = n - r\lceil \delta(1 - 1/q)\rceil$; hence $\mathrm{rk}\, H = r\lceil 2\delta(1 - 1/q)\rceil$, $\mathrm{rk}\, H_0 = r\lceil \delta(1 - 1/q)\rceil$, and $\mathrm{rk}\, H_1 =$

$\operatorname{rk} H - \operatorname{rk} H_0 = r\lceil 2\delta(1-1/q)\rceil - r\lceil \delta(1-1/q)\rceil$. For $x > 0$, we have $\lceil x\rceil \geq \lceil 2x\rceil - \lceil x\rceil$; therefore, $\kappa := \operatorname{rk} H_0 \geq \operatorname{rk} H_1$.

By Theorem 161(a), the matrix H defines a reduced basic generator matrix

$$H(D) = \widetilde{H}_0 + D\widetilde{H}_1 \tag{13.9}$$

of a convolutional code of dimension κ, while its dual which we refer to as a convolutional BCH code is of dimension $n - \kappa$.

Now H_1 is the parity check matrix of a cyclic code, D_1 of the form given in Lemma 162, *i.e.* the defining set of D_1 is Z_1 as defined in (13.5) with $\alpha = \delta + 1$ and $\beta = 2\delta$. Since H_1 is linearly independent of H_0 we have $x \not\equiv 0 \bmod q$ in the definition of Z_1.

By Theorem 161(c), the free distance of the convolutional BCH code is bounded as $\min\{d_0 + d_1, d\} \leq d_f \leq d$. By Lemma 162, $d_1 \geq \Delta(\delta+1, 2\delta)$ and by the BCH bound $d_0 \geq \delta + 1$. Thus $d_f \geq \delta + 1 + \Delta(\delta+1, 2\delta)$. The dual free distance also follows from Theorem 161(c) as $d_f^\perp \geq d^\perp$. But $d^\perp \geq \delta_{\max} + 1$ by [8, Lemma 12]. □

2. Hole's Convolutional BCH Codes

In the previous construction of convolutional BCH codes we started with a BCH code with parity check matrix $H = H_{2\delta+1,1}$, see equation (13.8), and obtained H_0 to be the expansion of $H_{\delta+1,1}$. An alternate splitting of H gives us the Hole's convolutional BCH codes [73]. Because of space constraints we will not explore the details or other choices of splitting the parity check matrix of the parent BCH code.

We notice that if the matrix H satisfies the conditions in Theorem 161, then the convolutional code has non-catastrophic encoder. Furthermore the minimum free distance of this code is given by $d_f \geq d_{H_0} + d_{H_1}$ if $d_{H_0H_1} > d_{H_0} + d_{H_1}$, where d_{H_0}, d_{H_1}, and $d_{H_0H_1}$ are the minimum distances of the block codes $[n, n-\mu]$, $[n, n-\mu+\lambda]$, and

$[n, n-2\mu+\lambda]$ respectively, see [73, Proposition 2] for more details. Also, $d_f = d_{H_0H_1}$ if $d_{H_0H_1} \leq d_{H_0}+d_{H_1}$. We have showed in [11] that there exist a $[n, n-r\lceil(\delta-1)(1-1/q)\rceil]$ nonbinary dual-containing BCH code with designed distance $\delta = 2t+1$ and length $n = q^r - 1$ for $2 \leq \delta < \delta_{\max} = (q^{\lceil r/2\rceil} - 1 - (q-2)[r \text{ odd}])$ and $r = \text{ord}_n(q)$.

Let us construct the matrices H_0 and H_1 as follows. Let α be a primitive element in $\mathbb{F}_{q^r}$. Let $2 \leq t < q^{\lceil r/2\rceil-1} + 1$ and $r \geq 3$. Assume the matrix $\mathbf{H} = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$ has size $t(1-1/q) \times n$. We can extend every row of H into r-tuples of powers of α. Now, the matrix H_0 has size $(\lceil t(1-1/q)\rceil - 1)r \times n$ taking the first $(\lceil t(1-1/q)\rceil - 1)r$ rows of H.

$$H_0 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & (\alpha^3)^{(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-4} & \alpha^{2(\delta-4)} & \cdots & \alpha^{(\delta-4)(n-1)} \end{bmatrix}. \tag{13.10}$$

The matrix H_1 has size $(\lceil t(1-1/q)\rceil - 1)r \times n$ where all elements are zero except at the last row of H.

$$H_1 = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{\delta-2} & \alpha^{2(\delta-2)} & \cdots & \alpha^{(\delta-2)(n-1)} \end{bmatrix}. \tag{13.11}$$

Theorem 164. *Let H be a parity check matrix defined by $H_0 + DH_1$. If H is canonical, then there exists an $(n, k, m; d_f)$ convolutional code with $n = q^r - 1$, $k = n - r\lceil t(1-1/q)\rceil - r$, $m = r$, and $d_f \geq \delta$ for $2 \leq \delta = 2t+1 < \delta_{\max} = (q^{\lceil r/2\rceil} - 1 - (q-2)[r \text{ odd}])$.*

Proof. We first show that the parity check matrix $H = H_0 + DH_1$ is canonical. We notice that a) H_0 has full rank $(\lceil t(1-1/q)\rceil - 1)r$ rows; since it generates a BCH code with parameters $[n, n-(\lceil t(1-1/q)\rceil - 1)r]$. b) the last r rows of H_1 are linearly independent. c) the rows of the matrix H_0 are different and linearly independent of the last r rows of H_1. Therefore from [73, Proposition 1], The parity check matrix H is canonical and it generates a convolutional code C with parameters $(n, n-(\lceil t(1-1/q)\rceil - 1)r, r)$. Second, we compute the free distance of C. Notice that the matrix H_0 defines a BCH code with minimum distance $d_{H_0} \geq 2t-1 = \delta - 2$ from the BCH bound. Also, the matrix H_1 defines a BCH code with minimum distance at least 2 if two columns are equal. Therefore, the BCH code generated by $\mathbf{H} = \begin{bmatrix} H_0 \\ H_1 \end{bmatrix}$ with parameters $[n, n - \lceil t(1-1/q)\rceil r]$ has minimum distance $d_{\mathbf{H}} \geq \delta = 2t+1$. From [73, Proposition 2], the convolutional code C has free distance $d_f \geq \delta$. □

D. Constructing Quantum Convolutional Codes from Convolutional BCH Codes

In this section we derive one family of quantum convolutional codes derived from BCH codes. We briefly describe the stabilizer framework for quantum convolutional codes, see also [10, 69, 113]. The stabilizer is given by a matrix

$$S(D) = (X(D)|Z(D)) \in \mathbb{F}_q[D]^{(n-k)\times 2n}. \tag{13.12}$$

which satisfies the symplectic orthogonality condition $0 = X(D)Z(1/D)^t - Z(D)X(1/D)^t$. Let $\mathcal{C}$ be a quantum convolutional code defined by a stabilizer matrix as in eq. (13.12). Then n is called the frame size, k the number of logical qudits per frame, and k/n the rate of $\mathcal{C}$. It can be used to encode a sequence of blocks with k qudits in each block (that is, each element in the sequence consists of k quantum systems each of which is q-dimensional) into a sequence of blocks with n qudits.

The memory of the quantum convolutional code is defined as

$$m = \max_{1\leq i\leq n-k, 1\leq j\leq n} (\max(\deg X_{ij}(D), \deg Z_{ij}(D))). \tag{13.13}$$

We use the notation $[(n, k, m)]_q$ to denote a quantum convolutional code with the above parameters. We can identify $S(D)$ with the generator matrix of a self-orthogonal classical convolutional code over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$, which gives us a means to construct convolutional stabilizer codes. Analogous to the classical codes we can define the free distance, d_f and the degree ν, prompting an extended notation $[(n, k, m; \nu, d_f)]_q$. All the parameters of the quantum convolutional code can be related to the associated classical code as the following propositions will show. For proof and further details see [10][1].

Proposition 165. Let $(n, (n-k)/2, \nu; m)_q$ be a convolutional code such that $C \leq C^\perp$, where the dimension of $C^\perp$ is given by $(n + k)/2$. Then an $[(n, k, m; \nu, d_f)]_q$ convolutional stabilizer code exists whose free distance is given by $d_f = \mathrm{wt}(C^\perp \backslash C)$, which is said to be pure if $d_f = \mathrm{wt}(C^\perp)$.

Proposition 166. Let C be an $(n, (n-k)/2, \nu; m)_{q^2}$ convolutional code such that $C \subseteq C^{\perp_h}$. Then there exists an $[(n, k, m; \nu, d_f)]_q$ convolutional stabilizer code, where $d_f = \mathrm{wt}(C^{\perp_h} \setminus C)$.

Under some restrictions on the designed free distance, we can use convolutional codes derived in the previous section to construct quantum convolutional codes. These codes are slightly better than the quantum block codes of equivalent error correcting capability in the sense that their rates are slightly higher.

[1]A small difference exists between the notion of memory defined here and the one used in [10].

Theorem 167. *Assume the same notation as in Theorem 163. Then there exists a quantum convolutional code with parameters* $[(n, n-2\kappa, n)]_q$, *where* $\kappa = r\lceil\delta(1-1/q)\rceil$. *Its free distance* $d_f \geq \delta + 1 + \Delta(\delta+1, 2\delta)$, *and it is pure to* $d' \geq \delta_{\max} + 1$.

Proof. We construct a unit memory $(n, n-\kappa)_q$ classical convolutional BCH code as per Theorem 163. Its polynomial parity check matrix $H(D)$ is as given in equation (13.9). Using the same notation in the proof, we see that the code contains its dual if H is self-orthogonal. But given the restrictions on the designed distance, we know from [8, Theorem 3] that the BCH block code defined by H contains its dual. It follows from Theorem 161(b) that the convolutional BCH code contains its dual. From [10, Corollary 6], we can conclude that there exists a convolutional code with the parameters $[(n, n-2\kappa, n)]_q$. By Theorem 163 the free distance of the dual is $d' \geq \delta_{\max} + 1$, from whence follows the purity. □

Another popular method to construct quantum codes makes use of codes over $\mathbb{F}_{q^2}$.

Lemma 168. *Let* $2 \leq 2\delta < \lfloor n(q^r-1)/(q^{2r}-1)\rfloor$, *where and* $r = \mathrm{ord}_n(q^2)$. *Then there exist quantum convolutional codes with parameters* $[(n, n-2\kappa, n)]_q$ *and free distance* $d_f \geq \delta + 1 + \Delta(\delta+1, 2\delta)$, *where* $\kappa = r\lceil\delta(1-1/q^2)\rceil$.

Proof. By Theorem 163 there exists an $(n, n-\kappa, 1)_{q^2}$ convolutional BCH code with the polynomial parity check matrix as in equation (13.9). The parent BCH code has design distance $2\delta+1$ and given the range of δ, we know by [10, Theorem 14] that it contains its Hermitian dual. By Theorem 161(b), the convolutional code also contains its Hermitian dual. By [10, Theorem 5], we can conclude that there exists a convolutional stabilizer code with parameters $[(n, n-2\kappa, n)]_q$. □

In [10], we have shown generalized Singleton bound for convolutional stabilizer codes. The free distance of an $[(n, k, m; \nu, d_f)]_q$ $\mathbb{F}_{q^2}$-linear pure convolutional stabilizer code is bounded by

$$d_f \quad \leq \quad \frac{n-k}{2}\left(\left\lfloor \frac{2\nu}{n+k} \right\rfloor + 1\right) + \nu + 1. \tag{13.14}$$

The bound can be reformulated in terms of the memory m instead of the total constraint length ν. Observe that if $m = 0$, then it reduces to the quantum Singleton bound viz. $d_f \leq (n-k)/2 + 1$.

Corollary 169. *A pure $((n, k, m, d_f))_q$ linear quantum convolutional code obeys*

$$d_f \leq \frac{n-k}{2}\left\lfloor \frac{m(n-k)}{n+k} \right\rfloor + (n-k)(m+1)/2 + 1.$$

Proof. The proof is actually straightforward. It follows from [10, Theorem 7] and the fact that $\delta \leq m(n-k)/2$ □

E. QCC from Product Codes

Let (n, k, m) be a classical convolutional code that encodes k information into n bits with memory order m. We construct quantum convolutional codes based on product codes as shown in [68]. We explicitly determine parameters of the constructed codes with the help of results from [8]. We follow the natation that has been used in [69].

Lemma 170. *Let $C_1 = (n_1, k_1, m_1)$ be a classical linear convolutional code over $\mathbb{F}_q$. Also, let $C_2 = (n_2, k_2, m_2)$ be an Euclidean self-orthogonal linear code over $\mathbb{F}_q$. Then the product code $C_1 \otimes C_2 = (n_1n_2 - m, n_1n_2 - k_1k_2, m)$ defines a quantum convolutional code with memory $m_1 * m_2$.*

Proof. See [68, Theorem 10]. □

Now, we can restrict ourselves to one class of codes. Consider the convolutional BCH codes derived in this chapter [4]. We know that the code is dual-containing if

$\delta \leq \delta_{max}$. In our construction, we do not require both C_1 and C_2 to be convolutional codes or even self-orthogonal. We choose C_1 to be an arbitrary convolutional code and C_2 can be self-orthogonal block or convolutional code as shown in Theorem 170. Therefore, it is straightforward to derive quantum convolutional BCH codes from BCH product codes as shown in Theorem 171. The reason we use this construction rather than the convolutional unit memory code construction is because the quantum codes derived from product codes have efficient encoding circuits as shown in [69].

Theorem 171. *Let n be a positive integer such that $\gcd(n, q) = 1$. Let C_1 be a convolutional BCH code with length n, designed distance δ_1 and memory m. Let $C_2^\perp$ be a BCH code with designed distance $2 \leq \delta_2 \leq q^{\lceil r/2 \rceil} - 1 - (q-2)[r \text{ odd}]$. then there exists a quantum convolutional BCH code constructed from the product code $C_1 \otimes C_2$ and with the same parameters as C_1.*

Proof. We know that the code C_2 is self-orthogonal since $2 \leq \delta_2 \leq q^{\lceil r/2 \rceil} - 1 - (q - 2)[r \text{ odd}]$. From [68], the convolutional product code $C_1 \otimes C_2$ is self-orthogonal and it has memory m. From [4, Proposition 1.], there exists a quantum convolutional BCH code with the given parameters. □

F. Efficient Encoding and Decoding Circuits of QCC-BCH

Quantum convolutional codes promise to make quantum information more reliable because they have online encoding and decoding circuits. What we mean by online encoder and decoder is that the encoded and decoded qudits can be sent or received with a constant delay. The phase estimation algorithm can be used to measure the received quantum information. In this section, we design efficient encoding and decoding circuits for unit memory quantum convolutional codes derived in this chapter [4, 10]. We use the framework established in [69, 70].

Grassl and Rötteler showed that an encoder circuit $\mathcal{E}$ for a quantum convolutional code C exists if the gates in $\mathcal{E}$ can be arranged into a circuit of finite depth. This can be applied to quantum convolutional codes derived from CSS-type classical codes, as well as product codes as shown in [69, Theorem 5].

Let us assume we have two classical codes C_1 and C_2 with parameters (n, k_1) and (n, k_2) and represented by a parity check matrices H_1 and H_2, respectively. Let us construct the matrix

$$\left(\begin{array}{c|c} H_2(D) & 0 \\ 0 & H_1(D) \end{array}\right) \subseteq \mathbb{F}_q[D]^{(2n-k_1-k_2)\times 2n}$$

where $H_i(D)$ is the polynomial matrix of the matrix H_i.

We can assume that the matrix $H = H_1 + H_2D$ defines a convolutional BCH code. The matrices $H_1(D)$ and $H_2(D)$ correspond to non-catastrophic and delay-free encoders. They also have full-rank k_1 and k_2 [4]. The following theorem shows that there exists an encoding circuit for quantum convolutional codes derived from convolutional BCH codes.

Theorem 172. *Let Q be a quantum convolutional code derived from convolutional BCH code as shown in Theorem 163. Then Q has an encoding circuit whose depth is finite.*

Proof. We know that there is a convolutional BCH code with a generator matrix $H = H_1 + H_2D$. Furthermore, the matrices H_1 and H_2 define two BCH codes with parameters (n, k_1) and (n, k_2). Let us construct the stabilizer matrix

$$(X(D)|Z(D)) = \left(\begin{array}{c|c} H_2(D) & 0 \\ 0 & H_1(D) \end{array}\right) \subseteq \mathbb{F}_q[D]^{(2n-k_1-k_2)\times 2n}. \qquad (13.15)$$

The matrices $H_1(D)$ and $H_2(D)$ correspond to two encoders satisfying i) they correspond to non-catastrophic encoders as shown in [4, Theorem 3.]. ii) they have full-ranks $n-k_1$ and $n-k_2$. iii) they have delay-free encoders. Therefore, they have a Smith normal form given by

$$A_1(D)H_2(D)B_1(D) = \begin{pmatrix} I & 0 \end{pmatrix}, \tag{13.16}$$

for some chosen matrices of $A_1(D) \in \mathbb{F}_q[D]^{(n-k_2)\times(n-k_2)}$ and $B_1(D) \in \mathbb{F}_q[D]^{n\times n}$.

□

G. Conclusion and Discussion

In this chapter, we presented a general method to derive unit memory convolutional codes, and applied it to construct convolutional BCH codes. In addition, we derived two families of quantum convolutional codes based on BCH codes. By this construction, other families of convolutional cyclic codes can be derived and convolutional stabilizer codes can be also constructed.

CHAPTER XIV

DISSERTATION CONCLUSION

The operations of a quantum computer take advantage of quantum mechanical phenomena, such as superposition and entanglement, to solve certain problems efficiently and more quickly than their classical counterparts. However, our ability to mitigate the noise resulting from decoherence effects will determine whether or not a quantum computer can be built. Henceforth, quantum error correcting codes are needed to correct quantum information.

In this dissertation, I studied various aspects of quantum error control codes – the key component of fault-tolerant quantum information processing. I presented the fundamental theory and necessary background of quantum block and convolutional codes, and subsystem codes. I constructed many families of quantum error control codes over finite fields.

Quantum Block Codes. I established conditions when BCH codes are self-orthogonal (or dual-containing) with respect to Euclidean an Hermitian inner products. Henceforth, I derived two families of nonbinary quantum BCH codes [8, 11]. I studied duadic group algebra codes given a finite group with odd and even orders, and I set conditions when there are μ_{-1} and μ_{-q} splitters for elements of this group. Consequently, I derived a family of quantum duadic codes with remarkable minimum distance [7, 12]. Finally, I investigated LDPC codes and constructed classes of self-orthogonal LDPC codes based on orthogonal *Latin* Squares and finite geometries [3, 13]. Hence, I derived families of quantum LDPC codes, in which they can be decoded using standard known-iterative decoders.

Subsystem Codes. I gave an introduction to subsystem codes, and then I presented several methods for subsystem code constructions. I derived families of subsystem codes derived from BCH and RS code, and I presented a family of MDS and optimal subsystem codes [5, 6, 9]. In addition, I demonstrated tables of lower and upper bounds on subsystem code parameters.

Quantum Convolutional Codes. I established a general framework for deriving quantum convolutional codes from block codes – known as unit memory quantum convolutional codes. I derived the first families of quantum convolutional codes based on RS and BCH codes [4, 10]. Using our formalism, it is possible to construct other families of quantum convolutional codes. Also, I established bounds on the quantum convolutional code parameters – generalized Singleton bound.

A. Open Problems

Some of the open-related problems to the work done in this dissertation are listed below.

i) In this dissertation, I presented many families of quantum block and convolutional codes derived from BCH and RS codes. It will be interesting to construct other families of quantum block and convolutional codes and compare them with the aforementioned constructed codes. In addition, why the new families are superior in comparison to other known families. I gave a formulation for generalized Singleton bound, it remains open question to derive other bounds on the parameters of quantum convolutional codes.

ii) I constructed some new families of subsystem codes. It will be interesting to construct additional new families of subsystem codes and compare their performance with the codes presented in part II of this dissertation.

iii) One can construct quantum codes based on the entanglement property of quantum states. It will be interesting to generalize some of the constructed families in this dissertation to quantum error control codes with entanglement.

iv) How can a family of stabilizer codes use fault-tolerant quantum computing? What is its threshold value? Can it be improved? If so, what are the assumptions that need to be made to improve it?

v) We know that error avoiding codes (subsystem codes) can be constructed from block codes. Do we have a similar scenario for quantum convolutional codes where the errors can be isolated into subsystems, i.e. subsystem convolutional codes?

vi) Study the probability of undetected errors for some families of stabilizer and subsystem codes and search for codes with undetected error probability that approaches zero.

vii) We know that Fire codes and burst-error codes can correct errors beyond half of their minimum distance. Do we have quantum stabilizer codes in which errors have some nice structure so that we can correct beyond the minimum distance?

B. Author Contributions

During my Ph.D. studies I investigated various problems in both classical and quantum error control codes. In addition, I studied capacity of network coding and networked data storage algorithms for wireless and sensor networks.

Quantum Error Control Codes. While this dissertation highlighted some of my work in quantum error control codes, there are also some families of quantum codes that have not been mentioned in this dissertation. The following list shows some of my contributions.

- S. A. Aly and A. Klappenecker, Subsystem Code Constructions, IEEE International Symposium on Information Theory, ISIT08, Toronto, Canada, submitted 2008.
- S. A. Aly, A. Klappenecker, P.K. Sarvepalli, On Quantum and Classical BCH Codes, IEEE Transaction on Information Theory, 53(3):1183–1188, 2007.
- S. A. Aly, A. Klappenecker, and P. Sarvepalli. Primitive quatnum BCH codes over finite fields. *Proc. 2006 IEEE International Symposium on Information Theory, Seattle, USA*, pages 1114 – 1118, July 2006.
- S. A. Aly, A. Klappenecker, and P. Sarvepalli. Remarkable degenerate quantum stabilizer codes derived from duadic codes. *Proc. 2006 IEEE International Symposium on Information Theory, Seattle, USA*, pages 1105–1108, July 2006.
- S. A. Aly, A. Klappenecker, and P. Sarvepalli. Subsystem codes. *Proceedings of the 45th Allerton Conference on Communication, Control, and Computing, Urbana, IL*, September 2006.
- P.K. Sarvepalli, S. A. Aly, and A. Klappenecker. Nonbinary stabilizer codes. In G. Chen, L. Kauffman, and S. Lomonaco, editors, *The Mathematics of Quantum Computation and Quantum Technology.* Taylor & Francis, 2007.
- S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli. Quantum convolutionlal BCH codes. *10th Canadian Workshop on Information Theory, CWIT '07*, pages 180 – 183, 6-8 June 2007.
- S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Duadic group algebra codes.

Proc. 2007 IEEE International Symposium on Information Theory, Nice, France, pages 2096–2100, June 2007.

- S. A. Aly, A. Klappenecker, and P. K. Sarvepalli. Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes. *Proc. 2007 IEEE International Symposium on Information Theory, Nice, France*, pages 821–825, June 2007.

Capacity of Network Coding. I studied network coding capacity for wireless network networks, and established upper and lower bounds on the capacity of network coding.

- S. A. Aly, V. Kapoor, A. Klappenecker, H. Lee, and J. Meng, On network coding for wireless sensor networks,IEEE International Symposium on Information Theory, ISIT08, Toronto, CA, submitted 2008.
- S. A. Aly, V. Kapoor, A. Klappenecker, and J. Meng, Bounds on the network coding capacity for wireless random networks, Third Workshop on Network Coding, Theory, and Applications, San Diego, California, Jan 29, 2007.
- Z. Kong, S. A. Aly, E. Soljanin, E. Yan, and A. Klappenecker, Network coding capacity of random wireless networks under a signal-to-interference-and-noise model, Proceedings of the 45th Allerton Conference on Communication, Control, and Computing, Urbana, IL, October, 2007.
- Z. Kong, S. A. Aly, E. Soljanin, E. Yan, and A. Klappenecker, Network coding capacity of random wireless networks under a signal-to-interference-and-noise model, submitted to IEEE Trans. Inform. Theory, 2007.

Networked Data Storage Algorithms I designed networked data storage algorithms for large-scale wireless sensor networks based on Fountain codes.

- S. A. Aly, Z. Kong, and E. Soljanin, Fountain codes based distributed storage algorithms for large-scale wireless sensor networks, submitted to IEEE/ACM Information Processing of Sensor Networks, IPSN 2008.

- S. A. Aly, Z. Kong, and E. Soljanin, Raptor codes based distributed storage algorithms for wireless sensor networks, IEEE ISIT 2008.

Coding Theory and Cryptography I studied various methods to construct LDPC codes derived from combinatorial objects and finite geometry. I constructed regular LDPC codes based on nonprimtive BCH codes and based on Latin squares.

- S. A. Aly, A. Klappenecker, and E. Soljanin, Constructions of regular LDPC codes derived from non-primitive BCH codes, International Journal of Communication Letter, 2008.

- S. A. Aly, On Quantum Hamming Bound, Technical Report, Department of Computer Science, Texas A&M University, November, 2007.

- S. A. Aly, Quantum LDPC codes derived from Latin squares, Technical Report, Department of Computer Science, Texas A&M University, April 2008.

- S. A. Aly, K. Alsamara, H. Abu-Salem, A multicast security of simple network management protocol, International Journal of Management Review, Volume 1, number 3, 2005.

- H. Abu-Salem, S. A. Aly, K. Mostafa, Verification and Analysis of Security Protocols Using Colored Petri Nets, International Arab Conference on Information Technology (ACIT05), Al-Isra Private University, Jordan, 6th -8th December 2005.

REFERENCES

[1] P. Aliferis and A. W. Cross, "Subsystem fault tolerance with the bacon-shor code," *Physical Review Letters*, vol. 98, no. 220502, 2007, quant-ph/0610063.

[2] S. A. Aly, "A note on quantum hamming bound," Technical Report, Department of Computer Science, Texas A&M University, November 2007, arXiv:quant-ph/0711.4603.

[3] ——, "A class of quantum LDPC codes constructed from finite geometries," in *Proc. 2008 IEEE International Symposium on Information Theory*, Toronto, Canada, Submitted 2008, arXiv:quant-ph/0712.4115.

[4] S. A. Aly, M. Grassl, A. Klappenecker, M. Rötteler, and P. K. Sarvepalli, "Quantum convolutional BCH codes," in *10th Canadian Workshop on Information Theory, CWIT '07*, 6-8 June 2007, pp. 180 – 183.

[5] S. A. Aly and A. Klappenecker, "Structures and constructions of subsysem codes over finite fields," *IEEE Trans. Inform. Theory*, 2008, on submission.

[6] ——, "Subsysem code constructions," in *Proc. 2008 IEEE International Symposium on Information Theory, Toronto, Canada, Submitted*, 2008, arXiv:quant-ph/0712.4321v2.

[7] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "Duadic group algebra codes," in *Proc. 2007 IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 2096–2100.

[8] ——, "On quantum and classical BCH codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.

[9] ——, "Subsystem codes," in *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2006.

[10] ——, "Quantum convolutional codes derived from Reed-Solomon and Reed-Muller codes," in *Proc. 2007 IEEE International Symposium on Information Theory*, June Nice, France, 2007, pp. 821–825.

[11] ——, "Primitive quantum BCH codes over finite fields," in *Proc. 2006 IEEE International Symposium on Information Theory*, Seattle, USA, July 2006, pp. 1114 – 1118.

[12] ——, "Remarkable degenerate quantum stabilizer codes derived from duadic codes," in *Proc. 2006 IEEE International Symposium on Information Theory*, Seattle, USA, July 2006, pp. 1105–1108.

[13] S. A. Aly, A. Klappenecker, and E. Soljanin, "Constructions of regular LDPC derived from nonprimitive BCH codes," *International Journal of Communication Letters*, on preparation, 2007.

[14] V. Arvind, P. P. Kurur, and K. R. Parthasarathy, "Nonstabilizer quantum codes from abelian subgroups of the error group," *Quantum Physics e-prints*, 2002, quant-ph/0210097.

[15] A. E. Ashikhmin, A. M. Barg, E. Knill, and S. N. Litsyn, "Quantum error detection II: Bounds," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 789–800, 2000.

[16] A. E. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[17] A. E. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 4, pp. 1206–1215, 1999.

[18] E. F. Assmus and J. D. Key, *Polynomial Codes and Finite Geometries, Handbook of Coding Theory*, V. Pless and W. Hufffman, Eds. Amsterdam: Elsevier, 1998, vol. 2, chapter 16.

[19] D. Bacon, "Operator quantum error correcting subsystems for self-correcting quantum memories," *Phys. Rev. A.*, vol. 73, no. 012340, 2006.

[20] D. Bacon and A. Casaccino, "Quantum error correcting subsystem codes from two classical linear codes," in *Proc. of the 45th Allerton Conference on Communication, Control, and Computing*, Monticello, Illinois, September 2006.

[21] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Physical Review A*, vol. 54, pp. 3824–3851, 1996.

[22] T. Berger and L. de Maximy, "Cyclic projective Reed-Muller codes," in *Proc. of Applied Algebra, Algebraic Algorithms and Error Correcting Codes*, vol. AAECC-14, no. 2227, in LNCS, Springer-Verlag, 2001, pp. 77–81.

[23] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[24] R. E. Blahut, *Algebraic Codes for Data Transmission.* Cambridge: Cambridge University Press, 2003.

[25] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Information and Control*, vol. 3, pp. 279–290, 1960.

[26] ——, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, 1960.

[27] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symb. Comp.*, vol. 24, pp. 235–266, 1997.

[28] S. B. Bravyi and A. Y. Kitaev, "Quantum codes on a lattice with boundary," 1998, quant-ph/9810052.

[29] T. Brun, I. Devetak, and M. Hsieh, "Catalytic quantum error correction," 2006, arXiv:quant-ph-0608027v2.

[30] 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*, vol. 44, pp. 1369–1387, 1998.

[31] A. Calderbank and P. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 1996.

[32] P. Charpin, "Open problems on cyclic codes," in *Handbook of Coding Theory*. Amsterdam: North-Holland, 1998, vol. I,II, pp. 963–1063.

[33] H. F. Chau, "Quantum convolutional codes error-correcting codes," *Phys. Rev. A*, vol. 58, no. 2, pp. 905–909, 1998.

[34] ——, "Good quantum convolutional error-correction codes and their decoding algorithm exist," *Phys. Rev. A*, vol. 60, no. 3, pp. 1966–1974, 1999.

[35] R. Cleve, "Quantum stabilizer codes and classical linear codes," *Phys. Rev. A*, vol. 55, no. 6, pp. 4054–4059, 1997.

[36] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A*, vol. 56, no. 1, pp. 76–82, 1997.

[37] G. Cohen, S. Encheva, and S. Litsyn, "On binary constructions of quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2495–2498, 1999.

[38] P. Cohn, *Basic Algebra – Groups, Rings, and Fields.* London: Springer, 2005.

[39] A. C. A. de Almeida and R. Palazzo Jr., "Comment on quantum convolutional error-correcting codes," *Phys. Rev. A*, vol. 72, no. 026301, 2005.

[40] ——, "A concatenated [(4, 1, 3)] quantum convolutional code," in *Proc. IEEE Inform. Theory Workshop*, San Antonio, TX, 2004, p. 28.

[41] P. Delsarte, "Bounds for unrestricted codes by linear programming," *Philips Res. Reports*, vol. 27, pp. 272–289, 1972.

[42] M. Esmaeili, T. Gulliver, and N. Secord, "A link between quasi-cyclic codes and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 1, pp. 431–435, 1998.

[43] M. Esmaeili, T. Gulliver, N. Secord, and S. Mahmoud, "Quasi-cyclic structure of Reed-Muller codes and their smallest regular trellis diagram," *IEEE Trans. Inform. Theory*, vol. 43, no. 3, pp. 1040–1052, 1997.

[44] K. Feng, "Quantum codes $[[6,2,3]]_p$, $[[7,3,3]]_p$ $(p \geq 3)$ exist," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2384–2391, 2002.

[45] ——, "Quantum error-correcting codes," in *Coding Theory and Cryptology.* Hackensack, NJ: World Scientific, 2002, pp. 91–142.

[46] K. Feng and Z. Ma, "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3323–3325, 2004.

[47] G. D. Forney Jr., “Convolutional codes I: Algebraic structure,” *IEEE Trans. Inform. Theory*, vol. 16, no. 6, pp. 720–738, 1970.

[48] ——, “Use of sequential decoders to analyze convolutional code structure,” *IEEE Trans. Inform. Theory*, vol. 16, no. 6, pp. 793–795, 1970.

[49] G. D. Forney Jr., M. Grassl, and S. Guha, “Convolutional and tail-biting quantum error-correcting codes,” *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 865–880, 2007.

[50] G. D. Forney Jr. and S. Guha, “Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes,” in *Proc. of 2005 IEEE Intl. Symposium on Information Theory*, Adelaide, Australia, 2005, pp. 1028–1032.

[51] M. H. Freedman and D. A. Meyer, “Projective plane and planar quantum codes,” *Found. Comput. Math.*, vol. 1, no. 3, pp. 325–332, 2001.

[52] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, “Strongly-MDS convolutional codes,” *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 584–598, 2006.

[53] H. Gluesing-Luerssen and W. Schmale, “Distance bounds for convolutional codes and some optimal codes,” 2003. [Online]. Available: arXiv.org:math/0305135

[54] ——, “On cyclic convolutional codes,” *Acta. Appl. Mathematicae*, vol. 82, pp. 183–237, 2004.

[55] ——, “On doubly-cyclic convolutional codes,” 2004. [Online]. Available: arXiv.org:math/0410317

[56] D. Gorenstein and N. Zierler, "A class of error-correcting codes in p^m symbols," *J. Soc. Indust. Appl. Math.*, vol. 9, pp. 207–214, 1961.

[57] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862–1868, 1996.

[58] ——, "Stabilizer codes and quantum error correction," 1997, Caltech Ph. D. dissertation, eprint: quant-ph/9705052.

[59] ——, "Fault-tolerant quantum computation with higher-dimensional systems," *Chaos, Solitons, Fractals*, vol. 10, no. 10, pp. 1749–1758, 1999.

[60] ——, "An introduction to quantum error correction," in *Proc. of Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium*, S. J. Lomonaco, Jr., Ed. Providence, RI: American Mathematical Society, 2002, pp. 221–235, eprint: quant-ph/0004072.

[61] ——, "Quantum error correction and fault-tolerance," 2005, eprint: quant-ph/0507174.

[62] M. Grassl, "Algorithmic aspects of error-correcting codes," in *Proc. of the Mathematics of Quantum Computing*, R. Brylinski and G. Chen, Eds. Baca Raton, FL: CRC Press, 2001, pp. 223–252.

[63] M. Grassl and T. Beth, "Cyclic quantum error-correcting codes and quantum shift registers," in *Proc. Royal Soc. London Series A*, vol. 456, no. 2003, 2000, pp. 2689–2706.

[64] ——, "Quantum BCH codes," in *Proc. X. Int'l. Symp. Theoretical Electrical Engineering*, Magdeburg, 1999, pp. 207–212.

[65] M. Grassl, T. Beth, and M. Rötteler, "On optimal quantum codes," *Internat. J. Quantum Information*, vol. 2, no. 1, pp. 757–775, 2004.

[66] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed-Solomon codes," in *Applied Algebra, Algebraic Algorithms and Error-correcting Codes*, ser. Honolulu, HI, Lecture Notes in Comput. Sci. Berlin: Springer, 1999, vol. 1719, pp. 231–244.

[67] M. Grassl, A. Klappenecker, and M. Rötteler, "Graphs, quadratic forms, and quantum codes," in *Proc. 2002 IEEE Intl. Symp. Inform. Theory.* IEEE, Lausanne, Switzerland, 2002, p. 45.

[68] M. Grassl and M. Rötteler, "Quantum block and convolutional codes from self-orthogonal product codes," in *Proc. 2005 IEEE Intl. Symposium on Information Theory*, Adelaide, Australia, 2005, pp. 1018–1022.

[69] ——, "Constructions of quantum convolutional codes," in *Proc. 2007 IEEE Intl. Symposium on Information Theory*, Nice, France, 2007, pp. 816–820.

[70] ——, "Non-catastrophic encoders and encoder inverses for quantum convolutional codes," in *Proc. 2006 IEEE Intl. Symposium on Information Theory*, Seattle, WA, USA, 2006, pp. 1109–1113.

[71] M. Grassl, M. Rötteler, and T. Beth, "Efficient quantum circuits for non-qubit quantum error-correcting codes," *Internat. J. Found. Comput. Sci.*, vol. 14, no. 5, pp. 757–775, 2003.

[72] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, 1959.

[73] K. J. Hole, “On classes of convolutional codes that are not asymptotically catastrophic,” *IEEE Trans. Inform. Theory*, vol. 46, no. 2, pp. 663–669, 2000.

[74] M. Hsieh, I. Devetak, and T. Brun, “General entanglement-assisted quantum error-correcting codes,” 2006, arXiv:quant-ph-07082142v1.

[75] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes.* Cambridge: Cambridge University Press, 2003.

[76] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional coding.* Digital and Mobile Communication, New York: John Wiley, 1999.

[77] J. Justesen, E. Paaske, and M. Ballan, “Quasi-cyclic unit memory convolutional codes,” *IEEE Trans. Inform. Theory*, vol. 36, no. 3, pp. 540–547, 1990.

[78] G. Kabatiansky, E. Krouk, and S. Semenov, *Error Correcting Codes and Security for Data Networks.* New York: John Wiley, 2005.

[79] T. Kasami, S. Lin, and W. Wesley Peterson, “Polynomial codes,” *IEEE Trans. Inform. Theory*, vol. 14, pp. 807–814, 1968.

[80] J. Kempe, D. Bacon, D. Lidar, and K. Whaley, “Theory of decoherence-free, fault-tolerant, universal quantum computation,” *PRA*, vol. 63, p. 042307, 2001.

[81] A. Ketkar, A. Klappenecker, S. Kumar, and P. Sarvepalli, “Nonbinary stabilizer codes over finite fields,” *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4892 – 4914, 2006.

[82] J.-L. Kim, “New quantum-error-correcting codes from Hermitian self-orthogonal codes over GF(4),” in *Proc. of the Sixth Intl. Conference on Finite Fields and Applications.* Oaxaca, Mexico, Springer-Verlag, May 21-25, 2002, pp. 209–213.

[83] J.-L. Kim and J. Walker, "Nonbinary quantum error-correcting codes from algebraic curves," 2004, submitted to a special issue of Com^{2}MaC Conference on Association Schemes, Codes and Designs in Discrete Math.

[84] A. Kitaev, "Topological quantum codes and anyons," in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-first Century and the Millennium*, ser. Proc. Sympos. Appl. Math. Providence, RI: Amer. Math. Soc., 2002, vol. 58, pp. 267–272.

[85] A. Klappenecker and M. Rötteler, "Beyond stabilizer codes I: Nice error bases," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2392–2395, 2002.

[86] A. Klappenecker and P. Sarvepalli, "Clifford code constructions of operator quantum error correcting codes," 2006, arXiv:quant-ph/0604161.

[87] E. Knill, "Group representations, error bases and quantum codes," 1996, Los Alamos National Laboratory Report LAUR-96-2807.

[88] ——, "Fault-tolerant postselected quantum computation: Threshold analysis," *arXiv.org:quant-ph/0404104*, 2004.

[89] ——, "On protected realizations of quantum information," 2006, eprint: quant-ph/0603252.

[90] E. Knill and R. Laflamme, "A theory of quantum error–correcting codes," *Physical Review A*, vol. 55, no. 2, pp. 900–911, 1997.

[91] E. Knill, R. Laflamme, and W. Zurek, "Threshold accuracy for quantum computation," e-print quant-ph/9610011.

[92] J. J. Kong, "Classical and quantum convolutional codes: Design and implementation," Ph.D. dissertation, University of Minnesota, 2005.

[93] J. J. Kong and K. K. Parhi, "Quantum convolutional codes design and their encoder architectures," *in Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 1131 – 1135, 2004.

[94] S. Konyagin and I. Shparlinksi, *Character Sums with Exponential Functions and Their Applications.* Cambridge: Cambridge University Press, 1999.

[95] D. W. Kribs, R. Laflamme, and D. Poulin, "Unified and generalized approach to quantum error correction," *Phys. Rev. Lett.*, vol. 94, no. 180501, 2005.

[96] G. Lachaud, "The parameters of projective Reed-Muller codes," *Discret. Math.*, vol. 81, p. 217221, 1990.

[97] ——, "Projective Reed-Muller codes," *Coding Theory and Applications, Lecture Notes in Comput. Sci.*, vol. 311, pp. 125–129, Berlin-New York: Springer, 1988.

[98] G. Lachaud, I. Lucien, D. Mercier, and R. Rolland, "Group structure on projective spaces and cyclic codes over finite fields," *Finite Fields and Their Applications*, vol. 6, no. 2, pp. 119–129, 2000.

[99] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correction code," 1996. [Online]. Available: arXiv.org:quant-ph/9602019

[100] K. Lally, "Algebraic lower bounds on the free distance of convolutional codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2101–2110, 2006.

[101] L. Lee, "Short unit-memory byte-oriented binary convolutional codes having maximal free distance," *IEEE Trans. Inform. Theory*, vol. 22, no. 3, pp. 349–352, 1976.

[102] J. Leon, J. Masley, and V. Pless, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. 30, no. 5, pp. 709–714, 1984.

[103] V. Levenshtein, “Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces,” *IEEE Trans. Inform. Theory*, vol. 41, no. 5, pp. 1303–1321, 1995.

[104] R. Li and X. Li, “Binary construction of quantum codes of minimum distance three and four,” *IEEE Trans. Inform. Theory*, vol. 50, no. 6, pp. 1331–1336, 2004.

[105] D. Lidar, I. Chuang, and K. Whaley, “Decoherence-free subspaces for quantum-computation,” *Phys. Rev. Letters*, vol. 81, pp. 2594–2597, 1998.

[106] S. Lin and D. Costello, *Error Control Coding.* Letanon, IN: Pearson Prentice Hall, 2nd edition, 2004.

[107] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1977.

[108] J. Massey, D. Costello, and J. Justesen, “Polynomial weights and code constructions,” *IEEE Trans. Inform. Theory*, vol. 19, pp. 101–110, 1973.

[109] R. Matsumoto and T. Uyematsu, “Constructing quantum error correcting codes for p^m-state systems from classical error correcting codes,” *IEICE Trans. Fundamentals*, vol. E83-A, no. 10, pp. 1878–1883, 2000.

[110] R. McEliece, E. Rodemich, j. H. Rumsey, and L. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities,” *IEEE Trans. Inform. Theory*, vol. 23, no. 2, p. 157, 1977.

[111] M. Nielsen and I. Chang, *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 2000.

[112] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, no. 17, pp. 1 779 021–4, 2003.

[113] ——, "Quantum convolutional codes: Fundamentals," 2004, arXiv:quant-ph/0401134.

[114] H. Ollivier and J. P. Tillich, "Trellises for stabilizer codes: definition and uses," *Physical Review A*, vol. 74, no. 032304, 2006, quant-ph/0512041.

[115] H. Ollivier and J.-P. Tillich, "Interleaved serial concatenation of quantum convolutional codes: gate implementation and iterative error estimation algorithm," in *Proc. of the 26th Symposium on Information Theory in the Benelux*, Brussels, Belgium, 2005, p. 149.

[116] W. W. Peterson and W. J. Weldon Jr., *Error-correcting Codes.* Cambridge, MA: MIT Press, 1972.

[117] P. Piret, "On a class of alternating cyclic convolutional codes," *IEEE Trans. Inform. Theory*, vol. 21, no. 1, pp. 64–69, 1975.

[118] ——, "Structure and construction of cyclic convolutional codes," *IEEE Trans. Inform. Theory*, vol. 22, no. 2, pp. 147–155, 1976.

[119] ——, *Convolutional Codes: An Algebraic Approach.* Cambridge, MA: The MIT Press, 1988.

[120] ——, "A convolutional equivalent to Reed-Solomon codes," *Philips J. Res.*, vol. 43, pp. 441–458, 1988.

[121] D. Poulin, "Stabilizer formalism for operator quantum error correction," *Phys. Rev. Lett.*, vol. 95, no. 230504, 2005.

[122] J. Preskill, "Reliable quantum computers," in *Proc. Roy. Soc.*, vol. A 454, 1998, pp. 385–410.

[123] E. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[124] L. Ribes and P. Zalesskii, *Profinite Groups.* New York: Springer, 1st edition, 2000.

[125] C. Roos, "On the structure of convolutional and cyclic convolutional codes," *IEEE Trans. Inform. Theory*, vol. 25, no. 6, pp. 676–683, 1979.

[126] J. Rosenthal and R. Smarandache, "Maximum distance separable convolutional codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, pp. 15–32, 1999.

[127] ——, "Constructions of MDS-convolutional codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 5, pp. 2045–2049, 2001.

[128] J. Rosenthal and E. York, "BCH convolutional codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1833–1844, 1999.

[129] M. Rötteler, M. Grassl, and T. Beth, "On quantum MDS codes," in *Proc. 2004 IEEE Intl. Symposium on Information Theory*, Chicago, USA, 2004, p. 355.

[130] V. Roychowdhury and F. Vatan, *Lecture Notes in Computer Science.* New York: Springer, 1998, pp. 325–336.

[131] J. Rushanan, "Topics in integral matrices and abelian group codes," Ph.D. dissertation, California Institute of Technology, 1986.

[132] ——, "Duadic codes and difference sets," *J. Combin. Theory Ser. A*, vol. 57, pp. 254–261, 1991.

[133] P. K. Sarvepalli, S. A. Aly, and A. Klappenecker, "Nonbinary stabilizer codes," in *The Mathematics of Quantum Computation and Quantum Technology*, G. Chen, L. Kauffman, and S. Lomonaco, Eds. London: Taylor & Francis, 2007.

[134] P. K. Sarvepalli and A. Klappenecker, "Quantum Reed-Muller codes," in *Proc. 2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, 2005.

[135] D. Schlingemann, "Stabilizer codes can be realized as graph codes," *Quantum Inf. Comput.*, vol. 2, no. 4, pp. 307–323, 2002.

[136] A. Shabani and D. A. Lidar, "Theory of initialization-free decoherence-free subspaces and subsystems," *PRA*, vol. 72, p. 042303, 2005.

[137] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 2, pp. 2493–2496, 1995.

[138] ——, "Fault-tolerant quantum computation," in *Proc. 37th Ann. Symp. on the Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 1996, p. 56, quant-ph/9605011.

[139] I. Shparlinski, "On the dimension of BCH codes," *Problemy Peredachi Informatsii*, vol. 25, no. 1, pp. 77–80, 1988, (In Russian).

[140] M. H. Smid, *On Duadic Codes.* Dept. of Math., Univ. of Amsterdam: Amsterdam, the Netherlands, 1986.

[141] ——, "Duadic codes," *IEEE Trans. Inform. Theory*, vol. 3, pp. 432–433, 1987.

[142] A. B. Sorensen, "Projective Reed-Muller codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 6, pp. 1567–1576, 1991.

[143] A. M. Steane, "Multiple-particle interference and quantum error correction," in *Proc. Roy. Soc., London A*, vol. 452, 1996, pp. 2551–2577.

[144] ——, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, vol. 77, pp. 793–797, 1996.

[145] ——, "Enlargement of Calderbank-Shor-Steane codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.

[146] A. M. Steane and B. Ibinson, "Fault-tolerant logical gate networks for Calderbank-Shor-Steane codes," *Phys. Rev. A.*, vol. 72, no. 052335, 2005.

[147] H. Stichtenoth and C. Voß, "On the dimension of subfield subcodes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 90–93, 1990.

[148] ——, "Generalized Hamming weights of trace codes," *IEEE Trans. Inform. Theory*, vol. 40, no. 2, pp. 554–558, 1994.

[149] C. Thommesen and J. Justesen, "Bounds on distances and error exponents of unit-memory codes," *IEEE Trans. Inform. Theory*, vol. 29, no. 5, pp. 637–649, 1983.

[150] D.-W. Yue and G.-Z. Feng, "Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2625–2628, 2000.

[151] D.-W. Yue and Z.-M. Hu, "On the dimension and minimum distance of BCH codes over GF(q)," *Jour. of Electron.*, vol. 18, pp. 263–269, 1996, (In Chinese).

[152] P. Zanardi and M. Rasetti, "Noiseless quantum codes," *Phys. Rev. Lett.*, vol. 79, p. 3306, 1997.

VITA

Salah Abdelhamid Awad Aly Ahmed

salah@cs.tamu.edu

Education

- Ph.D. Computer Science, College of Engineering, Texas A&M University, TX, USA May 2008, Concentration: Quantum Computing and Error Control Codes.
- Master of Computer Science, DePaul University, Chicago, IL, USA June 2004, Concentration: Security, Multimedia and Computer Networks.
- Master of Science (M. Sc.), Faculty of Science, Cairo University, Egypt June 2002, Major: Computer Science and Mathematics.
- Bachelor of Science (B. Sc.), Faculty of Science, Mansoura University, Egypt June 1997, Double Major: Computer Science and Mathematics.

Research Interests

- Innovative algorithms and concepts of computing (quantum, biological, or classical computing), networking, information security and cryptography.
- Coding theory and network coding for data storage and transmission in wireless networks, bioinformatics, and history.

Selected Publications

My list of publications can be found on my website:
http://people.tamu.edu/∼salah/academia.html

- S. A. Aly and A. Klappenecker, Subsystem Code Constructions, IEEE International Symposium on Information Theory, ISIT08, Toronto, CA, submitted 2008.
- S. A. Aly, A. Klappenecker, P.K. Sarvepalli, On Quantum and Classical BCH Codes, IEEE Transaction on Information Theory, 53(3):1183–1188, 2007.
- S. A. Aly, and A. Klappenecker, P. K. Sarvepalli, Quantum Convolutional Codes Derived from Reed-Solomon and Reed-Muller Codes, IEEE International Symposium on Information Theory, Nice, France, June 24-29, 2007.

Address: 325 Harvey R. Bright Building, Dept. of Computer Science, TAMU, College Station, TX 77843-3112, USA.