UNSW
AUSTRALIA

Quantum Error Correction and Stabilizer Codes

Author:

Yixuan Xie

Supervisor:

Prof. Jinhong Yuan

A thesis submitted in fulfilment of the requirements

for the degree of Doctor of Philosophy

in the

School of Electrical Engineering and Telecommunications

The University of New South Wales, Australia

May 2016

"We cannot clone, perforce; instead, we split
Coherence to protect it from that wrong
That would destroy our valued quantum bit
And make our computation take too long.

Correct a flip and phase -that will suffice.
If in our code another error's bred,
We simply measure it, then God plays dice,
Collapsing it to X or Y or zed.

We start with noisy seven, nine, or five
And end with perfect one. To better spot
Those flaws we must avoid, we first must strive
To find which ones commute and which do not.

With group and eigenstate, we've learned to fix
Your quantum error with our quantum tricks."

'Quantum Error Correction Sonnet' - Daniel Gottesman

THE UNIVERSITY OF NEW SOUTH WALES, AUSTRALIA

Abstract

School of Electrical Engineering and Telecommunications

Doctor of Philosophy

Quantum Error Correction and Stabilizer Codes

by Yixuan Xie

Quantum error-correcting codes (QECCs) will be the ultimate enabler of future quantum computing and quantum information processing. Stabilizer codes are the most important class of QECCs since the first discovery of QECCs in the mid-1990s. In this thesis, we study the design of QECCs and provide several contributions to quantum stabilizer code constructions.

The first contribution is the design of families of quantum stabilizer codes using quadratic residues (QR) sets and difference sets. We study the distance property and dimension for the families of quantum stabilizer codes constructed from QR sets. We give three design criteria for constructing quantum stabilizer codes from difference sets. We show that using the subsets of difference sets can further improve the proposed code performance.

We then design families of quantum low-density parity-check (LDPC) codes from classical quasi-cyclic LDPC codes for large-scale quantum systems. The proposed quantum LDPC codes of quasi-cyclic structure and various code rates are constructed from a family of proto-graph LDPC codes based on the QR set and Latin square. We provide two constructions based on the adjunction and concatenation of a proto-matrix and one construction based on the unique transformation of a

proto-matrix. We derive the dimension of the proposed quantum LDPC codes and provide a lower bound for its minimum distance. The performance of the proposed quantum LDPC codes over quantum depolarizing channels with iterative sum-product decoding algorithms is illustrated. Furthermore, we propose a construction of quantum LDPC codes with rate at least 0.9 by performing tensor product operation between two non-binary parity-check matrices obtained from the idempotent polynomials of QR/NQR sets.

Next, we study quantum synchronizable codes that correct both quantum noise and block synchronization errors. We propose a general construction of quantum synchronizable codes with CSS structure from classical chain-containing cyclic codes, and derive a distance bound using rational function for the proposed quantum synchronizable codes.We design a class of quantum synchronizable codes from classical quadratic residue codes over binary field. We show that these codes are a subclass of the proposed chain-containing cyclic codes, and their code length and dimension are equal to Mersenne prime and one, respectively.

Lastly, inspired by the phenomenon of channel mismatch effect for classical LDPC codes, we investigate the effect of channel mismatch for quantum LDPC codes over quantum depolarizing channels. We show that the degraded performance due to the channel mismatch can be mitigated by introducing a weighted channel information into the iterative sum-product decoder.

Contents

Abstract iii

Contents v

List of Figures ix

List of Tables xi

Abbreviations xiii

Symbols xv

1 Introduction 1
- 1.1 Motivation . . . 1
- 1.2 A brief background . . . 2
- 1.3 Contribution and layout of the thesis . . . 7

2 Background on QEC and QECCs 15
- 2.1 Quantum information . . . 15
  - 2.1.1 Qubit . . . 15
  - 2.1.2 Unitary operators . . . 17
  - 2.1.3 Pauli group . . . 22
- 2.2 Quantum error correction . . . 23
  - 2.2.1 Overview . . . 23
  - 2.2.2 Basic strategy of QEC . . . 24
  - 2.2.3 Quantum bit-flip repetition code . . . 27
  - 2.2.4 Quantum phase-flip repetition code . . . 30
  - 2.2.5 Shor's 9-qubit error correction code . . . 32
- 2.3 Stabilizer formalism and stabilizer codes . . . 33
  - 2.3.1 Stabilizer group . . . 33
  - 2.3.2 Stabilizer codes . . . 34
  - 2.3.3 Logical operators . . . 37
  - 2.3.4 Examples of stabilizer codes . . . 38
    - 2.3.4.1 Three qubit bit-flip code . . . 38

2.3.4.2 The 5-qubit perfect code . . . 39
2.3.4.3 The 7-qubit Hamming code . . . 40
2.4 From quantum codes to classical code spaces . . . 41
2.4.1 Basic concepts and arithmetics over $\mathbb{F}_4$ . . . 41
2.4.2 Direct translation from classical H into quantum stabilizer generator . . . 43
2.4.3 Parity-check matrix for stabilizer code over $\mathbb{F}_2$ . . . 45

3 Quantum Block Codes 49
3.1 Classical linear block codes . . . 49
3.2 Construction of quantum codes . . . 52
3.2.1 Construction of QECCs over symplectic dual space . . . 52
3.2.2 Construction of QECC over Hermitian dual space . . . 53
3.2.3 Construction of QECC over Euclidean dual space . . . 53
3.3 Encoding of stabilizer codes . . . 54
3.3.1 CSS codes: encoding and error correction . . . 54
3.3.2 Encoding of general stabilizer codes . . . 56
3.4 Bounds for quantum codes . . . 58

4 Stabilizer Codes from Quadratic Residue Sets and Difference Sets 61
4.1 Type-I quantum stabilizer codes from QR sets . . . 61
4.1.1 Quadratic (non-) residue sets and idempotent polynomials . 62
4.1.2 Design of Type-I stabilizer codes of length $N = 4n - 1$ . . . 64
4.1.3 Design of Type-I stabilizer codes of length $N = 4n + 1$ . . . 67
4.1.4 Constructed codes . . . 74
4.2 Type-II quantum stabilizer codes from difference sets . . . 76
4.2.1 Preliminaries . . . 76
4.2.2 Proposed DSS code constructions . . . 78
4.2.3 Extension of DSS codes . . . 82
4.2.4 Codes performance . . . 82
4.3 Chapter summary . . . 83

5 Sparse-Graph Quantum LDPC Codes 87
5.1 Background on quantum LDPC codes . . . 88
5.1.1 Latin squares . . . 91
5.1.2 Proto-graph quasi-cyclic LDPC codes . . . 92
5.2 New constructions on quasi-cyclic quantum LDPC codes . . . 93
5.2.1 Proto-matrices of QCS codes . . . 94
5.2.2 Type-I-A QCS codes from QR set of prime p=4n-1 . . . 96
5.2.3 Type-I-B QCS codes from QR set of prime p=4n-1 . . . 97
5.2.4 Type-II QCS codes from QR set of size p = 4n+1 . . . 99
5.2.5 Lower bound on minimum distance of Type-II QCS codes . 101
5.2.6 Examples . . . 104
5.2.7 Constructed codes . . . 106
5.2.8 Simulation results and performance evaluation . . . 107

5.3 Quantum LDPC codes From Tensor Product of Parity-Check Matrices 113
5.3.1 Pre-lifting with idempotent polynomials . . . 113
5.3.2 Tensor product construction method . . . 116
5.3.3 Simulation results . . . 118
5.4 Chapter summary . . . 121

6 Quantum Synchronizable Codes 123
6.1 Quantum synchronizable code . . . 124
6.1.1 Encoding . . . 125
6.1.2 Synchronization recovery . . . 126
6.2 Chain - containing quantum synchronizable codes . . . 129
6.2.1 q-ary cyclic codes . . . 129
6.2.2 Chain-containing cyclic codes . . . 132
6.3 The minimum distance of CC-QSCs . . . 134
6.3.1 Known bounds . . . 135
6.3.2 Bounding minimum distance of cyclic codes using rational function . . . 135
6.3.3 Minimum distance of proposed QSC codes . . . 137
6.4 A class of QSCs from quadratic residue codes . . . 139
6.4.1 Dual-containing cyclic codes: $\mathcal{C}_2^{\perp} \subset \mathcal{C}_2$ . . . 139
6.4.2 Cyclic supercodes of $\mathcal{C}_2$ . . . 141
6.4.3 Maximum misalignment tolerance . . . 142
6.5 Chapter summary . . . 145

7 Channel Mismatch For Quantum LDPC Codes Over Depolarizing Channel 147
7.1 Behaviour of classical sum-product decoder . . . 148
7.2 Channel mismatch over quantum depolarizing channel . . . 150
7.2.1 Quantum channel models . . . 150
7.2.2 Quantum channel estimation . . . 152
7.2.3 Quantum decoding algorithm . . . 153
7.2.3.1 Tanner graph of QECCs . . . 153
7.2.3.2 Belief propagation decoding of QECCs . . . 154
7.2.4 Quantum LDPC codes over depolarizing channels . . . 156
7.2.5 Improved decoding of depolarizing channels . . . 158
7.3 Chapter summary . . . 160

8 Thesis Conclusion 163

A Appendix 169
A.1 Proof for Proposition 5.7 . . . 169

Bibliography **175**

List of Figures

2.1 Interaction between quantum state and environment. 26
2.2 Quantum error correction with ancilla qubits 27
2.3 Circuit for 3-qubit bit-flip repetition code. 28
2.4 Encoding circuit for the 3-qubit phase-flip repetition code. The Hadamard gates transform the computational basis into Hadamard basis for phase error correction. 31

3.1 Known quantum bounds. The curves are $\triangle$: Quantum Singleton bound (SB), $\square$: Quantum Hamming bound (HB), $\times$: Quantum Gilbert-Varshamov bound for general quantum code and $\bigtriangledown$: Quantum Gilbert-Varshamov bound for quantum CSS codes. 60

4.1 BLER (solid lines) and QBER (dash lines) performances of DSS codes listed in TABLE 4.4 and comparison with the $[[13, 7]]$ code in [95]. 85
4.2 BLER (solid lines) and QBER (dash lines) performances of DSS codes of block size $N = 398$ with different weights given in TABLE 4.5. 85

5.1 The parity-check matrix for $[[366, 185]$ quantum Type-II QCS code in Example 5.3. 105
5.2 BLER of Type-I-A QCS codes. 109
5.3 BLER of Type-I-B QCS codes. 109
5.4 BLER of Type-II QCS codes. 110
5.5 BLER of Type-I-B QCS codes with $v = 61$ and $n = 3, 5, 6, 8$. . . . 110
5.6 Performance comparison between Type-II QCS codes with $v = 79$ and $n = 3, 4, 7, 10$ and the quantum CSS codes Code-C-2^8 and Code-D-2^9 in [75]. Note that the BLER plotted here for Code-C-2^8 and Code-D-2^9 is a function of $f = 3f_m/2$, where f_m is the marginal probability used in [75], and the BLER for the entire CSS code is shown. 111
5.7 Code performance of the proposed proto-graph quantum LDPC codes. $\square : [[1651, 1551]], R^Q = 0.94$; $\bigtriangledown : [[1638, 1523]], R^Q = 0.93$. . . 120

7.1 Probability of block error as a function of estimated flip probability when the true flip probability is fixed. 149
7.2 Tanner graph for the 5-qubit code with stabilizer generator (2.40). . 154

7.3 Probability of block error as a function of estimated flip probability when the true flip probability is fixed. 157
7.4 Comparison of block error rate of Codes A and B. 161

List of Tables

2.1 Commutative operation of Pauli group $\mathcal{P}_1$. 22
2.2 Error recovery for three-qubit bit-flip code 39
2.3 $\mathbb{F}_4$ elements to Pauli operators 43

4.1 Stabilizer of $[[13, 1, 5]]$ quantum stabilizer code. 74
4.2 Type-I stabilizer codes of length $N = 4n + 1$ for $n \leq 25$. $d^{\dagger}$ is the minimum weight of operator $E \in \mathcal{S}$. Underlined numbers indicate that d_{min} meets the lower bound of the achievable minimum distance given in [91]. The number with brackets is the Perfect code in [13]. 75
4.3 Type-I stabilizer codes of length $N = 4n - 1$ for $n \leq 25$. $d^{\dagger}$ is the minimum weight of operator $E \in \mathcal{S}$. 75
4.4 Different block size quantum stabilizer codes constructed from our proposed method. 84
4.5 Subset $D' \subset D$ of different size for DSS codes of $N = 398$. 84

5.1 Constructed $[[kv, kv-\rho'(v-1)-1, d^Q]]$ Type-I-A, $[[2kv, 2kv-\rho'v+\rho'-1, d^Q]]$ Type-I-B and $[[kv, kv-\rho'v+\rho'-1, d^Q]]$ Type-II QCS codes. 107
5.2 Parameters of Type-II QCS codes with $v = 79$ and variable n. . . . 107
5.3 Parameters of Type-I-B QCS codes with $v = 61$ and variable n. . . 108

7.1 Optimal $\Delta\hat{f}$ for different f. 160

Abbreviations

BCH	**B**ose-**C**haudhuri-**H**ocquenghem
BIBD	**B**alanced **I**ncomplete **B**lock **D**esign
BLER	**Bl**ock **E**rror **R**ate
BSC	**B**inary **S**ymmetric **C**hannel
CSS	**C**alderbank-**S**hor-**S**teane
CPM	**C**irculant **P**ermutation **M**atrix
DSS	**D**ifference **S**et **S**tabilizer
EA	**E**ntanglement-**A**ssisted
LDGM	**L**ow-**D**ensity **G**enerator **M**atrix
LDPC	**L**ow-**D**ensity **P**arity-**C**heck
MSE	**M**ean **S**quare **E**rror
NQR	**N**on-**Q**uadratic **R**esidues
QBER	**Q**u**b**it **E**rror **R**ate
QC	**Q**uasi-**C**yclic
QCS	**Q**uasi-**C**yclic **S**tabilizer
QEC	**Q**uantum **E**rror **C**orrection
QECCs	**Q**uantum **E**rror-**C**orrecting **C**odes
QSC	**Q**uantum **S**ynchronizable **C** codes
QR	**Q**uadratic **R**esidues
RM	**R**eed-**M**uller
RS	**R**eed-**S**olomon
SIP	**S**ymplectic **I**nner **P**roduct
s. t.	**s**uch **t**hat
w. r. t.	**w**ith **r**espect **t**o

Symbols

$\mathbf{a} \circ \mathbf{b}$	Commutative operation between two vectors
$\langle \mathbf{a}, \mathbf{b} \rangle$	Hermitian inner product between two vectors
$\mathbf{a} \cdot \mathbf{b}$	Euclidean inner product between two vectors
$\otimes$	Tensor product
$\boxplus$	Adjunction operation
$\|*\rangle$	Column vector
$\langle *\|$	Row vector
$\|\psi\rangle$	A quantum state
$\dagger$	Hermitian transpose
$\forall$	For all
$\exists$	There exist
tr :	Trace mapping
Φ :	Pauli operator to binary $2N$-tuple
$I - gate$	Pauli I operator
$X - gate$	Pauli X operator
$Z - gate$	Pauli Z operator
$Y - gate$	Pauli Y operator
$CNOT$	Controlled-NOT gate
$\mathscr{H}$	Hadamard matrix of order 2
$[\ ]^T$	Transpose of a matrix
$\mathcal{C}$	Classical linear code
$\mathcal{C}^{\perp}$	Classical linear dual code of $\mathcal{C}$
$[n, k, d]$	A classical linear code

$[[N, K, d_{min}]]$	A quantum code
$\mathbb{C}$	Complex domain
$\mathbb{C}^N$	N-dimensional complex space
$\mathbb{Z}$	Integer domain
$\mathbb{Z}^+$	Positive integer domain
$\mathbb{F}_q$	Finite field of q elements
$\mathbb{F}_{q^r}$	Extension field of $\mathbb{F}_q$
$f(x)$	Univariate polynomial
$a(x) \mid b(x)$	$a(x)$ divides $b(x)$
$a(x) \nmid b(x)$	$a(x)$ can not divides $b(x)$
$\mathbb{F}_q[x]$	Polynomial ring over field $\mathbb{F}_q$
$\mathbb{F}_q[x]/\left(X^N - 1\right)$	Quotient ring
$dim(\mathcal{C})$	Dimension of a code
$Rank(H)$	Rank of a matrix
$\mathbb{I}_{p\times p}$	All-one matrix of size p
$\mathbb{I}_{diag(0),p\times p}$	All-one matrix with zero diagonal
I_v	Identity matrix of size v
$\mathcal{R}_{I_k}$	Reverse identity matrix of size k
P^v	Circulant permutation matrix of order v
$deg(f(x))$	Degree of a polynomial
$ord(f(x))$	Order of a polynomial
$min(*)$	Minimum
$max(*)$	Maximum
$\mathcal{Q}^{\mathcal{R}}$	Quadratic residue set
$\mathcal{Q}^{\mathcal{NR}}$	Quadratic non-residue set
$\mathbf{Z}_p^{\times}$	Multiplicative group of order p
$\mathcal{V}$	Vector space
$\mathcal{H}$	Hilbert space
$\mathcal{P}_N$	Pauli group of N qubits
$\mathcal{S}$	Stabilizer (or stabilizer group)
$\mathcal{M}$	Stabilizer generators

$\mathcal{C}_{\mathcal{S}}$	Quantum code space stabilized by $\mathcal{S}$
$\mathscr{M}_X(E)$	Error syndrome measured by Pauli X operators
$\mathscr{M}_Z(E)$	Error syndrome measured by Pauli Z operators
$\mathcal{N}(\mathcal{S})$	Normalizer of the stabilizer $\mathcal{S}$
$wt(\mathbf{v})$	Weight of a vector $\mathbf{v}$; number of nonzero positions
d_{min}	Minimum distance of a stabilizer code
$\Delta\hat{f}^{(f)}$	weighting factor as a function of f
$\Delta\hat{f}_{avg}$	average weighting factor

To my wife Bai. . .

Chapter 1

Introduction

1.1 Motivation

Quantum computing and quantum information processing are new interdisciplinary fields, which have recently attracted many researchers from physics, mathematics, and engineering. The power of quantum computers comes from their ability to use quantum mechanical principles such as superposition, measurement, and entanglement. Arguably, one of the most attractive features of quantum computing is that quantum algorithms are conjectured to solve a certain computational problems exponentially faster than any classical algorithm. For instance, Shor's factoring algorithm [1] and Grover's search algorithm in [2].

Unlike classical information, quantum information is represented by the states of quantum systems. Such a quantum system is affected by *decoherence effect* due to inevitable interaction between the quantum system and its environment. Hence, it is infeasible to perform quantum computation without a remediation of the decoherence that tends to destroy such a quantum system. Quantum error correction (QEC) is one of the foundation stones for quantum information processing. Similar to classical communication systems, quantum error-correcting codes (QECC) are essential for stabilizing and protecting fragile quantum systems against the undesirable effects of decoherence. Both classical error correction and QEC are

concerned with the fundamental problem of communications in the presence of noise. The challenge of performing QEC consists two parts: first, the physics of error processes and their reversal, and secondly the construction of a good quantum error-correcting code.

The aim of this thesis is to study quantum error correction and develop novel techniques for constructing quantum error-correcting codes. We specifically focus on the design of numerous quantum stabilizer codes of short, moderate and long lengths based on classical codes over the binary field.

1.2 A brief background

In 1995, inspired by the classical 3-bit repetition code, Shor conceived the first QECC, which had a code rate of $\frac{1}{9}$ [3]. The code was capable of correcting arbitrary quantum errors on a single qubit due to the remarkable finding of *error discretization*. This discovery not only dispelled the notion that conceiving QECCs was infeasible, but opens an interdisciplinary research area. The general theoretical frameworks that describe the requirements of good QECCs are well studied in [10] and [9]. Meanwhile, Steane proposed a simpler construction compared to the 9-qubit code, where only 7 qubits are required to protect a single qubit from general quantum errors [4, 5]. Finally, Bennett *et al.* [10] and Laflamme *et al.* [13] discovered the perfect 5 qubit code, which is the shortest quantum code that is capable of correcting any error on a single qubit. The word 'perfect' refers to the fact that this code achieves quantum Singleton bound [93] and quantum Hamming bound [14, 94], such that it does the same job as the 7-qubit and 9-qubit code with only 4 redundancy qubits. The following works in [6–8] showed that a class of quantum codes, namely *Calderbank-Shor-Steane (CSS) codes*, can be constructed from a pair of classical linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ that satisfy some orthogonal constraint. With the aid of CSS construction, the problem of finding good quantum codes was reduced to finding good *dual-containing* or *self-orthogonal* classical

codes. The 7-qubit code was a typical example of quantum codes constructed from the dual-containing $[7, 4, 3]_2$ Hamming code.

The construction of these classic short quantum codes mentioned above are non-systematic. That is, each code was described using a tensor product operation over a vector space of certain dimension, which is tedious when designing quantum codes with a large number of qubits. The remarkable *stabilizer formalism* generalized the design of quantum codes by wisely using the concepts of *group theory* with error operators represented by *Pauli group*. The theory of *stabilizer group* and *stabilizer codes* was formalized by Gottesman [14, 15], which yield many useful insights into the design of QECCs and permitted new codes to be developed from many classical perspectives, *e.g.,* classical linear codes over binary and quaternary fields [6–8, 14].

Compared with CSS construction, the stabilizer formalism defines a more general class of quantum codes by imposing a more relaxed orthogonal constraint upon the underlying classical codes. In other words, stabilizer codes constitute a wide range of quantum codes designed from various different classical codes, where the class of CSS codes can be considered as a subclass of stabilizer codes. The stabilizer formalism has undoubtedly provided a cornerstone for a wide range of different quantum codes developed in the literature. The class of algebraic structured quantum codes, such as quantum Bose-Chaudhuri-Hocquenghem (BCH) codes [8, 16–19], quantum Reed-Solomon (RS) codes [20] and quantum Reed-Muller (RM) codes [21], was investigated in the late 90s. Comparing between classical block codes and convolutional codes, convolutional codes can encode with higher efficiency and the encoding operation depends on current as well as a number of past information bits. Inspired by these features, Chau conceived the first quantum convolutional code [22] and generalized the classical Viterbi decoding algorithm into quantum settings [23]. Later, many works on quantum convolutional codes were proposed, for example, [24–26, 58, 59, 106, 107, 109]. The class of maximum-distance-separable (MDS) codes is an important class of codes, because they attain maximum minimum distances. Example of classical MDS codes are the well-known RS codes and extended RS codes, whereas the famous

$[[5,1,3]]$ [93] quantum code is the first quantum MDS code. The construction of quantum MDS codes have been exhaustively investigated in the literature, *e.g.,* [31, 44–50, 108]. After the famous $[[5,1,3]]$ code, Chau [44] constructed quantum codes with parameters $[[5,1,3]]$ based on the integers modulo n. Feng [45] presented quantum MDS codes with parameters $[[6,2,3]]_p$ and $[[7,3,3]]_p$, where p is an odd prime. Grassl *et al.* [50] constructed families of quantum codes with parameters $[[n, n-2d+2, d]]_q$, where $3 \leq n \leq q$ and $1 \leq d \leq n/2+1$, and $[[q^2-s, q^2-s-2d+2, d]]_q$, where $1 \leq d \leq q$ and $s = 0, 1$, by means of Euclidean and Hermitian self-orthogonal extended RS codes, respectively. They also have constructed other families of quantum MDS codes of length up to $q+1$ and some quantum MDS codes of length up to q^2+1, including code $[[6,2,3]]_p$ and $[[7,3,3]]_p$, for $p \geq 3$ [108]. Sarvepalli *et al.* [31] showed the existence of q-ary quantum MDS codes with parameters $[[q^2-q\alpha, q^2-q\alpha-2v-2, v+2]]_q$, where $0 \leq v \leq q-2$ and $0 \leq \alpha \leq q-v-1$, by means of classical generalized RM codes. Wang *et al.* [49] have constructed quantum MDS codes with parameters $[[n, n-2k, k+1]]_q$ where $n = q^2+1$ and $k = q; n = q^2-l, l \leq q-l-1$ and $0 \leq l \leq q-2; n = mq-l, k \leq m-1, 0 \leq l < m$ and $1 < m < q; n \leq q$ and $k \leq \lfloor n/2 \rfloor$, derived from generalized RS codes. Guardia [48] showed the existence of quantum MDS codes with parameters $[[q^2+1, q^2-2d+3, d]]_q$, where $q = 2^t, t \geq 1$ and $3 \leq d \leq q+1$ is an odd integer. Although so, there are still a lot of quantum MDS codes difficult to be constructed. It is a great challenge to construct new quantum MDS codes and a even more challenge to construct quantum MDS codes with relatively large minimum distance.

Further, many different coding techniques have also been adopted into the design of quantum stabilizer codes, for example, non-additive and non-binary quantum stabilizer codes [28–30, 32, 33], codeword stabilized quantum codes [27] and quantum synchronizable codes [140–142]. Note that not all classical codes are suitable for the design of quantum codes due to the requirement of orthogonality. A significant break through in this dilemma is the emergence of *entanglement-assisted quantum error-correcting codes* [78–81], which exploit pre-shared entanglement qubits between the transmitter and receiver such that the classical codes used

to construct entanglement assisted quantum codes do not necessarily have to be dual-containing or self-orthogonal. Later, this concept was extended to numerous code constructions, *e.g.,* [38, 82–85]. In the past decade, quantum Turbo codes [37, 38, 128, 129], quantum polar codes [111–114] as well as quantum low-density parity-check (LDPC) codes [39, 62–64] are popular codes that have been well-studied since classical LDPC and Polar codes are capacity achieving codes, and more importantly, there exists a practical iterative decoder for LDPC and Turbo codes.

MacKay *et. al.* [39] generalized the design of quantum LDPC codes based on the prior works in [60–62] for large-scale (a large number of qubits involved) quantum computation and information processing. They conjectured that good quantum LDPC codes with practical decoders could exist due to the fact that 1) the conventional sparse-graph LDPC codes [43, 51] are capacity achieving codes [52, 53], which ascertain both the sparseness of a code and an efficient decoding algorithm, and 2) decoding algorithms, such as the *sum-product* algorithm, can be practically implemented. The sparseness of the parity-check matrix of LDPC codes is of particular interest in the quantum domain due to a small number of interactions per qubit when performing an error correction procedure, and also makes quantum LDPC codes highly degenerate. The degeneracy of a quantum code is a striking feature, in that the code can be used to correct more errors than they can uniquely identify, *e.g.,* [34], which is impossible for a classical code.

The design of general quantum stabilizer codes from conventional LDPC codes is non-trivial. In particular, the design of conventional LDPC codes utilizing randomness [51, 54, 55] is not helpful in the design of quantum LDPC codes. To construct powerful quantum LDPC codes, many researchers dedicated their work in this direction and a wide range of different types of sparse-graph quantum LDPC codes has been proposed. The *bicycle* and *unicycle* codes with unavoidable cycles of length 4 proposed by Mackay *et. al.* [39] are typical examples of quantum LDPC codes from the family of classical dual-containing LDPC codes. Additionally, MacKay *et al.* proposed the class of Cayley graph-based quantum LDPC codes [40] whose minimum distance is lower bounded by a logarithmic function

of its code length. The class of Cayley graph-based quantum LDPC codes was further investigated by Couvreur *et al.* [41, 42]. Moreover, Lou *et al.* proposed the quantum LDPC codes of CSS structure from classical low-density generator matrix (LDGM) codes [76, 77]. However, these codes suffer from cycles of length 4. Hagiwara *et al.* conceived a class of quantum LDPC codes based on conventional *quasi-cyclic* (QC) LDPC codes [67]. Such a quantum LDPC code has girth of at least 6 by carefully designing the pair of QC-LDPC codes using algebraic combinatorics. Later, the class of quantum QC-LDPC codes was extended to the non-binary field [72, 74, 75] with higher decoding complexity, and further extended to the class of spatially-coupled quantum QC-LDPC codes [69, 73], which was capable of achieving a performance similar to a non-binary QC-LDPC code only when its code length was very large. Furthermore, many mathematical tools have also been used when designing quantum LDPC codes. For instance, the classes of quantum LDPC codes derived from finite geometries and Latin squares were proposed by Aly *et al.* [65, 66]. Djordjevic exploited the Balanced Incomplete Block Designs (BIBD) in [71]. The design of quantum stabilizer codes based on syndrome assignment by parity-check matrices is proposed in [70]. Notably, Camara *et al* [63, 64] were the first to conceive quantum LDPC codes from classical self-orthogonal quaternary LDPC codes, which means the proposed quantum codes are of non-CSS structure. Later, Tan *et al.* proposed a number of systematic constructions for self-orthogonal quantum LDPC codes [68], four of which were based on scrambling and rotation of circulant permutation matrices (CPMs), while one was derived from binary LDPC-convolutional codes.

However, most of the above mentioned constructions of quantum sparse-graph codes suffer from disappointingly small minimum distances, namely whenever they have non-vanishing rate and parity-check matrices with bounded row-weight, their minimum distance is either proved to be bounded, or unknown and with little hope for unboundedness. The point has been made several times that minimum distance is not everything, because there are complex decoding issues involved, whose behavior depends only in part on the minimum distance, and also because a poor asymptotic behavior may be acceptable when one limits oneself to practical

lengths. Nevertheless, very poor minimum distances will imply significant error floors. It has been proved [156] that a sufficient large growing minimum distance - for quantum LDPC codes - is enough to imply a non-zero decoding threshold. In other words, the code corrects almost all error patterns of weight up to a value linear in the block length. Finally, the minimum distance has been the most studied parameter of error-correcting codes and given that asymptotically good (dimension and minimum distance both linear in the blocklength) quantum LDPC codes are expected to exist, it is of great theoretical interest, and possibly also practical, to devise quantum LDPC codes with large, growing, minimum distance [154–157].

1.3 Contribution and layout of the thesis

In this thesis, two families of quantum stabilizer codes based on classical block codes are constructed, including small-scale; tens to hundreds of qubits, quantum stabilizer codes designed from quadratic residue (QR) sets and difference sets. For large-scale quantum systems, where hundreds to thousands of qubits are involved, novel constructions of quantum LDPC codes based on the classical Proto-graph LDPC codes and Latin square are proposed. These constructions employ various construction techniques, such as circulant concatenation, matrix transformations and tensor product operations, into the design of quantum LDPC codes of quasi-cyclic structure. Furthermore, a family of quantum synchronizable codes from classical nested cyclic codes is proposed. Such a family of quantum codes are capable of correcting both standard quantum errors and synchronization errors by making good use of the cyclic property of a classical cyclic code. Lastly, we investigate the channel mismatch effect for quantum LDPC codes decoded under iterative sum-product decoding algorithm over quantum depolarizing channels.

In the following, the structure and contribution of each chapter of the thesis is given. There are eight chapters in total, presenting the motivation for pursuing this thesis, reviews of the relevant literature and background, research results,

analysis of proposed quantum stabilizer codes and quantum LDPC codes, as well as the conclusion we reach through the research.

Chapter 1

This chapter starts with an exposition of the key impedance in quantum information processing, which is the motivation for the works presented in this thesis. A brief review of the history of quantum error correction and quantum error-correcting codes is followed by the perspective for the work involved.

Chapter 2

Chapter 2 provides fundamental background knowledge related to the materials presented in this thesis. It covers an introduction on quantum computation, quantum error correction, the relationship between quantum error-correcting codes and classical error-correcting codes, and most importantly, the stabilizer formalism and stabilizer codes. The materials in this chapter are well-studied in past decades and no new results provided.

Chapter 3

This chapter focuses on the perspective of designing quantum stabilizer codes from classical linear block codes. A brief overview of classical linear block codes is followed by the description of three dual spaces, such that different categories of classical codes can be used to construct quantum stabilizer codes. They are the Euclidean dual space, Hermitian dual space and the symplectic dual space. The encoding of CSS and general stabilizer codes, together with examples, and some known distance bounds for quantum stabilizer codes are given thereafter.

Chapter 4

In Chapter 4, we propose two types, Type-I and Type-II, quantum stabilizer codes using quadratic residue sets of prime modulus given by the form $p = 4n \pm 1$ and difference sets of parameters $(4n-1, 2n-1, n-1)$, where $n \in \mathbb{Z}^+$. The proposed Type-I stabilizer codes are of cyclic structure and

code length $N = p$. They are constructed based on multi-weight circulant matrix generated from *idempotent* polynomial, which is obtained from a quadratic residue set. The proposed Type-II quantum stabilizer codes from difference sets is named difference set stabilizer codes (DSS). We give three design criteria for constructing quantum stabilizer codes from difference sets, and illustrate the performance of the proposed DSS codes over quantum depolarizing channels with low-complexity majority-logic decoder. In addition, we show that the performance of proposed DSS codes can be further improved by constructing the stabilizer codes from subsets of a difference set rather than from a difference set itself.

Part of the work this chapter has been published in:

> [C3] Y. Xie, J. Yuan and R. Malaney, "Quantum Stabilizer Codes From Difference Sets," *IEEE Procs. on Inter. Symp. Info. Theory (ISIT)*, 2013.

Some of the key results are briefly listed here.

Contributions

- We prove that the dimension of the proposed stabilizer codes from QR sets is k when n is even with a prime $p = 4n - 1$, and 1 when n is odd with a prime $p = 4n + 1$.
- We prove that the minimum distance for stabilizer codes of length $N = 4n + 1$ is upper bounded by the size of QR set k.
- We show that the constructed Type-I stabilizer codes meet the distance bounds as shown in the literature.
- We show that the cyclic difference sets of parameters $(4n-1, 2n-1, n-1)$, where $n \geq 2$, can be generated by using a primitive element of a cyclic group.
- By using shifts (translates) of a difference set, we show that the resulting circulant permutation matrices are self-orthogonal matrices.

- We further show that if $2n-1$ can be factorized for some value of n, *i.e.*, the difference set contains subsets, the qubit error rate over quantum depolarizing channel can be further improved by constructing the codes using subsets of a difference set.

Chapter 5

The materials in Chapter 5 are related to the design of large quantum systems, which hundreds or thousands of qubits are involved. In particular, we give a novel design of quantum LDPC codes from a much smaller Tanner graph, namely the proto-graph. We then construct families of proto-graph quantum LDPC codes based on the prime QR sets used in Chapter 4 and Latin squares. We derive the minimum distance and dimension of the proposed quantum LDPC codes for various constructions. Finally, we show examples of the proposed quantum LDPC codes and illustrate their performance over quantum depolarizing channels with an iterative sum-product decoding algorithm. Furthermore, we extend the design of proto-graph quantum LDPC codes by introducing two additional constructions, namely *Construction A* and *Construction B*. The first construction relies on the method of lifting with a simpler pre-lifting method, whereas the second construction adopts the operation of *tensor product*. Such a operation is applied to two non-binary parity-check matrices that are derived from the idempotents of QR/NQR sets, so that the resulting quasi-cyclic LDPC codes are self-orthogonal w. r. t. the SIP.

The work in this chapter has been submitted:

[J1] Y. Xie, J. Yuan and Q. (Tyler) Sun, "Proto-graph Based Quantum LDPC codes From Quadratic Residue Sets," *IEEE Trans. Comm.*.

[C1] Y. Xie and J. Yuan, "Proto-graph Quantum LDPC Codes From Tensor Product of Parity-Check Matrices," *IEEE Procs. on GlobeCom Workshop*, 2015.

Some of the key results are briefly listed here.

Contributions

- We adopt the idea of proto-graph into the design of quantum LDPC. We show that for regular proto-graphs, the proto-matrix that representing a proto-graph is a non-orthogonal Latin square.
- We obtain a set of transformation matrices based on the transversal of these non-orthogonal Latin squares, so that by transforming the proto-matrix, the resulting QC-LDPC codes are always self-orthogonal w. r. t. the symplectic inner product (SIP) constraint.
- We provide three classes of quantum LDPC codes proposed from prime QR sets of $p = 4n \pm 1$, including Type-I-A and Type-I-B codes for $p = 4n - 1$ and Type-II codes for $p = 4n + 1$.
- We prove that the self-orthogonality between the pair of QC-LDPC codes is invariant w. r. t. the order of CPM for the proposed Type-I-B and Type-II codes, whereas for Type-I-A codes the order of CPMs must be equal to p.
- The minimum distance of the proposed Type-II codes is lower bounded by $2(\rho' + 1) - \max\{wt(\mathbf{a}|\mathbf{b})\}$, where ρ' is the minimum column weight of the underlying QC-LDPC codes, and $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_2^{2N}$ is an element in the symplectic dual space.
- The Tanner graph of the parity-check matrix of the underlying QC-LDPC codes for the proposed Type-II QCS codes contains only cycles of length six, whereas for both Type-I-A and Type-I-B QCS codes, the girth is four.
- By using QR sets of prime size with parameter $p = 4n \pm 1, n \geq 2$, and its associated *idempotent* polynomials, the proposed *Construction A* yields a $[[pv, pv - \rho, d_{min}]]$ proto-graph quantum LDPC code, where $\rho < pv$ and $v \in \mathbb{Z}^+$ is the order of the CPM.
- *Construction B* yields proto-graph quantum LDPC codes of parameters $[[p^2v, p^2v - \gamma(v-1) - 1, d_{min}]]$, where $\gamma \in \mathbb{Z}^+$ is the size of the extension field $\mathbb{F}_{2^\gamma}$ of binary field $\mathbb{F}_2$. Such a class of proto-graph quantum LDPC codes have a quantum code rate at least $R^Q > 0.9$.

Chapter 6

In Chapter 6, we study the concept of quantum synchronizable codes (QSC), which is a class of quantum stabilizer codes that correct not only the standard quantum noises, but also block misalignment errors. We construct a family of classical codes that is suitable for the design of quantum synchronizable codes of CSS structure based on classical chain-containing cyclic codes. We also provide a distance bound that is derived using rational functions for the proposed chain-containing cyclic codes.

This is a joint work with Dr Fujiwara from CalTech, USA. Part of the work has been published in the paper:

> [C2] Y. Xie, J. Yuan and Y. Fujiwara, "Quantum Synchronizable Codes From Quadratic Residue Codes and Their Supercodes," *IEEE Procs. on Info. Theory Workshop (ITW)*, 2014.
>
> [J2] Y. Xie and J. Yuan, "q-ary Chain-containing Quantum Synchronizable Codes" *IEEE. Trans. Comm. Lett.*, Vol. 20, No. 3, 414 – 417, 2016.

Some of the key results are briefly listed here.

Contributions

- We provide necessary condition for classical cyclic codes that are suitable for the constructions of QSCs.
- We derive the distance lower bound for the proposed QSC codes from supercodes/subcodes of the chain-containing cyclic codes.
- The class of QR codes is a subclass of the proposed chain-containing cyclic codes such that the constructed QSC codes from QR codes have dimension $K = 1$ and the maximum misalignment tolerance is equal to the code length N.

Chapter 7

Chapter 7 begins with discussion of an interesting channel mismatch effect for classical LDPC codes over a binary symmetric channel (BSC), where

the channel information is unknown to the decoder. We then investigate the channel mismatch effect for quantum LDPC codes under an iterative sum-product decoding algorithm over a quantum depolarizing channel. We demonstrate that the degraded performance due to channel mismatch can be suppressed by inserting a proper estimation of the channel as the input of a decoder. A brief overview of quantum sum-product decoding algorithm over the quantum depolarizing channels is also introduced.

Part of the work in this chapter has been published in:

> [C4] Y. Xie, J. Li, R. Malaney and J. Yuan, "Channel identification and its impact on quantum LDPC code performance," *IEEE Procs. on Aus. Comm. Theory Workshop (AusCTW)*, pp. 140 - 144, 2012.
>
> [C5] Y. Xie, J. Li, R. Malaney and J. Yuan, "Improved Quantum LDPC Decoding Strategies for the Misidentified Quantum Depolarization Channel," *IEEE Procs. on European Signal Processing Conference, 2016.*.

Some of the key results are briefly listed here.

Contributions

- We show that for quantum LDPC codes over a depolarizing channel, underestimated channel information causes severe performance loss compared to when the channel is overestimated.
- We introduce a weighting factor $\Delta\hat{f}$ that is added to the estimated value of a channel, so that the estimation of the channel information is an overestimation for high probability, which can be used as an input to the decoder to mitigate the effect of channel mismatch.
- We show that the proposed method of channel estimation can reduce the effect of channel mismatch up to 50% compared to the decoding scenario without the weighting factor.

Chapter 8

Chapter 8 concludes the thesis by summarizing the Ph.D research work. In

addition to the research results, a brief discussion on possible future work is also given.

Chapter 2

Background on QEC and QECCs

This chapter is a self-contained introduction on quantum information and quantum error correction. An adequate level of quantum mechanics is also provided as a prerequisite to understanding the concept of quantum error correction. A number of existing well-known quantum codes is shown at the end of the chapter. Readers who are interested in quantum mechanics are referred to standard textbooks such as [11, 12] or survey tutorials such as [9, 93, 138].

2.1 Quantum information

2.1.1 Qubit

Single qubit system : A fundamental unit of classical information is a *bit*. Each bit can only exist in one of the two distinct values 0 or 1. The choice of binary number naturally comes from classical logic of *true* or *false*, respectively. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, *qubit*. Unlike the classical bits, a qubit can exist in coherent *superposition* of its two states $|0\rangle$ and $|1\rangle$, where the notation '$|\,\rangle$' is called Ket [11], which is used to represent a quantum state. Mathematically, the notation represents a 2-dimensional column vector $|0\rangle = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $|1\rangle = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. An

arbitrary quantum state of an single qubit $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.1}$$

where $\{|0\rangle, |1\rangle\}$ is known as a set of *computational basis states* for a single qubit, and $|\psi\rangle$ is an *orthonormal* state because

$$\begin{aligned} &\langle 0|1\rangle = \langle 1|0\rangle = 0, \\ &|\alpha|^2 + |\beta|^2 = 1, \quad \alpha, \beta \in \mathbb{C}. \end{aligned} \tag{2.2}$$

The operation $\langle 0|1\rangle$ denotes the inner product between two states and the notation '$\langle\ |$' is called Bra, or a 2-dimensional row vector $\langle 0| = [\begin{smallmatrix}1\\0\end{smallmatrix}]^T$ and $\langle 1| = [\begin{smallmatrix}0\\1\end{smallmatrix}]^T$, equivalently. Thus, the state of a single qubit is a *unit vector* in a 2-dimensional complex vector space.

N-qubit system : For an N-qubit quantum system, the general orthonormal state $|\psi\rangle$ is expressed as

$$|\psi\rangle = \sum_{i=0}^{2^N-1} \alpha_i |\mathbf{v}_i\rangle, \tag{2.3}$$

where $\mathbf{v}_i \in \mathbb{F}_2^N$ is a binary N-tuple that runs over all binary strings of length N and $\sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1$. Since there are 2^N complex coefficients α_i, $|\psi\rangle$ is a unit vector in a 2^N-dimensional complex vector space and each computational state represented by $|\mathbf{v}_i\rangle$ is the shorthand for the N-fold *tensor product* ('$\otimes$') operation. *E.g.,* $|00\cdots0\rangle$ is the shorthand for $|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$. The state space $\{|\psi\rangle\}$ for N qubits is the *Hilbert space* denoted by $\mathcal{H} \simeq \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ with dimension 2^N.

Entangled states : Two qubits are said to be *entangled* if they cannot be expressed as a tensor product of the single qubit. For instance, the state

$$|\psi\rangle = \alpha|00\rangle + \beta|11\rangle,\ \alpha, \beta \in \mathbb{C},$$

is a typical example of entangled states. It is entangled since

$$\alpha|00\rangle + \beta|11\rangle \neq (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)\,,$$

where the right hand side expands into

$$\alpha_1\alpha_2|00\rangle + \beta_1\alpha_2|10\rangle + \alpha_1\beta_2|01\rangle + \beta_1\beta_2|11\rangle,$$

for any nonzero $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$ subject to normalization.

The set of entangled orthonormal states for two qubits are the Bell states [11],

$$\left\{ \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad \frac{|01\rangle - |10\rangle}{\sqrt{2}} \right\},$$

which is also referred to as the Einstein-Podolsky-Rosen (EPR) pairs.

2.1.2 Unitary operators

An *unitary operator* U is a linear operator that satisfies

$$U^\dagger U = I \quad \text{with} \quad U^{-1} = U^\dagger,$$

where $U^\dagger$ is the Hermitian transpose (or mathematically, the conjugate transpose) of U and I is the identity matrix. Moreover, a unitary transformation on a quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a linear operation that can be expressed as

$$U\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha U\left(|0\rangle\right) + \beta U\left(|1\rangle\right).$$

We shall see some typical examples of unitary operators for single qubit, two qubits and three qubits states.

1. **Quantum gates for single qubit**

The *Pauli matrices* $\{I, X, Z, Y\}$ (also known as the Pauli I, X, Y, Z-gate) form a basis of unitary operators acting on a single qubit, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

and the imaginary component $i = \sqrt{-1}$ is the phase of the operator. Each operator from left to right represents no action, bit-flip, phase-flip and a combination of both bit-flip and phase-flip on a single qubit. Note that $X^2 = Z^2 = Y^2 = I$ and $Y = iXZ$. Moreover, each Pauli operator is *unitary* since $X = X^\dagger$, $Z = Z^\dagger$ and $Y = Y^\dagger$, which implies $U^\dagger U = I$ for $U \in \{I, X, Z, Y\}$. The behaviour of each operator on a single qubit is shown in the following:

$$\begin{aligned}
&I(\alpha|0\rangle + \beta|1\rangle) \\
&= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \left(\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle, \\
&X(\alpha|0\rangle + \beta|1\rangle) \\
&= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \left(\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \alpha \begin{bmatrix} 0 \\ 1 \end{bmatrix} + \beta \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \alpha|1\rangle + \beta|0\rangle, \\
&Z(\alpha|0\rangle + \beta|1\rangle) \\
&= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \left(\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ -1 \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle, \\
&Y(\alpha|0\rangle + \beta|1\rangle) \\
&= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \left(\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \alpha \begin{bmatrix} 0 \\ i \end{bmatrix} + \beta \begin{bmatrix} -i \\ 0 \end{bmatrix} = i(\alpha|1\rangle - \beta|0\rangle).
\end{aligned} \tag{2.4}$$

From (2.4), we observe that an I operator has no effect to the qubit. A X operator flip the value between the computational basis $|0\rangle$ and $|1\rangle$, whereas a Z operator flip the sign of basis $|1\rangle$ but not $|0\rangle$. Finally, a Y operator does both to the qubit.

Another single qubit unitary operator is the *Hadamard gate*. It transforms a

basis $|0\rangle$ or $|1\rangle$ state into an orthonormal superposition state via the following transformation:

$$\mathscr{H}(|0\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \equiv \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{2.5}$$

and

$$\mathscr{H}(|1\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \equiv \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) . \tag{2.6}$$

The matrix $\mathscr{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is the Hadamard matrix of order 2. Note that, the Hadamard transformation is the key transformation to enable the correction of a phase-flip error (a Pauli Z operator) of a QECC. By transforming the computational basis $\{|0\rangle, |1\rangle\}$ into Hadamard basis $\{\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) , \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)\}$ via Hadamard transformations, the effect of a Z operator acting on Hadamard basis is equivalent to a X operator acting on the basis $\{|0\rangle, |1\rangle\}$. Thus, a Pauli Z operator behaves similarly as a Pauli X operator under different computational basis. We shall see more on this in the section of quantum error correction.

2. **Quantum gates for two qubits**

The analogues of a classical XOR gate is a *controlled-NOT gate* (CNOT), which is an unitary operator acting on two or more qubits. A CNOT gate flips the second qubit (the target qubit) if and only if the first qubit (the control qubit) is $|1\rangle$. The CNOT operation can be expressed as

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{2.7}$$

or equivalently $|a,b\rangle \xrightarrow{CNOT} |a, a \oplus b\rangle$, where '$\oplus$' is the binary addition. For example, $|00\rangle \xrightarrow{CNOT} |00\rangle, |01\rangle \xrightarrow{CNOT} |01\rangle, |10\rangle \xrightarrow{CNOT} |11\rangle, |11\rangle \xrightarrow{CNOT} |10\rangle$.

More generally, if U is an unitary operator on single qubits with matrix representation

$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix},$$

then the *controlled-U* gate operates on two qubits in such a way that the first qubit serves as a control, and only if the control qubit is $|1\rangle$, the transformation of the target qubit (the second qubit) based on U is performed. It maps the basis states as follows:

$$\begin{aligned}
&|00\rangle \xrightarrow{C(U)} |00\rangle, \\
&|01\rangle \xrightarrow{C(U)} |01\rangle, \\
&|10\rangle \xrightarrow{C(U)} |1\rangle U\left(|0\rangle\right) = |1\rangle\left(u_{11}|0\rangle + u_{21}|1\rangle\right), \\
&|11\rangle \xrightarrow{C(U)} |1\rangle U\left(|1\rangle\right) = |1\rangle\left(u_{12}|0\rangle + u_{22}|1\rangle\right).
\end{aligned}$$

When U is one of the Pauli operators $\{X, Y, Z\}$, the terms *controlled-X, controlled-Y* and *controlled-Z* are sometimes used. The matrix representation of $C(U)$ is

$$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}.$$

If $U = X$, then $C(U) = CNOT$, and it is the CNOT matrix in (2.7).

The *swap gate* is another type of unitary operators that swaps the position of two qubits w. r. t. the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. It is represented by

the matrix

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.8}$$

3. **Quantum gates for three qubits**

   The *Toffoli gate*, also known as the *controlled-CNOT* (CCNOT) gate, is a three-qubit gate. If the first two qubits are both in the state $|1\rangle$, it applies a Pauli X operator on the third. The equivalent matrix representation is

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

   Similarly, the *Fredkin gate*, also known as the *controlled-SWAP* (CSWAP) gate, is another three-qubit gate that swaps the position of the second and the third qubit if the first qubit is in the state $|1\rangle$. The equivalent matrix representation is

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

2.1.3 Pauli group

A Pauli operator on N qubits has the form $cO_1O_2\dots O_N$, where each $O_i \in \{I, X, Y, Z\}$ and $c = i^{\{0,1,2,3\}} \in \{\pm 1, \pm i\}$ is the overall phase of the operator. This operator takes an N-qubit state $|l_1 l_2 \cdots l_N\rangle$ to $cO_1|l_1\rangle \otimes O_2|l_2\rangle \otimes \cdots \otimes O_N|l_N\rangle$ according to (2.4). For instance, $XIZ(|000\rangle + |111\rangle) = X|0\rangle \otimes I|0\rangle \otimes Z|0\rangle + X|1\rangle \otimes I|1\rangle \otimes Z|1\rangle \equiv |100\rangle - |011\rangle$.

Furthermore, Pauli operators form a group together with the overall phase factor c. Let $\mathcal{P}_1 = \{\pm 1, \pm i\} \times \{I, X, Z, Y\}$ be the single qubit *Pauli group*. Then the N-fold tensor product of $\mathcal{P}_1$ forms an N-qubit Pauli group

$$\mathcal{P}_N = \{\pm 1, \pm i\} \times \{I, X, Z, Y\}^{\otimes N}. \tag{2.9}$$

The elements of $\mathcal{P}_N$ either *commute* or *anti-commute*. For any two operators $E, F \in \mathcal{P}_N$, define

$$E \circ F := \prod_{j=1}^{N} E_j \circ F_j, \tag{2.10}$$

where $E_j \circ F_j = +1$ if $E_j F_j = F_j E_j$ and $E_j \circ F_j = -1$ if $E_j F_j = -E_j F_j$. Hence, two Pauli operators either *commute* ($E \circ F = +1$) or *anti-commute* ($E \circ F = -1$). For $E, F \in \mathcal{P}_1$, this commutative operation is summarized in TABLE 2.1.

E\ F	I	X	Y	Z
I	+1	+1	+1	+1
X	+1	+1	-1	-1
Y	+1	-1	+1	-1
Z	+1	-1	-1	+1

TABLE 2.1: Commutative operation of Pauli group $\mathcal{P}_1$.

This property is particular important since it is the key to the quantum codes of stabilizer formalism, which we will introduce later.

2.2 Quantum error correction

2.2.1 Overview

Error-correction methods are widely used in communication systems. To communicate, a sender needs to send information to a receiver over a noise communication channel. The disturbance (or noises) of the channel can affect the information carried. To transmit information reliably in the presence of noise through a communication channel, the sender needs to *encode* the information by adding *redundancy digits* before the transmission. After transmission, the receiver *decodes* the information. Classically, the simplest way to add redundancy bits is to repeat the information bits, *e.g.,* $0 \rightarrow 000$ and $1 \rightarrow 111$, and transmit all the bits through a communication channel. By performing the majority rule at the receiver side, the transmitted information bits can be recovered reliably whenever the number of erroneous bits flipped by the noise is less than half of the length of the transmitted sequence. This is also known as the repetition code.

This principle of communication systems applies to the quantum systems as readily as to the classical setting. However, there are fundamental differences between quantum information processing and its classical counterpart because a quantum system can exist in the form of superposition state. The three important differences that require new ideas to be introduced to make such quantum error correcting codes possible are:

- **No-cloning theorem** [11] The no-cloning theorem states that it is impossible to duplicate a quantum state $|\psi\rangle$ to give $|\psi\rangle \otimes |\psi\rangle$. This can be shown in the following. If we assume that U is a linear transformation of replication, which maps the state

$$|\psi\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle. \tag{2.11}$$

Since U is linear, the following should hold:

$$(|\psi\rangle + |\theta\rangle) \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle + |\theta\rangle \otimes |\theta\rangle. \tag{2.12}$$

However, the right-hand side of the transformation does not equivalent to $(|\psi\rangle + |\theta\rangle) \otimes (|\psi\rangle + |\theta\rangle)$. Therefore, we can not replicate quantum state $|\varphi\rangle = |\psi\rangle + |\theta\rangle$ to obtain $|\varphi\rangle \otimes |\varphi\rangle$.

- **Quantum measurement destroys quantum information:** In quantum mechanics, measuring a quantum superposition state generally collapses the superposition property, or destroys the encoded quantum information. This means that we cannot examine a qubit to determine its quantum state, that is, the values of the complex coefficient α_i. For instance, when we measure the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we get either the result 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$.

- **Quantum bit (Qubit) errors are continuous:** Recall that a quantum superposition state of N qubits is often described by a vector space in a 2^N-dimensional Hilbert space. *Unitary errors* consist of a rotation of this vector and hence there exists a continuum of possible errors. In contrast, only bit-flip errors may occur for classical bits. These possible impairments have a continuous nature and the erroneous state may lie anywhere on the surface of the Bloch sphere [11].

2.2.2 Basic strategy of QEC

The discovery of the first quantum error-correcting codes was made by Shor [3] in 1995. He realized that quantum error-correction can be formulated as a digital process after all; measurement of the quantum syndrome *projects* the continuum of quantum error onto a *discrete* error basis. In another word, syndrome measurement digitizes the quantum error by measuring the discretized error basis without measuring the quantum state itself. By doing so the quantum information carried by the original state remains intact.

To explain in more detail, the process of digitization of quantum error is based on the observation of any interaction between a quantum system and an environment system. Consider the following interaction between a single qubit state formed by the basis $\{|0\rangle, |1\rangle\}$ and an environment $|e\rangle$:

$$|e\rangle|0\rangle \rightarrow |e_1\rangle|0\rangle + |e_2\rangle|1\rangle,$$
$$|e\rangle|1\rangle \rightarrow |e_3\rangle|0\rangle + |e_4\rangle|1\rangle,$$

where $|e\rangle$ is the initial state of the environment and $|e_i\rangle$ are states of the environment, not necessarily orthogonal or normalized. Then the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ interacting with $|e\rangle$ is

$$\begin{aligned} |e\rangle|\psi\rangle \rightarrow & \alpha\left(|e\rangle|0\rangle\right) + \beta\left(|e\rangle|1\rangle\right) \\ & \alpha\left(|e_1\rangle|0\rangle + |e_2\rangle|1\rangle\right) + \beta\left(|e_3\rangle|0\rangle + |e_4\rangle|1\rangle\right). \end{aligned} \tag{2.13}$$

We can write the Equation (2.13) in terms of different orthonormal states of single qubit, that is, in the terms of $\{\alpha|0\rangle + \beta|1\rangle, \alpha|0\rangle - \beta|1\rangle, \alpha|1\rangle + \beta|0\rangle, \alpha|1\rangle - \beta|0\rangle\}$. Then, the following equivalent expression can be obtained:

$$\begin{aligned} & \alpha\left(|e_1\rangle|0\rangle + |e_2\rangle|1\rangle\right) + \beta\left(|e_3\rangle|0\rangle + |e_4\rangle|1\rangle\right) \\ \equiv & \frac{1}{2}[(|e_1\rangle + |e_4\rangle)(\alpha|0\rangle + \beta|1\rangle) + (|e_1\rangle - |e_4\rangle)(\alpha|0\rangle - \beta|1\rangle) \\ & + (|e_2\rangle + |e_3\rangle)(\alpha|1\rangle + \beta|0\rangle) + (|e_2\rangle - |e_3\rangle)(\alpha|1\rangle - \beta|0\rangle)]. \end{aligned} \tag{2.14}$$

Note that each one of the orthonormal state is actually a unitary transformation of $|\psi\rangle$ under a Pauli operator given in (2.4). Hence,

$$\begin{aligned} |e\rangle|\psi\rangle \rightarrow & \alpha\left(|e_1\rangle|0\rangle + |e_2\rangle|1\rangle\right) + \beta\left(|e_3\rangle|0\rangle + |e_4\rangle|1\rangle\right) \\ \equiv & \frac{1}{2}[(|e_1\rangle + |e_4\rangle)I|\psi\rangle + (|e_1\rangle - |e_4\rangle)Z|\psi\rangle \\ & + (|e_2\rangle + |e_3\rangle)X|\psi\rangle + (|e_2\rangle - |e_3\rangle)(-i)Y|\psi\rangle]. \end{aligned} \tag{2.15}$$

As shown in Equation (2.15), the interaction between a quantum state and an environment can be discretized into a linear combination of the original state and

its transformations under Pauli operators X, Z and Y. Hence, the Pauli matrices form a complete set such that every possible transformation of the qubits can be described by the set $\{I, X, Y, Z\}$.

In a general quantum system, an arbitrary state $|\psi\rangle$ interacted with the environment $|e\rangle$, as shown in Figure 2.1, produce a superposition state

$$|e\rangle |\psi\rangle \rightarrow \sum_i |e_i\rangle (M_i |\psi\rangle) \tag{2.16}$$

as the outcome. Each error operator M_i is a tensor product of Pauli matrices acting on the system $|\psi\rangle$.

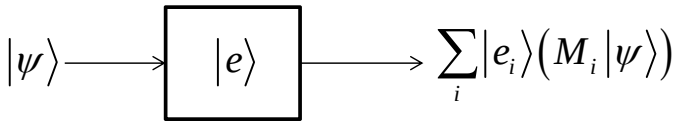

FIGURE 2.1: Interaction between quantum state and environment.

Error correction is a process which takes the erroneous state $M_i|\psi\rangle$ to $|\psi\rangle$. To see closely how quantum error correction is achieved, consider the noisy state

$$\sum_i |e_i\rangle (M_i |\psi\rangle) .$$

The error correction procedure works by introducing another system called *ancilla*, which is often initialized as the zero state $|0\rangle_a$. The unitary interaction between a quantum system, say $|\psi\rangle$, and $|0\rangle_a$, denoted as $\mathcal{A}$, is carefully designed to have the property

$$\mathcal{A} (|0\rangle_a M_i |\psi\rangle) = |\mathbf{s}_i\rangle_a (M_i |\psi\rangle) , \tag{2.17}$$

where $|\mathbf{s}_i\rangle_a$ of the ancilla state are orthonormal for all M_i. This interaction is known as *syndrome extraction*. The syndrome $\mathbf{s}_i$ contains information about the error that occurred. Furthermore, to prevent the destruction of encoded quantum information, the state of the ancilla $|\mathbf{s}_i\rangle_a$ depends only on the error, and not on the quantum state $|\psi\rangle$ itself. By applying $\mathcal{A}$ to the corrupted state on the right hand side of Equation (2.16), we obtain the result

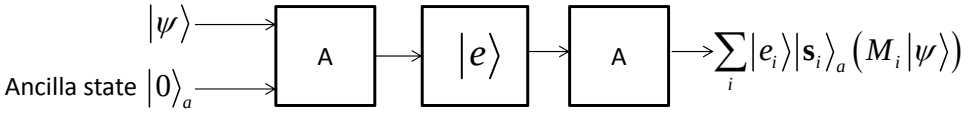

FIGURE 2.2: Quantum error correction with ancilla qubits

$$\mathcal{A}\left(|0\rangle_a \sum_i |e_i\rangle\, M_i\, |\psi\rangle\right) = \sum_i |e_i\rangle\, |\mathbf{s}_i\rangle_a\, (M_i\, |\psi\rangle) \tag{2.18}$$

as shown in Figure 2.2. Since the state $|\mathbf{s}_i\rangle_a$ is orthonormal, the superposition state is projected onto

$$\sum_i |e_i\rangle\, |\mathbf{s}_i\rangle_a\, (M_i\, |\psi\rangle) \rightarrow |e_i\rangle\, |\mathbf{s}_i\rangle_a\, M_i\, |\psi\rangle \tag{2.19}$$

if the basis $|\mathbf{s}_i\rangle_a$ is measured for some values of $\mathbf{s}_i$. Then the decoding process is to deduce M_i from $\mathbf{s}_i$, so that the recovery operation is simply apply M_i^{-1} to obtain the final corrected state $|e_i\rangle\, |\mathbf{s}_i\rangle_a\, |\psi\rangle$.

Note that, the state $|\psi\rangle$ has now been corrected, the state of the environment is of no importance and the ancilla state can be reused.

2.2.3 Quantum bit-flip repetition code

By making use of ancilla states wisely, the idea of the classical repetition code is applicable to quantum error correction. Consider the simplest quantum error correction method in Fig. 2.3. Suppose Alice wishes to transmit a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob through a channel which introduces bit-flip X errors randomly. To encode the state, Alice prepares two extra ancilla qubit $|0\rangle$ and obtains the state

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |00\rangle = \alpha|000\rangle + \beta|100\rangle$$

to encode her single qubit state. Followed by two CNOT operations on each of the extra qubits, the encoded state before passing through the single bit-flip error

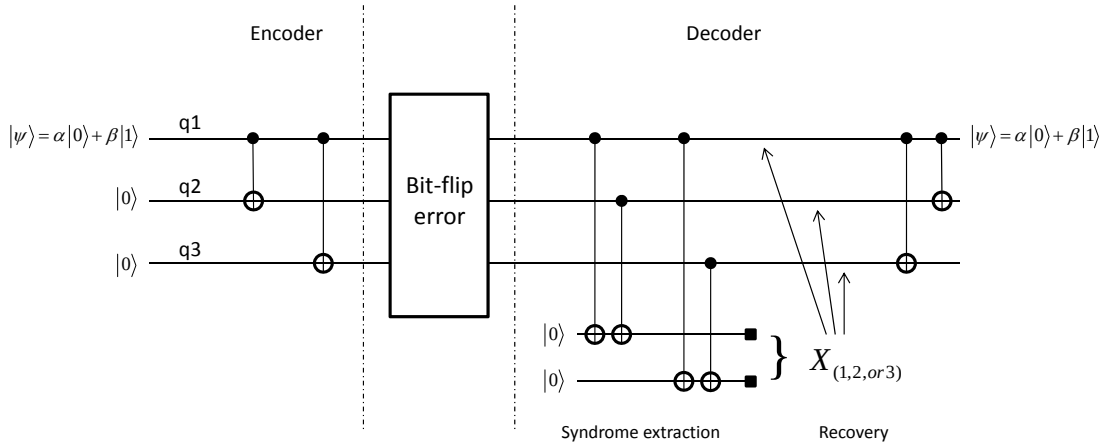

FIGURE 2.3: Circuit for 3-qubit bit-flip repetition code.

channel is

$$|\overline{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle.$$

Now we have generated a rate $\frac{1}{3}$ quantum repetition code.

If a bit-flip error occurred randomly and independently on each qubit with probability of ε, then Bob receives one of the following possible states:

$$\begin{array}{cc} \textit{State} & \textit{Probability} \\ \alpha|000\rangle + \beta|111\rangle & (1-\varepsilon)^3 \\ \alpha|100\rangle + \beta|011\rangle & \varepsilon(1-\varepsilon)^2 \\ \alpha|010\rangle + \beta|101\rangle & \varepsilon(1-\varepsilon)^2 \\ \alpha|001\rangle + \beta|110\rangle & \varepsilon(1-\varepsilon)^2 \\ \alpha|110\rangle + \beta|001\rangle & \varepsilon^2(1-\varepsilon) \\ \alpha|101\rangle + \beta|010\rangle & \varepsilon^2(1-\varepsilon) \\ \alpha|011\rangle + \beta|100\rangle & \varepsilon^2(1-\varepsilon) \\ \alpha|111\rangle + \beta|000\rangle & \varepsilon^3. \end{array} \tag{2.20}$$

To be able to detect and correct any bit-flip errors, Bob introduces two more ancilla qubits state $|00\rangle$. Bob uses the state to gather information about the error. He first carries out CNOT operations from the first and second received qubits to the first ancilla qubit, then from the first and third received qubits to the second

ancilla qubit. Thus, we obtain the total states of all five qubits as

$$\begin{array}{ll} \textit{State} & \textit{Probability} \\ (\alpha\,|000\rangle + \beta\,|111\rangle)\,|00\rangle & (1-\varepsilon)^3 \\ (\alpha\,|100\rangle + \beta\,|011\rangle)\,|11\rangle & \varepsilon(1-\varepsilon)^2 \\ (\alpha\,|010\rangle + \beta\,|101\rangle)\,|10\rangle & \varepsilon(1-\varepsilon)^2 \\ (\alpha\,|001\rangle + \beta\,|110\rangle)\,|01\rangle & \varepsilon(1-\varepsilon)^2 \\ (\alpha\,|110\rangle + \beta\,|001\rangle)\,|01\rangle & \varepsilon^2(1-\varepsilon) \\ (\alpha\,|101\rangle + \beta\,|010\rangle)\,|10\rangle & \varepsilon^2(1-\varepsilon) \\ (\alpha\,|011\rangle + \beta\,|100\rangle)\,|11\rangle & \varepsilon^2(1-\varepsilon) \\ (\alpha\,|111\rangle + \beta\,|000\rangle)\,|00\rangle & \varepsilon^3 \end{array} \tag{2.21}$$

Bob then measures the two ancilla qubits in the basis of $|0\rangle$ and $|1\rangle$. This gives him two classical bits of information. This information is called *error syndrome*, which helps to diagnose the error in the received qubits. For instance:

Syndrome	**Action**
00	*nothing*
01	$X \rightarrow 3^{rd} qubit$
10	$X \rightarrow 2^{nd} qubit$
11	$X \rightarrow 1^{st} qubit$

(2.22)

This is also the *recovery* stage as shown in the Fig. 2.3. Suppose that Bob's measurement gives '10'. By examining Equation (2.21), the state of the received qubits must be either $\alpha|010\rangle+\beta|101\rangle$ or $\alpha|101\rangle+\beta|010\rangle$ with probability of $\varepsilon(1-\varepsilon)^2$ and $\varepsilon^2(1-\varepsilon)$, respectively. Assume that $\varepsilon < 0.5$, state $\alpha|010\rangle + \beta|101\rangle$ is more likely to happen. Thus, Bob corrects the state by applying a Pauli X operator to the second qubit. This procedure corrects the bit-flip error since $X^2 = I$, and the original three qubit stated $\alpha|000\rangle + \beta|111\rangle$ is recovered from the corrupted state $\alpha|010\rangle + \beta|101\rangle$. Finally, to extract the single qubit state which Alice sent, Bob applies two CNOT operations from the first qubit to the second and third, obtaining the state $\alpha|0\rangle + \beta|1\rangle$. Hence, the decoding process has completed and Bob received the exact state sent by Alice. Note that, analogous to the classical

3-bit repetition code, the method above has a probability of success greater than $1-\varepsilon$ when $\varepsilon < 0.5$. On the other hand if $\varepsilon > 0.5$, state $\alpha|101\rangle + \beta|010\rangle$ will be most likely to happen, which will cause decoding error for Bob after applying X operator on the second qubit. Moreover, this example of correction is designed to succeed whenever either no qubit or just one is corrupted. The failure probability is the probability that at least two qubits are corrupted by the channel.

2.2.4 Quantum phase-flip repetition code

A 3-qubit phase-flip repetition code is slightly different from the 3-qubit bit-flip repetition code. The reason for this is because a Pauli Z operator will not alter the value between basis $|0\rangle$ and $|1\rangle$, instead, it only change the sign of $|1\rangle$. Therefore, as mentioned in the Section 2.1.2 of this chapter, a set of new basis is required in order to detect and correct a phase-flip error. These are the *Hadamard basis* obtained from the transformation of Hadamard gates. According to the transformations given in Equations (2.5) and (2.6), denote by

$$\begin{aligned} |+\rangle \equiv \mathscr{H}|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ |-\rangle \equiv \mathscr{H}|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned} \tag{2.23}$$

The transformation of a Pauli Z operator interchanges between Hadamard basis $|+\rangle$ and $|-\rangle$, that is,

$$\begin{aligned} Z|+\rangle = Z\left(\mathscr{H}|0\rangle\right) &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\ &= \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\ &\equiv \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle \right) \\ &= |-\rangle \end{aligned} \tag{2.24}$$

and vice and versa. Consequently, analogues to the 3-qubit bit-flip repetition code, a 3-qubit phase-flip repetition code encodes $|0\rangle$ and $|1\rangle$ via Hadamard basis as

$$\begin{aligned} |0\rangle \rightarrow |\bar{0}\rangle &= |+++\rangle, \\ |1\rangle \rightarrow |\bar{1}\rangle &= |---\rangle, \end{aligned} \tag{2.25}$$

to protect against the single qubit phase error. Consider the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the encoded state is

$$\begin{aligned} |\psi\rangle \rightarrow |\bar{\psi}\rangle &= \alpha|+++\rangle + \beta|---\rangle. \\ &= \frac{\alpha}{2\sqrt{2}}((|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)) \\ &+ \frac{\beta}{2\sqrt{2}}((|0\rangle - |1\rangle)(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)) \\ &= \frac{\alpha}{2\sqrt{2}}\left(\sum_i |\mathbf{v}_i\rangle\right) + \frac{\beta}{2\sqrt{2}}\left(\sum_i (-1)^{wt(\mathbf{v}_i)}|\mathbf{v}_i\rangle\right), \end{aligned} \tag{2.26}$$

where each $\mathbf{v}_i$ is a binary 3-tuple that runs over all binary strings of length 3, and $wt(\mathbf{v}_i)$ is the number of 1's. The encoding circuit of this state is depicted in Figure 2.4.

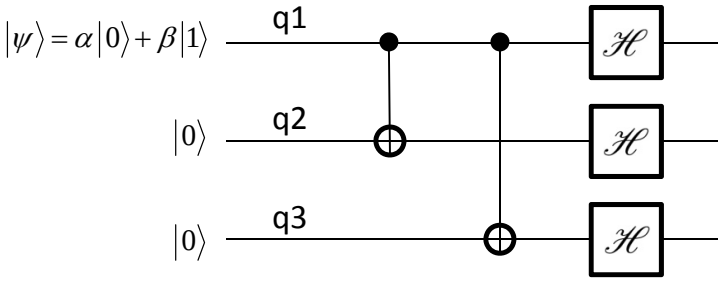

FIGURE 2.4: Encoding circuit for the 3-qubit phase-flip repetition code. The Hadamard gates transform the computational basis into Hadamard basis for phase error correction.

2.2.5 Shor's 9-qubit error correction code

The first quantum code able to correct both bit and phase flips was discovered in mid-90s by Shor [3]. It encodes a single qubit in 9 qubits. The encoded states are:

$$|\overline{0}\rangle = \left(\tfrac{1}{\sqrt{2}}\right)^3(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$|\overline{1}\rangle = \left(\tfrac{1}{\sqrt{2}}\right)^3(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle),$$

If we expand the above expression in full, we have

$$\begin{aligned}|\overline{0}\rangle = \left(\tfrac{1}{\sqrt{2}}\right)^3(&|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \\ &+ |111000000\rangle + |111000111\rangle + |11111000\rangle + |111111111\rangle), \\ |\overline{1}\rangle = \left(\tfrac{1}{\sqrt{2}}\right)^3(&|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \\ &- |111000000\rangle + |111000111\rangle + |111111000\rangle - |111111111\rangle),\end{aligned}$$

where $\frac{1}{2\sqrt{2}}$ is the coefficient of each computational basis such that $8 \times \left(\frac{1}{2\sqrt{2}}\right)^2 = 1$. Since Pauli X and Z are anti-commute (see TABLE 2.1), a single bit-flip in the first three qubits can be detected by using Pauli operators Z_1Z_2, Z_2Z_3 (a short-hand for $ZZIIIIIII$ and $IZZIIIIII$) to perform diagnostic operations on $|\overline{0}\rangle$ or $|\overline{1}\rangle$. Similarly, operators Z_4Z_5 and Z_5Z_6 detect a bit-flip error in the next three qubits, and operators Z_7Z_8 and Z_8Z_9 detect a bit-flip in the last three qubits. The phase error can be also detected by applying operators $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$. It can be verified easily that these eight operators $T = \{Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\}$ form a commuting set which can therefore be measured simultaneously. The outcome of the measurement is a 8-dimensional vector with elements from the set $\{+1, -1\}$ indicating whether each operator commutes with the erroneous state.

2.3 Stabilizer formalism and stabilizer codes

2.3.1 Stabilizer group

One important class of quantum error-correcting codes is *Stabilizer* codes [14, 15], sometimes known as *additive* quantum codes, whose construction is analogous to classical linear codes. Unlike Shor's 9-qubit code, where the code is described in the state vector description, the advantage of the stabilizer formalism is that quantum codes can be compactly described by working with the operators that stabilize them rather than by working with the state itself. For instance, consider the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.27}$$

and two operators X_1X_2 and Z_1Z_2. It is easy to verify that these two operators cause no effect on the state, that is, $X_1X_2|\psi\rangle = |\psi\rangle$, $Z_1Z_2|\psi\rangle = |\psi\rangle$. We say that the state $|\psi\rangle$ is *stabilized* by $\{X_1X_2, Z_1, Z_2\}$. Moreover, $|\psi\rangle$ is the unique quantum state which is stabilized by operators $\{X_1X_2, Z_1Z_2\}$.

The idea of stabilizer formalism lies in the use of *group theory*. Recall that $\mathcal{P}_N = \{\pm 1, \pm i\} \times \{I, X, Z, Y\}^{\otimes N}$ is a group closed under the operation of matrix multiplication. Denote by $\mathcal{S} \subset \mathcal{P}_N$ a subgroup of the N-qubit Pauli Group. Then we have the following definition of a *stabilizer*.

Definition 2.1. Let $\mathcal{V} = \{|\psi\rangle\}$ be a vector space of N-qubit states and $\mathcal{S} \subset \mathcal{P}_N$ be a subgroup of the N-qubit Pauli group. Then $\mathcal{V}$ is fixed by every element of $\mathcal{S}$, that is

$$S|\psi\rangle = |\psi\rangle, \forall S \in \mathcal{S}, |\psi\rangle \in \mathcal{V}. \tag{2.28}$$

Hence, $\mathcal{S}$ is the *stabilizer* of the vector space $\mathcal{V}$.

Furthermore, not all subgroups $\mathcal{S}$ of the N-qubit Pauli group can be used as a stabilizer for a non-trivial vector space $\mathcal{V}$. The two necessary conditions for a subgroup $\mathcal{S}$ to be able to be used as a stabilizer are 1) $\mathcal{S}$ is Abelian containing

only commuting elements and 2) $-I \notin \mathcal{S}$ since the only solution to $-I|\psi\rangle = |\psi\rangle$ is $|\psi\rangle = 0$, which is a trivial vector space. This is also true for condition 1) when $E, F \in \mathcal{S}$, if $EF = -FE$ we have $|\psi\rangle = EF|\psi\rangle = -FE|\psi\rangle = -|\psi\rangle$, which implies that $|\psi\rangle = 0$ for identity $|\psi\rangle = -|\psi\rangle$ holds. Thus, $\mathcal{V}$ a trivial vector space.

2.3.2 Stabilizer codes

The Abelian subgroup $\mathcal{S}$ may be compactly described by its *generators*. Denote by $\mathcal{M} = \{g_i | 1 \leq i \leq m\} \in \mathcal{P}_N$, a set of linearly independent Pauli operators such that $\mathcal{S} = \mathbf{span}\,(\mathcal{M})$, where each element of $\mathcal{S}$ can be expressed as a product of elements of $\mathcal{M}$.

Recall that a stabilizer group $\mathcal{S}$ is an Abelian subgroup of $\mathcal{P}_N$ such that a non-trivial subspace $\mathcal{C}_\mathcal{S} \subset \mathcal{H}$ is fixed (or stabilized) by $\mathcal{S}$. The subspace $\mathcal{C}_\mathcal{S}$ defines a quantum code space

$$\mathcal{C}_\mathcal{S} = \{|\psi\rangle \in \mathcal{H} \mid M|\psi\rangle = |\psi\rangle, \forall M \in \mathcal{S}\}.$$

If $\mathcal{S}$ is generated by $\mathcal{M} = \{g_1, g_2, \ldots, g_m\}$, where $\mathcal{M}$ is the $m = N-K$ independent stabilizer generators, then the code space $\mathcal{C}_\mathcal{S}$ encodes K logical qubits into N physical qubits and it is able to correct $t = \lfloor \frac{d_{min}-1}{2} \rfloor$ errors. This code $\mathcal{C}_\mathcal{S}$ is called an $[[N, K, d_{min}]]$ *quantum stabilizer code.*

The $N - K$ stabilizer generators may be regarded as the check operators of the code. The role is analogous to the rows of the parity-check matrix of a classical code. If the state is undamaged, the measurement outcome is $m_i = +1$. Conversely $m_i = -1$ if state is damaged. Then the state is orthogonal to the code space and an error has been detected. Thus, measuring the stabilizer generators allows the *error syndrome* to be determined.

Suppose an error acts on an N-qubit state. Any operator E_a either commute or anti-commute with a given stabilizer generator $g_i \in \mathcal{M}$. If $E_a \in \mathcal{P}_N$ commutes

with g_i, then

$$g_i E_a \left|\psi\right\rangle = E_a g_i \left|\psi\right\rangle = E_a \left|\psi\right\rangle \qquad \forall \left|\psi\right\rangle \in \mathcal{C}_\mathcal{S}, \tag{2.29}$$

so the operator E preserves the value of the measurement outcome, $m = +1$. However, if E and g_i anti-commute, then

$$g_i E_a \left|\psi\right\rangle = -E_a g_i \left|\psi\right\rangle = -E \left|\psi\right\rangle, \tag{2.30}$$

then $m = -1$. This indicates the error is detected by measuring the stabilizer generator g_i. In general, for stabilizer generator g_i and errors E_a, we may write

$$g_i E_a = (-1)^{s_i} E_a g_i \tag{2.31}$$

where $s_i \in \{+1, -1\}$, $i = 1, 2 \ldots, m$, constitute the syndrome for the error E_a as $(-1)^{s_i}$ will be the result of measuring g_i.

When correcting more than one errors E_a and E_b, one must make sure that $E_a|\psi\rangle$ is orthogonal to $E_b|\phi\rangle$, where $|\psi\rangle, |\phi\rangle \in \mathcal{C}_\mathcal{S}$. The sufficient and necessary conditions for error recovery are [10, 93],

$$\begin{aligned} &1) \quad \langle\psi|E_b^\dagger E_a|\phi\rangle = 0 \\ &2) \quad \langle\phi|E_b^\dagger E_a|\phi\rangle = \langle\psi|E_b^\dagger E_a|\psi\rangle, \end{aligned} \tag{2.32}$$

where † denotes conjugate transpose. In order to correct two errors, one must always be able to distinguish error E_a acting on one basis codeword $|\phi\rangle$ from error E_b acting on a different basis codeword $|\psi\rangle$. This is only true when $E_a|\phi\rangle$ is orthogonal to $E_b|\psi\rangle$ as shown in condition 1). The second condition requires that for each of the errors E_a, E_b, the following relationship applies

$$\langle\psi|E_b^\dagger E_a|\phi\rangle = \Delta_{ba}, \tag{2.33}$$

where $\Delta_{ba} = \langle a_b|a_a\rangle$ ($|a\rangle$ is the state of ancilla). This relation is satisfied provided that, for errors E_a and E_b, one of the following holds:

$$\begin{aligned} &(1) \quad E_b^\dagger E_a \in \mathcal{S}, \\ &(2) \quad \text{There is an } g \in \mathcal{M} \text{ that anti-commutes with } E_b^\dagger E_a. \end{aligned} \tag{2.34}$$

In (1) of (2.34), $\langle\psi|E_b^\dagger E_a|\psi\rangle = \langle\psi|\psi\rangle = 1$, for $|\psi\rangle \in \mathcal{C}_\mathcal{S}$. In (2) of (2.34), suppose $g \in S$ and $gE_b^\dagger E_a = -E_b^\dagger E_a g$, then

$$\langle\psi|E_b^\dagger E_a|\phi\rangle = \langle\psi|E_b^\dagger E_a g|\phi\rangle = -\langle\psi|gE_b^\dagger E_a|\phi\rangle = -\langle\psi|E_b^\dagger E_a|\phi\rangle \tag{2.35}$$

implies that $\langle\psi|E_b^\dagger E_a|\psi\rangle = 0$. In general, a stabilizer code corrects the error $E = \pm E_a E_b$ if either $E \in \mathcal{S}$ is an element of the stabilizer or anti-commute with some elements of $\mathcal{S}$ (see (2.34)). Recovery may fail if there is an $E_b^\dagger E_a$ that commutes with every element of the stabilizer but does not lie within the stabilizer itself. The reason that $E_b^\dagger E_a$ commutes with every element of the stabilizer is because $E_a|\psi\rangle$ and $E_b|\psi\rangle$ have exactly the same error syndrome. Consequently, if E_a error occurs, there is a risk that mistakenly interpret it as an E_b error.

Denote by $\mathbb{E} \subset \mathcal{P}_N$ a collection of Pauli operators. Then $\mathbb{E}$ is a set of correctable error operators for $\mathcal{C}_\mathcal{S}$ [7, 15] if

$$E^\dagger F \notin \mathcal{N}(\mathcal{S}) - \mathcal{S}, \ \ \forall E, F \in \mathcal{P}_N, \tag{2.36}$$

where $\mathcal{N}(\mathcal{S})$ is the *normalizer* of $\mathcal{S}$ in $\mathcal{P}_N$, which defined as the set of elements that fix $\mathcal{S}$ under conjugation, that is,

$$\mathcal{N}(\mathcal{S}) = \{A \in \mathcal{P}_N | A^\dagger M A \in \mathcal{S}, \forall M \in \mathcal{S}\}.$$

Note that $\mathcal{N}(\mathcal{S})$ is a collection of all operators in $\mathcal{P}_N$ that commutes with $\mathcal{S}$. Hence, $\mathcal{S} \subset \mathcal{N}(\mathcal{S})$. Then the minimum distance d_{min} of a stabilizer code is given by

$$d_{min} \triangleq min(wt(E)) \ \ \mathbf{s.t.} \ \ E \in \mathcal{N}(\mathcal{S}) - \mathcal{S}, \tag{2.37}$$

where the *weight*, $wt(E)$, of an operator is the number of non-identity positions. If the stabilizer group $\mathcal{S}$ contains element of weight less than d_{min}, then it is a *degenerate* quantum stabilizer code, otherwise, it is a *non-degenerate* quantum stabilizer code.

To correct errors of weight t or less, the particular error operator is determined based on error syndrome $\mathbf{s} = [s_1, s_2, \ldots, s_m] \in \{+1, -1\}$ after simultaneously measuring the set of stabilizer generators $\mathcal{M}$. For a non-degenerate stabilizer code, the error syndrome is unique defined for every correctable errors $E \in \mathbb{E}$, whereas for a degenerate stabilizer code, the error syndrome for different error is not unique.

2.3.3 Logical operators

Given a stabilizer $\mathcal{S}$ and its $m = N - K$ stabilizer generators $\mathcal{M}$, we can choose any one of the 2^K orthogonal vectors in the code space $\mathcal{C}_\mathcal{S}$ to act as our encoded logical states. Using *logical operators* is one method to choose such a state in a systematic way. Since all the elements of $\mathcal{N}(\mathcal{S})$ commute with $\mathcal{S}$ and $\mathcal{S} \subset \mathcal{N}(\mathcal{S})$ fixes $\mathcal{C}_\mathcal{S}$, elements of $\mathcal{N}(\mathcal{S}) - \mathcal{S}$ have non-trivial effect on $|\psi\rangle \in \mathcal{C}_\mathcal{S}$. Hence, the set $\mathcal{N}(\mathcal{S}) - \mathcal{S}$ have natural interpretation of encoded logical operators that act on the K encoded qubit in $\mathcal{C}_\mathcal{S}$. Consider the following example.

Example 2.1. *Consider the stabilizer group $\mathcal{S}$ is generated by two generators $g_1 = ZZI$ and $g_2 = ZIZ$. Then $\mathcal{S} = \{III, ZZI, ZIZ, IZZ\}$ and*

$$\mathcal{N}(\mathcal{S}) - \mathcal{S} = \{\pm 1, \pm i\} \times \{XXX, YYX, YXY, XYY, ZII, IZI, IIZ, ZZZ, YYY, XXY, XYX, YXX\}.$$

If we take two operators $\{XXX, ZII\}$, it can be easily verified that $\mathcal{N}(\mathcal{S}) - \mathcal{S} = (XXX)\mathcal{S} \cup (ZII)\mathcal{S} \cup (XXX)(ZII)\mathcal{S}$. Let $\mathcal{C}_\mathcal{S} = \{|\overline{0}\rangle = |000\rangle, |\overline{1}\rangle = |111\rangle\}$. Then we see that $XXX|\overline{0}\rangle = |\overline{1}\rangle$, $XXX|\overline{1}\rangle = |\overline{0}\rangle$ and $ZII|\overline{0}\rangle = |\overline{0}\rangle$, $ZII|\overline{1}\rangle = -|\overline{1}\rangle$.

In other words, XXX acts like an encoded X operator that flips the value between encoded qubits and ZII acts like an encoded Z operator that flips the sign of the encoded state $|\overline{1}\rangle$.

Denote by $\mathcal{N}(\mathcal{S})/\mathcal{S}$ the quotient group, where each element of $\mathcal{N}(\mathcal{S})$ can be expressed as RM where $M \in \mathcal{S}$ and $R \notin \mathcal{S}$. The group is equivalent to the Pauli group of size $K = N-m$ and can be generated by $2K$ equivalent classes of encoded logical X and logical Z operators $\{\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_K, \bar{Z}_1, \bar{Z}_2, \ldots, \bar{Z}_K\}$. It is worth noting that this logical operator set is non-unique as long as they satisfies

$$\begin{aligned} &\bar{X}_i \circ \bar{X}_j = +1, \\ &\bar{Z}_i \circ \bar{Z}_j = +1, \\ &\bar{X}_i \circ \bar{Z}_j = +1, \quad \text{for} \quad i \neq j, \\ &\bar{X}_i \circ \bar{Z}_j = -1, \quad \text{for} \quad i = j. \end{aligned} \tag{2.38}$$

2.3.4 Examples of stabilizer codes

2.3.4.1 Three qubit bit-flip code

This code is the same code shown in Example 2.1 with $\mathcal{C}_\mathcal{S} = \{|000\rangle, |111\rangle\}$, where a single qubit is encoded into a block of three according to

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\overline{\psi}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle\,,$$

and protect against single bit-flip error acting on any single qubit. The stabilizer for this code is generated by the two generators Z_1Z_2 and Z_2Z_3. Clearly, any error combination of two elements from the set $\{I, X_1, X_2, X_3\}$ anti-commutes with at least one of the stabilizer generators (For example, $X_1, X_2, X_3, X_1X_2, X_2X_3, X_1X_3$ are the possible errors). Therefore, the set$\{I, X_1, X_2, X_3\}$ forms a set of correctable error for the three qubit bit-flip code with stabilizer generators Z_1Z_2, Z_2Z_3. Error correction is performed by measuring the stabilizer generators and perform recovery operation based on the syndrome vector given in TABLE 2.2.

Qubit flipped	Z_1Z_2	Z_2Z_3	Recovery operation
None	+1	+1	no action
Qubit 1	-1	+1	Apply X_1
Qubit 2	-1	-1	Apply X_2
Qubit 3	+1	-1	Apply X_3

TABLE 2.2: Error recovery for three-qubit bit-flip code

2.3.4.2 The 5-qubit perfect code

The $[[5, 1, 3]]$ stabilizer code achieves the quantum Hamming bound [14] and proves that five is the minimum number of physical qubits needed to encode a single logical qubit. This code has the minimum distance of three, which achieves the quantum Singleton bound [13]

$$N - K \geq 2(d_{min} - 1). \tag{2.39}$$

Hence, it is named 'perfect' code [10, 13]. The generator of the stabilizer $\mathcal{S}$ is

$$\mathcal{M} = \begin{pmatrix} Z & Z & X & I & X \\ X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \end{pmatrix} \tag{2.40}$$

which can protect against any error of type X, Y, Z acting on a single qubit. This construction encodes one qubit into five qubits and has distance of three. Since $K = 1$, the two logical operators that generates the quotient group $\mathcal{N}(\mathcal{S})/\mathcal{S}$ are

$$\bar{X}_1 = XXXXX, \bar{Z}_1 = ZZZZZ.$$

The code space that contains 2^K basis codewords is denoted as $\mathcal{C}_\mathcal{S} = \{|\bar{0}\rangle, |\bar{1}\rangle\}$, where

$$\begin{aligned}|\bar{0}\rangle &= \sum_{M\in\mathcal{S}} M|00000\rangle \\ &= |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle \\ &\quad -|00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &\quad -|10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle,\end{aligned} \tag{2.41}$$

and

$$\begin{aligned}\left|\bar{1}\right\rangle &= \bar{X}_1\left|\bar{0}\right\rangle \\ &= |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle \\ &\quad -|11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ &\quad -|01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle,\end{aligned} \tag{2.42}$$

where the coefficient term $\frac{1}{\sqrt{2^{N-m}}} = \frac{1}{4}$ in front of every orthogonal basis is omitted.

2.3.4.3 The 7-qubit Hamming code

Steans's 7-qubit code [4] is constructed from the classical $\mathcal{C} = [7, 4, 3]_2$ Hamming code. The parity-check matrix of the Hamming code is

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{2.43}$$

The rows have an even number of 1's, and any two of them overlap by an even number of 1's, so $\mathcal{C}^{\perp} \in \mathcal{C}$. This is a typical example of designing quantum codes from dual-containing classical codes, which we will provide further explanation in the next chapter. Here, by replacing each nonzero element of H with a X operator and later on replace each nonzero element of H with a Z operator, we obtain 6

stabilizer generators

$$\mathcal{M} = \begin{pmatrix} I & I & I & X & X & X & X \\ I & X & X & I & I & X & X \\ X & I & X & I & X & I & X \\ I & I & I & Z & Z & Z & Z \\ I & Z & Z & I & I & Z & Z \\ Z & I & Z & I & Z & I & Z \end{pmatrix}. \tag{2.44}$$

Since $K = 7 - 6 = 1$, we can encode one qubit into seven qubits and the two codewords of this code can be expressed explicitly as

$$\begin{aligned} \left|\bar{0}\right\rangle &= \tfrac{1}{\sqrt{8}} \begin{pmatrix} |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \end{pmatrix} \\ \left|\bar{1}\right\rangle &= \tfrac{1}{\sqrt{8}} \begin{pmatrix} |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + \\ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \end{pmatrix} \end{aligned} \tag{2.45}$$

The encoded $|\bar{0}\rangle$ state is the superposition of the even codewords in the Hamming code and the encoded $|\bar{1}\rangle$ is the superposition of the odd codewords in the Hamming code. Since $K = 1$, the two logical operators that generates the quotient group $\mathcal{N}(\mathcal{S})/\mathcal{S}$ are

$$\bar{X}_1 = XXXIIII, \;\; \bar{Z}_1 = ZZZIIII. \tag{2.46}$$

2.4 From quantum codes to classical code spaces

2.4.1 Basic concepts and arithmetics over $\mathbb{F}_4$

To start with this section, it is important to get familiar with arithmetics in $\mathbb{F}_4$. For detailed explanations, readers are referred to standard textbooks, *e.g.,* [35, 56, 57, 99].

The addition and multiplication tables for the four elements $\{0, 1, \omega, \bar{\omega} = \omega^2\}$ over $\mathbb{F}_4$ are:

$+$	0	1	ω	$\bar{\omega}$
0	0	1	ω	$\bar{\omega}$
1	1	0	$\bar{\omega}$	ω
ω	ω	$\bar{\omega}$	0	1
$\bar{\omega}$	$\bar{\omega}$	ω	1	0

$\cdot$	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	ω	$\bar{\omega}$	1
$\bar{\omega}$	0	$\bar{\omega}$	1	ω

It is important to note that these additions and multiplications are not the rules of modulo-4 addition and multiplication in $\mathbb{F}_4$. For example $1+1 = \omega+\omega = \bar{\omega}+\bar{\omega} = 0$. In fact, the elements of $\mathbb{F}_4$ are expressed in a univariate *polynomials* over $\mathbb{F}_2$, that is, a polynomial of degree 1 with coefficients are elements of $\mathbb{F}_2$. *e.g.*,

$\mathbb{F}_4$ Elements	polynomial in $\mathbb{F}_{2^2}$	binary 2-tuple
0	0	00
1	1	01
ω	x	10
$\bar{\omega}$	$x+1$	11

(2.47)

These polynomials obey the addition and multiplication rules of $\mathbb{F}_4$ if addition and multiplication are modulo over the primitive polynomial $x^2 + x + 1$. For example, $\bar{\omega} \times \bar{\omega} = x^2 + (1+1)x + 1 = x + 1 + 2x + 1 = x = \omega$.

Furthermore, a direct mapping can be done between Pauli group $\mathcal{P}_1$ and the elements of Galois field $\mathbb{F}_4$ consisting of the elements $\{0, 1, \omega, \bar{\omega}\}$ (See TABLE 2.3). The addition of elements in $\mathbb{F}_4$ maps to the multiplication of elements of the $\mathcal{P}_1$ (up to a $\pm$ sign). For example, $\bar{\omega} + \omega = 1$ corresponds to $Y \cdot Z = X$, and $\bar{\omega} + 1 = \omega$ corresponds to $Y \cdot X = -Z$. However, the Pauli operators do not map perfectly onto the elements of $\mathbb{F}_4$, since there is no operation in $\mathcal{P}_1$ corresponding to the multiplication of elements in $\mathbb{F}_4$.

Denote by $\mathrm{tr} : \mathbb{F}_4 \to \mathbb{F}_2^2$ with $\mathrm{tr}(x) = x + \bar{x}$ for $x \in \mathbb{F}_4$, where $\bar{x} = x^2$ is the conjugate of x. Then the commutative relationship between Pauli operators in $\mathbb{F}_4$

$\mathbb{F}_4$	$\mathcal{P}_1$
0	I
1	X
ω	Z
$\bar{\omega}$	Y

TABLE 2.3: $\mathbb{F}_4$ elements to Pauli operators

is computed using the *trace inner product* defined as follows

$$\langle P_1, P_2 \rangle = \mathrm{tr}(P_1 \bar{P}_2) = 0, \tag{2.48}$$

where two elements $P_1, P_2 \in \mathbb{F}_4$ are commutative if their trace inner product is zero. The notation $\langle *, * \rangle$ represents the *Hermitian inner product* between two vectors, that is,

$$\langle \mathbf{z_1}, \mathbf{z_2} \rangle = \mathrm{tr}\left(\sum_i z_{1_i} \bar{z}_{2_i} \right).$$

Note that, since $x^2 + x + 1 = 0$ is a primitive polynomial of $\mathbb{F}_4$, $\mathrm{tr}(0) = \mathrm{tr}(1) = 0$ and $\mathrm{tr}(\omega) = \mathrm{tr}(\bar{\omega}) = 1$.

2.4.2 Direct translation from classical H into quantum stabilizer generator

It is tempting to link between the stabilizer generator and the rows of parity-check matrix H of a classical code, since their role is analogous in a certain way. However, it is not correct to translate directly from the rows of H into the stabilizer generators according to the mapping in (2.47) and TABLE 2.3. As mentioned before, there is no operation in the Pauli group equivalent to multiplication in $\mathbb{F}_4$. The rows of H span the dual space of the classical code over $\mathbb{F}_4$ since the code is linear, any vector in the dual space could be generated by summing together selected rows of H, each multiplied by an element ω of $\mathbb{F}_4$ (because any element of $\mathbb{F}_4$ may be written as $a + b\omega, a, b \in \{0, 1\}$). Therefore, in the N-qubit Pauli group, the above procedure corresponds to multiplying together not only the direct translations of the H, but also the translations of the H after each row has been

multiplied by ω in $\mathbb{F}_4$. The complete procedure for finding the stabilizer generators corresponding to a classical $\mathbb{F}_4$ code is:

1. Translate the rows of H from $\mathbb{F}_4$ to $\mathcal{P}_N$.
2. Translate the rows of ωH from $\mathbb{F}_4$ to $\mathcal{P}_N$.

For example, the perfect $[[5,1,3]]_2$ quantum code was derived from the classical $[5,3,3]_4$ Hamming code over $\mathbb{F}_4$ with parity check matrix

$$H = \begin{pmatrix} 1 & \omega & \omega & 1 & 0 \\ 0 & 1 & \omega & \omega & 1 \end{pmatrix}. \tag{2.49}$$

The corresponding quantum stabilizer could be obtained by first translating the rows of H according to Table 2.3, *i.e.,* we obtain two stabilizer generators $XZZXI$ and $IXZZX$. Then translate the rows of ωH:

$$\begin{aligned} \omega \begin{pmatrix} 1 & \omega & \omega & 1 & 0 \end{pmatrix} &= \begin{pmatrix} \omega & \bar{\omega} & \bar{\omega} & \omega & 0 \end{pmatrix} \Rightarrow ZYYZI \\ \omega \begin{pmatrix} 0 & 1 & \omega & \omega & 1 \end{pmatrix} &= \begin{pmatrix} 0 & \omega & \bar{\omega} & \bar{\omega} & \omega \end{pmatrix} \Rightarrow IZYYZ \end{aligned}$$

Therefore, the stabilizer generators for the $[[5,1,3]]_2$ perfect code derived from direct translation of H is given in part (a) of Equation (2.50).

$$\underset{(a)}{\mathcal{M} = \begin{pmatrix} X & Z & Z & X & I \\ I & X & Z & Z & X \\ Z & Y & Y & Z & I \\ I & Z & Y & Y & Z \end{pmatrix}} \qquad \underset{(b)}{\mathcal{M}_{alt} = \begin{pmatrix} Z & Z & X & I & X \\ X & Z & Z & X & I \\ I & X & Z & Z & X \\ X & I & X & Z & Z \end{pmatrix}} \tag{2.50}$$

Alternatively, the $[[5,1,3]]_2$ perfect code can be represented in terms of only I, X, Z, which is obtained by multiplying rows 3 and 4 of $\mathcal{M}$ with rows 2 and 1 of $\mathcal{M}$, respectively. In particular, the resulting generator $\mathcal{M}_{alt}$ is given in part (b) of (2.50) is cyclic.

2.4.3 Parity-check matrix for stabilizer code over $\mathbb{F}_2$

A general prescription is provided above for generating a quantum stabilizer code from a classical code over $\mathbb{F}_4$. Consequently, the classical $\mathbb{F}_4$ code is restricted to satisfy the two necessary criteria that all the stabilizer generators must commute with each other, and that each must square to the identity.

To examine closely, it is not difficult to observe that, since $Y = XZ$ if we ignore the phase factor i, any element E of the N-qubit Pauli group (up to a $\pm$ sign) can be expressed as a product of X's and Z's, *i.e.,*

$$E = X_E \cdot Z_E, \tag{2.51}$$

where Z_E and X_E are tensor product of Z's and X's, respectively. More precisely, a Pauli operator can be written as

$$(\mathbf{a}|\mathbf{b}) := X(\mathbf{a})Z(\mathbf{b}) = \bigotimes_{i=1}^{N} X^{a_i} \cdot \bigotimes_{i=1}^{N} Z^{b_i} \tag{2.52}$$

where $\mathbf{a}, \mathbf{b}$ are binary sequence of length N. We know that multiplication in Pauli group $\mathcal{P}_N$ is equivalent to binary addition. Thus, for two operators E and F of $\mathcal{P}_N$ represented by binary $2N$-tuples $(\mathbf{a}|\mathbf{b})$ and $(\mathbf{a}'|\mathbf{b}')$,

$$EF = (-1)^{\mathbf{a}'\cdot\mathbf{b}+\mathbf{b}'\cdot\mathbf{a}}(\mathbf{a}+\mathbf{a}'|\mathbf{b}+\mathbf{b}'), \tag{2.53}$$

where '+' is the binary addition and '$\cdot$' is the usual dot product. The phase factor $(-1)^{\mathbf{a}'\cdot\mathbf{b}+\mathbf{b}'\cdot\mathbf{a}}$ arises because it counts the number of times Z and X overlap. Since elements of a Pauli group commute or anti-commute, two Pauli operators commute *iff* the corresponding binary vectors are orthogonal with respect to the *symplectic inner product* defined as

$$(\mathbf{a}|\mathbf{b}) \circ (\mathbf{a}'|\mathbf{b}') := \mathbf{a}' \cdot \mathbf{b} + \mathbf{b}' \cdot \mathbf{a}. \tag{2.54}$$

Define the mapping $\Phi : \mathcal{P}_N \to \mathbb{F}_2^{2N}$. Then $\Phi(\mathcal{P}_1) = \{(0|0), (1|0), (0|1), (1|1)\}$. This implies that the binary $2N$-tuple $(\mathbf{a}|\mathbf{b})$ of an element $E \in \mathcal{P}_N$ can be obtained by

$$\Phi(E) = (\mathbf{a}|\mathbf{b}).$$

In this representation, $a_j = 1$ indicates a bit-error on qubit j, $b_j = 1$ indicates a phase error on qubit j, and both errors on the same qubit are represented by $a_j = b_j = 1$. For example,

$$\begin{aligned} E &= XYYZI \to \Phi(E) = (11100|01110), \\ F &= XYZYY \to \Phi(F) = (11011|01111). \end{aligned} \tag{2.55}$$

For a stabilizer group $\mathcal{S}$ generated from a set of independent stabilizer generators $\mathcal{M} = \{g_1, g_2, \ldots, g_m\}$, define the parity-check matrix H of $\mathcal{S}$ by representing each row of H as $\Phi(g_j)$ for $1 \leq j \leq m$ and $g_j \in \mathbf{g}$. Then the resulting H of size $m \times 2N$ is of the form $H = [H_1|H_2]$, where

$$H_1 = \begin{bmatrix} \mathbf{a}_{g_1} \\ \mathbf{a}_{g_2} \\ \vdots \\ \mathbf{a}_{g_m} \end{bmatrix} \text{ and } H_2 = \begin{bmatrix} \mathbf{b}_{g_1} \\ \mathbf{b}_{g_2} \\ \vdots \\ \mathbf{b}_{g_m} \end{bmatrix}.$$

Let $\mathbf{h}_i = (\mathbf{a}_{g_i}|\mathbf{b}_{g_i})$ and $\mathbf{h}_{i'} = (\mathbf{a}_{g_{i'}}|\mathbf{b}_{g_{i'}})$ be two rows of H, where $1 \leq i, i' \leq m$ and $i \neq i'$. Since any two elements of $\mathcal{S}$ must commute, $\mathbf{h}_i$ and $\mathbf{h}_{i'}$ must be orthogonal with respect to the twisted inner product given in (2.54). This implies that for m independent stabilizer generators to be commutative, the Symplectic Inner Product (SIP) must be satisfied:

$$H_1 H_2^T + H_2 H_1^T = \mathbf{0}^{m \times m} \pmod 2, \tag{2.56}$$

where $\mathbf{0}^{m \times m}$ is a zero matrix and 'T' denotes the transpose of a matrix. We call (2.56) the SIP constraint hereafter.

We now see the connection between a quantum stabilizer code over $\mathbb{F}_4$ and $\mathbb{F}_2$.

From (2.47), we know that any element in $\mathbb{F}_4$ can be expressed in the form $a+b\omega$. Therefore, the direct translation of the parity-check matrix H according to TABLE 2.3 can be expressed as

$$H = H_1 + \omega H_2.$$

The SIP constraint in this case between two rows $\mathbf{h}_i, \mathbf{h}_j \in H$, $i \neq j$, is given by

$$\begin{aligned}
\langle \mathbf{h}_i, \mathbf{h}_j \rangle &= \mathrm{tr}\left((\mathbf{h}_{i_1} + \omega \mathbf{h}_{i_2})(\mathbf{h}_{j_1} + \bar{\omega}\mathbf{h}_{j_2})\right) \\
&= \mathrm{tr}\left(\mathbf{h}_{i_1}\mathbf{h}_{j_1} + \omega \mathbf{h}_{i_2}\mathbf{h}_{j_1} + \bar{\omega}\mathbf{h}_{i_1}\mathbf{h}_{j_2} + \omega\bar{\omega}\mathbf{h}_{i_2}\mathbf{h}_{j_2}\right) \\
&= \mathrm{tr}\left(\mathbf{h}_{i_1}\mathbf{h}_{j_1}\right) + \mathrm{tr}\left(\omega \mathbf{h}_{i_2}\mathbf{h}_{j_1}\right) + \mathrm{tr}\left(\bar{\omega}\mathbf{h}_{i_1}\mathbf{h}_{j_2}\right) + \mathrm{tr}\left(\omega\bar{\omega}\mathbf{h}_{i_2}\mathbf{h}_{j_2}\right) \\
&= 0 + \mathbf{h}_{i_2}\mathbf{h}_{j_1} + \mathbf{h}_{i_1}\mathbf{h}_{j_2} + 0 \\
&= \mathbf{h}_{i_2}\mathbf{h}_{j_1} + \mathbf{h}_{i_1}\mathbf{h}_{j_2}
\end{aligned} \tag{2.57}$$

since $\mathrm{tr}(0) = \mathrm{tr}(1) = 0$, $\mathrm{tr}(\omega) = \mathrm{tr}(\bar{\omega}) = 1$ and $\omega\bar{\omega} = 1$. It can be seen that the symplectic inner product defined over $\mathbb{F}_2$ given in Equation (2.54) is equivalent to the one defined over $\mathbb{F}_4$ given in Equation (2.57).

Chapter 3

Quantum Block Codes

This chapter presents background materials and terminologies of classical linear block codes and constructions of stabilizer quantum block codes from classical codes. We show how stabilizer codes are related to classical linear codes. The central idea behind this relationship is the fact that whether an error is detectable is irrelevant to the phase information. This means the phase can be ignored after the mapping $\Phi : \mathcal{P}_N \to \mathbb{F}_q^{2n}$ defined in Section 2.4.3 and studying the image of stabilizer $\mathcal{S}$ and normalizer $\mathcal{N}(\mathcal{S})$. The encoding procedure of quantum Calderbank-Shor-Steane (CSS) and general stabilizer codes is also provided.

3.1 Classical linear block codes

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

$$\mathbb{F}_q^n[x] = \{f(x) \in \mathbb{F}_q[x] | deg\,(f(x)) < r\}, \tag{3.1}$$

where $f(x)$ is a polynomial of maximum degree r, and $\mathbb{F}_q[x]$ is a polynomial ring. If $r = 1$, then the field $\mathbb{F}_q$ has p integer elements $\{0, 1, \ldots, p-1\}$ with modulo p additions and multiplications. Detailed surveys of algebraic coding theory over finite fields can be found in [35, 56, 57]. Let $\alpha \in \mathbb{F}_q$ and $\alpha^{q-1} = 1$, then α is called

a *primitive element* in $\mathbb{F}_q$ and all the nonzero elements of $\mathbb{F}_q$ can be expressed in $q-1$ consecutive powers of the primitive element α, that is, $\mathbb{F}_q = \{\alpha^0 = 1, \alpha, \alpha^2 \ldots, \alpha^{q-1} = 1, \alpha^q = \alpha, \alpha^\infty = 0\}$.

Let $\mathbb{F}_q^n$ be a vector space with dimension n. A code $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$. A $[n, k]$ linear code, which encodes k information bits into n bits, is generated by a generator matrix G of size $k \times n$. Then the code space $\mathcal{C}$ is the span of its generator matrix G and is defined as

$$\mathcal{C} = \{\mathbf{m}G \mid \forall \mathbf{m} \in \mathbb{F}_q^k\}, \tag{3.2}$$

where $\mathbf{m} = (m_0, m_1 \cdots m_{k-1})$ is a vector of length k over $\mathbb{F}_q$ and $\mathcal{C}$ contains $|\mathcal{C}| = 2^k$ valid codewords. The *weight* of a codeword $\mathbf{u} \in \mathcal{C}$, $wt(\mathbf{u})$, is the number of nonzero positions in $\mathbf{u}$. The *Hamming distance* between two codewords $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ is the number of positions in which $\mathbf{u}$ and $\mathbf{v}$ differ

$$d(\mathbf{u}, \mathbf{v}) = |\{i \mid 0 \leq i \leq n-1, u_i \neq v_i\}| = wt(\mathbf{u} - \mathbf{v}). \tag{3.3}$$

Then the minimum Hamming distance of a linear code $\mathcal{C} \in \mathbb{F}_q^n$ is the minimum weight of a nonzero codeword in $\mathcal{C}$. That is $d(\mathcal{C}) = min(wt(\mathbf{u}))$ for $\mathbf{u} \in \mathcal{C}$ and $\mathbf{u} \neq 0$. Given the minimum distance d of a code $\mathcal{C}$, the maximum number of errors t that can be corrected by $\mathcal{C}$ is

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor, \tag{3.4}$$

which is often used to measure the performance of a code; the higher the minimum distance d, the better ability to correct errors.

Since $\mathcal{C}$ has dimension k, size of 2^k, then there also exists a dual space $\mathcal{C}^\perp \subset \mathbb{F}_q^n$ of $\mathcal{C}$ defined as

$$\mathcal{C}^\perp = \{\mathbf{v} \mid \mathbf{v} \in \mathbb{F}_q^n, \mathbf{v} \cdot \mathbf{u} = 0 \; \forall \mathbf{u} \in \mathcal{C}\}, \tag{3.5}$$

where $\mathbf{v} \cdot \mathbf{u}$ is the usual Euclidean inner product $\mathbf{v} \cdot \mathbf{u} = \sum_{i=0}^{n-1} v_i u_i$ between two vectors in $\mathbb{F}_q$. It is generally said that $\mathbf{u}$ is orthogonal to $\mathbf{v}$ if their Euclidean inner product is zero. The dual space $\mathcal{C}^\perp$ is the span of a $(n-k) \times n$ matrix H such that

$$GH^T = 0. \tag{3.6}$$

The matrix H is called the *parity check matrix* of $\mathcal{C}$ and is used to verify whether a vector of length n is valid codeword. A vector $\mathbf{u}$ is a valid codeword in $\mathcal{C}$ if and only if $H\mathbf{u}^T = 0$. Assume $\mathbf{u} \in \mathcal{C}$ is sent over a noisy communication channel. If the received vector $\mathbf{r} = \mathbf{u} + \mathbf{e}$, where $\mathbf{e}$ is the added noise introduced by the channel, we can extract information about the noise from $\mathbf{r}$ by performing error detection using H, that is,

$$\mathbf{s} = \mathbf{r}H^T = (\mathbf{u} + \mathbf{e})H^T = \mathbf{e}H^T. \tag{3.7}$$

The syndrome vector $\mathbf{s}$ then can be used to decode the error $\mathbf{e}$ from $\mathbf{r}$ to obtain the correct codeword $\mathbf{u}$. However, there is a possibility that $\mathbf{e}H^T \in \mathcal{C}$ is also a valid codeword, then vector $\mathbf{e}$ is undetectable, which causes a decoding error.

If $[n, k, d]_q$ denotes the set of parameters of a code $\mathcal{C}$ over $\mathbb{F}_q$, then $[n, n-k, d^\perp]_q$ denotes the set of parameters of the dual code $\mathcal{C}^\perp$. Through out the entire thesis, we denote a quantum stabilizer code in Section 2.3.2 using double brackets [[ ]], and single brackets [ ] for a classical linear code to distinguish between quantum codes and classical codes.

If $\mathcal{C}^\perp \subseteq \mathcal{C}$, then the code is *dual-containing* (sometimes it is also known as *weakly self-dual* codes). It means that codewords in $\mathcal{C}^\perp$ are also in $\mathcal{C}$. Hence, $\mathcal{C}^\perp$ is a subspace of $\mathcal{C}$. If $\mathcal{C} \subseteq \mathcal{C}^\perp$, then $\mathcal{C}$ is called *self-orthogonal*. If $\mathcal{C}^\perp = \mathcal{C}$, the code is called *self-dual*. Self-orthogonal and dual-containing codes are important to the derivation of quantum stabilizer codes, and highly related to our work in the later part of this thesis. Self-dual linear codes are also good potential candidates for designing quantum codes, *e.g.,* [39].

3.2 Construction of quantum codes

There have been numerous families of classical codes. The most notable are the Bose-Chaudhuri-Hocquenghem (BCH) code, the Reed-Solomon (RS) code, the Reed-Muller (RM) code, algebraic and projective geometry codes. Modern codes such as Turbo codes and low-density parity-check codes have also been well studied. Notably, in order to design quantum stabilizer codes from these classical codes, one must ensure that the underlying classical codes satisfy certain orthogonal constraints.

For completeness, we recall some general constructions of QECCs from classical codes for q-dimensional quantum digits, *qudits*, where q is an arbitrary prime power. A 2-dimensional quantum digit is called qubit.

3.2.1 Construction of QECCs over symplectic dual space

The symplectic inner product (SIP) defined in Equation (2.54) is generalized on the space $(\mathbb{F}_q \times \mathbb{F}_q)^n \equiv \mathbb{F}_q^n \times \mathbb{F}_q^n$ as

$$(\mathbf{v}, \mathbf{w}) * (\mathbf{v}', \mathbf{w}') := \mathbf{v} \cdot \mathbf{w}' - \mathbf{v}' \cdot \mathbf{w} = \sum_{i=0}^{n-1} v_i w_i' - v_i' w_i. \tag{3.8}$$

The subtraction operation is equivalent to addition when $q = 2$ as given in (2.54) for binary vectors. The dual code of a code $\mathcal{C}$ over $\mathbb{F}_q \times \mathbb{F}_q$ w. r. t. (3.8) is

$$\mathcal{C}^* := \{(\mathbf{v}, \mathbf{w}) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \mid \forall \mathbf{c} \in \mathcal{C} \ : \ (\mathbf{v}, \mathbf{w}) * \mathbf{c} = 0\}. \tag{3.9}$$

Theorem 3.1. *[108] (QECCs from Symplectic dual) For $\mathcal{C} = [n, k]_q$ and $\mathcal{C}^* = [n, n-k]_q$ over $\mathbb{F}_q \times \mathbb{F}_q$. If $\mathcal{C} \subseteq \mathcal{C}^*$, then there exists a $[[N, K, d_{min}]]_q$ QECC encoding $K = n - k$ qudits into $N = n$ qudits with minimum distance $d_{min} = min\{wt(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}^* \backslash \mathcal{C}\}$.*

3.2.2 Construction of QECC over Hermitian dual space

Next, consider a classical linear code over $\mathbb{F}_{q^2}$. The inner product on space $\mathbb{F}_{q^2}^n$ is the *Hermitian inner product* defined by

$$\mathbf{v} * \mathbf{w} := \sum_{i=0}^{n-1} v_i w_i^q. \tag{3.10}$$

Again, classical codes over $\mathbb{F}_{q^2}$ which are self-orthogonal w. r. t. (3.10) give rise to QECCs.

Theorem 3.2. *[108] (QECC from Hermitian dual) Let $\mathcal{C} \subset \mathbb{F}_{q^2}^n$ be a linear $[n,k]_q$ self-orthogonal code over $\mathbb{F}_{q^2}$. Then there exists a $[[N,K,d_{min}]]_q = [[n, n-2k, d_{min}]]_q$ QECC, where $d_{min} = min\{wt(\mathbf{v}) \mid \mathbf{v} \in \mathcal{C}^* \backslash \mathcal{C}\}$.*

Proof. The proof can be found in ([108]). □

3.2.3 Construction of QECC over Euclidean dual space

Finally, the construction of the so-called *Calderbank-Shor-Steane* (CSS) codes [4–6] uses the notion of duality w. r. t. the *Euclidean inner product*

$$\mathbf{v} \cdot \mathbf{w} = \sum_{i=0}^{n-1} v_i w_i, \tag{3.11}$$

for which the dual code is denoted by $\mathcal{C}^\perp$.

Theorem 3.3. *[11] (QECC from Euclidean dual (CSS codes)) Let $\mathcal{C}_1 = [n, k_1, d_1]_q$ and $\mathcal{C}_2 = [n, k_2, d_2]_q$ be linear codes over $\mathbb{F}_q$ with $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1$. Then there exists a QECC of parameters $[[N,K,d_{min}]]_q = [[n, k_1 + k_2 - n, d_{min}]]_q$ with $d_{min} = min\{wt(\mathbf{v} \mid \mathbf{v} \in \left(\mathcal{C}_1 \backslash \mathcal{C}_2^\perp\right) \cup \left(\mathcal{C}_2 \backslash \mathcal{C}_1^\perp\right))\}$.*

In particular, if $\mathcal{C} = [n,k,d]_q$ is a linear code over $\mathbb{F}_q$ and $\mathcal{C}^\perp \subseteq \mathcal{C}$. Then we have the following result on construction of QECC from dual-containing or weakly self-dual classical codes.

Corollary 3.4. *Let $\mathcal{C} = [n, k, d]_q$ be a dual-containing code over $\mathbb{F}_q$. Then there exists a $[[n, 2k - n, d_{min}]]_q$ QECC with $d_{min} = min\{wt(\mathbf{v} \mid \mathbf{v} \in \mathcal{C} \backslash \mathcal{C}^{\perp})\}$.*

3.3 Encoding of stabilizer codes

We shall see in this part of the chapter the encoding process of stabilizer codes of CSS structure and general structure. We focus on binary codes since binary codes are highly relevant to the work in later chapters.

3.3.1 CSS codes: encoding and error correction

An important class of quantum codes designed from classical codes over Euclidean dual space is called *Calderbank-Shor-Steane* (CSS) codes, named after the inventors. CSS codes are an important subclass of stabilizer codes. Let $\mathcal{C}_1 = [n, k_1]$ and $\mathcal{C}_2 = [n, k_2]$ be two classical linear codes such that $\mathcal{C}_2 \subset \mathcal{C}_1$ and both $\mathcal{C}_1$ and $\mathcal{C}_2^{\perp}$ correct t errors. Then a $[[n, k_1 - k_2]]$ CSS code of $\mathcal{C}_1$ over $\mathcal{C}_2$ capable of correcting t qubits can be constructed via the following encoding method. Let $\mathbf{x} \in \mathcal{C}_1$ be any codeword. Then the quantum state $|\mathbf{x} + \mathcal{C}_2\rangle$ is

$$|\mathbf{x} + \mathcal{C}_2\rangle \equiv \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\mathbf{y} \in \mathcal{C}_2} |\mathbf{x} + \mathbf{y}\rangle, \tag{3.12}$$

where addition is over binary field. It is easy to see that the state $|\mathbf{x}+\mathcal{C}_2\rangle$ depends only upon the *cosets* of $\mathcal{C}_1/\mathcal{C}_2$. If two elements $\mathbf{x}_1, \mathbf{x}_2 \in \mathcal{C}_1$ such that $\mathbf{x}_1 + \mathbf{x}_2 \in \mathcal{C}_2$, then $|\mathbf{x}_1 + \mathcal{C}_2\rangle = |\mathbf{x}_2 + \mathcal{C}_2\rangle$. Conversely, if $\mathbf{x}_1$ and $\mathbf{x}_2$ belong to different cosets of $\mathcal{C}_2$, there exist no $\mathbf{y}_1, \mathbf{y}_2 \in \mathcal{C}_2$ such that $\mathbf{x}_1 + \mathbf{y}_1 = \mathbf{x}_2 + \mathbf{y}_2$. Thus, $|\mathbf{x}_1 + \mathcal{C}_2\rangle$ and $|\mathbf{x}_2 + \mathcal{C}_2\rangle$ are orthonormal states. Hence, the CSS code constructed from $\mathcal{C}_1$ over $\mathcal{C}_2$ is the vector space spanned by $|\mathbf{x} + \mathcal{C}_2\rangle$ for all $\mathbf{x} \in \mathcal{C}_1$. The dimension of the CSS code is determined by the number of cosets of $\mathcal{C}_2$ in $\mathcal{C}_1$, that is, $\frac{|\mathcal{C}_1|}{|\mathcal{C}_2|} = 2^{k_1 - k_2}$, and therefore, this is an $[[n, k_1 - k_2]]$ quantum CSS code.

The 7-qubit code shown in Section 2.3.4.3 is a typical example of quantum CSS code with $\mathcal{C}_1 = \mathcal{C}$ and $\mathcal{C}_2 = \mathcal{C}^\perp$ such that $\mathcal{C}^\perp \subset \mathcal{C}$ for a classical linear code $\mathcal{C} = [n, k, d]$. This is known as the dual-containing classical codes or weakly self-dual codes.

The codeword states in this case is given by

$$\left|\mathbf{x} + \mathcal{C}^\perp\right\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\mathbf{y}\in\mathcal{C}^\perp} |\mathbf{x} + \mathbf{y}\rangle \tag{3.13}$$

for $\mathbf{x} \in \mathcal{C}$. The dimension of this CSS code is $\frac{|\mathcal{C}|}{|\mathcal{C}^\perp|} = 2^{k-(n-k)} = 2^{2k-n}$.

Denote by $E = (\mathbf{e}_1|\mathbf{e}_2)$ a Pauli error operator after the mapping $\Phi : \mathcal{P}_N \to \mathbb{F}_2^{2n}$. The vector $\mathbf{e}_1$ describes an occurrence of a bit-flip error with a 1, whereas the vector $\mathbf{e}_2$ describes an occurrence of a phase-flip error with a 1. If $|\mathbf{x} + \mathcal{C}_2\rangle$ in Equation (3.12) is the original encoded state then the corrupted state is

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{(\mathbf{x}+\mathbf{y})\cdot\mathbf{e}_2} |\mathbf{x} + \mathbf{y} + \mathbf{e}_1\rangle.$$

To detect where bit flips occurred, recall from the previous section, it is convenient to use an ancilla state initialized at $|0\rangle_a$ to store the error syndrome. Thus, by using the parity-check matrix H_1 for the code $\mathcal{C}_1$, we can effectively take the state $|\mathbf{x} + \mathbf{y} + \mathbf{e}_1\rangle|0\rangle_a$ to $|\mathbf{x} + \mathbf{y} + \mathbf{e}_1\rangle|H_1(\mathbf{x} + \mathbf{y} + \mathbf{e}_1)\rangle_a$ and produce the state

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{(\mathbf{x}+\mathbf{y})\cdot\mathbf{e}_2} |\mathbf{x} + \mathbf{y} + \mathbf{e}_1\rangle|H_1\mathbf{e}_1\rangle_a.$$

Since $\mathbf{x} + \mathbf{y} \in \mathcal{C}_1$, the ancilla state $|H_1\mathbf{e}_1\rangle$ contains only the syndrome about the error $\mathbf{e}_1$. The error $\mathbf{e}_1$ can be inferred from the error syndrome $H_1\mathbf{e}_1$ after the ancilla state is measured. The recovery is performed simply by applying Pauli X-gates to the qubits at whichever the positions in the error $\mathbf{e}_1$ a bit flip occurred. After all the bit flip errors been removed, the recovered state is

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{(\mathbf{x}+\mathbf{y})\cdot\mathbf{e}_2} |\mathbf{x} + \mathbf{y}\rangle. \tag{3.14}$$

To detect a phase error, each qubit in the state (3.14) is transformed using Hadamard gates, and taking to the state

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_{\mathbf{z}} \sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{(\mathbf{x}+\mathbf{y})\cdot(\mathbf{z}+\mathbf{e}_2)} |\mathbf{z}\rangle, \tag{3.15}$$

where the sum is over all possible values for N bit $\mathbf{z}$. Let $\mathbf{z}' = \mathbf{z} + \mathbf{e}_2$, then the state is equivalent to

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_{\mathbf{z}'} \sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{(\mathbf{x}+\mathbf{y})\cdot\mathbf{z}'} |\mathbf{z}' + \mathbf{e}_2\rangle.$$

If $\mathbf{z}' \in \mathcal{C}_2^{\perp}$, then

$$\sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{\mathbf{y}\cdot\mathbf{z}'} = |\mathcal{C}_2|,$$

whereas $\mathbf{z}' \notin \mathcal{C}_2^{\perp}$ implies

$$\sum_{\mathbf{y}\in\mathcal{C}_2} (-1)^{\mathbf{y}\cdot\mathbf{z}'} = 0.$$

Thus, the transformed state in Equation (3.15) can be rewritten as

$$\frac{1}{\sqrt{\frac{2^n}{|\mathcal{C}_2|}}} \sum_{\mathbf{z}'\in\mathcal{C}_2^{\perp}} (-1)^{(\mathbf{x})\cdot\mathbf{z}'} |\mathbf{z}' + \mathbf{e}_2\rangle,$$

which is similar to the case when detecting a bit flip error. By using ancilla states and the parity-check matrix H_2 for the code $\mathcal{C}_2^{\perp}$, error syndrome $H_2\mathbf{e}_2$ can be obtained, and correct the phase error $\mathbf{e}_2$ using Pauli Z-gates. The recovered states is

$$\frac{1}{\sqrt{\frac{2^n}{|\mathcal{C}_2|}}} \sum_{\mathbf{z}'\in\mathcal{C}_2^{\perp}} (-1)^{(\mathbf{x})\cdot\mathbf{z}'} |\mathbf{z}'\rangle.$$

The error-correction is completed by applying Hadamard transformation to each qubit once again.

3.3.2 Encoding of general stabilizer codes

To encode a general stabilizer code, consider the binary check matrix $H = [H_1|H_2]$ for an $[[N, K, d_{min}]]$ stabilizer code. Note that this matrix has $m = N - K$ rows

(m independent stabilizer generators). Since the dual-space of H is of dimension $2N-m \equiv (2(m+K)-m) = m+2K$, the normalizer group $\mathcal{N}(\mathcal{S})$ that commutes with $\mathcal{S}$ can be considered as the dual-space of $\mathcal{S}$ generated by an $(m+2K)\times 2N$ binary matrix. The last $2K$ rows are the logical operators $\bar{\mathbf{X}}$ and $\bar{\mathbf{Z}}$ with $|\bar{\mathbf{X}}| = |\bar{\mathbf{Z}}| = K$. Note that the choices of $\bar{\mathbf{X}}$ and $\bar{\mathbf{Z}}$ are non-unique and the following is a simple and most general way to obtain the set of $2K$ logical operators $\{\bar{\mathbf{X}}, \bar{\mathbf{Z}}\}$.

Since $\mathcal{S} = \langle \mathcal{M} \rangle$, we can always replace a generator g_i with $g_i g_j$ for some other generator g_j. The corresponding effect on the binary check matrices is to add row j with row i in both H_1 and H_2. In addition, by rearranging the corresponding columns in both matrices, the positions of qubits are altered. Combining these two operations, one can transform $H = [H_1|H_2]$ into *standard form* [15] given by

$$H_{std} = \begin{array}{r} R_{H_1}\{ \\ m-R_{H_1}\{ \end{array} \left(\begin{array}{ccc|ccc} I & A_1 & A_2 & B & C_1 & C_2 \\ 0 & 0 & 0 & D & I & E \\ \underbrace{}_{R_{H_1}} & \underbrace{}_{m-R_{H_1}} & \underbrace{}_{K} & \underbrace{}_{R_{H_1}} & \underbrace{}_{m-R_{H_1}} & \underbrace{}_{K} \end{array} \right),$$

where R_{H_1} is the rank of H_1.

To obtain $\{\bar{\mathbf{X}}, \bar{\mathbf{Z}}\}$ that satisfies conditions in (2.38), we obtain $\bar{\mathbf{X}}$ and $\bar{\mathbf{Z}}$ as

$$\bar{\mathbf{X}} = K\{(\underbrace{0}_{R_{H_1}} \underbrace{E^T}_{m-R_{H_1}} \underbrace{I}_{K} | \underbrace{C_2^T}_{R_{H_1}} \underbrace{0}_{m-R_{H_1}} \underbrace{0}_{K}) \tag{3.16}$$

and

$$\bar{\mathbf{Z}} = K\{(\underbrace{0}_{R_{H_1}} \underbrace{0}_{m-R_{H_1}} \underbrace{0}_{K} | \underbrace{A_2^T}_{R_{H_1}} \underbrace{0}_{m-R_{H_1}} \underbrace{I}_{K}), \tag{3.17}$$

respectively.

The operation of encoding a general stabilizer code can be described as [15]

$$|\overline{x_1, x_2, \cdots, x_K}\rangle \rightarrow \left(\prod_{1\le i\le m} (I+g_i) \right) \bar{X}_1^{x_1} \bar{X}_2^{x_2} \cdots \bar{X}_K^{x_K} |00\cdots 0\rangle, \tag{3.18}$$

where $\bar{X}_i \in \bar{\mathbf{X}}$ is the encoded X operator on the i-th qubit, and the state $|\overline{x_1, x_2, \ldots, x_K}\rangle$ is a quantum codeword. The binary K-tuples $[x_1, x_2, \ldots, x_K]$ represent one of the 2^K possible basis states that can be encoded into. Since the basis codeword is defined to be $|\overline{00\cdots0}\rangle = \left(\prod_{1\leq i\leq m}(I+g_i)\right)|00\cdots0\rangle$ and a Pauli Z operator does not generally affect the basis of a state, only $\bar{X}_i$ operators are used during the encoding process.

3.4 Bounds for quantum codes

Similar to classical codes, bounds that compare the performance of quantum codes also exist. In this small subsection, we are omitting detailed explanations but simply state the most important results on quantum bounds for stabilizer codes.

Given a stabilizer code $[[N, K, d_{min}]]$, the quantum Hamming bound for binary field [14] is given by

$$\sum_{j=0}^{t} 3^j \binom{N}{j} \leq 2^m, \tag{3.19}$$

and the code efficiency (code rate) is asymptotically upper bounded by

$$\frac{K}{N} \leq 1 - \delta^Q \log_2(3) - h_2(\delta^Q), \tag{3.20}$$

where $m = N - K$ is the number of stabilizer generators, $t = \lfloor \frac{d_{min}-1}{2} \rfloor$ is the number of correctable errors, and $\delta^Q = \frac{t}{N}$. In (3.20), $h_2(*)$ is the binary entropy function $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Note that this quantum Hamming bound valid for *non-degenerate* stabilizer codes, and for many years, it is unknown whether this bound holds for *degenerate* codes. There are no known degenerate codes that guarantee success that violate the quantum Hamming bound [14] [110].

The quantum Gilbert-Varshamov (GV) bound is [7]

$$\sum_{j=0}^{2t} 3^j \binom{N}{j} \leq 2^m, \tag{3.21}$$

and the code efficiency is asymptotically lower bounded by

$$\frac{K}{N} \geq 1 - 2\delta^Q \log_2(3) - h_2(2\delta^Q). \tag{3.22}$$

In addition, the Gilbert-Varshamov bound for an $[[N, K, d_{min}]]$ CSS code [6] is then given by

$$\frac{K}{N} \geq 1 - 2h_2(2\delta^Q). \tag{3.23}$$

Furthermore, any (degenerate and non-degenerate) quantum code must satisfy the quantum Singleton bound [93]

$$N - K \geq 4t. \tag{3.24}$$

Hence, the asymptotic code efficiency is given by

$$\frac{K}{N} \leq 1 - 4\delta^Q. \tag{3.25}$$

Any quantum codes that satisfy (3.24) with equality are called quantum maximum distance separable (MDS) codes.

The above known quantum bounds in the literature are depicted in Figure. 3.1 with code rate $\frac{K}{N}$ in terms of its normalized distance $\frac{d_{min}}{N}$, where $\frac{d_{min}}{N} \approx 2\delta^Q$ for sufficiently large N.

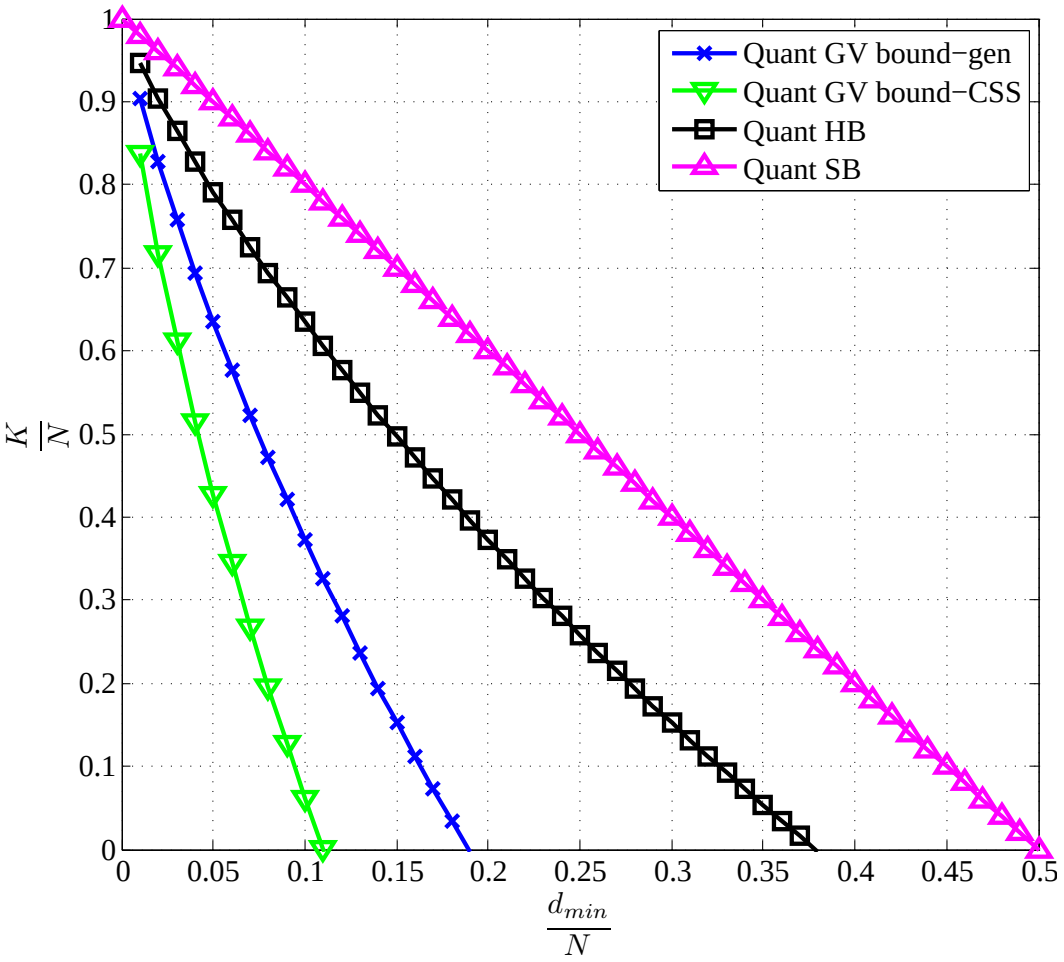

FIGURE 3.1: Known quantum bounds. The curves are △: Quantum Singleton bound (SB), □: Quantum Hamming bound (HB), ×: Quantum Gilbert-Varshamov bound for general quantum code and ▽: Quantum Gilbert-Varshamov bound for quantum CSS codes.

Chapter 4

Stabilizer Codes from Quadratic Residue Sets and Difference Sets

In this chapter, we design two types of stabilizer codes from *quadratic residue (QR) sets* and *difference sets*, respectively. We name them Type-I and Type-II stabilizer codes. The proposed stabilizer codes are non-CSS structures such that the underlying classical codes are self-orthogonal w. r. t. the SIP constraint described by Theorem 3.1 in Section 3.2.1.

4.1 Type-I quantum stabilizer codes from QR sets

Denote by $H = [H_1|H_2]$ the parity-check matrix of a stabilizer $\mathcal{S}$, where H_1 and H_2 are the generator matrices of two classical linear codes, respectively. We design the pair of matrices H_1 and H_2 simultaneously so that the two linear codes are self-orthogonal w. r. t. the SIP condition given in (2.56). In this section, we design $[[N, K, d_{min}]]_2$ Type-I quantum stabilizer codes over the finite field of order two by exploiting the notion of quadratic residue sets. We omit the subscript '2' for stabilizer codes designed from binary linear codes. We show that the proposed construction method using *idempotents* of cyclic codes generated from QR sets

can apply to any quadratic residue set of prime modulus $p = 4n \pm 1$ for $n \in \mathbb{Z}$. In addition, we prove that the minimum distance for stabilizer codes of length $N = 4n+1$ is upper bounded by the size of the quadratic residue set k. Moreover, the code rate for stabilizer codes of length $N = 4n-1$ is determined by $\frac{K}{N} = \frac{k}{p}$, and the code rate approaches $\frac{1}{2}$ as n goes to infinity, whereas the code rate for stabilizer codes of length $N = 4n+1$ is $\frac{K}{N} = \frac{1}{p}$. Furthermore, the family of stabilizer codes of length $N = 4n-1$ has a constant minimum distance of 2, which is related to the work in [92].

4.1.1 Quadratic (non-) residue sets and idempotent polynomials

Let $\mathbf{Z}_p^\times$ be a multiplicative group of order $p-1$, where p is a prime of the form $p = 4n \pm 1$. Denoted by $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ the quadratic residue set and quadratic non-residue set, respectively. Take α as a primitive element in $\mathbb{F}_p$. Then we have the following.

Lemma 4.1. $\mathcal{Q}^{\mathcal{R}} = \{\alpha^{2i} | 1 \leq i \leq \frac{p-1}{2}\}$ *and* $\mathcal{Q}^{\mathcal{NR}} = \{\alpha^{2i-1} | 1 \leq i \leq \frac{p-1}{2}\}$ *with* $|\mathcal{Q}^{\mathcal{R}}| = |\mathcal{Q}^{\mathcal{NR}}| = \frac{p-1}{2}$.

From Lemma 4.1, $\mathcal{Q}^{\mathcal{R}} \cup \mathcal{Q}^{\mathcal{NR}} = \{1, 2, \ldots, p-1\}$ when p is a prime since there are exactly half odd and half even integer numbers in $\mathbf{Z}_p^\times$. Furthermore, for $1 \leq i, i' \leq \frac{p-1}{2}$ and $i \neq i'$, $\alpha^{2i} \cdot \alpha^{2i'} \equiv \alpha^{2i-1} \cdot \alpha^{2i'-1} = \alpha^{0(\bmod 2)} \in \mathcal{Q}^{\mathcal{R}}$ and $\alpha^{2i-1} \cdot \alpha^{2i'} = \alpha^{1(\bmod 2)} \in \mathcal{Q}^{\mathcal{NR}}$. We have the following property as a direct consequence of Lemma 4.1.

Lemma 4.2. *For* $1 \leq i \leq \frac{p-1}{2}$,

$$\begin{aligned} \alpha^{2i}\mathcal{Q}^{\mathcal{R}} &= \alpha^{2i-1}\mathcal{Q}^{\mathcal{NR}} \equiv \mathcal{Q}^{\mathcal{R}}, \\ \alpha^{2i-1}\mathcal{Q}^{\mathcal{R}} &= \alpha^{2i}\mathcal{Q}^{\mathcal{NR}} \equiv \mathcal{Q}^{\mathcal{NR}}. \end{aligned} \tag{4.1}$$

Let $\bar{\mathcal{Q}}^{\mathcal{R}} = \{0, \mathcal{Q}^{\mathcal{NR}}\}$ and $\bar{\mathcal{Q}}^{\mathcal{NR}} = \{0, \mathcal{Q}^{\mathcal{R}}\}$ be the complementary set of $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$, respectively. Then for each $\mathbf{Z}_p^\times$, we can construct four cyclic codes $\mathcal{C}_R$, $\bar{\mathcal{C}}_R$,

$\mathcal{C}_{NR}$ and $\bar{\mathcal{C}}_{NR}$ associated to $\mathcal{Q}^{\mathcal{R}}$, $\bar{\mathcal{Q}}^{\mathcal{R}}$, $\mathcal{Q}^{\mathcal{NR}}$ and $\bar{\mathcal{Q}}^{\mathcal{NR}}$, respectively. One way to obtain a generator matrix for these codes is to use their *idempotent polynomial*. Define $\{\mathbb{Q}^r(x), \bar{\mathbb{Q}}^r(x), \mathbb{Q}^{nr}(x), \bar{\mathbb{Q}}^{nr}(x)\} \in \mathbb{F}_2[x]/(x^p-1)$ the idempotent polynomial for $\mathcal{C}_R$, $\bar{\mathcal{C}}_R$, $\mathcal{C}_{NR}$ and $\bar{\mathcal{C}}_{NR}$ over $\mathbb{F}_2$ of a prime p. Then

$$\begin{aligned} \mathbb{Q}^r(x) &= \sum_{i\in\mathcal{Q}^{\mathcal{R}}} x^i, & \bar{\mathbb{Q}}^r(x) &= 1 + \sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^i, \\ \mathbb{Q}^{nr}(x) &= \sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^i, & \bar{\mathbb{Q}}^{nr}(x) &= 1 + \sum_{i\in\mathcal{Q}^{\mathcal{R}}} x^i. \end{aligned} \tag{4.2}$$

Denote by

$$\mathbf{P} := \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ddots & \ddots & \ddots & 1 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \tag{4.3}$$

a square *circulant permutation matrix* (CPM) of order v such that $P^v = P^0 = I_v$, where I_v is the identity matrix of size v. Note that P is of weight one since it has only one non-zero element in each row and column.

The generator matrix for $\mathcal{C}_R$ is obtained as

$$G_{\mathcal{C}_R} = \sum_{i\in\mathcal{Q}^{\mathcal{R}}} P^i, \tag{4.4}$$

where the i-th power of P is the i-th cyclic shift of P, and $P^0 = I$ is the identity matrix. The transpose of $\mathbb{Q}^r(x)$ is then given by $\mathbb{Q}^r(x^{-1})$. Hence, in matrix representation, it is equivalent to

$$G^T_{\mathcal{C}_R} = \sum_{i\in\mathcal{Q}^{\mathcal{R}}} P^{p-i}. \tag{4.5}$$

Since $\mathcal{C}_R$ is a cyclic code, where each row of $G_{\mathcal{C}_R}$ is a cyclic shift of the previous row by one position, $G_{\mathcal{C}_R}$ can be completely characterized in its idempotent polynomial $\mathbb{Q}^r(x)$. Similar representations are used for $\bar{\mathcal{C}}_R$, $\mathcal{C}_{NR}$ and $\bar{\mathcal{C}}_{NR}$.

4.1.2 Design of Type-I stabilizer codes of length $N = 4n-1$

We now look at Type-I stabilizer codes of length $N = 4n - 1$ by designing multi-weight circulant matrices H_1 and H_2 from the idempotent polynomials in (4.2). Then, we analyse the dimension of Type-I stabilizer codes by constructing a pair of sub-matrices H_1^{sub} and H_2^{sub} from H_1 and H_2. We denote a matrix using capital letters and a polynomial using the corresponding lower case letters. *e.g.,* $h_1(x)$ is the polynomial of a parity-check matrix H_1.

Proposition 4.3. *For an even n and a prime $p = 4n - 1$, let $H_1 = G_{\bar{\mathcal{C}}_R}$ and $H_2 = G_{\mathcal{C}_R}$. Denote by H_1^{sub} and H_2^{sub} a pair of sub-matrices with $Rank(H_1^{sub}) = p - k - 1$ and $Rank(H_2^{sub}) = p - k$. Then, H_1^{sub} and H_2^{sub} are self-orthogonal w. r. t. the SIP, and the resulting parity-check matrix $H = [H_1^{sub}|H_2^{sub}]$ is a $[[N, K, d_{min}]] = [[p, k, d_{min} = 2]]$ Type-I stabilizer code.*

Proof. When n is even, $p = 4n - 1 \equiv -1 \pmod 8$, by the 2^{nd} Supplement to the Law of Quadratic Reciprocity [57], $2 \in \mathcal{Q}^{\mathcal{R}}$ and $-2 \notin \mathcal{Q}^{\mathcal{R}}$. From (4.2), $h_1(x) = 1 + \sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^i$ and $h_2(x) = \sum_{j\in\mathcal{Q}^{\mathcal{R}}} x^j$. Since $-\mathcal{Q}^{\mathcal{R}} = \mathcal{Q}^{\mathcal{NR}}$ and for $f(x) = (x^a + x^b) \in \mathbb{F}_2[x]$, $f(x)^2 = (x^a + x^b)^2 = x^{2a} + x^{2b}$, we have

$$\begin{aligned} h_1(x)h_2(x^{-1}) &= \left(\sum_{j\in\mathcal{Q}^{\mathcal{R}}} x^{-j}\right) + \left(\sum_{j\in\mathcal{Q}^{\mathcal{R}}} x^{-j}\right)\left(\sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^{i}\right) \\ &\equiv \left(\sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^{i}\right) + \left(\sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^{2i}\right). \end{aligned} \tag{4.6}$$

By Lemma 4.2, $(\sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^{2i}) = (\sum_{i\in\mathcal{Q}^{\mathcal{NR}}} x^{i})$ since $2 \in \mathcal{Q}^{\mathcal{R}}$ is an element of the QR set. Hence, $H_1H_2^T = \mathbf{0} \pmod 2$. Similarly, $H_2H_1^T \equiv \mathbf{0} \pmod 2$ implies that H_1 and H_2 are commuting pairs for even n.

Since $\mathcal{Q}^{\mathcal{R}} \bigcup \mathcal{Q}^{\mathcal{NR}} = \mathbf{Z}_p^{\times}$. Then H_1 and H_2 are complementary matrices, that is

$$H_1 + H_2 = \mathbb{I}_{p\times p}, \tag{4.7}$$

where $\mathbb{I}_{p\times p}$ is an all-one matrix of size $p \times p$. Denote by $\mathscr{M}_X(E)$ and $\mathscr{M}_Z(E)$ the two binary m-tuple error syndromes measured by H_1 and H_2, respectively.

Since $\mathscr{M}(E) = (\mathscr{M}_X(E) + \mathscr{M}_Z(E)) \pmod 2$, we have $\mathscr{M}(Y_1) = \mathscr{M}(Y_2) = \ldots = \mathscr{M}(Y_p) = [1, 1, \ldots, 1]^m$. Thus, this code cannot distinguish between two single weight Y operators. Hence, $d_{min} = 2$. □

The rank of $H = [H_1^{sub}|H_2^{sub}]$ constructed from *Proposition 4.3* is determined from the following lemma.

Lemma 4.4. *For n is even and $p = 4n - 1$ is a prime, let $H_1 = G_{\bar{\mathcal{C}}_R}$ and $H_2 = G_{\mathcal{C}_R}$ with, respectively, the idempotent polynomials $h_1(x) := 1 + \sum_{i=1}^{k} x^{-d_i}$ and $h_2(x) := \sum_{i=1}^{k} x^{d_i}$, where $d_{1,2,\ldots,k} \in \mathcal{Q}^{\mathcal{R}}$. The rank of H_1 and H_2 is*

$$Rank(H_1) = p - (k + 1), \tag{4.8}$$

$$Rank(H_2) = p - k. \tag{4.9}$$

Let H_1^{sub} (resp. H_2^{sub}) be the sub-matrix of H_1 (resp. H_2) with $Rank(H_1^{sub}) = Rank(H_1)$ (resp. $Rank(H_2^{sub}) = Rank(H_2)$). The resulting parity-check matrix $H = [H_1^{sub}|H_2^{sub}]$ is a $[[N, K, d_{min}]] = [[p, k, d_{min}]]$ quantum stabilizer code.

Proof. Let α be a primitive p-th root of unity in some field $\mathbb{F}_p$. To prove the lemma, it is equivalent to finding the number of roots of $h_1(x)$ and $h_2(x)$ in $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$.

Since $p = 4n - 1 \equiv -1 (\text{mod } 8)$ when n is even, we shall show that corresponding to each d_i in $\mathcal{Q}^{\mathcal{R}}$, either α^{d_i} or α^{-d_i} is a root of $h_2(x)$. Since p is not congruent to 1 modulo 4, by the 1^{st} Supplement to the Law of Quadratic Reciprocity [57], -1 is not a quadratic residue, and we have $\{d_1, d_2, \ldots, d_k\} \cup -\{d_1, d_2, \ldots, d_k\} = \mathcal{G}_{\mathbb{Z}_p}^{\times}$. Consequently, $\bigcup_{1 \le i \le p-1} \{\alpha^{d_i}, \alpha^{-d_i}\} = \{\alpha, \alpha^1, \cdots, \alpha^{p-1}\}$. Hence for all $1 \le j \le p - 1$, $h_2(\alpha^{d_i}) + h_2(\alpha^{-d_i}) = \sum_{j=1}^{k} \alpha^{d_j d_i} + \sum_{j=1}^{k} \alpha^{-d_j d_i} = \sum_{j=1}^{p-1} \alpha^{j d_i} = 1 + \sum_{j=0}^{p-1} \alpha^{j d_i} = 1$, where the last equality holds due to $\alpha^{d_i} \neq 1$ being a root of $x^p - 1 = (x - 1)(x^{p-1} + x^{p_2} + \ldots + x + 1)$. Again, by the 2^{nd} Supplement to the Law of Quadratic Reciprocity, $2 \in \mathcal{Q}^{\mathcal{R}}$ in $\mathcal{G}_{\mathbb{Z}_p}^{\times}$. Then the quadratic residue set $\{d_1, d_2, \ldots, d_k\}$ is closed under multiplication by 2. As a result, $h_2(\alpha^{2d_i}) = h_2(\alpha^{d_i})$. This implies that $h_2(\alpha^{d_i})$ is an element in $\mathbb{F}_2$. Thus, either $h_2(\alpha^{d_i}) = 0$ or

$1 - h_2(\alpha^{-d_i}) = h_2(\alpha^{d_i}) = 1$. We conclude that either α^{d_i} or α^{-d_i} is a root of $h_2(x)$. Hence, when n is even, $Rank(H_2) = p - k$.

Similarly, for $h_1(x) := 1 + \sum_{i=1}^{k} x^{-d_i}$ for $-d_{1,2,\ldots,k} \in \mathcal{Q}^{\mathcal{NR}}$, we have

$$\{0\} \bigcup \{\alpha^{-d_i} | 1 \leq i \leq k\}$$

are the set of roots for $h_1(x)$. Hence, $Rank(H_1) = p - (k+1)$. □

Corollary 4.5. *For n is odd and $p = 4n - 1$ is a prime, let $H_1 = G_{\bar{\mathcal{C}}_R}$ and $H_2 = G_{\mathcal{C}_R}$. The rank of H_1 and H_2 is*

$$Rank(H_1) = p - 1, \tag{4.10}$$

$$Rank(H_2) = p. \tag{4.11}$$

Let H_1^{sub} (resp. H_2^{sub}) be the sub-matrix of H_1 (resp. H_2) with $Rank(H_1^{sub}) = Rank(H_1)$ (resp. $Rank(H_2^{sub}) = Rank(H_2)$). The resulting parity-check matrix $H = [H_1^{sub}|H_2^{sub}]$ is a trivial $[[N, K, d_{min}]] = [[p, 0, d_{min}]]$ quantum stabilizer code.

Proof. In this case, $p = 4n - 1$ is equivalent to $p = 3 \bmod 8$. Denote by $min(\mathcal{Q}^{\mathcal{R}})$ the smallest value in $\{d_1, d_2, \ldots, d_k\}$. Then, $f(x) = x^{min(\mathcal{Q}^{\mathcal{R}})} \cdot \sum_{i=1}^{k} x^{(d_i - min(\mathcal{Q}^{\mathcal{R}}))}$. Since $min(\mathcal{Q}^{\mathcal{R}}) = 1$, there are at most $p - 1 - min(\mathcal{Q}^{\mathcal{R}})$ non-zero roots of $f(x)$. By the 2^{nd} Supplement to the Law of Quadratic Reciprocity, $2 \in \mathcal{Q}^{nr}$ is a quadratic non-residue in $\mathcal{G}_{\mathbb{Z}_p}^{\times}$, hence the order of 2 in $\mathcal{G}_{\mathbb{Z}_p}^{\times}$ is $p - 1$. Assume α^i for some $0 \leq i \leq p - 1$ is also a root of $f(x)$. Since $f(x)$ is a polynomial over field $\mathbb{F}_2$, $f(\alpha^{i \cdot 2^j}) = f(\alpha^i)^{2^j} = 0$ for all $0 \leq j \leq p - 1$, which implies that there are $p - 1$ distinct roots of $f(x)$. But this contradicts that $f(x)$ has at most $p - 1 - min(\mathcal{Q}^{\mathcal{R}}) < p - 1$ non-zero roots. Hence, no roots of $f(x)$ are in the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-1}\}$ and $Rank(H_2) = p - K$, where $K = 0$. By the same argument in *Lemma 4.4*, $Rank(H_1) = p - 1$. □

Corollary 4.6. *The above analyses for n is even or odd also apply to the case when $H_1 = G_{\bar{\mathcal{C}}_{NR}}$ and $H_2 = G_{\mathcal{C}_{NR}}$.*

Example 4.1. *Take $n = 2$ as an example. We have a $(p, k, \lambda) = (7, 3, 1)$ difference set, and $\mathcal{Q}^{\mathcal{R}} = \{1, 4, 2\} \pmod 7$ is the set of quadratic residues. Let $H_1(x) = \mathbb{Q}^r(x)^{\pi_1(\mathcal{Q}^{\mathcal{R}})} = x(x + x^2 + x^4)$ and $H_2(x) = \mathbb{Q}^r(x)^{\pi_4(\mathcal{Q}^{\mathcal{R}})} = x^4(x + x^2 + x^4)$. Since n is even, $Rank(H) = Rank(H_1) = Rank(H_2) = p - k = 7 - 3 = 4$, it is a $[[p, K, d_{min}]] = [[7, 3, d_{min}]]$ quantum stabilizer code and the parity-check matrix is*

$$H = \left(\begin{array}{c|c} 0011010 & 0100011 \\ 0001101 & 1010001 \\ 1000110 & 1101000 \\ 0100011 & 0110100 \end{array}\right). \tag{4.12}$$

Furthermore, the set of logical X and Z operators are

$$\bar{\mathbf{X}} = \begin{pmatrix} IZIIXII \\ IIZIIXI \\ IIIZIIX \end{pmatrix} \text{ and } \bar{\mathbf{Z}} = \begin{pmatrix} ZIZZZII \\ ZZZIIZI \\ IZZZIIZ \end{pmatrix}. \tag{4.13}$$

It can be verified easily that properties in (2.38) are satisfied for $\bar{\mathbf{X}}$ and $\bar{\mathbf{Z}}$. Since $\{\bar{\mathbf{X}}, \bar{\mathbf{Z}}\} \in \mathcal{N}(\mathcal{S}) \backslash \mathcal{S}$, $d_{min} = 2$ because $wt(\bar{X}^1) = 2$. Thus, H in (4.12) this is a $[[7, 3, 2]]$ Type-I stabilizer code. □

Example 4.2. *For $n = 2$ and $p = 7$, $\mathcal{Q}^{\mathcal{R}} = \{1, 2, 4\}$ and $\bar{\mathcal{Q}}^{\mathcal{R}} = \{0, 3, 5, 6\}$. Let $h_1(x) = \bar{\mathbb{Q}}^r(x)$ and $h_2(x) = \mathbb{Q}^r(x)$. We have $h(x) = [1 + x^3 + x^5 + x^6 | x^1 + x^2 + x^4]$ and $Rank(H_1) = p - k - 1 = 3$ and $Rank(H_2) = p - k = 4$. Consider two error operators $E_1, E_2 \in \mathcal{P}_N$, where $E_1 = IIIYIII$ and $E_2 = IIYIIII$, by measuring all four stabilizer generators on each of the operators, we obtain the syndrome $\mathscr{M}(E_1) = [1, 1, 1, 1]^T$ and $\mathscr{M}(E_2) = [1, 1, 1, 1]^T$. Since $\mathscr{M}(E_1) = \mathscr{M}(E_2)$, the code can not distinguish Y errors on arbitrary two qubits. Thus, $2 \geq d_{min}$.* □

4.1.3 Design of Type-I stabilizer codes of length $N = 4n+1$

We now look at Type-I stabilizer codes of length $N = 4n + 1$.

Proposition 4.7. *For an odd n and a prime $p = 4n+1$, let $H_1 = G_{\mathcal{C}_R}$, $H_2 = G_{\mathcal{C}_{NR}}$, and H_1^{sub}, H_2^{sub} be the sub-matrices of H_1 and H_2, respectively. Then H_1^{sub} and H_2^{sub} are self-orthogonal w. r. t. the SIP, and the rank is $Rank(H_1^{sub}) = Rank(H_2^{sub}) = p-1$. The resulting parity-check matrix $H = [H_1^{sub}|H_2^{sub}]$ is a $[[N, K, d_{min}]] = [[p, 1, d^{\dagger} \geq d_{min} \geq 3]]$ quantum stabilizer code, where $d^{\dagger} = min(wt(E))$ for $E \in \mathcal{S}$.*

Since $p = 4n + 1 \equiv 1 \pmod p$, by *Theorem 14* in [70], matrices $H_1 = G_{\mathcal{C}_R}$ and $H_2 = G_{\mathcal{C}_{NR}}$ are commutating pairs and have rank $p - 1$. Moreover, since $k = \frac{p-1}{2} = 2n$, both H_1 and H_2 are even weight circulant matrices. Hence, we have the following lemma.

Lemma 4.8. *For an odd $n > 1$ and a prime $p = 4n + 1$, let $\mathcal{C}_R$ and $\mathcal{C}_{NR}$ be two linear cyclic code spanned by $H_1 = G_{\mathcal{C}_R}$ and $H_2 = G_{\mathcal{C}_{NR}}$, respectively. Then $\mathcal{C}_R$ and $\mathcal{C}_{NR}$ are linear even code that contain codewords of even weight only. For $a \in \mathcal{C}_R$ and $b \in \mathcal{C}_{NR}$, $min(wt(a)) = min(wt(b)) = 2$.*

Proof. Let c_1, c_2 be rows of H_1, then

$$wt(c_1 + c_2) = wt(c_1) + wt(c_2) - 2wt(c_1 \cap c_2). \tag{4.14}$$

Since $|\mathcal{Q}^{\mathcal{R}}| = k$, we have $wt(c_1) = wt(c_2) = k$ and $2wt(c_1 \cap c_2) = 0 \pmod 2$. Thus, $wt(c_1 + c_2) \equiv 0 \pmod 2$. By induction, for any codeword $a \in \mathcal{C}_R$, $wt(a) = 0 \pmod 2$. Let b be any codeword of $\mathcal{C}_{NR}$. Similarly, we can also show by induction that $wt(b) = 0 \pmod 2$. Thus, $\mathcal{C}_R$ and $\mathcal{C}_{NR}$ are even codes with $wt(a) = wt(b) = 0 \pmod 2$.

We know that an even code has a generator polynomial $g(x)$ that is divisible by $(1 + x)$. Thus, any $\mathbb{Q}^r(x)$ over $\mathbb{F}_2$ is divisible by $(1 + x)$. Since $Rank(H_1) = p - 1$ implies that $dim(\mathcal{C}_R) = p - 1$, the generator polynomial for $\mathcal{C}_R$ has degree of one. Hence, $g(x) = 1 + x$ is the generator polynomial of $\mathcal{C}_R$ for any prime length $p = 4n + 1$ with an odd n. Therefore, for any codeword $a \in \mathcal{C}_R$, we have $wt(a) = \{2i | 1 \leq i \leq \frac{p-1}{2}\}$ and $min(wt(a)) = 2$. Similarly, an even code $\mathbb{Q}^{nr}(x)$ is also divisible by $g(x)$, which implies that $\mathcal{C}_R \equiv \mathcal{C}_{NR}$. Hence, the minimum weight of codewords spanned by H_1 and H_2 is always 2. □

By *Lemma 4.8*, we know that $\mathcal{C}_R = \langle h_1(x) \rangle \equiv \langle g(x) \rangle$ and $\mathcal{C}_R \equiv \mathcal{C}_{NR}$, where $g(x) = 1 + x$. Let $H_1^{sub} = G$ generated from $g(x)$ and $H_2^{sub} = G_{\mathcal{C}_{NR}}$ with rank $p-1$. By linear operation on rows and columns of H_1^{sub} and H_2^{sub}, we transform $H = [H_1^{sub}|H_2^{sub}]$ into its *reduced row-echelon* form

$$H_{rref} = \left[\begin{array}{c|c} \underbrace{\begin{array}{c} \\ I_{(p-1)\times(p-1)} \\ \\ \end{array}}_{H_1^{sub'}} & \begin{array}{c} 1 \\ 1 \\ \vdots \\ 1 \end{array} H_2^{sub'} \end{array}\right], \tag{4.15}$$

where $H_1^{sub'}$ and $H_2^{sub'}$ are equivalent matrices for H_1^{sub} and H_2^{sub}, respectively.

Note that each row of $H_1^{sub'}$ is of weight 2 and the linear combination between any two rows of $H_1^{sub'}$ is also a codeword of weight 2. The corresponding row weight of $H_2^{sub'}$ is then determined by the following lemma.

Lemma 4.9. *Let c be a row of $H_2^{sub'}$, where $H_2^{sub'}$ is the equivalent matrix of H_2^{sub} given in (4.15). Then $min(wt(c)) = k$ and $max(wt(c)) = k + 2$.*

Proof. Let $h_1(x) = \mathbb{Q}^r(x)$ and $h_2(x) = \mathbb{Q}^{nr}(x)$. Since n is odd and p is a prime of the form $p = 4n + 1$, by the 1^{st} Supplement to the Law of Reciprocity, $-1 \in \mathcal{Q}^{\mathcal{R}}$ and $2 \notin \mathcal{Q}^{\mathcal{R}}$. Then by *Lemma 4.2*, $h_1(x) = h_1(x^{-1})$ (resp. $h_2(x) = h_2(x^{-1})$) and $h_1(x)^2 = h_2(x)$ (resp. $h_2(x)^2 = h_1(x)$). Equivalently,

$$H_1 H_1^T = kI + (n-1)\mathbb{I}_{diag(0),p\times p} + H_2 \equiv H_2 \pmod 2 \tag{4.16}$$

and

$$H_2 H_2^T = kI + (n-1)\mathbb{I}_{diag(0),p\times p} + H_1 \equiv H_1 \pmod 2, \tag{4.17}$$

where $\mathbb{I}_{diag(0),p\times p}$ is a all-one matrix with zero diagonal of size $p \times p$. It can be seen that the maximum and minimum overlapping between a pair of rows in either H_1 or H_2 is n and $n-1$, respectively. Thus, using (4.14), the row weight of $H_2^{sub'}$ is $2k - 2n = k$, assuming two rows having the maximum overlapping, or to $2k - 2(n-1) = k + 2$, assuming two rows having the minimum overlapping. □

From the above, we have the following result.

Lemma 4.10. *Let $E \in \mathcal{S}$ be a Pauli operator of weight $wt(E)$, where $\mathcal{S}$ is the stabilizer group spanned by $H = [H_1^{sub}|H_2^{sub}]$. Let $d^\dagger = min(wt(E))$ be the minimum weight of operator in $\mathcal{S}$. Then we have $d^\dagger \leq k$.*

Proof. From *Lemma 4.8*, we know that $\mathcal{C}_R \equiv \mathcal{C}_{NR}$. Thus, for any $E \in \mathcal{S}$, $\Phi(E) = (a|b) \in \mathbb{F}_2^{2N}$ with $a, b \in \mathcal{C}_R$. The weight of E is determined by

$$wt(E) \equiv wt(a|b) = wt(a) + wt(b) - wt(a \cap b). \tag{4.18}$$

Then, the minimum weight, $d^\dagger$, is given by

$$d^\dagger = min\{wt(a) + wt(b) - wt(a \cap b)\}. \tag{4.19}$$

Since $min(wt(a)) = 2$, Equation (4.19) is equivalent to

$$\begin{aligned} d^\dagger &= min \left\{ \begin{array}{l} \underset{a \in \mathcal{C}_R, wt(a)=2}{min} \{wt(a) + wt(b) - wt(a \cap b)\}, \\ \underset{a \in \mathcal{C}_R, wt(a)\neq 2}{min} \{wt(a) + wt(b) - wt(a \cap b)\} \end{array} \right\} \\ &\leq min(wt(a)) + wt\,(b|wt(a) = 2) - wt(a \cap b). \end{aligned} \tag{4.20}$$

We know from *Lemma 4.9* that $max(wt(b)) = k + 2$ and $min(wt(b)) = k$ when $wt(a) = 2$. Therefore,

$$\begin{aligned} d^\dagger &\leq min(wt(a)) + min[wt(b)|wt(a) = 2] - max(wt(a \cap b)) \\ &\leq 2 + k - min\{wt(a), wt(b)\} \equiv k. \end{aligned} \tag{4.21}$$

□

To encode such a code, note that Equation (4.15) is already in the standard form given in (3.16),

$$H_{std} = \left(H_1^{sub'} |\ B\ \ C\right), \tag{4.22}$$

where B is a $(p-1)\times(p-1)$ square matrix and C is a single $(p-1)\times 1$ column vector. Therefore, the logical operators $\bar{Z}_1$ and $\bar{X}_1$ for $K=1$ are

$$\bar{Z}_1 = (0,0,\ldots,0|1,1,\ldots,1) \tag{4.23}$$

and

$$\bar{X}_1 = \left(0,0,\ldots,0,1|\ C^T\ \ 0\right). \tag{4.24}$$

The minimum distance d_{min} of a stabilizer code that is defined as

$$d_{min} = min(wt(F))\ \ \textbf{s.t.}\ \ F \in \mathcal{N}(\mathcal{S})\backslash\mathcal{S}, \tag{4.25}$$

can be determined by the following lemma.

Lemma 4.11. *Let $F \in \mathcal{N}(S)\backslash\mathcal{S}$ be a Pauli operator of weight $wt(F)$. The minimum distance d_{min} is upper bounded by*

$$d_{min} = min(wt(F)) \leq k-1 \tag{4.26}$$

Proof. The subset $\mathcal{N}(\mathcal{S})\backslash\mathcal{S}$ is generated by multiplying $\mathcal{S}$ with $\bar{X}_1$, $\bar{Z}_1$ and $\bar{X}_1\bar{Z}_1$. Let $\Phi(\bar{X}_1) = (a_{\bar{X}_1}|b_{\bar{X}_1})$ and $\Phi(\bar{Z}_1) = (a_{\bar{Z}_1}|b_{\bar{Z}_1})$. Let $\Phi(F) = (a'|b') \in \mathbb{F}_2^{2N}$ and $\Phi(E) = (a|b) \in \mathbb{F}_2^{2N}$ be the binary $2N$-tuples for $F \in \mathcal{N}(\mathcal{S})\backslash\mathcal{S}$ and $E \in \mathcal{S}$, respectively. The binary N-tuples a' and b' are determined by one of the linear combinations

$$\begin{aligned} a' &\in \{a + a_{\bar{X}_1}, a + a_{\bar{Z}_1}, a + (a_{\bar{X}_1} + a_{\bar{Z}_1})\}, \\ b' &\in \{b + b_{\bar{X}_1}, b + b_{\bar{Z}_1}, b + (b_{\bar{X}_1} + b_{\bar{Z}_1})\}. \end{aligned} \tag{4.27}$$

Since $min(wt(b)) = k$ given that $min(wt(a)) = 2$ for $E \in \mathcal{S}$, the weight of the column vector C in (4.24) is $wt(C) \geq k$. Thus, we have

$$\begin{aligned} wt(a_{\bar{X}_1}) = 1, \quad wt(b_{\bar{X}_1}) \geq k, \\ wt(a_{\bar{Z}_1}) = 0, \quad wt(b_{\bar{Z}_1}) = p. \end{aligned} \tag{4.28}$$

The minimum distance d_{min} is given by

$$\begin{aligned} d_{min} &= min(wt(F)) \equiv min(wt(a'|b')) \\ &= min\{wt(a') + wt(b') - wt(a' \cap b')\}. \end{aligned} \tag{4.29}$$

Since either $wt(b) = k+2$ or $wt(b) = k$ given that $min(wt(a)) = 2$, by considering all the possible cases for the given $wt(b)$ and $min(wt(a))$, Equation (4.29) can be expanded into Equation (4.30), where $\Omega = max(wt(a' \cap b'))$.

By using (4.27) and (4.28), the upper bound for d_{min} is

$$\begin{aligned} d_{min} &\leq min\{k, k+2, k, k-1\} \\ &\leq k-1 \leq d^{\dagger}. \end{aligned} \tag{4.31}$$

We have now completed the proof. □

The lower bound on the minimum distance d_{min} can be interpreted as the following. Since

$$h_1(x) + h_2(x) = \mathbb{Q}^r(x) + \mathbb{Q}^{nr}(x) = \sum_{i=1}^{p-1} x^i, \tag{4.32}$$

we have

$$H_1 + H_2 = \mathbb{Q}^r(P) + \mathbb{Q}^{nr}(P) = \sum_{i=1}^{p-1} P^i = \mathbb{I}_{diag(0),p\times p}. \tag{4.33}$$

Let $E \in \mathcal{N}(\mathcal{S})\backslash\mathcal{S}$ have weight $wt(E) = 1$. Then for $1 \leq i \leq p$, $\{\mathscr{M}_Z(E_i), \mathscr{M}_X(E_i), \mathscr{M}(E_i)\} = [H_1|H_2|\mathbb{I}_{diag(0),p\times p}]$ are distinct column vectors. Hence, $d_{min} \geq 3$ and

---

$$d_{min} \leq min \left\{ \begin{array}{l} min\,(wt(a')|wt(a) = 2) + wt\,(b'|min(wt(a')), wt(b) = k) - \Omega, \\ min\,(wt(a')|wt(a) = 2) + wt\,(b'|min(wt(a')), wt(b) = k+2) - \Omega, \\ min\,(wt(b')|wt(b) = k) + wt\,(a'|min(wt(b')), wt(a) = 2) - \Omega, \\ min\,(wt(b')|wt(b) = k+2) + wt\,(a'|min(wt(b')), wt(a) = 2) - \Omega \end{array} \right\}. \tag{4.30}$$

$H = [H_1^{sub}|H_2^{sub}]$ of length $N = 4n + 1$ is a Type-I stabilizer code that corrects at least one error. We now give an example of Type-I stabilizer codes of length $N = 4n + 1$.

Example 4.3. *When* $n = 1$ *and* $p = 5$, *then* $\mathcal{Q}^{\mathcal{R}} = \{1, 4\} \pmod 5$ *and* $\mathcal{Q}^{\mathcal{NR}} = \{2, 3\} \pmod 5$. *Let*

$$\mathbb{Q}^r(x) = x + x^4 \quad and \quad \mathbb{Q}^{nr}(x) = x^2 + x^3$$

be the first row of $\mathbb{Q}^r(P)$ *and* $\mathbb{Q}^{nr}(P)$, *respectively. Since,* n *is odd, we obtain the parity matrices*

$$H_1^{sub} = \begin{pmatrix} 01001 \\ 10100 \\ 01010 \\ 00101 \end{pmatrix} \quad and \quad H_2^{sub} = \begin{pmatrix} 00110 \\ 00011 \\ 10001 \\ 11000 \end{pmatrix} \tag{4.34}$$

of a $[[5, 1, d_{min}]]$ *quantum stabilizer code by removing the last row of matrices* $\mathbb{Q}^r(P)$ *and* $\mathbb{Q}^{nr}(P)$. *Note that, this code is equivalent to the well-known perfect* $[[5, 1, 3]]$ *quantum stabilizer code [13] if we remove the forth row of* $\mathbb{Q}^r(P)$ *and* $\mathbb{Q}^{nr}(P)$ *in stead of the first row. It is known that this code has* $d_{min} = 3$ *that can correct arbitrary single error. Furthermore,* $d^\dagger = 4 > d_{min}$ *which implies that this code is a non-degenerate quantum stabilizer code.* □

Example 4.4. *For* $n = 3$ *and* $p = 13$, $\mathcal{Q}^{\mathcal{R}} = \{1, 3, 4, 9, 10, 12\} \pmod{13}$ *and* $\mathcal{Q}^{\mathcal{NR}} = \{2, 5, 6, 7, 8, 11\} \pmod{13}$. *Thus*

$$\mathbb{Q}^r(x) = x + x^3 + x^4 + x^9 + x^{10} + x^{12}$$

and

$$\mathbb{Q}^{nr}(x) = x^2 + x^5 + x^6 + x^7 + x^8 + x^{11}. \tag{4.35}$$

The rank $Rank(H) = Rank(H_1^{sub}) = Rank(H_2^{sub}) = 13 - 1 = 12$. *This is a* $[[13, 1, d_{min}]]$ *quantum stabilizer code. The stabilizer and the set of logical operators* $\bar{X}_1$ *and* $\bar{Z}_1$ *are shown in TABLE 4.1. Let* $E = g_2 g_4 \bar{X}_1$. *Then* $E =$

g_1	X	Z	Z	I	Z	I	I	I	Z	I	Z	Z	X
g_2	I	Y	I	Z	Z	Z	I	I	Z	Z	Z	I	Y
g_3	Z	Z	X	I	I	Z	Z	I	Z	Z	I	I	X
g_4	I	I	I	X	Z	I	Z	Z	Z	Z	I	Z	X
g_5	I	Z	Z	I	Y	Z	I	Z	I	Z	I	Z	Y
g_6	Z	Z	I	Z	Z	Y	Z	I	I	I	I	Z	Y
g_7	Z	I	I	I	I	Z	Y	Z	Z	I	Z	Z	Y
g_8	Z	I	Z	I	Z	I	Z	Y	I	Z	Z	I	Y
g_9	Z	I	Z	Z	Z	Z	I	Z	X	I	I	I	X
g_{10}	I	I	Z	Z	I	Z	Z	I	I	X	Z	Z	X
g_{11}	I	Z	Z	Z	I	I	Z	Z	Z	I	Y	I	Y
g_{12}	Z	Z	I	Z	I	I	I	Z	I	Z	Z	X	X
$\bar{X}_1$	I	Z	I	I	Z	Z	Z	Z	I	I	Z	I	X
$\bar{Z}_1$	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

TABLE 4.1: Stabilizer of $[[13, 1, 5]]$ quantum stabilizer code.

$IXIYZIIIIIZY \in \mathcal{N}(\mathcal{S})\backslash\mathcal{S}$ *has* $wt(E) = 5$. *Note that this stabilizer* $\mathcal{S}$ *has distance* $d^\dagger = 6$ *and the minimum distance of this code is* $d_{min} = 5 < d^\dagger$. *Hence, this is a non-degenerate* $[[13, 1, 5]]$ *stabilizer code that is capable of correcting arbitrary two errors.* □

4.1.4 Constructed codes

In this section, we constructed Type-I stabilizer codes of length $N = 4n + 1$ and $N = 4n - 1$ for $n \leq 25$ and the results are listed in TABLEs 4.2 and 4.3. The codes in TABLE 4.2 are Type-I $[[N, K, d_{min}]] = [[4n + 1, 1, d^\dagger \geq d_{min} \geq 3]]$ stabilizer codes. The corresponding $d^\dagger$ of the codes, which denotes the minimum weight of an operator $E \in \mathcal{S}$, is also shown in the table. From these two tables, it can be seen that $d_{min} < d^\dagger$ for all n, which means they are all non-degenerate stabilizer codes. Further, we find that for the code lengths $N = 4n + 1$, $n = 1, 3$ and 7, our constructed Type-I stabilizer codes in TABLE 4.2 achieve the highest minimum distance as given in [91]. Moreover, our constructed Type-I stabilizer codes, $[[37, 1, 11]]$, $[[53, 1, 15]]$, $[[61, 1, 17]]$ and $[[101, 1, 21]]$ meet the lower bound of the achievable minimum distance given in [91]. As shown in TABLE 4.2, for $n = 1$, our Type-I stabilizer code is equivalent to the *perfect* $[[5, 1, 3]]$ code [13].

Interestingly, it has $d^\dagger = 4 > d_{min}$ shown in brackets, where $d^\dagger = 4n$. Also, for $n = 3$ and 7, our $[[13, 1, 5]]$ and $[[29, 1, 11]]$ Type-I stabilizer codes are equivalent to the codes proposed in [7]. Furthermore, the codes in TABLE 4.3 are Type-I $[[N, K, d_{min}]] = [[4n-1, 2n-1, 2]]$ codes, where the code rate $\frac{K}{N}$ is approximately half and $d_{min} = 2$ for any even n that gives a prime $p = 4n - 1$. The minimum distance $d^\dagger$ of stabilizer $\mathcal{S}$ is also listed in the table.

The equality of the quantum Hamming bound (3.19) and the quantum Singleton bound (3.24) holds for $[[5, 1, 3]]$ Type-I stabilizer code when $n = 1$. In this case, $t = n$ is the number of correctable errors. For other Type-I stabilizer codes of $N = 4n + 1$ with $N > 5$, the code efficiency is upper bounded by the quantum Hamming bound for $t < n$ or $d_{min} < 2n + 1 = k + 1$.

n	$[[N, K, d_{min}]]$	$d^\dagger \leq 2n$
1	[[5,1,3]]	(4)
3	[[13,1,5]]	6
7	[[29,1,11]]	12
9	[[37,1, 11]]	12
13	[[53,1,15]]	16
15	[[61,1,17]]	18
25	[[101,1,21]]	22

TABLE 4.2: Type-I stabilizer codes of length $N = 4n + 1$ for $n \leq 25$. $d^\dagger$ is the minimum weight of operator $E \in \mathcal{S}$. Underlined numbers indicate that d_{min} meets the lower bound of the achievable minimum distance given in [91]. The number with brackets is the Perfect code in [13].

n	$[[N, K, d_{min}]]$	$d^\dagger$
2	$[[7, 3, 2]]$	4
6	$[[23, 11, 2]]$	8
8	$[[31, 15, 2]]$	8
12	$[[47, 23, 2]]$	12
18	$[[71, 35, 2]]$	16
20	$[[79, 39, 2]]$	16

TABLE 4.3: Type-I stabilizer codes of length $N = 4n - 1$ for $n \leq 25$. $d^\dagger$ is the minimum weight of operator $E \in \mathcal{S}$.

4.2 Type-II quantum stabilizer codes from difference sets

In this section, we construct Type-II stabilizer codes, difference sets stabilizer (DSS) codes. We first introduce some preliminaries on the theories of the cyclic group and difference sets which are the foundation of our proposed constructions. We then propose an efficient construction method that leads to our general quantum DSS codes.

4.2.1 Preliminaries

1) Cyclic group

Let $\mathbf{Z}_p^\times$ be a multiplicative group of order p.

Definition 4.12. For any multiplicative group $\mathbf{Z}_p^\times$ of order p, it is *cyclic* if there exists an element $\alpha \in \mathbf{Z}_p^\times$ such that, any element $b \in \mathbf{Z}_p^\times$ can be expressed as $b = \alpha^i$ for some integer i. Such an element α is named the generator of the cyclic group.

Consider the multiplicative group $\mathcal{G}_{\mathbb{Z}_7}^\times$. Both elements 3 and 5 generate the entire group, *e.g.,*

$$3^1 = 3,\ 3^2 = 3 \odot 3 = 2,\ 3^3 = 3^2 \odot 3 = 2 \odot 3 = 6,$$
$$3^4 = 3^3 \odot 3 = 6 \odot 3 = 4,\ 3^5 = 3^4 \odot 3 = 4 \odot 3 = 5$$
$$3^6 = 3^5 \odot 3 = 5 \odot 3 = 1.$$

A useful theorem is the following.

Theorem 4.13. *[99] For every prime p, the multiplicative group*

$$\mathbf{Z}_p^\times = \{1, 2, \cdots, p-1\}$$

is cyclic.

2) Difference sets

Definition 4.14. [97] A (p, k, λ) difference set is a subset D of a multiplicative group $\mathbf{Z}_p^{\times}$ such that the order of the group is p, the size of D is k, and each element of $\mathbf{Z}_p^{\times}$ can be expressed as a difference $(d_i - d_j) \bmod p$ of elements from D in exactly λ times.

As an example, $D = \{1, 2, 4\}$ is a $(p, k, \lambda) = (7, 3, 1)$ difference set because each element in $\mathcal{G}_{\mathbb{Z}_7}^{\times}$ can be written as the difference of two integers from the set D in exactly $\lambda = 1$ way, as can be seen below:

$$\left\{ \begin{array}{lll} 1-2=6 & 2-1=1 & 4-1=3 \\ 1-4=4 & 2-4=5 & 4-2=2 \end{array} \right\} \mod 7. \tag{4.36}$$

3) Shift of a difference set

Lemma 4.15. *For every difference set D of size k, we may construct $p-1$ different shifts of the original set, such that each shift is also a difference set that generates elements of $\mathbf{Z}_p^{\times}$. We denote such shift operations as $\mathcal{S}(D, s)$, where $s = \{1, 2, \ldots, p-1\}$.*

For example, if $D = \{1, 2, 4\} \subset \mathcal{G}_{\mathbb{Z}_7}^{\times} = \{1, 2, \ldots, 6\}$, the 6 shifts of D are

$$\begin{aligned} &D = \{1, 2, 4\}, \\ &\mathcal{S}(D, 1) = \{2, 3, 5\},\ \mathcal{S}(D, 2) = \{3, 4, 6\}, \\ &\mathcal{S}(D, 3) = \{4, 5, 0\},\ \mathcal{S}(D, 4) = \{5, 6, 1\}, \\ &\mathcal{S}(D, 5) = \{6, 0, 2\},\ \mathcal{S}(D, 6) = \{0, 1, 3\}. \end{aligned} \tag{4.37}$$

We denote a multi-weight CPM of the form

$$h\,(x)^{\mathcal{S}(D,1)} = x^{d_1} + x^{d_2} + x^{d_3}, \tag{4.38}$$

where $\{d_1 = 2, d_2 = 3, d_3 = 5\} \in \mathcal{S}(D, 1)$. Thus, we generate a multi-weight circulant matrix of weight $k = 3$, which is equivalent to the size of D, as $H = \sum_{i \in \mathcal{S}(D,1)} P^i$, where P is the CPM defined in (4.3).

Our proposed method for constructing a DSS code is based on a series of circulant matrices, where each circulant matrix is generated from a difference set D, or its shift $\mathcal{S}(D, s)$, and the resulting parity-check matrix $H = [H_1|H_2]$ is self-orthogonal w. r. t. the SIP constraint.

4.2.2 Proposed DSS code constructions

Our proposed construction focuses on the difference sets with parameters [96]-[98]

$$(p, k, \lambda) = (4n - 1, 2n - 1, n - 1) \tag{4.39}$$

for an *even* integer $n \geq 2$ that results in a prime number $p = 4n - 1$.

To generate a difference set D, consider the multiplicative group

$$\mathcal{G}_{\mathbb{Z}_7}^{\times} = \{1, 2, \cdots, 6\}$$

of order 7. By taking the powers of a non-generator element $\beta \in \mathcal{G}_{\mathbb{Z}_7}^{\times}$, say $\beta = 4$, we have $\beta^2 = (16 \mod 7) = 2$ and $\beta^3 = \beta^2 \odot \beta = (2 \odot 4 \mod 7) = 1$. An interesting feature of D is that by taking the powers of any element $d \in D\backslash\{1\}$, the new set $\{d^1, d^2, d^3\} = \{1, 2, 4\}$ and is equivalent to D. We now present the following theorem:

Theorem 4.16. *For every prime p, the multiplicative group $\mathbf{Z}_p^{\times}$ possesses one difference set $D = \{\beta, \beta^2, \ldots, \beta^k\}$ of size k such that each element of D is a non-generator element of $\mathbf{Z}_p^{\times}$ and each element of $D\backslash\{1\}$ also generates the difference set D* iff *k is not factorable.*

Proof. Assume k is not factorable. Let $D = \{\beta, \beta^2, \ldots, \beta^k\}$, if $\theta = \beta^i$ for $i = \{1, 2, \ldots, k-1\}$, then $\theta^2 = \beta^{2(i)}$, $\theta^3 = \beta^{3(i)}$, ..., $\theta^j = \beta^{j(i)}$. To prove that when $j = k$, $\{\theta, \theta^2, \ldots \theta^j\} = D$, we consider the first case when $i = 1$ and $1 \leq j \leq k$, and we obtain $\{\theta, \theta^2, \ldots \theta^j\} = \{\beta, \beta^2, \ldots \beta^j\} = D$. For the second case when $i \neq 1$ and $1 \leq j \leq k$, if $ij < k$, we know that $\theta^j = \beta^{ij} \in D$, otherwise, for $ij > k$,

$\theta^j = \beta^{ij} = \beta^{mk+r}$, where m is an multiple of k and $1 \leq r < k$ is a remainder. Since $\beta^k = 1$, $\theta^j = \beta^{ij} = \beta^{nk+r} = \beta^r$ will be an element in D. However, if k can be factorized, hence, k can be decomposed into a series of factors $\Upsilon = \{\upsilon_1, \upsilon_2, \ldots, \upsilon_a\}$. These factors can be used to generate a unique sequence of divisors of k,

$$\Xi = \left\{ \xi_l : \forall \xi_l = \prod_{n=1}^{w} \upsilon_n, 1 \leq w \leq a, \exists m = \frac{k}{\xi_l} \right\}.$$

If $i = \xi_l \in \Xi$, then, $\theta^j = \beta^{j(i)} = \beta^{j\frac{k}{m}}$. When $j = m$, $\theta^j = \beta^k$ where $m \neq k$ is a divisor of k. In other words, if k is factorable and $i = \xi_l \in \Xi$, β^i only generates a subset of D. □

By using difference sets acquired from Theorem 4.16, the following theorem for designing DSS codes is now given:

Theorem 4.17. *For any two shift operations of a difference set* $D = \{d_1, d_2, \cdots, d_t\}$, $\mathcal{S}(D, s_1)$, $\mathcal{S}(D, s_2)$, $\{s_1, s_2\} \in \{1, 2, \ldots p-1\}$ *and* $s_1 \neq s_2$, *the corresponding circulant matrices derived from the polynomials* $h_1(x) = \sum_{i \in \mathcal{S}(D,s_1)} x^i$, $h_2(x) = \sum_{i \in \mathcal{S}(D,s_2)} x^i$ *are self-orthogonal w. r. t. the SIP constraint.*

Proof. From (4.38), we denote

$$\begin{aligned} h_1(x) &= \textstyle\sum_{i \in \mathcal{S}(D,s_1)} x^i = x^{d_1+s_1} + x^{d_2+s_1} + \cdots x^{d_t+s_1}, \\ h_2(x) &= \textstyle\sum_{i \in \mathcal{S}(D,s_2)} x^i = x^{d_1+s_2} + x^{d_2+s_2} + \cdots x^{d_t+s_2}. \end{aligned}$$

Then

$$\begin{aligned} & h_1(x)\, h_2(x^{-1}) \\ &= \left(\textstyle\sum_{i \in \mathcal{S}(D,s_1)} x^i\right) \left(\textstyle\sum_{i \in \mathcal{S}(D,s_2)} x^{-i}\right) \\ &= x^{(d_1+s_1)-(d_1+s_2)} + x^{(d_1+s_1)-(d_2+s_2)} + \cdots \\ & x^{(d_1+s_1)-(d_t+s_2)} + \cdots \; x^{(d_t+s_1)-(d_{t-1}+s_2)} + x^{(d_t+s_1)-(d_t+s_2)} \\ &= kx^{(s_1-s_2)} + x^{(d_1-d_2)+(s_1-s_2)} + \cdots \\ & x^{(d_1-d_t)+(s_1-s_2)} + \cdots x^{(d_t-d_{t-1})+(s_1-s_2)}. \end{aligned} \tag{4.40}$$

Similarly, we have

$$\begin{aligned}
&h_2(x)\,h_1(x^{-1}) \\
&= \left(\textstyle\sum_{i\in\mathcal{S}(D,s_2)} x^i\right)\left(\textstyle\sum_{i\in\mathcal{S}(D,s_1)} x^{-i}\right) \\
&= x^{(d_1+s_2)-(d_1+s_1)} + x^{(d_1+s_2)-(d_2+s_1)} + \cdots \\
&x^{(d_1+s_2)-(d_t+s_1)} + \cdots\ x^{(d_t+s_2)-(d_{t-1}+s_1)} + x^{(d_t+s_2)-(d_t+s_1)} \\
&= kx^{(s_2-s_1)} + x^{(d_1-d_2)+(s_2-s_1)} + \cdots \\
&x^{(d_1-d_t)+(s_2-s_1)} + \cdots x^{(d_t-d_{t-1})+(s_2-s_1)}.
\end{aligned} \tag{4.41}$$

By combining equations (4.40) and (4.41), we obtain

$$\begin{aligned}
&h_1(x)\,h_2(x^{-1}) + h_2(x)\,h_1(x^{-1}) \\
&= k\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) + x^{d_1-d_2}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)\cdots \\
&+x^{d_1-d_t}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right) + \cdots \\
&x^{d_t-d_{t-1}}\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right).
\end{aligned} \tag{4.42}$$

By taking modulo 2 sum upon the first term in (4.42), $k\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)$ is reduced to $\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)$ since k is always an odd number, as given in (4.39). The rest of the terms in (4.42) are distinct differences between two elements d_u, d_v of the difference set D. Thus, equation (4.42) can be rearranged as

$$\begin{aligned}
&h_1(x)h_2(x^{-1}) + h_2(x)h_1(x^{-1}) \\
&= \left(1 + \sum_{u=1}^{k}\sum_{\{v=1,v\neq u\}}^{k} x^{d_u-d_v}\right)\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right).
\end{aligned} \tag{4.43}$$

In Equation (4.43), the term $\left(1 + \sum_{u=1}^{k}\sum_{\{v=1,v\neq u\}}^{k} x^{d_u-d_v}\right)$ represents an all-one square matrix, where each polynomial degree is a distinct difference between two elements $\{d_u,\ d_v\} \in D$. Moreover, the second term $\left(x^{(s_1-s_2)} + x^{(s_2-s_1)}\right)$ is also a circulant matrix of weight 2, so each entry of the resulting circulant matrix $H_1H_2^T + H_2H_1^T$ is a summation of the corresponding column of the second term. Thus, we have proved the theorem by showing that equation (4.43) is always a circulant matrix that contains only even integers, which is an all-zero square matrix when taking the modulo 2 sum. □

From Theorem 4.17, we know that any two shifts of a difference set D would yield a trivial quantum stabilizer code with rate $R^Q = 0$. In order to construct non-trivial quantum stabilizer codes we introduce the following three constructions, A, B and C:

Construction A. *Let* $h_1(x) = [g_1(x)^{\mathcal{S}(D,s_1)}, g_2(x)^{\mathcal{S}(D,s_2)}]$ *and* $h_2(x) = [g_1(x)^{\mathcal{S}(D,s_3)}, g_2(x)^{\mathcal{S}(D,s_4)}]$, *where the set* $\{s_1, s_2, s_3, s_4\}$ *represents the distinct shifts of* D. *This construction method generates a rate* $R^Q = \frac{1}{2}$ *quantum stabilizer code with parity-check matrix* $H = [H_1|H_2]$ *that is self-orthogonal w. r. t. the SIP.*

Example 4.5. *Using Construction A and the* $(7, 3, 1)$ *difference set in (4.36), consider two parity-check matrices* $h_1(x) = [g_1(x)^{\mathcal{S}(D,1)}, g_2(x)^{\mathcal{S}(D,3)}]$ *and* $h_2(x) = [g_1(x)^{\mathcal{S}(D,4)}, g_2(x)^{\mathcal{S}(D,2)}]$, *where each shift* $\mathcal{S}(D, s)$ *is obtained from (4.37). The combined parity-check matrix has the form of*

$$\begin{aligned} h(x) &= [h_1(x)|h_2(x)] \\ &= [\ x^2 + x^3 + x^5, \quad 1 + x^4 + x^5 \ | \\ &\qquad x + x^5 + x^6, \quad x^3 + x^4 + x^6 \ ]. \end{aligned}$$

By Theorem 4.13,

$$\begin{aligned} & h_1(x)h_2(x^{-1}) + h_2(x)h_1(x^{-1}) \\ &= \begin{bmatrix} x^2 + x^3 + x^5, & 1 + x^4 + x^5 \end{bmatrix} \begin{bmatrix} x^{-1} + x^{-5} + x^{-6} \\ x^{-3} + x^{-4} + x^{-6} \end{bmatrix} + \\ &\quad \begin{bmatrix} x + x^5 + x^6, & x^3 + x^4 + x^6 \end{bmatrix} \begin{bmatrix} x^{-2} + x^{-3} + x^{-5} \\ 1 + x^{-4} + x^{-5} \end{bmatrix} \\ &= \mathbf{0} \pmod 2, \end{aligned}$$

*where '***0***' denotes all zeros square matrix.*

To construct a quantum stabilizer code of rate greater than $\frac{1}{2}$, Construction A can be extended as follows:

Construction B. *Let* $h_1(x) = [g_1(x)^{\mathcal{S}(D,s_1)}, g_2(x)^{\mathcal{S}(D,s_2)}, \ldots, g_l(x)^{\mathcal{S}(D,s_l)}]$ *be a serial concatenation of* l *circulant matrices. Similarly, let* $H_2(x) = [g_1(x)^{\mathcal{S}(D,q_1)},$

$g_2(x)^{\mathcal{S}(D,q_2)}, \ldots, g_l(x)^{\mathcal{S}(D,q_l)}]$ *be another set of* l *circulant matrices. Such a construction generates a quantum stabilizer code of rate* $R^Q = \frac{(l-1)}{l}$ *that is self-orthogonal w. r. t. the SIP constraint.*

Example 4.6. *Consider* $l = 3$, $h_1(x) = [g_1(x)^{\mathcal{S}(D,1)}, g_2(x)^{\mathcal{S}(D,4)}, g_3(x)^{\mathcal{S}(D,5)}]$ *and* $h_2(x) = [g_1(x)^{\mathcal{S}(D,2)}, g_2(x)^{\mathcal{S}(D,3)}, g_3(x)^{\mathcal{S}(D,6)}]$, *the quantum code has rate* $R^Q = \frac{2}{3}$, *and is of the form*

$$\begin{aligned} h(x) &= [h_1(x)|h_2(x)] \\ &= [\ x^2+x^3+x^5,\ \ x^1+x^5+x^6,\ \ 1+x^2+x^6\ \ | \\ &\qquad x^3+x^4+x^6,\ \ 1+x^4+x^5,\ \ 1+x^1+x^3\ \ ]. \end{aligned}$$

4.2.3 Extension of DSS codes

Although the proposed construction methods satisfy the SIP constraint, the constructed quantum stabilizer codes are too dense in that both the performance and the decoding complexity can be affected. As such, we provide an improved construction method in order to reduce the weight of the circulant matrix. From Theorem 4.16, we know that if $\theta = \beta^i$ where i is a divisor of k, a cyclic subset $D' \subset D$ can be obtained. To generate a circulant matrix of low weight, we extend the constructions A and B as follows:

Construction C. *Let* $h_1(x) = [g_1(x)^{\mathcal{S}(D',s_1)}, g_2(x)^{\mathcal{S}(D',s_2)}, \ldots, g_l(x)^{\mathcal{S}(D',s_l)}]$ *and* $h_2(x) = [g_1(x)^{\mathcal{S}(D',q_1)}, g_2(x)^{\mathcal{S}(D',q_2)}, \ldots, g_l(x)^{\mathcal{S}(D,q_l)}]$, *where* D' *is a cyclic subset of* D *with cardinality* $|D'| = k' < k$ *and* l *needs to be an even number. The SIP constraint is satisfied* iff $(s_1+s_2+\ldots+s_l)\ mod\ p = (q_1+q_2+\ldots+q_l)\ mod\ p$, *and* $(s_j+s_{j+1})\ mod\ p = (q_j+q_{j+1})\ mod\ p$ *for every odd integer number* $1 \leq j < l$.

4.2.4 Codes performance

Here we provide simulation results of some constructed DSS codes. We note that to reduce the decoding complexity, classical cyclic codes are commonly decoded using a majority-logic decoder, which is a type of hard-decision decoding

algorithm. Since our DSS codes are constructed from circulant matrices, we performed majority-logic decoding [99] [100] on our codes. Note this decoding is used simply for simulation-speed issues, given that we are interested in relative performances only of the codes (similar relative performances will be found if slower BP decoders are utilized). Our simulations are carried out over the quantum depolarizing channel. This channel creates X, Y and Z errors independently with equal flip probability $\frac{f}{3}$. In our simulations an approximation has been made at the decoder side to further reduce the complexity of decoding by considering only the marginal flip probability $f_m = \frac{2f}{3}$ of each received bit.

Based on the proposed construction method, Table 4.4 illustrates a set of stabilizer codes with different size p. The performance of these sample codes is plotted in Fig. 4.1. The quantum code rate of all codes is $R^Q = \frac{1}{2}$. Here we see the relative performance of some DSS codes as a function of block length. Interestingly from Fig. 4.1, the block error rate (BLER) and qubit error rate (QBER) reduces significantly for decreasing block size. One possible explanation for this is that the distance property of DSS codes is irrelevant to the block size of the code, but is relevant to the size of the difference set. Note also, for comparison we have adopted one code $[[13, 7]]$ from [95] and passed it through our decoder. The main point here is that we can see that code performance is comparable to our $[[14, 7]]$ DSS code.

Fig. 4.2 illustrates the BLER (solid lines) and QBER (dash lines) of a DSS code of block size $N = 398$ with different weights. From this figure, we observe that the performance of the code improves when the weight of each circulant matrix is low. The subset D' for each circulant weight is provided in TABLE 4.5.

4.3 Chapter summary

In this chapter, two types of quantum stabilizer codes were proposed based on quadratic residue sets of prime modulus and prime difference sets. By juxtaposing cyclic permutation matrices, a number of different construction methods proposed

n	(p, k, λ)	D
2	(7,3,1)	{1 2 4}
6	(23,11,5)	{1 2 3 4 6 8 9 12 13 16 18}
12	(47,23,11)	{1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42}
50	(199,99,49)	{1 2 4 5 7 8 9 10 13 14 16 18 20 23 25 26 28 29 31 32 33 35 36 40 43 45 46 47 49 50 51 52 53 56 57 58 61 62 63 64 65 66 70 72 79 80 81 86 89 90 91 92 94 98 100 102 103 104 106 111 112 114 115 116 117 121 122 123 124 125 126 128 130 131 132 139 140 144 145 151 155 157 158 160 161 162 165 169 172 175 177 178 180 182 184 187 188 193 196}
126	(503,251,125)	{1 2 3 4 6 7 8 9 11 12 13 14 16 18 21 22 23 24 25 26 27 28 32 33 36 39 42 43 44 46 47 48 49 50 52 54 56 59 61 63 64 66 67 69 72 73 75 77 78 79 81 83 84 85 86 88 91 92 94 95 96 97 98 99 100 104 108 112 113 117 118 121 122 126 128 129 131 132 134 138 141 143 144 145 146 147 150 154 155 156 158 161 162 166 168 169 170 172 173 175 176 177 182 183 184 185 188 189 190 192 194 196 197 198 199 200 201 205 207 208 216 219 223 224 225 226 229 231 233 234 236 237 242 243 244 249 252 253 255 256 257 258 262 263 264 265 268 271 273 275 276 281 282 283 285 286 288 289 290 291 292 293 294 297 299 300 301 308 310 312 316 317 322 323 324 325 329 332 336 338 339 340 343 344 346 350 351 352 354 355 361 363 364 366 367 368 370 373 376 378 379 380 383 384 387 388 389 392 393 394 396 397 398 400 401 402 410 413 414 416 421 423 427 429 432 433 435 438 441 443 445 446 448 450 452 458 462 463 465 466 468 469 472 473 474 483 484 486 488 493 498}

TABLE 4.4: Different block size quantum stabilizer codes constructed from our proposed method.

k'	D'
$k' = 3$	{1 92 106}
$k' = 9$	{1 43 58 92 106 162 175 178 180}
$k' = 11$	{1 18 61 62 63 103 114 121 125 139 188}
$k' = 33$	{1 5 8 18 25 28 40 52 61 62 63 64 90 92 98 103 106 111 114 116 117 121 123 125 132 139 140 144 157 172 182 187 188}

TABLE 4.5: Subset $D' \subset D$ of different size for DSS codes of $N = 398$.

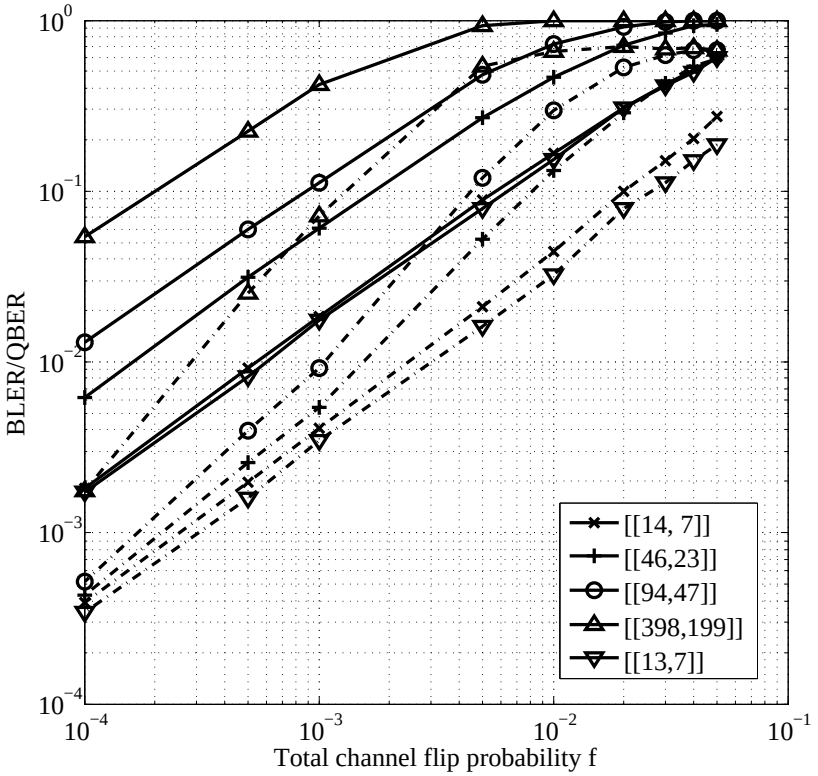

FIGURE 4.1: BLER (solid lines) and QBER (dash lines) performances of DSS codes listed in TABLE 4.4 and comparison with the $[[13, 7]]$ code in [95].

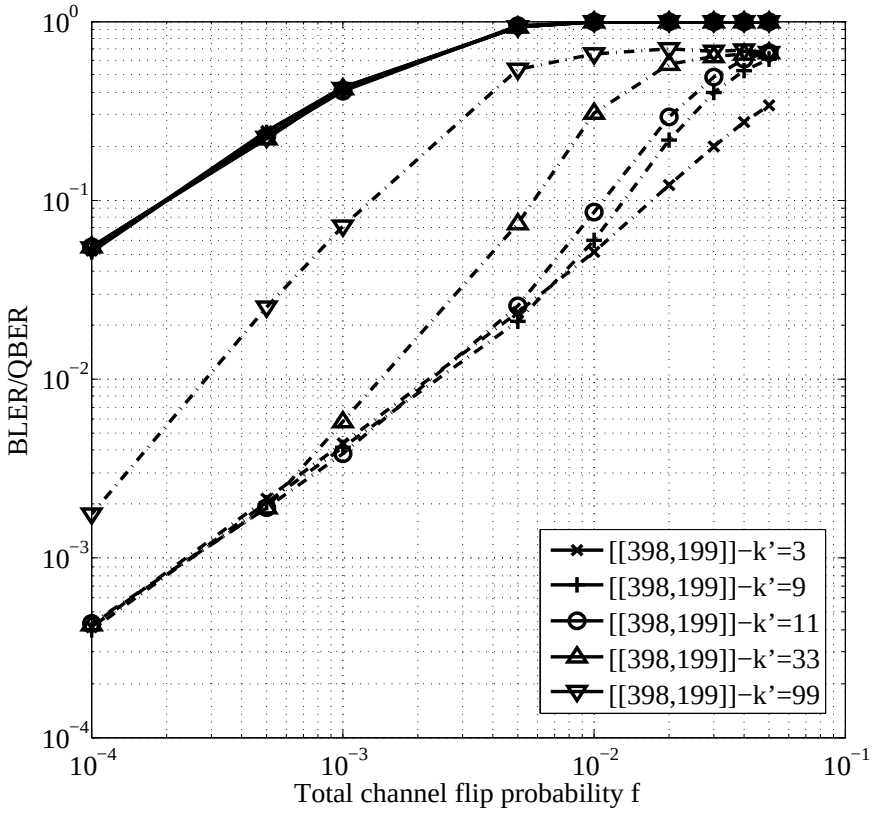

FIGURE 4.2: BLER (solid lines) and QBER (dash lines) performances of DSS codes of block size $N = 398$ with different weights given in TABLE 4.5.

based on the property of QR sets and difference sets such that the constructed quantum codes are always self-orthogonal w. r. t. the SIP constraint. The minimum distance for Type-I stabilizer codes of length $N = 4n + 1$ is closely related to the size of quadratic residue sets while the dimension of the codes is a constant. The code rate for Type-I stabilizer codes of length $N = 4n - 1$ is near half.

Furthermore, the proposed construction methods for DSS codes generate a difference set from a single input parameter and ensures the constructed codes are self-orthogonal w. r. t. the SIP constraint. From simulation results, DSS code performances can be improved by constructing from the subsets of a difference set.

Chapter 5

Sparse-Graph Quantum LDPC Codes

Although the pioneers' work describes a new field of research, and has proven that 'good' quantum error-correcting codes do exist, however, the method of proof was non-constructive, and the theory was developed based on very short block of qubits (*e.g.*, the 5 qubit codes, Shor's 9 qubit code, and Steane's 7 qubit code). Thus it is not practicable to build a huge quantum circuit when the number of qubits becomes large or even of moderate length. Also, no practical decoding algorithm (*i.e.*, an algorithm for which the decoding time is polynomial in the block length) exists for these codes.

This stands in contrast to the situation with classical error correction, where practically decodable codes exist which, when optimally decoded, achieve information rates close to the Shannon limit. Low-density parity-check (LDPC) codes [43, 51] are an example of such codes. The sparseness of the parity-check matrices makes the codes easy to encode and decode. It is also worth emphasizing that the *sum-product algorithm* solves the decoding problem for low-density parity-check codes at noise levels far greater than the maximum noise level correctable by any code decoded by a traditional bounded-distance decoder. Since the parity-check matrix

is sparse, a quantum low-density parity-check code would have the additional attractive property that only a small number of interactions per qubit are required in order to determine the error that has occurred. Such conjecture is made by Mackay *et. al* in [39]. Moreover, since practical decoding algorithms have been found for classical low-density parity check codes, it seems likely that a practical decoding algorithm will also exist for quantum low-density parity-check codes.

In this chapter, we design classes of quantum LDPC codes, from conventional quasi-cyclic (QC) proto-graph LDPC codes. We first introduce the basics of conventional proto-graph LDPC codes. Then a class of quantum LDPC codes, namely quasi-cyclic stabilizer (QCS) codes, are derived from a *proto-matrix* of *Latin square* structure, where each proto-matrix is obtained using quadratic residue sets and quadratic non-residue sets of prime modulus given by the form $p = 4n \pm 1$. We then show another class of quantum LDPC codes constructed based on the tensor product of a pair of non-binary parity-check matrices. The resulting quantum LDPC codes are of rates as high as above 0.9.

5.1 Background on quantum LDPC codes

Conventional sparse-graph LDPC codes [43, 51] are capacity achieving codes [52, 53] which ascertain both the sparseness of a code and efficient decoding algorithm. However, the design of general quantum stabilizer (non-CSS) codes from conventional LDPC codes is limited by the orthogonality constraint, that is, the underlying pair of classical codes must be orthogonal with respect to the symplectic inner product. The idea of quantum LDPC codes was first given by Postol in [62], whereas generalization of quantum LDPC codes was proposed a few years later by MacKay *et al.* [39]. Thereafter, a wide range of different types of sparse-graph quantum codes have been proposed, *e.g.,* [64]-[75], many of them are quantum CSS codes. Most of these constructions are based on the design of structured *quasi-cyclic* (QC) LDPC codes using *circulant permutation matrix* (CPM) since the orthogonality requirement can be satisfied easily compared to that of using a

random LDPC codes. To determine the cyclic shift of a CPM, various techniques have been applied, for instance, algebraic construction of quantum LDPC codes from Latin squares [65] and finite geometries [66]. Alternatively, cyclic shifts can be obtained by solving a set of linear equations (*e.g.,*[75]) or by searching for different combination of integer numbers that satisfy a certain necessary condition (*e.g.,* [68]).

In this chapter, we propose several constructions of quantum LDPC codes that do not require to calculate or search the cyclic shifts of CPMs for the underlying protograph LDPC codes [86]. As introduced in [65] a class of quantum LDPC codes of CSS structure can be constructed using a pair of QC-LDPC codes derived from orthogonal Latin squares. Inspired by this, we construct quantum LDPC codes of non-CSS structure, called quasi-cyclic stabilizer (QCS) codes, using conventional regular protograph LDPC codes derived from non-orthogonal Latin squares. More specifically, we use *quadratic residue (QR) sets* of prime modulus as the basic building block of our protomatrix, and show that by arranging the elements of a QR set in a particular way, the resulting protomatrix is a non-orthogonal Latin square, where each entry represents a cyclic shift of a CPM. Further, we obtain a set of transformation matrices from the *transversal* of Latin squares for QR sets of parameter $p = 4n - 1$, or from the cyclic shifts of reverse identity matrix for QR sets of parameter $p = 4n + 1$. By applying these transformations among the pre-obtained protomatrices, the binary protograph QC-LDPC codes lifted from the equivalent protomatrices are also self-orthogonal with respect to the symplectic inner product. Upon construction of such a type of QCS codes we show that the orthogonality requirement of the proposed QCS codes preserves for an arbitrary order of CPMs.

In our proposed design, we consider quadratic residue sets of size $k = \frac{p-1}{2}$, where $p = 4n \pm 1$ is a prime and $n \in \mathbb{Z}^+$ is a positive integer. There are three types of QCS codes proposed in this chapter and they are here called 'Type-I-A', 'Type-I-B' and 'Type-II'. All these codes are quantum LDPC codes of non-CSS structure. The underlying binary parity-check matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ for each type of QCS codes are derived from a pair of protomatrice $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, respectively, such that

$\mathbf{H}_1$ and $\mathbf{H}_2$ are self-orthogonal with respect to the symplectic inner product. The main constructions of the proposed three types of QCS codes are summarized in the following.

1. For a prime $p = 4n - 1$, $n \in \mathbb{Z}^+$ and a pair of protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, Type-I-A QCS codes of length $N = kp$ are constructed by superimposing a $k \times k$ all-zero protomatrix $\mathbf{O}_k$ to either $\mathbf{H}_{1proto}$ or $\mathbf{H}_{2proto}$. The dimension of Type-I-A QCS codes is $K = kp - k(p-1) - 1$ and $K = kp - k(p-2) - 1$ for odd n and even n, respectively.

2. For a prime $p = 4n - 1$, $n, v \in \mathbb{Z}^+$ and a pair of protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, Type-I-B QCS codes of length $N = 2kv$ and dimension $K = 2kv - \rho' v + \rho' - 1$ are constructed by using transformation matrices $\mathbf{D} \in \mathscr{P}$, where $\rho' \leq k$ is the column weight of the derived QC-LDPC codes and v is the order of CPMs, and the set of transformation matrices $\mathscr{P}$ is obtained based on transversals of $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$.

3. For a prime $p = 4n + 1$, $n, v \in \mathbb{Z}^+$ and a pair of protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, Type-II QCS codes of length $N = kv$ and dimension $K = kv - \rho' v + \rho' - 1$ are constructed by swapping the columns of $\mathbf{H}_{1proto}$ or $\mathbf{H}_{2proto}$. The permutation of columns are performed using cyclic shifts of reverse identity matrix of size k.

We give a lower bound on the minimum distance of the proposed Type-II QCS codes. By proving that the Tanner graphs of the underlying protograph LDPC codes are free of cycles of length four according to [87], we show that the minimum distance of Type-II QCS codes can be lower bounded in terms of the minimum distances of the underlying protograph LDPC codes obtained based on the results from [88] [89].

The performance of the proposed three types of QCS codes is also shown. The constructed codes are decoded over a quantum depolarizing channel using an iterative sum-product decoder. The simulation environment is analogous to that of decoding a sparse classical quaternary code under the sum-product algorithm

(SPA) [150] [151]. Simulation results show that the proposed QCS codes of moderate code length (a few hundreds to a few thousands) outperform some of the literature codes in the waterfall region. In addition, and outperform the rate half quantum LDPC codes from [75] in the error floor region (block error rate around $\sim 10^{-7}$) with a low decoding complexity.

We first give a preliminary on Latin squares and classical proto-graph LDPC codes. Then we give explicit design procedures of QCS codes from quadratic residue sets (see Section 4.1.1) with parameter $p = 4n \pm 1$, including the designs of Type-I-A QCS codes and Type-I-B QCS codes for $p = 4n-1$, and the design of Type-II QCS codes for $p = 4n + 1$. We present some constructed codes and simulation results of these codes over the quantum depolarizing channel model with the iterative sum-product decoding algorithms afterwards.

5.1.1 Latin squares

Definition 5.1. Let $L = \{l_1, l_2, \ldots, l_q\}$ be a set of q elements. A $q \times q$ square matrix

$$\mathscr{S} = \begin{bmatrix} s_{(1,1)} & s_{(1,2)} & \cdots & s_{(1,q)} \\ s_{(2,1)} & s_{(2,2)} & \cdots & s_{(2,q)} \\ \vdots & \vdots & \ddots & \ddots \\ s_{(q,1)} & s_{(q,2)} & \cdots & s_{(q,q)} \end{bmatrix}, \tag{5.1}$$

is a Latin square of order q if each row and column of $\mathscr{S}$ contains each element of L exactly once. A Latin square is called *commutative* if the cell (i, j) and (j, i) for $1 \leq i, j \leq q$ contain the same element of L, that is, $\mathscr{S} = \mathscr{S}^T$.

Definition 5.2. Two Latin squares of order q, $\mathscr{S} = [s_{(i,j)}]$ and $\mathscr{U} = [u_{(i,j)}]$, are orthogonal *iff* the q^2 order pair $(s_{(i,j)}, u_{(i,j)})$ are distinct for all $1 \leq i, j \leq q$.

Definition 5.3. A *transversal* $\mathcal{T} \subset \{(i, j)|1 \leq i, j \leq q\}$ of a Latin square of order q is such a set of q cells that each row and each column only contains one cell, and the q cells contain q different elements in L.

Proposition 5.4. *Let $\mathscr{S}$ be a Latin square of order q and $\mathcal{T}$ be a transversal of $\mathscr{S}$. Denote by $\boldsymbol{\pi}_{\mathcal{T}}$ a $q \times q$ transformation matrix. Then the (i,j)-th entry of $\boldsymbol{\pi}_{\mathcal{T}}$ has value of 1 if the cell $(i,j) \in \mathcal{T}$ and 0 if the cell $(i,j) \notin \mathcal{T}$ for $1 \leq i,j, \leq q$.*

Corollary 5.5. *A left multiplication of $\mathscr{S}$ by $\boldsymbol{\pi}_{\mathcal{T}}$, $\boldsymbol{\pi}_{\mathcal{T}}\mathscr{S}$, is equivalent to a permutation of rows of $\mathscr{S}$, whereas a right multiplication S by $\boldsymbol{\pi}_{\mathcal{T}}$, $\mathscr{S}\boldsymbol{\pi}_{\mathcal{T}}$, is equivalent to a permutation of columns of $\mathscr{S}$.*

5.1.2 Proto-graph quasi-cyclic LDPC codes

A circulant permutation matrix defined in (4.3) has order v such that

$$\mathbf{P}^v = \mathbf{P}^0 = \mathbf{I}_v,$$

where I_v is the identity matrix of size v. Let $f(x) = \sum_{i=1}^{l} x^{r_i}$ be a univariate polynomial of l distinct terms such that $0 \leq r_1 < r_2 < \ldots < r_l < v$. We define a weight-$l$ CPM as $\mathbf{A} = f(\mathbf{P}) := \sum_{i=1}^{l} \mathbf{P}^{r_i}$. Furthermore, the transpose of $\mathbf{A}$ is denoted as $\mathbf{A}^T = f(\mathbf{P}^{-1}) = \sum_{i=1}^{l} \mathbf{P}^{v-r_i} = \sum_{i=1}^{l} \mathbf{P}^{-r_i}$.

Let $\mathbf{B} = [b_{i,j}]_{1\leq i\leq c, 1\leq j\leq d} \in \mathbb{Z}^+$ be a protomatrix of size $c \times d$, where each entry denotes the weight of a CPM. The summations

$$\mathbf{d_c} = \left\{\sum_{i=1}^{c} b_{i,j}\right\}, 1 \leq j \leq d, \quad \text{and} \quad \mathbf{d_r} = \left\{\sum_{j=1}^{d} b_{i,j}\right\}, 1 \leq i \leq c, \tag{5.2}$$

represent the set of column degrees and row degrees of the derived parity-check matrix, respectively. To construct a parity-check matrix $\mathbf{H}$ from $\mathbf{B}$, each non-zero entry of $\mathbf{B}$ is *lifted* using a weight-$b_{i,j}$ CPM of order v such that $v \gg \max(b_{i,j})$, and the zeros are lifted using an all-zero matrix of size $v \times v$. The null space of $\mathbf{H}$ gives a binary QC-LDPC code of length dv.

Example 5.1. *Considering a proto-matrix $\mathbf{B} = [3\ 2]^{1\times 2}$ of column weights 2 and 3, and row weight 5. A parity check matrix $\mathbf{H}$ can be obtained by lifting $\mathbf{B}$ with*

CPMs $\mathbf{P}$ *of order* v*, such that* $v \gg 3$*. This can be expressed as,*

$$\mathbf{B} = \begin{bmatrix} 3 & 2 \end{bmatrix} \xrightarrow{(\mathbf{P},v)} \mathbf{H} = \begin{bmatrix} \sum_{i=1}^{3} \mathbf{P}^{r_i} & \sum_{i=1}^{2} \mathbf{P}^{r_i} \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

The multi-weight CPM on the left consists of P *with permutations* $\{r_1, r_2, r_3\} = \{0, 2, 3\}$*, whereas the multi-weight CPM on the right consists of* P *with permutations* $\{r_1, r_2\} = \{0, 2\}$*.*

5.2 New constructions on quasi-cyclic quantum LDPC codes

As briefly introduced in Section II, the SIP constraint upon a quantum code complicates the design of quantum LDPC codes from an arbitrary protomatrix $\mathbf{B}$. In this chapter, we focus on the design of quantum LDPC codes using the $k \times k$ protomatrix

$$\mathbf{B} = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}, \tag{5.3}$$

where $k = \frac{p-1}{2}$ is the size of $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$. We first obtain a pair of protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ by replacing each '1' inside $\mathbf{B}$ with an element from $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$, respectively. We then lift $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ with CPMs to obtain a pair of binary matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ that is orthogonal with respect to the SIP. In the following subsections, we 1) discuss the design of $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ from $\mathbf{B}$; 2) show explicit construction methods of the proposed Type-I-A, Type-I-B and Type-II QCS codes; 3) derive a lower bound on the minimum distance of Type-II QCS codes and 4) provide exemplifying codes at the end of this chapter.

5.2.1 Proto-matrices of QCS codes

Let $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ be a quadratic residue and non-residue set that contains $k = \frac{p-1}{2}$ elements, respectively. From Lemma 4.1, $\mathcal{Q}^{\mathcal{R}} \bigcup \mathcal{Q}^{\mathcal{NR}} = \{1, 2, \ldots, p-1\}$ if p is a prime. Let $\beta = \alpha^2$, where α is a primitive element of the finite field $\mathbb{F}_p$. Since $\alpha^2 \in \mathcal{Q}^{\mathcal{R}}$ and $k = \frac{p-1}{2}$, β is a primitive k-th root of unity and $\mathcal{Q}^{\mathcal{R}}$ is closed under multiplication by β. Thus, β is the *generator element* of $\mathcal{Q}^{\mathcal{R}}$ and we can express $\mathcal{Q}^{\mathcal{R}}$ as

$$\mathcal{Q}^{\mathcal{R}} = \{\beta^0 = 1, \beta, \ldots, \beta^{k-1}\}.$$

To represent $\mathcal{Q}^{\mathcal{NR}}$ in terms of β, we consider prime p for two cases.

1) $p = 4n - 1$

By the First supplement to quadratic reciprocity [57], $-1 \in \mathcal{Q}^{\mathcal{NR}}$ for a prime $p = 4n - 1$. Thus, according to Lemma 4.2,

$$\mathcal{Q}^{\mathcal{NR}} = -1 \times \{1, \beta, \ldots, \beta^{k-1}\} \equiv -\mathcal{Q}^{\mathcal{R}} \tag{5.4}$$

and $\beta^i + (-\beta^i) = 0 \pmod{p}$ for $0 \leq i \leq k-1$. Moreover, we construct integer vectors $\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}$ and $\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}$ as

$$\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}} = \begin{bmatrix} \mathcal{Q}^{\mathcal{R}}(1) & \mathcal{Q}^{\mathcal{R}}(2) & \cdots & \mathcal{Q}^{\mathcal{R}}(k) \end{bmatrix} = \begin{bmatrix} 1 & \beta & \ldots & \beta^{k-1} \end{bmatrix} \tag{5.5}$$

and

$$\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}} = -\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}, \tag{5.6}$$

where $\mathcal{Q}^{\mathcal{R}}(j)$ (resp. $\mathcal{Q}^{\mathcal{NR}}(j)$), $1 \leq j \leq k$, represents the j-th element of $\mathcal{Q}^{\mathcal{R}}$ (resp. $\mathcal{Q}^{\mathcal{NR}}$).

2) $p = 4n + 1$

In the case when a prime $p = 4n + 1$, $\pm 1 \in \mathcal{Q}^{\mathcal{R}}$ by the First supplement to quadratic reciprocity [57]. Thus,

$$\mathcal{Q}^{\mathcal{R}} = \{\beta^0 = 1, \beta, \ldots, \beta^{k-1}\} \equiv \pm\{1, \beta, \ldots, \beta^{\frac{k}{2}-1}\}. \tag{5.7}$$

Let

$$\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}} = \left[1, \beta, \ldots, \beta^{\frac{k}{2}-1}, -1, -\beta, \ldots, -\beta^{\frac{k}{2}-1}\right]. \tag{5.8}$$

From Lemma 4.2, we know that $\alpha^{2i-1} \cdot \alpha^{2i} \in \mathcal{Q}^{\mathcal{NR}}$ for $1 \leq i \leq \frac{p-1}{2}$, where $\alpha^{2i} \in \mathcal{Q}^{\mathcal{R}}$ and $\alpha^{2i-1} \in \mathcal{Q}^{\mathcal{NR}}$. Therefore, the integer vector $\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}$ can be obtained from $\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}$ based on the relation

$$\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}} = \gamma \mathbf{h}_{\mathcal{Q}^{\mathcal{R}}} \,(\mathrm{mod}\, p)\,,$$

where $\gamma \in \mathcal{Q}^{\mathcal{NR}}$.

For both cases, we obtain $k - 1$ permutations of $\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}$ and $\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}$ by performing column-swapping. Since $\beta^k = \beta^0 = 1 \,(\mathrm{mod}\, p)$, $\beta^k \beta^i \equiv \beta^{k+i} \equiv \beta^{i(\,\mathrm{mod}\, k)}$, the column-swapping performed here is equivalent to cyclic shift of $\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}$ and $\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}$ towards left. More specifically, for $0 \leq i \leq k-1$, the i-th cyclic left shift of $\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}$ and $\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}$ is expressed as

$$\mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^i \equiv \beta^i \mathbf{h}_{\mathcal{Q}^{\mathcal{R}}} \quad \text{and} \quad \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^i \equiv \beta^i \mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}, \tag{5.9}$$

respectively. For a fixed $\mathbf{B}$ given in (5.3), the protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ are obtained by replacing the i-th all-one row of $\mathbf{B}$ with $\mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^i$ and $\mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^i$, respectively. The final $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ are

$$\mathbf{H}_{1proto} = \begin{bmatrix} \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^0 \\ \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^1 \\ \vdots \\ \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^{k-1} \end{bmatrix} \quad \text{and} \quad \mathbf{H}_{2proto} = \begin{bmatrix} \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^0 \\ \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^1 \\ \vdots \\ \mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^{k-1} \end{bmatrix}. \tag{5.10}$$

Note that, both $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ are square matrices that contain k different permutations of $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$, respectively. Since $\mathbf{H}_{1proto}(i,j) = \mathbf{H}_{1proto}(j,i)$ for $0 \leq i,j \leq k-1$, $\mathbf{H}_{1proto} = \mathbf{H}_{1proto}^T$ and similarly $\mathbf{H}_{2proto} = \mathbf{H}_{2proto}^T$. Thus, by Definition 5.1, $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ are commutative Latin squares of order k with every element of $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ appearing exactly once in every row and every column. Furthermore, since $(\mathbf{H}_{1proto}(i,j), \mathbf{H}_{2proto}(i,j))$ and $(\mathbf{H}_{1proto}(i',j'), \mathbf{H}_{2proto}(i',j'))$ are identical pairs for $i' = i \pm 1 \pmod k$ and $j' = j \mp 1 \pmod k$, by Definition 5.2, $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ are non-orthogonal Latin squares. By lifting $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ with $\mathbf{P}$ of order v, we obtain a pair of parity-check matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ of size $vk \times vk$, each consisting of $k \times k$ weight-1 CPMs.

5.2.2 Type-I-A QCS codes from QR set of prime p=4n-1

We now design Type-I-A QCS codes for $p = 4n-1$ from $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ given in (5.10).

Denote by $\boxplus$ the operation of *adjunction*, *e.g.*, $(\beta^i \boxplus \beta^j) \equiv (\mathbf{P}^{\beta^i} + \mathbf{P}^{\beta^j})$. Let $\mathbf{O}_M$ be an all-zero protomatrix of size $M \times M$. For a given pair of protomatrices $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, we construct $\mathbf{H}_{proto}$ in the following way,

$$\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H'}_{2proto}] = [\mathbf{H}_{1proto} \mid \mathbf{H}_{2proto} \boxplus \mathbf{O}_k], \tag{5.11}$$

where $k = \frac{p-1}{2}$ and $\mathbf{H}_{2proto} \boxplus \mathbf{O}_k$ is performed element-wise.

Lemma 5.6. *For a positive integer n and a prime $p = 4n-1$, let $\mathbf{O}_k$ be the $k \times k$ all-zero protomatrix. Then the parity-check matrix $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H'}_2]$ lifted from the protomatrix $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H}_{2proto} \boxplus \mathbf{O}_k]$ is self-orthogonal with respect to the SIP.*

Proof. Let $\mathbf{F} = [f_{i,j}(x)]^{k \times k}$ and $\mathbf{T} = [t_{i,j}(x)]^{k \times k}$ be the $k \times k$ circulant array of $\mathbf{H}_1$ and $\mathbf{H'}_2$, respectively, where $f_{i,j}(x) = x^{\mathbf{H}_{1proto}(i,j)}$ and $t_{i,j}(x) = 1 + x^{\mathbf{H}_{2proto}(i,j)}$ are univariate polynomials of the (i,j)-th CMP for $0 \leq i,j \leq k-1$. Since

$\mathbf{H}_{1proto} = -\mathbf{H}_{2proto}$ and for $0 \leq i \leq k-1$, the first row of $\mathbf{F}\mathbf{T}^T + \mathbf{T}\mathbf{F}^T$ is

$$\left\{ \sum_{j=0}^{k-1} \left[x^{\beta^j} \left(1 + x^{\beta^{(j+i) \bmod k}} \right) + x^{-\beta^j} \left(1 + x^{-\beta^{(j+i) \bmod k}} \right) \right] \right\}. \tag{5.12}$$

The rest $k-1$ rows are the cyclic shift of Equation (5.12) towards right. Moreover, express the two terms inside the summation as $x^{\beta^j} + x^{\beta^j(1+\beta^i)} + x^{-\beta^j} + x^{-\beta^j(1+\beta^i)}$. Since $\mathcal{Q}^{\mathcal{R}} \cup \mathcal{Q}^{\mathcal{NR}} = \mathbf{Z}_p^{\times}$ for a prime $p = 4n-1$ and for $0 \leq j \leq k-1$, the polynomial $\sum_{j=0}^{k-1}(x^{\beta^j} + x^{-\beta^j})$ represents an all-one matrix of zero diagonal. Similarly, for either $(1+\beta^i) \in \mathcal{Q}^{\mathcal{R}}$ or $\in \mathcal{Q}^{\mathcal{NR}}$, $\{\beta^j(1+\beta^i), -\beta^j(1+\beta^i)\}$ generates $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ according to lemma 4.2. Thus, the polynomial $\sum_{j=0}^{k-1}(x^{\beta^j(1+\beta^i)} + x^{-\beta^j(1+\beta^i)})$ also represents an all-one matrix of zero diagonal. Hence, $\mathbf{F}\mathbf{T}^T + \mathbf{T}\mathbf{F}^T = 0(\text{mod}2)$ and the pair of binary matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ is self-orthogonal with respect to the SIP. □

Proposition 5.7. *For a positive integer n and a prime $p = 4n-1$. Let $v = p$. The quadratic residue set $\mathcal{Q}^{\mathcal{R}}$ and the quadratic non-residue set $\mathcal{Q}^{\mathcal{NR}}$ yield a $[[N, K]] = [[kp, kp - Rank\,(\mathbf{H})]]$ QCS code, where the parity-check matrix $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H}'_2]$ has rank $Rank\,(\mathbf{H}) = k(p-1)+1$ when n is odd and $Rank\,(\mathbf{H}) = k(p-2)+1$ when n is even. We call this type of QCS codes based on adjunction operation Type-I-A QCS codes.*

Proof. See Appendix A.1. □

5.2.3 Type-I-B QCS codes from QR set of prime p=4n-1

In this sub-section, we show an alternative construction method for Type-I QCS codes such that the adjunction operation is no longer required for prime $p = 4n-1$. Denote by

$$\mathbf{R}_{\mathbf{I}_k} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & 0 & 1 & 0 & 0 \\ 0 & \iddots & 0 & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \tag{5.13}$$

a reverse identity matrix of size k, where $k = \frac{p-1}{2}$. The product of $\mathbf{H}_{1proto}\mathbf{R}_{\mathbf{I}_k}$ and $\mathbf{H}_{2proto}\mathbf{R}_{\mathbf{I}_k}$ generates a different Latin square $\mathbf{H'}_{1proto}$ and $\mathbf{H'}_{2proto}$ of order k that is equivalent to $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, respectively. This transformation is equivalent to the matrix column-swapping

$$\mathbf{H}_{1proto}(i,j) \rightarrow \mathbf{H'}_{1proto}(i, k-j-1), 0 \leq i,j \leq k-1,$$

where each (i,j) represents the coordinate of the i-th row and j-th column of $\mathbf{H}_{1proto}$.

Lemma 5.8. *For a positive integer n and a prime $p = 4n-1$, let $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ be the protomatrices of the form given in (5.10), respectively. Let*

$$\mathbf{H'}_{1proto} = \mathbf{R}_{\mathbf{I}_k}\mathbf{H}_{1proto} \quad \textit{and} \quad \mathbf{H'}_{2proto} = \mathbf{R}_{\mathbf{I}_k}\mathbf{H}_{2proto} \tag{5.14}$$

be the equivalent Latin square of $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$, respectively. Then the binary matrix $\mathbf{H} = [\mathbf{A}_1 \mid \mathbf{A}_2] = [\mathbf{H}_1 \ \mathbf{H'}_2 \mid \mathbf{H}_2 \ \mathbf{H'}_1]$ lifted from $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \ \mathbf{H'}_{2proto} \mid \mathbf{H}_{2proto} \ \mathbf{H'}_{1proto}]$ is self-orthogonal with respect to the SIP.

Proof. Let $\mathbf{F} = [f_{i,j}(x)]^{k\times k}$ and $\mathbf{T} = [t_{i,j}(x)]^{k\times k}$ be the $k \times k$ circulant array of $\mathbf{H}_1$ and $\mathbf{H}_2$, where $f_{i,j}(x) = x^{\mathbf{H}_{1proto}(i,j)}$ and $t_{i,j}(x) = x^{\mathbf{H}_{2proto}(i,j)}$ are weight-1 CPMs for $0 \leq i,j \leq k-1$. Consider the case $\hat{\mathbf{F}} = \mathbb{R}_k\mathbf{F}$ and $\hat{\mathbf{T}} = \mathbb{R}_k\mathbf{T}$, where $\mathbb{R}_k = [r_{i,k-i-1}(x)]^{k\times k}$ is the $k \times k$ reverse identity matrix with $r_{i,k-i-1}(x) = 1$ for $0 \leq i \leq k-1$. Since $\mathbb{R}_k = \mathbb{R}_k^T = \mathbb{R}_k^{-1}$, we have

$$\begin{aligned}
\mathbf{A}_1\mathbf{A}_2^T + \mathbf{A}_2\mathbf{A}_1^T &= \left(\mathbf{F}\mathbf{T}^T + \hat{\mathbf{T}}\hat{\mathbf{F}}^T\right) + \left(\mathbf{T}\mathbf{F}^T + \hat{\mathbf{F}}\hat{\mathbf{T}}^T\right) \\
&= \left(\mathbf{F}\mathbf{T}^T + \left(\mathbb{R}_k\mathbf{T}\mathbf{F}^T\mathbb{R}_k^T\right)\right) + \left(\mathbf{T}\mathbf{F}^T + \left(\mathbb{R}_k\mathbf{F}\mathbf{T}^T\mathbb{R}_k^T\right)\right) \\
&= \left(\mathbf{F}\mathbf{T}^T + \mathbf{T}\mathbf{F}^T\right) + \left(\mathbf{T}\mathbf{F}^T + \mathbf{F}\mathbf{T}^T\right) = \mathbf{0}(\text{mod}2).
\end{aligned} \tag{5.15}$$

Hence, we have $\mathbf{A}_1\mathbf{A}_2^T = \mathbf{A}_2\mathbf{A}_1^T$ and $\mathbf{A}_1\mathbf{A}_2^T + \mathbf{A}_2\mathbf{A}_1^T = \mathbf{0} \pmod 2$. □

Note that for $p = 4n-1$ and odd $k = \frac{p-1}{2}$, $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ consist of k different transversal $\mathcal{T}$ such that their transformation matrices $\boldsymbol{\pi}_{\mathcal{T}}$ are cyclic shifts of identity matrix $\mathbf{I}_k$. We construct a set of reverse matrices from $\boldsymbol{\pi}_{\mathcal{T}}$ using $\mathbf{R}_{\mathbf{I}_k}$.

Corollary 5.9. *For Type-I-B QCS codes, let* $\mathscr{P} = \{\mathbf{R}_{\mathbf{I}_k}\boldsymbol{\pi}_{\mathcal{T}_i} \equiv \mathbf{R}_{\mathbf{I}_k}\mathbf{P}^i, 0 \leq i \leq k-1\}$ *be a set of transformation matrices for* $\mathbf{H}_{1proto}$ *and* $\mathbf{H}_{2proto}$*, where the permutation matrix* $\boldsymbol{\pi}_{\mathcal{T}_i}$ *is the* i*-th cyclic shift of the* $k \times k$ *identity matrix. For* $\mathbf{D} \in \mathscr{P}$*, we construct the equivalent protomatrices*

$$\mathbf{H'}_{1proto} = \mathbf{D}\mathbf{H}_{1proto} \quad \textit{and} \quad \mathbf{H'}_{2proto} = \mathbf{D}\mathbf{H}_{2proto}$$

based on row-swapping. Then for an arbitrary order v *of* $\mathbf{P}$*, the binary parity-check matrix* $\mathbf{H} = [\mathbf{A}_1 \mid \mathbf{A}_2]$ *lifted from* $\mathbf{H}_{proto} = [\mathbf{H}_{1proto}\ \mathbf{H'}_{2proto} \mid \mathbf{H}_{2proto}\ \mathbf{H'}_{1proto}]$ *is always self-orthogonal with respect to the SIP.*

Proof. Since $\mathbb{R}_k\mathbb{R}_k^T$ is the identity matrix, $\mathbf{D}\mathbf{D}^T$ equals to the identity matrix. Thus, the SIP constraint can be satisfied for different $\mathbf{D} \in \mathscr{P}$ used. Furthermore, since $\mathbf{A}_1\mathbf{A}_2^T = \mathbf{A}_2\mathbf{A}_1^T$ from Lemma 5.8 is irrelevant to the order of CPMs, the non-zero values of $\mathbf{A}_1\mathbf{A}_2^T + \mathbf{A}_2\mathbf{A}_1^T$ are always even for an arbitrary order of $\mathbf{P}$. □

Proposition 5.10. *For positive integers* n *and* $\rho' \leq k$*, a prime* $p = 4n-1$ *and a* $v > p$*, the quadratic residue set* $\mathcal{Q}^{\mathcal{R}}$ *and quadratic non-residue set* $\mathcal{Q}^{\mathcal{NR}}$ *yield a* $[[N, K]] = [[2kv, 2kv - \rho'(v-1) - 1]]$ *QCS code. We call this type of QCS codes Type-I-B QCS codes.*

Proof. By removing $k - \rho'$ rows from $\mathbf{H}_{proto}$, the sub-matrices $\mathbf{A}_1^{sub}$ and $\mathbf{A}_2^{sub}$ of size $\rho' v \times 2kv$ define a QCS code of rate at least $R^Q = 1 - \frac{\rho'}{2k}$. Further, since each of the v rows of $\mathbf{A}_1$ and $\mathbf{A}_2$ lifted from $\mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}}\right)^i$ and $\mathscr{C}\left(\mathbf{h}_{\mathcal{Q}^{\mathcal{NR}}}\right)^i$ sum to the all-one vector, the rank of the parity-check matrices $\mathbf{A}_1^{sub}$ and $\mathbf{A}_2^{sub}$ is at most $\rho'(v-1)+1$ (*e.g.*, see [87]). □

5.2.4 Type-II QCS codes from QR set of size p = 4n+1

In this section, we design $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ given in (5.10) for Type-II QCS codes. Recall that

$$\mathbf{h}_{\mathcal{Q}^{\mathcal{R}}} = \left[1, \beta, \ldots, \beta^{\frac{k}{2}-1}, -1, -\beta, \ldots, -\beta^{\frac{k}{2}-1}\right]$$

for a prime $p = 4n + 1$ and $k = \frac{p-1}{2} = \frac{4n}{2} = 2n$ is an even integer. The associated protomatrix $\mathbf{H}_{1proto}$ is a commutative Latin square of the form

$$\mathbf{H}_{1proto} = \begin{bmatrix} 1 & \cdots & \beta^{\frac{k}{2}-1} & -1 & \cdots & -\beta^{\frac{k}{2}-1} \\ \vdots & \iddots & \iddots & \iddots & \iddots & \vdots \\ \beta^{\frac{k}{2}-1} & \iddots & -\beta^{\frac{k}{2}-2} & -\beta^{\frac{k}{2}-1} & \iddots & \beta^{\frac{k}{2}-2} \\ -1 & \iddots & -\beta^{\frac{k}{2}-1} & 1 & \iddots & \beta^{\frac{k}{2}-1} \\ \vdots & \iddots & \iddots & \iddots & \iddots & \vdots \\ -\beta^{\frac{k}{2}-1} & \cdots & \beta^{\frac{k}{2}-2} & \beta^{\frac{k}{2}-1} & \cdots & -\beta^{\frac{k}{2}-2} \end{bmatrix} \equiv \begin{bmatrix} \mathbf{h}_{11} & \mathbf{h}_{12} \\ \mathbf{h}_{21} & \mathbf{h}_{22} \end{bmatrix}, \tag{5.16}$$

where $\mathbf{h}_{11} = \mathbf{h}_{22}$, $\mathbf{h}_{12} = \mathbf{h}_{21}$ and $\mathbf{h}_{11} = -\mathbf{h}_{12}$. Let $\gamma \in \mathcal{Q}^{\mathcal{N}\mathcal{R}}$. We construct

$$\mathbf{H}_{2proto} = \gamma \begin{bmatrix} \mathbf{h}_{11} & \mathbf{h}_{12} \\ \mathbf{h}_{21} & \mathbf{h}_{22} \end{bmatrix} (\text{mod } p).$$

Let $\mathbf{R}_{\mathbf{I}_k}$ be the reverse identity matrix of size $k \times k$ given in (5.13) and $\mathscr{P} = \{\mathbf{R}_{\mathbf{I}_k}\mathbf{P}^i, 0 \leq i \leq k-1\}$ be a set of transformation matrices.

Lemma 5.11. *For a positive integer n and a prime $p = 4n + 1$, let $\mathbf{H}_{1proto}$ and $\mathbf{H}_{2proto}$ be the protomatrices of the form given in (5.10). Let $\mathbf{H'}_{1proto} = \mathbf{H}_{1proto}\mathbf{D}$ (resp. $\mathbf{H'}_{2proto} = \mathbf{H}_{2proto}\mathbf{D}$) be the equivalent Latin square of $\mathbf{H}_{1proto}$ (resp. $\mathbf{H}_{2proto}$) constructed from column-swapping, where $\mathbf{D} \in \mathscr{P}$. The binary matrix $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H'}_2]$ (resp. $\mathbf{H} = [\mathbf{H'}_1 \mid \mathbf{H}_2]$) lifted from $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H'}_{2proto}]$ (resp. $\mathbf{H}_{proto} = [\mathbf{H'}_{1proto} \mid \mathbf{H}_{2proto}]$) is self-orthogonal with respect to the SIP.*

Proof. From Equation (5.16), we know that $\mathbf{h}_{11} = \mathbf{h}_{22}$, $\mathbf{h}_{21} = \mathbf{h}_{12}$ and $\mathbf{h}_{11} = -\mathbf{h}_{12}$. The lifted parity-check matrix $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H'}_2]$ can be expressed as

$$\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H'}_2] = \left[\begin{array}{cc|cc} \mathbf{A}_{11} & \mathbf{A}_{12} & \mathbf{B}_{11} & \mathbf{B}_{12} \\ \mathbf{A}_{12} & \mathbf{A}_{11} & \mathbf{B}_{12} & \mathbf{B}_{11} \end{array}\right],$$

where $\mathbf{H}_1\mathbf{H}'^T_2$ is given by

$$\mathbf{H}_1\mathbf{H}'^T_2 = \begin{bmatrix} \left(\mathbf{A}_{11}\mathbf{B}_{11}{}^T + \mathbf{A}_{12}\mathbf{B}_{12}{}^T\right) & \left(\mathbf{A}_{11}\mathbf{B}_{12}{}^T + \mathbf{A}_{12}\mathbf{B}_{11}{}^T\right) \\ \left(\mathbf{A}_{12}\mathbf{B}_{11}{}^T + \mathbf{A}_{11}\mathbf{B}_{12}{}^T\right) & \left(\mathbf{A}_{12}\mathbf{B}_{12}{}^T + \mathbf{A}_{11}\mathbf{B}_{11}{}^T\right) \end{bmatrix}.$$

By expressing $\mathbf{H}_1$ and $\mathbf{H}'_2$ in the polynomial form similar to lemma 5.6, it can be verified that

$$\begin{aligned} \mathbf{A}_{11}\mathbf{B}_{11}{}^T = \mathbf{B}_{12}\mathbf{A}_{12}{}^T, \;\; \mathbf{A}_{12}\mathbf{B}_{11}{}^T = \mathbf{B}_{12}\mathbf{A}_{11}{}^T, \\ \mathbf{A}_{11}\mathbf{B}_{12}{}^T = \mathbf{B}_{11}\mathbf{A}_{12}{}^T, \;\; \mathbf{A}_{12}\mathbf{B}_{12}{}^T = \mathbf{B}_{11}\mathbf{A}_{11}{}^T. \end{aligned} \tag{5.17}$$

This implies that

$$\mathbf{H}_1\mathbf{H}'^T_2 \equiv \begin{bmatrix} \left(\mathbf{B}_{11}\mathbf{A}_{11}{}^T + \mathbf{B}_{12}\mathbf{A}_{12}{}^T\right) & \left(\mathbf{B}_{11}\mathbf{A}_{12}{}^T + \mathbf{B}_{12}\mathbf{A}_{11}{}^T\right) \\ \left(\mathbf{B}_{12}\mathbf{A}_{11}{}^T + \mathbf{B}_{11}\mathbf{A}_{12}{}^T\right) & \left(\mathbf{B}_{12}\mathbf{A}_{12}{}^T + \mathbf{B}_{11}\mathbf{A}_{11}{}^T\right) \end{bmatrix} = \mathbf{H}'_2\mathbf{H}_1^T. \tag{5.18}$$

Thus, $\mathbf{H}_1$ and $\mathbf{H}'_2$ are orthogonal with respect to the SIP. The proof completes. □

Proposition 5.12. *For positive integers n, $\rho' \leq k$, a prime $p = 4n + 1$ and a $v > p$, the quadratic residue set $\mathcal{Q}^{\mathcal{R}}$ and the quadratic non-residue set $\mathcal{Q}^{\mathcal{NR}}$ yield a $[[N, K]] = [[kv, kv - \rho'(v-1) - 1]]$ QCS code. We call this type of QCS codes Type-II QCS codes.*

Proof. Refer to the proof for Proposition 5.10. □

5.2.5 Lower bound on minimum distance of Type-II QCS codes

It is known that a Tanner graph of a stabilizer matrix over $\mathbb{F}_4$ contains inevitable cycles of length four due to the orthogonality requirement. This means that every commuting pair of operators in a stabilizer $\mathcal{S}$ must have an even number of overlapping positions with non-identity elements according to (2.10). In the following,

the girth of their underlying binary matrices $\mathbf{H}_1$ and $\mathbf{H'}_2$ is studied, and a lower bound on the minimum distance for Type-II QCS codes is given.

In [87], it is shown that a cycle in the Tanner graph of a conventional QC-LDPC code can be considered as a sequence of the corresponding $v \times v$ CPMs. Thus, a cycle of length $2i$ in a conventional binary QC-LDPC code can be expressed as the sequence $(j_0, l_0); (j_1, l_1); \ldots; (j_k, l_k); \ldots; (j_{i-1}, l_{i-1}); (j_0, l_0)$, where (j_k, l_k) stands for the j_k-th row and l_k-th column of $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H}_{2proto}]$, and the semicolon between (j_k, l_k) and (j_{k+1}, l_{k+1}) can be considered as (j_{k+1}, l_k). Clearly, $j_k \neq j_{k+1}$ and $l_k \neq l_{k+1}$. Therefore, the necessary and sufficient condition for the existence of the cycle of length $2i$ is [87]

$$\sum_{k=0}^{i-1}(h_{j_k,l_k} - h_{j_{k+1},l_k}) = 0 \,(\mathrm{mod}\ v)\,, \tag{5.19}$$

where each h_{j_k,l_k} represents an element in $\mathbf{H}_{proto}$. For example, for $i = 2$, the girth of a Tanner graph is four if there exists a sequence $(j_0, l_0); (j_1, l_1); (j_0, l_0)$ such that the condition in (5.19) is satisfied. This condition is used to show that the length of a cycle in a protograph LDPC code can be calculated using the shift values of their circulants.

Lemma 5.13. *The binary matrix* $\mathbf{H} = [\mathbf{H_1} \mid \mathbf{H'}_2]$ *lifted from* $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H'}_{2proto}]$ *has girth at least six.*

Proof. Recall that $\mathbf{h}_{\mathcal{QR}} = \left[1, \beta, \beta^2, \beta^3, \ldots, \beta^{k-1}\right]$ and $\mathbf{h}_{\mathcal{QNR}} = \gamma \mathbf{h}_{\mathcal{QR}} (\mathrm{mod}\ p)$ for a prime $p = 4n + 1$, where $\gamma \in \mathcal{Q}^{\mathcal{NR}}$. Let $i_1 \neq i_2$ for $0 \leq i_1, i_2 \leq k - 1$. Since the j-th row of $\mathbf{H}_{1proto}$ (resp. $\mathbf{H}_{2proto}$) is the j-th cyclic left shift of $\mathbf{h}_{\mathcal{QR}}$ (resp. $\mathbf{h}_{\mathcal{QNR}}$) for $0 \leq j \leq k - 1$, the difference between row i_1 and row i_2 of $\mathbf{H}_{proto}$ is given by

$$\left[\beta^{i_1}\mathbf{h}_{\mathcal{QR}} \quad \beta^{i_1}\mathbf{h}_{\mathcal{QNR}}\right] - \left[\beta^{i_2}\mathbf{h}_{\mathcal{QR}} \quad \beta^{i_2}\mathbf{h}_{\mathcal{QNR}}\right] = \left[(\beta^{i_1} - \beta^{i_2})\mathbf{h}_{\mathcal{QR}} \quad (\beta^{i_1} - \beta^{i_2})\mathbf{h}_{\mathcal{QNR}}\right]. \tag{5.20}$$

For either $(\beta^{i_1} - \beta^{i_2}) \in \mathcal{Q}^{\mathcal{R}}$ or $(\beta^{i_1} - \beta^{i_2}) \in \mathcal{Q}^{\mathcal{NR}}$, the unique sets $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ are generated according to lemma 2. Thus, the difference between arbitrary two rows of $\mathbf{H}_{proto}$ is a vector that contains $p-1$ distinct elements from $\mathbf{Z}_p^{\times}$. Moreover,

since $\mathbf{H'}_{2proto} = \mathbf{H}_{2proto}\mathbf{D}$ is a column permutated version of $\mathbf{H}_{2proto}$, where $\mathbf{D} \in \mathscr{P}$ is a transformation matrix, the difference between row i_1 and row i_2 of $\mathbf{H}_{proto}$ is also permuted. Hence, the lifted binary parity-check matrix $\mathbf{H}$ contains no cycles of length four since there exist no sequences $(j_0, l_0); (j_1, l_1); (j_0, l_0)$ in $\mathbf{H}_{proto}$ such that the condition in (5.19) that can be satisfied. Therefore, the girth of binary $\mathbf{H}$ of Type-II QCS codes is at least six. □

Since the Tanner graph of binary $\mathbf{H}$ is free of cycles of length four, it is straightforward that the Tanner graphs of $\mathbf{H}_1$ and $\mathbf{H'}_2$ are also free of cycles of length four. In the following, we show that the minimum distance of Type-II QCS codes can be lower bounded in the terms of the minimum distance of the underlying binary LDPC codes.

Proposition 5.14. *For positive integers n, $\rho' \leq k$, a prime $p = 4n + 1$ and a $v > p$, the proposed Type-II QCS codes have the minimum distance lower bounded by $d^Q \geq 2(\rho' + 1) - \max(wt(\mathbf{a} \cap \mathbf{b}))$, where $(\mathbf{a} \mid \mathbf{b}) \in \mathbb{F}_2^{2N}$ is an element in the symplectic dual space $\mathcal{C}^\circ$.*

Proof. Recall from Section II-B that the minimum distance of a non-CSS quantum LDPC code is defined as

$$\begin{aligned} d^Q &:= \min\{wt(\mathbf{a} \mid \mathbf{b}) \mid (\mathbf{a} \mid \mathbf{b}) \in \mathcal{C}^\circ \setminus \mathcal{C}\} \\ &\equiv \min\{wt(\mathbf{a}) + wt(\mathbf{b}) - wt(\mathbf{a} \cap \mathbf{b}) \mid (\mathbf{a} \mid \mathbf{b}) \in \mathcal{C}^\circ \setminus \mathcal{C}\}, \end{aligned} \tag{5.21}$$

where $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^N$. Let $d_1 = wt(\mathbf{a})$ and $d_2 = wt(\mathbf{b})$ be the distance of the pair of protograph LDPC codes with parity-check matrices $\mathbf{H}_1$ and $\mathbf{H'}_2$, respectively. It is known from [88] [89], that the minimum distance of LDPC codes is lower bounded by $d_{c_{\min}} + 1$, where $d_{c_{\min}}$ denotes the minimum column weight of the parity-check matrix, if the associated Tanner graph is free from cycles of length four. Since both $\mathbf{H}_1$ and $\mathbf{H'}_2$ have a constant column weight $\rho' \leq k$ and their Tanner graphs do not have cycles of length four according to lemma 5.13, the minimum distance d_1 and d_2 are both lower bounded by $\rho' + 1$. Hence, the minimum distance of Type-II QCS codes is lower bounded by $d^Q \geq 2(\rho' + 1) - \max(wt(\mathbf{a} \cap \mathbf{b}))$. □

$$\mathbf{H}_{proto} = \left[\begin{array}{cccccccccc|cccccccccc} 1 & 3 & 9 & 5 & 4 & 2 & 6 & 7 & 10 & 8 & 10 & 8 & 2 & 6 & 7 & 9 & 5 & 4 & 1 & 3 \\ 3 & 9 & 5 & 4 & 1 & 8 & 2 & 6 & 7 & 10 & 8 & 2 & 6 & 7 & 10 & 3 & 9 & 5 & 4 & 1 \\ 9 & 5 & 4 & 1 & 3 & 10 & 8 & 2 & 6 & 7 & 2 & 6 & 7 & 10 & 8 & 1 & 3 & 9 & 5 & 4 \\ 5 & 4 & 1 & 3 & 9 & 7 & 10 & 8 & 2 & 6 & 6 & 7 & 10 & 8 & 2 & 4 & 1 & 3 & 9 & 5 \\ 4 & 1 & 3 & 9 & 5 & 6 & 7 & 10 & 8 & 2 & 7 & 10 & 8 & 2 & 6 & 5 & 4 & 1 & 3 & 9 \end{array}\right] \tag{5.22}$$

5.2.6 Examples

Example 5.2. *For* $n = 3$, $p = 4n - 1 = 11$, $\mathcal{Q}^{\mathcal{R}} = \{1, 3, 4, 5, 9\}$ *and* $\mathcal{Q}^{\mathcal{NR}} = -\mathcal{Q}^{\mathcal{R}} = \{10, 8, 7, 6, 2\}$. *Choose* $\mathbf{D} \in \mathscr{P}$ *as*

$$\mathbf{D} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Let $\mathbf{H'}_{1proto} = \mathbf{D}\mathbf{H}_{1proto}$ *and* $\mathbf{H'}_{2proto} = \mathbf{D}\mathbf{H}_{2proto}$ *be the equivalent protomatrix of* $\mathbf{H}_{1proto}$ *and* $\mathbf{H}_{2proto}$, *respectively. Then*

$$\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \quad \mathbf{H'}_{2proto} \mid \mathbf{H}_{2proto} \quad \mathbf{H'}_{1proto}]$$

is shown in Equation (5.22). Note that in this example, the Tanner graph of the parity-check matrix $\mathbf{H}$ *lifted from* $\mathbf{H}_{proto}$ *given in Equation (5.22) contains cycles of length four. According to the condition (5.19), consider the sequence* $(j_0, l_0); (j_1, l_1);\ (j_0, l_0) = (1, 1); (2, 10); (1, 1)$. *This sequence is a cycle of length* 4 *since* $1 - 3 + 10 - 8 = 0 \,(\mathrm{mod}\, v)$ *for any arbitrary* v. *Hence, the binary parity-check matrix in (5.22) has cycles of length* 4. *Furthermore, let* $\rho' = k = 5$ *and* $v = 31$ *the lifted* $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H}_2]$ *is a* $[[2kv, 2kv - \rho' v + \rho' - 1]] = [[310, 159]]$ *Type-I-B QCS code.*

Let $\mathbf{O}_M$ *be a* 5×5 *all-zero matrix and* $v = p$. *Then the associated Type-I-A QCS*

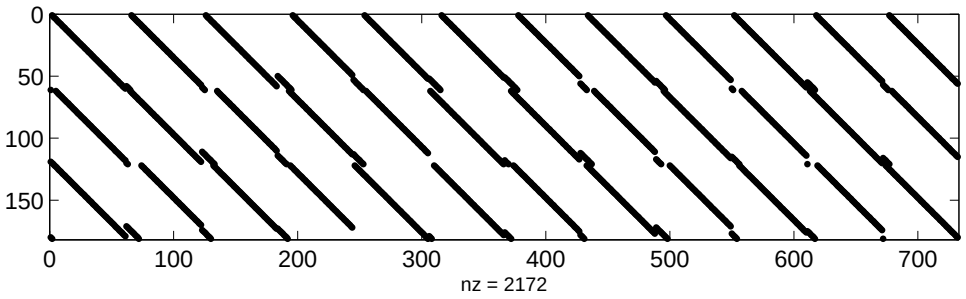

FIGURE 5.1: The parity-check matrix for [[366, 185] quantum Type-II QCS code in Example 5.3.

codes can be constructed by superimposing $\mathbf{O}_5$ *to either* $\mathbf{H}_{1proto}$ *or* $\mathbf{H}_{2proto}$. *Let* $\mathbf{H'}_{2proto} = \mathbf{H}_{2proto} \boxplus \mathbf{O}_5$, *we have* $\mathbf{H} = [\mathbf{H}_1 \mid \mathbf{H'}_2]$ *lifted from* $\mathbf{H}_{1proto} = [\mathbf{H}_{1proto} \mid \mathbf{H'}_{2proto}]$ *is a* $[[kp, k-1]] = [[55, 4]]$ *Type-I-A QCS code.*

Example 5.3. *For* $n = 3$ *and* $p = 4n + 1 = 13$, *we have* $\mathcal{Q}^{\mathcal{R}} = \{1, 3, 4, 9, 10, 12\}$ *and* $\mathcal{Q}^{\mathcal{NR}} = \{2, 5, 6, 7, 8, 11\}$ *with* $k = \frac{p-1}{2} = 6$. *Let* $\beta = 4$ *and* $\gamma = 2 \in \mathcal{Q}^{\mathcal{NR}}$. *Then*

$$\mathbf{h}_{1proto} = \{1, 4, 3, 12, 9, 10\} \equiv \{1, 4, 3, -1, -4, -3\} \pmod{13}$$

and

$$\mathbf{h}_{2proto} = \gamma \mathbf{h}_{1proto} = \{2, 8, 6, 11, 5, 7\} \equiv \{2, 8, 6, -2, -8, -6\} \pmod{13}.$$

Let $\mathbf{H}'_{1proto} = \mathbf{H}_{1proto}\mathbf{R}_{\mathbf{I}_k}$. *The final protomatrix is given by Equation (5.23).*

Let $\rho' = 3$ *and* $v = 61$, *the rank of* $\mathbf{H}_1$ *and* $\mathbf{H}_2$ *is* $\rho'(v-1)+1 = 3(61-1)+1 = 181$. *We obtain a* $[[kv, kv - \rho' v + \rho' - 1]] = [[366, 185]]$ *Type-II QCS code of rate* $R^Q \approx 0.5$ *by removing the last three rows of* $\mathbf{H}_{proto}$. *The parity-check matrix of this code is shown in Fig. (5.1) Furthermore, consider the protomatrix* $\mathbf{H}_{proto}$ *given by (5.23), we now show that the binary matrix* $\mathbf{H}$ *lifted from* $\mathbf{H}_{proto}$ *is free of cycles of length four. It can be verified that for any arbitrary pair of rows, the differences between each pair of elements are distinct. This implies that there exist no sequences* $(j_0, l_0); (j_1, l_1); (j_0, l_0)$ *such that the condition in (5.19) is satisfied. Furthermore, when* $i = 3$, *the sequence* $(j_0, l_0); (j_1, l_1); (j_2, l_2); (j_0, l_0) =$

$$
\begin{aligned}
\mathbf{H}_{proto} &= \left[\mathbf{H}'_{1proto}|\mathbf{H}_{2proto}\right] \\
&= \left[\begin{array}{cccccc|c}
10 & 9 & 12 & 3 & 4 & 1 & \\
1 & 10 & 9 & 12 & 3 & 4 & \\
4 & 1 & 10 & 9 & 12 & 3 & \\
3 & 4 & 1 & 10 & 9 & 12 & 2\begin{pmatrix} 1 & 4 & 3 & 12 & 9 & 10 \\ 4 & 3 & 12 & 9 & 10 & 1 \\ 3 & 12 & 9 & 10 & 1 & 4 \\ 12 & 9 & 10 & 1 & 4 & 3 \\ 9 & 10 & 1 & 4 & 3 & 12 \\ 10 & 1 & 4 & 3 & 12 & 9 \end{pmatrix} \\
12 & 3 & 4 & 1 & 10 & 9 & \\
9 & 12 & 3 & 4 & 1 & 10 &
\end{array}\right] \\
&= \left[\begin{array}{cccccc|cccccc}
10 & 9 & 12 & 3 & 4 & 1 & 2 & 8 & 6 & 11 & 5 & 7 \\
1 & 10 & 9 & 12 & 3 & 4 & 8 & 6 & 11 & 5 & 7 & 2 \\
4 & 1 & 10 & 9 & 12 & 3 & 6 & 11 & 5 & 7 & 2 & 8 \\
3 & 4 & 1 & 10 & 9 & 12 & 11 & 5 & 7 & 2 & 8 & 6 \\
12 & 3 & 4 & 1 & 10 & 9 & 5 & 7 & 2 & 8 & 6 & 11 \\
9 & 12 & 3 & 4 & 1 & 10 & 7 & 2 & 8 & 6 & 11 & 5
\end{array}\right]
\end{aligned}
\tag{5.23}
$$

$(4,12);(5,1);(6,3);(4,12)$ *form a cycle of length* 6*, that is*

$$\sum_{k=0}^{2}(h_{j_k,l_k} - h_{j_{k+1},l_k}) = 6 - 11 + 12 - 9 + 3 - 1 = 0 \,(\mathrm{mod}\ v)\,.$$

Thus, the binary check matrix $\mathbf{H}$ *over* $\mathbb{F}_2$ *has girth six.*

5.2.7 Constructed codes

TABLE 5.1 is a list of parameters of the constructed Type-I-A, Type-I-B and Type-II QCS codes. The listed codes have code rate ~ 0.5 due to the pair of parity-check matrices are rank deficient. The code length of the set of Type-I-A codes for different n are $N = vk$, where $v = p$, and the dimension of each code is $K = kv - \rho'(v-1) - 1$, where $\rho' = \frac{k-1}{2}$. The set of codes are constructed by removing $\frac{k+1}{2}$ rows from the bottom of $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H}'_{2proto}]$. The resulting parity-check matrices have rank $\rho'(v-1)+1$ for both odd and even v. Moreover, the set of Type-I-B QCS codes is constructed from quadratic residue set of parameters $n = 3$ and $p = 4n - 1 = 11$ given in Example 2. The equivalent non-orthogonal Latin squares $\mathbf{H}'_{1proto}$ and $\mathbf{H}'_{2proto}$ are obtained by performing left multiplication (row-swapping) using arbitrary transformation matrix $\mathbf{D} \in \mathscr{P}$. The final protomatrix $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \;\; \mathbf{H}'_{2proto} \mid \mathbf{H}_{2proto} \;\; \mathbf{H}'_{1proto}]$ is lifted with $\mathbf{P}$ of orders $v = 32, 61, 113$ and 199. The dimension of the constructed Type-I-B QCS codes is $K = 2kv - \rho'(v -$

TABLE 5.1: Constructed $[[kv, kv - \rho'(v-1) - 1, d^Q]]$ Type-I-A, $[[2kv, 2kv - \rho' v + \rho' - 1, d^Q]]$ Type-I-B and $[[kv, kv - \rho' v + \rho' - 1, d^Q]]$ Type-II QCS codes.

Type-I-A $p = 4n-1$ $\rho' = \frac{k-1}{2}$					Type-I-B $p = 4n-1$ $\rho' = k$					Type-II $p = 4n+1$ $\rho' = \frac{k}{2}$				
n	k	v	N	K	n	k	v	N	K	n	k	v	N	K
5	9	19	171	98	3	5	32	320	164	3	6	79	474	239
6	11	23	253	142	3	5	61	610	309	3	6	100	600	302
8	15	31	465	254	3	5	113	1130	569	3	6	199	1194	599
11	21	43	903	482	3	5	199	1990	999	3	6	401	2406	1205

TABLE 5.2: Parameters of Type-II QCS codes with $v = 79$ and variable n.

Type-II $p = 4n+1$ $\rho' = \frac{k}{2}$ $v = 79$			
n	k	N	K
3	6	474	239
4	8	632	319
7	14	1106	559
10	20	1580	799

$1) - 1$, where $\rho' = k$. Furthermore, the set of Type-II QCS codes are obtained from quadratic residue set of parameters $n = 3$ and $p = 4n + 1 = 13$ given in Example 5.3. Let $\rho' = \frac{k}{2}$, we remove $\frac{k}{2}$ rows from the bottom of $\mathbf{H}_{proto} = [\mathbf{H}_{1proto} \mid \mathbf{H'}_{2proto}]$ to obtain a subprotomatrix $\mathbf{H}^{sub}_{proto}$, where $\mathbf{H'}_{2proto} = \mathbf{H}_{2proto}\mathbf{R}_{\mathbf{I}_k}$. We lift $\mathbf{H}^{sub}_{proto}$ with different orders of $\mathbf{P}$ (*e.g.*, $v = 79, 100, 199$ and 401) to generate Type-II QCS codes of different lengths with quantum code rate of at least 0.5. In addition, TABLE 5.2 and 5.3 are set of Type-I-B and Type-II QCS codes constructed from CPMs of a fix order v and various n for $\rho' = k$ and $\rho' = \frac{k}{2}$, respectively.

5.2.8 Simulation results and performance evaluation

In this section, we provide simulation results of the proposed protograph quantum LDPC codes over a quantum depolarizing channel under the iterative sum-product

TABLE 5.3: Parameters of Type-I-B QCS codes with $v = 61$ and variable n.

Type-I-B			
$p = 4n - 1$	$\rho' = k$		$v = 61$
n	k	N	K
3	5	610	309
5	9	1098	557
6	11	1342	681
8	15	1830	929

algorithm (SPA). The decoding process is performed over Galois field $\mathbb{F}_4$ [150] [151] by applying the isomorphism between the Pauli operators $\{I, X, Z, Y\}$ and the Galois field $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega} = \omega^2\}$, or the equivalent $\mathbb{F}_{2^2} = \{00, 10, 01, 11\}$. The isomorphism is given by the element identification

$$I \leftrightarrow 0, \;\; X \leftrightarrow 1, \;\; Z \leftrightarrow \omega, \;\; Y \leftrightarrow \bar{\omega},$$

and the operation identification

$$\textit{multiplication} \leftrightarrow \textit{addition}, \;\; \textit{commutativity} \leftrightarrow \textit{trace inner product}.$$

The input of the decoder is the syndrome vector $\mathbf{s} = \{+1, -1\}^{N-K}$. We assume the decoder knows the channel depolarizing strength $0 < f < 1$ and the all-zero vector is transmitted. The message passing along the edges of a Tanner graph from each qubit node is a probability vector $[1 - f, f/3, f/3, f/3]$, and each value from left to right in the vector represents the probability of a single Pauli error $E \in \mathcal{P}_1$ acting on the j-th qubit, that is, $\Pr(E_j = I) = 1 - f$ and $\Pr(E_j = X) = \Pr(E_j = Z) = \Pr(E_j = Y) = f/3$. Furthermore, *random perturbation* is also used to break the symmetry of degeneracy errors [150]. The strength of the random perturbation is 0.1 and the maximum number of iterations between each perturbation is 40. The maximum iteration number for the sum-product decoder is 50. To effectively compute the check node operation, the FFT-based SPA [127] is used in our simulations.

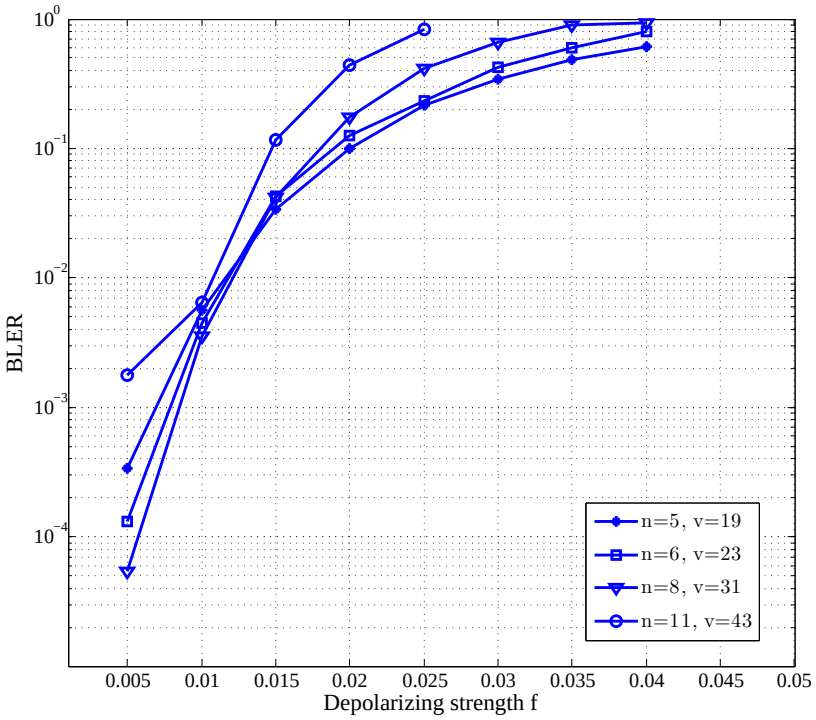

FIGURE 5.2: BLER of Type-I-A QCS codes.

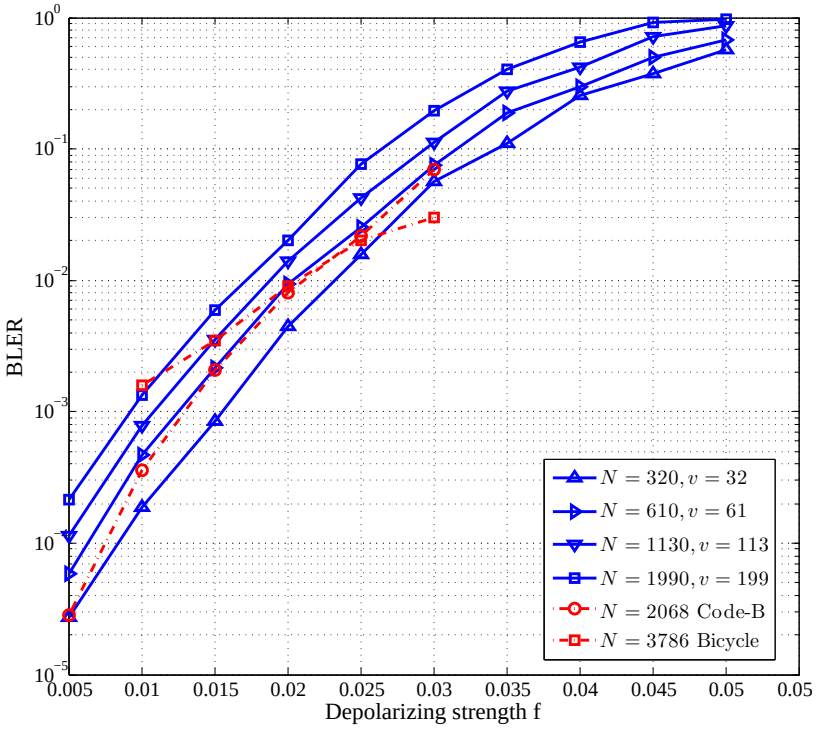

FIGURE 5.3: BLER of Type-I-B QCS codes.

Figures 5.2, 5.3 and 5.4 present the block error rate (BLER) of Type-I-A, Type-I-B and Type-II QCS codes listed in TABLE 5.1. From Figure 5.2, we see that as n increases the BLER of Type-I-A QCS codes improves in the waterfall region.

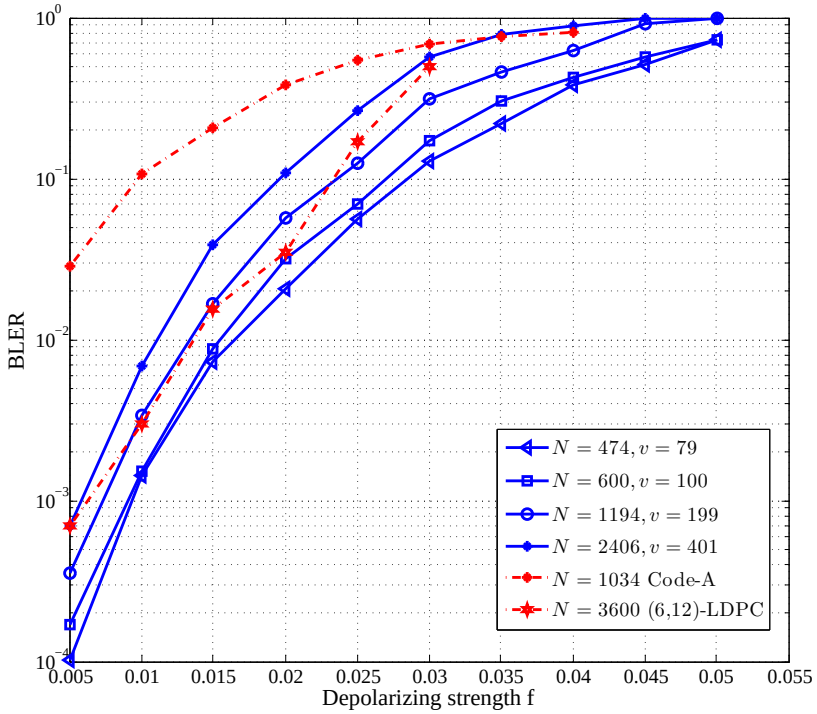

FIGURE 5.4: BLER of Type-II QCS codes.

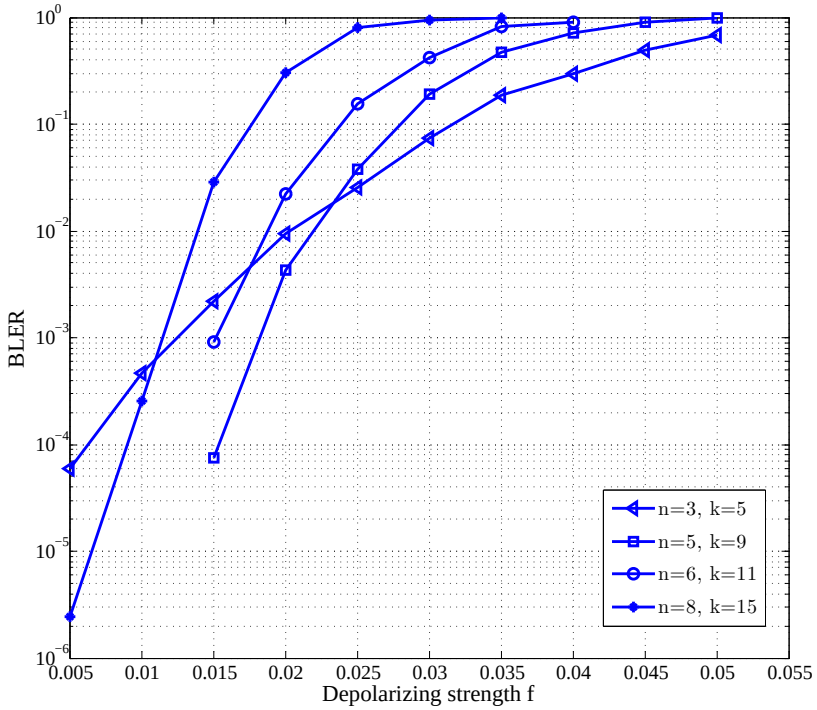

FIGURE 5.5: BLER of Type-I-B QCS codes with $v = 61$ and $n = 3, 5, 6, 8$.

However, as n further increases, an early error floor appears due to the vast number of trapping sets created by the high column and row weights. In Figures 5.3 and 5.4, the performance of the proposed Type-I-B and Type-II QCS codes is compared

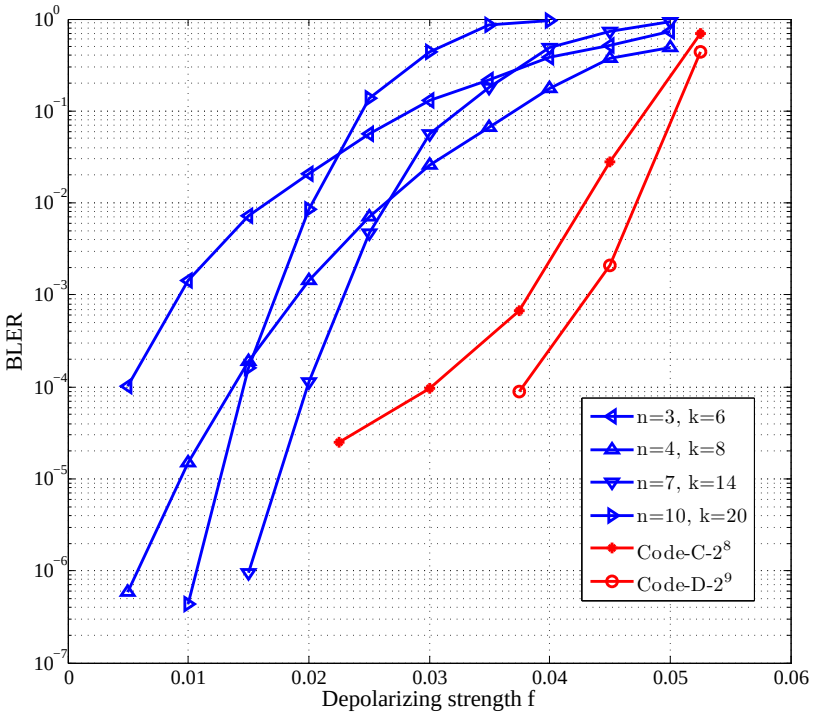

FIGURE 5.6: Performance comparison between Type-II QCS codes with $v = 79$ and $n = 3, 4, 7, 10$ and the quantum CSS codes Code-C-2^8 and Code-D-2^9 in [75]. Note that the BLER plotted here for Code-C-2^8 and Code-D-2^9 is a function of $f = 3f_m/2$, where f_m is the marginal probability used in [75], and the BLER for the entire CSS code is shown.

to some of the quantum LDPC codes in the literature. The two codes denoted as 'Code-A' and 'Code-B' of length $N = 1034$ and $N = 2068$ are quantum LDPC codes constructed from multi-weight circulant matrices and by performing matrix scramble, respectively [68]. Moreover, the performance of the '$(6, 12)$-regular' quantum LDPC code from [64] and MacKay's 'Bicycle' codes of column weight 12 from [39] is also shown in the Figures. We can see from Figure 5.3 that Type-I-B QCS codes show improving performance when the depolarizing strength f is low compared to the Bicycle code. In addition, an approximately 0.0025 performance gain is achieved by Type-I-B QCS code of length $N = 320$ compared to Code-B of length $N = 2068$. Furthermore, as shown in Figure 5.4, the performance of Type-II QCS codes with moderate code lengths outperform Code-A approximately two orders of magnitude for low f, and outperform the $(6, 12)$-regular code for high f.

Comparing the performance between Type-I-B and Type-II QCS codes given in TABLE 5.1, it can be seen that for codes with similar length, the performance

of Type-I-B codes is approximately a half order of magnitude better than Type-II codes. Furthermore, the performance of Type-I-B and Type-II QCS codes is better when the code length N is shorter. As can be seen from TABLE 5.1, the column and row weights of the constructed Type-I-B and Type-II QCS codes stay constant as the code length increases. Moreover, as v increases, the quantum code rate approaches a half. This implies that there is an increasing number of redundant rows in the parity-check matrix. Thus, the minimum distance of Type-I-B and Type-II QCS codes does not grow with the code length. Hence, the error correction capability remains unchanged, which causing a performance lost as v increases.

The performance of the constructed Type-I-B and Type-II QCS codes given in TABLE 5.2 and TABLE 5.3 are shown in Figures 5.5 and 5.6. These codes are constructed from CPMs of a fixed order ($v = 61$ for Type-I-B QCS codes in TABLE 5.2 and $v = 79$ for Type-II QCS codes TABLE 5.3), whereas the column weight of their parity-check matrices varies as n increases. It can be seen from the figures that as n increases, the warterfall region of both Type-I-B and Type-II QCS codes become steeper and no error floor appears for block error rate up to $10^{-6} \sim 10^{-7}$. On the other hand, as n increases, a constant performance gap of approximately 0.005 is shown for different Type-I-B QCS code of $n = 3, 5, 6$ and 8, whereas the Type-II QCS code of $n = 7$ achieves $0.01 \sim 0.015$ performance gain compared to Type-II QCS codes of $n = 3, 4$, and 10.

We also compare the performance of the constructed Type-II QCS codes with the rate half quantum LDPC codes constructed in [75]. In Figure 5.6, 'Code-C-2^8' and 'Code-C-2^9' are length $N = 8768$ and $N = 10728$ quantum LDPC codes in [75], respectively, where 2^8 and 2^9 represent the field size that the iterative decoding algorithm is performed over. From the figure, we see that no error floor appears for the proposed Type-II QCS codes when BLER reaches $\sim 10^{-7}$, whereas an early error floor appears for Code-C-2^8 and Code-C-2^9. Moreover, in term of decoding complexity, the SPA performed over $\mathbb{F}_4$ for the proposed QCS codes requires less computational complexity compared to that of performing over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$ for Code-C-2^8 and Code-C-2^9,

5.3 Quantum LDPC codes From Tensor Product of Parity-Check Matrices

In this section, we consider two designs, namely *Construction A* and *Construction B*. For both designs, we use quadratic residue (QR) sets of prime size with parameter $p = 4n \pm 1, n \geq 2$, and its associated *idempotent polynomials* defined in (4.2) to construct the desired proto-matrix. We show that for Construction A, the proposed method yields a $[[pv, pv - \rho, d_{min}]]$ proto-graph quantum LDPC code, where $\rho < pv$ and $v \in \mathbb{Z}^+$ is the order of the CPM. Moreover, Construction B explores the design of proto-graph quantum LDPC codes by performing tensor product between two non-binary parity-check matrices obtained from the idempotent polynomials of a QR set. The resulting proto-graph quantum LDPC codes are of parameters $[[p^2v, p^2v - \gamma(v-1) - 1, d_{min}]]$, where $\gamma \in \mathbb{Z}^+$ is the size of the extension field $\mathbb{F}_{2^\gamma}$ of binary field $\mathbb{F}_2$. Such a class of proto-graph quantum LDPC codes have a quantum code rate at least $R^Q > 0.9$.

In this part of the chapter, we shall look at different construction methods of quantum LDPC codes based on proto-matrix

$$\mathbf{B} = [u \quad u]^{1\times 2}, \tag{5.24}$$

where $u \in \mathbb{Z}^+$.

5.3.1 Pre-lifting with idempotent polynomials

Construction A. *For $n \in \mathbb{Z}^+$ and $p = 4n + 1$ being a prime integer, let*

$$\mathbf{B} = \begin{bmatrix} u & u \end{bmatrix}, \quad u = \frac{p-1}{2} \tag{5.25}$$

and the pre-lifted proto-matrix

$$\mathbf{B}_M = \begin{bmatrix} \mathbb{Q}^r(P) & \mathbb{Q}^{nr}(P) \end{bmatrix}, \quad M = p. \tag{5.26}$$

To obtain the non-binary proto-matrix

$$H_{proto} = \begin{bmatrix} H_{1proto} & H_{2proto} \end{bmatrix}, \tag{5.27}$$

we replace non-zero elements of $\mathbf{B}_M$ *with elements of* $\mathcal{Q}^{\mathcal{R}}$ *and* $\mathcal{Q}^{\mathcal{NR}}$*. Thus, the entries of* H_{1proto} *and* H_{2proto} *are determined by*

$$H_{1proto} = \sum_{i=1}^{\frac{p-1}{2}} \alpha^{2i} P^{\alpha^{2i}} \quad and \quad H_{2proto} = \sum_{i=1}^{\frac{p-1}{2}} \alpha^{2i-1} P^{\alpha^{2i-1}}. \tag{5.28}$$

Then for an arbitrary $v \in \mathbb{Z}^+$ *and* $v >> p$*, the resulting parity-check matrices*

$$\begin{aligned} &H_1 = \left[P^{H_{1proto}(i,j)} \right] \quad and \quad H_2 = \left[P^{H_{2proto}(i,j)} \right], \\ &\forall H_{1proto}(i,j) \neq 0, \forall H_{2proto}(i,j) \neq 0, \end{aligned} \tag{5.29}$$

lifted from H_{1proto} H_{2proto} *are self-orthogonal with respect to the SIP. If the* (i,j)*-th element of* H_{1proto} *or* H_{2proto} *is zero, we lift it with an* $v \times v$ *all-zero matrix.*

Example 5.4. *Consider the case when* $n = 3$ *and* $p = 13$ *is a prime. The QR set and NQR set generated by* $\alpha = 4$ *are*

$$\mathcal{Q}^{\mathcal{R}} = \{4, 3, 12, 9, 10, 1\} \ and \ \mathcal{Q}^{\mathcal{NR}} = \{2, 8, 6, 11, 5, 7\}$$

with idempotent polynomials

$$\begin{aligned} \mathbb{Q}^r(x) &= x + x^3 + x^4 + x^9 + x^{10} + x^{12}, \\ \mathbb{Q}^{nr}(x) &= x^2 + x^5 + x^6 + x^7 + x^8 + x^{11}. \end{aligned}$$

The proto-matrix $\mathbf{B} = [6 \quad 6]$ *is pre-lifted into* $\mathbf{B}_{13} = \begin{bmatrix} \mathbb{Q}^r(P) & \mathbb{Q}^{nr}(P) \end{bmatrix}$*. By replacing non-zero elements of* $\mathbf{B}_{13}$ *with elements of* $\mathcal{Q}^{\mathcal{R}}$ *or* $\mathcal{Q}^{\mathcal{NR}}$ *according to (5.28), we obtain the proto-matrix* $H_{proto} = [H_{1proto} \quad H_{2proto}]$ *with* H_{1proto} *and* H_{2proto} *given*

by

$$H_{1proto} = \begin{bmatrix} 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 \\ 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 \\ 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 \\ 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 \\ 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 \\ 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 \\ 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 & 0 \\ 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 & 0 \\ 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 & 4 \\ 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 & 3 \\ 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 & 0 \\ 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 & 1 \\ 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 & 9 & 10 & 0 & 12 & 0 \end{bmatrix} \tag{5.30}$$

and

$$H_{2proto} = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 \\ 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 \\ 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 \\ 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 \\ 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 & 7 \\ 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 & 6 \\ 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 & 5 \\ 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 5 & 6 & 7 & 8 & 0 & 0 & 11 & 0 & 0 \end{bmatrix}. \tag{5.31}$$

In this particular example, the girth is 4 *since*

$$H_{1proto}(1,5) - H_{1proto}(2,5) = H_{1proto}(1,11) - H_{2proto}(2,11).$$

Similar indices can also be found in H_{2proto}.

Let $v \in \mathbb{Z}^+$ *and* $v >> p$. *We obtain a pair of parity-check matrices* H_1 *and* H_2 *of size* $13v \times 13v$ *that are self-orthogonal with respect to the SIP. Hence, by removing any rows of* H_1 *and* H_2, *the resulting sub-matrices* H_1^{sub} *and* H_2^{sub} *of size* $\rho \times 13v$ *are*

also self-orthogonal with respect to the SIP, where $\rho < 13v$. *Let* $H = [H_1^{sub}|H_2^{sub}]$, *then* H *defines a quantum LDPC code of parameters* $[[13v, 13v - \rho, d_{min}]]$.

5.3.2 Tensor product construction method

In this section, we introduce the second construction method for high rate quantum LDPC codes using tensor product of two non-binary matrices.

For $n \in \mathbb{Z}^+$ and $p = 4 - 1$ being a prime, let

$$\mathbf{B}_M = \begin{bmatrix} A_1 & A_2 \end{bmatrix}, \quad M = p, \tag{5.32}$$

where $A_1 = \mathbb{Q}^r(P)$ and $A_2 = \bar{\mathbb{Q}}^r(P)$ with $Rank(A_1) = \frac{p+1}{2}$ and $Rank(A_2) = \frac{p-1}{2}$. Note that A_1 and A_2 are generator matrices of quadratic residue codes [35]. Denote by $\Lambda_m(G) : \mathbb{F}_2 \to \mathbb{F}_{2^m}$ the transformation of matrix G from base field $\mathbb{F}_2$ to extension field $\mathbb{F}_{2^m}$. We propose the following construction method.

Construction B. *Let* $A_1^{''} = \Lambda_{\frac{p+1}{2}}(A_1)$ *and* $A_2^{''} = \Lambda_{\frac{p-1}{2}}(A_2)$ *be of the form*

$$\begin{aligned} A_1^{''} &= \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,p} \end{bmatrix} \\ A_2^{''} &= \begin{bmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,p} \end{bmatrix}, \end{aligned} \tag{5.33}$$

where $a_{1,i}$ *and* $b_{1,i}$ *for* $1 \leq i \leq p$ *are elements of* $\mathbb{F}_{2^{\frac{p+1}{2}}}$ *since* $\mathbb{F}_{2^{\frac{p-1}{2}}} \subset \mathbb{F}_{2^{\frac{p+1}{2}}}$. *Then the matrices* $h_1^{''}$ *and* $h_2^{''}$ *defined as the tensor product of* $A_1^{''}$ *and* $A_2^{''}$ *is given by*

$$\begin{aligned} h_1^{''} = A_1^{''} \otimes A_2^{''} &= \begin{bmatrix} a_{1,1}A_2^{''} & a_{1,2}A_2^{''} & \dots & a_{1,p}A_2^{''} \end{bmatrix}, \\ h_2^{''} = A_2^{''} \otimes A_1^{''} &= \begin{bmatrix} b_{1,1}A_1^{''} & b_{1,2}A_1^{''} & \dots & b_{1,p}A_1^{''} \end{bmatrix}. \end{aligned} \tag{5.34}$$

The components of the matrices $h_1^{''}$ *and* $h_2^{''}$ *are products of components from the matrices* $A_1^{''}$ *and* $A_2^{''}$. *These products are formed according to the rules of multiplication for elements from* $\mathbb{F}_{2^{\frac{p+1}{2}}}$. *Let* $\gamma = \frac{p-1}{2}$. *We generate the matrices* $H_1^{''}$ *and*

$H_2^{''}$ *as*

$$H_1^{''} = \begin{bmatrix} h_1^{''} \\ (h_1^{''})^2 \\ \vdots \\ (h_1^{''})^{\gamma} \end{bmatrix}, \quad H_2^{''} = \begin{bmatrix} h_2^{''} \\ (h_2^{''})^2 \\ \vdots \\ (h_2^{''})^{\gamma} \end{bmatrix}. \tag{5.35}$$

Let $v \in \mathbb{Z}^+$ *and* $v >> p$. *By performing the lift operation on* $H_1^{''}$ *and* $H_2^{''}$, *we obtain two matrices* $H_1 = [P^{e_{i,j}}] \in \{0,1\}^{\gamma v \times p^2 v}$ *and* $H_2 = [P^{e_{i,j}}] \in \{0,1\}^{\gamma v \times p^2 v}$ *of size* $\gamma v \times p^2 v$ *that are self-orthognal with respect to the SIP. Note that the rank of* H_1 *and* H_2 *is given by* $Rank(H_1) = Rank(H_2) = \gamma(v-1)+1$, *which means the proposed Construction B yields proto-graph quantum LDPC codes with parameters* $[[p^2 v, p^2 v - \gamma(v-1) - 1, d_{min}]]$.

We now provide an example illustrating how the construction is performed.

Example 5.5. *Consider the case when* $n = 2$ *and* $p = 7$. *The idempotent polynomials* $\mathbb{Q}^r(x) = x + x^2 + x^4$ *and* $\bar{\mathbb{Q}}^r(x) = 1 + x^3 + x^5 + x^6$ *are obtained from* $\mathcal{Q}^{\mathcal{R}} = \{1, 2, 4\}$ *and* $\bar{\mathcal{Q}}^{\mathcal{R}} = \{0, 3, 5, 6\}$. *Let*

$$A_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix} \quad \textit{and} \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{5.36}$$

be the generator matrices of the binary $[7, 4, 3]$ *and* $[7, 3, 4]$ *quadratic residue codes, respectively. Then we obtain*

$$A_1^{''} = \Lambda_4(A_1) = \begin{bmatrix} \alpha^3 & 1 & \alpha^4 & \alpha^5 & \alpha^{13} & \alpha^9 & \alpha^2 \end{bmatrix} \tag{5.37}$$

over $\mathbb{F}_{2^4}$ *with primitive polynomial* $m_1^{''}(x) = 1 + x + x^4$ *and*

$$A_2^{''} = \Lambda_3(A_2) = \begin{bmatrix} \alpha^5 & \alpha^4 & \alpha^2 & 1 & \alpha^1 & \alpha^6 & \alpha^3 \end{bmatrix} \tag{5.38}$$

over $\mathbb{F}_{2^3}$ *with primitive polynomial* $m_2''(x) = 1 + x + x^3$ *for some primitive element* α. *The resulting tensor product codes with check matrices* h_1'' *and* h_2'' *are given by*

$$h_1'' = A_1'' \otimes A_2''$$
$$= \begin{bmatrix} \alpha^8 & \alpha^7 & \alpha^5 & \alpha^3 & \alpha^4 & \alpha^9 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^2 & 1 & \alpha \\ \alpha^6 & \alpha^3 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha^{10} & \alpha^7 & \alpha^{10} & \alpha^9 & \alpha^7 \\ \alpha^5 & \alpha^6 & \alpha^{11} & \alpha^8 & \alpha^3 & \alpha^2 & 1 & \alpha^{13} & \alpha^{14} & \alpha^4 & \alpha & \alpha^{14} \\ \alpha^{13} & \alpha^{11} & \alpha^9 & \alpha^{10} & 1 & \alpha^{12} & \alpha^7 & \alpha^6 & \alpha^4 & \alpha^2 & \alpha^3 & \alpha^8 & \alpha^5 \end{bmatrix}$$

and

$$h_2'' = A_2'' \otimes A_1''$$
$$= \begin{bmatrix} \alpha^8 & \alpha^5 & \alpha^9 & \alpha^{10} & \alpha^3 & \alpha^{14} & \alpha^7 & \alpha^7 & \alpha^4 & \alpha^8 & \alpha^9 & \alpha^2 \\ \alpha^{13} & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^7 & 1 & \alpha^{11} & \alpha^4 & \alpha^3 & 1 & \alpha^4 \\ \alpha^5 & \alpha^{13} & \alpha^9 & \alpha^2 & \alpha^4 & \alpha^1 & \alpha^5 & \alpha^6 & \alpha^{14} & \alpha^{10} & \alpha^3 & \alpha^9 \\ \alpha^6 & \alpha^{10} & \alpha^{11} & \alpha^4 & 1 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^8 & \alpha^1 & \alpha^{12} & \alpha^5 \end{bmatrix}.$$

Let $\gamma = 3$. *The corresponding matrices* H_1'' *and* H_2'' *are given in Equations (5.39) and (5.40) (next page). Let* $v \in \mathbb{Z}^+$ *and* $v >> p$. *By lifting* H_1'' *and* H_2'' *with* P *of order* v, *we obtain* H_1 *and* H_2 *that are self-orthogonal with respect to the SIP. Thus,* H_1 *and* H_2 *yield a proto-graph quantum LDPC code of parameter* $[[49v, 46v + 2, d_{min}]]$.

5.3.3 Simulation results

We now provide simulation results of the proposed proto-graph quantum LDPC codes over quantum depolarizing channels with an iterative sum-product decoding algorithm. The input of the decoding algorithm is the syndrome vector $\mathbf{s}$ with entries in $\{+1, -1\}$. We assume the depolarizing channel with marginal flip probability $\frac{2f}{3}$ of X errors and Z errors, where f is the total depolarizing strength of the channel, and assume the decoder knows the marginal flip probability $f_m = \frac{2f}{3}$.

Fig. 5.7 shows the block error rate (BLER) performance of quantum LDPC codes constructed from Constructions A and B. The code denoted as 'Code-lifting' is a $[[13v, 13v - \rho, d_{min}]] = [[1651, 1551, d_{min}]]$ proto-graph quantum LDPC code with code rate $R^Q = 0.94$, and the code denoted as 'Code-tensor' is a $[[42v, 39v +$

$$H_1^{''} =$$

$$\begin{bmatrix} \alpha^8 & \alpha^7 & \alpha^5 & \alpha^3 & \alpha^4 & \alpha^9 & \alpha^6 & \alpha^5 & \alpha^4 & \alpha^2 & 1 & \alpha & \alpha^6 & \alpha^3 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^4 & \alpha^5 & \alpha^{10} & \alpha^7 & \alpha^{10} & \alpha^9 & \alpha^7 & \alpha^5 & \alpha^6 & \alpha^{11} & \alpha^8 & \alpha^3 & \alpha^2 & 1 & \alpha^{13} & \alpha^{14} & \alpha^4 & \alpha & \alpha^{14} & \alpha^{13} & \alpha^{11} & \alpha^9 & \alpha^{10} & 1 & \alpha^{12} & \alpha^7 & \alpha^6 & \alpha^4 & \alpha^2 & \alpha^3 & \alpha^8 & \alpha^5 \\ \alpha & \alpha^{14} & \alpha^{10} & \alpha^6 & \alpha^8 & \alpha^3 & \alpha^{12} & \alpha^{10} & \alpha^8 & \alpha^4 & 1 & \alpha^2 & \alpha^{12} & \alpha^6 & \alpha^3 & \alpha & \alpha^{12} & \alpha^8 & \alpha^{10} & \alpha^5 & \alpha^{14} & \alpha^5 & \alpha^3 & \alpha^{14} & \alpha^{10} & \alpha^{12} & \alpha^7 & \alpha & \alpha^6 & \alpha^4 & 1 & \alpha^{11} & \alpha^{13} & \alpha^8 & \alpha^2 & \alpha^{13} & \alpha^{11} & \alpha^7 & \alpha^3 & \alpha^5 & 1 & \alpha^9 & \alpha^{14} & \alpha^{12} & \alpha^8 & \alpha^4 & \alpha^6 & \alpha & \alpha^{10} \\ \alpha^9 & \alpha^6 & 1 & \alpha^9 & \alpha^{12} & \alpha^{12} & \alpha^3 & 1 & \alpha^{12} & \alpha^6 & 1 & \alpha^3 & \alpha^3 & \alpha^9 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^{12} & 1 & 1 & \alpha^6 & 1 & \alpha^{12} & \alpha^6 & 1 & \alpha^3 & \alpha^3 & \alpha^9 & \alpha^9 & \alpha^6 & 1 & \alpha^9 & \alpha^{12} & \alpha^{12} & \alpha^3 & \alpha^{12} & \alpha^9 & \alpha^3 & \alpha^{12} & 1 & 1 & \alpha^6 & \alpha^6 & \alpha^3 & \alpha^{12} & \alpha^6 & \alpha^9 & \alpha^9 & 1 \end{bmatrix} \tag{5.39}$$

$$H_2^{''} =$$

$$\begin{bmatrix} \alpha^8 & \alpha^5 & \alpha^9 & \alpha^{10} & \alpha^3 & \alpha^{14} & \alpha^7 & \alpha^7 & \alpha^4 & \alpha^8 & \alpha^9 & \alpha^2 & \alpha^{13} & \alpha^6 & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^7 & 1 & \alpha^{11} & \alpha^4 & \alpha^3 & 1 & \alpha^4 & \alpha^5 & \alpha^{13} & \alpha^9 & \alpha^2 & \alpha^4 & \alpha & \alpha^5 & \alpha^6 & \alpha^{14} & \alpha^{10} & \alpha^3 & \alpha^9 & \alpha^6 & \alpha^{10} & \alpha^{11} & \alpha^4 & 1 & \alpha^8 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^8 & \alpha & \alpha^{12} & \alpha^5 \\ \alpha & \alpha^{10} & \alpha^3 & \alpha^5 & \alpha^6 & \alpha^{13} & \alpha^{14} & \alpha^{14} & \alpha^8 & \alpha & \alpha^3 & \alpha^4 & \alpha^{11} & \alpha^{12} & \alpha^{10} & \alpha^4 & \alpha^{12} & \alpha^{14} & 1 & \alpha^7 & \alpha^8 & \alpha^6 & 1 & \alpha^8 & \alpha^{10} & \alpha^{11} & \alpha^3 & \alpha^4 & \alpha^8 & \alpha^2 & \alpha^{10} & \alpha^{12} & \alpha^{13} & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^{12} & \alpha^5 & \alpha^7 & \alpha^8 & 1 & \alpha & \alpha^{12} & \alpha^6 & \alpha^{14} & \alpha & \alpha^2 & \alpha^9 & \alpha^{10} \\ \alpha^9 & 1 & \alpha^{12} & 1 & \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^6 & \alpha^{12} & \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^9 & \alpha^3 & 1 & \alpha^6 & \alpha^3 & \alpha^6 & 1 & \alpha^3 & \alpha^{12} & \alpha^9 & 1 & \alpha^{12} & 1 & \alpha^9 & \alpha^{12} & \alpha^6 & \alpha^{12} & \alpha^3 & 1 & \alpha^3 & \alpha^{12} & 1 & \alpha^9 & \alpha^{12} & \alpha^3 & 1 & \alpha^3 & \alpha^{12} & 1 & \alpha^9 & \alpha^3 & \alpha^9 & \alpha^6 & \alpha^9 & \alpha^3 & \alpha^6 & 1 \end{bmatrix} \tag{5.40}$$

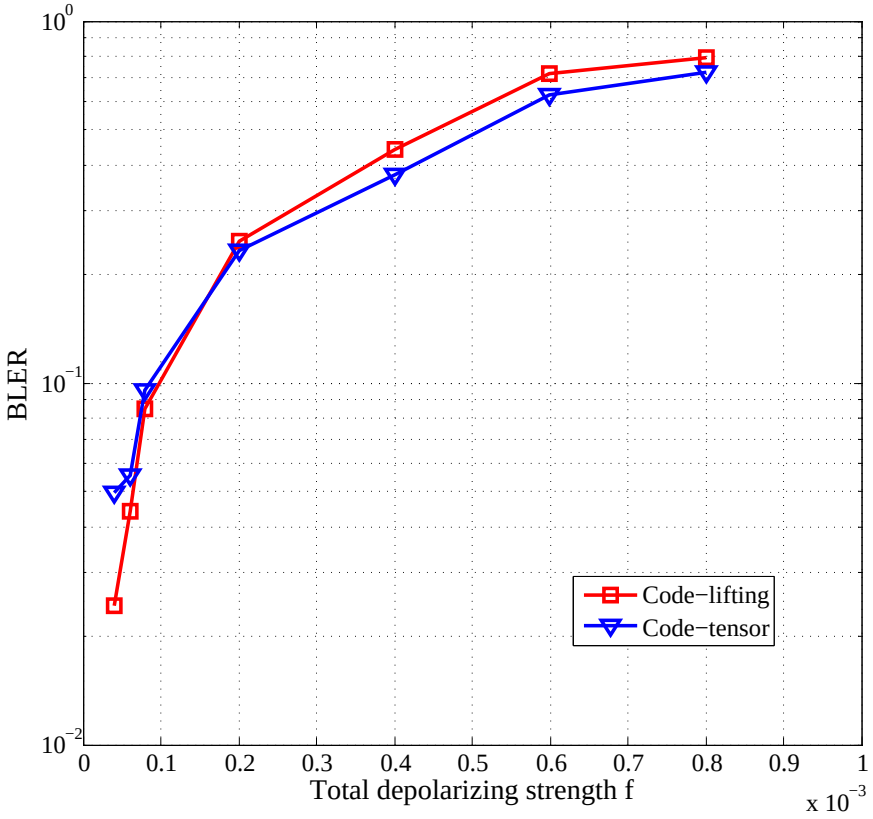

FIGURE 5.7: Code performance of the proposed proto-graph quantum LDPC codes. $\square$: $[[1651, 1551]]$, $R^Q = 0.94$; $\bigtriangledown$: $[[1638, 1523]]$, $R^Q = 0.93$.

$2, d_{min}]] = [[1638, 1523, d_{min}]]$ proto-graph quantum LDPC code with code rate $R^Q = 0.93$. The former code is constructed based on the QR set shown in Example 5.4 with CPM order $v = 127$ and $\rho = 100$. The later code is constructed based on the QR set shown in Example 5.5 with associated non-binary parity-check matrices given in (5.39) and (5.40). For the second code, we first shorten the parity-check matrices H_1'' and H_2'' by removing the common columns $\{1, 9, 17, 25, 33, 41, 49\}$ in both matrices, then we lift the shortened parity-check matrices with CPM of order $v = 39$. Note that since the difference between H_1'' and H_2'' at these column positions is a $\gamma \times 1$ all-zero vector, removing these columns will preserve the orthogonality of the resulting binary matrices. From the figure, the proposed proto-graph quantum LDPC code constructed from lifting method shows better performance compare to the code constructed from tensor product method when the total flip probability of the channel approaches to zero.

5.4 Chapter summary

In this chapter, we developed a systematic way to design general stabilizer quantum LDPC codes of quasi-cyclic structure using the notion of proto-matrix (and proto-graph). By designing a Latin square based proto-matrix using quadratic (non-) residue sets of prime modulus, and its equivalent matrices using transformation matrices, the proposed construction methods yield a wide range of quantum LDPC codes with different code lengths and rates. Furthermore, we proposed a class of proto-graph quantum LDPC codes with code rate as high as above 0.9 by using tensor product operation between a pair of non-binary parity-check matrices. In the last, it is interesting to determine the minimum distance of proto-graph quantum LDPC codes in the future work and to develop an efficient sum-product decoding algorithm for the tensor product quantum LDPC codes.

Chapter 6

Quantum Synchronizable Codes

In classical communication systems, misalignment in block synchronization is another type of error that causes catastrophic failure, where the information processing device misidentifies the boundaries of an information block. For instance, assume that each chunk of information is encoded into a block of three consecutive bits in a stream of bits b_i so that the data has a frame structure. If four blocks of information are encoded, we have twelve ordered bits $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11})$ in which each of the four blocks (b_0, b_1, b_2), (b_3, b_4, b_5), (b_6, b_7, b_8), and (b_9, b_{10}, b_{11}) forms an information chunk. If, for example, misalignment occurs to the right by two bits when attempting to retrieve the second block of information, the device will wrongly read out b_5, b_6, and b_7 instead of the correct set of bits b_3, b_4, and b_5. The same kind of error in block synchronization may be considered for a stream of qubits.

A *quantum synchronizable code* (QSC) is a coding scheme that corrects general quantum noise represented by Pauli errors as well as block synchronization errors. A theoretical framework of quantum synchronizable coding was first introduced in [140] as a quantum analogue of synchronizable coding in classical coding theory that attempts to correct both bit flips and block synchronization errors [139]. Subsequent studies have improved the original construction method and given further examples of quantum synchronizable codes [141, 142].

In general, quantum synchronizable codes can be constructed from classical cyclic codes with additional properties through a method similar to the one studied in [143]. However, while the quantum analogue of cyclic codes given in [143] only requires a cyclic code that contains its dual, the known general construction for quantum synchronizable codes requires a chain of three cyclic codes satisfying further complicated properties, making it harder to explicitly construct promising examples.

In this chapter, we construct quantum synchronizable codes by exploiting special classical cyclic codes over the finite field $\mathbb{F}_2$ of order 2, called quadratic residue codes. Quadratic residue codes tend to have large minimum distances [35]. Thus, it is reasonable to expect that quantum error-correcting codes that exploit quadratic residue codes possess good error correction performance. We show that quantum synchronizable codes from quadratic residue codes also have good block synchronization capabilities. In fact, the proposed quantum synchronizable codes attain the known upper bound on the maximum tolerable magnitude of misalignment in some cases. Note that the concept of the proposed method also applies to the general cyclic codes.

We begin with an overview of what quantum synchronizable codes are and how they deal with misalignment errors. We then study the general classical q-ary cyclic codes and derive a general construction of QSC using nested cyclic codes. We then use classical quadratic residue codes to demonstrate our general construction of QSCs.

6.1 Quantum synchronizable code

An $[[n, k]]$ *quantum error-correcting code* is a coding scheme that encodes k logical qubits into n physical qubits. As in the classical case, n and k are the *length* and *dimension* of the code, respectively. Typically, quantum error-correcting codes are designed to correct the effects of bit errors and phase errors caused by Pauli operators X and Z respectively under the assumption that both bit error due to X

and phase error due to Z may occur on the same qubit. A (c_l, c_r)-$[[n, k]]$ *quantum synchronizable code* is an $[[n, k]]$ quantum error-correcting code that corrects not only bit errors and phase errors but also misalignment to the left by c_l qubits and to the right by c_r qubits for some nonnegative integers c_l and c_r.

The general construction method for quantum synchronizable codes developed in [140, 141] employs a notion in finite algebra. Let $f(x) \in \mathbb{F}_2[x]$ be a polynomial over $\mathbb{F}_2$ such that $f(0) = 1$. The *order* $\mathrm{ord}\,(f(x))$ of the polynomial $f(x)$ is the cardinality $|\{x^a \pmod{f(x)} \mid a \in \mathbb{Z}\}|$, where $\mathbb{Z}$ is the set of positive integers.

Theorem 6.1. *[141] Let $\mathcal{C}_1 = \langle g_1(x)\rangle$ and $\mathcal{C}_2 = \langle g_2(x)\rangle$ be two cyclic codes of parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$ with $k_1 > k_2$ respectively such that $\mathcal{C}_2 \subset \mathcal{C}_1$ and $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_2$. Define $f(x)$ of degree $k_1 - k_2$ to be the quotient of $\frac{g_2(x)}{g_1(x)}$ over $\mathbb{F}_2[x]/(x^n - 1)$. For any pair of nonnegative integers c_l, c_r satisfying $c_l + c_r < \mathrm{ord}\,(f(x))$, there exists a (c_l, c_r)-$[[n + c_l + c_r, 2k_2 - n]]$ quantum synchronizable code that corrects at least up to $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors and at least up to $\lfloor \frac{d_2-1}{2} \rfloor$ phase errors.*

Theorem 6.1 requires a pair of cyclic codes $\mathcal{C}_1, \mathcal{C}_2$ of the same length and dimension $k_1 > k_2 > \lceil \frac{n}{2} \rceil$ to construct a quantum synchronizable code of positive dimension. To design a good quantum synchronizable code, it is generally desirable to choose cyclic codes with good minimum distances while ensuring $\mathrm{ord}\,(f(x))$ to be as large as possible. In addition to these criteria, the cyclic codes must satisfy the chain condition that $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_2 \subset \mathcal{C}_1$. Note that this is stronger than the dual-containing condition for the quantum cyclic codes given in [143]. In what follows, when a pair of cyclic codes is written as $\mathcal{C}_1$ and $\mathcal{C}_2$, we always assume that they satisfy the chain condition and that their generator polynomials are $g_1(x)$ and $g_2(x) = f(x)g_1(x)$ for some polynomial $f(x)$, respectively.

6.1.1 Encoding

Since $dim\,(\mathcal{C}_2) = k_2$ and $dim\left(\mathcal{C}_2^{\perp}\right) = n - k_2$, the dimension of the cosets is $dim\left(\mathcal{C}_2/\mathcal{C}_2^{\perp}\right) = k_2 - n + k_2 = 2k_2 - n$. Hence, the number of cosets is 2^{2k_2-n}.

Let $\mathcal{B} = \{b_i(x) \mid 0 < i \leq 2^{2k_2-n}\}$ be a system of representatives of the cosets. Then the set

$$V = \left\{ \left| \mathcal{C}_2^{\perp} + b_i(x) \right\rangle \;\middle|\; b_i(x) \in \mathcal{B} \right\}$$

of 2^{2k_2-n} quantum states forms an orthogonal basis of a vector space of dimension 2^{2k_2-n}, where

$$\left| \mathcal{C}_2^{\perp} + b_i(x) \right\rangle = \frac{1}{\sqrt{|\mathcal{C}_2^{\perp}|}} \sum_{c(x) \in \mathcal{C}_2^{\perp}} |c(x) + b_i(x)\rangle \,.$$

Take an arbitrary $2k_2 - n$-qubit state $|\psi\rangle$ to be encoded. Using the standard encoder for Calderbank-Shor-Steane (CSS) codes [11], the state $|\psi\rangle$ is transformed into n-qubit state $|\psi\rangle_{enc} = \sum_i \alpha_i |v_i\rangle$, where $v_i \in V$.

Recall that $g_1(x)$ is the generator polynomial of $\mathcal{C}_1$. Apply the unitary operator U_g that adds the coefficient vector of $g_1(x)$:

$$U_g |\psi\rangle_{enc} \to \sum_i \alpha_i |v_i + g_1\rangle.$$

Let c_r, c_l be nonnegative integers such that $c_l + c_r < \operatorname{ord}(f(x))$. By attaching extra c_l and c_r ancilla qubits to the left and to the right of the original state respectively and then applying CNOT gates, the state is taken to the final encoded $(n+c_l+c_r)$-qubit state

$$|0\rangle^{\otimes c_l} U_g(|\psi\rangle_{enc}) |0\rangle^{\otimes c_r} \to \sum_i \alpha_i |l_i, v_i + g_1, r_i\rangle = |\Psi\rangle_{enc},$$

where l_i and r_i are the last c_l and the first c_r portions of the vector $v_i + g_1$, respectively.

6.1.2 Synchronization recovery

Assume that the device gathered qubits of one block length, that is, consecutive $n + c_l + c_r - 1$ qubits, and tries to correct errors caused by Pauli operators and misalignment if necessary. Let $\mathcal{T} = (t_0, t_1, \ldots, t_{n+c_l+c_r-1})$ be the collection of

$n + c_l + c_r$ qubits at the output of the quantum channel. If block synchronization is correct, $\mathcal{T}$ forms a properly aligned block encoded as $|\Psi\rangle_{enc}$. We assume that $\mathcal{T}$ may be misaligned by θ qubits to the right, where $-c_l \leq \theta \leq c_r$. When θ is negative, it means that misalignment is to the left by $|\theta|$ qubits.

Let $\mathcal{S} = (s_0, s_1, \ldots, s_{n+c_l+c_r-1})$ be the $n + c_l + c_r$ qubits of $|\Psi\rangle_{enc}$. The device first focuses on consecutive n qubits $\mathcal{W} = (t_{c_l}, t_{c_l+1}, \ldots, t_{c_l+n-1})$ in the middle of $\mathcal{T}$. Because of the potential misalignment, this set of qubits is $\mathcal{W} = (s_{c_l+\theta}, s_{c_l+1+\theta}, \ldots, s_{c_l+n-1+\theta})$.

Let E be the $(n + c_l + c_r)$-fold tensor product of single Pauli operators that represents errors that occurred on $|\Psi\rangle_{enc}$. The corrupted state at the quantum channel output is given by

$$E|\Psi\rangle_{enc} = \sum_i \alpha_i (-1)^{(l_i, v_i+g_1, r_i)\cdot \mathbf{e_p}} |(l_i, v_i + g_1, r_i) + \mathbf{e_b}\rangle,$$

where $\mathbf{e_b}$ and $\mathbf{e_p}$ are binary vectors representing bit and phase errors, respectively.

The device first corrects bit errors on $\mathcal{W}$ and then detects misalignment. Let $\mathcal{H}_{\mathcal{C}_1}$ be the full-rank parity-check matrix of $\mathcal{C}_1$ used for encoding. Using the stabilizer generators defined by $\mathcal{C}_1$, the decoding circuit obtains the syndrome for bit errors as in the standard two-step decoding of a CSS code:

$$E|\Psi\rangle_{enc}|0\rangle^{\otimes n-k_1} \rightarrow E|\Psi\rangle_{enc}|\mathbf{e_b}\mathcal{H}_{\mathcal{C}_1}^T\rangle.$$

If the number of bit errors is at most $\lfloor \frac{d_1-1}{2} \rfloor$ in $\mathcal{W}$, applying X Pauli operators to the qubits specified by $\mathbf{e_b}\mathcal{H}_{\mathcal{C}_1}^T$ eliminates all bit errors within the window $\mathcal{W}$.

The next step is to identify how many qubits away $\mathcal{W}$ is from the correct position $\mathcal{S}$, that is, identifying the magnitude θ. To this end, we manipulate the polynomials used as the labels of each basis state. Such operations can be done, for example, by a quantum shift register given in [143].

Note that the condition that $\mathcal{C}_2^\perp \subset \mathcal{C}_2 \subset \mathcal{C}_1$ implies that any codeword $c_i^\perp(x) \in \mathcal{C}_2^\perp$ also belongs to $\mathcal{C}_2$ and $\mathcal{C}_1$. Hence, each basis of the state of $\mathcal{S}$ is a sum of states of

the form

$$\left|c_i^{\perp}(x) + b_i(x) + g_1(x)\right\rangle = \\ |v_1(x)f(x)g_1(x) + v_2(x)f(x)g_1(x) + g_1(x)\rangle\,,$$

for some polynomials $v_1(x)$ and $v_2(x)$ whose degrees are less than k_2. Because of the misalignment, each basis of the state of $\mathcal{W}$ is a linear combination of states of the form $\left|x^{\theta}\left(c_i^{\perp}(x) + b_i(x) + g_1(x)\right)\right\rangle$. Thus, the quotient of the label of each basis of the state of $\mathcal{W}$ divided by $g_1(x)$ is $x^{\theta}(v_1(x)f(x) + v_2(x)f(x) + 1)$. Dividing this quotient by $f(x)$ gives x^{θ} as the remainder. Thus, if $c_l + c_r < \mathrm{ord}(f(x))$, the synchronization error θ is uniquely determined.

Once we know the number of qubits that $\mathcal{W}$ is misaligned, the same error correction for bit errors can be applied to the qubits outside the initial window $\mathcal{W}$ by sliding the window on the $n + c_r + c_l$ consecutive qubit frame. If the channel introduces at most $\lfloor \frac{d_1-1}{2} \rfloor$ bit errors on any n consecutive qubits, then all bit errors can be corrected and obtain the state $E'|\Psi\rangle_{enc}$, where E' introduces only phase errors.

To correct phase errors E' on our $n + c_r + c_l$ consecutive qubits, the process of extension operation and the unitary operation U_g is reversed since we only care about the phase errors upon the n qubits in $\mathcal{W}$ without any misalignment error. The reverse operation is

$$E'|\Psi\rangle_{enc} \to \sum_i \alpha_i (-1)^{(v_i+g_1)\cdot(e_n+(0,e_l)+(e_r,0))}|v_i\rangle, \tag{6.1}$$

where (e_l, e_n, e_r) is the binary error vector. The notation $(0, e_l)$ and $(e_r, 0)$ is the n-dimensional binary vector by padding $n - c_l$ and $n - c_r$ zeros, respectively. The encoded state $|\Psi\rangle_{enc}$ is stabilized by the stabilizer generated by $\mathcal{C}_2$. Denote by e_p the total number of phase error among the $n + c_l + c_r$ qubits. If $e_p \leq \frac{d_2-1}{2}$, we can correctly diagnose the effect of $(e_n + (0, e_l) + (e_r, 0))$ through the standard phase error correction procedure for CSS codes. That is

$$E''|\psi\rangle_{enc}|0\rangle^{n-k_2} \to E''|\psi\rangle_{enc}|\mathcal{H}_{\mathcal{C}_2}\left(e_n + (0, e_l) + (e_r, 0)\right)\rangle, \tag{6.2}$$

where $\mathcal{H}_{\mathcal{C}_2}$ is the parity-check matrix of $\mathcal{C}_2$ and E'' is the phase error on $|\psi\rangle$ caused

by $(e_n + (0, e_l) + (e_r, 0))$. Based on the error syndrome obtained by measuring the last $n - k_2$ ancilla qubits, applying Z operators on appropriate qubits removes the phase error and completes the error correction procedure.

Recognised quantum synchronizable codes employ well-known classes of cyclic codes called *narrow-sense Bose-Chaudhuri-Hocquenghem* (BCH) *codes* [140] and *punctured Reed-Muller codes* [141]. The design of QSCs from finite geometry can also be found in [142].

6.2 Chain - containing quantum synchronizable codes

6.2.1 q-ary cyclic codes

Let q be a power of a prime. Denoted by $\mathbb{F}_q$ the finite field of order q, and $\mathbb{F}_q[x]$ the set of all univariate polynomials with coefficients in $\mathbb{F}_q$ and the indeterminant x. A q-ary *cyclic* code $\mathcal{C}$ of length n, dimension k and minimum distance $d = \min\{\mathrm{wt}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}$, where $\mathrm{wt}(\mathbf{c})$ is the number of nonzero entries in $\mathbf{c}$, is denoted by $[n, k, d]_q$. The *dual code* $\mathcal{C}^\perp$ is defined as

$$\mathcal{C}^\perp = \{\mathbf{c}' \in \mathbb{F}_q^n \mid \mathbf{c}' \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$$

where $\mathbf{c}' \cdot \mathbf{c}$ is the dot-product and $\dim(\mathcal{C}^\perp) = n - \dim(\mathcal{C}) = n - k$.

By regarding a codeword $\mathbf{c}$ as a coefficient vector of a polynomial in $\mathbb{F}_q[x]$, an $[n, k, d]_q$ cyclic code $\mathcal{C}$ is an ideal in the ring $\mathbb{F}_q[x]/(x^n - 1)$ generated by the unique monic polynomial $g(x)$ of minimum degree. Each codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ is associated with a polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]$ that is divisible by $g(x)$. Thus, this unique polynomial $g(x)$ is called the *generator polynomial* of cyclic code $\mathcal{C}$ and has degree $deg\,(g(x)) = n - dim(\mathcal{C}) = n - k$. We

may understand cyclic codes as

$$\mathcal{C} = \{m(x)g(x) \mid m(x) \in \mathbb{F}_q[x], deg(m(x)) < k\}. \tag{6.3}$$

The polynomial $h(x)$ such that $g(x)h(x) = x^n - 1$ is called the *check polynomial* of $\mathcal{C}$. The dual code $\mathcal{C}^\perp$ is generated by the reciprocal polynomial of $h(x)$ which is given by

$$\mathcal{C}^\perp = \langle g^\perp(x) = x^{\deg(h(x))}h(x^{-1})\rangle. \tag{6.4}$$

We know from (6.3) that any codeword of $\mathcal{C}$ is a multiple of the generator polynomial $g(x)$ with roots in $\mathbb{F}_{q^z}$, where z is the smallest integer such that the code length n divides $q^m - 1$ (m is also known as the multiplicative order of q). Cyclic codes are often defined by the set of roots that could be obtained using the notions of *cyclotomic cosets*. A q-cyclotomic coset $C_{s,n}$ of s modulo n is the set

$$C_{s,n} = \{sq^i \mod n \mid \forall i = 0, 1, \ldots, n_s - 1\},$$

where n_s is the smallest integer such that $sq^{n_s} \equiv s \mod n$. Since $C_{s,n} = C_{s',n}$ for $s' \in C_{s,n}$, we may take

$$S_n = \{\min\{t \mid t \in C_{s,n}\} \mid t \in \mathbb{Z} \cup \{0\}\}$$

as a system of representatives of the cyclotomic cosets by picking the smallest element from each set.

Let α be an n-th root of unity in $\mathbb{F}_{q^z}$. By definition, the unique *irreducible minimal polynomial* $M_s(x) \in \mathbb{F}_q[x]$ of α^s can be expressed as

$$M_s(x) = \prod_{i \in C_{s,n}} (x - \alpha^i).$$

The *defining set* $\mathcal{D}$ of a q-ary cyclic code $\mathcal{C}$ is the set containing the indices of the zeros of the generator polynomial $g(x)$. Since the integers modulo n are partitioned

into cyclotomic cosets in a way described as

$$\{0, 1, \ldots, n-1\} = \bigcup_{s \in S_n} C_{s,n}, \tag{6.5}$$

the defining set of a q-ary cyclic code is given by

$$\mathcal{D} := \{i : g(\alpha^i) = 0\} = \bigcup_{\{s_i \mid 1 \leq i \leq |S_n|\} \subset S_n} C_{s_i,n}.$$

Hence, the generator polynomial $g(x)$ of degree $n-k$ of a q-ary cyclic code can be expressed as

$$g(x) = \prod_{\{s_i \mid 1 \leq i \leq |S_n|\} \subset S_n} M_{s_i}(x).$$

Because of the one-to-one correspondence between cyclic codes and monic divisors of $x^n - 1$, deleting one or more factors $M_s(x)$ gives another generator polynomial that results in a cyclic code of higher dimension.

Definition 6.2. Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two cyclic codes of length n. If $\mathcal{C}_2 \subseteq \mathcal{C}_1$, that is, if $\mathcal{C}_1$ contains all codewords of $\mathcal{C}_2$, then the generator polynomial $g_1(x)$ divides every codeword of $\mathcal{C}_2$, which means that for every $c(x) \in \mathcal{C}_2$ there exits a polynomial $f(x)$ of degree $\deg(c(x)) - (n - \dim(\mathcal{C}_1))$ such that $c(x) = f(x)g_1(x)$ in $\mathbb{F}_2[x]$. The smaller code $\mathcal{C}_2$ is a *subcode* of $\mathcal{C}_1$ while $\mathcal{C}_1$ is a *supercode* of $\mathcal{C}_2$. A cyclic code is *dual-containing* if it is a supercode of its dual code.

In the following, we design chain-containing (nested) quantum synchronizable codes. We require that, for any two cyclic codes $\mathcal{C}_1, \mathcal{C}_2 \in \mathscr{C}$ of parameters $[n, k_1, d_1]$ and $[n, k_2, d_2]$,

1. $g_1(x) \mid g_2(x) \mid g_2^{\perp}(x)$ for $\mathcal{C}_1 = \langle g_1(x) \rangle, \mathcal{C}_2 = \langle g_2(x) \rangle$.
2. $deg(g_2(x)) + deg(g_2^{\perp}(x)) = n$.

Note that '$a(x) \mid b(x)$' denotes the polynomial $b(x)$ is divisible by polynomial $a(x)$.

6.2.2 Chain-containing cyclic codes

We know that a generator polynomial of a q-ary cyclic code can be obtained from the product of minimal polynomials over $\mathbb{F}_q$. Therefore, by constructing supercodes of a given cyclic code, the special containing property can be fulfilled. Let $\Lambda = \{M_s(x) : s \in S_n\} \in \mathbb{F}_q[x]$ be the set of monic irreducible factors of $x^n - 1$. If $gcd(n, q) = 1$, there are no multiple factors. We can find all cyclic codes of length n over $\mathbb{F}_q$ by taking any of the $2^{|\Lambda|} - 2$ non-trivial monic factors of $x^n - 1$ as a generator polynomial.

Suppose $\mathcal{C}_2 = \langle g_2(x) = \prod_{i\in\mathcal{I},\mathcal{I}\subset S_n} M_i(x)\rangle$. Then by removing one $M_i(x)$, we obtain a supercode $\mathcal{C}_3 = \langle g_3(x) = \frac{g_2(x)}{M_i(x)}\rangle$ of $\mathcal{C}_2$ with $k_3 > k_2$, and removing a product $M_i(x) \cdot M_{i'}(x), i \neq i'$, we obtain a supercode $\mathcal{C}_4 = \langle g_4(x) = \frac{g_2(x)}{M_i(x)M_{i'}(x)}\rangle$ of both $\mathcal{C}_2$ and $\mathcal{C}_3$. Thus, $\mathcal{C}_2 \subset \mathcal{C}_3 \subset \mathcal{C}_4$ because $g_4(x) \mid g_3(x) \mid g_2(x)$. To obtain the dual code $\mathcal{C}_2^\perp$ such that $\mathcal{C}_2^\perp \subset \mathcal{C}_2$, from (6.4), the generator polynomial of $\mathcal{C}_2^\perp$ is

$$g_2^\perp(x) = x^{h(x)}h(x^{-1}) \equiv g_2(x)f(x), \tag{6.6}$$

where $h(x)$ is the check polynomial and

$$f(x) = \prod_{j\in S_n, j\notin\pm\mathcal{I}} M_j(x), \quad \forall j, M_j(x) \nmid g_2(x) \tag{6.7}$$

with

$$deg(f(x)) = n - 2\left(\sum_{i\in\mathcal{I},\mathcal{I}\subset S_n} |C_{i,n}|\right), \ \forall i, M_i(x) \mid g_2(x). \tag{6.8}$$

The following proposition states the necessary conditions when constructing a quantum synchronizable code from q-ary cyclic code.

Proposition 6.3. *(Chain-containing cyclic codes) Let n, m be some positive integers and q be a prime such that n divides $q^m - 1$ and $gcd(n, q) = 1$. The set of monic irreducible minimal polynomials $\Lambda = \{M_s(x) : s \in S_n\} \in \mathbb{F}_q[x]$ form a set of factors of $x^n - 1$. Let $\mathcal{C}_2 = \langle g_2(x) = \prod_{i\in\mathcal{I},\mathcal{I}\subset S_n} M_i(x)\rangle$ be a cyclic code of parameters $[n, k_2, d_2]$, then there exist $2^{|\mathcal{I}|} - 2$ supercodes $\mathcal{C}_1 = [n, k_1 > k_2, d_1 < d_2]$*

that contain $\mathcal{C}_2$, and its dual code $\mathcal{C}_2^{\perp} = \langle g_2^{\perp}(x) \rangle$ is a subcode of $\mathcal{C}_2$ if $g_2^{\perp}(x)$ satisfies the conditions (6.6) and (6.7). Then there exist a quantum synchronizable code of parameters $(c_l, c_r) - [[n + c_l + c_r, 2k_2 - n, d_{min}]]$. ■

Proof. Since $g_2(x)$ is reducible over $\mathbb{F}_{q^m}$ and $\mathcal{I} \subset S_n$, the number of removable factors are $\{1, 2, \ldots, |\mathcal{I}| - 1\}$, which implies

$$\binom{|\mathcal{I}|}{1} + \binom{|\mathcal{I}|}{2} + \cdots + \binom{|\mathcal{I}|}{|\mathcal{I}| - 1} = 2^{|\mathcal{I}|} - \binom{|\mathcal{I}|}{0} - \binom{|\mathcal{I}|}{|\mathcal{I}|} \equiv 2^{|\mathcal{I}|} - 2 \tag{6.9}$$

supercodes $\mathcal{C}_1$ that contain $\mathcal{C}_2$. Let α be a primitive n-th root of unity, then $g_2(\alpha^i) = g_2(\alpha^{iq}) = g_2(\alpha^{iq^2}) = \ldots = g_2(\alpha^{iq^{|C_{i,n}|}}) = 0$ for all $i \in \mathcal{I}$ and each cardinality $|C_{i,n}|$ divides m. By Equation (6.4) where $g_2^{\perp}(x)$ can be interpreted as the reciprocal polynomial of the check polynomial $h(x)$, we have, for all $i \in \mathcal{I}$,

$$g_2(\alpha^i) = g_2^{\perp}(\alpha^i) \equiv \alpha^{deg(h(x))} h(\alpha^{-i}) = 0$$

if $g_2(x) \mid g_2^{\perp}(x)$. Thus, $-\mathcal{I}$ is a set of roots of $h(x)$. Furthermore, recall that the associated defining set of $\mathcal{C}_2$ is determined as $\mathcal{D}_{\mathcal{C}_2} = \bigcup_{i \in \mathcal{I}} C_{i,n}$. Since $x^n - 1 = \prod_{j=0}^{n-1} (x - \alpha^j) = g_2(x)h(x)$, $h(\alpha^j) = 0 \ \forall j \notin \mathcal{D}_{\mathcal{C}_2}$. By the argument above where α^{-j} is also a root of $h(x)$, we have $-i \notin \mathcal{D}_{\mathcal{C}_2}$ for all $i \in \mathcal{I}$. Consequently, the defining set $\mathcal{D}_{\mathcal{C}_2^{\perp}} = \bigcup_{i \in \mathcal{I}} C_{-i,n} \bigcup_{i' \notin \pm\mathcal{I}} C_{i',n}$ and for any minimal polynomial $M_{i'}$, where $i' \notin \pm\mathcal{I}$, it has no roots in both $\mathcal{D}_{\mathcal{C}_2}$ and $-\mathcal{D}_{\mathcal{C}_2}$. Hence, condition (6.7) follows. □

Corollary 6.4. *Let $\mathcal{C}$ be a cyclic code generated by the polynomial $g(x)$ with the roots $\alpha^{\pm i}$ for $\pm i \in \mathcal{D}_{\mathcal{C}}$. Then, $\mathcal{C}$ is a reversible cyclic code that* ***cannot*** *be used to construct quantum synchronizable code.*

Example 6.1. *For $n = 26$ and $q = 3$, given that the generator polynomial of $\mathcal{C}_2$ is $g_2(x) = M_1(x) \cdot M_2(x) \cdot M_4(x) \cdot M_7(x)$, the defining set $\mathcal{D}_{\mathcal{C}_2} = C_{1,26} \cup C_{2,26} \cup C_{4,26} \cup C_{7,26}$ of cyclic code $[26, 14, d_2]_3$ is obtained from the cyclotomic cosets $C_{1,26} = \{1, 3, 9\}, C_{2,26} = \{2, 6, 18\}, C_{4,26} = \{4, 10, 12\}$ and $C_{7,26} = \{7, 11, 21\}$. Since $\mathcal{I} = \{1, 2, 4, 7\}$ and $|\mathcal{I}| = 4$, there are $2^4 - 2 = 14$ possible supercodes $\mathcal{C}_1$ obtained from $\mathcal{C}_2$ such that $\mathcal{C}_2 \subset \mathcal{C}_1$. Furthermore, $-\mathcal{I} \notin \mathcal{D}_{\mathcal{C}_2}$ and $-i \notin C_{i,26}$ for all $i \in \mathcal{I}$. We*

have $\mathcal{I} \cap -\mathcal{I} = \emptyset$. *Therefore* $h(x) = f(x) \prod_{i \in \mathcal{I}} M_{-i}(x)$, *where* $f(x) = M_0(x) M_{13}(x)$ *with degree* $26 - 2 \times 12 = 2$. *Hence,* $\mathcal{C}_2^{\perp} = \langle g_2^{\perp}(x) = x^{14} h(x^{-1}) \rangle$ *is a subcode of* $\mathcal{C}_2$. □

Example 6.2. *For* $n = 28$ *and* $q = 3$, *the cyclotomic cosets modulo* 28 *are*

$$\begin{aligned} &C_{0,28} = \{0\}, C_{1,28} = \{1, 3, 9, 27, 25, 19\}, \\ &C_{2,28} = \{2, 6, 18, 26, 22, 10\}, C_{4,28} = \{4, 12, 8, 24, 16, 20\}, \\ &C_{5,28} = \{5, 15, 17, 23, 13, 11\}, C_{7,28} = \{7, 21\}, C_{14,28} = \{14\}. \end{aligned} \tag{6.10}$$

By inspection, for $g_2(x) = \prod_{i \in \mathcal{I}, \mathcal{I} \subset S_n} M_i(x)$, *where* $S_n = \{0, 1, 2, 4, 5, 7, 14\}$, *we have* $\pm i \in C_{i,n}$. *Further, for any subset* $\mathcal{I}$ *of* S_n, *the associated defining set* $\mathcal{D}_{\mathcal{C}_2}$ *is exactly the same as the defining set generated by the inverse* $-\mathcal{I}$, e.g., $C_{1,28} = C_{27,28}$. *Hence,* $g_2(x) \nmid g_2^{\perp}(x)$. □

6.3 The minimum distance of CC-QSCs

In this section, we study the distance property for quantum synchronizable codes under the CSS structure. It is known that the quantum minimum distance of a CSS code is given by

$$\begin{aligned} &d_{min} := \min\{d_1, d_2\}, \text{where} \\ &d_1 := \min\{|\mathbf{c}|, \mathbf{c} \in \mathcal{C}_1 \backslash \mathcal{C}_2^{\perp}\}, \\ &d_2 := \min\{|\mathbf{c}|, \mathbf{c} \in \mathcal{C}_2 \backslash \mathcal{C}_1^{\perp}\}. \end{aligned} \tag{6.11}$$

Since the minimum distance of quantum CSS codes can be determined, we shall review some of the important distance bounds first, then derive distance bounds for quantum synchronizable codes of CSS structure constructed from the proposed method in terms of d_1 and d_2.

6.3.1 Known bounds

Theorem 6.5. *[146, 147](BCH bound) Let $[n, k, d]_q$ be a q-ary cyclic code of length n, dimension k, distance d, and with defining set $\mathcal{D}$. Let*

$$\{b, b+1, b+2, \ldots, b+\delta-2\} \subseteq \mathcal{D}.$$

Then $d \geq d_{BCH} \triangleq \delta$.

If $b = 1$, the cyclic code is called *Narrow-sense BCH code.*

Theorem 6.6. *[145](HT bound) Let $[n, k, d]_q$ be a q-ary cyclic code of length n, dimension k, distance d, and with defining set $\mathcal{D}$. Let*

$$\{b + z_1 m_1 + z_2 m_2, \forall z_1 = 0, 1, \ldots \delta - 2, \forall z_2 = 0, 1, \ldots, v\} \subseteq \mathcal{D}$$

where $gcd(n, m_1) = 1$ and $gcd(n, m_2) = 1$. Then $d \geq d_{HT} \triangleq \delta + v$.

If $v = 0$, the HT bound in theorem 6.6 becomes the BCH bound. Generalization of the HT bound was proposed by Roos [102, 103]. Sometimes the actual distance of a code is greater than δ just by looking at the roots; such an approach to this question was generalized by van Lint and Wilson [101].

6.3.2 Bounding minimum distance of cyclic codes using rational function

The BCH bound provides a lower bound to d if the zeros of the generator polynomial is known. The bound can be derived from rational functions [148] using the representation of Mattson-Solomon polynomial [35] for cyclic codes. We can extend Mattson-Solomon polynomials of a codeword into infinite series, which can be further expressed as a summation of rational functions. In this case, the lower bound of the minimum distance of a cyclic code can be determined by the degree of numerator of the rational function. For any codeword $c(x) = \sum_{i=0}^{n-1} c_i x^i$ of a

$[n, k, d]_q$ q-ary cyclic code, the Mattson-Solomon polynomial of $c(x)$ can be express as $\sum_{j=0}^{n-1} c(\alpha^j)x^j$. We extend the polynomial into the form of infinite series $\sum_{j=0}^{\infty} c(\alpha^j)x^j$ with repeating coefficients for every n values. Therefore, we have

$$\sum_{j=0}^{\infty} c(\alpha^j)x^j = \sum_{i=0}^{n-1}\sum_{j=0}^{\infty} c_i(\alpha^i x)^j \equiv \sum_{i=0}^{n-1} \frac{c_i}{1-\alpha^i x}. \tag{6.12}$$

The last term is a summation of rational functions with the degree of the denominator at most n. The infinite series $\sum_{j=0}^{\infty} c(\alpha^{j+b})x^j$ of a codeword $c(x)$ with $\delta - 1$ consecutive roots $\{b, b+1, b+2, \ldots, b+\delta-2\} \subseteq \mathcal{D}$ can be expressed as

$$\sum_{j=0}^{\infty} c(\alpha^{j+b})x^j = \sum_{i=0}^{n-1} \frac{c_i\alpha^{ib}}{1-\alpha^i x} \equiv 0 \pmod{x^{\delta-1}}. \tag{6.13}$$

Let $\mathcal{A}$ be the set of indexes of non-zero coefficients of $c(x) \in [n, k, d]_q$, and $|\mathcal{A}| = d$. Equation (6.13) can be written as

$$\frac{h(x)}{f(x)} \equiv 0 (\mathrm{mod} x^{\delta-1}), \tag{6.14}$$

where

$$h(x) = \sum_{i\in\mathcal{A}} \left(c_i\alpha^{ib} \prod_{l\in\mathcal{A}, l\neq j} (1-\alpha^l x) \right), \delta - 1 \leq deg(h(x)) \leq d-1 \tag{6.15}$$

and

$$f(x) = \prod_{i\in\mathcal{A}} \left(1-\alpha^i x\right), deg(f(x)) = d. \tag{6.16}$$

Hence, $d \geq d_{BCH} = \delta$ implies $h(x) \equiv 0 \left(\mathrm{mod} x^{\delta-1}\right)$.

The period $\mathcal{P}$ of the rational function $\frac{h(x)}{f(x)}$, $\mathcal{P}\left(\frac{h(x)}{f(x)}\right)$, is a positive integer p such that

$$h(x)(-x^p+1) = f(x)(\sum_{i=0}^{p-1} s_i x^i) \tag{6.17}$$

holds. In other words, $\frac{h(x)}{f(x)}$ is a periodic function with repeated non-zero positions. To associate this property with a q-ary cyclic code, let

$$\sum_{i=0}^{n-1} c_i \frac{\alpha^{ib} h(\alpha^i x)}{f(\alpha^i x)} = \sum_{j=0}^{\infty} s_j c(\alpha^{j+b}) x^j \equiv 0 (\text{mod } \ x^{\theta-1}), \tag{6.18}$$

where $c(x) \in \mathcal{C}$ of weight $wt(\mathbf{c}) = d = |\mathcal{A}|$. Then the sequence

$$s_0 c(\alpha^b), s_1 c(\alpha^{b+1}), s_2 c(\alpha^{b+2}), \ldots, s_{\theta-2} c(\alpha^{b-1+\theta-1})$$

is a zero-sequence of maximal length $\theta - 1$. Hence, either s_j or $c(\alpha^{b+j})$ is zero for $0 \leq j \leq \theta - 1$.

Similar to the case of the BCH bound, the left-hand side of (6.18) can be rearranged into

$$\frac{\sum_{i \in \mathcal{A}} \left(c_i \alpha^{ib} h(\alpha^i x) \prod_{l \in \mathcal{A}, l \neq i} f(\alpha^i x) \right)}{\prod_{i \in \mathcal{A}} f(\alpha^i x)}, \tag{6.19}$$

then the minimum distance d of a q-ary cyclic code $[n, k, d]_q$ is lower bound as

$$d \geq d^* \triangleq \left\lceil \frac{\theta - v - 1}{u} + 1 \right\rceil, \tag{6.20}$$

where u and v are the degree of the denominator and numerator, respectively.

6.3.3 Minimum distance of proposed QSC codes

In the context of quantum synchronizable codes, we require a pair of cyclic codes of same length such that their minimum distance is maximized while the misalignment tolerance approaches to the known upper bound derived in [141].

Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be two q-ary cyclic codes of parameters $[n, k_1, d_1]_q$ and $[n, k_2, d_2]_q$, respectively. Let $\mathcal{D}_{\mathcal{C}_1}$ and $\mathcal{D}_{\mathcal{C}_2}$ be the associated defining set of the two codes. If $\mathcal{C}_2 \subset \mathcal{C}_1$, $g_1(x) \mid g_2(x)$ and $\mathcal{D}_{\mathcal{C}_1} \subset \mathcal{D}_{\mathcal{C}_2}$. The BCH bound of

$\mathcal{C}_2$ using the notion of rational function is given by

$$\sum_{j=0}^{\infty} g_2\left(\alpha^{j+b_2}\right)x^j \equiv 0\left(\mathrm{mod}\, x^{\delta-1}\right), \tag{6.21}$$

where $\{b_2, b_2+1, \ldots, b_2+\delta-2\} \subset \mathcal{D}_{\mathcal{C}_2}$ for some positive integer $b_2 < n$. Since $g_1(x)$ is a factor of $g_2(x)$, we can write $g_2(x) = g_1(x)f(x)$ for some polynomial $f(x)$. Let $c_2(x) \in \mathcal{C}_2$ be any codeword, then

$$\begin{aligned}
\sum_{j=0}^{\infty} c_2\left(\alpha^{j+b_2}\right)x^j &\equiv \sum_{j=0}^{\infty} g_1\left(\alpha^{j+b_2}\right)\bar{f}\left(\alpha^{j+b_2}\right)x^j \\
&\equiv \sum_{j=0}^{\infty} x^j \sum_{i=0}^{n-1} g_{1_i}\left(\alpha^{j+b_2}\right)^i \sum_{k=0}^{n-1} \bar{f}_k\left(\alpha^{j+b_2}\right)^k \\
&\equiv \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} g_{1_i}\bar{f}_k\alpha^{b_2(i+k)} \sum_{j=0}^{\infty} \alpha^{j(i+k)}x^j \\
&\equiv \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} \frac{g_{1_i}\bar{f}_k\alpha^{b_2(i+k)}}{1-\alpha^{(i+k)}x} \\
&\equiv 0\left(\mathrm{mod}\ x^{\delta-1}\right),
\end{aligned} \tag{6.22}$$

where $\bar{f}(x) = f(x)m(x)$ for some message polynomial $m(x)$. Denoted by $\mathcal{W}_1$ and $\mathcal{W}_2$ the set of non-zero positions of $g_1(x)$ and $\bar{f}(x)$, respectively, and $|\mathcal{W}_1| = d_1$, $|\mathcal{W}_2| = d_f$. We can write (6.22) as

$$\begin{aligned}
&\frac{\sum_{i\in\mathcal{W}_1}\left(\sum_{k\in\mathcal{W}_2}\left(g_{1_i}\bar{f}_k\alpha^{b_2(i+k)}\prod_{m\in\mathcal{W}_2,m\neq k}\left(1-\alpha^{(i+m)}x\right)\right)\prod_{z\in\mathcal{W}_1,z\neq i}\prod_{s\in\mathcal{W}_2}\left(1-\alpha^{(z+s)}x\right)\right)}{\prod_{i\in\mathcal{W}_1}\prod_{k\in\mathcal{W}_2}(1-\alpha^{(i+k)}x)} \\
&\equiv 0\left(\mathrm{mod}\ x^{\delta-1}\right),
\end{aligned} \tag{6.23}$$

where the degree of the denominator is $|\mathcal{W}_1|\cdot|\mathcal{W}_2| = d_1d_f$. The degree of the numerator is at most $|\mathcal{W}_1|\cdot|\mathcal{W}_2| - 1 = d_1d_f - 1$, and $d_1d_f - 1 \geq \delta - 1$. Hence

$$d_1 \geq \left\lceil \frac{\delta}{d_f} \right\rceil \quad \text{or} \quad d_f \geq \left\lceil \frac{\delta}{d_1} \right\rceil. \tag{6.24}$$

Since $k_2 < k_1$, $d_2 \geq d_1 \geq \lceil \frac{\delta}{d_f} \rceil$.

6.4 A class of QSCs from quadratic residue codes

In the rest of the chapter, we construct a class of quantum synchronizable codes by exploiting special classical cyclic codes over the finite field $\mathbb{F}_2$ of order 2, called quadratic residue codes. Quadratic residue codes tend to have large minimum distances [35]. Thus, it is reasonable to expect that quantum error-correcting codes that exploit quadratic residue codes possess good error correction performance. We show that quantum synchronizable codes from quadratic residue codes also have good block synchronization capabilities. Since we only consider binary codes from now on, the subscript 2 in $[n, k, d]_2$ is omitted.

Recall that Theorem 6.1 requires a pair of cyclic codes $\mathcal{C}_1$, $\mathcal{C}_2$ of parameters $[n, k_1]$ and $[n, k_2]$ with $k_1 > k_2$ that satisfy the condition $\mathcal{C}_2^{\perp} \subseteq \mathcal{C}_2 \subset \mathcal{C}_1$. We first construct a cyclic code $\mathcal{C}_2$ in such a way that its dual code $\mathcal{C}_2^{\perp}$ is a subspace of $\mathcal{C}_2$. We then obtain a cyclic supercode $\mathcal{C}_1$ by inserting codewords into $\mathcal{C}_2$. While we only apply this idea to a small, specific class of cyclic codes, this general principle of producing supercodes may be applicable to other cyclic codes to ensure good synchronization recoverability if code lengths are primes.

6.4.1 Dual-containing cyclic codes: $\mathcal{C}_2^{\perp} \subset \mathcal{C}_2$

Let p be a prime of the form $p \equiv \pm 1 \pmod 8$. Define $\mathcal{Q}^{\mathcal{R}} = \{x^2 \pmod p \mid 1 \leq x \leq \frac{p-1}{2}\}$ and $\mathcal{Q}^{\mathcal{NR}} = \{1, 2, \ldots, p-1\} \backslash \mathcal{Q}^{\mathcal{R}}$ to be the sets of $\frac{p-1}{2}$ nonzero quadratic residues and $\frac{p-1}{2}$ quadratic non-residues respectively. Take a primitive p-th root α of unity in $\mathbb{F}_{2^t}$, where t is the smallest positive integer such that p divides $2^t - 1$. Let

$$g_{\mathcal{R}}(x) = \prod_{i \in \mathcal{Q}^{\mathcal{R}}} \left(x - \alpha^i\right) \text{ and } g_{\mathcal{NR}}(x) = \prod_{i \in \mathcal{Q}^{\mathcal{NR}}} \left(x - \alpha^i\right).$$

Note that $g_{\mathcal{R}}(x)$ and $g_{\mathcal{NR}}(x)$ are both in $\mathbb{F}_2[x]$. The pair $\mathcal{C}_{\mathcal{R}} = \langle g_{\mathcal{R}}(x) \rangle$ and $\mathcal{C}_{\mathcal{NR}} = \langle g_{\mathcal{NR}}(x) \rangle$ are $[p, \frac{p+1}{2}]$ cyclic codes known as *quadratic residue codes* over

$\mathbb{F}_2$. By the same token, the two polynomials

$$\bar{g}_{\mathcal{R}}(x) = (x-1)\prod_{i\in\mathcal{Q}^{\mathcal{R}}}\left(x-\alpha^i\right)$$

and

$$\bar{g}_{\mathcal{NR}}(x) = (x-1)\prod_{i\in\mathcal{Q}^{\mathcal{NR}}}\left(x-\alpha^i\right)$$

generate $[p, \frac{p-1}{2}]$ cyclic codes $\bar{\mathcal{C}}_{\mathcal{R}} = \langle \bar{g}_{\mathcal{R}}(x)\rangle$ and $\bar{\mathcal{C}}_{\mathcal{NR}} = \langle \bar{g}_{\mathcal{NR}}(x)\rangle$. The latter pair may also be referred to as quadratic residue codes in the literature. It is known that quadratic residue codes tend to have large minimum distances. The following is a well-known general lower bound, known as the square root bound.

Theorem 6.7. *(Square Root Bound) The minimum distance d of a quadratic residue code of length p is at least $\sqrt{p}$. If $p \equiv -1 \pmod 4$, then $d^2 - d + 1 \geq p$.*

For small quadratic residue codes, tables of exact parameters can be found in [144].

To take advantage of quadratic residue codes for constructing quantum synchronizable codes, we use the fact that the larger one of each pair is dual-containing if the length is -1 modulo 8. A detailed account on the properties of quadratic residue codes and their duals can be found in [35, Ch. 16]. For convenience, we give a short proof of the simple fact.

Lemma 6.8. *The quadratic residue codes $\mathcal{C}_{\mathcal{R}}$, $\mathcal{C}_{\mathcal{NR}}$, $\bar{\mathcal{C}}_{\mathcal{R}}$ and $\bar{\mathcal{C}}_{\mathcal{NR}}$ of length $p \equiv -1 \pmod 8$ have the following properties:*

$$\begin{aligned} &1) \qquad \mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}}, \quad \mathcal{C}_{\mathcal{NR}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{NR}}. \\ &2) \qquad \mathcal{C}_{\mathcal{R}}^{\perp} \subset \mathcal{C}_{\mathcal{R}}, \quad \mathcal{C}_{\mathcal{NR}}^{\perp} \subset \mathcal{C}_{\mathcal{NR}}. \end{aligned}$$

Proof. Since $\mathcal{Q}^{\mathcal{R}}$ and $\mathcal{Q}^{\mathcal{NR}}$ are disjoint and do not contain 0, we have $x^p - 1 = (x-1)\, g_{\mathcal{R}}(x) g_{\mathcal{NR}}(x)$. The zeros of $g_{\mathcal{R}}(x)$ and $g_{\mathcal{NR}}(x)$ are $\{\alpha^i \mid i \in \mathcal{Q}^{\mathcal{R}}\}$ and $\{\alpha^i \mid i \in \mathcal{Q}^{\mathcal{NR}}\}$, respectively. Hence by Equation (6.4), the zeros of $\mathcal{C}_{\mathcal{R}}^{\perp}$ are 1 and α^{-i} for $i \in \mathcal{Q}^{\mathcal{NR}}$, and the zeros of $\mathcal{C}_{\mathcal{NR}}^{\perp}$ are 1 and α^{-i} for $i \in \mathcal{Q}^{\mathcal{R}}$. Note that $\alpha^i \in \mathcal{Q}^{\mathcal{R}}$ if and only if i is even and that $\alpha^i \in \mathcal{Q}^{\mathcal{NR}}$ if and only if i is odd. When

$p \equiv -1 \pmod 8$, we have $i \in \mathcal{Q}^{\mathcal{R}}$ if and only if $-i \in \mathcal{Q}^{\mathcal{NR}}$. Hence, $\mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}}$ and $\mathcal{C}_{\mathcal{NR}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{NR}}$. Since $\mathcal{C}_{\mathcal{R}} = \langle g_{\mathcal{R}}(x) \rangle$ and $\mathcal{C}_{\mathcal{R}}^{\perp} = \bar{\mathcal{C}}_{\mathcal{R}} = \langle \bar{g}_{\mathcal{R}}(x) \rangle$, it is trivial that $\mathcal{C}_{\mathcal{R}}$ is dual-containing. By the same token, $\mathcal{C}_{\mathcal{NR}}$ is a dual-containing code. □

Example 6.3. *Consider the set of nonzero quadratic residues modulo* 31

$$\begin{aligned}\mathcal{Q}^{\mathcal{R}} &= \{1, 2^2, 3^2, 4^2, \ldots, 15^2\} \\ &= \{1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8\}.\end{aligned}$$

The generator polynomial of the quadratic residue code $\mathcal{C}_{\mathcal{R}}$ *of length* $p = 31$ *is then*

$$g_{\mathcal{R}}(x) = x^{15} + x^{12} + x^7 + x^6 + x^2 + x + 1.$$

Multiplying by $x + 1$ *gives the generator polynomial of* $\bar{\mathcal{C}}_{\mathcal{R}}$

$$\bar{g}_{\mathcal{R}}(x) = x^{16} + x^{15} + x^{13} + x^{12} + x^8 + x^6 + x^3 + x + 1.$$

Plugging $g_{\mathcal{R}}(x)$ *into Equation (6.4) also gives* $\bar{g}_{\mathcal{R}}(x)$*, which means that this is the generator polynomial of the dual code* $\mathcal{C}_{\mathcal{R}}^{\perp}$ *as well.* ■

6.4.2 Cyclic supercodes of $\mathcal{C}_2$

Lemma 6.8 provides a $[p, \frac{p+1}{2}, d]$ dual-containing cyclic code $\mathcal{C}_2$ for prime $p \equiv -1 \pmod 8$ with $d \geq \sqrt{p}$. To obtain another cyclic code $\mathcal{C}_1$ such that $\mathcal{C}_2 \subset \mathcal{C}_1$, we increase the number of codewords by deleting a factor from the generator polynomial of $\mathcal{C}_2$ we already have. Note that, by definition, a cyclic code is a subcode of another if its generator polynomial is divisible by the other. Thus, if the generator polynomial of $\mathcal{C}_2$ has more than one factor, deletion always gives a supercode. As the following proposition shows, a particularly interesting case is when p is a Mersenne prime.

Proposition 6.9. *Let* $\mathcal{C} = \mathcal{C}_{\mathcal{R}}$ *be the quadratic residue code of length* p *generated by* $g_2(x) = \prod_{i \in \mathcal{Q}^{\mathcal{R}}} (x - \alpha^i)$*. If* $p = 2^l - 1$*, then* $g_2(x)$ *can be factored into* $\frac{2^{l-1}-1}{l}$

irreducible polynomials of degree l, that is,

$$g_2(x) = \prod_j M_j(x), \tag{6.25}$$

where $M_s(x)$ is the minimal polynomial of α^s over $\mathbb{F}_2$ and $\deg(M_j(x)) = l$ for all j.

The above proposition can be proved through the concept of cyclotomy [35] described in Section 6.2.1. Note that for any s, the cardinality $|C_{s,n}|$ is a divisor of $|C_{1,n}|$. When n is a Mersenne prime $2^l - 1$, we have $|C_{1,n}| = l$. Because l is also a prime, when n is a prime of the form $n = p = 2^l - 1$, each $C_{s,n}$ is of size l as well, proving Proposition 6.9.

Because of the one-to-one correspondence between cyclic codes and monic divisors of $x^n - 1$, deleting one or more factors $M_j(x)$ gives another generator polynomial that results in a cyclic code of higher dimension containing the dual-containing cyclic code $\mathcal{C}_\mathcal{R}$. Trivially, if we delete z factors, the dimension of the supercode is higher than that of $\mathcal{C}_\mathcal{R}$ by zl. Applying Theorem 6.1 to this supercode as $\mathcal{C}_1$ together with the dual-containing quadratic residue code gives a quantum synchronizable code.

It is also notable that any supercode $\mathcal{C}_1$ obtained by deleting a minimal polynomial of the quadratic residue code is also dual-containing. Thus, we have a chain of cyclic codes, each of which is dual-containing itself and contains all smaller ones. Therefore, we can construct a quantum synchronizable code from any pair of codes in the chain.

6.4.3 Maximum misalignment tolerance

In the context of quantum synchronizable codes, we would like to maximize $\mathrm{ord}(f(x))$, where $f(x)$ is the quotient in Theorem 6.1, in order to tolerate as large magnitude of misalignment as possible. It is known that the maximum tolerable magnitude of a quantum synchronizable code is upper bounded by its length

[141]. We prove that the quantum synchronizable codes from quadratic residue codes given in the previous subsection attain this bound.

Lemma 6.10. *Let $\mathcal{C}_1 = \langle g_1(x) \rangle$ and $\mathcal{C}_2 = \langle g_2(x) \rangle$ be cyclic codes of length p such that $\mathcal{C}_2 \subset \mathcal{C}_1$ and $\mathcal{C}_1 \neq \mathcal{C}_2$. Define $f(x)$ to be the polynomial such that $g_2(x) = f(x)g_1(x)$. If p is a prime, then* $\operatorname{ord}(f(x)) = p$.

Proof. Because the generator polynomial of a cyclic code of length p divides $x^p - 1$, its factor also divides $x^p - 1$. Hence, the factor $f(x)$ of $g_2(x)$ divides $x^p - 1$ as well, which implies that $x^p \equiv 1 \pmod{f(x)}$. Hence, because $\operatorname{ord}(f(x)) = |\{x^a \pmod{f(x)} \mid a \in \mathbb{N}\}|$, the order of $f(x)$ is a divisor of p. Since p is a prime and $f(x) \neq 1$ by assumption, we have $\operatorname{ord}(f(x)) = p$ as desired. □

We now give our main theorem.

Theorem 6.11. *Let $p = 2^l - 1$ be a Mersenne prime. For nonnegative integers c_l, c_r and z such that $c_l + c_r < p$ and $z \leq \frac{2^{l-1}-l-1}{l}$, there exists a quantum synchronizable code of parameters (c_l, c_r)-$[[p + c_l + c_r, 2zl + 1]]$.*

Proof. Take a quadratic residue code of length $p = 2^l - 1$ generated by the nonzero quadratic residues. By Proposition 6.9, its generator polynomial has $\frac{2^{l-1}-1}{l}$ minimal polynomials of degree l as its factors. Thus we have a chain of $\frac{2^{l-1}-1}{l}$ cyclic codes in which a code contains all other smaller ones. Note that a supercode of a dual-containing code is also dual-containing. Thus, by applying Theorem 6.1 and Lemma 6.10 the cyclic code generated by the polynomial that is obtained by deleting z factors and another one obtained by deleting $z + y$ factors for some positive integer y, we obtain a quantum synchronizable code of desired parameters. □

Example 6.4. *As in Example 6.3, let $p = 2^5 - 1$ and take the set $\mathcal{Q}^{\mathcal{R}} = \{x^2 \pmod{p} \mid 1 \leq x \leq 2^{l-1} - 1\}$ of nonzero quadratic residues modulo 31. Then $\mathcal{Q}^{\mathcal{R}}$ is the union of $\frac{2^4-1}{5} = 3$ cyclotomic cosets of field $\mathbb{F}_{2^5}$ as follows.*

$$\mathcal{Q}^{\mathcal{R}} = C_{1,31} \cup C_{5,31} \cup C_{7,31},$$

where

$$C_{1,31} = \{1, 2, 4, 8, 16\},$$
$$C_{5,31} = \{5, 10, 20, 9, 18\},$$
$$C_{7,31} = \{7, 14, 28, 25, 19\}.$$

Let $\mathcal{C}_2 = \langle g_{\mathcal{R}}(x) \rangle$. *Since* $g_{\mathcal{R}}(x)$ *is the product of the minimal polynomials* $M_s(x)$ *of* α^s *over* $\mathbb{F}_2$ *for* $s \in \mathcal{Q}^{\mathcal{R}}$, *we have*

$$g_{\mathcal{R}}(x) = M_1(x)M_5(x)M_7(x),$$

with

$$M_1(x) = x^5 + x^2 + 1,$$
$$M_5(x) = x^5 + x^4 + x^2 + x + 1,$$
$$M_7(x) = x^5 + x^3 + x^2 + x + 1.$$

Note that each one of $M_1(x)$, $M_5(x)$ *and* $M_7(x)$ *divides* $x^{31} - 1$. *Let* $\mathcal{C}_1 = \langle g_1(x) = \frac{g_{\mathcal{R}}(x)}{f(x)} \rangle$. *If we delete* $z = 1$ *minimal polynomial,* $f(x) = M_j(x)$ *for* $j \in \{1, 5, 7\}$, *the dimension of* $\mathcal{C}_1$ *is* $\dim(\mathcal{C}_1) = p - \deg(g_{\mathcal{R}}(x)) + zl = 31 - 15 + 5 = 21$. *If we delete* $z = 2$ *factors, then* $f(x) = M_{j_1}(x)M_{j_2}(x)$ *for* $j_1, j_2 \in \{1, 5, 7\}$ *and* $j_1 \neq j_2$, *so the dimension of* $\mathcal{C}_1$ *in this case is* $\dim(\mathcal{C}_1) = 31 - 15 + 10 = 26$. *In both cases, the* $\mathrm{ord}\,(f(x)) = 2^l - 1 = p = 31$. *Since* $\deg(g_{\mathcal{R}}(x)) = 15$ *and* $\dim(\mathcal{C}_2) = 16$, *for arbitrary pair of non-negative integer* c_l *and* c_r *such that* $c_l + c_r < 31$, *we have a* (c_l, c_r)-$[[31 + c_l + c_r, 1]]$ *quantum synchronizable code.*

Further, let $z = 1$ *and* $\mathcal{C}_2 = \langle g_{\mathcal{R}}(x) \rangle \subset \mathcal{C}_3$ *with* $\mathcal{C}_3 = \langle M_{j_1}(x)M_{j_2}(x) \rangle$ *for* $j_1, j_2 \in \{1, 5, 7\}$ *and* $j_1 \neq j_2$. *If* $y = 1$, *by removing* $z + y = 2$ *minimal polynomials* $M_i(x)$ *from* $g_{\mathcal{R}}(x)$, *we obtain another cyclic code* $\mathcal{C}_4$ *such that* $\mathcal{C}_2 \subset \mathcal{C}_3 \subset \mathcal{C}_4$. *Since* $\dim(\mathcal{C}_3) = 21 > \lceil \frac{n}{2} \rceil$, *by Theorem 6.1 for* $c_l + c_r < 31$, $\mathcal{C}_3$ *and* $\mathcal{C}_4$ *form a* (c_l, c_r)-$[[31 + c_l + c_r, 2zl + 1 = 11]]$ *quantum synchronizable code.* ■

6.5 Chapter summary

In this chapter, we studied the concept of QSCs and proposed a general method for constructing QSCs using chain-containing classical cyclic codes. The proposed construction is particularly flexible when the length is not a Mersenne prime because since any pair of dual-containing cyclic codes from a chain-containing cyclic codes is eligible for the construction of QSC. This adds variety in dimension and minimum distance to the resulting QSC. Furthermore, we showed that the proposed QSCs from quadratic residue codes of length equal Mersenne prime possess the highest possible tolerance against synchronization errors, while the dimension of this codes is one.

Chapter 7

Channel Mismatch For Quantum LDPC Codes Over Depolarizing Channel

Classical LDPC codes were originally proposed by Gallager in the 1960s [43]. However, LDPC codes remained largely unnoticed until their re-discovery in the mid-90s [123] [131]. Since then hundreds of papers have been published outlining the near optimal performance of LDPC codes over a wide range of noisy wireless communication channels. In almost all of such previous works it was assumed that the characteristics of the noisy wireless channel were known. However, the reality is that in many cases an exact determination of the wireless channel is unavailable. Indeed, several works have in fact investigated the case where a channel mismatch (or channel misidentification) occurs, which in turn impacts on the performance of the LDPC decoder (*e.g.* [125]).

From the perspective of the work reported here, the most interesting aspect of such channel mismatch studies is the asymmetry in the LDPC code performance as a function of the channel crossover probability for the binary symmetric channel (BSC). In fact, the main focus of the work described here is an investigation of whether such asymmetric LDPC code performance carries over from the classical

BSC to quantum LDPC codes operating over the quantum depolarizing channel. Interestingly, an asymmetry behaviour in performance is observed as a function of the estimated channel flip probability, showing that the performance of a quantum LDPC code would experience a reduced degradation when the channel is overestimated (a higher estimation) instead of underestimated (a lower estimation), provided the overestimated channel knowledge still within the threshold limit of the code.

In this chapter, we first investigate the behaviour of the classical sum-product decoder under channel mismatch conditions. Then a brief introduction on belief propagation for QECC with the help of the Tanner graph is provided. Then we explore the behaviour of a quantum decoder when simulating over a quantum depolarizing channel and show how the decoding strategy we outline here leads to a significant improvement in performance relative to decoders that simply utilize the estimated channel parameter.

7.1 Behaviour of classical sum-product decoder

It is well known in classical coding that low-density parity-check codes are good rate achievable codes [119] [131], given an optimal decoder. The best algorithm known to decode them is the sum-product algorithm, also known as iterative probabilistic decoding or belief propagation (BP). The performance of sparse-graph codes can be improved if knowledge about the channel is known at the decoder side. However, in practical situations the decoder is unlikely to know the channel's characteristics exactly; thus, the robustness of the decoder to channel mismatches is also an important issue when designing practical codes.

In [125], MacKay *et.al* investigated the sensitivity of Gallager's codes [119] to the assumed noise level (classical bit-flip probability) when decoded by belief propagation. A useful result therein is that the belief propagation decoder for LDPC codes appears to be robust to channel mismatches because the block error probability is

not a very sensitive function of the assumed noise level. In addition, an underestimation of channel characteristics deteriorates the performance more compared to an overestimation of channel characteristics. This behaviour is shown in Fig. 7.1.

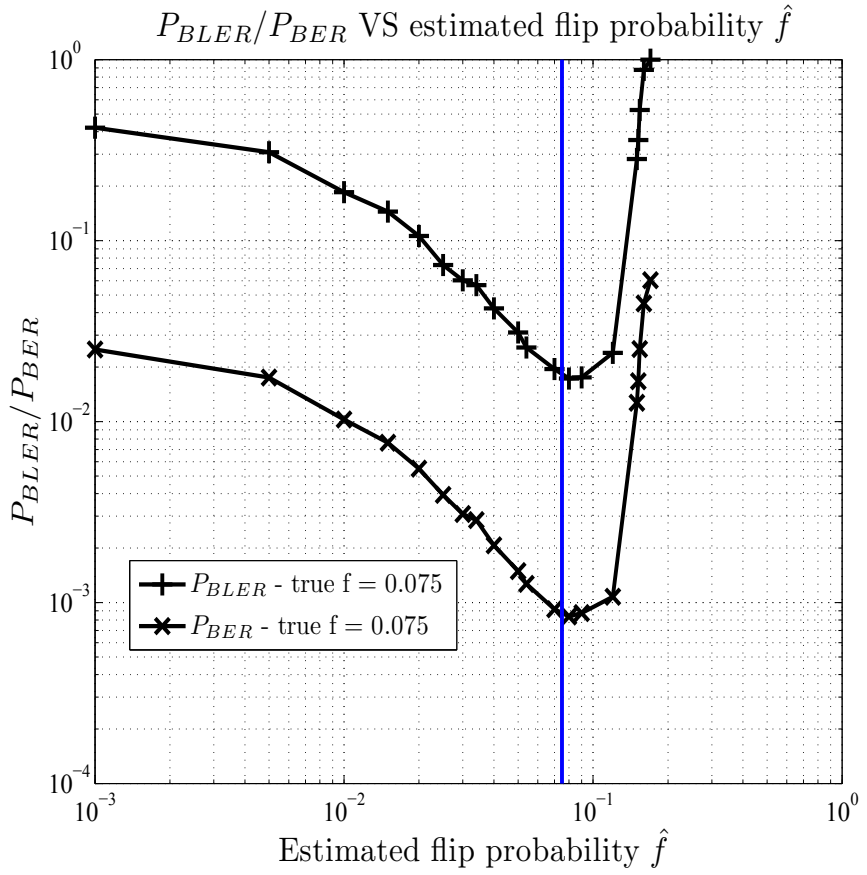

FIGURE 7.1: Probability of block error as a function of estimated flip probability when the true flip probability is fixed.

Our results shown in Fig. 7.1 are for a rate half code of block length $N = 2040$ over a binary symmetric channel. The code is a $(3, 6)$ regular LDPC code which is constructed with the length of the cycle maximized. The plot shows the probability of block and bit error (P_{BLER}/P_{BER}) as a function of assumed flip probability $\hat{f}$ when the true flip probability f is fixed throughout the simulation.

By inspection, the plotted result shows a similar behaviour to that found by MacKay in [125]. The vertical straight line indicates the true value of the noise level, and the minimum point of the plot is approximately at the intersection between the lines. This infers that an optimal performance of a practical sum-product decoder can be achieved when the input of the decoder is the true noise level (true

flip probability). The slope towards the left of the graph is steeper than the slope towards the right, indicating that underestimation (an estimation smaller than the true flip probability) of the noise level degrades the performance more than overestimation (an estimation larger than the true flip probability) does. However, when the estimated noise level is far too large, there is a significant increase in the error probability. Such higher estimation of noise level can be thought of as the classical Shannon's limit, which theoretically represents the threshold (f_{thr}) for the noise level that guarantees reliable transmission at a certain rate. For the code shown in Fig. 7.1, since it is a rate half code, the Shannon's limit is 0.11 computed from the capacity function $C = 1 - H_2(f)$, where $H_2(f) = -f\log_2(f) - (1-f)\log_2(1-f)$ is the binary entropy function. As can be seen from the figure, a sudden increase of error probability occurs when $\hat{f} > 0.11$. However, as $f < \hat{f} < 0.11$, the slop of P_{BLER} curve is less steep compared to that of $\hat{f} < f$.

7.2 Channel mismatch over quantum depolarizing channel

Motivated by the decoding asymmetry discussed above for classical LDPC codes, we now wish to explore whether a similar asymmetry in decoding performance is achieved for quantum LDPC codes. As stated below several well-known classes of quantum codes such as quantum stabilizer codes can be designed from existing classical codes. Upon construction of such codes we will then investigate the decoding performance under asymmetrical estimates of the quantum channel parameters. The quantum channel we investigate is the widely adopted depolarization channel.

7.2.1 Quantum channel models

Given some initial system state $|\Psi_s\rangle$, a decoherence model can be built by studying the time evolution of the system state's interaction with some external environment

with initial state $|\Psi_e\rangle$. Without loss of generality we can assume $|\Psi_s\rangle$ and $|\Psi_e\rangle$ are initially not entangled with each other.

In terms of the density operators $\rho_s = |\Psi_s\rangle\langle\Psi_s|$ and $\rho_e = |\Psi_e\rangle\langle\Psi_e|$, the initial state of the combined total system can be written as $\rho_s \otimes \rho_e$. The closed evolution of $\rho_s \otimes \rho_e$ can be described by a unitary U via $U(\rho_s \otimes \rho_e)U^\dagger$. To obtain the output system state, ρ_s^{out}, after some closed evolution U, we use $\rho_s^{out} \equiv \varepsilon(\rho_s) = \mathrm{Tr}_e\left[U(\rho_s \otimes \rho_e)U^\dagger\right]$ where Tr_e is the partial trace over the environment's qubits. The channel $\rho_s^{out} \equiv \varepsilon(\rho_s)$ is a completely positive, trace preserving, map which provides the required evolution of ρ_s. It is possible to describe such maps directly using an operator-sum representation,

$$\varepsilon(\rho_s) = \sum_{a=1}^{N_o} K_a \rho_s K_a^\dagger, \text{ where } \sum_{a=1}^{N_o} K_a^\dagger K_a = I, \tag{7.1}$$

and where $K_{a=1\ldots N_o}$ represent the so-called Kraus operators, with N_o being the number of Kraus operators [132].

There are of course decoherence channels modelled on specific qubit-environment interactions (e.g. see [11]). In this work we will consider only the depolarization channel. Let us introduce the depolarization parameter, f', of a qubit where $0 \leq f' \leq 1$, with $f' = 1$ meaning complete depolarization and $f' = 0$ meaning no depolarization. If we denote the set of Pauli matrices using σ_i (here $i = 0, 1, 2, 3$), that is, $\sigma_0 = I, \sigma_1 = X, \sigma_2 = Z, \sigma_3 = Y$, the depolarization channel for a single qubit can be defined as $\varepsilon(\rho_s) = (1 - f')\rho_s + f'\frac{\sigma_o}{2}$. Using the relation $\sigma_o = \frac{1}{2}\left(\rho_s + \sum_{j=1}^{3} \sigma_j \rho_s \sigma_j\right)$, we see that the Kraus operators for the depolarization channel can be written $K_1 = \sqrt{1 - \frac{3f'}{4}}\sigma_o$, $K_2 = \sqrt{\frac{f'}{4}}\sigma_x$, $K_3 = \sqrt{\frac{f'}{4}}\sigma_y$, and $K_4 = \sqrt{\frac{f'}{4}}\sigma_z$. Note that it is also possible to parameterize the depolarization channel as

$$\varepsilon(\rho_s) = (1 - f)\rho_s + \frac{f}{3}\sum_{j=1}^{3} \sigma_j \rho_s \sigma_j, \tag{7.2}$$

where $f = \frac{3}{4}f'$. This latter form is more convenient for decoding purposes, and below we term f as the *true flip probability*.

7.2.2 Quantum channel estimation

In what follows we will assume the true value of f is unknown *a priori*, and must first be measured via some channel identification procedure. This estimate of f, which we will refer to as $\hat{f}$, will be used in a decoder in order to measure its performance relative to a decoder in which the true f is utilized.

In general, quantum channel identification proceeds by inputting a known quantum state σ (the probe) into a quantum channel Γ_p that is dependent on some parameter p (in our case $p = f$). By taking some quantum measurements on the output quantum state $\Gamma_p(\sigma)$ which leads to some result R, we then hope to estimate p. The input quantum state may be unentangled, entangled with an ancilla qubit (or qudit), or entangled with another probe. Multiple probes could be used, or the same probe can be recycled (*i.e.* sent through the channel again).

As can be imagined many experimental schemes could be developed along these lines, and the performance of each scheme (*i.e.* how well it estimates the true value of the parameter p) could be analyzed. However, in this study we will take a different tactic. Here we will simply assume an experimental set-up is realized that obtains the information-theoretical *optimal* performance.

Optimal channel estimation via the use of the quantum Fisher information has been well studied in recent years, particularly in regard to the determination of the parameter f of the depolarizing channel (*e.g.* [133], [134], [135], [136], [137]). Defining $\rho_f = \Gamma_f(\sigma)$, the quantum Fisher information about f can be written as

$$J(f) = J(\rho_f) = \mathrm{tr}\left[\rho_f\right] L_f^2,$$

where L_f is the symmetric logarithmic derivative defined implicitly by

$$2\partial_f \rho_f = L_f \rho_f + \rho_f L_f,$$

and where ∂_f signifies partial differential w.r.t. f. With the quantum Fisher information in hand, the quantum Cramer-Rao bound can then be written as

$$\text{mse}\left[\hat{f}\right] \geq (N_m J(f))^{-1}$$

where $\text{mse}\left[\hat{f}\right]$ is the mean square error of the unbiased estimator $\hat{f}$, and N_m is the number of independent quantum measurements.

7.2.3 Quantum decoding algorithm

The appropriate decoding algorithm to decode quantum LDPC codes is based on the classical sum-product algorithm since the most common quantum channel model, shown in (7.2), is analogous to the classical 4-ary symmetric channel. The received values at the decoder side can be mapped to measurement outcomes $s \in \{+1, -1\}^M$ (syndrome) of the received qubit sequence, and this syndrome is then used in error estimation and recovery. Assuming an initial quantum state representing a codeword, the initial probabilities p_i for the i-th qubit of the state undergoing an X, Y or Z error are

$$p_i = \begin{cases} \frac{f}{3} & for \quad X,\ Y,\ and\ Z \\ 1-f & for \quad\quad I \end{cases}, \tag{7.3}$$

where f is the flip probability known at the decoder.

The standard BP algorithm operates by sending messages along the edges of the Tanner graph. We shall introduce Tanner graph for QECCs and belief propagation decoding algorithm for QECCs now.

7.2.3.1 Tanner graph of QECCs

A QECC can be represented by a decorated Tanner graph. This is a bipartite graph $S = (V, E)$ with vertices $V = Q \cup C$ where the subset of vertices Q represent the N qubits, and the other subset C represent the $m = N - K$ stabilizer generators,

where K is the encoded number of qubits. The graph has an edge $(q, c) \in E$ iff check c acts non-trivially on qubit q. The Tanner graph for the 5-qubit code in (2.40) is shown in Fig. 7.2. When two checks c and $c^{'}$ both act non-trivially on at least two qubits in common, say q and $q^{'}$, the stabilizer group S will contain a cycle 4-loop $(c, q, c^{'}, q^{'})$.

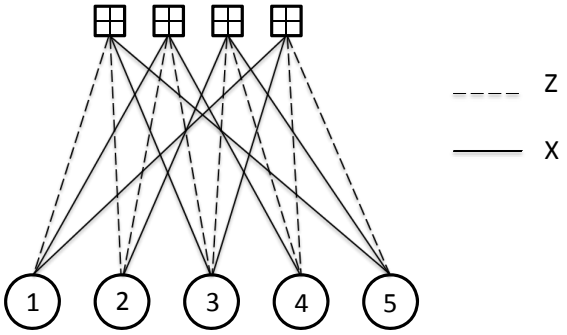

FIGURE 7.2: Tanner graph for the 5-qubit code with stabilizer generator (2.40).

To avoid the presence of a cycle 4-loop, one could make sure that no pair of checks c and $c^{'}$ act on more than one common qubit. However, the commutation condition between two checks depends on the number of positions that a X operator overlaps with a Z operator, or the non-identity positions are the same Pauli operator. This argument leads to the conclusion that every edge connected to qubit q must be the same operator, for instance, Z operator. If this is the case, the code fails to detect the weight-1 Z error that acts on qubit q since all the operators used to diagnosis qubit q are Z, which commutes with the Z error. In conclusion, Tanner graph of QECCs must unavoidably contain cycle 4-loops.

7.2.3.2 Belief propagation decoding of QECCs

Consider the simplest error model, Pauli channels that have the form

$$\xi(\rho) = \sum_{E \in P_N} p(E) E \rho E^{\dagger}, \tag{7.4}$$

where $p(E) \geq 0$ and $\sum_E p(E) = 1$ are probability of error operator and the sum of all the possible errors are equal to 1, respectively. Let $\mathcal{P}_N$ be a Pauli group of

size N. A memoryless Pauli channel is one for which the probability factors as $p(E) = \prod_{q=1}^{N} p_q(E_q)$ for all $E = E_1 E_2 \dots E_N \in P_N$. A particular relevant example is the *depolarizing channel* for which $p_q(I) = 1 - \varepsilon$ and $p_q(X) = p_q(Y) = p_q(Z) = \varepsilon/3$ for all q, and for some depolarizing strength $0 \leq \varepsilon \leq 1$.

Once the N qubits are prepared in a code state $|\psi\rangle$, they are sent through the channel and states $\rho = \xi(|\psi\rangle\langle\psi|)$ is obtained by the receiver. To detect the possible errors at the receiver, the m stabilizer generators are measured simultaneously and outcome the error syndrome $s = (s_1, s_2, \dots, s_M) \in \{\pm 1\}^M$. When the error E that corrupted the register commutes with $S_i, i \in \{1, 2, \dots, M\}$, the syndrome bit s_i takes value $+1$ because $S_i E|\psi\rangle = E S_i|\psi\rangle = E|\psi\rangle$. When E anti-commutes with S_i, $S_i E|\psi\rangle = -E S_i|\psi\rangle = -E|\psi\rangle$ is obtained, and hence $s_i = -1$. The syndrome vector will be used to perform belief propagation decoding as a decoder input.

Belief propagation operates by sending a message along the edges of the Tanner graph (*e.g.* Fig.7.2). Messages from qubit q to check c are denoted by $m_{q\to c}$ and messages from check c to qubit q are denoted $m_{c\to q}$. Messages received at and sent by qubit q are probability distribution over E_q. In other words, each message appears as a vector of 4 positive numbers, one for each value $E_q = I, X, Y, Z$. Note that the neighbours of qubit q and check c are defined as $n(q)$ and $n(c)$.

To initialize the algorithm, each qubit q sends out its message vector of size 4 to all its neighbour $m_{q\to c}(E_q) = p_q(E_q))$, where $p_q(E_q) = p_q(X) = p_q(Y) = p_q(Z) = \varepsilon/3$ in depolarizing channel. Upon reception of these messages, each check sends out a message to its neighbouring qubits given by

$$m_{c\to q}(E_q) = \sum_{E_{1\dots N} \in \{E | E \,\circ\, S^T = s_j)\}} \prod_{q' \in n(c)\backslash q} m_{q'\to c}(E_{q'}), \tag{7.5}$$

where $n(c)\backslash q$ denotes all neighbours of c except q. The sum is over all error operators that tested with stabilizer that gives $s_i = +1$ or -1.

Upon reception of these messages, each qubit sends out a message to its neighbouring checks given by

$$m_{q\to c}(E_q) = p(E_q) \prod_{c' \in n(q)\backslash c} m_{c'\to q}(E_q), \tag{7.6}$$

where $n(q)\backslash c$ denotes all neighbours of q except c. $p_q(E_q)$ is the prior probability distribution of errors.

Equations (7.5) and (7.6) define an iterative procedure that is the core of BP algorithm. The beliefs of each qubit node $b_q(E_q)$ are computed as follows

$$b_q(E_q) = p_q(E_q) \prod_{c\in n(q)} m_{c\to q} E_q. \tag{7.7}$$

After each iteration of message passing, the maximum probability of error $p_q(E_q) = max\{p_q(I), p_q(X), p_q(Z), p_q(Y)\}$ for each qubit q can be obtained. If the obtained error E satisfy the syndrome constraint, the decoding procedure will halt and output E as the detected error vector; otherwise, the iteration procedure continues until a valid result is obtained or the maximum iteration number is reached. Finally, the recovery process is achieved by reapplying the decoded error vector E to the received state.

7.2.4 Quantum LDPC codes over depolarizing channels

In this section, we investigate the dependence of the performance of a quantum LDPC code on the estimated flip probability $\hat{f}$ of a depolarizing channel using the same quantum LDPC code simulated in [149], which is Code A of [68]. In each decoding process, the decoder performed an iterative message passing algorithm (sum-product decoding algorithm) until it either found a valid codeword (regardless of whether it is the word transmitted) or reached a maximum number of 200 iterations. The simulation plots herein is the probability of block error (P_{BLER}) as a function of the estimated flip probability.

In the simulations, the noise vectors were generated to have weight exactly fN, where N was the block length of the code ($N = 1034$) and f is the true flip probability for the depolarizing channel. The decoder assumed an estimated flip probability $\hat{f}$. We varied the value of $\hat{f}$ while the true flip probability f is fixed. The results of our simulations are shown in Fig. 7.3.

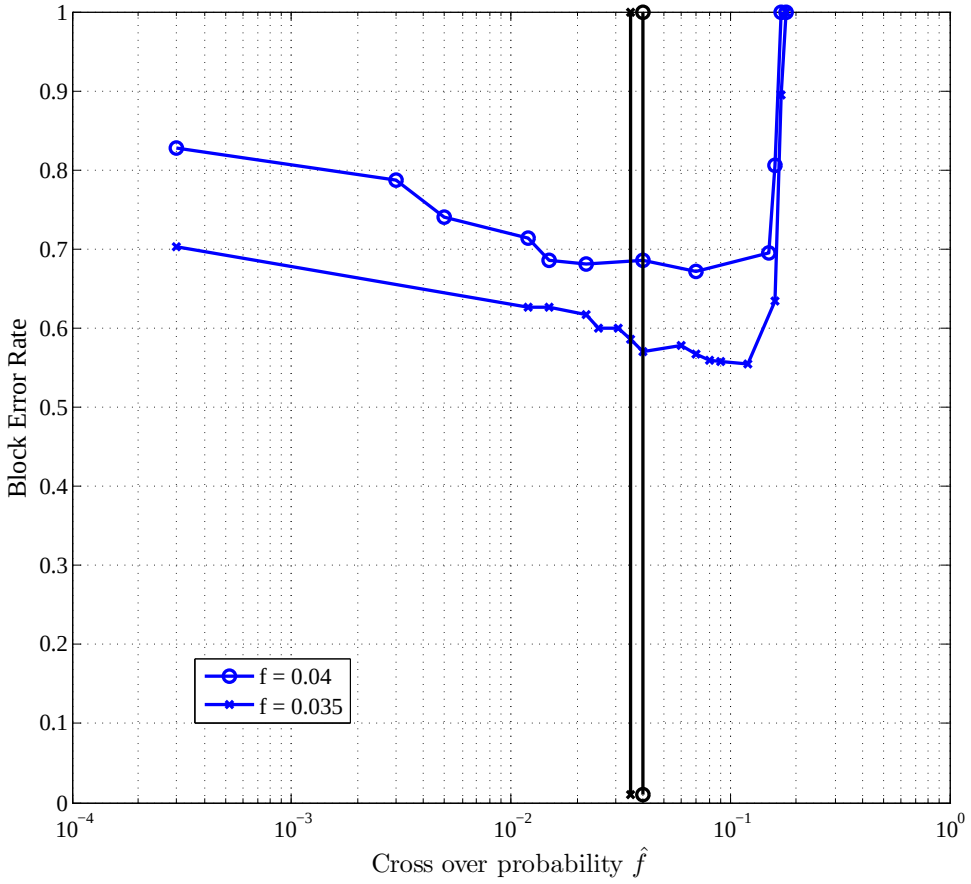

FIGURE 7.3: Probability of block error as a function of estimated flip probability when the true flip probability is fixed.

Similar to the case of classical LDPC codes discussed earlier, we can see from Fig. 7.3 that optimal performance in the quantum LDPC code can be obtained when the input at the decoder is the true flip probability, *i.e* exact channel information is known. The trend of the curve in Fig. 7.3 also shows an overestimate of f is less costly than an underestimate of f, provided that the estimation of channel flip probability, $\hat{f}$, is less than some threshold f^Q_{thr}. For the code shown in Fig. 7.3, the theoretical threshold is $f^Q_{thr} = 0.1893$ (the capacity of classical 4-ary symmetric channel computed from $C_{4-ary} = 2 - H_2(f) - f\log_2(3)$). If $\hat{f} > f^Q_{thr}$, there is a catastrophic increase in the error probability. In the following section, we show

that an improvement in performance of the sum-product decoder can be achieved if $\hat{f} < f_{thr}^{Q}$. Note that the P_{BLER} as a function of $\hat{f}$ shown in Fig. 7.3 is code dependent, which only a small range of P_{BLER} can be shown due to the error correction capability of Code A.

7.2.5 Improved decoding of depolarizing channels

In this section, a numerical approach to improving the performance of the sum-product decoder is described. The asymmetric behaviour of the sum-product decoder shown in Fig. 7.3 implies that in the case of channel mismatch, an over-estimation of the channel flip probability is more desirable than underestimation.

Consider the case where a decoder can only attain partial channel information by probing the quantum channel using un-entangled or entangled quantum states. Given such partial information we will then weight our estimate of the channel parameter (at the decoder side) to larger values (rather than smaller values) of the estimated flip probability.

For a given true flip probability f, the probability of block error shown in Fig. 7.3 can fit approximately by:

$$P_{BLER}^{(f)}(\hat{f}) \approx a + b\hat{f}^3 + c\hat{f}^5 + d\hat{f}^7 + e\sqrt{\hat{f}}ln(\hat{f}), \tag{7.8}$$

where a, b, c, d, e are constants (the approximation gives a 2% tolerance). Assuming our estimator of $\hat{f}$ is centred on the true flip probability (*i.e.* an unbiased estimator), has a variance derived from its quantum Fisher information (*i.e.* an optimal estimator), and has a known probability density function $P(\hat{f})$, we can then make an estimate of what constant should be added to any estimated $\hat{f}$ in order to maximally improve the decoder performance.

Note that, for the case where the qubit probe is in an unentangled state, the quantum Fisher information about f can be shown to be $(N_m J(f))^{-1} = [f(2-f)]$. The average probability of block error for a given f can then be estimated using

the equation

$$\tilde{P}^{(f)}_{BLER} = \int_0^{f^Q_{thr}} P(\hat{f}) P^{(f)}_{BLER}(\hat{f}) d\hat{f}. \tag{7.9}$$

The performance of the sum-product decoder can be improved if a factor $\Delta\hat{f}$ is added to the estimated value of $\hat{f}$. That is, $\hat{f} \rightarrow \hat{f} + \Delta\hat{f}$. The question then becomes, given some channel what is the optimal $\Delta\hat{f}$ that minimizes the expected probability of error? To answer this, Equation (7.9) is modified to

$$\tilde{P}^{(f)}_{BLER}(\Delta\hat{f}) = \int_0^{f^Q_{thr}} P(\hat{f}) P^{(f)}_{BLER}(\hat{f} + \Delta\hat{f}) d\hat{f}, \tag{7.10}$$

The optimal $\Delta\hat{f}$ is then the solution to

$$\frac{\partial}{\partial \Delta\hat{f}} \tilde{P}^{(f)}_{BLER}(\Delta\hat{f}) = 0. \tag{7.11}$$

One could repeat this process for a range of true channel flip probabilities, and derive an estimate of the $\Delta\hat{f}$ averaged over the range of true flip probabilities where QECCs can be expected to be of relevance, that is

$$\Delta\hat{f}_{avg} = \int_0^{f^Q_{thr}} P(f|\hat{f}) \Delta\hat{f}^{(f)} df. \tag{7.12}$$

For the same code (Code A) as that used in Fig. 7.3, assume a uniform distribution for $P(f|\hat{f})$, and taking $N_m = 1$ in the Fisher information, we found that value of $\Delta\hat{f}_{avg}$ to be very weakly dependent on f (see Table 7.1). This means that simply adding to each estimated $\hat{f}$ the additional factor $\Delta\hat{f}_{avg}$ led to substantial performance improvement. The magnitude of this improvement can be seen in Fig. 7.4. In this figure $\Delta\hat{f}_{avg} \approx 0.01422$ is applied at the the decoder to provide the improved error correction (shown are the fraction of blocks in error P_{BLER}), denoted as 'CodeA $- \hat{f} + \Delta\hat{f}_{avg}$'. The notation 'CodeA $- \hat{f}$' in this figure is for the case where the input to the SP decoder is $\hat{f}$ only, whereas the notation 'CodeA $- f$' is for the case where the input to the decoder is the true flip probability f. As can be seen improvements of up to $\sim 50\%$ can found from the new strategy ($\hat{f} + \Delta\hat{f}_{avg}$),

relative to the case of just utilizing the estimated $\hat{f}$. Similar results to those shown were found for other codes investigated, although the factor to be added was found to be a function of the code. For example, in another code investigated (Code B using Construction method III of [68] code length $N = 2068$) a $\Delta\hat{f}_{avg} \approx 0.00365$ was found to be better and the performance improvement is up to $\sim 30\%$ relative to the case of utilizing the estimate $\hat{f}$ (the corresponding optimal $\Delta\hat{f}$ for each different true flip probability f for Code B is also listed in TABLE 7.1 and see also Fig. 7.4 for simulation improvement). Of course, improved channel estimation also alters the details of our analysis, with more accurate measurements (*e.g.* a higher number of measurements N_m of the channel) leading to smaller $\Delta\hat{f}_{avg}$, and smaller improvements in performance.

TABLE 7.1: Optimal $\Delta\hat{f}$ for different f.

Code A		Code B	
f	$\Delta\hat{f}$	f	$\Delta\hat{f}$
0.04	0.02638	0.05	0.00554
0.03	0.01659	0.04	0.00471
0.02	0.01292	0.03	0.00397
0.01	0.00097	0.02	0.00268
		0.01	0.00134

Finally, it is perhaps worth illustrating how the use of optimal $\Delta\hat{f}$ for each f (denoted as 'CodeA $- \hat{f} + \Delta\hat{f}$' in Fig. 7.4), rather than $\Delta\hat{f}_{avg}$ for every f, impact the results. From Fig. 7.4 we can see that if the optimal $\Delta\hat{f}$ for each true f is applied for $f > 0.025$, the error performance is better compared to the case of using $\Delta\hat{f}_{avg}$ for every f (see the magnified portion in Fig 7.4). This is true since $\Delta\hat{f}_{avg}$ provides excess weight for small f and less weight for large f.

7.3 Chapter summary

In this chapter we have investigated possible improvements in the decoding strategies of quantum LDPC decoders in the quantum depolarization channel. The importance of the channel mismatch effect in determining the performance of quantum LDPC codes has very recently been shown to lead to a degradation in

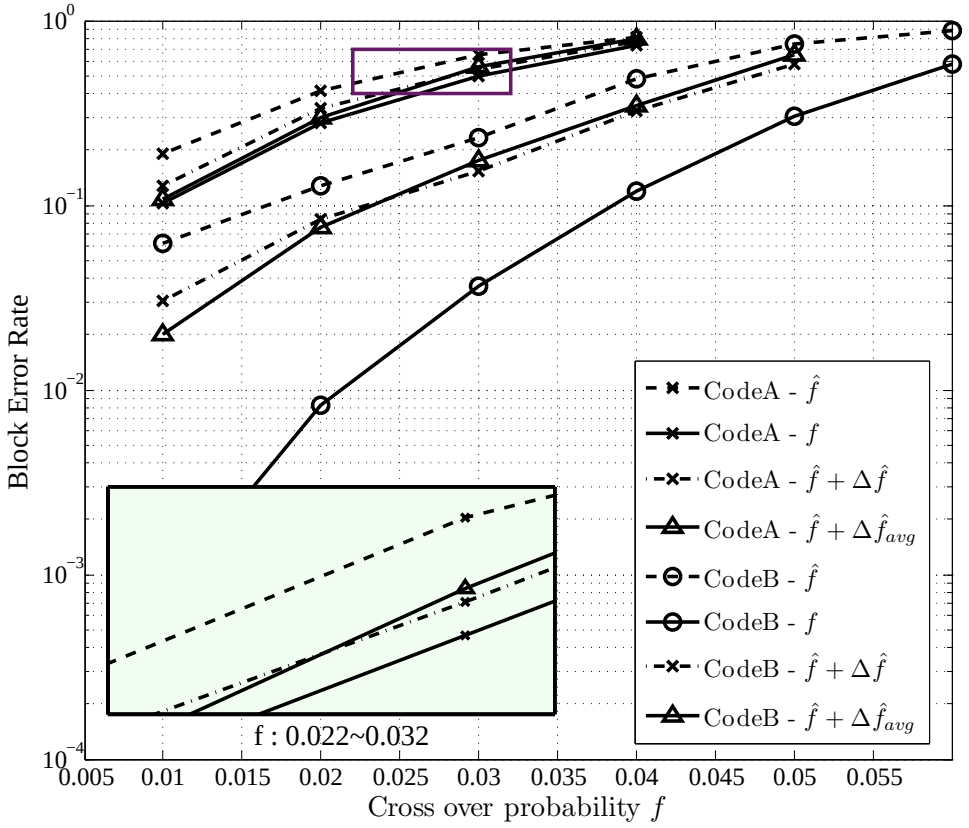

FIGURE 7.4: Comparison of block error rate of Codes A and B.

the qubit error performance. We have illustrated how such a performance gap in the qubit error performance can be substantially reduced. The new strategies for quantum LDPC decoding we provided here are based on previous insights from classical LDPC decoders in mismatched channels, where an asymmetry in performance is known as a function of the estimated bit-flip probability. We first showed how similar asymmetries carry over to the quantum depolarizing channel. We then showed that when a weighted estimate of the depolarization flip parameter to larger values is assumed, performance improvement by as much as 50% was found. We conjecture that all quantum channels which are misidentified, or for which only partial channel information is available, will benefit from similar decoding strategies to those outlined here.

The work outlined here will be of practical importance when large-scale quantum networks are built, and sophisticated quantum error correction codes are deployed in order to maintain the entanglement between the distributed entangled qubit pairs that underpins these emerging networks. The strategies described here will

ultimately manifest themselves in an improved performance of entanglement-based QKD, or any other entanglement-based quantum communication application, deployed over such future networks.

Chapter 8

Thesis Conclusion

Inspired by the needs of the quantum computer, which takes advantage of quantum mechanical phenomena, such as superposition of states and entanglements between qubits, to solve certain problems efficiently and faster than their classical counterparts, the ability to mitigate the noise resulting from decoherence will determine whether building a quantum computer is feasible. Quantum error-correcting codes are essential to correct quantum information.

In this thesis, we investigated various aspects of quantum error-correcting codes. We provided a self-contained introduction on the fundamental theory of quantum error correction and stabilizer coding, and constructed various families of quantum error-correcting codes over a finite field. The constructed codes can correct standard bit-flip and phase flip errors. More interestingly, with a certain containing property satisfied, the proposed stabilizer codes constructed from classical cyclic codes are also capable of correcting synchronization errors.

Two types of quantum stabilizer codes were proposed based on quadratic residue sets of prime modulus and prime difference sets of parameters $(4n-1, 2n-1, n-1)$ with $n \geq 2$. The minimum distance for Type-I stabilizer codes of length $N = 4n+1$ is closely related to the size of quadratic residue sets while the dimension is a constant, whereas the code rate for the stabilizer codes of length $N = 4n - 1$ is nearly half. The constructed Type-I stabilizer codes of length $N = 4n +$

1 achieve the distance lower bound given in the literature. Furthermore, the proposed construction methods for DSS codes generate a difference set from a single input parameter and ensure that the constructed codes satisfy the symplectic inner product constraint. We proposed three methods for constructing DSS codes from either a full difference set or a subset of a difference set. Simulation results, using a low-complexity majority-logic decoding algorithm, show that by designing DSS codes from subsets of a difference set, the qubit error rate can be reduced.

We then designed large-scale quantum stabilizer codes by proposing a systematic design of stabilizer quantum LDPC codes with quasi-cyclic structure using the notion of proto-matrix (and proto-graph). By designing a Latin square based proto-matrix from quadratic (non-) residue sets of prime modulus, and its equivalent matrices using transformation matrices, the proposed construction methods yielded a wide range of quantum LDPC codes with different code lengths and rates. We proposed three types of proto-graph quantum LDPC codes, Type-I-A, Type-I-B and Type-II. For prime QR set of parameters $p = 4n - 1$, the Type-I-A QCS codes of length $N = pk$ are constructed using the method of adjunction with dimension $K = k-1$ and $K = 2k-1$ for odd n and even n, respectively. Moreover, the Type-I-B quantum LDPC codes of length $N = 2kv$ are constructed using the method of concatenation with dimension $K \geq 2kv-\rho' v+\rho'-1$, where $\rho' \leq \rho$ is the column weight of the derived QC-LDPC codes. For prime QR sets of parameters $p = 4n+1$, a necessary transformation of the proto-matrix is required to construct Type-II quantum LDPC codes of length $N = kv$ with a dimension lower bounded by $K \geq kv - \rho' v + \rho' - 1$. We showed that for $\rho' \leq \rho$, the minimum distance of the proposed Type-I-B and Type-II codes is lower bounded by $2\rho' - 1$. In addition, by applying transformations among proto-matrices, the proposed design of Type-I-B codes significantly reduce the number of cycles of length 4 compared to Type-I-A codes. We also show that the proposed Type-I-B codes over quantum depolarizing channel with sum-product decoding algorithm outperform both Type-I-A and Type-II quantum LDPC codes. Furthermore, the proposed two constructions, namely Construction A and B, showed that the pre-lifting of a proto-graph can be performed using the idempotent polynomials of QR/NQR sets, and the quantum

LDPC codes constructed from tensor product operation yields a class of quantum codes of rates as high as above 0.9.

We further proposed a class of quantum synchronizable codes from classical Q-ary chain-containing cyclic codes and showed that the proposed method enables a flexible construction of quantum synchronizable codes of various different dimensions over different order of finite field. The proposed quantum synchronizable codes of CSS structure is a type of quantum stabilizer code that corrects both standard quantum errors and misalignment errors. The minimum distance of the proposed chain-containing quantum synchronizable codes can be bounded using rational functions. We showed that the quantum synchronizable codes from classical quadratic residue codes possess the highest possible tolerance against synchronization errors.

Nevertheless, in practical settings, the channel mismatch effect on the performance of quantum LDPC codes has been discussed. The performance loss due to the channel mismatch can be reduced by using a weighted estimate of the channel parameter.

Future Research Directions

Here we discuss some future works that are interesting and relevant to some of the materials presented in this thesis.

1. The proposed quantum LDPC codes were based on a square all-one matrix. A challenging extension work of this would be the exploration of designing quantum LDPC codes from irregular proto-matrix or semi-regular (either fix the degree of rows or columns), which would further enhance the sparsity of quantum LDPC codes and improve its decoding performance. Moreover, it is also interesting to design self-orthogonal QC-LDPC codes from sparse proto-graphs in order to maximise the girth of the lifted code.

2. The construction methods for the proposed Type-I-B and Type-II quantum LDPC codes are based on the use of transformation matrices, which alter the

elements of QR and NQR sets. It would be interesting to design proto-graph quantum LDPC codes using difference sets so that the resulting proto-graph is sparse and the girth of the derived codes can be maximized.

3. Designing proto-graph based spatial-coupled quantum LDPC codes is a future work, since the spatial-coupled quantum LDPC codes are the only family of quantum codes that approaches to the Hashing bound for Pauli channels. [69].

4. In Chapter 5, the proposed quantum synchronizable codes are of CSS structure, which was initially proposed in [140]. It would be interesting to construct quantum synchronizable codes of non-CSS structure, since the dimension of CSS codes is inefficient compared to a non-CSS stabilizer code.

5. It would also be interesting to study the phenomenon of channel mismatch effect for a general quantum channel. To this end, it is desirable to introduce new or modified decoding algorithms for quantum LDPC codes with the presence of channel mismatch.

6. The conventional belief propagation decoding algorithm used to decode a quantum LDPC code does not address the issue of degeneracy. Since degeneracy of quantum codes is one of the beneficial properties compared to its classical counterpart, designing deterministic belief propagation decoding method that addresses degeneracy issue for quantum LDPC codes is an interesting but challenging task.

7. Notice that the quantum LDPC codes designed from tensor product operation are capable of correcting bursts of errors and bursts of bursts of errors if the pair of quasi-cyclic LDPC codes are properly designed. This is due to the efficient two-stage decoding method for tensor product block codes, which was first introduced in [130]. Hence, it is interesting to design an efficient two stage sum-product decoder for quantum LDPC codes constructed from tensor product operation.

8. When implementing general quantum error correcting codes, one big challenge comes from the complexity of the quantum circuits, for both encoding and decoding. To verify and enhance the control ability to implement complex quantum circuits are critical tasks for implementing QECCs in building scalable quantum computers. Coherent control of some of the simplest single-erasure-error- correcting code, such as the $((4, 2^2, 2))$ and the $((5, 2^1, 3))$ codes, have been demonstrated in optical systems [152] and nuclear magnetic resonance (NMR) systems [153], respectively. The main difficulty for implementing a quantum code is that the quantum devices are subject to errors, from inevitable coupling to the uncontrollable environment, or from other mechanisms such as imperfection in controlled operations. The errors damage the coherence, and consequently can reduce the computational ability of quantum computers. In order to protect quantum coherence, scheme of *fault-tolerant* quantum computation [11, 15] is important, which would be one of interesting future topics to pursue.

Appendix A

Appendix

A.1 Proof for Proposition 5.7

Let $\{d_1, d_2, \ldots, d_k\}$ be the k elements of the quadratic residue set $\mathcal{Q}^{\mathcal{R}}$, and $\sigma_1, \sigma_2, \ldots, \sigma_k$ be k permutations of $\{1, 2, \ldots, k\}$ such that $d_{\sigma_1(j)}, d_{\sigma_2(j)}, \ldots, d_{\sigma_k(j)}$ are distinct for every $1 \leq j \leq k$. The parity-check matrix H_1 over $\mathbb{F}_2$ is then expressed as

$$H_1 = \begin{bmatrix} P_{11}^{d_{\sigma_1(1)}} & \cdots & P_{1k}^{d_{\sigma_1(k)}} \\ \vdots & \ddots & \vdots \\ P_{k1}^{d_{\sigma_k(1)}} & \cdots & P_{kk}^{d_{\sigma_k(k)}} \end{bmatrix},$$

where each P_{ij}^{d} denotes the d-th power of P. Let α be a primitive p-th root of unity and $\mathbb{F}_2(\alpha)$ be the minimal finite field containing both $\mathbb{F}_2$ and α. Denote by V the $p \times p$ Vandermonde matrix generated by α over $\mathbb{F}_2(\alpha)$:

$$V_p = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{p-1} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{p-1} & \cdots & \alpha^{(p-1)(p-1)} \end{bmatrix}.$$

Since α is a primitive p-th root of unity, α^i is a root of $x^p - 1$ and not equal to 1 for all $1 \leq i \leq p-1$. Moreover, since $x^p - 1 = (x-1)(x^{p-1} + \cdots + 1)$, $\sum_{j=0}^{p-1} \alpha^{ij} = 0$ for all $1 \leq i \leq p-1$. Furthermore, since 2 and p are co-prime, summation of 1 by p times is still equal to 1 over $\mathbb{F}_2$. It is then easy to check that the inverse of V_p is:

$$V_p^{-1} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(p-1)} \\ \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{-(p-1)} & \cdots & \alpha^{-(p-1)(p-1)} \end{bmatrix}.$$

For $0 \leq i \leq p-1$, denote by $\mathcal{D}(\alpha^i)$ the $p \times p$ matrix with diagonal entries equal to $\{1, \alpha^i, \cdots, \alpha^{i(p-1)}\}$, that is,

$$\mathcal{D}(\alpha^i) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \alpha^i & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha^{i(p-1)} \end{bmatrix}.$$

Thus,

$$P^1 = V_p \cdot \mathcal{D}(\alpha) \cdot V_p^{-1}.$$

Hence for any $0 \leq d \leq p-1$, we have

$$P^d = V_p \cdot \mathcal{D}(\alpha^d) \cdot V_p^{-1}.$$

The matrix H_1 can then be decomposed into

$$H_1 = Diag\left(V_p\right) \cdot \tilde{H}_1 \cdot Diag\left(V_p^{-1}\right), \tag{A.1}$$

where

$$\tilde{H}_1 = \begin{bmatrix} \mathcal{D}(\alpha^{d_{\sigma_1(1)}}) & \cdots & \mathcal{D}(\alpha^{d_{\sigma_1(k)}}) \\ \vdots & \ddots & \vdots \\ \mathcal{D}(\alpha^{d_{\sigma_k(1)}}) & \cdots & \mathcal{D}(\alpha^{d_{\sigma_k(k)}}) \end{bmatrix},$$

$$Diag\,(V_p) = \begin{bmatrix} V_p & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & V_p \end{bmatrix},$$

and

$$Diag\left(V_p^{-1}\right) = \begin{bmatrix} V_p^{-1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & V_p^{-1} \end{bmatrix}.$$

Since both $Diag(V_p)$ and $Diag(V_p^{-1})$ have full rank kp, $Rank(H_1) = Rank(\tilde{H}_1)$.

Note that $\tilde{H}_1$ can be regarded as a block matrix with $k \times k$ blocks each of which is a $p \times p$ diagonal matrix. We can then rearrange the columns and rows in $\tilde{H}_1$ to form a block diagonal matrix $\tilde{\tilde{H}}_1$ with each block of size $k \times k$, that is

$$\tilde{\tilde{H}}_1 = \begin{bmatrix} C_0 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & C_1 & \ddots & \mathbf{0} \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & C_{p-1} \end{bmatrix},$$

where

$$C_j = \begin{bmatrix} \alpha^{jd_{\sigma_1(1)}} & \cdots & \alpha^{jd_{\sigma_1(k)}} \\ \vdots & \vdots & \vdots \\ \alpha^{jd_{\sigma_k(1)}} & \cdots & \alpha^{jd_{\sigma_k(k)}} \end{bmatrix}$$

for all $0 \leq j \leq p-1$. Obviously,

$$Rank(\tilde{H}_1) = Rank(\tilde{\tilde{H}}_1) = \sum_{j=0}^{p-1} Rank(C_j).$$

Since C_0 is an all-one matrix of size $k \times k$, $Rank(C_0) = 1$. Furthermore, since each row of H_{1proto} is a cyclic shift of the first row, we denote

$$\begin{aligned} \sigma_2(1, \cdots, k) &= (\sigma_1(2), \sigma_1(3), \cdots, \sigma_1(1)), \\ &\vdots \\ \sigma_k(1, \cdots, k) &= (\sigma_1(k), \cdots, \sigma_1(k-2), \sigma_1(k-1)). \end{aligned}$$

Thus, C_j is a circulant matrix over $\mathbb{F}_2(\alpha)$. Let U be the $k \times k$ cyclic permutation matrix in the same form as P except for the different size. Then,

$$C_j = \alpha^{jd_{\sigma_1(1)}} U^0 + \alpha^{jd_{\sigma_1(2)}} U^1 + \cdots + \alpha^{jd_{\sigma_1(k)}} U^{k-1}.$$

Let β be a primitive k^{th} root of unity, $\mathcal{D}(\beta^i)$ be the $k \times k$ diagonal matrix with diagonal entries equal to $\{1, \beta^i, \cdots, \beta^{i(k-1)}\}$, and V_k be the $k \times k$ Vandermonde matrix (over $\mathbb{F}_2(\alpha)(\beta)$) generated by β. Since $U = V_k \cdot \mathcal{D}(\beta) \cdot V_k^{-1}$ and $U^i = V_k \cdot \mathcal{D}(\beta^i) \cdot V_k^{-1}$, we have

$$C_j = V_k \cdot \left(\sum_{i=0}^{k-1} \alpha^{jd_{\sigma_1(i+1)}} \mathcal{D}(\beta^i) \right) \cdot V_k^{-1}.$$

Thus, the rank of C_j is equal to the number of nonzero diagonal entries in

$$\sum_{i=0}^{k-1} \alpha^{jd_{\sigma_1(i+1)}} \mathcal{D}(\beta^i).$$

Equivalently, it is equal to $k - z$, where z is the number of roots of the polynomial $f_j(x) = \sum_{i=0}^{k-1} \alpha^{jd_{\sigma_1(i+1)}} x^i$ that belong to $\{1, \beta, \cdots, \beta^{k-1}\}$. Since p and k are co-prime and $\alpha^p = \beta^k = 1$, it can be deduced that $f_j(\beta^i) \neq 0$ for all $1 \leq j \leq p-1$ and $1 \leq i \leq k-1$. Next, note that $f_j(1) = \sum_{i=0}^{k-1} \alpha^{jd_{\sigma_1(i+1)}} = \sum_{i=1}^{k} \alpha^{jd_i}$. Thus, (i) when n is odd, $\sum_{i=1}^{k} \alpha^{jd_i} \neq 0$ for all $1 \leq j \leq p-1$; (ii) when n is even, there are exactly $\frac{p-1}{2} = k$ elements in $\{\alpha, \cdots, \alpha^{p-1}\}$ which are roots of $\sum_{i=1}^{k} x^{d_i}$. Now, we

can obtain

$$\begin{aligned} Rank(H_1) &= Rank(C_0) + \cdots + Rank(C_{p-1}) \\ &= \begin{cases} 1 + k(p-1), & \text{when } n \text{ is odd} \\ 1 + k(p-1) - k, & \text{when } n \text{ is even} \end{cases}. \end{aligned}$$

Similarly, the rank of H_2 can be proved to be 1 deficient from the rank of H_1. Since each P_{ij}^d of H_2 has weight equal to 2, *i.e.,* $(P^d + P^0)$, the diagonal matrix $\mathcal{D}$ will have the form

$$\mathcal{D}(1+\alpha^i) = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1+\alpha^i & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1+\alpha^{i(p-1)} \end{bmatrix}.$$

Then $\tilde{H}_2$ will be written as

$$\tilde{H}_2 = \begin{bmatrix} \mathcal{D}(1+\alpha^{d_{\sigma_1(1)}}) & \cdots & \mathcal{D}(1+\alpha^{d_{\sigma_1(k)}}) \\ \vdots & \ddots & \vdots \\ \mathcal{D}(1+\alpha^{d_{\sigma_k(1)}}) & \cdots & \mathcal{D}(1+\alpha^{d_{\sigma_k(k)}}) \end{bmatrix}.$$

Note that the first entry of $\mathcal{D}(1+\alpha^i)$ is always 0. By rearranging the columns and rows of $\tilde{H}_2$, we turn $\tilde{H}_2$ into a block diagonal matrix $\tilde{\tilde{H}}_2$ of the same format as $\tilde{\tilde{H}}_1$ with $Rank(C_0) = 0$. Hence, $Rank(H_2) = Rank(H_1) - 1$. Furthermore, we know that the row rank of a matrix equals to its column rank. We also know that there exists a sub-matrix H^{sub} with non-zero determinant of size $Rank(H_1) \times Rank(H_1)$. Therefore, the rank of the parity-check matrix H is given by $Rank(H) = max\{Rank(H_1), Rank(H_2)\} = Rank(H_1)$. We have now completed the proof.

Bibliography

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *in Proc. of the 35th Annual Symp. on Foundations of Comp. Sci.*, pp. 124 - 134, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," *in Proc. of the 28th Annual ACM Symp. on Theory of Comp.*, pp. 212 - 219, 1996.

[3] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, vol. 52, pp. 2493 - 2496, 1995.

[4] A. Steane, "Multiple particle interference and quantum error correction," *in Proc. Royal Society of London*, vol. 452, no. 1954, pp. 2551 - 2577, 1996.

[5] A. M. Steane, "Error Correcting Codes in Quantum Theory," *Phys. Rev. Lett.*, vol. 77, pp. 793 - 797, 1996.

[6] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098 - 1105, 1996.

[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405 - 409, 1997.

[8] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, " Quantum error correction via codes over GF(4)," *IEEE Trans. Inf. Theory*, vol. 44, No. 4, pp. 1369 - 1387, 1998.

[9] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola and W. H. Zurek, "Introduction to Quantum Error Correction," *arXiv:quant-ph/0207170v1*, 2002.

[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824 - 3851, 1996

[11] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", *Cambridge Uni. Press*, New York, 2000.

[12] D. A. Lidar and T. A Brun, "'Quantum error correction', *Cambridge Uni. Press*, 2013.

[13] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code, *Phys. Rev. Lett.*, vol. 77, no. 1, pp. 198 - 201, 1996.

[14] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, pp. 1862 - 1868, 1996.

[15] D. Gottesman, "Stabilizer codes and quantum error correction", *Ph.D Thesis*, Caltech, 1997.

[16] M. Grassl, T. Beth and T. Pellizzari, "Codes for the quantum erasure channel," *Phys. Rev. A,* vol. 56, pp. 33 - 38, 1997.

[17] M. Grassl and T. Beth, "Quantum BCH codes," *in Proc. Int. Symp. Theo. Elec. Engin.*, pp. 207 - 212, 1999.

[18] S. A. Aly, A. Klappenecker, and P K. Sarvepalli, "On quantum and classical BCH codes", *IEEE Trans. Info. Theo.*, vol. 53, No. 3, pp. 1183 - 1188, 2007.

[19] A. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2492 - 2495, 1999.

[20] M. Grassl, W. Geiselmann and T. Beth, "Quantum Reed-Solomon codes," *App. Alge. Algorm. and Error-Correcting Codes*, vol. 1719, pp. 231 - 244, 1999.

[21] A. Steane, "Quantum Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1701 - 1703, 1999.

[22] H. F. Chau, "Quantum convolutional error-correcting codes," *Phys. Rev. A*, vol. 58, pp. 905 - 909, 1998.

[23] H. F. Chau, "Good quantum -convolutional error-correction codes and their decoding algorithms exist," *Phys. Rev. A*, vol. 60, pp. 1966 - 1974, 1999.

[24] A. C. A. de Almeida and R. Palazzo Jr., "A concatenated [(4, 1, 3)] quantum convolutional code," *in Proc. IEEE Infor. Theo. Workshop*, 2004.

[25] M. Grassl and M. Roetteler, "Constructions of quantum convolutional codes," *in Proc. IEEE Int. Symp. Info. Theo.,* 2007.

[26] G. D. Forney, Jr., M. Grassl, and S. Guha, "Convolutional and tailbiting quantum error-correcting codes," *IEEE Trans. Info. Theory*, vol. 53, no. 3, pp. 865 - 880, 2007.

[27] A. Cross, G. Smith, J. A. Smolin and B. Zeng, "Codeword stabilized quantum code", *IEEE Trans. Info. Theo.*, vol. 55, pp. 433 - 438, 2009.

[28] E. M. Rains, "Nonbinary Quantum Codes", *IEEE Trans. Info. Theo.*, vol. 45, pp. 1827 - 1831, 1999.

[29] A. Ashikhmin and E. Knill, "Non-binary quantum stabilizer codes," *IEEE Trans. Info. Theo.*, vol. 47, pp. 3065 - 3072, 2001.

[30] , A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields", *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4892 – 4914, 2006.

[31] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum Reed-Muller codes", *in Proc. Int. Symp. Inform. Theory (ISIT)*, pp. 1023 — 1027, 2005.

[32] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A Nonadditive Quantum Code," *Phys. Rev. Lett.*, vol. 79, pp. 953 - 954, 1997.

[33] J. A. Smolin, G. Smith, and S. Wehner, "Simple Family of Nonadditive Quantum Codes," *Phys. Rev. Lett.*, vol. 99, pp. 130505 - 130508, 2007.

[34] G. Smith and J. A. Smolin, "Degenerate Quantum Codes for Pauli Channels," *Phys. Rev. Lett.*, vol. 98, p. 030501, 2007.

[35] F. J. MacWilliams and N. J. A. Sloane, "The theory of error-correcting codes", *North-holland Publishing Company.* 2nd edition, 1978.

[36] M. Grassl and T. Beth, "Cyclic quantum Error-correcting codes and quantum shift registers", *in Proc. R. Soc. London Ser. A*, vol. 456, pp. 2689 - 2706, 2000.

[37] Z. Babar, S. X. Ng and L. Hanzo, "EXIT-Chart-Aided Near-Capacity Quantum Turbo Code Design", *IEEE Trans. Vehi. Tech.*, vol. 64, pp. 866 - 875, 2015.

[38] M. Wilde, M.-H. Hsieh and Z. Babar, "Entanglement-Assisted Quantum Turbo Codes," *IEEE Trans. Info. Theory*, vol. 60, no. 2, pp. 1203 - 1222, 2014.

[39] D. MacKay, G. Mitchison and P. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2315 - 2330, 2004.

[40] D. Mackay, G. Mitchison and A. Shokrollahi, "More sparse-graph codes for quantum error correction," *www.inference.phy.cam.ac.uk/mackay/cayley.pdf*, 2007

[41] A. Couvreur, N. Delfosse and G. Zemor, "A construction of quantum LDPC codes from cayley graphs," *IEEE Proc. Int. Symp. Info. Theory*, pp. 643 - 647, 2011.

[42] A. Couvreur, N. Delfosse and G. Zemor, "A construction of quantum LDPC codes from cayley graphs," *IEEE Trans. Info. Theory*, vol. 59, no. 9, pp. 6087 - 6098, 2013.

[43] R.G. Gallager, "Low-Density Parity-Check Codes", *Cambridge, MA: MIT Press*, 1963.

[44] H. F. Chau, "Five quantum register error correction code for higher spin systems," *Phys. Rev. A*, vol. 56, p. R1, 1997.

[45] K. Feng, "Quantum codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ $p \geq 3$ exist", *IEEE Trans. Info. Theory*, vol. 48, no. 8, pp. 2384 -– 2391, 2002.

[46] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Letters*, vol. 77, pp. 198-201, 1996.

[47] Z. Li, L. J. Xing, and X. M. Wang, "Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A*, vol. 77, pp. 012308(1)–012308(4), 2008.

[48] G. G. La Guardia, "New Quantum MDS Codes", *IEEE Trans. Info. Theory*, vol. 57, no. 8, 2011.

[49] L. Wang and S. Zhu, "New quantum MDS codes derived from constacyclic codes", *Jour. Quantum Info. Processing*, vol. 14, no. 3, pp. 881 – 889, 2015.

[50] M. Grassl and M. Rotteler, "Quantum MDS Codes over Small Fields", *http://arxiv.org/pdf/1502.05267v1.pdf*, 2015.

[51] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, pp. 399 - 431, 1999.

[52] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 619 - 637, 2001.

[53] S.-Y. Chung, G. Forney, T. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 db of the shannon limit," *IEEE Comm. Lett.*, vol. 5, pp. 58 - 60, 2001.

[54] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Comm.*, vol. 49, no. 10, pp. 1727 - 1737, 2001.

[55] S. ten Brink, G. Kramer, and A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," *IEEE Trans. Comm.*, vol. 52, no. 4, pp. 670 - 678, Apr. 2004.

[56] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes," *Cambridge University Press*, 2003.

[57] E. R. Berlekamp, "Algebraic Coding Theory," *McGraw-Hill*, 1st edition, 1968.

[58] H. Ollivier and J. P. Tillich, "Description of a quantum convolutional code," *Phys. Rev. Lett.*, vol. 91, p. 177902, 2003.

[59] H. Ollivier and J. P. Tillich, "Quantum convolutional codes: fundamentals," *quant-ph/0401134*, 2004.

[60] E. Dennis, "Quantum codes on high-genus surfaces," quant-ph/0007072.

[61] E. Dennis, A. Kitaev, A. Landahl and J. Preskill, "Topological quantum memory," *J. Math. Phys*, vol. 43, pp. 4452 - 4505. quant-ph/0110143, 2002.

[62] M. S. Postol, "A proposed quantum low-density parity-check codes," arXiv: quant-ph/0108131, 2001.

[63] T. Camara, H. Ollivier, and J. P. Tillich, "A class of quantum LDPC codes: construction and performance under iterative decoding," *IEEE Proc. Int. Symp. Info. Theory*, pp. 811 - 815, 2007.

[64] T. Camara, H. Ollivier, and J. P. Tillich, "Constructions and performance of classes of quantum LDPC codes", *arxiv:quant-ph/0502086v2*, 2005

[65] S. A. Aly, "A class of quantum LDPC codes derived from Latin squares and combinatorial objects," *Technical report*, Dep. of Comp. Sci, Texas A&M University, 2007.

[66] S. A. Aly, "A class of quantum LDPC codes constructed from finite geometries," *in Proc. IEEE GlobeCom*, pp. 1 - 5, 2008.

[67] M. Hagiwara and H. Imai, "Quantum Quasi-cyclic LDPC codes," *in Proc. IEEE Int. Symp. Inf. Theory*, pp. 806 - 810, 2007.

[68] P. Tan and J. Li, "Efficient quantum stabilizer codes: LDPC and LDPC-convolutional constructions," *IEEE Trans. Inf. Theory*, vol. 56, pp. 476 - 491, 2010.

[69] M. Hagiwara, K. Kasai, H. Imai, and K. Sakaniwa, "Spatially coupled quasi-cyclic quantum LDPC codes," *in Proc. IEEE Int. Symp. Inf. Theory*, pp. 638 - 642, 2011.

[70] C. Y. Lai and C. C. Lu, "A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices," *IEEE Trans. Inf. Theory*, vol. 57, No. 10, pp. 7163 - 7179, 2011.

[71] I. B. Djordjevic. "Quantum LDPC codes from incomplete block designs," *IEEE Comm. Lett.*, vol. 12, pp. 389 - 391, 2008.

[72] I. Andriyanova, D. Maurice, and J. P. Tillich, "Quantum LDPC codes obtained by non-binary constructions," *In Proc. IEEE Int. Symp. Inf. Theory*, pp. 343 - 347, 2012.

[73] I. Andriyanova, D. Maurice, and J. P. Tillich, "Spatially coupled quantum LDPC codes," *In Proc. IEEE Inf. Theory. Workshop*, pp. 327 - 331, 2012.

[74] K. Kasai, M. Hagiwara, H. Imai and K. Sakaniwa, "Non-binary Quasi-Cyclic quantum LDPC codes," *in Proc. IEEE Int. Symp. Inf. Theory*, pp. 653 - 657, 2011.

[75] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum Error Correction beyond the Bounded Distance Decoding Limit," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 1223 - 1230, 2012.

[76] H. Lou and J. Garcia-Frias, "Quantum error-correction using codes with low-density generator matrix," *IEEE 6th Workshop on Sig. Proc. Adv. in Wireless Comm.*, pp. 1043 - 1047, 2005.

[77] H. Lou and J. Garcia-Frias, "On the application of error-correcting codes with low-density generator matrix over different quantum channels," *Int. ITG-Conf on Source and Channel Coding*, pp. 1 - 6, 2006.

[78] G. Bowen, "Entanglement required in achieving entanglement-assisted channel capacities," *Phys. Rev. A*, vol 66, p. 052313, 2002.

[79] T. Brun, I. Devetak and M. H. Hsieh, "Correcting Quantum Errors with Entanglement", *Science*, vol. 314, no. 5798, 2006.

[80] T. Brun, I. Devetak and M. H. Hsieh, "General entanglement-assisted quantum error-correcting codes," *IEEE Proc. Int. Symp. Info. Theory*, pp. 2101 - 2105, 2007.

[81] M.-H. Hsieh, I. Devetak and T. Brun, "General entanglement-assisted quantum error-correcting codes," *Phys. Rev. A*, vol. 76, p. 062313, 2007.

[82] M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," *IEEE Proc. Int. Symp. Info. Theory*, pp. 445 - 449, 2011

[83] M.-H. Hsieh, T. Brun and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Phys. Rev. A*, vol. 79, p. 032340, 2009.

[84] M. Wilde and T. Brun, "Entanglement-assisted quantum convolutional coding," *Phys. Rev. A*, vol. 81, p. 042333, 2010.

[85] M. Wilde and J. Renes, "Quantum polar codes for arbitrary channels," *IEEE Proc. Int. Symp. Info. Theory*, pp. 334 - 338, 2012.

[86] J. Thorpe. "Low-Density Parity-Check codes constructed from protographs", *In The Interplanetary Network Progress Report*, Jet Propulsion Laboratory (JPL), pp. 1-7, 2003.

[87] M. P. C. Fossorier, "Quasi-Cyclic Low-Density Parity-Check Codes From Circulant Permutation Matrices," *IEEE Trans. Inf. Theory*, vol 50, no. 8, pp. 1788 - 1793, 2004.

[88] Y. Kou, S. Lin and M. P. C. Fossorier, "Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results", *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711 - 2736, 2001.

[89] Q. Huang, Q. Diao, S. Lin and K. Abdel-Ghaffar, "Cyclic and Quasi-Cyclic LDPC Codes on Constrained Parity-Check Matrices and Their Trapping Sets", *IEEE, Trans. Inf. Theory*, vol. 58, no. 5, pp. 2648 - 2671, 2012.

[90] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes," *Quantum Information Computation*, vol. 8, pp. 987–1000, 2008.

[91] M. Grassl, "Bounds on the Minimum Distance of Linear Codes and Quantum Codes" [Online]. http://codetables.de.

[92] E. M. Rains, "Quantum Codes of Minimum Distance Two," *IEEE Trans. Info. Theory*, vol. 45, no. 1, 1999.

[93] E. Knill and R. Laflamme, "A theory of quantum error correcting codes," *Phys. Rev. A*, vol. 55, pp. 900 - 911, 1997.

[94] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Phys. Rev. Lett.*, vol. 77, pp. 2585 - 2588, 1996.

[95] S. M Zhao, Y. Xiao, Y. Zhu, X. L. Zhu and M. H. Hsieh, " New class of quantum codes constructed from cyclic difference set", *Int. Jour. Quant. Infor.,* vol. 10, No. 1, 2012.

[96] L. D. Baumert, "Cyclic Difference Sets", *Lecture Notes in Mathematics 182,* New York: Springer-Verlag, 1971.

[97] T. Beth, D. Jungnickel and H. Lenz, "Design Theory", *Cambridge University Press*, New York, 1986.

[98] I. Anderson, "Combinatorial Designs: Construction Methods", *Ellis Horwood Limited*, 1990.

[99] W. E. Ryan, and S. Lin, "Channel Codes: classical and Modern," *Cambridge University Press*, 2009.

[100] S. Lin and D. J. Castello, Jr, " Error Control Coding, second edition" *Pearson Prentice Hall*, 2004.

[101] J. van Lint and R. Wilson, "On the Minimum Distance of Cyclic Codes," *IEEE Trans. Info. Theory*, vol. 32, no. 1, pp. 23 - 40, 1986.

[102] C. Roos, "A generalization of the BCH bound for cyclic codes, including the Hartmann–Tzeng bound," *J. Comb. Theory Ser. A*, vol. 33, no. 2, pp. 229 – 232, 1982.

[103] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Info. Theory*, vol. 29, no. 3, pp. 330 – 332, 1983.

[104] Garcia-Frias, J. and Kejing Liu, "Design of near-optimum quantum error-correcting codes based on generator and parity-check matrices of LDGM codes", *42nd Annual Conference on Information Sciences and Systems,* pp. 562 - 567, 2008.

[105] Kejing Liu and Garcia-Frias, J., "Optimization of LDGM-based quantum codes using Density Evolution", *48th Annual Allerton Conference on Communication, Control, and Computing (Allerton),* pp 881 - 886, 2010.

[106] Forney, G.D. and Guha, S., "Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes", *Proceedings. International Symposium on Information Theory, 2005,* pp 1028 - 1032, 2005.

[107] Grassl, M. and Rotteler, M., "Quantum block and convolutional codes from self-orthogonal product codes", *Proceedings. International Symposium on Information Theory, 2005,* pp 1018 - 1022, 2005.

[108] M. Grassl, and M. Rotteler, "On optimal quantum codes," *Int. Journal. of Quant. Info.*, vol. 2, No. 1, pp. 55 - 64, 2004.

[109] Aly, S.A. and Grassl, M. and Klappenecker, A. and Rotteler, M. and Sarvepalli, P.K., "Quantum Convolutional BCH Codes", *CWIT '07. 10th Canadian Workshop on Information Theory, 2007,* pp 180 - 183, 2007.

[110] P. Sarvepalli and A. Klappenecker, "Degenerate quantum codes and the quantum Hamming bound", *Phys. Rev. A*, vol. 81, pp. 032318, 2010.

[111] M. Wilde and S. Guha, "Polar codes for degradable quantum channels", *IEEE Trans. Info. Theory*, vol. 59, no. 7, pp. 4718 - 4729, 2013.

[112] M. Wilde and Joseph M. Renes, "Quantum polar codes for arbitrary channels", *http://arxiv.org/abs/1201.2906v2*, 2012.

[113] J. M. Renes, Frederic Dupuis and Renato Renner, "Efficient polar coding of quantum information", *Phys. Rev. Lett.*, vol. 109, p. 050504, 2012.

[114] J. Renes and M. Wilde, "Polar codes for private and quantum communication over arbitrary channels," *IEEE Trans. Info. Theory*, vol. 60, no. 6, pp. 3090 - 3103, 2014.

[115] Peiyu Tan and Jing Li, "Efficient Quantum Stabilizer Codes: LDPC and LDPC-Convolutional Constructions", *IEEE Transactions on Information Theory,*, Vol. 56, pp 476 - 491, 2010.

[116] P. W. Shor, "Quantum error-correction", *Phys. Rev. A*, Vol. 52, 1995.

[117] T. Hurley, "Group rings and rings of matrices", *Inter. J. Pure Appl. Math.*, 31, no. 3, pp 319 - 335, 2006.

[118] C. Milies, S. Sehgal, "An introduction to Group Rings", *Klumer*, 2002.

[119] R. G. Gallager, "Low-density parity-check codes," *PhD*, MIT, 1963.

[120] V. Zyablov and M. Pinsker, "Estimation of the error-correction complexity of Gallager low-density codes" Prob. Pered. Inform., vol. 11, pp. 23-26, 1975.

[121] G. A. Margulis, "Explicit construction of graphs without short cycles and low density codes" Combinatorica, vol. 2, no. 1, pp. 71-78, 1982.

[122] R. Tanner, "A recursive approach to low complexity codes," IEEE Trans. Inform. Theory, vol. IT-27, pp. 533-547, 1981.

[123] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes" Electron. Lett., vol. 32, pp. 1645-1646, 1996.

[124] N. Wiberg, "Codes and decoding on general graphs," Dissertation no.440, Dept. Elect. Eng. Linkoping Univ., Linkoping, Sweden, 1996.

[125] D. MacKay, C. Hesketh, "Performance of Low Density Parity Check Codes as a Function of Actual and Assumed Noise Levels", *Electronic Notes in Theoretical Computer Science*, vol. 74, 2003.

[126] L. Qi, G. Chen, C. Huijuan, T. Kun, "Channel Mismatch Effect on Performance of Low Density Parity Check Codes," IMACS Multiconference on Computational Engineering in Systems Applications, Beijing, 2006.

[127] D. Declercq and M. Fossorier, "Decoding algorithms for nonbinary LDPC codes over $GF(q)$", *IEEE Trans. Comm.*, vol. 55, no. 4, pp. 633 – 643, 2007.

[128] D. Poulin, J. P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, pp. 2776-2798, 2009.

[129] D. Poulin, J. P. Tillich, and H. Ollivier, "Quantum serial turbo-codes," *IEEE Proc. Int. Sym. Info. Theory*, pp. 310 - 314, 2008.

[130] J. K. Wolf, "On codes derivable from the tensor product of check matrices," *IEEE Trans. Info. Theory*, vol. 11, no. 2, pp. 281 - 284, 1965.

[131] D. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Info. Theory*, vol. 45, pp. 399-431, 1999.

[132] Kraus, K., "States, Effects and Operations: Fundamental Notions of Quantum Theory", *Lecture Notes in Physics*, vol. 190, Springer-Verlag, Heidelberg, Germany, 1983.

[133] A. Fujiwara, "Quantum channel identification problem," *Phys. Rev. A*, vol. 63, 042304, 2001.

[134] M. Sasaki, M. Ban, and S. M. Barnett, "Optimal parameter estimation of a depolarizing channel," *Phys. Rev. A*, vol. 66, 022308, 2002.

[135] A. Fujiwara and H. Imai, "Quantum parameter estimation of a generalized Pauli channel," *Journal of Physics A: Mathematical and General*, vol. 36, no. 29, pp. 8093–8103, 2003.

[136] M. R. Frey, A. L. Miller, L. K. Mentch, and J. Graham, "Score operators of a qubit with applications," *Quantum Information Processing*, vol. 9, pp. 629-641, 2010.

[137] M. R. Frey, D. Collins, and K. Gerlach, "Probing the qudit depolarizing channel," *Journal of Physics A: Mathematical and Theoretical*, vol. 44, no. 20, 205306, 2011.

[138] S. J. Devitt, W. J. Munro and K. Nemoto, "Quantum Error Correction for Beginners," *arXiv:0905.2794*

[139] R. C. Bose and J. G. Caldwell, "Synchronizable error-correcting codes," *Inf. Contr.*, vol. 10, pp. 616–630, 1967.

[140] Y. Fujiwara, "Block Synchronization for Quantum Information", *Phys. Rev. A*, vol. 87, 022344, 2013.

[141] Y. Fujiwara, V. D. Tonchev, and T. W. H. Wong, "Algebraic techniques in designing quantum synchronizable codes", *Phy. Rev. A*, vol. 88, 012318, 2013.

[142] Y. Fujiwara and P. Vandendriessche, "Quantum Synchronizable Codes From Finite Geometries", arXiv:1311.3416.

[143] M. Grassl and T. Beth, "Cyclic quantum error-correcting codes and quantum shift registers," *Proc. R. Soc. London Ser. A* vol. 456, 2689–2706 2000.

[144] W. C. Huffman and V. Pless, "Fundamentals of Error-Correcting Codes", *Cambridge Uni. Press*, Cambridge, 2003.

[145] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Inf. Control*, vol. 20, no. 5, pp. 489 – 498, 1972.

[146] A. Hocquenghem, "Codes correcteurs d'Erreurs," *Chiffres (Paris)*, vol. 2, pp. 147 – 156, 1959.

[147] R. C. Bose and D. K. R. Chaudhuri, "On a class of error correcting binary group codes," *Inf. Control*, vol. 3, no. 1, pp. 68 - 79, 1960.

[148] A. Zeh, A. W-Zeh and S. V. Bezzateev, "Decoding Cyclic Codes up to a New Bound on the Minimum Distance", *IEEE Trans. Info. Theory*, vol. 58, No. 6, 2012.

[149] Y. Xie, J. Li, R. Malaney and J. Yuan, "Channel identification and its impact on quantum LDPC code performance," *IEEE Procs. on Aus. Comm. Theory Workshop (AusCTW)*, pp. 140 - 144, 2012.

[150] D. Poulin and Y. Chung, "On the iterative decoding of sparse quantum codes", *Quantum Information Computation*, vol. 8, pp. 987 – 1000, 2008.

[151] Y.-J. Wang, B. C. Sanders, B.-M. Bai and X.-M. Wang, "Enchanced feedback iterative decoding of sparse quantum codes", *IEEE Trans. on Info. Theory*, vol. 58, no. 5, pp. 1231 – 1241, 2012.

[152] C.-Y. Lu, W.-B. Gao, J. Zhang, X.-Q. Zhou, T. Yang, J.-W. Pan, "Experimental quantum coding against qubit loss error", *Proc. Natl. Acad. Sci. USA*, 105, 11050, 2008.

[153] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, "Benchmarking Quantum Computers: The Five-Qubit Error Correcting Code", *Phys. Rev. Lett.* vol. 86, pp. 5811, 2001.

[154] J.-P. Tillich and G. Zemor, "Quantum LDPC codes with positive rate and minmum distance propositional to the square root bound", *IEEE Trans. on Info. Theory*, vol. 60, no. 2, pp. 1193 – 1202, 2014.

[155] A. Leverrier, J.-P. Tillich and G. zemor, "Quantum expander codes", *in Proc. IEEE Annual Symp. on Foundations of Comp. Sci.*, 2015.

[156] A. A. Kovalev and L. P. Pryadko, "Quantum Kronecker sum-product low-density parity-check codes with finite rate", *Phys. Rev. A*, vol. 88, pp. 012311, 2013.

[157] S. Bravyi and M. B. Hastings, "Homological product codes", *http://arxiv.org/pdf/1311.0885v1.pdf*, 2013.