UNIVERSITY OF SOUTHAMPTON
FACULTY OF ENGINEERING AND PHYSICAL SCIENCES
SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE

Quantum Topological Error Correction Codes for Quantum Computation and Communication

by

Daryus Chandra
BEng, MEng

A doctoral thesis submitted in partial fulfillment of the
requirements for the award of Doctor of Philosophy
at the University of Southampton

September 2019

SUPERVISORS:
Prof. Lajos Hanzo
FREng, FIEEE, FIET, DSc
Chair of Next Generation Wireless Research Group
and
Dr. Soon Xin Ng
PhD, BEng, CEng, FIET, SMIEEE, FHEA
Associate Professor

School of Electronics and Computer Science
Faculty of Engineering and Physical Sciences
University of Southampton
United Kingdom

Dedicated to my parents, Arman Chandra and Sriyati,
and to my brother, Darwis Chandra.
To all first-generation university students around the world:
“Yes, we can!”

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES
SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE

Doctor of Philosophy

Quantum Topological Error Correction Codes for Quantum Computation and Communication

by Daryus Chandra

The employment of quantum error correction codes (QECCs) within quantum computers potentially offers a reliability improvement for both quantum computation and communications tasks. However, the laws of quantum mechanics prevent us from directly invoking the mature family of classical error correction codes in the quantum domain. In order to circumvent the associated problems, the notion of quantum stabilizer codes (QSCs) was proposed in conjunction with syndrome-based decoding in the quantum regime. However, most of the powerful QSC schemes require long codewords for achieving a high performance, which potentially imposes additional challenges for implementation concerning their implementation, since their decoding may require longer than the quantum circuit's coherence time. Hence at the time of writing, QSCs exhibiting short to moderate codeword lengths are preferable. We commence by describing the pivotal problem encountered by classical error-correction codes, which also emerges when designing the QSCs, namely the intrinsic trade-off between the minimum distance versus coding rate. The complete formulation of this particular trade-off does not exist, but several lower and upper bounds can be found in the literature. It has been shown that a substantial gap can be observed between the upper and lower bound of the minimum distance, given the codeword length and the quantum coding rate. Hence, we propose an appealingly simple and invertible analytical approximation, for characterizing the trade-off between the quantum coding rate and the minimum distance of QSCs as well as their corresponding quantum bit error rate (QBER) performance upper-bound. For example, for a half-rate QSC having a codeword length of $n = 128$, the minimum distance is bounded by $11 < d < 22$, while our approximation yields a minimum distance of $d = 17$ for the above-mentioned code.

Next, we link this parametric study of the minimum distance versus quantum coding rate to the popular QSCs, namely to the family of quantum topological error correction codes (QTECCs). In order to construct the classical-to-quantum isomorphism, we conceive and investigate the family of classical topological error correction codes (TECCs), assuming that the bits of a codeword can be arranged in a lattice structure. We then present the classical-to-quantum isomorphism to pave the way for constructing their dual pairs in the quantum domain, which are the QTECCs. Finally, we characterize the performance of QTECCs in the face of the quantum depolarizing channel in terms of both their QBER and fidelity. Specifically, we demonstrate that for quantum coding rate $r_Q \approx 0$, the threshold probability of the QBER below which the colour, rotated-surface, surface, and toric codes

become capable of improving the uncoded QBER are given by 1.8×10^{-2}, 1.3×10^{-2}, 6.3×10^{-2} and 6.8×10^{-2}, respectively. Furthermore, we also demonstrate that we can achieve beneficial fidelity improvements above the minimum fidelity of 0.94, 0.97 and 0.99 by employing the $r_Q = 1/7$ colour code, the $r_Q = 1/9$ rotated-surface code, and the $r_Q = 1/13$ surface code, respectively.

However, QSCs require additional quantum gates for their employment. Incorporating more quantum gates for performing error correction potentially introduces further sources of quantum decoherence into quantum computers. In this scenario, the primary challenge is to find the sufficient condition required by each of the quantum gates for beneficially employing QECCs in order to yield reliability improvements, given that the quantum gates utilized by the QECCs also introduce quantum decoherence. In this treatise, we approach this problem by firstly presenting the general framework of protecting quantum gates by the amalgamation of the transversal configuration of quantum gates and QSCs, which can be viewed as syndrome-based QECCs. Secondly, we provide examples of the advocated framework by invoking QTECCs for protecting both transversal Hadamard gates and controlled (CNOT) gates. Both our simulation and analytical results explicitly show that by utilizing QTECCs, the fidelity of the quantum gates can be beneficially improved, provided that quantum gates satisfying a certain minimum depolarization fidelity threshold (F_{th}) are available. For instance, for protecting transversal Hadamard gates, the minimum fidelity values required for each of the gates in order to attain fidelity improvements are 99.74%, 99.73%, 99.87%, and 99.86%, when they are protected by colour, rotated-surface, surface, and toric codes, respectively. Unfortunately, these specific F_{th} values can only be obtained for a very large number of physical qubits ($n \to \infty$), when the quantum coding rate of the QTECCs approaches zero ($r_Q \to 0$).

Finally, in order to conceive QSCs exhibiting a high quantum coding rate, we modify the construction of QTECCs for conceiving a low-complexity concatenated quantum turbo code (QTC). The above-mentioned high quantum coding rate is obtained by combining the quantum-domain version of short-block codes (SBCs) also known as single parity-check (SPC) codes as the outer codes and quantum unity-rate codes (QURCs) as the inner codes. Despite its design simplicity, the proposed QTC yields a near-hashing-bound error correction performance. For instance, compared to the best half-rate QTC known in the literature, namely the quantum irregular convolutional codes (QIrCCs) combined with the QURC scheme, which operates at the distance of $D = 0.037$ from the quantum hashing bound, our novel QSBC-QURC scheme can operate at the lower distance of $D = 0.029$. It is also worth mentioning that this is the first instantiation of QTCs capable of adjusting the quantum encoders according to the quantum coding rate required for mitigating the Pauli errors imposed by the time-variant depolarizing probabilities of the quantum channel.

Declaration of Authorship

I, **Daryus Chandra**, declare that the thesis entitled **Quantum Topological Error Correction Codes for Quantum Computation and Communication** and the work presented in it are my own and has been generated by me as the result of my own original research. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University;
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
- Where I have consulted the published work of others, this is always clearly attributed;
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- I have acknowledged all main sources of help;
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
- Parts of this work have been published as: [1, 2, 3, 4].

Signed: .... Date: ....

Acknowledgements

First of all, I would like to wholeheartedly thank my supervisors Professor Lajos Hanzo and Dr Soon Xin Ng (Michael) for their guidance, patience, stimulation, and assistance during this journey. Their wisdom and their aspiration help me grow both as a researcher and more importantly as a person. Additionally, I wish to thank Dr Zunaira Babar, Dr Hung Viet Nguyen, Dr Panagiotis Botsinis, Dr Dimitrios Alanis, Dr Mohd Azri Mohd Izhar, Dr Laszlo Gyongyosi, Mrs Rosie Cane, Mr Yifeng Xiong, Mr Dong Pan, for their assistance in the development of my work and also for the fruitful discussions. I would also like to thank the faculty members of the Next Generation Wireless Research Group, namely Prof. Robert G. Maunder, Prof. Lie Liang Yang, Prof. Sheng Chen, Dr Mohammed El-Hajjar, Dr Rong Zhang. I also extend my gratitude to the rest of the members of the group for their support and inspiration. I acknowledge the use of the IRIDIS High-Performance Computing Facility and the associated support services at the University of Southampton in the completion of this work. Finally, I wish to thank my parents, Arman Chandra and Sriyati, as well as my brother, Darwis Chandra, for all their blessings and their relentless support. Ultimately, I am indebted to Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan) for providing financial support, which makes my unforgettable journey at the University of Southampton becomes possible.

List of Publications

Lead-Author Publications:

1. **D. Chandra**, Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Quantum Coding Bounds and a Closed-Form Approximation of the Minimum Distance Versus Quantum Coding Rate," *IEEE Access*, vol. 5, pp. 11557–11581, 2017.
   DOI: 10.1109/ACCESS.2017.2716367.

2. **D. Chandra**, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum Topological Error Correction Codes: The Classical-to-Quantum Isomorphism Perspective," *IEEE Access*, vol. 6, pp. 13729–13757, 2018.
   DOI: 10.1109/ACCESS.2017.2784417.

3. **D. Chandra**, Z. Babar, S. X. Ng, and L. Hanzo, "Near-Hashing-Bound Multiple-Rate Quantum Turbo Short-Block Codes," *IEEE Access*, vol. 7, pp. 52712–52730, 2019.
   DOI: 10.1109/ACCESS.2019.2911515.

4. **D. Chandra**, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum Topological Error Correction Codes Improve The Performance of Transversal Clifford Gates," *IEEE Access*, vol. 7, pp. 121501–121529, 2019.
   DOI:10.1109/ACCESS.2019.2936795.

Co-Author Publications:

5. Z. Babar, Z. B. K. Egilmez, L. Xiang, **D. Chandra**, R. G. Maunder, S. X. Ng, and L. Hanzo, "Polar Codes and Their Quantum-Domain Counterparts," *IEEE Communications Surveys & Tutorials*, 2019. Accepted.
   DOI: 10.1109/COMST.2019.2937923.

6. P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, **D. Chandra**, S. X. Ng, and L. Hanzo,, "Quantum Algorithms for Wireless Communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.
   DOI: 10.1109/COMST.2018.2882385.

7. Z. Babar, **D. Chandra**, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, “Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 970–1010, 2019.
   DOI: 10.1109/ACCESS.2016.2581978.

8. D. Alanis, P. Botsinis, Z. Babar, H. V. Nguyen, **D. Chandra**, S. X. Ng, and L. Hanzo, “Quantum-Aided Multi-Objective Routing Optimization Using Back-Tracing-Aided Dynamic Programming,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7856–7860, 2018.
   DOI: 10.1109/TCOMM.2018.2803068.

9. M. A. M. Izhar, Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, **D. Chandra**, S. X. Ng, and L. Hanzo, “Quantum Turbo Decoding for Quantum Channels Exhibiting Memory,” *IEEE Access,IEEE Access*, vol. 6, pp. 12369–12381, 2018.
   DOI: 10.1109/ACCESS.2018.2808373.

10. D. Alanis, P. Botsinis, Z. Babar, H. V. Nguyen, **D. Chandra**, S. X. Ng, and L. Hanzo, “A Quantum-Search-Aided Dynamic Programming Framework for Pareto Optimal Routing in Wireless Multihop Networks,” *IEEE Transactions on Communications*, vol. 66, no. 8, pp. 3485–3500, 2018.
    DOI: 10.1109/TCOMM.2018.2803068.

11. P. Botsinis, D. Alanis, S. Feng, Z. Babar, H. V. Nguyen, **D. Chandra**, S. X. Ng, R. Zhang, and L. Hanzo, “Quantum-Assisted Indoor Localization for Uplink mm-Wave and Downlink Visible Light Communication Systems,” *IEEE Access*, vol. 5, pp. 23327–23351, 2017.
    DOI: 10.1109/ACCESS.2017.2733557.

12. H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, **D. Chandra**, M. A. M. Izhar, S. X. Ng, and L. Hanzo, “Towards the Quantum Internet: Generalised Quantum Network Coding for Large-scale Quantum Communication Networks,” *IEEE Access*, vol. 5, pp. 17288–17308, 2017.
    DOI: 10.1109/ACCESS.2017.27387810.

13. H. V. Nguyen, P. Trinh, A. Pham, Z. Babar, D. Alanis, P. Botsinis, **D. Chandra**, S. X. Ng, and L. Hanzo, “Network Coding Aided Cooperative Quantum Key Distribution Over Free-Space Optical Channels,” *IEEE Access*, vol. 5, pp. 12301–12317, 2017.
    DOI: 10.1109/ACCESS.2017.2712288.

14. Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, **D. Chandra**, S. X. Ng, and L. Hanzo, “Serially Concatenated Unity-Rate Codes Improve Quantum Codes Without Coding-Rate Reduction,” *IEEE Communications Letters*, vol. 20, no. 10, pp. 1916–1919, 2016.
    DOI: 10.1109/LCOMM.2016.2593874.

15. H. V. Nguyen, Z. Babar, P. Botsinis, D. Alanis, **D. Chandra**, S. X. Ng, and L. Hanzo, “EXIT-Chart Aided Quantum Code Design Improves the Normalised Throughput of

Realistic Quantum Devices," *IEEE Access*, vol. 4, pp. 10194–10209, 2016.
DOI: 10.1109/ACCESS.2016.2591910.

16. P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, **D. Chandra**, S. X. Ng, and L. Hanzo, "Quantum-Aided Multi-User Transmission in Non-Orthogonal Multiple Access Systems," *IEEE Access*, vol. 4, pp. 7402–7424, 2016.
DOI: 10.1109/ACCESS.2016.2591904.

17. P. Botsinis, Z. Babar, D. Alanis, **D. Chandra**, H. V. Nguyen, S. X. Ng, and L. Hanzo,, "Quantum Error Correction Protects Quantum Search Algorithms Against Decoherence," *Scientific Reports* , vol. 6, 2016.
DOI:10.1038/srep38095.

18. Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, **D. Chandra**, S. X. Ng, R. G. Maunder, and L. Hanzo, "Fully-Parallel Quantum Turbo Decoder," *IEEE Access*, vol. 4, pp. 6073–6085, 2016.
DOI: 10.1109/ACCESS.2016.2581978.

Contents

List of Symbols

c	Number of preshared maximally-entangled qubit pairs
$\mathcal{C}_Q$	Quantum hashing bound for quantum coding rate given quantum depolarizing probability p
d	Minimum distance of a code
D	Distance from quantum hashing bound
d_{ea}	Minimum distance of an entanglement-assisted quantum code
δ	Normalized minimum distance
E	Entanglement consumption rate
G_i	The i-th stabilizer generator
$\mathcal{G}$	Stabilizer generator group
$\mathbf{H}$	Parity-check matrix of a code; Hadamard matrix
$H(x)$	Binary entropy of x
$\mathbf{I}$	Identity matrix
k	Length of information word; Number of logical qubits
n	Length of codeword; Number of physical qubits
p	Quantum depolarizing probability
$p_{\mathbf{I}}$	Probability of error-free qubit
$p_{\mathbf{X}}$	Probability of bit-flip errors
$p_{\mathbf{Z}}$	Probability of phase-flip errors
$p_{\mathbf{Y}}$	Probability of simultaneous bit-flip and phase-flip errors

p^*	Quantum hashing bound for quantum depolarizing probability given quantum coding rate r_Q
$\mathcal{P}_n$	n-tuple Pauli group
r	Classical coding rate
r_Q	Quantum coding rate
$\mathcal{R}$	Error recovery operator
$\widehat{\mathcal{R}}$	Effective error recovery operator
$\mathbf{s}$	Syndrome vector
S_i	The i-th stabilizer operator
$\widehat{S}_i$	The i-th effective stabilizer operator
$\mathcal{S}$	Stabilizer group
$\widehat{\mathcal{S}}$	Effective stabilizer group
t	Error correction capability of a code
θ	Entanglement ratio
U_f	Unitary transformation
$\mathcal{V}$	Quantum encoder
$\mathcal{V}^\dagger$	Quantum inverse encoder
$\widehat{\mathcal{V}}^\dagger$	Effective quantum inverse encoder
$\mathcal{C}(n,k,d)$	A classical error correction code having the parameters n, k, and d
$\mathcal{C}[n,k,d]$	A quantum error correction code having the parameters n, k, and d
$\|\psi\rangle$	Quantum state of qubits
$\otimes$	Tensor product

List of Acronyms

BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
CNOT	Controlled-NOT
CSS	Calderbank-Shor-Steane
DFS	Decoherence-Free Subspace
EA	Entanglement-Assisted
EXIT	EXtrinsic Information Transfer
GV	Gilbert-Varshamov
LDPC	Low-Density Parity-Check
LUT	Look-Up Table
MDS	Maximum Separable Distance
MRRW	McEliece-Rodemich-Rumsey-Welch
PCM	Parity-Check Matrix
QBCH	Quantum Bose-Chaudhuri-Hocquenghem
QBER	QuBit Error Ratio
QCC	Quantum Convolutional Code
QECC	Quantum Error Correction Code
QEDC	Quantum Error Detection Code
QIrCC	Quantum Irregular Convolutional Code
QLDPC	Quantum Low-Density Parity-Check
QPC	Quantum Polar Code

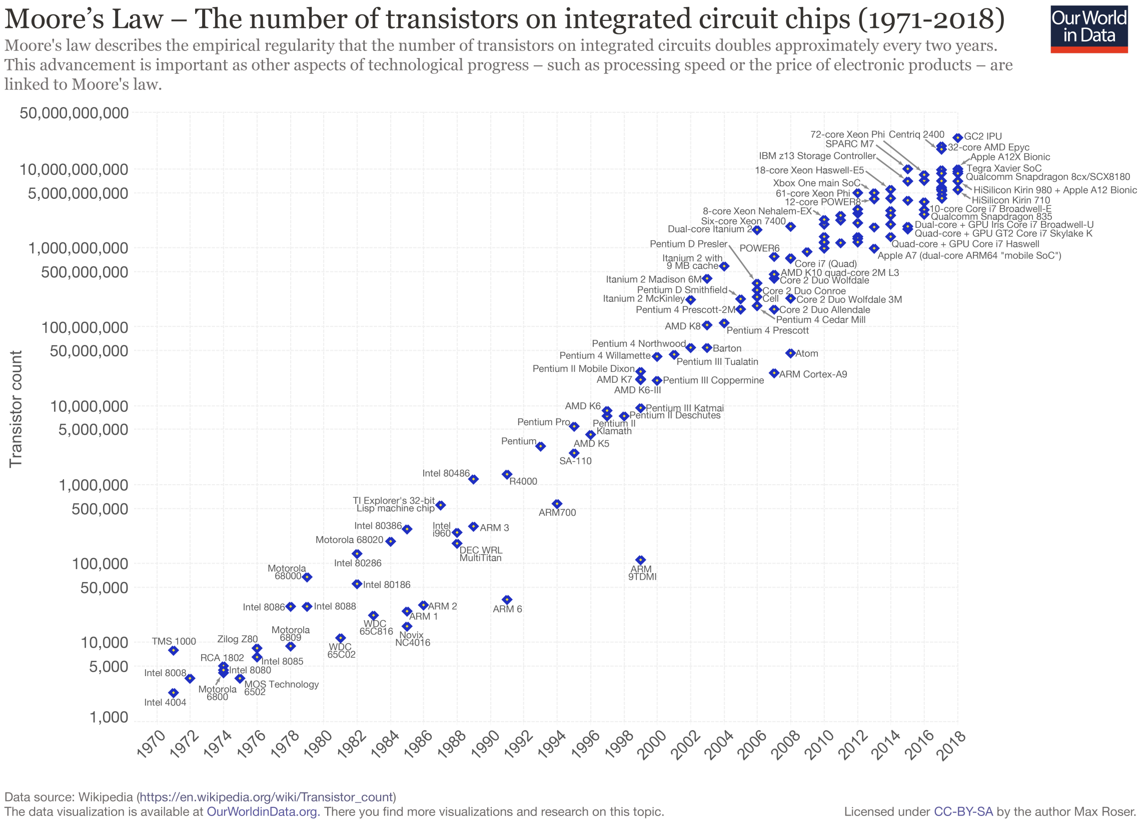
QRM	Quantum Reed-Muller
QRS	Quantum Reed-Solomon
QSBC	Quantum Short-Block Code
QSC	Quantum Stabilizer Code
QTC	Quantum Turbo Code
QTECC	Quantum Topological Error Correction Code
QURC	Quantum Unity-Rate Code
RS	Reed-Solomon
SBC	Short-Block Code
SPC	Single Parity-Check
TECC	Topological Error Correction Code

Chapter 1

Introduction

1.1 Motivation

In 1935, Erwin Schrödinger, an Austrian physicist, proposed a thought experiment to illustrate the interpretation of uncertainty in quantum mechanics. This thought experiment later acquired the fond connotation of the "Schrödinger's Cat" experiment [5, 6]. In this treatise, we will refer to another thought experiment, namely the "Black Box Experiment". Let us assume that we have a black box with a coin spinning in it. It does not need to be a fair coin. Inside the box, we then start spinning the coin. We do not have any prior knowledge about the coin, namely whether the coin is fair or biased and we do not know whether it landed on the face or the tail side when it finally stopped spinning. At this moment, we may say that the coin inside the box is within two states simultaneously and has a certain probability for each state. Let us continue the experiment by using several boxes. We may proceed by using two, three, or even an arbitrarily number of $n \in \mathbb{N}$ boxes for this experiment. Similarly, we spin all the n coins simultaneously and close the boxes before they collapse. Instantly, we will secure 2^n states from those coins concurrently, by using n coins and a single step of parallel spinning. This particular step of this simple thought experiment highlights the fact that we can increase the computational power exponentially if we can exploit the nature of uncertainty exhibited by quantum mechanics. Let us now continue the experiment to the following step. Up to this moment, all of the boxes are completely sealed and we have secured the 2^n states of the coins simultaneously. Now, we decide to open all of the boxes at once and observe all the coins. After observing the state of each coin in each box, we now in the position of observing a single specific state from all the 2^n possible states. This illustrates that the notion of quantum states suddenly collapse into a deterministic classical state due to the "observation", which is also often-termed in the parlance as "measurement". This property is exploited by quantum computers, which will create a very powerful computation tool that may jeopardize the secure classical communication channel, which up to this date only depends on the computational complexity associated with the underlying encryption algorithm. While classical cryptography is at risk of being deciphered by powerful quantum computers exploiting the quantum-parallelism, quantum-based communication offers an absolutely secure communication channel, since the act of any observation or measurement carried out by an eavesdropper will perturb the quantum states and informs the legitimate parties.



Moore's Law – The number of transistors on integrated circuit chips (1971-2018)

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are linked to Moore's law.

Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Licensed under CC-BY-SA by the author Max Roser.

Figure 1.1: The number of transistors on an integrated circuit is doubled every two years since 1971, as predicted by Gordon E. Moore in 1985 [7].

In 1965, Gordon E. Moore released the general rule of thumb projecting the number of transistors on a single integrated circuit chip based on his experiences in the semiconductor industry. This notable rule of thumb was later termed as "Moore's Law", which dictates that the number of the transistors on an integrated circuit chip will be doubled every two years [8]. This law has maintained its validity over the past few decades, as illustrated in Fig. 1.1, but unfortunately it is predicted that it will no longer remain valid beyond the early of the 2020s [9]. As we shrink further the transistor's size, we encounter new physical phenomena as we enter the nano-world, which can only be described using the postulates of quantum mechanics [10]. We encounter both pros and cons as we embark on this journey into the unknown. Firstly, the ability to create simultaneous states at any instant lends itself to high-power parallel computing by exploiting the quantum-domain superposition. Secondly, the collapse of quantum superposition into a classical state upon observation potentially allows us to conceive unbreachable communication schemes.

The field of theoretical quantum computing was established five decades after Schrödinger's Cat experiment by Richard Feynman who suggested how to simulate efficiently quantum physics using the so-called quantum computers [11]. Since then, diverse quantum-domain algorithms were invented and indeed have shown that the laws of quantum mechanics will help us to speed up the computational aspect of some applications [12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28]. In parallel to the quantum computing development, the quantum-based solutions capable of providing absolute security have also been conceived [29, 30, 31, 32, 33, 34, 35, 36, 37, 38].

Despite the above advances, the physical implementation of quantum computers is still far from perfection. Substantial efforts have been invested in building a scalable and reliable quantum computer relying on different solutions. For instance, by using spin electron techniques [39, 40], photonic chips [41, 42, 43], superconducting qubits [44, 45, 46], and recently also by using silicon [47, 48] as well as microwave-controlled trapped-ions [49, 50]. In order to arrive at the best architecture for quantum computers, the physical implementations of quantum computation have to satisfy the so-called "DiVincenzo's Criteria" [51] described below:

(a) **A scalable physical system with well-characterized qubits**. The elementary unit of information in classical computers is represented by *binary digit* or *bit*. Each bit can only hold a value of "0" or "1" at any instant, but not both. Meanwhile, the elementary unit of information in quantum computers is represented by a *quantum bit* or *qubit*. In quantum mechanics, the state of "0" and "1" are commonly represented using the Dirac notation, i.e. $|0\rangle$ for state "0" and $|1\rangle$ for state "1" [52]. Each qubit can hold a value of $|0\rangle$ or $|1\rangle$ or even the superposition of both states. The physical realization of a qubit should reliably distinguish the state $|0\rangle$ and $|1\rangle$ as well as allowing us to be in the superposition of both states. For instance, we can have a two-level quantum system using the two spin (up/down) states of a particle, or the ground and excited states of an atom, or the vertical and horizontal polarization of a single photon.

(b) **The ability to initialize the state of the qubits to a simple fiducial state**. One of the essential requirements in classical computing is to know the initial state of a register before starting the computations. Similar requirements are also applicable in the quantum domain. For instance, to initialize the process of quantum search and quantum factoring algorithms, the quantum registers have to supply a certain number of fresh auxiliary qubits in the state of $|0\rangle$. Similarly, quantum teleportation, quantum superdense coding, and quantum key distribution (QKD) also require the quantum registers to provide a continuous supply of fresh qubits in a certain superposition state.

(c) **Sufficiently long decoherence times, much longer than the gates' operation time**. In quantum computers, the qubits will be involved in a series of quantum-domain operations to carry out a certain quantum computation or quantum communication tasks. Ideally, a quantum computing algorithm and similarly a quantum communication scheme should be designed by ensuring that the computational process or transmission finishes before the qubits decohere. However, a long decoherence time does not necessarily mean that the qubits are far more reliable. We primarily care about the number of operations that can be performed before the qubits decohere. Hence, we should take into account the gate operation time. The maximal number of reliable operations in quantum computers is defined by the ratio of the qubits' decoherence time to the per-gate operation duration. A quantum solution having a higher maximal number of reliable operations may be more preferable because as we scale-up the quantum computers, the number of gate operations will increase.

(d) **A universal set of quantum gates**. The power of quantum computers in speeding up some computations only can be observed if a universal set of quantum gates exists. More specifically, a universal set of quantum gates entails not only the gates that can be simulated by classical probabilistic computers in polynomial time, namely quantum gates that belong to the Clifford group defined in [53], but also those that impose a higher simulation complexity. Hence, in order to develop fully functioning quantum computers achieving a beneficial quantum speed-up, a set of quantum gates outside the Clifford group also have to be realized.

(e) **A qubit-specific measurement capability**. Eventually, the results from a series of quantum operation of certain computational task have to be read out. For this reason, quantum computers need the measurement operators, which have to be reliable and capable of operating in various measurement bases.

Specifically, for quantum communications, there are two additional criteria, as described below:

(a) **The ability to convert stationary qubits to flying qubits and vice versa**. Numerous applications of quantum computers require the transmission of qubits to a different location. Hence, the capability of converting the stationary qubits to flying qubits is essential.

(b) **The capability of reliably transmitting flying qubits between specific locations**. To guarantee that the state of the qubits remains intact after their displacement to a different location, their protection against quantum decoherence is required, since we cannot completely isolate the interaction of the qubits with the surrounding environment, even if high-grade electromagnetic shielding and near-absolute-zero temperature are used.

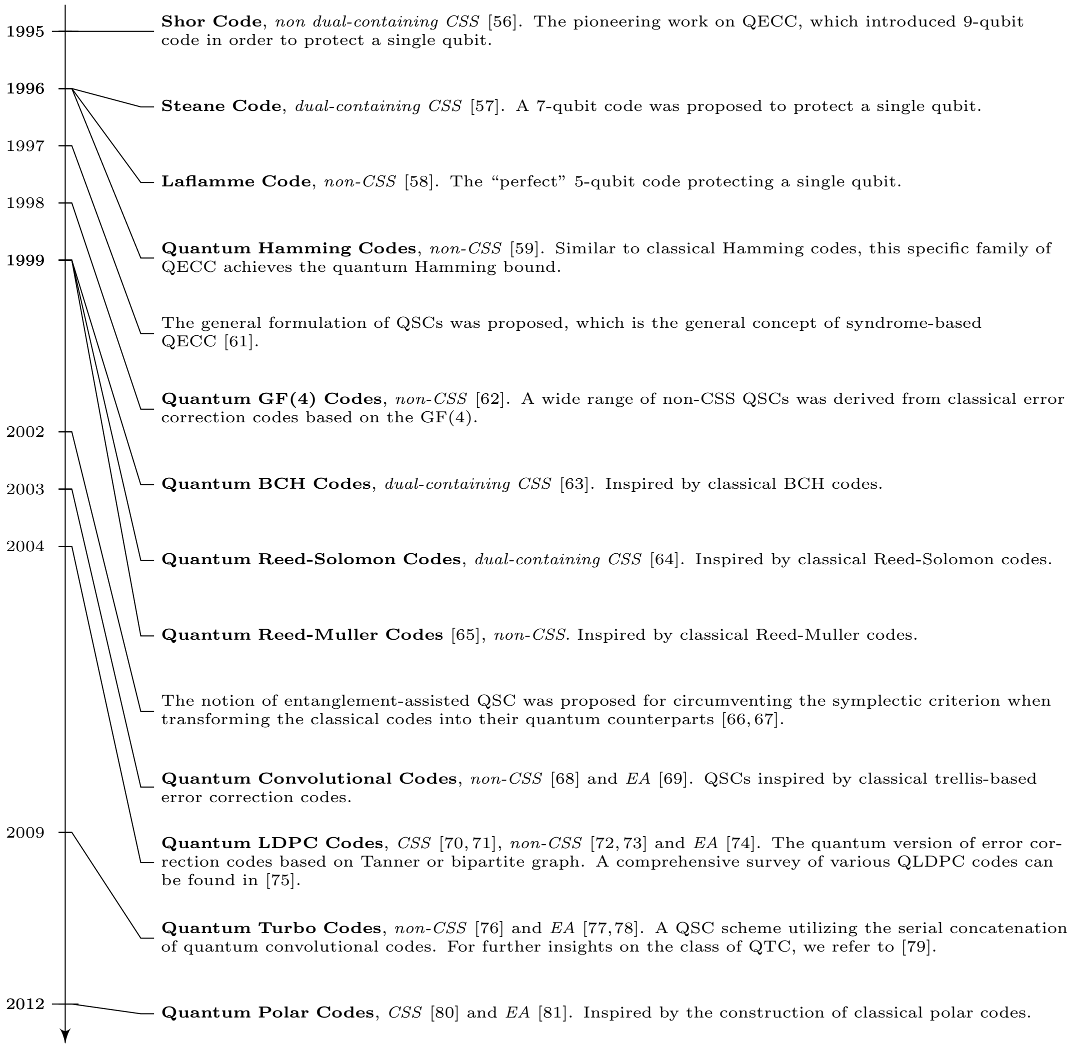
Quantum computers face the same problem as their classical counterparts, namely decoherence. The aforementioned criteria for developing scalable and reliable quantum computers may not be accomplishable if quantum decoherence cannot be mitigated. Therefore, it is a challenge to ensure the reliability of quantum computers in the face of ubiquitous quantum decoherence. Quantum error-correction code (QECC) constitutes one of the most popular techniques for tackling the deleterious effects of quantum decoherence. The employment of QECCs may enable quantum computers to operate in high reliability, in-line with the DiVincenzo's Criteria [54]. Therefore, we conclude that one of the key ingredients of realizing reliable quantum computers is the employment of QECCs inside quantum computers.

1.2 Historical Overview

1.2.1 Quantum Stabilizer Codes

The concept of protecting the quantum information from decoherence is similar to that of its classical counterpart by attaching redundancy to the information [55], which is then invoked later for error-correction. The quest for finding good QECCs was inspired by Shor, who introduced the 9-qubit code, which is judiciously often referred to as Shor's code [56]. Shor's code encodes a single information qubit, which is also referred to as the "logical qubit", into nine encoded qubits or "physical qubits". Shor's 9-qubit code is capable of protecting the nine physical qubits from any type of single-qubit error. Following the discovery of Shor's code, another QECC scheme, namely Steane's code, was proposed in [57]. The latter is capable of protecting the physical qubits from any single-qubit error by encoding a single logical qubit into seven physical qubits, instead of nine qubits. The question concerning the minimum number of physical qubits required to protect them from any type of single-qubit error was answered by Laflamme *et al.*, who proposed the 5-qubit quantum code having a quantum coding rate of 1/5 [58]. This 5-qubit may also be referred to as Laflamme's "perfect code" since the code construction achieves the quantum Hamming bound and the quantum Singleton bound of binary codes, which is the upper bound of the quantum coding rate, given the minimum distance of any QECC construction [59, 60].

The field of QECCs entered its golden age following the invention of quantum stabilizer codes (QSCs) [61, 62]. The QSC paradigm allows us to transform the classical error correction codes into their quantum counterparts. The QSCs also circumvent the problem of estimating both the number and the position of quantum-domain errors imposed by quantum decoherence without observing the actual quantum states, since observing the quantum states would collapse the qubits into classical bits. This extremely beneficial error estimation was achieved by introducing the syndrome-measurement based approach [61, 62]. In classical error correction codes, the syndrome-measurement based approach has been widely exploited as a popular error detection and correction procedure. Therefore, the formulation of QSCs expanded the search space of good QECCs to a broader horizon. This new paradigm of incorporating the classical to quantum isomorphisms, led to the transformation of classical codes to their quantum domain duals, such as quantum Bose-Chaudhuri-Hocquenghem (QBCH) codes [63, 82], quantum Reed-Solomon (QRS) codes [64], quantum Reed-Muller (QRM) codes [65], quantum convolutional codes (QCCs) [68, 83], quantum low-density parity-check (QLDPC) codes [71], quantum turbo codes (QTCs) [76], and quantum polar codes (QPCs) [80]. A timeline that portrays the milestones of QSCs, at a glance is depicted in Fig. 1.2. Although the QSC formulation creates an important class of QECCs, we note that there are also other classes of QECCs beside the QSCs, such as the class of decoherence-free subspace (DFS) codes [84, 85, 86]. DFS codes can be viewed as passive QECCs, while the QSCs are a specific example of the active ones. To elaborate a little further, DFS codes constitute a highly degenerate class of QECCs, which rely on the fact that the error patterns may preserve the state of physical qubits and therefore they do not necessarily require a recovery procedure. Due to



Shor Code, *non dual-containing CSS* [56]. The pioneering work on QECC, which introduced 9-qubit code in order to protect a single qubit.

Steane Code, *dual-containing CSS* [57]. A 7-qubit code was proposed to protect a single qubit.

Laflamme Code, *non-CSS* [58]. The "perfect" 5-qubit code protecting a single qubit.

Quantum Hamming Codes, *non-CSS* [59]. Similar to classical Hamming codes, this specific family of QECC achieves the quantum Hamming bound.

The general formulation of QSCs was proposed, which is the general concept of syndrome-based QECC [61].

Quantum GF(4) Codes, *non-CSS* [62]. A wide range of non-CSS QSCs was derived from classical error correction codes based on the GF(4).

Quantum BCH Codes, *dual-containing CSS* [63]. Inspired by classical BCH codes.

Quantum Reed-Solomon Codes, *dual-containing CSS* [64]. Inspired by classical Reed-Solomon codes.

Quantum Reed-Muller Codes [65], *non-CSS*. Inspired by classical Reed-Muller codes.

The notion of entanglement-assisted QSC was proposed for circumventing the symplectic criterion when transforming the classical codes into their quantum counterparts [66, 67].

Quantum Convolutional Codes, *non-CSS* [68] and *EA* [69]. QSCs inspired by classical trellis-based error correction codes.

Quantum LDPC Codes, *CSS* [70, 71], *non-CSS* [72, 73] and *EA* [74]. The quantum version of error correction codes based on Tanner or bipartite graph. A comprehensive survey of various QLDPC codes can be found in [75].

Quantum Turbo Codes, *non-CSS* [76] and *EA* [77, 78]. A QSC scheme utilizing the serial concatenation of quantum convolutional codes. For further insights on the class of QTC, we refer to [79].

Quantum Polar Codes, *CSS* [80] and *EA* [81]. Inspired by the construction of classical polar codes.

Figure 1.2: Timeline of important milestones in the QECC field, specifically in the development of QSCs. The code construction is highlighted with **bold** fonts, while the associated code type is printed in *italics*.

their strong reliance on the degeneracy property exhibited by QECCs without a classical counterpart, the class of DFS codes bears no resemblance to any classical error correction codes. Therefore, in this treatise, we focus our discussions purely on QSCs, which exhibit strong analogies with classical error correction codes.

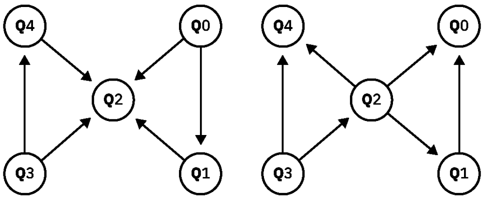
Even though intensive research efforts have been invested in exploring the field of QSCs, one of the mysteries remains unresolved. Since the development of the first QSC, one of the open problems has been how to determine the realistically achievable size of the codebook $|\mathcal{C}| = 2^k$, given the number of physical qubits n, the minimum distance of d, and the quantum coding rate of $r_Q = k/n$, where k denotes the number of logical qubits. The minimum distance d of the legitimate codewords is the parameter that defines the error correction capability of the corresponding code. The complete formulation of the realistically achievable minimum distance d, given the number of physical qubits n and the quantum coding rate r_Q is unknown at the time of writing, but several theoretical lower and upper bounds can be found in the literature [60, 87, 88]. Naturally, finding code constructions associated with growing minimum distances upon reducing the coding rate is desirable, since an increased minimum distance improves the reliability of quantum computation [54, 89, 90, 91, 92]. The trade-off between the quantum coding rate and the minimum distance as well as the codeword length is widely recognized, but the achievable minimum distance d of a quantum code given the quantum coding rate r_Q and codeword length n remains unresolved. For example, for a given codeword length of $n = 128$ and quantum coding rate of $r_Q = 1/2$, the achievable minimum distance is loosely bounded by $11 < d < 22$, while for $n = 1024$ and $r_Q = 1/2$, the achievable minimum distance is bounded by $78 < d < 157$. Naturally, having such a wide range of minimum distance is undesirable. For binary classical codes, this problem has been circumvented by the closed-form approximation proposed by Akhtman *et al* [93].

The challenge of creating the quantum counterpart of error correction codes lies in the fact that QSC constructions have to mitigate not only bit-flip errors but also phase-flip errors or both bit-flip and phase-flip errors. Based on how we mitigate those different types of errors, we can simply categorize QSCs as being in the class of Calderbank-Shor-Steane (CSS) codes [57, 88, 94] or as being non-CSS codes [62]. The CSS codes handle qubit errors by treating bit-flip errors and phase-flip errors as separate entities. By contrast, the class of non-CSS codes treat both bit-flip errors and phase-flip errors simultaneously. Since the CSS codes treat the bit-flip and phase-flip error correction procedures separately, in general, they exhibit a lower coding rate than their non-CSS counterparts having the same error correction capability. Furthermore, if we also consider the presence of quantum entanglement, we may conceive more powerful quantum code constructions as discussed in [66,67]. To elaborate, the family of entanglement-assisted quantum stabilizer codes (EA-QSCs) is capable of operating at a higher quantum coding rate than the unassisted QSC constructions at the same error correction capability, provided that error-free maximally-entangled qubits have already been preshared [66, 67].

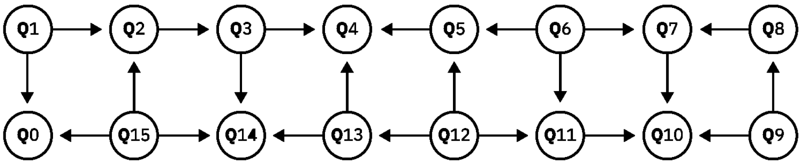
1.2.2 Quantum Topological Error Correction Codes

We have established that one of the essential prerequisites of constructing quantum computers is the employment of QECCs for ensuring that the computers operate reliably by mitigating the deleterious effects of quantum decoherence [51, 54, 95]. However, the laws of quantum mechanics prevent us from transplanting classical error correction codes directly into the quantum domain. To circumvent the constraints imposed by the nature of quantum physics, the notion of quantum stabilizer codes (QSCs) emerged [61, 62, 96]. The invention of QECCs and specifically the QSC formalism did not immediately eradicate all of the obstacles of developing reliable quantum computers. Employing the QSCs requires redundancy in the form of auxiliary quantum bits (qubits) to encode the logical qubits onto physical qubits. The redundant qubits are then utilized to invoke the error correction. Hence, additional components such as the quantum encoder and decoder circuits constructed from quantum gates are required. Therefore, the circuit-based implementation of a QSC itself has to be fault-tolerant to guarantee that the QSC circuit does not introduce additional decoherence into the quantum computers.

The notion of QSC triggered numerous discoveries in the domain of QECCs, which



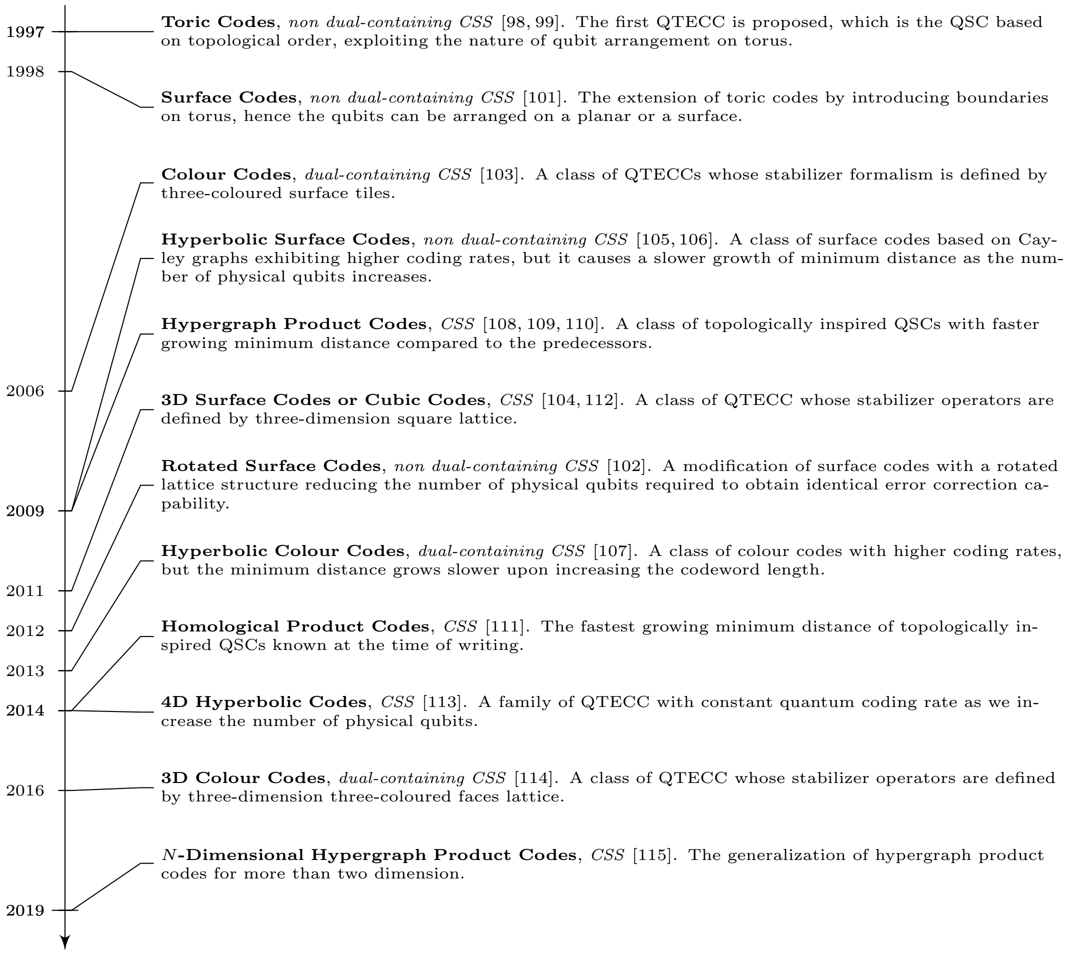
(a) 5 qubits (ibmqx2). (b) 5 qubits (ibmqx4).



(c) 16 qubits (ibmqx5).

Figure 1.3: The qubit arrangement of IBM's superconducting quantum computers. The circles represent the qubits, while the arrows represent the possible qubit interactions within the computers [97].

are inspired by classical error correction codes. Essentially, QSCs represent the quantum-domain version of the classical syndrome decoding-based error correction codes. Since the concept of utilizing the syndrome values for error correction is widely exploited in the classical domain, diverse classical error correction codes can be conveniently 'quantumized'. Consequently, we can find in the literature the quantum version of error correction codes based on algebraic formalisms such as those of the Bose-Chaudhuri-Hocquenghem (BCH) codes [63] and of Reed-Solomon (RS) codes [64], quantum codes based on a conventional trellis structure such as convolutional codes [68] and turbo codes [76, 79], quantum codes based on bipartite graphs, such as low-density parity-check (LDPC) codes [70,71,72,73,75], as well as quantum codes based on channel polarization, such as polar codes [80, 81]. Apart from exploiting the above isomorphism, there are also significant contributions on directly developing code constructions solely based on the pure quantum topology and homology, as exemplified by the family of toric codes [98, 99, 100], surface codes [101, 102], colour codes [103], cubic codes [104], hyperbolic surface codes [105, 106], hyperbolic color codes [107], hypergraph product codes [108,109,110] and homological product codes [111]. Unfortunately, this concept has not been widely explored in the classical domain. By contrast, in the quantum domain, having a code construction relying on the physical configuration of qubits is highly desirable for the conception of low-complexity high-reliability quantum computers. For instance, this strategy has been deployed for developing IBM's superconducting quantum computers, as shown in Fig. 1.3. From this figure, we can see the qubit arrangement of the three prototypes of IBM's quantum computer - which can be viewed online - namely the ibmqx2, ibmqx4, and ibmqx5 configurations [97]. The first two of the quantum computers are the 5-qubit quantum computers, while the last one is a 16-qubit quantum computer. The circles in Fig. 1.3 represent the qubits, while the arrows represent all the possible two-qubit interactions. It can be seen that the existing architectures impose a limitation, namely the two-qubit interactions can be only performed between the neighbouring qubits. Even though this particular limitation potentially imposes additional challenges, when it comes to QSCs deployment, the stabilizer effect can still be achieved by the corresponding qubit arrangement by invoking the QTECCs. A timeline that portrays the milestones of QTECCs, at a glance is portrayed in Fig. 1.4.



Toric Codes, *non dual-containing CSS* [98, 99]. The first QTECC is proposed, which is the QSC based on topological order, exploiting the nature of qubit arrangement on torus.

Surface Codes, *non dual-containing CSS* [101]. The extension of toric codes by introducing boundaries on torus, hence the qubits can be arranged on a planar or a surface.

Colour Codes, *dual-containing CSS* [103]. A class of QTECCs whose stabilizer formalism is defined by three-coloured surface tiles.

Hyperbolic Surface Codes, *non dual-containing CSS* [105, 106]. A class of surface codes based on Cayley graphs exhibiting higher coding rates, but it causes a slower growth of minimum distance as the number of physical qubits increases.

Hypergraph Product Codes, *CSS* [108, 109, 110]. A class of topologically inspired QSCs with faster growing minimum distance compared to the predecessors.

3D Surface Codes or Cubic Codes, *CSS* [104, 112]. A class of QTECC whose stabilizer operators are defined by three-dimension square lattice.

Rotated Surface Codes, *non dual-containing CSS* [102]. A modification of surface codes with a rotated lattice structure reducing the number of physical qubits required to obtain identical error correction capability.

Hyperbolic Colour Codes, *dual-containing CSS* [107]. A class of colour codes with higher coding rates, but the minimum distance grows slower upon increasing the codeword length.

Homological Product Codes, *CSS* [111]. The fastest growing minimum distance of topologically inspired QSCs known at the time of writing.

4D Hyperbolic Codes, *CSS* [113]. A family of QTECC with constant quantum coding rate as we increase the number of physical qubits.

3D Colour Codes, *dual-containing CSS* [114]. A class of QTECC whose stabilizer operators are defined by three-dimension three-coloured faces lattice.

***N*-Dimensional Hypergraph Product Codes**, *CSS* [115]. The generalization of hypergraph product codes for more than two dimension.

Figure 1.4: Timeline of important milestones in the area of QTECCs. The code construction is highlighted with **bold** while the associated code type is marked in *italics*.

Again, the Shor's 9-qubit code protects 9 physical qubits from any type of single-qubit error, namely bit-flip (**X**), phase-flip (**Z**), as well as from simultaneous bit and phase-flip (**Y**). Furthermore, as also alluded to above, not long after the discovery of the first QECCs, Steane invented the 7-qubit code, which was followed by Laflamme's perfect 5-qubit code [57, 58]. However, the construction of these codes does not naturally exhibit inherent fault-tolerance. Concisely, a QSC is said to be fault-tolerant if the circuit-based implementation of the QSC does not introduce more error than the error correction capability of the QSC, given that the quantum gates required for implementing the QSC are imperfect. The quantum circuit based implementation of these pioneering QSCs always involves a high number of qubit interactions within the codeword of physical qubits. As a consequence, an error caused by an imperfect gate potentially propagates to other qubits and instead of being eliminated, the deleterious effects of quantum decoherence are further aggravated.

At the current development of quantum computers, a QSC exhibiting fault-tolerance is more favourable, since the reliability of quantum gates is substantially lower than that of classical logic gates. The employment of QSCs is expected to mitigate the deleterious effect of the imperfect quantum gates. However, the QSC circuit itself is prone to decoherence. For the sake of constructing a fault-tolerant QSC scheme, the notion of quantum topological error correction codes (QTECCs) was proposed [98, 99]. The formulation of QTECCs offers substantial fault-tolerance improvements because they exhibit an increased minimum distance upon increasing the codeword length as well as the localized of stabilizer measurements. Nonetheless, one of the substantial drawbacks of QTECCs is the very low quantum coding rate. More specifically, the quantum coding rate of QTECCs tends to zero for a very long codeword. Another class of codes which are considered to be fault-tolerant QSCs is constituted by the family of QLDPC codes. The QLDPC codes inherit the property of fault-tolerance due to having a sparse parity-check matrix, which guarantees the limited interaction of the qubits in the same block of codewords. Even though QLDPC codes can achieve a good performance at a relatively high quantum coding rate, the construction of QLDPC has a bounded minimum distance [71, 110] and they require a long codeword. Even though intensive research efforts have been invested in exploring the QECC field, the fundamental trade-off between the quantum coding rate and the minimum distance remains unresolved. Having a high minimum distance is important for guaranteeing a low error floor region and the fault-tolerance. However, it is unfeasible to construct a QSC exhibiting high minimum distance without unduly reducing the quantum coding rate or increasing the number of physical qubits. This is only a specific example of the quantum coding rate versus minimum distance trade-off. Furthermore, the quantum coding rate versus minimum distance trade-off is not the only one involved in designing the QSCs, as seen in Fig. 1.5.

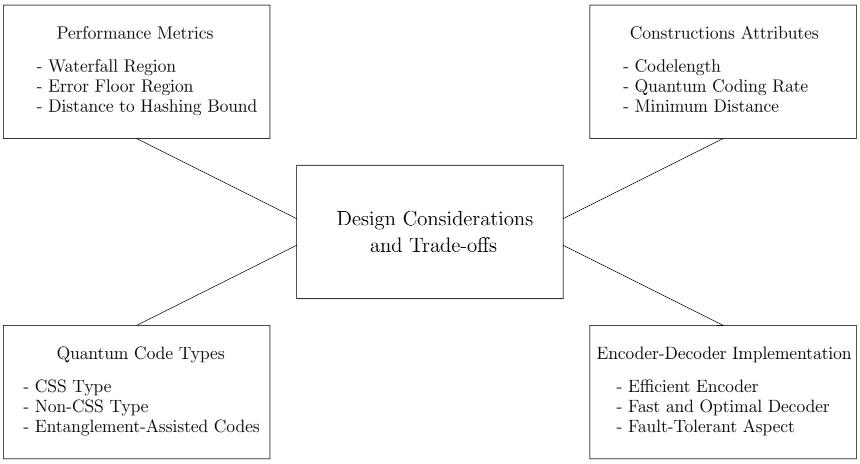


Figure 1.5: The conflicting design factors related to QECC code design.

1.2.3 Protecting Quantum Gates

Although the field of QECCs benefitted from a rapid pace of development, because under certain conditions we can transform various classes of powerful classical error correction codes into their quantum counterparts, several challenges remain, hindering the immediate employment of these powerful QSCs in quantum computers. Firstly, the reliability of the state-of-the-art quantum gates is still significantly lower compared to classical gates. For example, the reliability of a two-qubit quantum gate is between 90.00% – 99.90% across the various technology platforms, such as spin electronics, photonics, superconducting, trapped-ion, and silicon solutions [39, 40, 41, 42, 44, 46, 47, 48, 116]. Similar to the classical domain, invoking an error correction code within a quantum computer requires additional components. However, adding components for error correction also implies that we unavoidably introduce an additional source of decoherence into the quantum computers, since the encoder and decoder of QSCs are also composed of quantum gates. Secondly, the powerful QSCs such as QTCs, QPCs, and QLDPC codes require long codewords in order to operate close to the quantum Hashing bound. In other words, they require a very high number of physical quantum bits (qubits) to correct numerous errors. Additionally, the qubits have a relatively short coherence time [117], and hence, the error correction procedure has to be completed before the ensemble of the qubits starts decohering. Consequently, utilizing QSCs having a high number of qubits for correcting many errors has the potential threat of encountering an avalanche of more erroneous qubits before the error correction procedure is even completed. Thirdly, the state-of-the-art architecture of quantum computers imposes an additional challenge, where the interactions among the qubits are ideally limited to the nearest neighbour qubits, which can be arranged by introducing a lattice-based topological architecture. The aforementioned challenges impose limitations on creating a fault-tolerant error correction architecture.

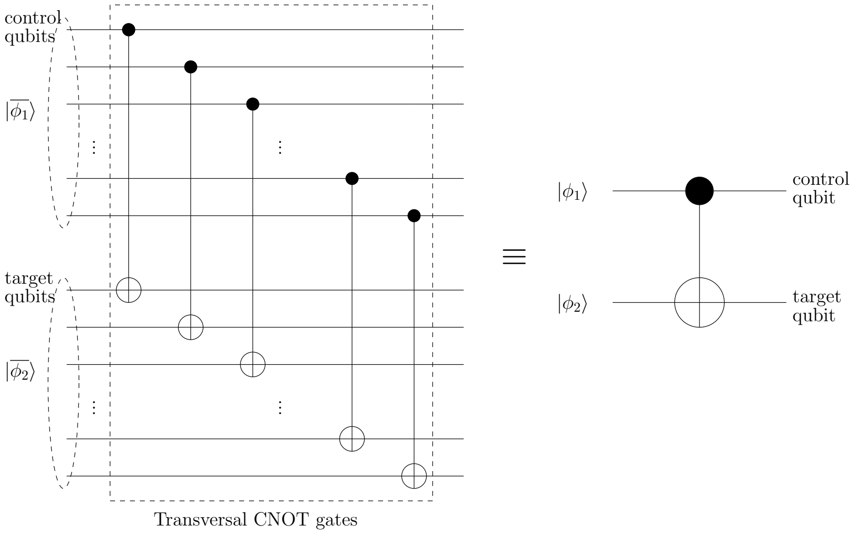


Figure 1.6: Under a certain formulation, a set of less-reliable identical quantum gates in transversal configuration can be used for conceiving a more reliable quantum gate.

The quest for creating fault-tolerant gates was initialized when the notion of transversal configuration was introduced for quantum gates [54, 91]. The concept of transversal gates relies on a parallel set of identical quantum gates invoked for carrying out the operation of a single quantum gate as illustrated in Fig. 1.6. The fact that transversal quantum Clifford gates preserve the stabilizer formalism after the conjugation operation creates an opportunity for employing a wide range of QSCs for protecting transversal quantum gates. However, the challenges we have described earlier suggest that the family of QTECCs is the most suitable candidate for protecting the transversal quantum gates. The motivation behind combining the QTECCs with the transversal configuration of quantum gates is that they conveniently complement each other. More explicitly, the transversal implementation has the benefit of stabilizer preservation, while the QTECCs provide localized stabilizer measurements, which consequently provides the benefit of a constant number of qubit interactions as we increase the number of physical qubits. Thus, the benefits provided by topologically inspired stabilizer formalism will not be affected by the transversal implementation of quantum gates. Hence, the localized action of stabilizer operators amongst the adjacent qubits, which offers fault-tolerance, is still preserved even after the desired quantum operation has been carried out by the transversal quantum gates.

However, the amalgamation of the QSCs and the transversal quantum gates can only be implemented for quantum Clifford gates and it is indeed not the universal set of quantum gates. To achieve the universality of quantum computation, a set of fault-tolerant non-Clifford quantum gates are also required. Fortunately, this can be achieved also using QSCs through a method referred to as magic state distillation [118], which is beyond the scope of this work. However, protecting Clifford gates is of significant importance, since the development of large-scale quantum computers relies heavily on improving their fidelity.

The threshold theorem defined in [119] was introduced for demonstrating that a quantum computation task at a vanishingly low qubit error ratio (QBER) can be achieved with the aid of QECCs even when relying on erroneous quantum gates as long as the error rate imposed by the quantum gates is below a certain threshold. Since the errorneous quantum gates may also provide erroneous stabilizer measurements, typically repeated stabilizer measurements are required for concluding the error correction procedure. The number of stabilizer measurements required for making a high-fidelity observation tends to grow as we increase the number of physical qubits utilized for QECCs. This specific problem has led to the emergence of the so-called single-shot QSCs [120, 121, 122, 123]. Assuming that the syndrome values acquired from the syndrome measurements are not reliable, we can still achieve a vanishingly low QBER for a specific quantum computation task given that we only perform a single stabilizer measurement for each stabilizer operator. However, the beneficial QSC constructions have to have a commensurately increased minimum distance as a function of the number of physical qubits. Unfortunately, the quantum coding rate of the two-dimensional QTECCs tends to zero as the codeword length increased [2, 124, 125]. We need to mention that the reliably observing the values from the stabilizer measurements is also of current research interest, which is highly relevant for the study of single-shot QSCs [126, 127, 128, 129]. Therefore, we can ask a judicious question: “Can we still utilize the two-dimensional QTECCs for fault-tolerant quantum computation, when relying only on a single stabilizer measurement for each of the stabilizer operators?” Arguably, the answer is yes, although certain conditions should be fulfilled before we can guarantee that the QSCs can offer substantial reliability improvements.

1.3 Outline of the Thesis

The rest of this thesis is organized as follows, which is also summarized in Fig. 1.7:

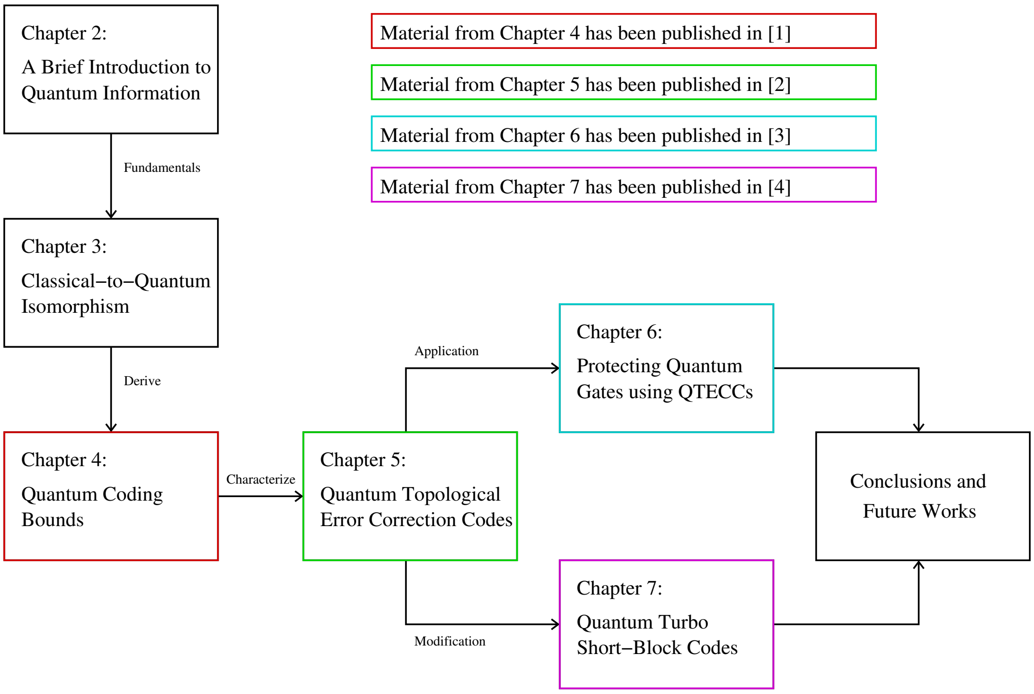


Figure 1.7: The outline of this thesis.

(a) In **Chapter 2**, we will provide an introduction to quantum information processing required for developing this thesis. We commence with the definition of the fundamental unit of quantum information conveyed by the quantum bit (qubit) in Section 2.2. This is followed by a rudimentary introduction to quantum information processing, including the reversible unitary transformations and the irreversible quantum measurement operation in Section 2.3. The various quantum decoherence models used on this report are elaborated on in Section 2.4. In Section 2.5, we present the *no-cloning theorem*, while in Section 2.6, we present the *quantum entanglement*.

(b) In **Chapter 3**, We present the duality of classical and quantum error correction codes with the aid of QSC constructions. Our objective is to highlight the similarities between the classical and quantum domain as well as to demonstrate how to transplant the well-known syndrome-based classical decoding concept into the quantum error correction codes. We commence with a brief review of classical syndrome-based decoding in Section 3.2. In Section 3.3, we present the similarities between the classical syndrome-based decoding and the quantum stabilizer codes (QSCs). Finally, in Section 3.4, we provide detailed examples of the QSC constructions protecting a single qubit, namely a 1/3-rate quantum repetition code, Shor's 9-qubit code, Steane's 7-qubit code, and the Laflamme's perfect 5-qubit code.

(c) In **Chapter 4**, we investigate the trade-off between the quantum coding rate versus the minimum distance of QSCs. We commence with the survey of the existing quantum coding bounds in the literature. This is followed by our proposal of a simple and invertible closed-form approximation for determining the realistically achievable minimum distance, given the quantum coding rate of both idealized infinite-length and practical finite-length codewords. Specifically, in Section 4.2, we survey the existing quantum coding bounds and derive some bounds by exploiting the classical-to-quantum isomorphism. These discussions are followed by our proposed closed-form approximation for the idealized asymptotical limit of having an infinite-length codeword in Section 4.3. Since the asymptotical limit has a little relevance for practical implementations, we also proposed an approximate formula for finite-length codewords. In order to unify our quantum coding bound formulation for both the entanglement-assisted QSCs and the unassisted QSCs dispensing with entanglement, we derive a closed-form approximation for arbitrarily entangled QSCs in Section 4.5.

(d) In **Chapter 5**, we conceive the explicit construction of classical topological error correction codes (TECCs) and their quantum-domain dual pairs, namely the quantum topological error correction codes (QTECCs). We carry out a detailed parametric study and derive the QBER upper bound expression. Explicitly, in Section 5.2, we commence with design examples of classical TECCs to pave the way for delving into the quantum domain, while in Section 5.3 we detail the corresponding QSC design examples of QTECCs. We continue by characterizing the performance of QTECCs in the context of the popular quantum depolarizing channel in terms of their QBER, their distance from Hashing bound, and their fidelity in Section 5.4.

(e) In **Chapter 6**, we conceive the general framework of protecting quantum gates using QSCs. Here, we consider the amalgamation of the transversal configuration of quantum Clifford gates and the QTECCs. This combination has been opted for because it retains the desirable properties of resulting in fault-tolerant QECCs, as a joint benefit of stabilizer preservation and localized stabilizer measurements. First, we proceed with the formulation of our framework in Section 6.2. This is followed by the design examples of QSC-protected Hadamard and CNOT gates in Section 6.3, where we invoke a simple quantum repetition code. In order to evaluate the performance of our proposed framework, in Section 6.4, we present the decoherence model utilized in our simulations. Then in Section 6.5, we quantify the performance of QTECC-protected transversal Hadamard gates and CNOT gates both in terms of their QBER and fidelity along with the derivation of the upper and lower bound of the attainable analytical QBER performance in the face of quantum depolarizing channel.

(f) In **Chapter 7**, we conceive a near-hashing bound quantum turbo short-block code relying on different-rate quantum encoders for combatting diverse quantum depolarizing probabilities. More explicitly, this multiple-rate scheme was conceived by concatenating quantum short-block codes (QSBCs) as the outer codes with a quantum unity-rate code (QURC) as the inner code, which we refer to as the QSBC-QURC construction. In contrast to two-dimensional QTECCs, whose quantum coding rate tends to zero for long codewords, the resultant QSBC-QURC scheme exhibits a relatively high quantum coding rate. Explicitly in Section 7.2, we present the general formulation of QSBCs in terms of their code construction, quantum encoder, and stabilizer measurement. This is followed by Section 7.3, where we propose a novel family of serially-concatenated QTCs by utilizing QSBCs as the outer codes and a QURC as the inner code, which we refer to as the QSBC-QURC scheme. We analyze the convergence behaviour of our iterative-decoding-aided QSBC-QURC scheme using extrinsic information transfer (EXIT) charts and evaluate its QBER and goodput in Section 7.4.

(g) Finally, in **Chapter 8**, we summarize our findings along with a range of promising future research directions.

1.4 Novel Contributions

Based on the aforementioned background, it is of pivotal significance to design QSCs capable of striking a compromise between the conflicting parameters, such as the quantum coding rate, minimum distance, codeword length, and fault-tolerance. More specifically, we focused our attention on the trade-off between the quantum coding rate and the minimum distance relying on the quantum coding bounds. In Chapter 4, our novel contributions [1] are:

(a) We provide a survey of the existing quantum coding bounds found in the literature, along with their relationship to the existing quantum stabilizer code constructions (QSCs). Moreover, to unveil the relationship between the classical and quantum coding bounds, we provide further insights into the classical to quantum isomorphism in the context of the associated coding bound formulations.

(b) We propose an appealingly simple and invertible formulation for characterizing the relationship between the quantum coding rate and the achievable minimum distance of QSCs. The resultant closed-form approximation of the quantum coding bound is suitable both for idealized infinite and practical finite-length codewords. More specifically, we show that using our closed-form approximation, we become capable of estimating the realistically achievable minimum distance of QSCs.

(c) Finally, we derive the quantum coding bounds of maximally-entangled QSCs in conjunction with arbitrary entanglement ratios and unify them with the unassisted QSCs.

Continuing the same line of investigation, we embark on a parametric study in the context of the quantum coding rate versus minimum distance for the popular QTECCs. Therefore, we also present the following contributions [2] in Chapter 5:

(a) We conceive the construction of classical error correction codes based on topological or lattice structures. Additionally, we demonstrate for a long codeword that the resultant codes have a resemblance to the classical low-density parity-check (LDPC) codes exhibiting reasonable code parameters.

(b) Following the introduction of both classical and quantum topological error correction codes as well as of the classical-to-quantum isomorphism, we offer a critical appraisal of QTECCs for a diverse set of code parameters.

(c) We derive the upper bound qubit error rate (QBER) expression of QTECCs in the face of the quantum depolarizing channel and characterize their fidelity.

Ultimately, the QTECCs can be exploited for improving the reliability of imperfect quantum gates. More specifically, we combine the QTECCs with the transversal implementation of quantum Clifford gates for demonstrating that the employment of QSCs is indeed capable of increasing the reliability of quantum gates. Therefore, we also present the following contributions [3] in Chapter 6:

(a) We present a general framework of transversal quantum gates protected by QSCs for gate-based quantum computers by performing only a single stabilizer measurement for each of the stabilizer operators for achieving error correction. We then demonstrate the employment of this framework in the context of both the transversal Hadamard and controlled-NOT (CNOT) gates protected by a simple quantum repetition code.

(b) We then demonstrate the benefits of two-dimensional QTECCs conceived for protecting transversal Hadamard as well as CNOT gates and quantify the qubit error ratio (QBER) improvements attained compared to the unprotected quantum gates.

(c) We present the upper bound and lower bound qubit error rate (QBER) performance of transversal quantum Clifford gates protected by QSCs.

(d) Based on the analytical QBER performance, we found the depolarizing probability threshold and the fidelity threshold to be satisfied by the quantum gates to achieve reliability improvements upon employing QTECCs. These thresholds mark the required performance target for the physical realization of fault-tolerant quantum gates relying on QTECCs.

The conventional QTECCs suffer from an unavoidable low quantum coding rate. This has motivated us to further improve the QTECC construction for increasing their quantum coding rate, but at the same time operating near to the quantum hashing bound. More explicitly, our main contributions in Chapter 7 can be summarized as follows: [4]:

- We present the general design of high-rate QSBCs exhibiting a minimum distance of $d = 2$, which constitute the family of quantum error detection codes (QEDCs). Explicitly, the proposed QSBC can have a block length as short as four physical qubits ($n = 4$) and it has a quantum coding rate of $r_Q = \frac{k}{k+1}$. As an additional benefit, the QSBCs have a scalable encoder structure and require only localized stabilizer measurements. Additionally, we demonstrate that the associated stabilizer measurement can be localized by arranging the physical qubits on a polygon structure, such as a square, hexagon, octagon, etc. Hence, this is the first instantiation of high-rate, scalable, short-length, and high-rate QEDCs.
- We amalgamate the QSBCs with the QURCs [130] for the sake of constructing soft-decision-aided QECCs without sacrificing the quantum coding rate, which results in a low-complexity high-rate QTC design. We refer to the resultant construction as

a QSBC-QURC scheme. Despite having low complexity, the QSBC-QURC scheme is capable of operating close to the achievable quantum hashing bound. Quantitatively, for instance, our simulation results demonstrate that a half-rate QSBC-QURC operates at the distance of $D = 0.029$ from the quantum hashing bound.

- Finally, we conceive the first instantiation of a multi-rate scheme for serial QTCs relying on the flexible scalability of the QSBC-QURC construction. We determine the specific depolarizing probability values at which it is beneficial to switch the quantum coding rate based on the minimum QBER requirement of 10^{-3}. Finally, we quantify the achievable goodput of the QSBC-QURC schemes conceived.

Chapter 2

Preliminaries on Quantum Information

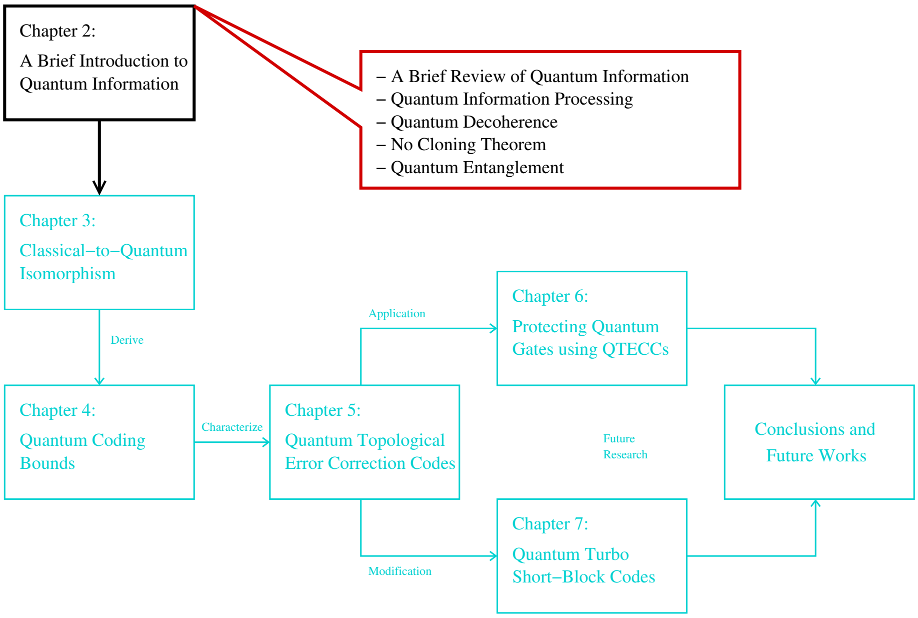


Figure 2.1: The outline of this thesis with the highlight of Chapter 2.

2.1 Introduction

In this chapter, we will highlight the concepts of quantum information processing required for the development of this thesis, paving the way from classical to quantum information theory. The rest of this chapter is organized as follows. We commence with an introduction to quantum information in Section 2.2, followed by a brief tour of quantum information processing in Section 2.3. The quantum channel models used on this treatise are elaborated on in Section 2.4. In Section 2.5, we present the *no-cloning theorem*, followed by *quantum entanglement* in Section 2.6. Finally, we conclude in Section 2.7.

2.2 A Brief Review of Quantum Information

We live in a world where information is transmitted and computed in binary form. Therefore, the fundamental unit of information in the classical domain is the *binary digit* or referred to as a *bit*, which can be defined as follows:

$$c = \{0, 1\}. \tag{2.1}$$

Consequently, in the classical domain, each of the classical bits can only carry the value of 0 or 1, not both. By contrast, in the quantum domain, the fundamental unit of information is represented by a *quantum bit* or *qubit.* The state of a qubit can be described as a linear combination of 0 and 1, which can be described in form of their superposition. However, this superposition of the two states will collapse to the corresponding classical state 0 or 1 upon observation or measurement. More specifically, the quantum state of a single qubit $|\psi\rangle$ can be formally expressed as

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle,\ \ \alpha_0, \alpha_1 \in \mathbb{C}, \tag{2.2}$$

where the probability of obtaining the classical state 0 and 1 upon measurement is given by $|\alpha_0|^2$ and $|\alpha_1|^2$, respectively. Since the values of α_0 and α_1 are associated with probability values, the unitary constraint of $|\alpha_0|^2 + |\alpha_1|^2 = 1$ is satisfied. A single-qubit system can also be viewed as a two-dimensional Hilbert space, where the computational basis vectors $|0\rangle$ and $|1\rangle$ are defined as follows:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.3}$$

Consequently, the quantum state of a single qubit given in Eq. (2.2), can also be represented by a two-dimension complex vector as follows:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix},\ \ \alpha_0, \alpha_1 \in \mathbb{C}. \tag{2.4}$$

The representation of the basis vector of ‘0’ using the notation $|0\rangle$ and the basis vector ‘1’ using the notation $|1\rangle$ is referred to as the *ket* notation. The terminology *ket* comes from the *bra-ket* notation [52], where the *bra* notation refers to $\langle\psi|$, while the *ket* notation is used for $|\psi\rangle$. The relationship between $|\psi\rangle$ and the $\langle\psi|$ is defined as follows:

$$\langle\psi| = |\psi\rangle^\dagger, \tag{2.5}$$

where the notation $|\psi\rangle^\dagger$ indicates the conjugate transpose of $|\psi\rangle$. Explicitly, based on the

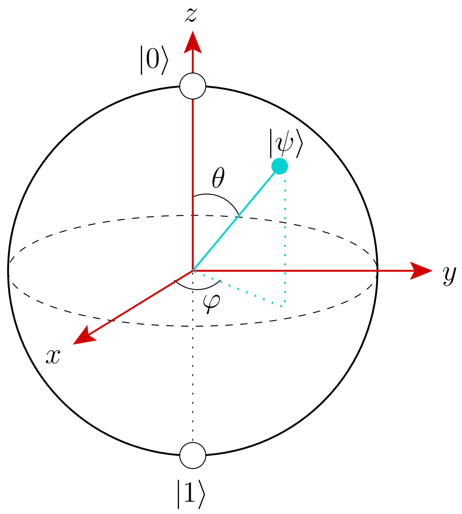


Figure 2.2: The Bloch sphere is the 3D representation of two-dimension complex vector space, which is parametrized by the variables θ and φ. A pure quantum state is represented by a point on the surface of a unit-radius. The computational basis of $|0\rangle$ corresponds to the north pole of the sphere, while the basis of $|1\rangle$ corresponds to the south pole.

vector representation of Eq. (2.4) and the definition of Eq. (2.5), we have

$$\langle\psi| = \begin{pmatrix} \alpha_0^* & \alpha_1^* \end{pmatrix}, \tag{2.6}$$

where α^* denotes the complex conjugate of α. Therefore, the following equality holds:

$$\langle\psi|\psi\rangle \equiv \langle\psi| \cdot |\psi\rangle = 1. \tag{2.7}$$

Since the coefficients α_0 and α_1 are complex numbers, without loss of generality, the state of a qubit can be more explicitly written as follows:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right). \tag{2.8}$$

Furthermore, since the coeffcient of $e^{i\gamma}$ has no observable effect, i.e. $e^{i\gamma}|\psi\rangle$ and $|\psi\rangle$ provide us with identical output probabilities upon measurements, the state of the qubit in Eq. (2.8) can be simplified to the following:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle. \tag{2.9}$$

Therefore, the quantum state of a qubit can be represented as a point on the surface of a unit-radius sphere, which is referred to as the Bloch sphere [131]. The point can be anywhere on the sphere and can be charcterized by two phase variables θ and φ. More explicitly, the 3D representation of a quantum state using the Bloch sphere is depicted in Fig. 2.2.

In general, a pair of vectors can be used as the basis vectors as long as both of them are orthonormal, i.e. both normalized and mutually orthogonal. For example, apart from the computational basis of $|0\rangle$ and $|1\rangle$ in the field of QECCs, the following Hadamard basis is also widely used:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \ |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.10}$$

More explicitly, the Hadamard basis can be viewed as the equal-weight superposition of the computational basis $|0\rangle$ and $|1\rangle$ according to the following definition:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{2.11}$$

and vice versa, the computational basis $|0\rangle$ and $|1\rangle$ can be expressed as an equal-weight superposition of the vectors from the Hadamard basis:

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}, \ |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}. \tag{2.12}$$

In order to extend the concept of quantum information to multi-qubit systems, we have to introduce the Kronecker tensor product or simply tensor product. Explicitly, for a pair of matrices $\mathbf{P}$ and $\mathbf{Q}$ having $(a \times b)$ elements and $(x \times y)$ elements, respectively, the resultant tensor product is a matrix having $(ax \times by)$ elements formulated by

$$\mathbf{P} \otimes \mathbf{Q} = \begin{pmatrix} p_{11}\mathbf{Q} & \cdots & p_{1(b-1)}\mathbf{Q} & p_{1b}\mathbf{Q} \\ p_{21}\mathbf{Q} & \cdots & p_{2(b-1)}\mathbf{Q} & p_{2b}\mathbf{Q} \\ \vdots & \ddots & \vdots & \vdots \\ p_{(a-1)1}\mathbf{Q} & \cdots & p_{(a-1)(b-1)}\mathbf{Q} & p_{(a-1)b}\mathbf{Q} \\ p_{a1}\mathbf{Q} & \cdots & p_{a(b-1)}\mathbf{Q} & p_{ab}\mathbf{Q} \end{pmatrix}. \tag{2.13}$$

For instance, a two-qubit system is represented by the tensor product between a pair of two-element vectors given in Eq. (2.4). More explicitly, let us consider two qubits having the state of $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. The superimposed state can be described as follows:

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} \\ \equiv \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \end{aligned} \tag{2.14}$$

where $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$. It can be observed that a two-qubit state is a superposition of all four possible states that can be generated by two classical bits i.e. 00, 01, 10 and

11. Additionally, the unitary constraint of $|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 + |\alpha_1\beta_0|^2 + |\alpha_1\beta_1|^2 = 1$ still holds. The tensor product of a pair of two-element vectors yields a vector consisting of 2^2 elements. Hence, the N-qubit system produces all of the 2^N possible states that can be generated by an N-bit sequence. If i is the decimal representation of an N-bit sequence, the N-qubit superposition state can be expressed by the Dirac notation as follows:

$$|\psi\rangle = \sum_{i=0}^{2^N-1} \alpha_i|i\rangle \text{ where } \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{2^N-1} |\alpha_i|^2 = 1. \tag{2.15}$$

As an instance of a very special case, where we have N qubits all having $|+\rangle$ state, provides us with the equal-weight superposition of 2^N possible states generated by all possible combination of N-bit sequences as follows:

$$|+\rangle^{\otimes N} \equiv |+\rangle_1 \otimes |+\rangle_2 \otimes \cdots \otimes |+\rangle_N = \frac{1}{\sqrt{2^N}} \sum_{i=0}^{2^N-1} |i\rangle, \tag{2.16}$$

where the superscript $\otimes N$ of $|+\rangle$ represents the N-fold tensor product. It can be observed that the probability of obtaining each of the 2^N quantum states upon their observation in the computational basis is equal to $\frac{1}{2^N}$. This particular state is often used as the initialized quantum state for various quantum computing algorithms, such as Shor's quantum factoring algorithm [13, 14] and Grover's quantum search algorithm [15, 18] as well as for quantum error correction codes.

2.3 Quantum Information Processing

So far we have described the quantum state of a qubit. Similar to the classical domain, the qubit can be manipulated to carry out a specific quantum computation or communication task. The evolution of quantum states can be classified into two categories: reversible and irreversible evolution. A reversible evolution is constituted by a unitary transformation, while an irreversible evolution is due to the measurement or observation of our quantum states, which involves an interaction with the so-called *observer*.

2.3.1 Unitary Transformation

For quantum computation and communication, the desired unitary transformations are carried out by components termed as quantum gates. In classical computers, the circuits rely on logical gates such as AND, OR, and XOR gates. Similar to the classical computer, a quantum computer relies on quantum gates, which can be mathematically represented by unitary transformation satisfying the following properties:

(a) Quantum gates, which are denoted by U, act linearly on the superposition of quantum states, which is defined as

$$U(\alpha_0|0\rangle + \alpha_1|1\rangle) = \alpha_0 U(|0\rangle) + \alpha_1 U(|1\rangle). \tag{2.17}$$

(b) The quantum gate U is characterized a unitary matrix for ensuring that the final probability of all possible quantum states after the transformation is equal to 1. The unitary nature of quantum gates is described as

$$UU^\dagger = \mathbf{I}, \tag{2.18}$$

where $U^\dagger$ is the Hermitian conjugate of U and $\mathbf{I}$ is an identity matrix.

Some of the basic quantum gates used in quantum computation and communication will be discussed in the following subsections.

2.3.1.1 Pauli Gates

First, we would like to introduce the quantum gates acting on a single qubit. Pauli gates or Pauli operators are the most common single-qubit quantum gates used for manipulating the quantum state of a single-qubit. Pauli gates are defined by Pauli matrices as follows:

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.19}$$

Let us assume that we have a single-qubit having a quantum state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. The Pauli matrix $\mathbf{X}$ transforms the quantum state of a single qubit into $|\psi'\rangle$ as follows:

$$\begin{aligned} |\psi'\rangle = \mathbf{X}|\psi\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_0 \end{pmatrix} \\ &\equiv \alpha_1|0\rangle + \alpha_0|1\rangle. \end{aligned} \tag{2.20}$$

The transformation due to the Pauli matrix $\mathbf{Z}$ is given by

$$\begin{aligned} |\psi'\rangle = \mathbf{Z}|\psi\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ -\alpha_1 \end{pmatrix} \\ &\equiv \alpha_0|0\rangle - \alpha_1|1\rangle, \end{aligned} \tag{2.21}$$

while the Pauli matrix $\mathbf{Y}$ transforms a single qubit $|\psi\rangle$ as follows:

$$\begin{aligned}|\psi'\rangle = \mathbf{Y}|\psi\rangle &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} i\alpha_1 \\ -i\alpha_0 \end{pmatrix} \\ &\equiv i\alpha_1|0\rangle - i\alpha_0|1\rangle. \end{aligned} \tag{2.22}$$

Normally, we use unitary transformations for activating the desired quantum-domain evolution of the quantum states of qubits. However, due to the interaction with the environment, or due to the imperfection of quantum gates themselves, or owing to the coherence time of the quantum bit, some undesired unitary transformations may also take place. In this case, each of the Pauli matrices may also be used for reflecting the discrete set of errors that may occur in a single-qubit system, such as a bit-flip error ($\mathbf{X}$), a phase-flip error ($\mathbf{Z}$), as well as both bit-flip and phase-flip error ($i\mathbf{XZ} = \mathbf{Y}$). Finally, the Pauli matrix $\mathbf{I}$ represents the identity operator. More details concerning this issue will be presented in Subsection 2.4.

2.3.1.2 Hadamard Gate

The Hadamard gate maps a pure state of $|0\rangle$ and $|1\rangle$ into an equiprobable superposition of both states. The transformations mapping the pure states by Hadamard gates are described below:

$$\mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+\rangle, \tag{2.23}$$

$$\mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-\rangle. \tag{2.24}$$

The Hadamard gates may be represented using a 2 × 2 matrix as

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{2.25}$$

The Hadamard gates can be used for transforming the computational basis of $|0\rangle$ and $|1\rangle$ into the Hadamard basis of $|+\rangle$ and $|-\rangle$, which will be shown later to be very useful for handling different types of quantum errors imposed by quantum decoherence. The interesting property of this transformation is that a Pauli matrix $\mathbf{X}$ in the computational basis $\{|0\rangle, |1\rangle\}$ behaves similarly to a Pauli matrix $\mathbf{Z}$ in the Hadamard basis $\{|+\rangle, |-\rangle\}$. More explicitly, let us assume that we have a single qubit having a quantum state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. This specific qubit can also be rewritten in the Hadamard basis as $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, where we have $\beta_0 = \frac{\alpha_0+\alpha_1}{\sqrt{2}}$ and $\beta_1 = \frac{\alpha_0-\alpha_1}{\sqrt{2}}$. The action of the Pauli matrix **X** in the computational basis $|0\rangle$ and $|1\rangle$ can be described as follows:

$$|\psi'\rangle = \mathbf{X}|\psi\rangle = \alpha_1|0\rangle + \alpha_0|1\rangle. \tag{2.26}$$

Now, the action of the Pauli matrix **Z** in the Hadamard basis is as follows:

$$|\psi'\rangle = \mathbf{Z}|\psi\rangle = \beta_1|+\rangle + \beta_0|-\rangle. \tag{2.27}$$

It can be observed from Eq. (2.26) and (2.27) that the effect of swapping the complex-valued coefficient between the basis vector in computational basis $|0\rangle$ and $|1\rangle$ is due to the Pauli matrix **X**, but in Hadamard basis this effect is the result of the Pauli matrix **Z**. Similarly, let us observe the effect of the Pauli matrix **Z** on the quantum state of a single qubit in the computational basis, which can be expressed as follows:

$$|\psi'\rangle = \mathbf{Z}|\psi\rangle = \alpha_0|0\rangle - \alpha_1|1\rangle. \tag{2.28}$$

By contrast, the effect of the Pauli matrix **X** on a single-qubit quantum state in the Hadamard basis can be written as

$$|\psi'\rangle = \mathbf{X}|\psi\rangle = \beta_0|+\rangle - \beta_1|-\rangle. \tag{2.29}$$

From Eq. (2.28) and (2.29), we can observe that the Pauli matrix **Z** flips the sign of the complex-valued coefficient of the basis vector $|1\rangle$. However, the sign of the complex-valued coefficient of the basis vector $|-\rangle$ is changed by the operation of the Pauli matrix **X** in Hadamard basis. This specific property will be beneficially exploited in the construction of QSCs, specifically when we are dealing with different types of errors imposed by quantum decoherence, as it will be detailed in Chapter 3.

2.3.1.3 Phase Gate

A phase gate **S** or equivalently i-phase shift gate transforms the quantum state of a single qubit by shifting the phase of state $|1\rangle$ by a factor of i, while the state of $|0\rangle$ remains intact. More specifically, the phase gate **S** is defined by a 2×2 matrix as follows:

$$\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{2.30}$$

The relationship between the phase gate **S** and Pauli gate **Z** is formulated below:

$$\mathbf{S} = \sqrt{\mathbf{Z}}, \tag{2.31}$$

$$\mathbf{S}^2 = \mathbf{Z}. \tag{2.32}$$

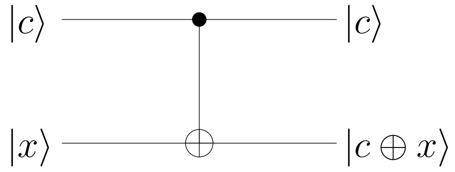


Figure 2.3: The quantum circuit of the CNOT gate, where $|c\rangle$ is the control qubit and $|x\rangle$ is the target qubit.

2.3.1.4 Controlled-NOT Gate

A controlled-NOT or CNOT gate acts similarly to XOR logic gate of a classical computer. To elaborate, the inputs of the CNOT gate are labelled as a control qubit $|c\rangle$ and a target qubit $|x\rangle$. When the control qubit $|c\rangle$ is in the state of $|1\rangle$, the target qubit $|x\rangle$ undergoes the NOT operation, or equivalently it is subjected to a Pauli matrix **X** imposing a bit-flip. Otherwise, the state of the target qubit $|x\rangle$ is left unchanged. Therefore, the transformation performed by a CNOT gate can be defined as

$$\mathbf{CNOT}(|c,x\rangle) \equiv |c,(c \oplus x)\rangle. \tag{2.33}$$

The CNOT gate can also be viewed as a controlled Pauli **X** gate and the corresponding matrix describing the CNOT gate operation is defined as follows:

$$\mathbf{CNOT} = \mathbf{CX} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{I} & 0 \\ 0 & \mathbf{X} \end{pmatrix}. \tag{2.34}$$

The quantum circuit representation of a CNOT gate is protrayed in Fig. 2.3.

The CNOT gate together with the Pauli gates, the Hadamard gate, and the phase gate create a special class of quantum gates called the Clifford group [132]. A special property of the Clifford group is that they can be efficiently simulated using classical computers. Consequently, a quantum circuit purely relying on quantum Clifford gates can be simulated efficiently in classical computer and hence, is not capable of offering any substantial quantum advantage in terms of computational speed-up. By contrast, a more general class of quantum computers capable of achieving computational advantages has to be capable of carrying out unitary transformations including the so-called non-Clifford quantum gates.

2.3.1.5 Toffoli Gate

A very popular example of non-Clifford quantum gate is constituted by Toffoli gate [133], which acts as a controlled-CNOT gate. However, the main difference that it has one target

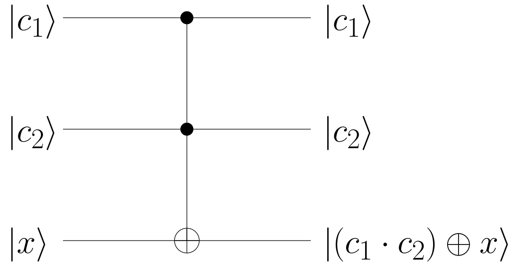


Figure 2.4: The quantum circuit for Toffoli gate.

qubit $|x\rangle$ and two control qubits, $|c_1\rangle$ and $|c_2\rangle$. The target qubit $|x\rangle$ undergoes a bit flip ($\mathbf{X}$) only when both of the control qubits $|c_1\rangle$ and $|c_2\rangle$ are in the state of $|1\rangle$. Otherwise, the state of the target qubit $|x\rangle$ remains intact. The Toffoli gate process the quantum state of three qubits, hence its matrix representation reflects the unitary transformation of 2^3 Hilbert space vectors. Explicitly, the unitary matrix of a Toffoli gate is defined as

$$\mathbf{CCNOT} \quad = \quad \mathbf{CCX} \quad = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.35}$$

The quantum circuit representation of a Toffoli gate is portrayed in Fig. 2.4. Furthermore, the generalized version of Toffoli gates is required for executing Grover's quantum search algorithm, which has been proved to offer beneficial quantum computation advantage [28, 134]. The generalized version of Toffoli gate, namely the $(n-1)$-controlled-NOT gate [135], which is denoted by $\mathbf{C^{\otimes(n-1)}NOT}$, transforms a vector of the 2^n-dimension in Hilbert space. This can be represented by a $(2^n \times 2^n)$-element unitary matrix as follows:

$$\mathbf{C^{\otimes(n-1)}NOT} = \begin{pmatrix} \mathbf{I}^{2^n-2} & \mathbf{0} \\ \mathbf{0} & \mathbf{X} \end{pmatrix}, \tag{2.36}$$

where $\mathbf{I}^{2^n-2}$ is an identity matrix of dimension $(2^n - 2)$, $\mathbf{X}$ is the Pauli matrix, and the rest of the elements of the matrix are equal to zero. According to the unitary transformation of Eq. (2.36), the Pauli matrix $\mathbf{X}$ will be applied to the target qubit $|x\rangle$, if all the $(n-1)$ quantum state of the control qubits sequence are equal to $|1\rangle$. This is a conceptuaply simple yet powerful unitary transformation carried out by a quantum gate, but it cannot be simulated efficiently using classical computers.

2.3.2 Quantum Measurement

We have briefly described the reversible evolution of quantum information, which is mathematically represented by unitary transformations and it is physically realized by quantum gates. Here, we continue by briefly describing the irreversible evolution of quantum information, namely quantum measurement. The final values of a specific quantum computation or quantum communication task have to be read out at the end. Hence, we need the so-called quantum measurement operators. Quantum measurement is described by a collection of measurement operators $\{M_i\}$, where i denotes the measurement outcome that may occur after observations. If a quantum system is in the state of $|\psi\rangle$ before measurement, the probability of the result i may be expressed as

$$p(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle. \tag{2.37}$$

Consequently, the resultant state after measurement is given by

$$|\psi'\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}} = \frac{M_i|\psi\rangle}{\sqrt{p(i)}}. \tag{2.38}$$

The set of measurement operators have to satisfy the so-called completeness criteria, which are defined as

$$\sum_i M_i^\dagger M_i = \mathbf{I}, \tag{2.39}$$

$$\sum_i p(i) = \sum_i \langle\psi|M_i^\dagger M_i|\psi\rangle = 1. \tag{2.40}$$

For example, for a pair of computational basis states $|0\rangle$ and $|1\rangle$, we have two measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. For an arbitrary qubit having a quantum state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, the probability of obtaining each state is formulated by

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = |\alpha_0|^2, \tag{2.41}$$

$$p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = |\alpha_1|^2. \tag{2.42}$$

Hence, the qubit state after measurement may be expressed as

$$|\psi'\rangle_{m=0} = \frac{M_0|\psi\rangle}{|\alpha_0|} = \frac{\alpha_0|0\rangle}{|\alpha_0|}, \tag{2.43}$$

$$|\psi'\rangle_{m=1} = \frac{M_1|\psi\rangle}{|\alpha_1|} = \frac{\alpha_1|1\rangle}{|\alpha_1|}. \tag{2.44}$$

Equations (2.43) and (2.44) explicitly reflect that a qubit will collapse into a classical bit after measurement. The quantum measurement is an irreversible process, because once we obtain our measurement results in form of classical states, it is impossible to learn the values of the complex coefficients of each of the basis vectors. Therefore, we cannot reconstruct the original quantum state from a single measurement result. Having said that, the quantum state can nonetheless be approximated with a specific level of certainty, as long as we can provide a reasonably large number of qubits prepared in an identical quantum state using a method called as quantum state tomography [136, 137].

2.4 Quantum Decoherence

Quantum computers are composed of numerous quantum gates, which are prone to environmental impairments resulting in a short coherence time. Consequently, due to the deleterious effects of quantum decoherence, the resultant quantum state at the output may not be the desired outcome of the quantum computation. In this treatise, the terminology quantum channels will be used for encapsulating all the aforementioned imperfections caused by the quantum decoherence. A quantum channel inflicting a single qubit error can be represented by the Pauli group $\mathcal{P}_1$, which defines the discrete set of possible unitary transformations imposed on a single qubit. Explicitly, the Pauli group $\mathcal{P}_1$ is defined as

$$\mathcal{P}_1 = \{eP : P \in \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}, e \in \{\pm 1, \pm i\}\}, \tag{2.45}$$

which is closed under multiplication. The unitary matrices $\mathbf{X}$ and $\mathbf{Z}$ represent the bit-flip and the phase-flip, respectively, while the matrix $\mathbf{Y}$ represents a simultaneous bit-flip and phase-flip. Finally, the identity unitary matrix $\mathbf{I}$ denotes the absence of error. These Pauli matrices have been defined in Eq. (2.19). Since the qubits whose quantum states only differ in their global phase can be deemed to be equivalent, the reduced Pauli group $\mathcal{P}_1$ denoted by $\mathcal{P}_1^*$ is often used for the sake of simulating the quantum errors by exploiting the Pauli-to-binary isomorphism [131], which is defined as

$$\mathcal{P}_1^* = \{\mathbf{I}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}\}. \tag{2.46}$$

From a different perspective, we can also investigate the quantum channel affecting on quantum information by describing the error effects as a unitary transformation $U(\Delta\theta.\Delta\varphi)$, which maps a point on the surface of the Bloch sphere into a different coordinate. Explicitly, using Eq. (2.9), we can define the quantum error imposed by the quantum channel as follows:

$$U(\Delta\theta, \Delta\varphi)|\psi\rangle = \cos\left(\frac{\theta + \Delta\theta}{2}\right)|0\rangle + e^{(i\varphi + \Delta\varphi)} \sin\left(\frac{\theta + \Delta\theta}{2}\right)|1\rangle, \tag{2.47}$$

where $(\theta + \Delta\theta)$ and $(\varphi + \Delta\varphi)$ are the new variables defining the resultant quantum state. By expanding the quantum state in Eq. (2.47), we can rewrite the unitary transformation of $U(\Delta\theta, \Delta\varphi)$ as follows [138]:

$$U(\Delta\theta, \Delta\varphi)|\psi\rangle = \alpha_{\mathbf{I}}\mathbf{I}|\psi\rangle + \alpha_{\mathbf{X}}\mathbf{X}|\psi\rangle + \alpha_{\mathbf{Z}}\mathbf{Z}|\psi\rangle + \alpha_{\mathbf{Y}}\mathbf{Y}|\psi\rangle, \tag{2.48}$$

where $\alpha_{\mathbf{I}}$, $\alpha_{\mathbf{X}}$, $\alpha_{\mathbf{Z}}$, and $\alpha_{\mathbf{Y}}$ are the resultant expansion coefficients. Here, we want to highlight that although the nature of quantum errors is continuous, the unitary transformation can be expressed as a linear combination of Pauli matrices **I**, **X**, **Z**, and **Y**. Furthermore, noting that apart from a phase-difference, the Pauli matrix **Y** is equivalent to the product of the Pauli matrices **X** and **Z**, i.e we have $i\mathbf{XZ} = \mathbf{Y}$, the expression given in Eq. (2.48) can be further simplified into the following:

$$U(\Delta\theta, \Delta\varphi)|\psi\rangle = \alpha_{\mathbf{I}}\mathbf{I}|\psi\rangle + \alpha_{\mathbf{X}}\mathbf{X}|\psi\rangle + \alpha_{\mathbf{Z}}\mathbf{Z}|\psi\rangle + \alpha_{\mathbf{XZ}}\mathbf{XZ}|\psi\rangle, \tag{2.49}$$

where now the quantum error can be described as a linear combination of the Pauli matrices **I**, **X**, **Z**, and **XZ**. At the end of the quantum computation or communication task, the continuous nature of quantum errors will be projected into one of the following possibilites: the absence of error (**I**), a bit-flip error **X**, a phase-flip error **Z**, or both bit-flip and phase-flip errors **XZ**. This concept is known as the discretization of quantum errors, which is a very useful tool when it comes to designing the associated QECCs for mitigating these error effects.

Now, let us now consider the more general concept of quantum channels affecting an N-qubit system. When considering the quantum state of an N-qubit system, the quantum channel may be described by the Pauli group $\mathcal{P}_n$, which is represented by an n-fold tensor product of $\mathcal{P}_1$ as defined below:

$$\mathcal{P}_n = \{P_1 \otimes P_2 \cdots \otimes P_n | P_j \in \mathcal{P}_1\}, \tag{2.50}$$

where the index j represents the j-th qubit of a system having n physical qubits. An operator $P \in \mathcal{P}_n$ transforms the legitimate quantum state $|\psi\rangle$ into an impaired quantum state $|\widehat{\psi}\rangle$, as formally described below:

$$|\widehat{\psi}\rangle = P|\psi\rangle. \tag{2.51}$$

The quantum channel inflicts an error $P \in \mathcal{P}_n$ on an N-qubit string, where each qubit may independently experience either a bit-flip error (**X**), a phase-flip error (**Z**), or both bit-flip and phase-flip error ($i\mathbf{XZ} = \mathbf{Y}$). The effect of each Pauli matrix has been described earlier in Subsection 2.3.1.1. Let us now proceed by applying the unitary transformations to the multi-qubit state of Eq. (2.14), which can also be represented as a four-element complex vector as follows:

$$|\psi\rangle = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}. \tag{2.52}$$

For instance, let us assume that the quantum channel inflicts a two-qubit unitary transformation of $(\mathbf{X} \otimes \mathbf{I})^1$ upon a two-qubit state. The evolution of the quantum state can be described as follows:

$$\begin{aligned}
|\psi'\rangle &= (\mathbf{X} \otimes \mathbf{I})\, |\psi\rangle \\
&= \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \\
&= \begin{pmatrix} 0 & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \begin{pmatrix} \alpha_{10} \\ \alpha_{11} \\ \alpha_{00} \\ \alpha_{01} \end{pmatrix} \\
&\equiv \alpha_{10}|00\rangle + \alpha_{11}|01\rangle + \alpha_{00}|10\rangle + \alpha_{01}|11\rangle. \qquad (2.53)
\end{aligned}$$

The final state of Eq. (2.53) can also be obtained without expanding the tensor product of the unitary transformation by flipping the state of the first qubit, since the unitary transformation of **XI** represents a bit-flip error occurs on the first qubit owing to the bit-flip (**X**), while the second qubit does not experience any impairment owing to the effect of identity (**I**). More explicitly, due to the unitary transformation **XI**, the state of $|00\rangle$ is changed to the state of $|10\rangle$. The same transformation is also applied to the states of $|01\rangle$, $|10\rangle$, and $|11\rangle$, where they are transformed to the states of $|11\rangle$, $|00\rangle$, $|10\rangle$, respectively. Hence, the magnitude associated with the state of $|00\rangle$ is no longer α_{00} and now it becomes α_{10}. Therefore, the coefficients associated with the states of $|01\rangle$, $|10\rangle$, and $|11\rangle$ now are α_{11}, α_{00}, and α_{01}, respectively.

In this treatise, we focus our discussions on the family of QSCs, which can be derived from their classical counterparts. Even though most of the well-known QSCs are derived on the basis of the classical-to-quantum isomorphism, there is a certain property of the QSCs, which can only be found in the quantum domain, i.e. it has no classical counterparts, namely the degeneracy property. More explicitly, a degeneracy property implies that a set

---

[1] For the sake of simplifying the notation, a set of Pauli matrices for defining a multi-qubit unitary transformation usually does not include the "$\otimes$" operator. For example, a unitary transformation $(\mathbf{X} \otimes \mathbf{Z} \otimes \mathbf{X} \otimes \mathbf{I})$ acting upon a 4-qubit operand can simply be rewritten as **XZXI**. In the rest of the thesis, the latter representation for stabilizer operators will be used, unless it is stated otherwise.

of different error patterns of $P \in \mathcal{P}_n$ may yield an identical corrupted state and consequently we only need a single error recovery operator for reinstating the original quantum state. For example, let us consider a two-qubit system having the following quantum state:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right), \tag{2.54}$$

and let us consider two different error patterns, which can be described as a pair of two-qubit unitary transformations given by $P_1 = \mathbf{IZ}$ and $P_2 = \mathbf{ZI}$. The resultant state after the error pattern P_1 is imposed on the two-qubit system can be described as follows:

$$\begin{aligned} |\psi_1'\rangle &= \mathbf{IZ}|\psi\rangle \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \\ &\equiv \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right), \end{aligned} \tag{2.55}$$

while applying P_2 to the state of $|\psi\rangle$ will result in the following quantum state:

$$\begin{aligned} |\psi_2'\rangle &= \mathbf{ZI}|\psi\rangle \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \\ &\equiv \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right). \end{aligned} \tag{2.56}$$

Since the error patterns $P_1 = \mathbf{IZ}$ and $P_2 = \mathbf{ZI}$ yield identical corrupted states $|\psi_1'\rangle = |\psi_2'\rangle$, they undoubtly require an identical recovery procedure. Indeed, exploiting the degeneracy property may potentially increase the error correction capability of QSCs. However, the question as to whether there exist degenerate QSCs that are capable of operating beyond the quantum Hamming bound, which is only applicable for non-degenerate QSCs, remains unresolved at the time of writing. Having said that, some research on finding the bounds of degenerate quantum codes can be found in [59, 139, 140].

The terminology of quantum channel incorporates numerous physical phenomena, including the imperfect quantum gates or quantum memories. In either of these cases, the qubits undergo a state change, which can be a linear combination of two types of quantum errors, which are described below:

- Amplitude error or bit-flip which turns the state $|0\rangle$ into $|1\rangle$, or state $|1\rangle$ into $|0\rangle$. We also encounter this type of errors in classical settings.
- Phase error or phase-flip which has no impact on the state $|0\rangle$, but it turns the state $|1\rangle$ into $-|1\rangle$. This type of error distinguishes a quantum system from classical systems.

The quantum channel may inflict an individual bit-flip ($\mathbf{X}$), a phase-flip ($\mathbf{Z}$), as well as a simultaneous bit-flip and phase-flip ($\mathbf{Y}$) error with a probability of $p_{\mathbf{X}}$, $p_{\mathbf{Z}}$, and $p_{\mathbf{Y}}$, respectively. These deleterious effects may be inflicted upon each of the qubits within the N-qubit block. For the sake of accommodating three different types of errors, the following are the common quantum channel models widely used for simulation.

2.4.1 Symmetric Quantum Depolarizing Channel

The *symmetric depolarizing channel* is characterized by the depolarizing probability p. It creates an N-tuple of Pauli matrices $P \in \mathcal{P}_n$ for an N-qubit system, where the i-th qubit undergoes either a bit-flip ($\mathbf{X}$) error, a phase-flip ($\mathbf{Z}$) error, or simultaneous bit-flip and phase-flip ($\mathbf{Y}$) errors with an equal probability of $p_e = p/3$, where p denotes the overall depolarizing probabilitye [75, 79, 141]. Hence the probability of error-free transmission is simply given by

$$p_{\mathbf{I}} = 1 - 3p_e = 1 - p. \tag{2.57}$$

In the realm of physical implementations, it has been observed that the probability of bit-flip errors ($p_{\mathbf{X}}$) is not equal to the probability of phase-flip errors ($p_{\mathbf{Z}}$) [142,143,144,145,146]. More specifically, popular materials invoked for producing quantum gates often exhibit an asymmetric behaviour, where the phase-flip errors are several orders of magnitude more likely to occur than the bit-flip errors.

2.4.2 Asymmetric Quantum Depolarizing Channel

The more realistic quantum channel model which relies on this assumption is referred to as an *asymmetric quantum depolarizing channel* [147]. In the asymmetric case, an extra parameter denoted as channel's asymmetry ratio α is introduced for portraying the ratio of the phase-flip probability $p_{\mathbf{Z}}$ and the bit-flip probability $p_{\mathbf{X}}$ as follows:

$$\alpha = \frac{p_{\mathbf{Z}}}{p_{\mathbf{X}}}. \tag{2.58}$$

In practice, the channel's asymmetry ratio has popular values of $\alpha = 10^2, 10^4, 10^6$ [142, 143, 144, 145, 146]. Again, since the probability of phase-flip errors ($p_{\mathbf{Z}}$) is several orders of magnitudes higher than that of bit-flip errors ($p_{\mathbf{X}}$), the probability of both phase and bit-flip errors ($p_{\mathbf{Y}}$) is assumed to be close to $p_{\mathbf{X}}$, which can be written as

$$p_{\mathbf{Y}} \approx p_{\mathbf{X}}. \tag{2.59}$$

Consequently, we can directly describe the parameters of the asymmetric depolarizing channel model using the depolarizing probability (p) and channel's asymmetry ratio (α) as follows:

$$p_{\mathbf{I}} = 1 - p, \tag{2.60}$$

$$p_{\mathbf{X}} = \left(\frac{1}{\alpha + 2}\right) p, \tag{2.61}$$

$$p_{\mathbf{Y}} = \left(\frac{1}{\alpha + 2}\right) p, \tag{2.62}$$

$$p_{\mathbf{Z}} = \left(\frac{\alpha}{\alpha + 2}\right) p. \tag{2.63}$$

2.4.3 Independent Binary-Symmetric Channel

By contrast, the *independent binary-symmetric channel* model assumes that each qubit may experience bit-flip errors ($\mathbf{X}$) and phase-flip errors ($\mathbf{Z}$) independently. This model is equivalent to the combination of two independent binary symmetric channels, where one channel inflicts only bit-flip ($\mathbf{X}$) errors and the other channel only inflict phase flip ($\mathbf{Z}$) errors. Therefore, the parameters describing the independent binary-symmetric channel model are

$$p_{\mathbf{I}} = 1 - p_{\mathbf{X}} - p_{\mathbf{Y}} - p_{\mathbf{Z}}, \tag{2.64}$$

$$p_{\mathbf{X}} = p_e^x \left(1 - p_e^z\right), \tag{2.65}$$

$$p_{\mathbf{Y}} = p_e^x p_e^z, \tag{2.66}$$

$$p_{\mathbf{Z}} = p_e^z \left(1 - p_e^x\right), \tag{2.67}$$

where p_e^x denotes the crossover or flip probability in the channel $\mathbf{X}$ and p_e^z the crossover or flip probability in the channel $\mathbf{Z}$. For the sake of approximating the symmetric quantum depolarizing channel, the crossover probability for each channel is assumed to be equal to $2p/3$, which can be written as

$$p_e^x = p_e^z = \frac{2p}{3}. \tag{2.68}$$

Therefore, the final parameters defining the independent binary-symmetric channel in Eq. (2.67), can be rewritten as follows:

$$p_{\mathbf{I}} = 1 - \left(\frac{4p}{3} - \frac{4p^2}{9}\right), \tag{2.69}$$

$$p_{\mathbf{X}} = \frac{2p}{3} - \frac{4p^2}{9}, \tag{2.70}$$

$$p_{\mathbf{Y}} = \frac{4p^2}{9}, \tag{2.71}$$

$$p_{\mathbf{Z}} = \frac{2p}{3} - \frac{4p^2}{9}. \tag{2.72}$$

Additionally, the independent binary-symmetric channel model can be extended directly to its the asymmetric version, which has $p_e^x \neq p_e^z$. It is important to note that most of our simulations in this treatise rely on the independent binary-symmetric channel model, although most of the analytical results are derived using the assumption having a symmetric quantum depolarizing channel.

2.4.4 Density Matrix

It is sometimes useful to represent all the quantum states and their evolution in the form of quantum density matrices. In general, the density matrix is used for representing the statistical properties of an ensemble of quantum states. Specifically, the density matrix is calculated as the sum of all the legitimate projections weighted with the associated probabilities p_i as follows:

$$\rho = \sum_{i=0}^{n} p_i |\psi_i\rangle\langle\psi_i|, \tag{2.73}$$

where $|\psi_i\rangle$ is the set of legitimate projected states and p_i is the probability of encountering the quantum state $|\psi_i\rangle$. For a single-qubit quantum state, the projections of the quantum state correspond to a pair of mutually orthogonal state vectors, which can be illustrated as a pair of antipodal points on the surface of Bloch sphere in Fig. 2.2. For a multi-qubit system, the projectors of a quantum state correspond to a set of mutually orthonormal state vectors, which satisfy

$$\langle\psi_i|\psi_j\rangle = \delta_{ij}, \tag{2.74}$$

where δ_{ij} is the Kronecker delta function.

A special case is when a quantum state is prepared as a pure state, implying that we have a single quantum state with certainty, while otherwise we have a mixed state. The density matrix of a pure quantum state can be further simplified to

$$\rho = |\psi\rangle\langle\psi|. \tag{2.75}$$

For instance, given a pure state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, where $\langle\psi| = |\psi\rangle^\dagger$, the density marix of the pure state $|\psi\rangle$ can be explicitly rewritten as

$$\rho = \begin{pmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* \\ \alpha_1^*\alpha_1 & |\alpha_1|^2 \end{pmatrix}. \tag{2.76}$$

Since we have $|\alpha_0|^2 + |\alpha_1|^2 = 1$, the following is true:

$$\mathrm{Tr}(\rho) = 1, \tag{2.77}$$

where $\mathrm{Tr}(A)$ denotes the trace of matrix A, which is equal to the sum of the main diagonal elements of a square matrix A.

One of the conveniences in using the density matrix representation exhibits itself when we try to calculate the outcome probabilities of the measurement operator M_i discussed in Subsection 2.3.2 applied to a mixed state having a density matrix ρ. For instance, upon applying a given measurement operator M_i to a mixed state having a density matrix ρ, the probability of obtaining the result i is given by

$$p(i) = \mathrm{Tr}(M_i^\dagger M_i \rho). \tag{2.78}$$

Additionally, quantum decoherence can be described as an evolution of the quantum density matrix. More specifically, we define a quantum channel $\mathcal{E}$, which maps an initial density matrix ρ into a new density matrix ρ' as follows:

$$\mathcal{E}(\rho) = \rho'. \tag{2.79}$$

Let us consider a quantum depolarizing channel. By definition, for a single-qubit pure quantum state $|\psi\rangle$ having a density matrix ρ, a quantum depolarizing channel maps the density matrix to the original density matrix ρ with a probability of $(1-p)$ and to a density matrix of a maximally mixed quantum state $\mathbf{I}/2$ with a probability of p. A conceptually appealing way of interpreting a maximally mixed state is to view it as an equal-weight superposition of all possible states generated by an n-bit string. Therefore, instead of keeping the quantum state intact all the time, the quantum depolarizing channel collapses the original quantum state with a probability of p into a totally random quantum state having a uniform distribution. Thus, the quantum depolarizing channel $\mathcal{E}$ affects a single-qubit system as follows:

$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{\mathbf{I}}{2}, \tag{2.80}$$

where $\mathbf{I}$ is the single-qubit identity Pauli matrix. Observe that the second term of $\mathbf{I}/2$ can also be rewritten as

$$\frac{\mathbf{I}}{2} = \frac{\rho + \mathbf{X}\rho\mathbf{X}^\dagger + \mathbf{Y}\rho\mathbf{Y}^\dagger + \mathbf{Z}\rho\mathbf{Z}^\dagger}{4}, \tag{2.81}$$

for any arbitrary ρ. Consequently, based on Eq. (2.81), the quantum depolarizing channel $\mathcal{E}$ of Eq. (2.80) may also be portrayed in a different way as follows:

$$\mathcal{E}(\rho) = (1 - \frac{3}{4}p)\rho + \frac{p}{4}\left(\mathbf{X}\rho\mathbf{X}^\dagger + \mathbf{Y}\rho\mathbf{Y}^\dagger + \mathbf{Z}\rho\mathbf{Z}^\dagger\right). \tag{2.82}$$

However, it is more convenient to parameterize the quantum depolarizing channel using p' as a parameter, so that we have

$$\mathcal{E}(\rho) = (1-p')\rho + \frac{p'}{3}\left(\mathbf{X}\rho\mathbf{X}^\dagger + \mathbf{Y}\rho\mathbf{Y}^\dagger + \mathbf{Z}\rho\mathbf{Z}^\dagger\right), \tag{2.83}$$

where $p' = 3p/4$. This is where we obtain the symmetric quantum depolarizing channel presented in Subsection 2.4.1. In general, for a simultaneous n-qubit system having 2^n

dimensions, the quantum depolarizing channel can be generalized as

$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{\mathbf{I}_{2^n}}{2^n}, \tag{2.84}$$

where $\mathbf{I}_{2^n}$ is a 2^n-dimension identity matrix. However, simulating the quantum depolarizing channel characterized in Eq. (2.84) classically is hard. Therefore, for an n-qubit system, we assume that each of the qubits experiences independently a quantum depolarizing channel. In this case, an n-qubit independent quantum depolarizing channel can be formulated as

$$\mathcal{E}(\rho^{\otimes n}) = \left[(1-p)\rho + p\frac{\mathbf{I}}{2}\right]^{\otimes n}. \tag{2.85}$$

In this treatise, we mainly focus our attention on the quantum depolarizing channel characterized in Eq. (2.85) and our classical simulation of the quantum systems investigated is designed to emulate the behaviour of this specific quantum channel model.

2.4.5 Fidelity

The effect of quantum decoherence will manifest itself in form of quantum errors upon measurements. Therefore, a systematic way of quantifying the effect of the quantum decoherence is required. A widely used metric for quantifying the deleterious effects of quantum decoherence is fidelity. More specifically, fidelity quantifies the closeness between two ensembles of quantum state. For a pure state $\rho = |\psi\rangle\langle\psi|$ and a mixed state σ, the fidelity can be calculated as

$$F(\rho,\sigma) = \langle\psi|\sigma|\psi\rangle. \tag{2.86}$$

In case of two pure quantum states having density matrices of $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, the fidelity can be simplified as

$$F(\rho,\sigma) = |\langle\psi|\phi\rangle|^2. \tag{2.87}$$

Any unitary transformation U applied to both quantum states will preserve the fidelity, since we have $U^\dagger U = \mathbf{I}$. For a pair of mixed states having density matrix ρ and σ, the fidelity is calculated using [169]

$$F(\rho,\sigma) = \left[\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]^2. \tag{2.88}$$

Let us now consider the example of a single-qubit symmetric quantum depolarizing channel, whose density matrix is presented in Eq. (2.80) of Subsection 2.4.4. By substituting the density matrix into σ of Eq. (2.86), we obtain

$$\begin{aligned} F(\rho,\sigma) &= \langle\psi|\sigma|\psi\rangle \\ &= \langle\psi|\left[(1-p)\rho + p\frac{\mathbf{I}}{2}\right]|\psi\rangle \\ &= (1-p)\langle\psi|\rho|\psi\rangle + \frac{p}{2}\langle\psi|\mathbf{I}|\psi\rangle \\ &= (1-p) + \frac{p}{2} \\ &= 1 - \frac{p}{2}. \end{aligned} \tag{2.89}$$

Hence, we can directly calculate the fidelity after taking into account the effect of a simultaneous n-qubit symmetric depolarizing channel by substituting the density matrix of Eq. (2.84) into σ of Eq. (2.86). Thus, we obtain

$$\begin{aligned} F(\rho,\sigma) &= \langle\psi|\sigma|\psi\rangle \\ &= \langle\psi|\left[(1-p)\rho + p\frac{\mathbf{I}_{2^n}}{2^n}\right]|\psi\rangle \\ &= (1-p)\langle\psi|\rho|\psi\rangle + \frac{p}{2^n}\langle\psi|\mathbf{I}_{2^n}|\psi\rangle \\ &= 1 - p + \frac{p}{2^n}. \end{aligned} \tag{2.90}$$

It can be observed that as $n \to \infty$, the value of fidelity tends to $F(\rho,\sigma) \approx 1-p$. By contrast, let us now consider the n-qubit independent symmetric depolarizing channel characterized in Eq. (2.85). Firstly, for any single-qubit density matrix of ρ_1, ρ_2, σ_1, and σ_2, the following equality holds:

$$F\left[(\rho_1 \otimes \rho_2), (\sigma_1 \otimes \sigma_2)\right] = F(\rho_1,\sigma_1)F(\rho_1,\sigma_1). \tag{2.91}$$

For a pair of identical quantum channels, where $\rho_1 = \rho_2 = \rho$ and $\sigma_1 = \sigma_2 = \sigma$, Eq. (2.91) can be simplified to

$$F\left(\rho^{\otimes 2}, \sigma^{\otimes 2}\right) = \left[F(\rho,\sigma)\right]^2. \tag{2.92}$$

Consequently, we can generalize this formulation into identical n-tuple quantum channels as follows:

$$F\left(\rho^{\otimes n}, \sigma^{\otimes n}\right) = \left[F(\rho,\sigma)\right]^n. \tag{2.93}$$

Finally, we can determine the fidelity of an independent n-qubit symmetric depolarizing channel based on the density matrix of Eq. (2.85). Thus, we obtain

$$\begin{aligned} F\left(\rho^{\otimes n}, \sigma^{\otimes n}\right) &= \left(1 - \frac{p}{2}\right)^n \\ &= 1 - \frac{np}{2} + \binom{n}{2}\left(\frac{p}{2}\right)^2 - \binom{n}{3}\left(\frac{p}{2}\right)^3 + \cdots \\ &= 1 - \frac{np}{2} + \mathcal{O}(p^2). \end{aligned} \tag{2.94}$$

Therefore, for a very small value of $p \ll 1$, the value of fidelity tends to $F \approx 1 - np/2$.

Now, the question arises, how we can calculate the fidelity from the observed quantum bit error rate (QBER), whilst relying on classical-domain simulation of quantum systems. For instance, let us assume that based on the classical-domain simulation of a single-qubit channel the observed QBER values for a bit-flip channel, for a phase-flip channel, as well as for a simultaneous bit-flip and phase-flip channel are denoted by $\text{QBER}_{\mathbf{X}}$, $\text{QBER}_{\mathbf{Z}}$, and $\text{QBER}_{\mathbf{Y}}$, respectively. Let us now calculate the fidelity of a pure bit-flip ($\mathbf{X}$) channel. Given a pair of pure quantum states $|\psi\rangle$ and $\phi = \mathbf{X}|\psi\rangle$, their fidelity can be calculated using Eq. (2.87) as follows:

$$F(\rho, \sigma) = |\langle\psi|\mathbf{X}|\psi\rangle|^2. \tag{2.95}$$

There is no specific value for this equation, since for different pure states ρ it gives us different fidelity values. However, for helping our analysis, the following Cauchy-Schwarz inequality always holds:

$$|\langle\psi|\phi\rangle|^2 \leq \langle\psi|\psi\rangle\langle\phi|\phi\rangle. \tag{2.96}$$

Consequently, we readily arrive the following inequality

$$\begin{aligned} |\langle\psi|\mathbf{X}|\psi\rangle|^2 &\leq \langle\psi|\psi\rangle\langle\psi|\mathbf{X}^\dagger\mathbf{X}|\psi\rangle \\ &\leq 1. \end{aligned} \tag{2.97}$$

Nonetheless, we also have the following trivial inequality:

$$|\langle\psi|\mathbf{X}|\psi\rangle|^2 \geq 0. \tag{2.98}$$

Therefore, for an observed pure bit-flip channel $\mathcal{E}$ acting on a pure quantum state ρ, which has the following description:

$$\mathcal{E}(\rho) = (1 - \text{QBER}_{\mathbf{X}})\rho + \text{QBER}_{\mathbf{X}}\mathbf{X}\rho\mathbf{X}^\dagger, \tag{2.99}$$

the fidelity is bounded by

$$1 - \text{QBER}_{\mathbf{X}} \leq F(\rho, \sigma) \leq 1. \tag{2.100}$$

This inequality can also be directly extended both to the phase-flip ($\mathbf{Z}$) channel as well as to the simultaneous bit-flip and phase-flip ($\mathbf{Y}$) channel. Therefore, we characterize write the quantum channel based on our observed QBER values as follows:

$$\mathcal{E}(\rho) = (1 - \text{QBER})\rho + \text{QBER}_{\mathbf{X}}\mathbf{X}\rho\mathbf{X}^\dagger + \text{QBER}_{\mathbf{Y}}\mathbf{Y}\rho\mathbf{Y}^\dagger + \text{QBER}_{\mathbf{Z}}\mathbf{Z}\rho\mathbf{Z}^\dagger, \tag{2.101}$$

where we have $\text{QBER} = \text{QBER}_{\mathbf{X}} + \text{QBER}_{\mathbf{Y}} + \text{QBER}_{\mathbf{Z}}$. For a pure input quantum state $|\psi\rangle$ having a density matrix of ρ, the fidelity is bounded by:

$$1 - \text{QBER} \leq F(\rho, \sigma) \leq 1. \tag{2.102}$$

For the specific case, where we have $\text{QBER}_{\mathbf{X}} = \text{QBER}_{\mathbf{Y}} = \text{QBER}_{\mathbf{Z}} = \text{QBER}/3$, the fidelity can be calculated similarly to the fidelity of a symmetric quantum depolarizing channel.

Since we have

$$\frac{\text{QBER}}{3}\left(\rho + \mathbf{X}\rho\mathbf{X}^\dagger + \mathbf{Y}\rho\mathbf{Y}^\dagger + \mathbf{Z}\rho\mathbf{Z}^\dagger\right) = \frac{2\text{QBER}}{3}\mathbf{I}, \tag{2.103}$$

the quantum channel given in Eq. (2.101), may also be expressed as

$$\mathcal{E}(\rho) = (1 - \frac{4\text{QBER}}{3})\rho + \frac{2\text{QBER}}{3}\mathbf{I}. \tag{2.104}$$

Thus, we obtain the fidelity value of

$$F(\rho, \sigma) = 1 - \frac{2}{3}\text{QBER}. \tag{2.105}$$

If we consider the value of QBER $= p$, the actual fidelity value drawn from the simulation value lies between the fidelity value of $F = 1 - 2p/3$ based Eq. (2.105) and of $F = 1 - p$ relying on Eq. (2.102). In the rest of this treatise, we assume that the fidelity values obtained from classical simulation results are exactly $F = 1 - p$ or $F = 1 -$ QBER. This assumption is chosen for convenience, bearing in mind that this is somewhat innacurate, since it gives a lower fidelity for a given p or QBER value than the true fidelity. Additionally, since the QBER value is obtained purely from the observation of classical simulation results, it is rather challenging to ensure that the observed values can always satisfy the condition of $\text{QBER}_\mathbf{X} = \text{QBER}_\mathbf{Y} = \text{QBER}_\mathbf{Z}$.

2.5 No-Cloning Theorem

The concept of copying or cloning the information to protect it is widely used in classical communication and information theory. Unfortunately, the same concept is no longer valid as we enter into the quantum domain due to the *no-cloning theorem*, which states that no unitary transformation can copy an arbitrary superposition of quantum states from one qubit to another qubit.

Proof. Let us assume that we have two orthogonal basis vector of $|\psi_1\rangle$ and $|\psi_2\rangle$. Let us consider a single-qubit system having a quantum state of $|\psi_1\rangle$, which acts as the data qubit, and another single-qubit system having a quantum state of $|\psi_t\rangle$, which acts as the target qubit for copying the quantum state from data qubit. Thus, the initial value before activating the copying mechanism is given by

$$|\psi'\rangle = |\psi_1\rangle \otimes |\psi_t\rangle. \tag{2.106}$$

Let us assume furthermore that there exists a unitary transformation U having a copying mechanism. Then ideally the final joint quantum state after copying is formulated as

$$U(|\psi_1\rangle \otimes |\psi_t\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle. \tag{2.107}$$

Upon assuming that this copying mechanism is applied to the second data qubit having a quantum state of $|\psi_2\rangle$, the copying procedure yields

$$U(|\psi_2\rangle \otimes |\psi_t\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle. \tag{2.108}$$

Let us now proceed with the cloning of a superimposed quantum state, i.e. $|\lambda\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$, where $\alpha_1, \alpha_2 \in \mathbb{C}$. The copying mechanism can be formulated as

$$U(|\lambda\rangle \otimes |\psi_t\rangle) = |\lambda\rangle \otimes |\lambda\rangle. \tag{2.109}$$

Expanding the left-hand side of Eq. (2.109) yields

$$\begin{aligned} U(|\lambda\rangle \otimes |\psi_t\rangle) &= U\left[(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle) \otimes |\psi_t\rangle\right] \\ &= U(\alpha_1|\psi_1\rangle \otimes |\psi_t\rangle) + U(\alpha_2|\psi_2\rangle \otimes |\psi_t\rangle) \\ &= \alpha_1|\psi_1\rangle \otimes |\psi_1\rangle + \alpha_2|\psi_2\rangle \otimes |\psi_2\rangle \\ &\equiv \alpha_1|\psi_1, \psi_1\rangle + \alpha_2|\psi_2, \psi_2\rangle. \end{aligned} \tag{2.110}$$

Upon simplifying the right-hand side of Eq. (2.109), we obtain

$$\begin{aligned} |\lambda\rangle \otimes |\lambda\rangle &= (\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle)(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle) \\ &= \alpha_1^2|\psi_1\rangle|\psi_1\rangle + \alpha_1\alpha_2|\psi_1\rangle|\psi_2\rangle + \alpha_1\alpha_2|\psi_2\rangle|\psi_1\rangle + \alpha_2^2|\psi_2\rangle|\psi_2\rangle \\ &\equiv \alpha_1^2|\psi_1, \psi_1\rangle + \alpha_1\alpha_2|\psi_1, \psi_2\rangle + \alpha_1\alpha_2|\psi_2, \psi_1\rangle + \alpha_2^2|\psi_2, \psi_2\rangle. \end{aligned} \tag{2.111}$$

Equating Eq. (2.110) and Eq. (2.111) yields

$$\alpha_1(\alpha_1 - 1)|\psi_1, \psi_1\rangle + \alpha_1\alpha_2|\psi_1, \psi_2\rangle + \alpha_1\alpha_2|\psi_2, \psi_1\rangle + \alpha_2(\alpha_2 - 1)|\psi_2, \psi_2\rangle = 0. \tag{2.112}$$

Equation (2.112) implies that the solution of the equation is given by $\alpha_1, \alpha_2 = \{0, 1\}$, which results in the quantum state $|\psi_1\rangle$ or $|\psi_2\rangle$ itself. We arrive at the conclusion that a quantum-domain copying operation is only capable of cloning the basis states $|\psi_1\rangle$ and $|\psi_2\rangle$, but fails to clone the superposition of the two states $|\lambda\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$.

2.6 Quantum Entanglement

Quantum entanglement is a unique property that only exists in the quantum domain, which has no counterparts in classical systems. It may be described as a phenomenon where a pair or a group of qubits is generated in such a way that the quantum state of the constituent qubit cannot be described indepedently. For instance, let us consider a two-qubit quantum system having a quantum state of $|\psi\rangle$. The quantum state of $|\psi\rangle$ is said to be separable if it can be expressed as a tensor product of two independent quantum states as follows:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle. \tag{2.113}$$

Otherwise, the quantum state $|\psi\rangle$ is said to be entangled. More explicitly, to provide a clearer picture about quantum entanglement, let us consider an arbitrary two-qubit state as follows:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{11}|11\rangle, \tag{2.114}$$

where $\alpha_{00}, \alpha_{11} \neq 0$. Let us now consider a quantum state constituted by the superposition of two individual qubits, which may be described as follows:

$$\begin{aligned} |\psi\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \end{aligned} \tag{2.115}$$

By equating Eq. (2.114) and Eq. (2.115), we arrive at

$$\alpha_{00}|00\rangle + \alpha_{11}|11\rangle \quad = \quad \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \tag{2.116}$$

Since the non-zero solution for α_{00}, α_{11}, α_0, α_1, β_0, and β_1 does not exist for Eq. (2.116), it is impossibe to decompose the state of the qubits in Eq. (2.114) into two individual qubit states as in Eq. (2.115).

To elaborate a little further, let us now consider a very specific quantum state defined as follows:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.117}$$

In this case, if we perform a quantum measurement on the first qubit in Eq. (2.117), we can determine the value of the second qubit immediately with absolute certainty. If the measurement result of the first qubit is 0, the result of measuring the second qubit will also be 0. Similarly, if the measurement result of the first qubit is 1, the result of observing the second qubit will also be 1. Consequently, this inherent correlation between the two qubits having a quantum state of $|\Phi^+\rangle$ is established even if they are separated in space. This interesting phenomenon was given the fond connotation of “spooky action at a distance” by Einstein.

Quantum entanglement enables a pair or a group of qubits to interact over a distance simultaneously, even if they are at the opposite sides of the universe. However, this intriguing fact does not mean that we can communicate faster than the speed of light. Although there is a connection between the entangled qubits, we still do not know what information is going to be transmitted, since we cannot observe the state of entangled qubits before their measurement. Hence, this connection cannot be used for information transmission. This condition is further elaborated on by the *no communication theorem*, which is a specific theorem of quantum information theory. However, the ability of creating entanglement may be exploited for beneficial applications such as for example QECCs [66, 67], quantum key distribution [30], quantum superdense coding [31], quantum teleportation [32], and quantum secure-direct communication [33].

2.7 Summary and Conclusions

This chapter provides a brief introduction to fundamental quantum information processing. We have highlighted the basic properties of the qubits along with the quantum evolutions acting on single-qubit and multi-qubit systems. We have categorized the quantum evolution into reversible evolution represented by the unitary transformations and the irreversible evolution constituted by quantum measurements. We have also introduced several quantum gates widely utilized in the development of this treatise. Additionally, we have presented various quantum channel models used for simulating the quantum decoherence imposed on the quantum information. Additionally, we have presented one of the fundamental limitations in the quantum domain, namely the no-cloning theorem, which states that we cannot replicate the quantum state of a qubit in an arbitrary superposition state. Finally, we have described one of the distinctive features of quantum information, namely the ability to create quantum entanglement. The rest of the thesis will be developed based on the knowledge presented in this chapter.

Chapter 3

On the Classical-to-Quantum Isomorphism of Error Correction Codes

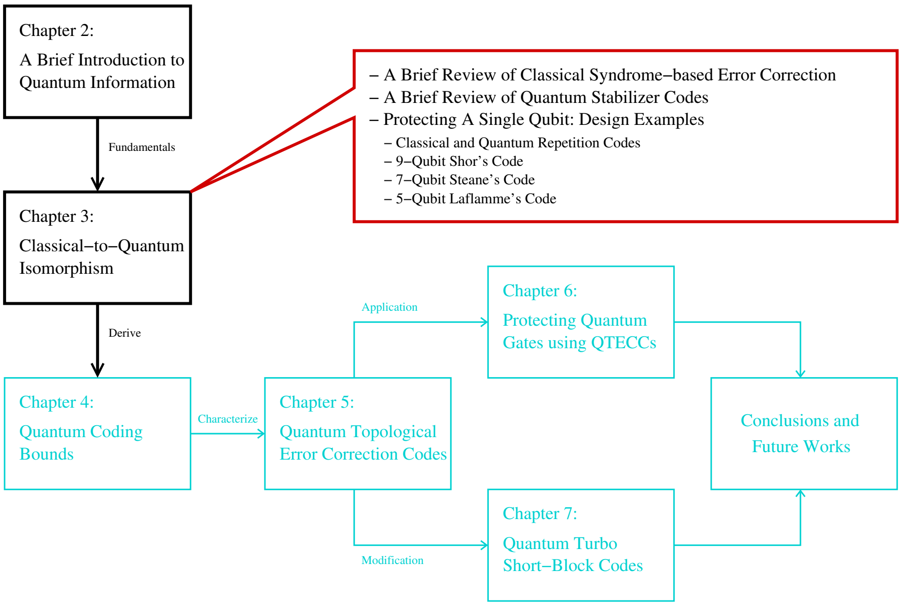


Figure 3.1: The outline of this thesis with the highlight of Chapter 3.

3.1 Introduction

In Chapter 2, we have discussed that quantum information suffers from qubit errors. In the classical domain, the deleterious effects of errors imposed by the channel can be mitigated using error correction codes by attaching redundancy to the information part. However, the laws of quantum mechanics prevent us from directly transplanting the classical error correction codes into the quantum domain owing to the following obstacles:

(a) **No-Cloning Theorem**. In the classical domain, the simplest technique of protecting the information bits is based on repetition coding, copying the same information bits several times. By contrast, in the quantum domain, this simple approach cannot be implemented, since no unitary quantum transformation is capable of performing this specific task. Formally, this is stated by the no-cloning theorem.

(b) **The quantum bit collapses into the corresponding classical bit upon measurement**. In the classical domain, the error correction decoders are typically fed by the bits received at the output of the demodulator. In the quantum domain, measuring the qubits represented by the superposition of the classical states will collapse the superposition into a single classical post-measurement state and consequently, we lose the original quantum information.

(c) **QECCs have to handle not only bit-flip errors but also phase-flip errors, as well as the simultaneous bit-flip and phase-flip errors**. By contrast, in the classical domain, we deal with a single type of error, which is the bit-flip error. In quantum domain, the nature of quantum decoherence is continuous and it can be modelled as a linear combination of bit-flip errors ($\mathbf{X}$), phase-flip errors ($\mathbf{Z}$), or both bit-flip and phase-flip errors ($i\mathbf{XZ} = \mathbf{Y}$). However, thanks to the beneficial effect of the stabilizer measurement, the continuous nature of quantum decoherence can be treated as a discrete set of independent errors imposed on the physical qubits.

Albeit all of the aforementioned obstacles hinder the development of QECC schemes, the invention of QSC formulation succeeded in circumventing these problems.

In this chapter, we present the classical-to-quantum isomorphism of the QSCs, demonstrating the duality between the classical and quantum domain. We will also show how to transplant the well-known syndrome-based decoding of classical codes into quantum codes. The rest of this chapter is organized as follows. We commence with a brief review of classical syndrome-based decoding in Section 3.2. This is followed by Section 3.3, where we present the similarities between classical syndrome-based decoding and the quantum stabilizer codes (QSCs). In Section 3.4, we provide the examples for the QSC constructions protecting a single qubit using 1/3-rate quantum repetition code, Shor's code, Steane's code and the perfect 5-qubit code. Finally, we conclude this chapter in Section 3.5.

3.2 A Brief Review of Classical Syndrome-based Decoding

As mentioned earlier, the problems revolving around the QECCs are effectively circumvented by QSCs, which essentially constitute the syndrome-based decoding version of QECCs. Hence, for the sake of shedding some light onto the parallelism between the classical and quantum regime, we proceed with the classical syndrome-based decoding first.

In the classical domain a $\mathcal{C}(n, k)$ code maps k information bits into n coded bits, where $k < n$. The purpose of attaching $(n-k)$ redundant bits is to facilitate error detection or even

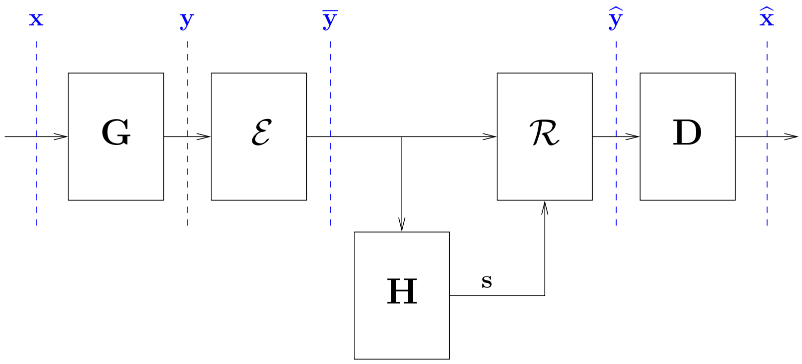


Figure 3.2: The basic model of classical error correction codes invoking syndrome-based decoding. The $\mathbf{G}$ denotes the generator matrix, which maps the k information bits $\mathbf{x}$ to the n coded bits $\mathbf{y}$. The channel $\mathcal{E}$ inflicts an error vector $\mathbf{e} \in \{0,1\}^n$ to the codeword $\mathbf{y}$ resulting the corrupted received bits $\overline{\mathbf{y}}$. The receiver calculates the syndrome vector $\mathbf{s}$ based on the PCM $\mathbf{H}$ and received bits $\overline{\mathbf{y}}$ to predict the number and the position of errors contained in the received bits $\overline{\mathbf{y}}$. The error recovery $\mathcal{R}$ generates the error recovery vector $\mathbf{r}$, which is applied to the received bits $\overline{\mathbf{y}}$. It collapses the received bits $\overline{\mathbf{y}}$ to one of the legitimate codedword $\mathbf{y}$ yielding the predicted codeword $\widehat{\mathbf{y}}$. Finally, we can readily determine the predicted information bits $\widehat{\mathbf{x}}$ from the predicted codeword $\widehat{\mathbf{y}}$.

error correction. Let us refer to Fig. 3.2 and consider the classical $\mathcal{C}(7,4)$ Hamming code, which maps 4 information bits into 7 coded bits and hence becomes capable of correcting a single error. In general, the mapping of the k information bits is performed by multiplying the information row vector $\mathbf{x}$ consisting of k elements by the generator matrix $\mathbf{G}$ having $(k \times n)$ elements. Explicitly, the mapping can be formulated as

$$\mathbf{y} = \mathbf{x} * \mathbf{G}, \tag{3.1}$$

where the resultant codeword $\mathbf{y}$ is a row vector having n elements, while the notation of $*$ represents the matrix multiplication over modulo-2. For instance, the generator matrix of the $\mathcal{C}(7,4)$ Hamming code is defined by

$$\mathbf{G}_{\text{Hamming}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{3.2}$$

From Eq. (3.1) and (3.2) we can generate the code space mapping shown in Table 3.1, where $\mathbf{x}_i$ denotes all the possible combination of information bits and $\mathbf{y}_i$ represents the associated legitimate codeword bits.

The generator matrix $\mathbf{G}$ can be arranged into a systematic form as

$$\mathbf{G} = (\mathbf{I}_k | \mathbf{P}), \tag{3.3}$$

Table 3.1: The code space mapping of the $\mathcal{C}(7,4)$ classical Hamming code.

i	$\mathbf{x}_i$	$\mathbf{y}_i$
1	0 0 0 0	0 0 0 0 0 0 0
2	0 0 0 1	0 0 0 1 1 1 1
3	0 0 1 0	0 0 1 0 0 1 1
4	0 0 1 1	0 0 1 1 1 0 0
5	0 1 0 0	0 1 0 0 1 0 1
6	0 1 0 1	0 1 0 1 0 1 0
7	0 1 1 0	0 1 1 0 1 1 0
8	0 1 1 1	0 1 1 1 0 0 1
9	1 0 0 0	1 0 0 0 1 1 0
10	1 0 0 1	1 0 0 1 0 0 1
11	1 0 1 0	1 0 1 0 1 0 1
12	1 0 1 1	1 0 1 1 0 1 0
13	1 1 0 0	1 1 0 0 0 1 1
14	1 1 0 1	1 1 0 1 1 0 0
15	1 1 1 0	1 1 1 0 0 0 0
16	1 1 1 1	1 1 1 1 1 1 1

where $\mathbf{I}_k$ is a $(k \times k)$ identity matrix and $\mathbf{P}$ is a matrix having $k \times (n-k)$ elements. The form given in Eq. (3.3) generates a systematic codeword $\mathbf{y}$ consisting of the k-bit information word $\mathbf{x}$ followed by $(n-k)$ parity bits. A generator matrix $\mathbf{G}$ is associated with an $(n-k) \times n$-element parity-check matrix (PCM) $\mathbf{H}$, which is defined as

$$\mathbf{H} = \left(\mathbf{P}^T | \mathbf{I}_{n-k}\right). \tag{3.4}$$

As an example, the generator matrix of the classical $\mathcal{C}(7,4)$ Hamming code of Eq. (3.2) is associated with the following PCM:

$$\mathbf{H}_{\text{Hamming}} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{3.5}$$

The PCM of $\mathbf{H}$ is constructed for ensuring that a valid codeword $\mathbf{y}$ satisfies the following requirement:

$$\mathbf{y} * \mathbf{H}^T = \mathbf{0}. \tag{3.6}$$

A received word $\overline{\mathbf{y}}$ may be contaminated by an error vector $\mathbf{e} \in \{0,1\}^n$ due to channel impairments, which is denoted by $\mathcal{E}$ in Fig. 3.2. More explicitly, the resultant received words corrupted by the additive noise $\mathcal{E}$ can be formulated as

$$\overline{\mathbf{y}} = \mathbf{y} + \mathbf{e}. \tag{3.7}$$

The error syndrome $\mathbf{s}$ is a row vector having $(n-k)$ elements obtained by the following calculation:

$$\begin{aligned}\mathbf{s} = \overline{\mathbf{y}} * \mathbf{H}^T &= (\mathbf{y} + \mathbf{e}) * \mathbf{H}^T \\ &= \mathbf{y} * \mathbf{H}^T + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{0} + \mathbf{e} * \mathbf{H}^T \\ &= \mathbf{e} * \mathbf{H}^T. \end{aligned} \tag{3.8}$$

The syndrome vector $\mathbf{s}$ contains the information related to the error pattern imposed by the channel. To elaborate, we have 2^k legitimate codewords generated by the all possible combination of the k information bits, 2^n possible received bit patterns of $\widehat{\mathbf{y}}$ and $2^{(n-k)}$ syndromes $\mathbf{s}$, each unambiguously identifying one of the $2^{(n-k)}$ error patterns, including the error-free scenario. Hence, for the classical $\mathcal{C}(7,4)$ Hamming code, the syndrome vector $\mathbf{s}_i$ can detect and correct a single error pattern as specified in Table 3.2. The error recovery $\mathbf{r}_i$ is determined based on the most likely error pattern. After obtaining the syndrome vector, the recovery vector $\mathbf{r}_i$ is applied to the received words to obtain the predicted codeword $\widehat{\mathbf{y}} = \overline{\mathbf{y}} + \mathbf{r}$, as depicted in Fig. 3.2. The application of the recovery operator to the received word always collapses it into one of the legitimate codewords $\mathbf{y}$, hence the predicted codeword $\widehat{\mathbf{y}}$ can be finally demapped in order to obtain the predicted information bits $\widehat{\mathbf{x}}$ using Table 3.1, as illustrated in Fig. 3.2. For linear systematic codes, this process can be simply performed by chopping the last $(n-k)$ bits, namely the redundant bits.

Table 3.2: The look-up table to determine the most likely error pattern $\mathbf{e}_i \in \mathcal{E}$ that corresponds to the syndrome value $\mathbf{s}_i$, which is created based on Eq. (3.5) and (3.8).

i	$\mathbf{s}_i$	$\mathbf{e}_i$
1	0 0 0	0 0 0 0 0 0 0
2	0 0 1	0 0 0 0 0 0 1
3	0 1 0	0 0 0 0 0 1 0
4	0 1 1	0 0 1 0 0 0 0
5	1 0 0	0 0 0 0 1 0 0
6	1 0 1	0 1 0 0 0 0 0
7	1 1 0	1 0 0 0 0 0 0
8	1 1 1	0 0 0 1 0 0 0

For more a detailed example let us consider k information bits of $\mathbf{x} = (1\ 1\ 0\ 1)$. The information bits are encoded using the classical $\mathcal{C}(7,4)$ Hamming code employing the generator matrix of Eq. (3.1), yielding the coded bits of $\mathbf{y} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Let us assume that the channel corrupts the legitimate codeword $\mathbf{y}$ by imposing an error pattern of $\mathbf{e} = (1\ 0\ 0\ 0\ 0\ 0\ 0)$ resulting the received word of $\overline{\mathbf{y}} = (0\ 1\ 0\ 1\ 1\ 0\ 0)$. Next, the received word is fed to the syndrome calculation block, which contains the PCM of Eq. (3.5). Based on Eq. (3.8), the received word $\overline{\mathbf{y}} = (0\ 1\ 0\ 1\ 1\ 0\ 0)$ generates the syndrome vector of $\mathbf{s} = (1\ 1\ 0)$. Utilizing the look-up table of Table 3.2, the error recovery vector becomes $\mathbf{r} = (1\ 0\ 0\ 0\ 0\ 0\ 0)$. Upon applying the error recovery vector, the received word $\overline{\mathbf{y}}$ is collapsed to one of the legitimate codewords $\mathbf{y}$ in Table 3.1, which is $\widehat{\mathbf{y}} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Assuming that the predicted codeword $\widehat{\mathbf{y}}$ is valid, the demapper decides to translate the predicted codeword $\widehat{\mathbf{y}} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$ to the predicted information bits as $\widehat{\mathbf{x}} = (1\ 1\ 0\ 1)$. Hence, the original information is successfully recovered. The whole process of syndrome calculation, error recovery and demapping jointly form the *decoding* process. It is important to note that in practice, the syndrome calculation, recovery operator and demapper are amalgamated into a single *decoder* block.

Let us now assume that the channel imposes an error pattern beyond the error correction capability of the classical $\mathcal{C}(7,4)$ Hamming code. For example, assume that we send the identical k information bits of $\mathbf{x} = (1\ 1\ 0\ 1)$ while the channel inflicts an error pattern of $\mathbf{e} = (1\ 1\ 0\ 0\ 0\ 0\ 0)$. As a result, we have the received codeword bits of $\overline{\mathbf{y}} = (0\ 0\ 0\ 1\ 1\ 0\ 0)$. Based on the received codeword, we have the syndrome vector of $\mathbf{s} = (0\ 1\ 1)$. Based on the syndrome vector, the error recovery of $\mathbf{r} = (0\ 0\ 1\ 0\ 0\ 0\ 0)$ is chosen. Consequently, the error recovery vector collapses the received word to the incorrect legitimate codeword, which is $\widehat{\mathbf{y}} = (0\ 0\ 1\ 1\ 1\ 0\ 0)$, instead of the correct codeword of $\mathbf{y} = (1\ 1\ 0\ 1\ 1\ 0\ 0)$. Since the demapper assumes that the error recovery completes the task perfectly, the demapper decides that the predicted information bits are $\mathbf{x} = (0\ 0\ 1\ 1)$. Compared to the original information bits, the predicted information bits are considered as an error. This example demonstrates that the classical $\mathcal{C}(7,4)$ Hamming code is unable to operate flawlessly beyond its error correction capability.

3.3 A Brief Review of Quantum Stabilizer Codes

The formulation of QSCs is capable of detecting both the number and the position of errors without actually observing the state of physical qubits, which is vitally important since otherwise, the quantum state will collapse to classical bits upon measurement. This was achieved by amalgamating the classical syndrome-based decoding with the QECCs. Similar to classical error correction codes, QSCs also rely on attaching redundant qubits to the information qubits for invoking error correction. The basic model of QSCs is depicted in Fig. 3.3, which will be contrasted to its classical pair in Fig. 3.2. To generate the codespace $\mathcal{C}$, the redundancy is constituted by $(n-k)$ auxiliary qubits. Next, a unitary transformation $\mathcal{V}$ transforms the k qubits in the state of $|\psi\rangle$ and the $(n-k)$ auxiliary qubits into an n qubits in the state of $|\overline{\psi}\rangle$. The unitary transformation of $\mathcal{V}$ represents the action of the *quantum encoder*. Explicitly, the mapping of the *logical qubits* constituting the state of $|\psi\rangle \in \mathbb{C}^{2^k}$ to the *physical qubits* forming the state of $|\overline{\psi}\rangle \in \mathbb{C}^{2^n}$ by the encoder $\mathcal{V}$ of Fig. 3.3 can be mathematically formulated as follows:

$$\mathcal{C} = \{|\overline{\psi}\rangle = \mathcal{V}(|\psi\rangle \otimes |0\rangle^{\otimes(n-k)})\}. \tag{3.9}$$

The QSCs rely on the stabilizer operators $S_i \in \mathcal{S}$, where $\mathcal{S}$ is the stabilizer set, for identifying the type, the number, and the position of the qubit errors. A stabilizer operator

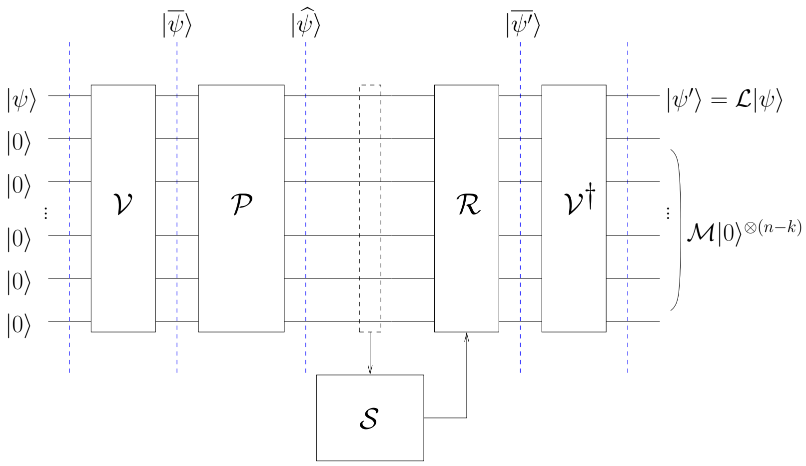


Figure 3.3: The basic model of QSCs implementation over the quantum depolarizing channel. The k logical qubits is mapped into n physical qubits with the aid of $(n-k)$ redundant/auxiliarry qubits (*ancillas*) to provide protection from the quantum decoherence. It is similar to the classical error correction model where $(n-k)$ redundant bits are added to k information bits in order to provide error correction. The quantum encoder $\mathcal{V}$ serves the same purpose with $\mathbf{G}$ of classical error correction codes in Fig. 3.2. The quantum encoder $\mathcal{V}$ transforms the state of k logical qubits $|\psi\rangle$ into the state of n physical qubits $|\overline{\psi}\rangle$ with the aid of $(n-k)$ ancillas. The quantum depolarizing channel imposes vector rerpesented by n-tupple Pauli operator $\mathcal{P} \in \mathcal{P}_n$. The syndrome operators $S_i \in \mathcal{S}$ generate eigenvalues of ± 1, which are analogue to the value 0 and 1 of classical syndrome vector, which is provided by the PCM $\mathbf{H}$ in Fig. 3.2. The error recovery $\mathcal{R}$ applies the correction according to the syndrome values provided by the syndrome measurements. Finally, the quantum inverse encoder $\mathcal{V}^\dagger$ transforms the predicted state of physical qubits $|\overline{\psi'}\rangle$ back to the predicted state of logical qubits $|\psi'\rangle$, which bears the same responsibility as the demapper $\mathbf{D}$ in classical syndrome-based decoding of Fig. 3.2.

S_i is an n-tuple Pauli operator, which preserves the state of physical qubits as defined below:

$$S_i|\overline{\psi}\rangle = |\overline{\psi}\rangle. \tag{3.10}$$

The quantum channel inflicts errors represented by n-tuple Pauli operators $P \in \mathcal{P}_n$, which transforms the encoded physical qubits that were originally in the state of $|\overline{\psi}\rangle$ to the potentially corrupted physical qubits in the state of $|\widehat{\psi}\rangle$, as seen in Fig. 3.3. More explicitly, this process can be described as follows:

$$|\widehat{\psi}\rangle = P|\overline{\psi}\rangle. \tag{3.11}$$

The stabilizer operators act similarly to the syndrome calculations routinely used in classical error correction codes. To elaborate a little further, a stabilizer operator will return an eigenvalue of +1, when an error operator P commutes with the stabilizer operator, while we arrive at the eigenvalue of −1, if it anti-commutes. The eigenvalues of +1 and −1 are analogous to the classic syndrome bit of 0 and 1, respectively, which can be defined as follows:

$$S_i|\widehat{\psi}\rangle = \begin{cases} |\widehat{\psi}\rangle & , \quad S_iP = PS_i \\ -|\widehat{\psi}\rangle & , \quad S_iP = -PS_i. \end{cases} \tag{3.12}$$

Therefore, the stabilizer operators naturally have to inherit the commutative property. Consequently, the product between the stabilizer operators S_i yields another legitimate stabilizer operator. Furthermore, the commutativity property implies that

$$S_i|\overline{\psi}\rangle = S_j|\overline{\psi}\rangle = S_iS_j|\overline{\psi}\rangle = |\overline{\psi}\rangle, \forall S_{i,j} \in \mathcal{S}, \tag{3.13}$$

suggesting that the stabilizer group $\mathcal{S}$ is closed under multiplication.

Based on the syndrome measurement by the stabilizer operators S_i, a recovery operator constituted by the n-tupple Pauli operator of $\mathcal{R} \in \mathcal{P}_n$ seen in Fig. 3.3 is applied to the corrupted physical qubit state $|\widehat{\psi}\rangle$, yielding the predicted state of the original encoded logical qubit $|\overline{\psi'}\rangle$, which is formulated as

$$|\overline{\psi'}\rangle = \mathcal{R}|\widehat{\psi}\rangle. \tag{3.14}$$

Finally, the inverse encoder $\mathcal{V}^\dagger$ of Fig. 3.3 performs the following transformation[1]:

$$\begin{aligned} \mathcal{V}^\dagger|\overline{\psi'}\rangle &= \mathcal{V}^\dagger\mathcal{R}|\widehat{\psi}\rangle \\ &= \mathcal{V}^\dagger\mathcal{R}\mathcal{P}|\overline{\psi}\rangle \\ &= \mathcal{V}^\dagger\mathcal{R}\mathcal{P}\mathcal{V}(|\psi\rangle \otimes |0\rangle^{\otimes(n-k)}) \\ &= (\mathcal{L}|\psi\rangle) \otimes (\mathcal{M}|0\rangle^{\otimes(n-k)}), \end{aligned} \tag{3.15}$$

where we have $\mathcal{V}^\dagger\mathcal{R}\mathcal{P}\mathcal{V} \equiv \mathcal{L} \otimes \mathcal{M}$ and $\mathcal{L} \in \mathcal{P}_k$ represents the error inflicted on the logical qubits according to $|\psi'\rangle = \mathcal{L}|\psi\rangle$, while $\mathcal{M} \in \mathcal{P}_{n-k}$ represents the residual error remained in the $(n-k)$ auxiliary qubits after the error correction procedure. In the case of $\mathcal{R} = \mathcal{P}$, we arrive at $\mathcal{R}\mathcal{P} = \mathbf{I}^{\otimes n}$, where $\mathbf{I}^{\otimes n}$ denotes an n-fold tensor product Pauli-$\mathbf{I}$ matrix. Another possibility is to arrive at $\mathcal{R}\mathcal{P} = S_i$. In either of these cases, the state of the physical qubits is not altered, since we have $\mathcal{R}\mathcal{P}|\overline{\psi}\rangle = |\overline{\psi}\rangle$. Therefore, the decoding procedure of Fig. 3.3 successfully recovers the original quantum state constituted by the logical qubits, yielding $|\psi'\rangle = |\psi\rangle$.

The stabilizer operators can be translated into the classical PCM $\mathbf{H}$ by mapping the Pauli matrices $\mathbf{I}$, $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ onto $(\mathbb{F}_2)^2$ as follows:

$$\begin{aligned} \mathbf{I} &\rightarrow \begin{pmatrix} 0 & | & 0 \end{pmatrix}, \\ \mathbf{X} &\rightarrow \begin{pmatrix} 0 & | & 1 \end{pmatrix}, \\ \mathbf{Y} &\rightarrow \begin{pmatrix} 1 & | & 1 \end{pmatrix}, \\ \mathbf{Z} &\rightarrow \begin{pmatrix} 1 & | & 0 \end{pmatrix}. \end{aligned} \tag{3.16}$$

This concept is also known as the *Pauli-to-binary isomorphism.* By exploiting the Pauli-

---

[1] The inverse encoder $\mathcal{V}^\dagger$ is the Hermitian transpose of encoder $\mathcal{V}$. It is referred to as the *inverse*, since it satisfies the unitary requirement of $\mathcal{V}^\dagger\mathcal{V} = \mathbf{I}$, as the inverse of the matrix does.

to-binary isomorphism, the stabilizer operators of any QSC can be represented as a pair of PCMs $\mathbf{H}_z$ and $\mathbf{H}_z$, where $\mathbf{H}_z$ is invoked for handling the phase-flip ($\mathbf{Z}$) errors and $\mathbf{H}_x$ for handling the bit-flip ($\mathbf{X}$) errors. Explicitly, the classical PCM representation of the QSC stabilizer operators may be written as follows:

$$\mathbf{H} = (\mathbf{H}_z|\mathbf{H}_x)\,. \tag{3.17}$$

The classical representation of the stabilizer operators gives the advantage of predicting and evaluating the performances of QSCs by treating them similarly to classical error correction codes. Additionally, it allows us to transform a pair of classical PCMs into the correponding quantum counterpart. However, to ensure that the commutative property is preserved in the quantum domain, a pair of classical PCMs have to satisfy the so-called *symplectic criterion* [62] given by

$$\mathbf{H}_z \cdot \mathbf{H}_x^T + \mathbf{H}_x \cdot \mathbf{H}_z^T = 0. \tag{3.18}$$

A special class of QSCs, namely the family of CSS codes, treats the phase-flip ($\mathbf{Z}$) and bit-flip ($\mathbf{X}$) errors as two separate entities. More specifically, this can be interpreted as having the PCMs of $\mathbf{H}_z$ and $\mathbf{H}_x$ in Eq. (3.17) formulated as $\mathbf{H}_z = \begin{pmatrix} \mathbf{H}'_z \\ 0 \end{pmatrix}$ and $\mathbf{H}_x = \begin{pmatrix} 0 \\ \mathbf{H}'_x \end{pmatrix}$, respectively. Therefore, the binary PCM $\mathbf{H}$ can be expressed as follows:

$$\mathbf{H} = \left(\begin{array}{c|c} \mathbf{H}'_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}'_x \end{array}\right). \tag{3.19}$$

Consequently, the symplectic criterion given in Eq. (3.18) can be reduced to the following criterion:

$$\mathbf{H}'_z \cdot {\mathbf{H}'_x}^T = 0. \tag{3.20}$$

Furthermore, we can formulate a CSS code by using a PCM of $\mathbf{H}'_z = \mathbf{H}'_x$ and the resultant quantum code may be referred to as a dual-containing quantum CSS code or self-orthogonal quantum CSS code. For dual-containing CSS codes, the symplectic criterion can be further simplified to $\mathbf{H}'_z{\mathbf{H}'_z}^T = 0$.

Again, the classical code constructions can be readily transformed into their quantum version provided that they satisfy the symplectic criterion of Eq. (3.18). The latter constraint prevents us from transplanting some well-known classical codes into the quantum domain. However, fortunately, this limitation can be relaxed by utilizing the family of EA-QSCs [66,67]. The luxury of being able to transform every type of classical codes into QSCs does not come without cost. Invoking the EA-QSC construction requires preshared maximally-entangled qubits before encoding procedure as detailed in [67]. However, the mechanism of presharing the maximally-entangled qubits allows us to transform a set of non-symplectic QSCs into their symplectic counterpart. For a crystal clear illustration, the classification and characterization of the QSCs are summarized in Fig. 3.4.

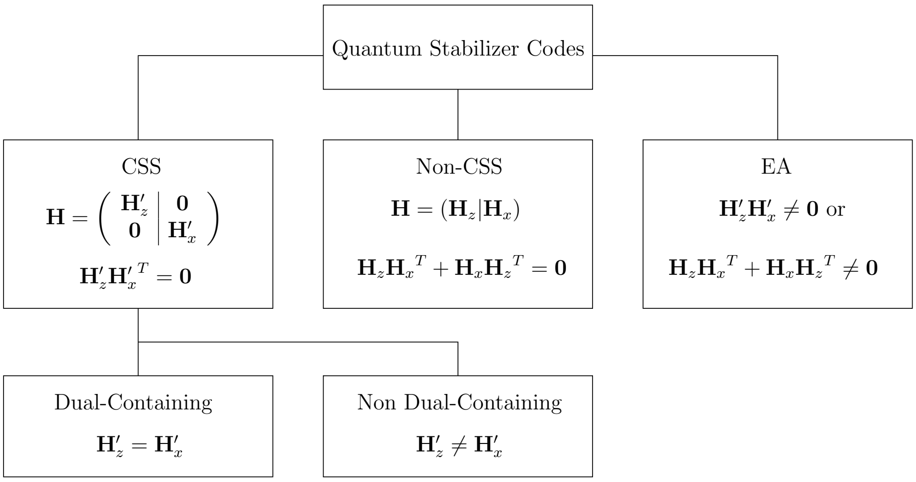


Figure 3.4: The classification and characterization of QSCs, where CSS stands for *Calderbank-Shor-Steane* and EA for *entanglement-assisted.*

3.4 Protecting A Single Qubit: Design Examples

In Chapter 1, we have already mentioned the three pioneering contributions on QSCs, which are only capable of handling a single qubit error, while in Section 3.3, we briefly highlighted the different types of QSC constructions. In this section, we will link up both ideas in a more concrete context.

3.4.1 Classical and Quantum 1/3-rate Repetition Codes

Before we delve deeper into the aforementioned QSCs, let us commence with a simple 1/3-rate classical repetition codes, which maps a binary digit of “0” or “1” into a vector that contains three replicas of each binary digit as

$$\begin{aligned} 0 &\xrightarrow{\mathbf{G}} \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, \\ 1 &\xrightarrow{\mathbf{G}} \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \end{aligned} \tag{3.21}$$

Hence, from this brief description of basic classical codes given in Section 3.2, the mapping in Eq. (3.21) can be encapsulated into a generator matrix **G** as given below:

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \tag{3.22}$$

From the generator matrix **G** given in Eq. (3.22) and the PCM formulation given in Eq. (3.3), we obtain the PCM **H** for a 1/3-rate classical repetition code encapsulated by

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{3.23}$$

where the first row returns the first bit of the two bits syndrome value and acccordingly the second row evaluates the second bit. Thus, it can be easily checked by using the syndrome computation of Eq. (3.8) that the syndrome value of (0 0) is obtained if the received word $\widehat{\mathbf{y}}$ is equal to the valid codeword, either (0 0 0) or (1 1 1). The syndrome computation yields a syndrome vector with $(n-k)$-element and in this case for a 1/3-rate classical repetition code, it generates a synfrome vector with two elements. Therefore, there are four possible outcomes from the syndrome computation and one of them indicates the error-free received word, which is the (0 0) syndrome. Since a 1/3-rate classical repetition code is considered as a short block code, the syndrome computation and the associated error pattern is readily checked using a look-up table, namely Table. 3.3.

Table 3.3: Syndrome computation and the associated error pattern for a 1/3-rate classical repetition code.

Syndrome (**s**)	Error Pattern (**e**)	Index of Corrupted Bit
(0 0)	(0 0 0)	-
(0 1)	(0 0 1)	3
(1 0)	(0 1 0)	2
(1 1)	(1 0 0)	1

Next, we proceed with with a simple 1/3-rate quantum repetition code that capable of recovering a bit-flip error. Let us assume that we have a quantum state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. As the consequence of the *No Cloning Theorem* of quantum mechanics, there is no unitary transformation U capable of mapping an arbitrary quantum state $|\psi\rangle$ onto a state of $|\overline{\psi}\rangle = |\psi\rangle^{\otimes 3}$. However, we are still allowed to make a copy of the orthogonal states. Hence, the code mapping of quantum state $|0\rangle$ and $|1\rangle$ by a unitary transformation U is defined by

$$\begin{aligned} |0\rangle_L &= U\left(|0\rangle \otimes |0\rangle^{\otimes 2}\right) = |000\rangle, \\ |1\rangle_L &= U\left(|1\rangle \otimes |0\rangle^{\otimes 2}\right) = |111\rangle. \end{aligned} \tag{3.24}$$

In a more general scenario, the mapping of a single logical qubits to n physical qubits is carried out by a unitary transformation referred to as quantum encoder $\mathcal{V}$, which can be encapsulated as follows:

$$|\overline{\psi}\rangle = \mathcal{V}\left(|\psi\rangle \otimes |0\rangle^{\otimes(n-1)}\right) = \alpha_0|0\rangle_L + \alpha_1|1\rangle_L, \tag{3.25}$$

where $|0\rangle_L$ denotes the encoded state of the logical qubit $|0\rangle$, $|1\rangle_L$ denotes the encoded state of logical qubit $|1\rangle$, while $|0\rangle^{\otimes n-1}$ represents the auxiliary or the redundant qubits (*ancillas*), and the superscript of $\otimes(n-1)$ represents $(n-1)$-fold of tensor products. Hence, for 1/3-rate quantum repetition codes, the state of the logical qubit $|\psi\rangle$ corresponds to the state of the physical qubit $|\overline{\psi}\rangle$ as given by

$$|\overline{\psi}\rangle = \mathcal{V}\left((\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle^{\otimes 2}\right) = \alpha_0|000\rangle + \alpha_1|111\rangle, \tag{3.26}$$

where the $|000\rangle$ defines the encoded logical qubit $|0\rangle_L$ and $|111\rangle$ defines the $|1\rangle_L$. Again, it is important to bear in mind that the state of $|\overline{\psi}\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$ is not equal to $|\overline{\psi}\rangle = |\psi\rangle^{\otimes 3}$. More explicitly, this relationship can also be expressed as $|\overline{\psi}\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle \neq |\psi\rangle^{\otimes 3}$. The state of the physical qubits of the 1/3-rate quantum repetition code is stabilized, or synonymously 'parity-checked' by the pair of stabilizer operators $S_1 = \mathbf{ZZI}$ and $S_2 = \mathbf{ZIZ}$. A valid codeword or a valid encoded state, which is not affected by the stabilizer operators S_1 and S_2, has an input state of $|\overline{\psi}\rangle$ and returns the state of $|\overline{\psi}\rangle$, hence it yields the so-called eigenvalues of +1, and more explicitly, it is described below:

$$\begin{aligned} S_1|\overline{\psi}\rangle &= \alpha_0|000\rangle + \alpha_1|111\rangle \equiv |\overline{\psi}\rangle, \\ S_2|\overline{\psi}\rangle &= \alpha_0|000\rangle + \alpha_1|111\rangle \equiv |\overline{\psi}\rangle. \end{aligned} \tag{3.27}$$

By contrast, if the stabilizer operators g_1 and g_2 are applied to the corrupted states $|\widehat{\psi}\rangle$, they both yield eigenvalues that are not in the all one state. For instance, let us assume that we received a corrupted state having a bit-flip error imposed on the first qubit of $|\overline{\psi}\rangle$ yielding $|\widehat{\psi}\rangle = \alpha_0|100\rangle + \alpha_1|011\rangle$. Then, upon applying the stabilizer operators $S_1 = \mathbf{ZZI}$ and $S_2 = \mathbf{ZIZ}$ to the state of $|\widehat{\psi}\rangle$, it may be readily showed after few steps that we arrive at the following eigenvalues:

$$\begin{aligned} S_1|\widehat{\psi}\rangle &= \mathbf{ZZI}(\alpha_0|100\rangle + \alpha_1|011\rangle) \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \alpha_1 \\ \alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -\alpha_1 \\ -\alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ &\equiv -\alpha_0|100\rangle - \alpha_1|011\rangle \equiv -|\widehat{\psi}\rangle, \end{aligned} \tag{3.28}$$

$$
\begin{aligned}
S_2|\widehat{\psi}\rangle &= \mathbf{ZIZ}(\alpha_0|100\rangle + \alpha_1|011\rangle) \\
&= \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ \alpha_1 \\ \alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ -\alpha_1 \\ -\alpha_0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \\
&\equiv -\alpha_0|100\rangle - \alpha_1|011\rangle \equiv -|\widehat{\psi}\rangle. \qquad (3.29)
\end{aligned}
$$

The resultant eigenvalues of ±1 act similarly to the syndrome vector of classical codes, where the eigenvalue +1 is associated with the classical syndrome value 0 and the eigenvalue −1 with the classical syndrome value 1. More explicitly, the single-qubit error patterns imposed on the 1/3-rate quantum repetition codes and the associated eigenvalues are portrayed in Table. 3.4. However, this specific construction is only capable of detecting and correcting a single bit-flip error imposed by the Pauli channel on the physical qubits, but no phase-flips.

Table 3.4: Single qubit bit-flip errors along with the associated eigenvalues in 1/3-rate quantum repetition where the eigenvalues act similarly with the syndrome values in classical linear block codes.

Received States $\lvert\widehat{\psi}\rangle$	Eigenvalue $g_1\lvert\widehat{\psi}\rangle$	Eigenvalue $g_2\lvert\widehat{\psi}\rangle$	Syndrome ($\mathbf{s}$)	Index of Corrupted Qubit
$\alpha_0\lvert 000\rangle + \alpha_1\lvert 111\rangle$	+1	+1	(0 0)	-
$\alpha_0\lvert 001\rangle + \alpha_1\lvert 110\rangle$	+1	−1	(0 1)	3
$\alpha_0\lvert 010\rangle + \alpha_1\lvert 101\rangle$	−1	+1	(1 0)	2
$\alpha_0\lvert 100\rangle + \alpha_1\lvert 011\rangle$	−1	−1	(1 1)	1

Since the physical qubits may experience not only bit-flip errors, but also phase-flip errors as well as both bit-flip and phase-flip errors, different mapping is necessitated to protect the physical qubits from phase-flip error. In order to protect the physical qubits from a phase-flip error, we may require a different basis but we can still invoke a similar approach. To elaborate further, the Hadamard transformation ($\mathbf{H}$) maps the computational basis of $\{|0\rangle, |1\rangle\}$ onto the Hadamard basis of $\{|+\rangle, |-\rangle\}$, where the state of $|+\rangle$ and $|-\rangle$ are defined as

$$|+\rangle \equiv \mathbf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad (3.30)$$

$$|-\rangle \equiv \mathbf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{3.31}$$

and the unitary Hadamard transformation **H**, which acts on a single qubit state, is given by

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.32}$$

A phase-flip error defined over the Hadamard basis of $\{|+\rangle, |-\rangle\}$ acts similarly to the bit-flip error defined over the computational basis of $\{|0\rangle, |1\rangle\}$. Hence, for handling of a single phase-flip error, the code mapping of 1/3-rate quantum repetition codes are given by

$$\begin{aligned} |0\rangle_L &= U\left(|0\rangle \otimes |0\rangle^{\otimes 2}\right) = |+++\rangle, \\ |1\rangle_L &= U\left(|1\rangle \otimes |0\rangle^{\otimes 2}\right) = |---\rangle. \end{aligned} \tag{3.33}$$

Hence, the logical qubit of $|\psi\rangle$ corresponding to the physical qubits $|\overline{\psi}\rangle$ is given by

$$|\overline{\psi}\rangle = \mathcal{V}\left((\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle^{\otimes 2}\right) = \alpha_0|+++\rangle + \alpha_1|---\rangle, \tag{3.34}$$

The state of physical qubits given in Eq. (3.34) can be stabilized by the operators $S_1 = \mathbf{XXI}$ and $S_2 = \mathbf{XIX}$. The detection and correction of a phase flip error can be carried out in analogy with the 1/3-rate quantum repetition code for handling the bit-flip error. The stabilizer operators can be derived from the classical PCM **H** by mapping the Pauli matrices **I**, **X**, **Y** and **Z** onto $(\mathbb{F}_2)^2$ using Pauli mapping given in Eq. 3.16. Each row of **H** is associated with a stabilizer operator $S_i \in \mathcal{S}$, where the i-th column of both $\mathbf{H}_z$ and $\mathbf{H}_x$ corresponds to the i-th qubit and the binary 1 locations represent the **Z** and **X** positions in the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$, respectively. For instance, for the 1/3-rate quantum repetition code, which is stabilized by the operators $S_1 = \mathbf{ZZI}$ and $S_2 = \mathbf{ZIZ}$, the PCM **H** is given as follows:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right). \tag{3.35}$$

Since the 1/3-rate quantum repetition code in this example can only correct a bit-flip (**X**) error, which is stabilized by the **Z** operators, the PCM $\mathbf{H}_x$ contains only zero elements. The same goes for a 1/3-rate quantum repetition code conceived for handling a phase-flip (**Z**) error, which is stabilized by the operators $S_1 = \mathbf{XXI}$ and $S_2 = \mathbf{XIX}$. The PCM **H** corresponding to this particular QSC is defined as follows:

$$\mathbf{H} = \left(\begin{array}{ccc|ccc} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right). \tag{3.36}$$

It is clearly shown in Eq. (3.35) and (3.36) that the PCM of a 1/3-rate quantum repetition code is similar to that of the 1/3-rate classical repetition code given in Eq. (3.23).

In order to encode the logical qubits into physical qubits, we require the unitary transformation $\mathcal{V}$ acting as the quantum encoder. To represent the quantum encoding circuit, one of the essential components is the controlled-NOT (CNOT) quantum gate, which has been described in Subsection 2.3.1.4. A logical qubit in the superimposed state of $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and a qubit in the pure state of $|0\rangle$ are manipulated by the quantum CNOT gate into following state:

$$\begin{aligned}
\mathbf{CNOT}(|\psi\rangle, |0\rangle) &= \mathbf{CNOT}(\alpha_0|0\rangle + \alpha_1|1\rangle, |0\rangle) \\
&= \mathbf{CNOT}(\alpha_0|00\rangle + \alpha_1|10\rangle) \\
&= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha_{00} \\ 0 \\ \alpha_{10} \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ 0 \\ 0 \\ \alpha_1 \end{pmatrix} \\
&\equiv \alpha_0|00\rangle + \alpha_1|11\rangle. \qquad (3.37)
\end{aligned}$$

Similarly, we may also use the CNOT definition given in Eq. (2.33) to determine the resultant state as described below:

$$\begin{aligned}
\mathbf{CNOT}(|\psi\rangle, |0\rangle) &= \mathbf{CNOT}(\alpha_0|0\rangle + \alpha_1|1\rangle, |0\rangle) \\
&= \mathbf{CNOT}(\alpha_0|00\rangle + \alpha_1|10\rangle) \\
&= \alpha_0|0, (0 \oplus 0)\rangle + \alpha_1|1, (1 \oplus 0)\rangle \\
&= \alpha_0|00\rangle + \alpha_1|11\rangle. \qquad (3.38)
\end{aligned}$$

For the sake of creating the encoded state of 1/3-rate quantum repetition code, we require a single logical qubit and two ancillas prepared in the pure state of $|0\rangle$, as described in Eq. (3.26). In the first step, the CNOT unitary transformation is performed between the logical qubit and the first ancilla, in which the logical qubit acts as the control qubit and the ancilla as the target qubit. The same step is repeated during the second stage between the logical qubit and the second ancilla, where the second ancilla is also preserved as the target qubit. Therefore, the encoding circuit of the 1/3-rate quantum repetition code can be represented as in Fig 3.5, which was designed for protecting the physical qubits from a single bit-flip error, as also seen in the mapping given in Eq. (3.24). For its 1/3-rate quantum repetition code counterpart protecting the physical qubits from a phase-flip error, we require the Hadamard transformation to obtain the mapping given in Eq. (3.33). The Hadamard transformation is required for changing the base of quantum repetition codes from the computational basis $\{|0\rangle, |1\rangle\}$ to the Hadamard basis $\{|+\rangle, |-\rangle\}$. Hence, we can readily create the encoding circuit for a 1/3-rate quantum repetition code for protecting the physical qubits from a phase-flip error by placing the Hadamard gates after the second stage as portrayed in Fig. 3.6.

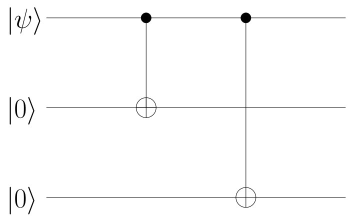


Figure 3.5: The encoding circuit of the 1/3-rate quantum repetition code protecting the physical qubits from a bit-flip error.

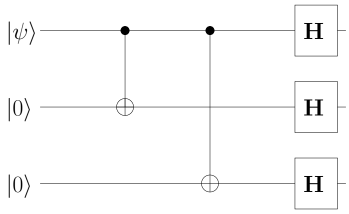


Figure 3.6: The encoding circuit of the 1/3-rate quantum repetition code protecting the physical qubits from a phase-flip error.

3.4.2 Shor's 9-Qubit Code

Since we have elaborated briefly on the construction of QSCs along with the Pauli to binary isomorphism, we may now proceed with the corresponding examples of different QSC constructions conceived for protecting the physical qubits from any type of a single qubit error. Firstly, we start with the Shor's code [56]. In order to protect the qubits from any type of single qubit error, a logical qubit is mapped onto nine physical qubits. This code may also be viewed as a concatenated version of two 1/3-rate quantum repetition codes, where the first stage is dedicated to the protection of the physical qubits from phase-flip errors, while the second stage is invoked for handling the bit-flip errors. To elaborate further, at the first stage of Shor's code, the state of a logical qubit is encoded by using the following mapping: $|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$. At the second stage, we encode each of the states of $|+\rangle$ to the state of $\left(|000\rangle + |111\rangle\right)/\sqrt{2}$, while the state of $|-\rangle$ is mapped to the state of $\left(|000\rangle - |111\rangle\right)/\sqrt{2}$. Therefore, the final state of the encoded logical qubits $|0\rangle_L$ and $|1\rangle_L$ are encapsulated as follows:

$$\begin{aligned}
|0\rangle_L &= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \\
&= \frac{1}{2\sqrt{2}}(|000000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \\
&+ |111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle), \qquad (3.39)\\
|1\rangle_L &= \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right) \\
&= \frac{1}{2\sqrt{2}}(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle \\
&- |111000000\rangle + |111000111\rangle + |111111000\rangle - |111111111\rangle). \qquad (3.40)
\end{aligned}$$

Based on the given description, the encoding circuit of Shor's code is portrayed in Fig. 3.7. The state determined by the nine physical qubits of Shor's code, where the latter defined in Eq. (3.39) and (3.40), is stabilized by the eight stabilizer operators which are listed in Table 3.5.

Table 3.5: The eight stabilizer operators of Shor's 9-qubit code, which stabilizes a single logical qubit with the aid of eight auxiliarry qubits.

S_i	Stabilizer Operator
S_1	**ZZIIIIIII**
S_2	**IZZIIIIII**
S_3	**IIIZZIIII**
S_4	**IIIIZZIII**
S_5	**IIIIIIZZI**
S_6	**IIIIIIIZZ**
S_7	**XXXXXXIII**
S_8	**IIIXXXXXX**

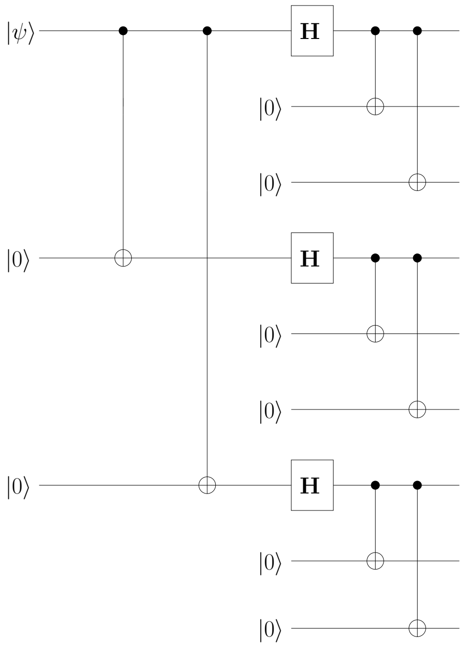


Figure 3.7: The encoding circuit $\mathcal{V}$ of Shor's 9-qubit code.

To elaborate a little further, Shor's code is a member of the class of non-dual-containing CSS codes. Explicitly, it belongs to the class of CSS codes because the stabilizer formalism of Shor's code implies that the code handles the **Z** error and the **X** error separately, whilst it is a non-dual-containing because the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ are not identical. Based on the list of stabilizer operators given in Table 3.5, the PCM **H** of Shor's code is given in Eq. (3.41), where each row of the PCM corresponds to each of the stabilizer operators listed in Table 3.5.

$$\mathbf{H}_{Shor} = \left(\begin{array}{ccccccccc|ccccccccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}\right). \tag{3.41}$$

The quantum coding rate (r_Q) of a quantum code $\mathcal{C}[n,k]$ is defined by the ratio of the number of logical qubits k to the number of physical qubits n, which can be formulated as

$$r_Q = \frac{k}{n}. \tag{3.42}$$

Hence again, for a Shor's 9-qubit code the quantum coding rate is $r_Q = 1/9$.

3.4.3 Steane's 7-Qubit Code

Steane's code was proposed to protect a single qubit from any type of error by mapping a logical qubit onto seven physical qubits, instead of nine qubits. In contrast to Shor's code, Steane's code is a dual-containing CSS code, since the PCMs $\mathbf{H}_z$ and $\mathbf{H}_x$ are equal to that of clasical Hamming code $\mathbf{H}_{Ham}$, which is given by

$$\mathbf{H}_{Ham} = \begin{pmatrix}
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1
\end{pmatrix}. \tag{3.43}$$

It can be confimed that the classical Hamming code is a dual-containing code, because it satisfies the condition $\mathbf{H}_{Ham}.\mathbf{H}_{Ham}^T = 0$. Therefore, the PCM $\mathbf{H}$ of Steane's code is defined as shown in Eq. (3.44).

$$\mathbf{H}_{Steane} = \left(\begin{array}{c|c} \mathbf{H}_{Ham} & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_{Ham} \end{array}\right) = \left(\begin{array}{ccccccc|ccccccc}
1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1
\end{array}\right). \tag{3.44}$$

Since Steane's code is a member of the dual-containing CSS codes, the encoded state of the logical qubit $|0\rangle_L$ and $|1\rangle_L$ may be determined from its classical code counterpart. Let $\mathcal{C}_1(7,4)$ be the Hamming code and $\mathcal{C}_2(7,3)$ be its dual. Both of the codes are capable of corrrecting one bit error. Hence, the resultant CSS quantum code derived from these codes, namely the $\mathcal{C}[n, k_1 - k_2] = \mathcal{C}[7,1]$, also capable of correcting a single qubit error. For

Steane's code the states of encoded logical qubit of $|0\rangle_L$ and $|1\rangle_L$ are defined as follows:

$$|0\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{x \in \mathcal{C}_1, \mathcal{C}_2} |x\rangle, \tag{3.45}$$

$$|1\rangle_L = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{x \in \mathcal{C}_1, x \notin \mathcal{C}_2} |x\rangle. \tag{3.46}$$

Since $\mathcal{C}_2$ is the dual of $\mathcal{C}_1$, by definition the PCM of $\mathcal{C}_2$, denoted by $\mathbf{H}(\mathcal{C}_2)$ is the generator matrix of $\mathcal{C}_1$, denoted by $\mathbf{G}(\mathcal{C}_1)$. Hence, the parity-check matrix of $\mathcal{C}_2$ can be written as

$$\mathbf{H}(\mathcal{C}_2) = \mathbf{G}(\mathcal{C}_1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{3.47}$$

Table 3.6: The code space of $\mathcal{C}_1$ and $\mathcal{C}_2$ for determining the encoded state of the Steane's code.

$x \in \mathcal{C}_1, \mathcal{C}_2$	$x \in \mathcal{C}_1, x \notin \mathcal{C}_2$
0000000	1111111
0111001	1000110
1011010	0100101
1100011	0011100
1101100	0010011
1010101	0101010
0110110	1001001
0001111	1110000

Based on the PCM given in Eq. (3.43) and (3.47), we can define the code space of $\mathcal{C}_1$ and $\mathcal{C}_2$, which is described in Table 3.6. Finally, using Eq. (3.45), (3.46), and also the code space given in Table 3.6, the encoded states of the logical qubit $|0\rangle_L$ and $|1\rangle_L$ of the Steane's code are as follows:

$$\begin{aligned} |0\rangle_L = \frac{1}{2\sqrt{2}}(&|00000000\rangle + |0111001\rangle + |1011010\rangle + |1100011\rangle \\ &+ |1101100\rangle + |1010101\rangle + |0110110\rangle + |0001111\rangle), \end{aligned} \tag{3.48}$$

$$\begin{aligned} |1\rangle_L = \frac{1}{2\sqrt{2}}(&|1111111\rangle + |1000110\rangle + |0100101\rangle + |0011100\rangle \\ &+ |0010011\rangle + |0101010\rangle + |1001001\rangle + |1110000\rangle). \end{aligned} \tag{3.49}$$

It can be readily seen that the quantum coding rate of Steane's 7-qubit code is 1/7. The encoding circuit of the Steane's 1/7-rate code can be seen in Fig. 3.8.

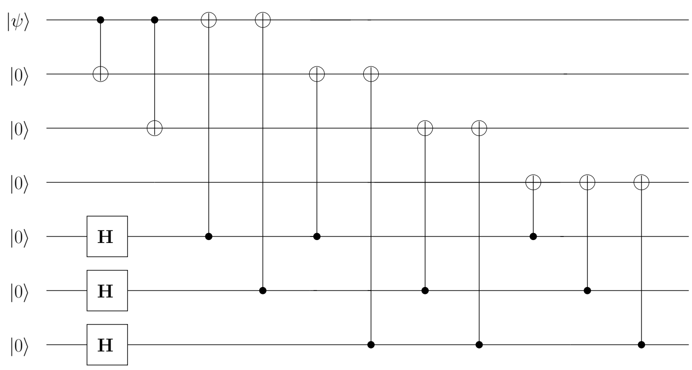


Figure 3.8: The encoding circuit $\mathcal{V}$ of Steane's 7-qubit code.

Table 3.7: The stabilizer operators of the Steane's 7-qubit code.

S_i	Stabilizer Operator
S_1	**ZZIZZII**
S_2	**ZIZZIZI**
S_3	**IZZZIIZ**
S_4	**XXIXXII**
S_5	**XIXXIXI**
S_6	**IXXXIIX**

3.4.4 Laflamme's 5-Qubit Code - The Perfect Code

Laflamme's code maps a single logical qubit onto a five physical qubits. Laflamme's code is also referred to as the "perfect code", because it has been proven that in order to protect a logical qubit, the lowest number of physical qubits required is five [59, 60]. The perfect 5-qubit code is a non-CSS code, since the stabilizer formalism is designed to handle the **Z** errors and **X** errors simultaneously. There are several existing designs related to the perfect 5-qubit code [58, 131] and in this treatise, we use the PCM formulation given in [131]. Explicitly, its non-CSS characteristics can be readily observed from the PCM $\mathbf{H}_{perfect}$ of the 5-qubit perfect code, which is specified as follows:

$$\mathbf{H}_{perfect} = \left(\begin{array}{ccccc|ccccc} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right). \tag{3.50}$$

Hence, the stabilizer operators of the 5-qubit code may be explicitly formulated as in Table 3.8.

In general, the encoded state of a QSC which encodes a single-logical qubit into n

Table 3.8: The stabilizer formalism of the perfect 5-qubit code.

S_i	Stabilizer Operator
S_1	**XZZXI**
S_2	**IXZZX**
S_3	**XIXZZ**
S_4	**ZXIXZ**

physical qubits can defined as follows [138]:

$$|0\rangle_L = \prod_{S_i \in \mathcal{S}} \frac{1}{\sqrt{N}} \left(\mathbf{I}^{\otimes n} + S_i\right) |0\rangle^{\otimes n}, \tag{3.51}$$

$$|1\rangle_L = \prod_{S_i \in \mathcal{S}} \frac{1}{\sqrt{N}} \left(\mathbf{I}^{\otimes n} + S_i\right) |1\rangle^{\otimes n}, \tag{3.52}$$

where the factor N is introduced to preserve the unitary constraint. Therefore, based on the stabilizer operators as well as on Eq. (3.51) and (3.52), the encoded state of Laflamme's 5-qubit code can be defined as follows:

$$\begin{aligned}|0\rangle_L = \frac{1}{\sqrt{N}} &\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right) \\ &\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)|0\rangle^{\otimes 5}, \end{aligned} \tag{3.53}$$

$$\begin{aligned}|1\rangle_L = \frac{1}{\sqrt{N}} &\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right) \\ &\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)\left(\mathbf{I}^{\otimes 5} + \mathbf{XZZXI}\right)|1\rangle^{\otimes 5}. \end{aligned} \tag{3.54}$$

Finally, we obtain

$$\begin{aligned}|0\rangle_L = \frac{1}{4}(&|00000\rangle - |00011\rangle + |00101\rangle - |00110\rangle + |01001\rangle + |01010\rangle - |01100\rangle - |01111\rangle \\ &- |10001\rangle + |10010\rangle + |10100\rangle - |10111\rangle - |11000\rangle - |11011\rangle - |11101\rangle - |11110\rangle),\end{aligned} \tag{3.55}$$

$$\begin{aligned}|1\rangle_L = \frac{1}{4}(&|11111\rangle - |11100\rangle + |11010\rangle - |11001\rangle + |10110\rangle + |10101\rangle - |10011\rangle - |10000\rangle \\ &- |01110\rangle + |01101\rangle + |01011\rangle - |01000\rangle - |00111\rangle - |00100\rangle - |00010\rangle - |00001\rangle).\end{aligned} \tag{3.56}$$

The same method can be utilized for determining the encoded state of a logical qubit for Shor's code and Steane's code. However, both Shor's code and Steane's code offer a more simplistic approach for determining their corresponding encoded states. The description for the efficient encoding circuit $\mathcal{V}$ for the 1/5-rate Laflamme's code can be found in [58, 148, 149].

Based on the aforementioned constructions, we evaluated the performance of the QSCs by simulation, in the context of quantum depolarizing channel. The performance of 9-qubit Shor's code, 7-qubit Steane's code and 5-qubit Laflamme's code are portrayed in Fig. 3.9

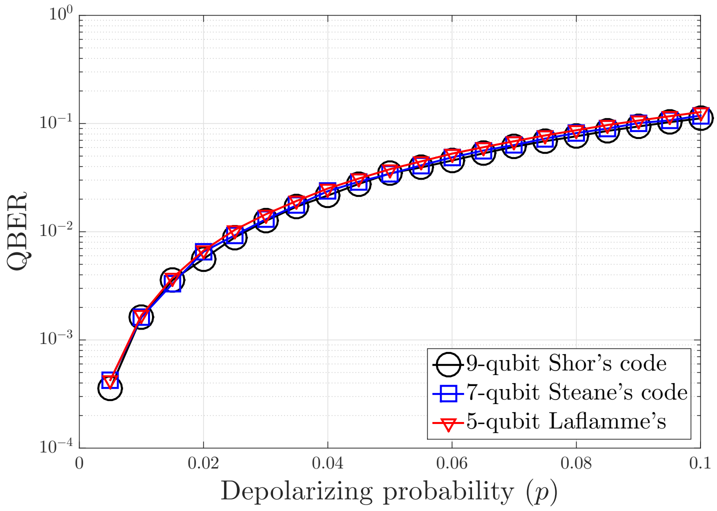


Figure 3.9: QBER performance of the QSCs protecting a single qubit, namely Shor's 9-qubit code, Steane's 7-qubit code and the perfect 5-qubit code, recorded for the quantum depolarizing channel. The similarity of performances is because all of the QSCs rely on hard-decision syndrome decoding and they all have the same error correction capabilities.

in terms of the qubit error rate (QBER) on given depolarizing probability (p). From the simulation result, it can be observed clearly that the performances of all three QSCs are quite similar. The similarity in performances is expected because all of the codes have the same error correction capability of correcting a single-qubit error. Also, they utilize the hard decision decoding based on syndrome measurement. From this result, we may conclude that for different codes with the same error correction capability, wherein classical coding theory it will be translated into the minimum distance property, they are associated with similar performances even though all of the codes have different codeword length. In this case, all of the QSCs have a single qubit error correction capability ($t = 1$), and it may be translated as the minimum distance of three ($d = 3$), but having different codeword length, 9-qubit, 7-qubit and 5-qubit for Shor's code, Steane's code and Laflamme's code, respectively. Another fact that we should point out that the three codes exhibit different code constructions. Shor's code belongs to non dual-containing CSS codes, while Steane's code is a member of dual-containing CSS codes, and finally, Laflamme's code or the perfect 5-qubit code has a construction of non-CSS codes.

3.5 Summary and Conclusions

The purpose of this chapter is to provide the similarities between the classical and quantum error correction codes. More specifically, the QSCs can be viewed as the syndrome-based version of QECCs, as exemplified by the 1/3-rate quantum repetition code. By using the classical-to-quantum Pauli isomorphism, we can observe that a QSC can be treated as a syndrome-based classical error-correction code, whose PCM can be separated into two independent PCMs, one for dealing with bit-flip ($\mathbf{X}$) errors, which is the PCM $\mathbf{H}_x$, and one for handling the phase-flip ($\mathbf{Z}$) errors, which is the PCM $\mathbf{H}_z$. Based on how to mitigate the **X** and the **Z** errors, a QSC can be classified either as a CSS code or a non-CSS code. The main difference between the two is the CSS codes handle the **X** and the **Z** errors independently, as exemplified by the PCMs of the Shor's code and the Steane's code, while the non-CSS codes treat them simultaneously, as exemplified by the PCM of the Laflamme's code.

We have simulated the QBER performance for the Shor's, Steane's and the Laflamme's code over the quantum depolarizing channel. The simulation results show a similar QBER performance for all of the aforementioned codes. The main reason is all of Shor's, Steane's and Laflamme's code exhibit the same minimum distance ($d = 3$), which translates directly to the error correction capability of the code ($t = 1$) despite of their differences in code type, codeword length and and quantum coding rate. Therefore, we believe that the trade-off between conflicting parameters in QSCs such as minimum distance, quantum coding rate and codeword length is a pivotal subject to investigate. This specific line of investigation will be carried out in Chapter 4.

Chapter 4

Quantum Coding Bounds and a Closed-Form Approximation of the Minimum Distance versus Quantum Coding Rate

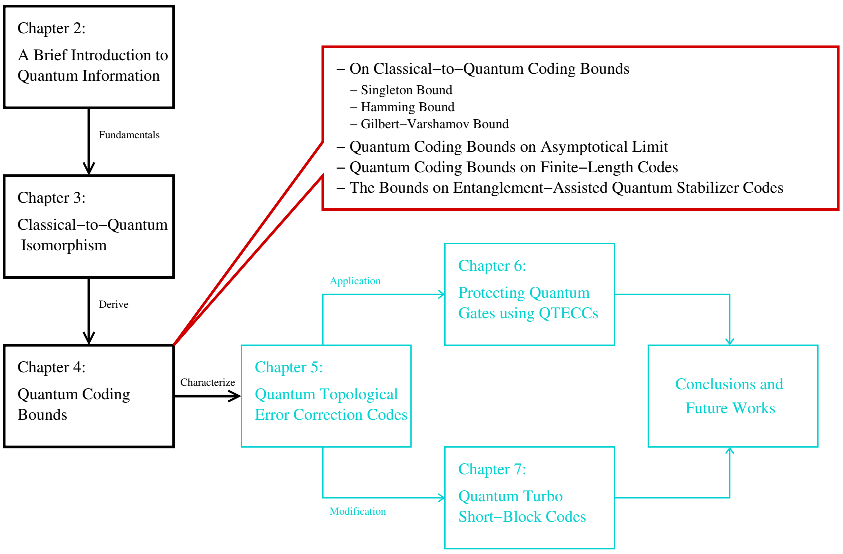


Figure 4.1: The outline of this thesis with the highlight of Chapter 4.

4.1 Introduction

The trade-off between the coding rate and the minimum distance as well as the codeword length is widely acknowledged in designing classical error correction codes. Since most of the QSCs are derived from their classical counterparts, the same problem persists. Even though extensive efforts have been invested in designing the QSCs, the question of how to determine the realistically achievable minimum distance d of a QSC given the quantum coding rate r_Q and codeword length n remains unresolved. For example, for a given codeword length of $n = 128$ and quantum coding rate of $r_Q = 1/2$, the achievable minimum distance is loosely bounded by $11 < d < 22$, while for $n = 1024$ and $r_Q = 1/2$, the achievable minimum distance is bounded by $78 < d < 157$. Naturally, having such a wide range of estimated minimum distance is undesirable. For binary classical codes, this problem has been circumvented by the closed-form approximation proposed by Akhtman *et al.* [93]. Therefore, in this chapter, we present an appealingly simple and invertible closed-form approximation for determining the realistically achievable minimum distance of a QSC, given the codeword length n and the quantum coding rate r_Q. Our formulation is suitable for both the idealized asymptotical case and for the practical finite-length codeword. Furthermore, our proposed closed-form approximation is also applicable to the family of EA-QSCs.

This chapter is organized as follows. In Section 4.2, we survey the existing quantum coding bounds and derive the bounds by exploiting the classical-to-quantum isomorphism. This is followed by our closed-form approximation proposed for the idealized asymptotical limit in Section 4.3. Since the asymptotical limit has limited relevance when it comes to practical implementations, we also propose an approximation for practical finite-length codewords. To unify the quantum coding bounds approximation for both entanglement-assisted and unassisted QSCs, we derive a closed-form approximation for arbitrarily entangled QSCs in Section 4.5. Finally, we conclude this chapter in Section 4.6.

4.2 On Classical to Quantum Coding Bounds

In this section, we present the classical to the quantum version of the most well-known coding bounds, namely the Singleton bound [150] and Hamming bound [151], which serve as the upper bounds, as well as the Gilbert-Varshamov (GV) bound [152], which acts as the lower bound. Although there are several ways of deriving the coding bounds in the quantum domain, we are interested in exploring the duality of coding bounds in the classical and quantum domain. Therefore, we present the derivation of quantum coding bounds using the classical to quantum isomorphism approach and demonstrate that the final results agree with the coding bounds that are derived from a purely quantum domain perspective.

4.2.1 Singleton Bound

The Singleton bound of classical binary code constructions $\mathcal{C}(n, k, d)$ is defined as

$$n - k \geq d - 1, \tag{4.1}$$

where the notation n denotes the codeword length, k for the length of information bits, and d for minimum distance amongst the codewords in codebook $\mathcal{C}$. Singleton bound acts as an upper bound in classical code constructions. The bound implies that the number of rows in a PCM associated with the length of syndrome vector, which is equal to $(n-k)$, has to be greater than $(d-1)$. For the QSC $\mathcal{C}[n,k,d]$, the rows of PCM correspond to the number of stabilizer operators. Since the stabilizer formalism has to correct both the bit-flip errors and the phase-flip errors, the classical Singleton bound of Eq. (4.1) can be readily transformed into the quantum Singleton bound as follows:

$$n-k \geq 2(d-1), \tag{4.2}$$

where n now may also be referred to as the number of physical qubits and k is the number of logical qubits. In order to show explicitly the trade-off between the minimum distance and the quantum coding rate, Eq. (4.2) can be modified to

$$\frac{k}{n} \leq 1-2\left(\frac{d-1}{n}\right). \tag{4.3}$$

In the quantum domain, the Singleton bound is also known as the Knill-Laflamme bound [87]. The QSCs achieving the quantum Singleton bound by satisfying the equality are classified as the quantum Maximum Separable Distance (MDS) codes. One of the well-known QSCs having a minimum distance $d=3$ that reaches the quantum Singleton bound is the perfect 5-qubit code $\mathcal{C}[n,k,d]=\mathcal{C}[5,1,3]$.

4.2.2 Hamming Bound

In classical binary coding, a codebook $\mathcal{C}(n,k,d)$ maps the information words containing k bits into a codeword of length n bits. The maximal number of errors, which is denoted by t that can be corrected by codebook $\mathcal{C}$ is given by

$$t=\lfloor\frac{d-1}{2}\rfloor. \tag{4.4}$$

Therefore the maximum size of a binary codebook $|\mathcal{C}|=2^k$ is bounded by the sphere-packing bound which is defined as:

$$2^k \leq \frac{2^n}{\sum\limits_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}}. \tag{4.5}$$

Since the QSCs have to correct three different types of error namely the bit-flip errors ($\mathbf{X}$), phase-flip errors ($\mathbf{Z}$), as well as both bit-flip and phase-flip errors ($\mathbf{Y}$), the size of the codebook for a QSC $\mathcal{C}[n,k,d]$ is now bounded by

$$2^k \leq \frac{2^n}{\sum\limits_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}3^j}. \tag{4.6}$$

By modifying Eq. (4.6), we can express explicitly the bound of the quantum coding rate as a function of the minimum distance d and codeword length n, as shown below:

$$\frac{k}{n} \leq 1 - \frac{1}{n} \log_2 \left(\sum_{j=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{j} 3^j \right). \tag{4.7}$$

If n tends to ∞, we obtain

$$\frac{k}{n} \leq 1 - \left(\frac{d}{2n} \right) \log_2 3 - H\left(\frac{d}{2n} \right), \tag{4.8}$$

where $H(x)$ is the binary entropy of x formulated as $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$. Equation (4.7) and (4.8) are also known as the quantum Hamming bound [60], which also constitutes the upper bound for QSC constructions.

4.2.3 Gilbert-Varshamov Bound

The same analogy exploited to derive the quantum Hamming bound may also be used for transforming the classical Gilbert-Varshamov (GV) bound, namely the lower bound for classical code constructions, into its quantum counterpart. In the classical domain, the GV bound for classical codes $\mathcal{C}(n, k, d)$ is formulated as

$$2^k \geq \frac{2^n}{\sum\limits_{j=0}^{d-1} \binom{n}{j}}. \tag{4.9}$$

Considering that the QSCs have to tackle three different types of errors, the size of the codebook $\mathcal{C}[n, k, d]$ is bounded by

$$2^k \geq \frac{2^n}{\sum\limits_{j=0}^{d-1} \binom{n}{j} 3^j}. \tag{4.10}$$

Hence, we can readily derive the quantum GV bound, the lower bound of the quantum coding rate as a function of the minimum distance d and codeword length n as follows:

$$\frac{k}{n} \geq 1 - \frac{1}{n} \log_2 \left(\sum_{j=0}^{d-1} \binom{n}{j} 3^j \right). \tag{4.11}$$

Again, if n aprroaches ∞, we obtain

$$\frac{k}{n} \geq 1 - \left(\frac{d}{n} \right) \log_2 3 - H\left(\frac{d}{n} \right), \tag{4.12}$$

where $H(x)$ is the binary entropy of x. The quantum GV bounds in Eq. (4.11) and (4.12) are valid for non-CSS QSCs. However, a special case should be considered for dual-containing quantum CSS codes. It will be shown in Section 4.4 that for some dual-containing CSS codes the code constructions violate the quantum GV bound. Hence, a special bound has to be derived to accomodate the dual-containing CSS codes. In the classical domain, a binary code $\mathcal{C}(n, k, d)$ maps a k-bit information word into an n-bit encoded codeword. The number of syndrome measurement operators is determined by the number of rows in the PCM $\mathbf{H}$ of $\mathcal{C}(n, k, d)$, which is equal to $(n - k)$. With a simple modification of Eq. (4.9), the number of syndrome measurement operators in $\mathcal{C}(n, k, d)$ is bounded by

$$2^{(n-k)} \leq \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{4.13}$$

Recall that the dual-containing quantum CSS codes rely on dual-containing classical binary codes, which satisfy the symplectic criterion of Eq. (7.8) and also comply with the constraint of $\mathbf{H}_z = \mathbf{H}_x$. Explicitly, half portion of the stabilizer operators of $\mathcal{C}[n, k, d]$ are mapped onto $\mathbf{H}_z$, while the other half are mapped onto $\mathbf{H}_x$. Therefore, the number of the stabilizer operators of a dual-containing quantum CSS code are bounded by

$$2^{\frac{(n-k)}{2}} \leq \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{4.14}$$

Based on Eq. (4.14), we may formulate the lower bound on the quantum coding rate of a dual-containing quantum CSS code as follows:

$$\frac{k}{n} \geq 1 - \frac{2}{n} \log_2 \left(\sum_{j=0}^{d-1} \binom{n}{j} \right). \tag{4.15}$$

As n approaches ∞, we obtain the quantum GV bound for CSS codes, as suggested in [88], which is formulated as

$$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right), \tag{4.16}$$

where $H(x)$ is the binary entropy of x. Based on the discussions above, we compare the asymptotic classical and quantum coding bounds in Table. 4.1 as well as in Fig. 4.3. Since the QSCs are designed to mitigate both bit-flip errors as well as phase-flip errors, the bounds of QSCs are significantly lower than those of their classical counterparts. Nevertheless, the general conception still holds, the Singleton bound serves as the loose upper bound, whilst the Hamming bound is the tighter upper bound.

4.3 Quantum Coding Bounds in the Asymptotical Limit

Although the classical to binary isomorphism assists us in the development of QSCs from the well-known classical code designs, the issue of determining the actual achievable minimum distance, given the coding rate and the codeword length remains unresolved. In the classical domain as we described previously, finding the unique solution to the realistically

Table 4.1: Comparison of various classical and quantum coding bounds.

Coding Bound	Asymptotic	
	Classical	Quantum
Singleton	$\frac{k}{n} \leq 1 - \left(\frac{d}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d}{n}\right)$
Hamming	$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right)\log_2 3 - H\left(\frac{d}{2n}\right)$
GV	$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d}{n}\right)\log_2 3 - H\left(\frac{d}{n}\right)$

Coding Bound	Finite-length	
	Classical	Quantum
Singleton	$\frac{k}{n} \leq 1 - \left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d-1}{n}\right)$
Hamming	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}\right)$	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}3^j\right)$
GV	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}\right)$	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}3^j\right)$

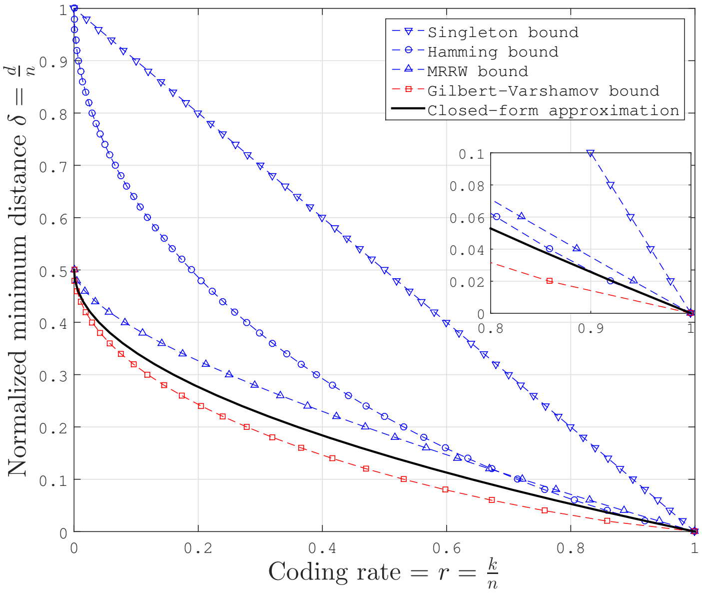


Figure 4.2: The trade-off between classical coding rate r and normalized minimum distance δ as described by classical binary coding bounds. A simple quadratic function $r(\delta) = (2\delta - 1)^2$, which satisfies all of the bounds, acts as a closed-form approximation for classical binary error correction codes as suggested in [93].

achievable minimum distance of binary classical codes is still an open problem, even though the upper bound and lower bound of the quantum coding rate versus the achievable minimum distance can be found in the literature [150, 151, 152, 153, 154]. The bounds for the classical code constructions are listed in Table. 4.2, while the corresponding asymptotic bounds are also plotted in Fig. 4.2. In the classical domain, the tightest lower bound was derived by Gilbert [152]. The Hamming bound [151] serves as a tight upper bound for high

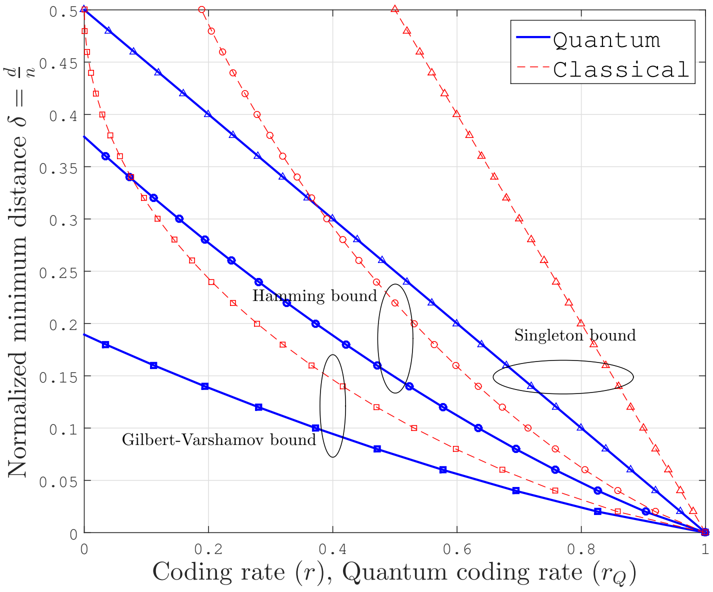


Figure 4.3: The evolution from asymptotic classical binary coding bounds to the asymptotic quantum coding bounds.

coding rates, while the McEliece-Rodemich-Rumsey-Welch (MRRW) bound [153] serves as the tightest upper bound for moderate and low coding rates. As seen in Fig. 4.2, the gap between the tight upper bounds and the lower bound is quite narrow. It was observed in [93] that a simple quadratic expression $r(\delta) = (2\delta - 1)^2$, where δ denotes the normalized minimum distance d/n, satisfies all the known asymptotic bounds.

Table 4.2: The coding bounds for classical code constructions, with a minor modification from [93].

Classical Bound	**Finite**	**Asymptotic**	**Notes**
Singleton [150]	$\frac{k}{n} \leq 1 - \left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{n}\right)$	a loose upper bound
Hamming [151]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}\right)$	$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right)$	tight upper bound for very high code rate
MRRW [153]		$\frac{k}{n} \leq H\left(\frac{1}{2} - \sqrt{\frac{d}{n}\left(1 - \frac{d}{n}\right)}\right)$	tightest known asymptotic upper bound for medium and low rate codes
Plotkin [154]	$\frac{k}{n} \leq \frac{1}{n}\left(1 - \log_2\left(2 - \frac{n}{d}\right)\right)$		tight upper bound for finite-length at $\delta > \frac{1}{2}$
GV [152]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}\right)$	$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right)$	tightest known lower bound

The well-known bounds for QSC constructions are listed in Table. 4.3 and they are also portrayed in Fig. 4.4. The quantum Singleton bound serves as the loose upper bound, the quantum Hamming bound as a tighter upper bound, and quantum GV bound as the tightest lower bound. However, a wide discrepancy can be observed between the upper bound and the lower bound. For the sake of narrowing this gap, the quantum Rain bound was derived using quantum weight enumerators [155]. To elaborate a little further, the quantum

Rain bound states that any quantum code of length n can correct at most $\lfloor \frac{n-1}{6} \rfloor$ errors. The resultant bound is only a function of codeword length n. Hence, under the asymptotic limit, the quantum Rain bound is a straigth line at $\delta = 1/3$, which does not exhibit any further trade-off between the quantum coding rate and the minimum distance. In order to enhance the accuracy of the quantum Rain bound, Sarvepalli and Klappenecker derived a quantum version of Griesmer bound [140]. By utilizing the quantum Griesmer bound and also the quantum Rain bound, a stronger bound was created for CSS type constructions. In this treatise, we will refer to this particular bound as the quantum Griesmer-Rain bound. For the sake of tightening the upper bound, Ashikhmin and Litsyn generalized the classical linear programming approach to the quantum domain using the MacWilliams identities [156]. The resultant quantum linear programming bound was proven to be tighter than the quantum Hamming bound in the low coding rate domain. As the quantum coding rate approaches zero, the achievable normalized minimum distance returned by the quantum Griesmer-Rain bound becomes $\delta = 0.33$ and that of quantum linear programming bound becomes $\delta = 0.32$.

Recall from Section 3.3 that the QSCs may exhibit either a CSS or non-CSS structure. For CSS codes, the minimum distance is upper-bounded by the quantum Hamming bound for moderate to high quantum coding rates and by the quantum Griesmer-Rain bound for low coding rates region, while it is also lower-bounded by the quantum GV bound for CSS codes. On the other hand, for non-CSS QSCs, the minimum distance is upper-bounded by the quantum Hamming bound for moderate to high coding rates and by the quantum linear-programming bound for low coding rates. It is also lower-bounded by the quantum GV bound for general quantum stabilizer codes. Even though substantial efforts have been invested in tightening the gap between the upper and lower bounds, a significant amount of discrepancy persists. Hence, creating a simple approximation may be beneficial for giving us further insights into the realistic construction of QSCs.

Analogous to the classical closed-form approximation of [93], we also found that there exists a simple closed-form quadratic approximation, which satisfies all the well-known quantum coding bounds. Explicitly for quantum stabilizer codes, the following quadratic function was found to satisfy all the quantum coding bounds:

$$r_Q\left(\delta\right) = \frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1 \text{ for } 0 \leq \delta \leq 0.2197. \tag{4.17}$$

We will further elaborate on the selection of this function in Section 4.5. It is important to note that the closed-form approximation is subject to the asymptotical bound for either CSS type or non-CSS type quantum code constructions. The closed-form approximation in Eq. (4.17) offers the benefit of simplicity and it has the inverse function as given by

$$\delta(r_Q) = \frac{3\left(\sqrt{2} - \sqrt{r_Q + 1}\right)}{4\sqrt{2}} \text{ for } 0 \leq r_Q \leq 1. \tag{4.18}$$

For a given quantum coding rate r_Q, it will correspond to a unique constant value of δ. Therefore, this closed-form approximation suggests that it is possible to create a code

Table 4.3: The well-known quantum coding bounds found in the literature.

Quantum Bound	**Finite-Length**	**Asymptotic**	**Notes**
Singleton [87]	$\frac{k}{n} \leq 1 - 2\left(\frac{d-1}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d}{n}\right)$	very loose upper bound
Hamming [60]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{j}3^j\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right)\log_2 3 - H\left(\frac{d}{2n}\right)$	tight upper bound for moderate and high coding rate
Griesmer-Rain [155, 140]	$\frac{k}{n} \leq 1 - \left(\frac{3d-4}{n}\right)$	$\frac{k}{n} \leq 1 - 3\left(\frac{d}{n}\right)$	tighter upper bound for low coding rates CSS codes
Linear Programming [156]		$\frac{k}{n} \leq H(\tau) + \tau\log_2 3 - 1$ $\tau = \frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}$	strengthen the upper bound
GV [60]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}3^j\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d}{n}\right)\log_2 3 - H\left(\frac{d}{n}\right)$	tight lower bound for general stabilizer codes
GV for CSS [88]		$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right)$	tight lower bound for CSS codes
	$\frac{k}{n} \geq 1 - \frac{2}{n}\log_2\left(\sum_{j=0}^{d-1}\binom{n}{j}\right)$		lower bound for dual-containing CSS codes

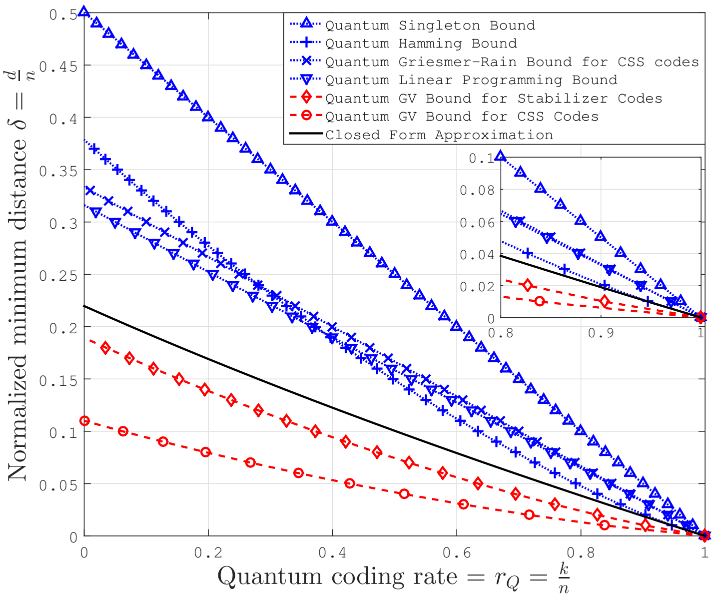


Figure 4.4: The trade-off between quantum coding rate r_Q and normalized minimum distance δ is characterized using quantum coding bounds. A simple quadratic closed-form $r_Q(\delta) = \frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1$ satisfies all of the well-known quantum coding bounds, which is portrayed by black solid lines. The blue dashed lines portrays the upper bounds, while the red dashed lines denotes the lower bounds.

construction whose minimum distance grows linearly with the codeword length at the asymptotical limit.

4.4 Quantum Coding Bounds on Finite-Length Codes

The asymptotic limits are only relevant for $n \to \infty$. For practical applications, we require code constructions with shorter codeword length, which necessitates a different formulation for the quantum coding bounds. Finding a closed-form approximation will be beneficial for determining the realistically attainable minimum distance for the given code parameters. The well-known quantum coding bounds are listed in Table 4.3 and also portrayed in Fig. 4.4. It is clearly seen that a simple quadratic approximation can satisfy all the well-known bounds. For the finite-length quantum codes, we propose the closed-form approximation of

$$r_Q(n,\delta) = a\delta^2 + b\delta + c. \tag{4.19}$$

To arrive at the closed-form approximation in Eq. (4.19), we have to determine three definitive points corresponding to realistic quantum code constructions. As an example in this treatise, we use three QSC constructions from the literature as listed below:

- For uncoded logical qubits and unity rate codewords, we have

$$r_Q(n,\delta) = r(n, \frac{1}{n}) = 1. \tag{4.20}$$

- For a high coding rate, we will use the construction given in [59]. For $n = 2^j$, there is a quantum stabilizer code construction $[n,k,d] = [n, n-j-2, 3]$, which can be used to correct $t = 1$ error. This code construction reaches the quantum Hamming bound. For arbitrary n, it can be written as

$$r_Q(n,\delta) = r(n, \frac{3}{n}) = 1 - \frac{1}{n}\log_2(n) - \frac{2}{n}. \tag{4.21}$$

- For a very low coding rate, we are using the quantum stabilizer code constructions derived from quadratic residues [157,158]. By using simple linear regression, we arrive at

$$r_Q(n,\delta) = r(n, \frac{2}{n} + \frac{1}{4}) = \frac{1}{n}. \tag{4.22}$$

Using the three definitive points from the constructions given in Eq. (4.20), (4.21) and (4.22), we arrive at a system of three linear equations, which have a unique value of a, b and c for an arbitrary value of n. More explicitly, we have

$$r_1 = a\delta_1^2 + b\delta_1 + c, \tag{4.23}$$

$$r_2 = a\delta_2^2 + b\delta_2 + c, \tag{4.24}$$

$$r_3 = a\delta_3^2 + b\delta_3 + c. \tag{4.25}$$

The analytical solution of Eq. (4.23), (4.24), and (4.25) is based on the following unique

Table 4.4: The list of QSC constructions that are used to plot practical code in Fig. 4.5.

$\mathcal{C}[n,k,d]$ for $n = 31$ and $n = 32$	
QBCH [63]	[31,1,7], [31,11,5], [31,21,3]
QRM [65]	[32,10,6], [32,25,3]
QGF(4) [62]	[31,1,11], [31,2,10], [31,21,4], [31,26,2], [32,1,11], [32,16,6], [32,22,4], [32,25,3], [32,30,2]

$\mathcal{C}[n,k,d]$ for $n = 63$ and $n = 64$	
QBCH [63]	[63,27,7], [63,39,5], [63,45,4], [63,51,3], [63,57,2]
QRM [65]	[64,35,6], [64,56,3]
QGF(4) [62]	[63,51,4], [63,55,3], [63,60,2], [64,44,6], [64,48,5], [64,52,4], [64,56,3], [64,62,2]

$\mathcal{C}[n,k,d]$ for $n = 127$ and $n = 128$	
QBCH [63]	[127,1,19], [127,15,16], [127,29,15], [127,43,13], [127,57,11], [127,71,9], [127,85,7], [127,99,5], [127,113,3]
QRM [65]	[128,35,12], [128,91,6], [128,119,3]
QGF(4) [62]	[127,114,4], [127,118,3], [127,124,2], [128,105,6], [128,110,5], [128,114,4], [128,119,3], [128,126,2]

parameter values:

$$a = \frac{(r_3 - r_2)\,\delta_1 + (r_1 - r_3)\,\delta_2 + (r_2 - r_1)\,\delta_3}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}, \tag{4.26}$$

$$b = \frac{(r_2 - r_3)\,\delta_1^2 + (r_3 - r_1)\,\delta_2^2 + (r_1 - r_2)\,\delta_3^2}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}, \tag{4.27}$$

$$c = \frac{(r_3\delta_2 - r_2\delta_3)\,\delta_1^2 + (r_1\delta_3 - r_3\delta_1)\,\delta_2^2 + (r_2\delta_1 - r_1\delta_2)\,\delta_3^2}{(\delta_2 - \delta_1)\,(\delta_3 - \delta_2)\,(\delta_1 - \delta_3)}. \tag{4.28}$$

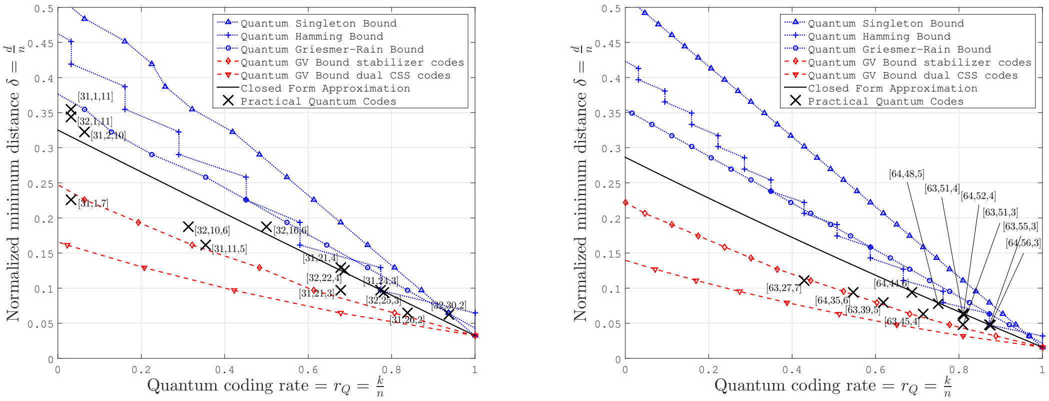
Despite the cluttered appearance of the analytical solution, it contains a simple closed-form approximation, because the value of r_1, r_2, r_3, δ_1, δ_2 and δ_3 may be easily calculated using Eq. (4.20), (4.21) and (4.22). Furthermore, the closed-form approximation derived for finite-length codewords has an inverse function of

$$\delta(n, r_Q) = \frac{-b - \sqrt{b^2 - 4a(c - r_Q)}}{2a}. \tag{4.29}$$

The accuracy of the proposed method is now tested for QSCs having codeword length of $n = \{31,\ 32,\ 63,\ 64,\ 127,\ 128\}$ as shown in Fig. 4.5. The list of practical QSC constructions which are used in these plots can be seen in Table. 4.4[1]. The closed-form approximation lies entirely between the upper and the lower quantum coding bounds. The practical QSCs are also plotted in the same figure to show the relative position with respect to the quantum coding bounds. The QSCs based on [62, 65] lays perfectly on approximation curves, but it has been observed in [159] that as the codeword length increases and the quantum coding rate is reduced, the exact value of the minimum distance becomes unclear. As depicted in Fig. 4.5(b) and 4.5(c), we can hardly find definitive points associated with actual codes to plot in the low quantum coding-rate region constructed from quantum $GF(4)$. Meanwhile,

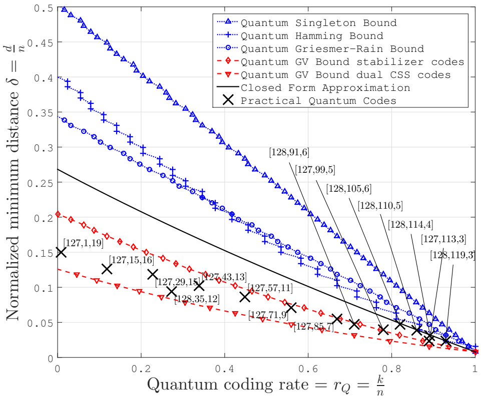
---

[1] A comprehensive list of practical quantum stabilizer codes can be found online at [159]. In this treatise, we only consider quantum stabilizer codes with a definitive minimum distance in the list.



(a) $n = 31$ and $n = 32$.

(b) $n = 63$ and $n = 64$.



(c) $n = 127$ and $n = 128$.

Figure 4.5: Quantum coding rate r_Q versus normalized minimum distance δ for finite-length QSCs. The points for portraying the practical QSCs are taken from QBCH codes [63], QRM codes [65] and quantum codes from $GF(4)$ formulation [62].

the QBCH code constructions lie quite close to the GV lower bound for dual-containing CSS codes. As predicted, since the constructions of QBCH codes rely on dual-containing CSS type constructions, which employ two separate PCMs for their stabilizer operators, we expect a lower coding rate compared to their non-CSS relatives.

The proposed closed-form approximation offers substantial benefits for the development of QSCs. We can readily find a fairly precise approximation of the realistically achievable minimum distance for given code parameters. For instance, for half-rate quantum stabilizer codes of length 128, the minimum distance is bounded by $11 < d < 22$. By using our formulation, we obtain $d(n = 128, r_Q = 1/2) = 17$ from our finite-length approximation. Likewise, for half-rate quantum stabilizer codes of length 1024, the minimum distance is bounded by $78 < d < 157$. Using our method, we can obtain $d(n = 1024, r_Q = 1/2) = 103$ from our asymptotic bound approximation. One of the logical questions that may arise concerns the existence of the corresponding codes. For example, does a half-rate QSCs relying on $n = 128$ physical qubits and a minimum distance of $d = 16$ exist? The answer to this question is not definitive. Let us refer to the code table given in [159], which is mainly based on the QSC constructions of [62]. Due to space limitations, we are unable to capture the entire table and the associated PCM formulation. However, it is shown in [159] that a half-rate QSC relying on $n = 128$ physical qubits indeed exists, although the minimum distance is only loosely specified by the bounds of $11 < d < 20$. The bound is similar to the quantum GV bound and to the quantum Hamming bound of the minimum distance given by $11 < d < 22$. By contrast, upon using our approximation, we have a minimum distance of $d = 17$, which is again only an approximation and it does not imply the existence of a quantum code having a similar minimum distance. Nonetheless, we believe that our approximation is beneficial for approximating the attainable QBER performance of QSCs based on hard-decision syndrome decoding for short to moderate codeword length as follows (without considering degeneracy):

$$\text{QBER}(n, d, p) = 1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i}, \tag{4.30}$$

where p is the depolarizing probability and the realistically achievable value of d is obtained from our approximation. In our view, the combination of our closed-form approximation and the QBER of Eq. (4.30) constitutes a useful benchmarker for the future development of QSCs, since it quantifies the realistically achievable QBER performance based on hard-decision syndrome-based decoding.

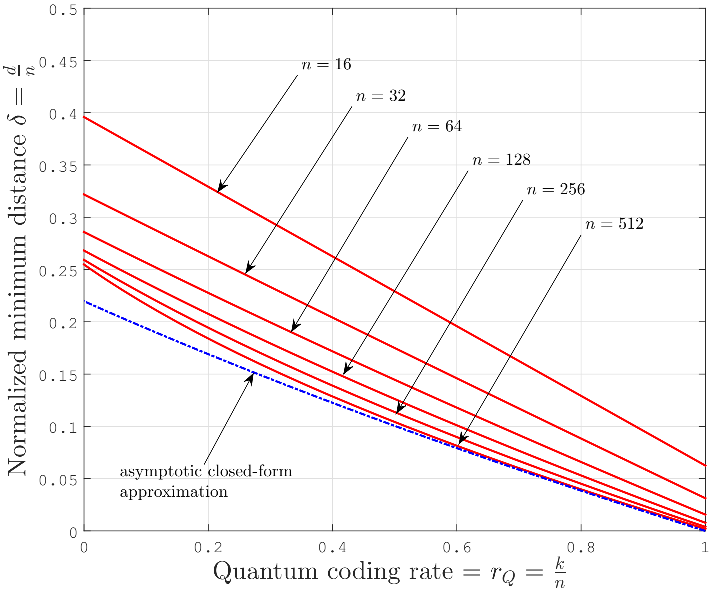


Figure 4.6: The evolution of our closed-form approximation for finite-length codewords parameterized by the codeword length n.

The evolution of our closed-form approximation as the codeword length increases for $n = \{31, 32, 63, 64, 127, 128\}$ can be seen in Fig. 4.6. By using our example, it can be clearly observed that as the codeword length increases, the derived approximation for finite-length codes slowly approaches the closed-form approximation of the asymptotic bound. However, inaccuracies emerge as the codeword length increases. This phenomenon emerges because we do not have definitive QSC constructions to rely on in the low coding rate region. In our approximation example, we are using the QSCs from quadratic residues construction for low coding rate region and the number of QSC constructions are very limited only for a handful codeword lengths. Meanwhile in the classical domain, in the low coding rate region, we have the simple repetition codes, with construction $\mathcal{C}(n, 1)$ having a normalized minimum distance of $\delta(n, r) = \delta(n, \frac{1}{n}) = 1$.

Albeit the finite and infinite-length-based approximation curves start to deviate for a very long codeword $n \gg 100$, the minimum distance still grows as the codeword length increases as portrayed in Fig. 4.7. Both the finite-length approximation and asymptotic approximation follow the same trend. For $n \gg 100$, we can simply utilize the asymptotic formulation given in Eq. (4.17) for calculating the quantum coding rate for a certain desired minimum distance, or the inverse of the asymptotic formulation in Eq. (4.18) to determine the realistically achievable minimum distance given the quantum coding rate. We can conclude from this figure that it is indeed possible to have a QSC construction with a growing minimum distance, as the codeword length increases.

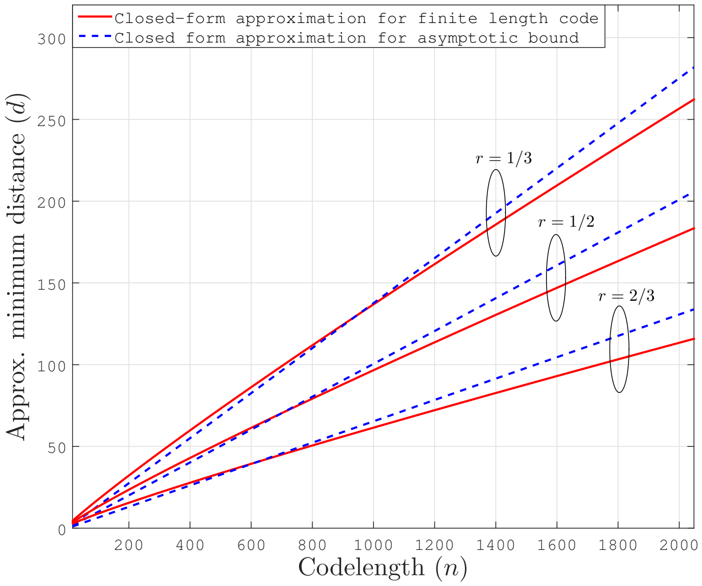


Figure 4.7: The growth of achievable minimum distance for short block QSCs versus the codeword length.

4.5 The Bounds on Entanglement-Assisted Quantum Stabilizer Codes

One of the distinctive characteristics of quantum systems, which does not bear any resemblance with the classical domain is the ability of creating entanglement. This unique property can be exploited for increasing the achievable minimum distance of quantum codes, hence increasing the error correction capability of QSCs. The EA-QSC constructions are denoted by $\mathcal{C}(n, k, d; c)$, where c denotes the number of preshared entangled qubits. It is important to note that even though the EA-QSCs expand the Pauli group operators from

$\mathcal{P}_n$ into $\mathcal{P}_{(n+c)}$, we only consider the error operators in $\mathcal{P}_n$. This is because the paradigm of EA-QSCs assumes that the preshared entangled qubits are not subjected to transmission error. Hence, for EA-QSCs, the quantum Hamming bound of Eq. (4.6) can be modified to

$$2^k \leq \frac{2^{n+c}}{\sum\limits_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor} \binom{n}{j} 3^j}, \tag{4.31}$$

where the notation d_{ea} denotes the minimum distance of EA-QSCs. Equation (4.31), can be rewritten to show explicitly the trade-off between quantum coding rate r_Q and minimum distance d_{ea} on EA-QSCs as follows:

$$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor} \binom{n}{j} 3^j\right) + \left(\frac{c}{n}\right). \tag{4.32}$$

When n tends to ∞, we yield

$$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right) + \left(\frac{c}{n}\right). \tag{4.33}$$

As encapsulated in Eq. (4.33), an additional conflicting parameter is involved in determining the quantum coding bounds, namely the entanglement consumption rate. The entanglement consumption rate E is the ratio between the number of preshared maximally entangled qubits c to the number of physical qubits n as encapsulated below:

$$E = \frac{c}{n}. \tag{4.34}$$

A maximally entangled[2] QSCs requires $c = n - k$ preshared qubit pairs. Hence, for a maximally entangled QSCs, the quantum Hamming bound of Eq. (4.33) can be reformulated as follows by substituting $c = n - k$ into Eq. (4.33), yielding:

$$\frac{k}{n} \leq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right). \tag{4.35}$$

Let us how consider the more general cases, where we may have a range of different entanglement ratios $0 \leq \theta \leq 1$. The entanglement ratio is defined as the ratio of preshared qubits c to the maximally-entangled preshared qubits $(n-k)$, yielding:

$$\theta = \frac{c}{n-k}. \tag{4.36}$$

The quantum Hamming bound for EA-QSCs with arbitrary entanglement ratios of θ is

---

[2] For a maximally-entangled QSCs, all of the auxiliary qubits required to generate the encoded state are already preshared using maximally entangled pair qubits. Hence, the maximal number of entangled pair qubits that can be shared beforehand is equal to the total number of auxiliary qubits, which is equal to $(n-k)$

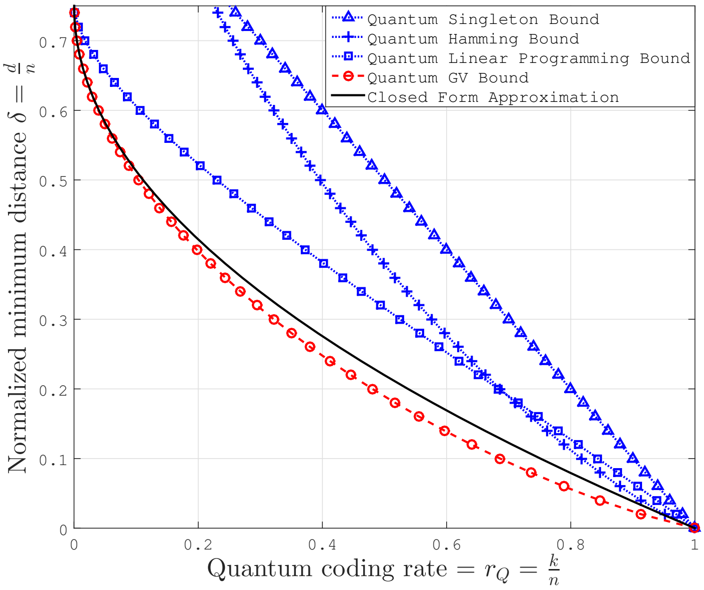


Figure 4.8: The asymptotic quantum coding bounds on EA-QSCs for maximally-entangled constructions. A simple quadratic function $r(\delta) = \frac{16}{9}\delta^2 - \frac{8}{3}\delta + 1$ satisfies all of the quantum coding bounds.

given by

$$\frac{k}{n} \leq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right). \tag{4.37}$$

Table 4.5: The entanglement-assisted quantum coding bounds found in the literature.

Quantum Bound	**Finite-Length**	**Asymptotic**	**Notes**
Singleton [67]	$\frac{k}{n} \leq 1 - 2\left(\frac{d_{ea}-1}{n}\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \leq 1 - 2\left(\frac{d_{ea}}{n}\right) + \left(\frac{c}{n}\right)$	very loose upper bound
Hamming [66]	$\frac{k}{n} \leq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{t=\lfloor\frac{d_{ea}-1}{2}\rfloor}\binom{n}{j}3^j\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right) + \left(\frac{c}{n}\right)$	tight upper bound
Linear Programming [160]		$\frac{k}{n} \leq H(\tau) + \tau\log_2 3 - 1 + \left(\frac{c}{n}\right)$ $\tau = \frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}$	strengthen the upper bound
Plotkin [161, 162]	$\frac{d_{ea}}{n} \leq \frac{3\left(4^k\right)}{8\left(4^k-1\right)}\left(1 + \left(\frac{k}{n}\right) + \left(\frac{c}{n}\right)\right)$	$\frac{d_{ea}}{n} \leq \frac{3}{8}\left(1 + \left(\frac{k}{n}\right) + \left(\frac{c}{n}\right)\right)$	upper bound for minimum distance
GV [162]	$\frac{k}{n} \geq 1 - \frac{1}{n}\log_2\left(\sum_{j=0}^{d_{ea}-1}\binom{n}{j}3^j\right) + \left(\frac{c}{n}\right)$	$\frac{k}{n} \geq 1 - \left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right) + \left(\frac{c}{n}\right)$	tight lower bound

The rest of the quantum coding bounds can readily be derived using the same analogy. The resultant entanglement-assisted quantum coding bounds are portrayed in Fig. 4.8 and 4.9. By substituting the entanglement ratio of $\theta = 0$, we arrive again at the quantum coding bounds derived for unassisted QSCs. By contrast, upon substituting into Eq. (4.37) the entanglement ratio $\theta = 1$, we have the quantum coding bounds for maximally-entangled QSCs. Figure 4.8 portrays the bounds on maximally-entangled QSCs. It is observed in Fig. 4.8 that at the point ($\delta = 0.75$), the quantum GV bound (lower bound) intersects the

Table 4.6: The asymptotic quantum coding bounds for EA-QSCs given the arbitrary entanglement ratios of θ.

Quantum Bound	**Entanglement Ratio** $= \theta$	**Maximally Entangled** $(\theta = 1)$
Singleton [67]	$\frac{k}{n} \leq 1 - \left(\frac{2}{1+\theta}\right)\left(\frac{d_{ea}}{n}\right)$	$\frac{k}{n} \leq 1 - \left(\frac{d_{ea}}{n}\right)$
Hamming [66]	$\frac{k}{n} \leq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right)$	$\frac{k}{n} \leq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{2n}\right)\log_2 3 - H\left(\frac{d_{ea}}{2n}\right)\right)$
Linear Programming [160]	$\frac{k}{n} \leq \frac{1}{1+\theta}\left(H\left(\tau\right) + \tau \log_2 3 - 1 + \theta\right)$	$\frac{k}{n} \leq \frac{1}{2}\left(H\left(\tau\right) + \tau \log_2 3\right)$
Plotkin [161,162]	$\frac{d_{ea}}{n} \leq \frac{3}{8}\left(1 + \theta + \frac{k}{n}\left(1-\theta\right)\right)$	$\frac{d_{ea}}{n} \leq \frac{3}{4}$
GV [162]	$\frac{k}{n} \geq 1 - \frac{1}{1+\theta}\left(\left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right)\right)$	$\frac{k}{n} \geq 1 - \frac{1}{2}\left(\left(\frac{d_{ea}}{n}\right)\log_2 3 - H\left(\frac{d_{ea}}{n}\right)\right)$

quantum linear programming bound (upper bound). Indeed, it is confirmed by the quantum Plotkin bound for the maximally-entangled QSC constructions shown in Table 4.6 that for asymptotical maximally-entangled QSCs the highest normalized minimum distance that can be achieved is $\delta = 0.75$. Hence, based on this observation, we propose a simple quadratic function as the closed-form approximation of entanglement-assisted quantum stabilizer codes that will satisfy all of the well-known bounds. A quadratic function associated with a symmetry line at ($\delta = 0.75$) and crossing the point of $(\delta, r) = (0, 1)$ is given by

$$r_Q(\delta) = \frac{16}{9}\delta^2 - \frac{8}{3}\delta + 1 \text{ for } 0 \leq \delta \leq 0.75. \tag{4.38}$$

The simple quadratic approximaton given in Eq. (4.38), can also be inverted, yielding

$$\delta(r_Q) = \frac{3}{4}(1 - \sqrt{r_Q}) \text{ for } 0 \leq r_Q \leq 1. \tag{4.39}$$

From the simple quadratic function in Eq. (4.38), we can also derive a simple closed-form approximation for a given arbitrary entanglement ratio of $0 \leq \theta \leq 1$, as shown below:

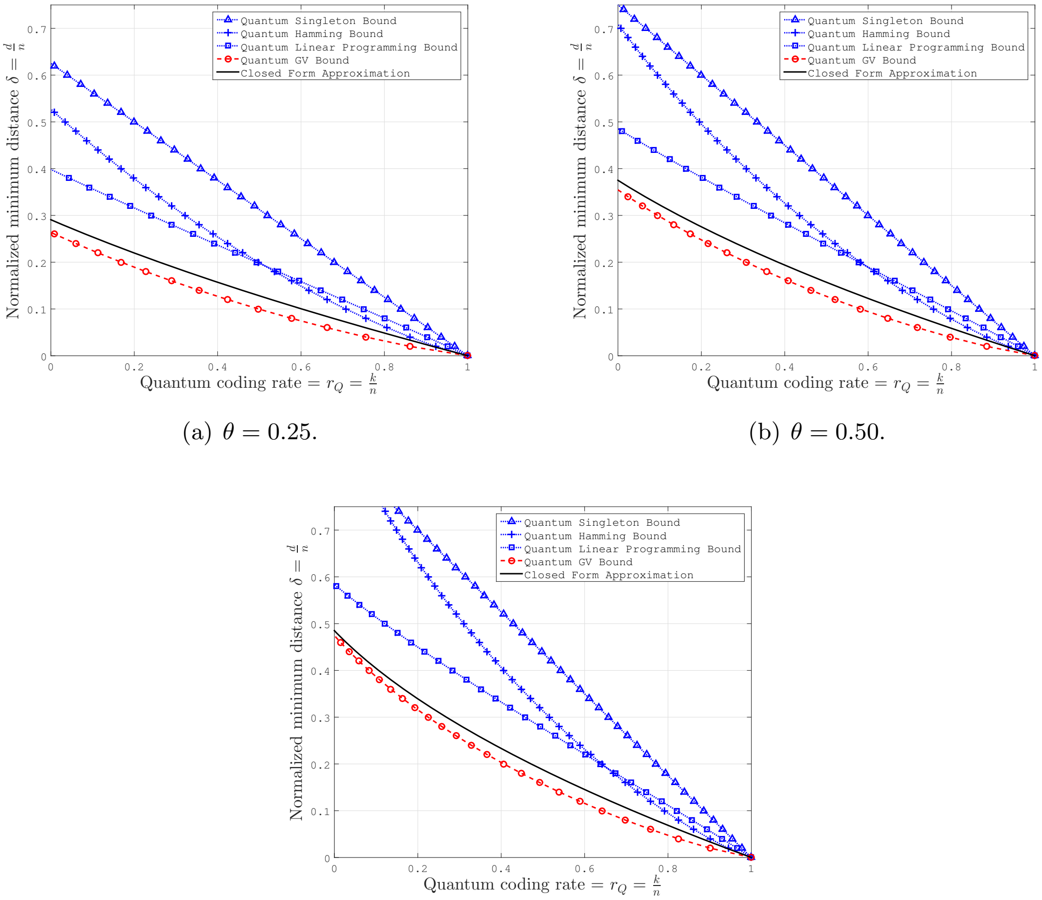
$$r_Q(\delta) = \frac{1}{1+\theta}\left(\frac{32}{9}\delta^2 - \frac{16}{3}\delta + 1 + \theta\right), \tag{4.40}$$

for $0 \leq \delta \leq \frac{3}{4}\left(1 - \sqrt{\frac{1-\theta}{2}}\right)$ and $0 \leq \theta \leq 1$. The expression given in Eq. (4.40) may be inverted to arrive at the following equation:

$$\delta(r_Q) = \frac{3(\sqrt{2} - \sqrt{r_Q(1+\theta) + (1-\theta)}}{4\sqrt{2}}, \tag{4.41}$$

for $0 \leq r_Q \leq 1$ and $0 \leq \theta \leq 1$.

The simple closed-form approximation given in Eq. (4.40) and (4.41) satisfies all entanglement-assisted quantum coding bounds for arbitrary entanglement ratios, as confirmed by Fig. 4.9. We should point out at this stage that as we substitute the value of $\theta = 0$ into Eq. (4.40) and (4.41), we comeback with the closed-form approximation presented in the Eq. (4.17) and (4.18) for unassisted asymptotic quantum coding bounds. Hence, we completed our closed-form approximations conceived for all of different constructions of quantum stabilizer codes.



(a) $\theta = 0.25$.

(b) $\theta = 0.50$.

(c) $\theta = 0.75$.

Figure 4.9: The asymptotic quantum coding bounds on EA-QSCs for entanglement ratios $\theta = \{0.25, 0.50, 0.75\}$.

4.6 Summary and Conclusions

We have conducted a survey of quantum coding bounds, which describe the trade-off between the quantum coding rate and the error correction capability for a wide range of QSC constructions. Furthermore, we provided insights into their relationships with their classical counterparts. For the family of unassisted QSCs, we have provided both lower and upper bounds for both CSS and non-CSS code constructions. For the EA-QSCs, we have presented the quantum coding bounds for maximally-entangled constructions and also for arbitrary entanglement ratios.

We also have proposed a closed-form approximation as a beneficial tool for analyzing the performance of QSCs. The resultant closed-form approximation may be indeed used as a simple benchmark for developing QSCs, because the resultant minimum distance δ and quantum coding rate r_Q values from our approximations are unambiguous. For instance, for a half-rate quantum stabilizer code having a given codeword length of $n = 128$, the minimum distance is bounded by $11 < d < 22$. By using our approximation, we arrive at $d(n = 128, r_Q = 1/2) = 16$ from our finite-length approximation. Likewise, for a half-rate quantum stabilizer code having the codeword length of 1024, the minimum distance is bounded by $78 < d < 157$. By using our proposal, we have an approximate minimum distance of $d(n = 1024, r_Q = 1/2) = 103$ from our asymptotic bound approximation. Ultimately, the proposed method can be utilized as an efficient tool for the characterization of quantum stabilizer codes.

Chapter 5

Quantum Topological Error Correction Codes: The Classical-to-Quantum Isomorphism Perspective

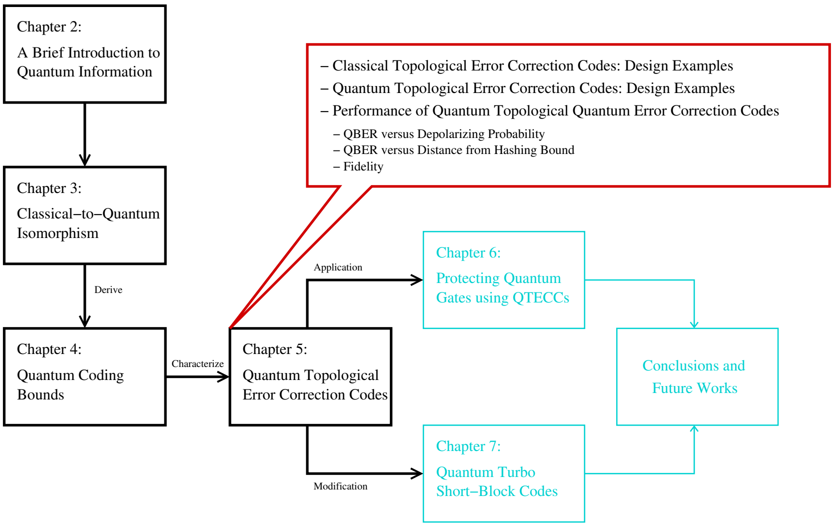
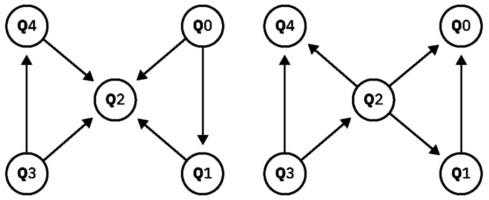


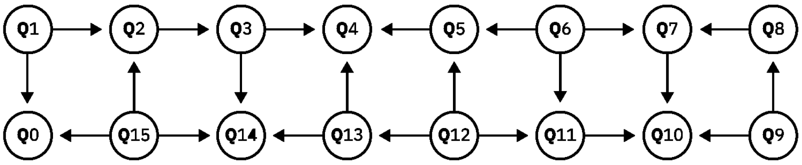
Figure 5.1: The outline of this thesis with the highlight of Chapter 5.

5.1 Introduction

In Chapter 3 and Chapter 4, we have demonstrated that classical error correction codes can be transformed into their quantum domain counterparts and we can readily characterize their associated QBER performances by exploiting the classical-to-quantum isomorphism as a function of their code parameters. However, the real physical implementations of quantum



(a) 5 qubits (ibmqx2). (b) 5 qubits (ibmqx4).



(c) 16 qubits (ibmqx5).

Figure 5.2: The qubit arrangement of IBM's superconducting quantum computers. The circles represent the qubits, while the arrows represent the possible qubit interactions within the computers [97].

computers impose additional challenges that prevent us from directly transplanting QSCs. Let us observed the layout of the physical qubits in IBM's quantum computers in Fig. 5.2. In these figures, the circles represent the qubits and the lines with the arrows represent the interaction between the qubits. Consequently, any quantum computation task performed by the quantum computers should be designed for accommodating the local interaction limitation. However, most of the QSCs derived from classical error correction codes may require interactions between distant qubits, which remains unrealistic at the current state-of-the-art. This particular constraint motivated the invention of new families of QSCs, which were specifically designed for circumventing these issues, namely the QTECCs. The stabilizer operators of QTECCs can be explicitly defined by the underlying lattice structure accommodating the qubits. Following the same line of investigation in Chapter 4, we will characterize the QBER performance of the QTECCs versus the code parameters given a certain lattice structure by exploiting the classical-to-quantum isomorphism.

The structure of this chapter is described in Fig. 1.7 and the rest of this treatise is organized as follows. In Section 5.2, we commence with design examples of classical TECCs to pave the way for delving into the quantum domain. In Section 5.3, we detail our QSC design examples for QTECCs. We continue by characterizing the performance of QTECCs over the popular quantum depolarizing channel in terms of QBER, distance from the hashing bound, and fidelity in Section 5.4. Finally, we conclude our discussion in Section 5.5.

5.2 Classical Topological Error Correction Codes: Design Examples

The classical error correction codes can be developed relying on diverse approaches [163]. We can find in the literature various family of codes based on algebraic formalisms, such as BCH codes and RS codes, codes based on conventional trellis structures such as convolutional codes and turbo codes, codes based on bipartite graphs such as LDPC codes, and codes based on channel polarization such as polar codes. Another approach that can be adopted to formulate a classical error correction code is by exploiting the topological or lattice structure. By assuming that we can arrange the bits of a codeword on a lattice structure, it can inherently provide us with an error correction scheme [164]. For instance, let us assume that a codeword of classical bits is arranged on the square lattice given in Fig. 5.3. The black circles laying on the edges of the lattice define the encoded information bits or the codeword. The red squares laying on the vertices of the lattice define the PCM of the codes, which also directly defines the syndrome values of the received codeword. The number of black circles is associated with the codeword length of n bits and the number of red squares is associated with the length of the syndrome vector or the number of rows of the PCM, which is equal to $(n-k)$ bits. For this particular square lattice seen in Fig. 5.3, the codeword length n is equal to 13 bits and the length $(n-k)$ of the syndrome vector is equal to 6 bits. Hence, the number of information bits k is equal to 7 bits. Therefore, this code has $2^7 = 128$ legitimate codewords out of the possible $2^{13} = 8192$ received words. Based on the above-mentioned construction, for example in classical BCH codes, we would be able to distinguish $2^{(13-7)} = 2^6 = 64$ distinct error patterns (including the error-free scenario) and correct a single bit error based on sphere packing bound.

The coding rate r is defined by the ratio between the information bits k to the codeword length n, yielding:

$$r = \frac{k}{n} \tag{5.1}$$

Hence, the coding rate of the square lattice code of Fig. 5.3 is $r = 7/13$.

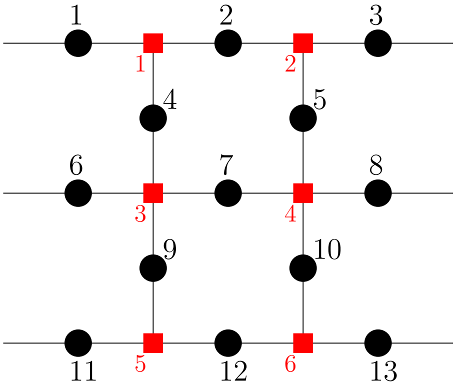


Figure 5.3: Example of a classical bit arrangement on a square lattice structure. The black circles laying on the edges of the lattice denote the bits of the codeword, while the vertices of the lattice denoted by red squares define the PCM and also the syndrome values.

Now, let us delve deeper into how the error correction works. Let us revisit the square lattice of Fig. 5.3. The k information bits are encoded to n-bit codewords, where $n > k$. Noise or decoherence imposed by the channel corrupts the legitimate codeword. The syndrome computation is invoked to generate the $(n-k)$-bit syndrome vector, which tells us both the predicted number and the position of the errors. In Fig. 5.3, each of the red squares indicates a syndrome bit of s_i. Hence, the syndrome vector $\mathbf{s}$ is a 6-bit vector, which is given by

$$\mathbf{s} = [s_1\ s_2\ s_3\ s_4\ s_5\ s_6]. \tag{5.2}$$

In the case of an error-free received codeword, the resultant syndrome vector is $\mathbf{s} = [0\ 0\ 0\ 0\ 0\ 0]$. By contrast, if an error is imposed on the codeword, it triggers a syndrome bit value of 1 at the adjacent syndrome bit positions. For example, if an error occurs at the bit index 4 of Fig. 5.3, it triggers the syndrome values of $s_1 = 1$ and $s_3 = 1$. The rest of the syndrome values remain equal to 0. Therefore, an error corrupting the bit index 4 generates a syndrome vector of $\mathbf{s} = [1\ 0\ 1\ 0\ 0\ 0]$. Hence, the decoder flips the value of bit index 4. Similarly, if an error occurs at bit number 3, it only triggers the syndrome value of $s_2 = 1$. Hence, it generates the syndrome vector of $\mathbf{s} = [0\ 1\ 0\ 0\ 0\ 0]$ and the error recovery procedure proceeds accordingly.

Now let us consider the ocurrence of two bit errors in the codeword. For instance, let us assume that errors occur at bit indices of 6 and 7 of Fig. 5.3. Note that both these errors affect s_3, therefore they cancel each other effect on s_3 out, hence generating a syndrome bit value of $s_3 = 0$. However, we still do not receive an all-zero syndrome vector, because the bit index 7 results in syndrome bit value of $s_4 = 1$ of Fig. 5.3. Therefore, the resultant syndrome vector due to a bit error in both bit 6 and 7 is $\mathbf{s} = [0\ 0\ 0\ 1\ 0\ 0]$. Since the syndrome vector of $\mathbf{s} = [0\ 0\ 0\ 1\ 0\ 0]$ is also associated with the error incident upon bit index 8, the error recovery procedure decides to flip bit 8 instead, because for the error probability less than 1/2, a single error occurance is more likely to happen than a double-error. This example is an illustration that the occurence of two bit errors in the codeword is beyond the error correction capability of the code given in Fig. 5.3. We conclude that the code based on the square lattice illustrated in Fig. 5.3 is capable of correcting only a single bit error. The error correction capability of t bits for a given code construction is defined by the minimum distance d of the code as formulated by

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor. \tag{5.3}$$

Hence, a code that is only capable of correcting a single error has a minimum distance of $d = 3$, as exemplified by the square lattice code given in Fig. 5.3. Moreover, the minimum distance of a square lattice code is defined by dimension of the lattice. Therefore, to increase the error correction capability of the code, we can simply increase the dimension of the lattice, which directly translates into increasing the minimum distance. The square lattice considered in our example can be generalized to a rectangular lattice structure having a dimension of $(l \times h)$, where l is the length of the lattice and h is the height of the lattice. In the case of a rectangular structure, the minimum distance is defined by

$$d = \min(l, h). \tag{5.4}$$

The codeword length is also uniquely defined by the dimension of the lattice. More explicitly, for a rectangular lattice of dimension $(l \times h)$, the codeword length is equal to the

Table 5.1: Constructing the PCM of the square lattice code of Fig. 5.3 with minimum distance of $d = 3$. Each row is associated with the syndrome operators denoted by red squares in Fig. 5.3

	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mathbf{h}_1$	1	1	0	1	0	0	0	0	0	0	0	0	0
$\mathbf{h}_2$	0	1	1	0	1	0	0	0	0	0	0	0	0
$\mathbf{h}_3$	0	0	0	1	0	1	1	0	1	0	0	0	0
$\mathbf{h}_4$	0	0	0	0	1	0	1	1	0	1	1	0	0
$\mathbf{h}_5$	0	0	0	0	0	0	0	0	1	0	1	1	0
$\mathbf{h}_6$	0	0	0	0	0	0	0	1	0	1	0	0	1

number of the lattice edges, which is given by

$$n\text{-edges} = n_{\text{square}} = 2lh - l - h + 1. \tag{5.5}$$

The number of rows in the PCM of a square lattice is defined by the number of faces or plaquettes of the rectangular lattice, which is formulated as follows:

$$n\text{-vertices} = n_{\text{square}} - k_{\text{square}} = h(l-1). \tag{5.6}$$

Hence, from Eq. (5.5) and (5.6), the number of information bits k encoded by the rectangular lattice codes is

$$\begin{aligned} k_{\text{square}} &= n_{\text{square}} - (n_{\text{square}} - k_{\text{square}}) \\ &= lh - l + 1. \end{aligned} \tag{5.7}$$

The most efficient code can be constructed by a square lattice, where $d = l = h$. Therefore, the expression given in Eq. (5.5) and (5.7) can be simplified to

$$n_{\text{square}} = 2d^2 - 2d + 1 \tag{5.8}$$

$$k_{\text{square}} = d^2 - d + 1. \tag{5.9}$$

Hence, the coding rate of square lattice based codes can be formulated as follows:

$$r_{\text{square}} = \frac{k_{\text{square}}}{n_{\text{square}}} = \frac{d^2 - d + 1}{2d^2 - 2d + 1}. \tag{5.10}$$

The PCM can be readily constructed in a similar fashion. Each red square of Fig. 5.3 represents the row of the PCM, where the adjacent black circles denote the index of the column containing a value of 1. For example, the first red square is adjacent to the black circles numbered 1, 2, and 4. Therefore, in the first row of the PCM, there are only three elements containing a value of 1 and those are marked by the index 1, 2, and 4. The remaining rows of the PCM are generated using the same principle. Explicitly, each row of the PCM of the square lattice code of Fig. 5.3 is portrayed in Table 5.1. Finally, the PCM

Table 5.2: Constructing the PCM of the triangular lattice code with minimum distance of $d = 3$. Each row is associated with the syndrome operators denoted by blue circles in Fig. 5.4

	1	2	3	4	5	6	7
$\mathbf{h}_1$	1	1	1	1	0	0	0
$\mathbf{h}_2$	0	0	1	1	1	1	0
$\mathbf{h}_3$	0	1	0	1	0	1	1

$\mathbf{H}$ of the square lattice code of Fig. 5.3 is given by

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1 \ \mathbf{h}_2 \ \mathbf{h}_3 \ \mathbf{h}_4 \ \mathbf{h}_5 \ \mathbf{h}_6 \end{bmatrix}^T . \qquad (5.11)$$

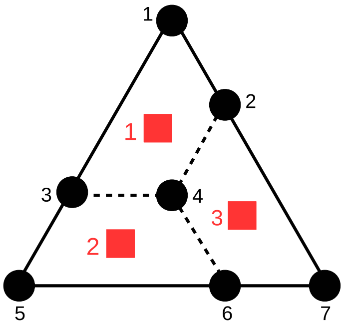


Figure 5.4: Example of a classical bit arrangement constructed over a triangular lattice structure. The black circles laying on the vertices of the lattice represent the codeword bits, while the faces or the plaquettes of the lattice denoted by red squares define the parity-check matrix and the syndrome bits of the error correction code. This configuration bears a resemblance to the $\mathcal{C}(7, 4)$ classical Hamming code.

The code construction based on the general lattice structure is not limited to a rectangular lattice. Let us consider, for instance, the triangular lattice of Fig. 5.4. The black circles laying on the vertex of the lattice define the codeword and the red squares on the faces of the lattice define the syndrome vector. The error correction principle of the triangular lattice code is similar to that of its square counterpart. Hence, the PCM of the triangular lattice code is readily derived using the following equation:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_1 \ \mathbf{h}_2 \ \mathbf{h}_3 \end{bmatrix}^T , \qquad (5.12)$$

where $\mathbf{h}_1$, $\mathbf{h}_2$, and $\mathbf{h}_3$ correspond to the syndrome bits given in Table 5.2. It is important to point out that the resultant triangular lattice code bears a strong resemblance to the classical $\mathcal{C}(7, 4, 3)$ Hamming code. Specifically, both codes have a codeword length of $n = 7$ and number of information bits of $k = 4$. Hence, the length of the syndrome vector is 3 bits. Consequently, the codes have 2^4 legitimate codewords out of the possible 2^7 received words. Based on the sphere packing bound, the codes are capable of distinguishing $2^3 = 8$ distinct error patterns including the error-free scenario. Therefore, both constructions are capable of correcting exactly a single error with an identical coding rate of $r = 4/7$.

Similar to its rectangular counterpart, increasing the error correction capability of a triangular lattice code is achieved by expanding the underlying lattice configuration. However, increasing the number of vertices of the triangular lattice structure is not as straightforward as that of its rectangular counterpart because it can be carried out in several different ways. In this example, we use the construction proposed in [103] and Fig. 5.5 illustrates how to increase the number of encoded bits of the triangular lattice code of Fig. 5.4 by using hexagonal tiles.

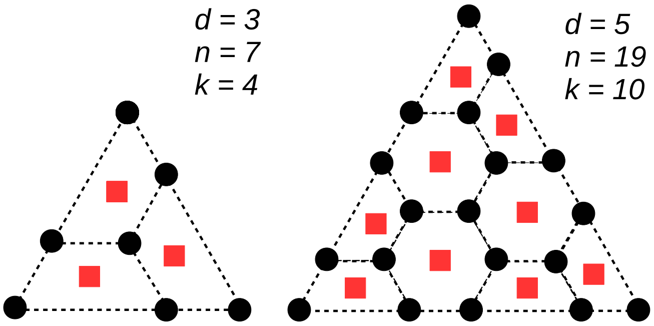


Figure 5.5: Extending the length of the triangular lattice code, which directly increases the numbers of error corrected.

Following the pattern of Fig. 5.5, the codeword length, which is also given by the number of vertices of the given lattices, is explicitly formulated as follows:

$$n\text{-vertices} = n_{\text{triangular}} = \frac{1}{4}(3d^2+1). \tag{5.13}$$

The number of faces in the triangular lattice, which corresponds to the number of rows of the PCM and also to the syndrome vector length, can be encapsulated as

$$n\text{-faces} = n_{\text{triangular}} - k_{\text{triangular}} = \frac{1}{8}(3d^2-3). \tag{5.14}$$

Hence, the number of information bits can be expressed as

$$\begin{aligned} k_{\text{triangular}} &= n_{\text{triangular}} - (n-k)_{\text{triangular}} \\ &= \frac{1}{8}(3d^2+5). \end{aligned} \tag{5.15}$$

Finally, the coding rate of the triangular lattice codes of Fig. 5.5 is formulated as follows:

$$r_{\text{triangular}} = \frac{k_{\text{triangular}}}{n_{\text{triangular}}} = \frac{3d^2+5}{2(3d^2+1)}. \tag{5.16}$$

Then, the normalized minimum distance, which directly correponds to the error correction capability per-bit of a code may be defined as:

$$\delta = \frac{d}{n} \tag{5.17}$$

For square lattice and triangular lattice codes, the normalized minimum distances are given by

$$\delta_{\text{square}} = \frac{d}{2d^2 - 2d + 1}$$
$$\delta_{\text{triangular}} = \frac{4d}{3d^2 + 1}. \tag{5.18}$$

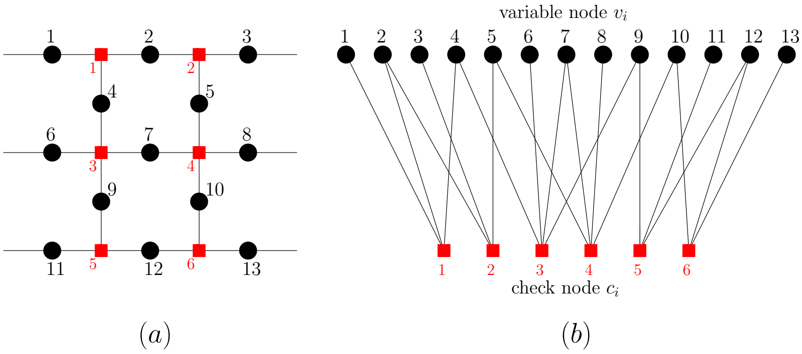


Figure 5.6: Example of how to represent the square lattice code. (a) The representation in lattice structure. (b) The representation in Tanner or bipartite graph.

In the rest of this treatise, we will consider the family of error correction codes based on lattice structures as a prominent representative of classical topological error correction codes (TECC). The lattice structures given in Fig. 5.3 and 5.4 can be transformed to Tanner graphs [165]. The dual representation of TECCs in the rectangular lattice domain and in the Tanner graph domain is given in Fig. 5.6 as exemplified by the square lattice code. We can observe that TECCs based on square lattices have a maximum row weight of $\rho_{\max} = 4$ and a maximum column weight of $\gamma_{\max} = 2$. By contrast, the codes based on triangular lattices have $\rho_{\max} = 6$ and $\gamma_{\max} = 3$. For a very long codeword, these properties lead to sparse PCMs. Hence, classical TECCs can be viewed as a specific family of LDPC codes. The asymptotical limit of the coding rate for LDPC codes based on TECCs can be directly derived from Eq. (5.10) and (5.16). As the codeword length tends to infinity ($n \to \infty$), the minimum distance d is also expected to tend to infinity. Hence, for the asymptotical limit we have

$$r^{\infty}_{\text{square}} = \lim_{d\to\infty} \frac{d^2 - d + 1}{2d^2 - 2d + 1} = \frac{1}{2}, \tag{5.19}$$
$$r^{\infty}_{\text{triangular}} = \lim_{d\to\infty} \frac{3d^2 + 5}{2(3d^2 + 1)} = \frac{1}{2}. \tag{5.20}$$

Let us observe Fig. 5.7, where we plot the minimum distance (d) versus coding rate (r) of TECCs based on Eq. (5.10) and (5.16). We also include the classical codes based on the sphere packing concept, namely the Hamming codes and the BCH codes, whose parameters are portrayed in Table 5.3 and 5.4, respectively. We also include some labels for several codes in the figure, in order to show how to convert the code parameters into data points in the figure. More explicitly, let us consider the specific triangular codes T1 and T2, where T1 represents the triangular code having a minimum distance of 3, which we have already used in the example in Fig. 5.4. As it has been elaborated on earlier,

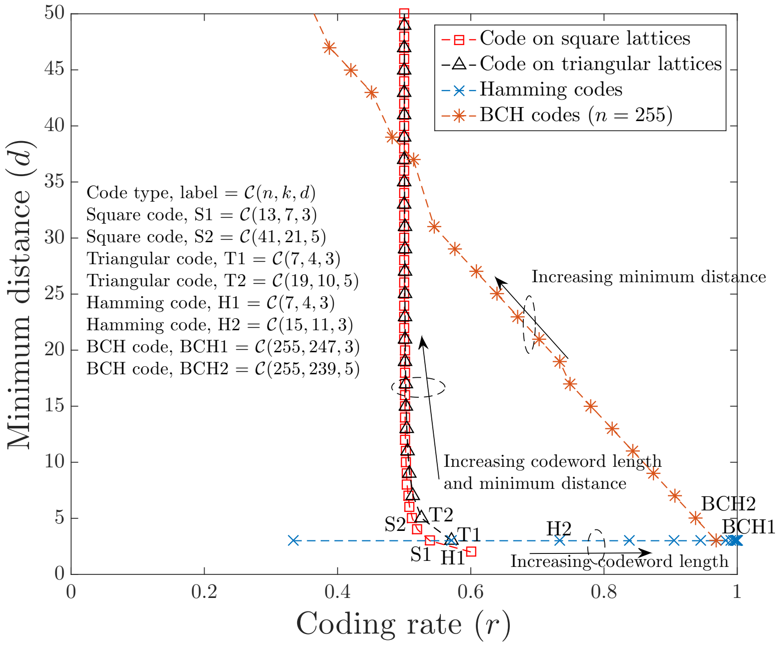


Figure 5.7: The coding rate versus minimum distance of TECCs. For asymptotical limit, the TECCs may be categorized into LPDC codes and the coding rates converge to $r = \frac{1}{2}$. We also include the BCH codes and Hamming codes for the sake of comparison. The coding rate for the square lattice based codes and the triangular lattice based codes are defined in Eq. (5.10) and (5.16), respectively. The code parameters for classical Hamming and BCH codes are described in Table 5.3 and 5.4, respectively. We put labels only for several codes as examples on how to convert the given code parameters into the figure.

the resultant code T1 is $\mathcal{C}(7, 4, 3)$. Hence, the coding rate is $r = 4/7 \approx 0.57$. Again, the triangular code T1 has identical code parameters to the Hamming code $\mathcal{C}(7, 4, 3)$, which is labelled H1. Hence, the same point in Fig. 5.7 represents both T1 and H1. Next, the code parameters of the triangular code T2 having a minimum distance of $d = 5$ are obtained using Eq. (5.13) and (5.15) for determining the codeword length n and the information length k, respectively. Explicitly, by substituting $d = 5$ into Eq. (5.13) and (5.15), we have $n = 19$ and $k = 10$. Finally, we arrive at the coding rate of $r = k/n = 10/19 \approx 0.53$ for the triangular code T2. The rest of the code parameters for square codes, triangular codes, Hamming codes and BCH codes are portrayed in the same way in Fig. 5.7.

In general, increasing the minimum distance of the codes while maintaining the codeword length can be achieved at the expense of reducing the coding rate. This phenomenon is perfectly reflected by the behaviour of classical BCH codes in Fig. 5.7. Explicitly, in Fig. 5.7 we portray BCH codes having a constant codeword length of $n = 255$, which are described in Table 5.4. As seen, upon increasing the minimum distance of BCH codes, the coding rate is gradually reduced. Next, increasing the coding rate while maintaining the minimum distance of the code can indeed be achieved by increasing the codeword length. In this case, the Hamming codes, whose code parameters are described in Table 5.3, reflect perfectly this phenomenon. Observe in Fig. 5.7, that for the Hamming codes exhibiting a constant minimum distance of $d = 3$, we can see the gradual increase of coding rate upon

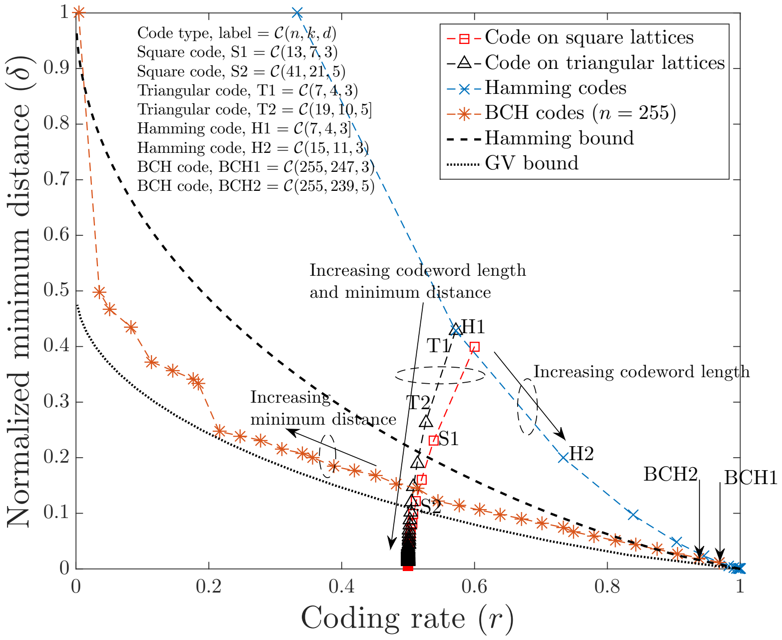


Figure 5.8: The coding rate versus normalized minimum distance of TECCs. For asymptotical limit, the TECCs may be categorized into LPDC codes and the coding rates converge to $r = \frac{1}{2}$, while the normalized minimum distances (δ) vanish to zero. In addition, we also include the classical Hamming and BCH codes, which constructed based on sphere packing bound, for the sake of comparison. The code parameters for classical Hamming and BCH codes are portrayed in Table 5.3 and 5.4, respectively. We put labels only for several codes as examples on how to convert the given code parameters into the figure.

increasing the codeword length. However, the behaviour of the BCH and Hamming codes is not reflected by the TECCs. Let us elaborate on the TECCs behaviour in Fig. 5.7. The increase of the minimum distance of TECCs upon increasing the codeword length looks very impressive since they do not seem to require much sacrifice in terms of coding rate reduction. In fact, the coding rate is saturated at approximately $r = 1/2$ for long codewords. This is indeed a rather different behaviour compared to that of the classical BCH codes. However, it is of pivotal importance to mention again that the increasing error correction capability per codeword does not necessarily imply the improvement of error correction capability per bit. Therefore, we have to normalize the performance to the codeword length

Table 5.3: Code parameters of classical Hamming code having a single error correction capability, which is used in Fig. 5.7 and 5.8. The coding rate r and normalized mnimum distance δ is calculated using Eq. (5.1) and (5.17), respectively.

n	k	d	n	k	d
3	1	3	127	120	3
7	4	3	255	247	3
15	11	3	511	502	3
31	26	3	1023	1013	3
63	57	3	...	...	...

Table 5.4: Code parameters of classical BCH codes having codeword length of $n = 255$, which is used in Fig. 5.7 and 5.8. The coding rate r and normalized mnimum distance δ is calculated using Eq. (5.1) and (5.17), respectively.

n	k	d	n	k	d	n	k	d
255	1	255	255	87	53	255	171	23
255	9	127	255	91	51	255	179	21
255	13	119	255	99	47	255	187	19
255	21	111	255	107	45	255	191	17
255	29	95	255	115	43	255	199	15
255	37	91	255	123	39	255	207	13
255	45	87	255	131	37	255	215	11
255	47	85	255	139	31	255	223	9
255	55	63	255	147	29	255	231	7
255	63	61	255	155	27	255	239	5
255	71	59	255	163	25	255	247	3
255	79	55						

to portray a fair comparison.

Let us now observe Fig. 5.8, where we plot the normalized minimum distance (δ) versus the coding rate (r) of TECCs based on Eq. (5.18). We include both the BCH codes as well as the Hamming codes for the sake of comparison. We also plot the classical Hamming bound [151] and GV bound [152] in this figure to portray the upper bound and lower bound of the normalized minimum distance, which correspond directly to the normalized error correction capability, given the coding rate. The classical Hamming bound is formulated as follows [151]:

$$\frac{k}{n} \leq 1 - H\left(\frac{d}{2n}\right), \tag{5.21}$$

where $H(x)$ is the binary entropy of x defined by $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$, while the classical GV bound is expressed as [152]

$$\frac{k}{n} \geq 1 - H\left(\frac{d}{n}\right). \tag{5.22}$$

The classical Hamming bound and GV bound defined in Eq. (5.21) and (5.22) are valid for asymptotical limit where $n \to \infty$.

The classical Hamming codes constitute the so-called *perfect codes* for a finite-length, since they always achieve the Hamming bound for finite-length codes[1]. Therefore, the Hamming codes also mark the upper bound of normalized minimum distance, given the coding rate of finite-length codewords. Secondly, the classical BCH codes having a codeword length of $n = 255$ lay perfectly - as expected - between the Hamming and GV bound in the asymptotical limit, as shown in Fig. 5.8. However, we observe an unusual behaviour for the family of TECCs, since the normalized minimum distance drops to zero upon increasing

---

[1] The Hamming bound for finite length codes has a different formulation from that of asymptotical limit. Therefore, we refer to [1] for further explanations.

Table 5.5: The code parameters of TECC-based LDPC codes.

Parameter	**Square lattice**	**Triangular lattice**
r	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
d	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$
δ	$\frac{d}{2d^2-2d+1}$	$\frac{4d}{3d^2+1}$
$\rho_{\max}$	4	6
$\gamma_{\max}$	2	3
Girth	6	4

the codeword length, while the coding rate saturates at $r = 1/2$. We hypothesize that since these codes were not designed using the sphere packing concept - which the Hamming and BCH codes are based on - the Hamming distance radius of the associated decoding sphere in the TECCs codespace is most likely to be non-identical for the different codewords. Also, the minimum distance of TECCs is only on the order of $\mathcal{O}(\sqrt{n})$, which implies that the codeword length of TECCs is proportional to the factor of $\mathcal{O}(d^2)$. By contrast, for classical BCH and Hamming codes the growth of the minimum distance is approximately linear, i.e. of order $\mathcal{O}(n)$. It can be seen that even though the growth of minimum distance per codeword of the TECCs appears to be impressive in Fig. 5.7, it is not fast enough to compensate for the undesired effect of the increasing codeword length. Hence, the TECC error correction capability per bit tends to zero in the asymptotical limit. Nevertheless, we leave the definitive answer for this peculiar phenomenon open for future research, since our focus in this treatise is on finding the classical-to-quantum isomorphism of TECCs.

Since the TECC associated with the asymptotical limit of $n \to \infty$ belongs to the family of LDPC codes, an efficient LDPC decoder such as the belief propagation (BP) technique [166] can be invoked for these code constructions. However, the normalized minimum distance of the LDPC codes based on topological order tends to zero, as the codeword length increases. Nevertheless, TECC-based LDPC codes exhibit several desirable code properties, such as an attractive coding rate ($r \approx 1/2$), structured construction and unbounded minimum distance. However, another aspect worth considering for TECC-based LDPC codes is the fact that we can find numerous cycles of length 4 in triangular constructions and cycles of length 6 in square constructions, which potentially degrades the performances of the codes. A summary of code parameters of TECC-based LDPC codes is given in Table 5.5.

5.3 Quantum Topological Error Correction Codes: Design Examples

Let us now delve deeper into the TECC concept in the quantum domain. The quantum version of TECCs, namely the QTECCs, constitute a member of the QSC family, whose stabilizer operators are defined by the underlying lattice structure. This formalism offers several benefits for the implementation of quantum computers. Firstly, it explicitly accommodates the physical implementation of quantum memory by mapping the qubits to the lattice arrangement exemplified by Fig. 5.3 and 5.4. Secondly, the localized nature of the stabilizer measurements confines the interaction amongst qubits and also eliminates the interaction of qubits associated with a specific quantum gate that physically far from each other. Thirdly, the number of errors corrected can be increased simply by extending the size of the lattice. For now, let us assume having a square lattice structure similar to Fig. 5.3 for defining the stabilizer operators of a surface code illustrated in Fig. 5.9 [101]. Explicitly, surface codes represent the quantum equivalent of classical TECCs on rectangular lattice structures. The physical qubits are portrayed by the black circles laying on the edge of the lattice, the **X** stabilizer operators are defined by the red squares on the lattice vertices, while the **Z** stabilizers are defined by the blue triangles on the lattice plaquettes (faces). The stabilizer operators of QTECCs are defined as follows:

$$A_v = \prod_{i \in \text{vertex}(v)} \mathbf{X}_i \ , \ B_p = \prod_{i \in \text{plaquette}(p)} \mathbf{Z}_i, \tag{5.23}$$

where i indicates the index of stabilizer operators containing the Pauli matrix **X** as well as **Z** and the rest of the stabilizer operators are given by the Pauli identity matrix **I**. Hence, the encoded state of the physical qubits of QTECCs is constrained within a code space $\mathcal{C}$ satisfying

$$\mathcal{C} = \{|\overline{\psi}\rangle \in \mathcal{H} | A_v|\overline{\psi}\rangle = |\overline{\psi}\rangle, \ B_p|\overline{\psi}\rangle = |\overline{\psi}\rangle; \ \forall v, p\}. \tag{5.24}$$

More specifically, let us revisit Fig. 5.9 for exemplifying the construction of the stabilizer operators of a QTECC, namely of the surface codes, which is one of the QTECC constructions whose stabilizer operators are defined by a rectangular lattice structure [101]. For instance, the red square on the vertex number 3 of Fig. 5.9 represents the **X** stabilizer operator of $A_3 = \mathbf{X}_4\mathbf{X}_6\mathbf{X}_7\mathbf{X}_9$ as seen in the row S_3 of Table 5.6. Similarly, the blue triangle on the plaquette number 5 of Fig. 5.9 defines the **Z** stabilizer operator of $B_5 = \mathbf{Z}_7\mathbf{Z}_9\mathbf{Z}_{10}\mathbf{Z}_{12}$ as seen in the line B_5 of Table 5.6. By performing the same evaluation for all of the red squares and blue triangles, we arrive at the stabilizer operators for the quantum surface codes, as listed in Table 5.6.

Let us now consider an example of how the error correction procedure works using the QTECCs, which is similar to the classical TECCs, by revisiting Fig. 5.9. For instance, let assume that the quantum decoherence imposes a bit-flip (**X**) error on the physical qubit index 7. Since, the **X**-type error commutes with the **Z** stabilizer operators, which are represented by the blue triangles, the adjacent **Z** stabilizer operators return the eigenstate values of -1 upon measurement. Consequently, the **Z** stabilizer measurements yield a

Table 5.6: The stabilizer operators (S_i) of the quantum surface code having the lattice construction of Fig. 5.9. The code has a minimum distance of 3 ($d = 3$), which means that it is only capable of correcting a single qubit error.

S_i	A_v	S_i	B_p
S_1	$\mathbf{X}_1\mathbf{X}_2\mathbf{X}_4$	S_7	$\mathbf{Z}_1\mathbf{Z}_4\mathbf{Z}_6$
S_2	$\mathbf{X}_2\mathbf{X}_3\mathbf{X}_5$	S_8	$\mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_7$
S_3	$\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7\mathbf{X}_9$	S_9	$\mathbf{Z}_3\mathbf{Z}_5\mathbf{Z}_8$
S_4	$\mathbf{X}_5\mathbf{X}_7\mathbf{X}_8\mathbf{X}_{10}$	S_{10}	$\mathbf{Z}_6\mathbf{Z}_9\mathbf{Z}_{11}$
S_5	$\mathbf{X}_9\mathbf{X}_{11}\mathbf{X}_{12}$	S_{11}	$\mathbf{Z}_7\mathbf{Z}_9\mathbf{Z}_{10}\mathbf{Z}_{12}$
S_6	$\mathbf{X}_{10}\mathbf{X}_{12}\mathbf{X}_{13}$	S_{12}	$\mathbf{Z}_8\mathbf{Z}_{10}\mathbf{Z}_{13}$

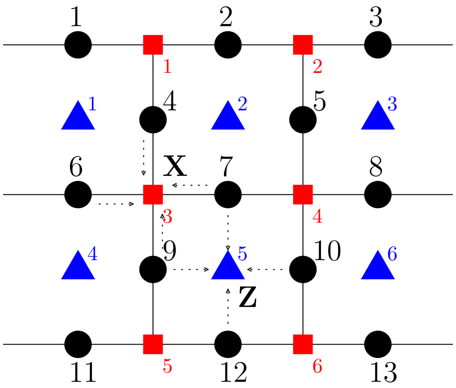


Figure 5.9: Example of qubit arrangement on a rectangular lattice structure. The black circle-based qubits on the edges of the lattice represent the physical qubits or the encoded state, the red square-based qubits lying on the vertices of the lattice act as the **X** stabilizer operators, while the blue triangle-based qubits lying on the plaquettes (faces) of the lattice constitute the **Z** stabilizer operators.

syndrome vector of $\mathbf{s}_z = [0\ 1\ 0\ 0\ 1\ 0]$, where only the vector elements of $i = 2, 5$ have the value of 1. For the a short block code considered in Fig. 5.9, the error recovery operators $\mathcal{R}$ are determined based on hard-decision maximum-likelihood (ML) decoding, which is translated into a simple look-up table (LUT) decoder. Therefore, based on the syndrome vector of $\mathbf{s}_z$, the error recovery operator $\mathcal{R}$ is given by $\mathcal{R} = \mathbf{X}_7$. Likewise, let us now assume that the qubit on index 7 also suffers from a **Z**-type error imposed by the quantum channel. The associated syndrome vector gleaned from the **X** stabilizer operators is $\mathbf{s}_x = [0\,0\,1\,1\,0\,0]$, where only the vector elements of $i = 3, 4$ have the value of 1. Thus, based on the syndrome vector of $\mathbf{s}_x$, the decoder applies the error recovery operator of $\mathcal{R} = \mathbf{Z}_7$.

The error correction capability t of a QSC $\mathcal{C}[n, k, d]$ can be determined by its minimum distance d as follows:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor. \tag{5.25}$$

Therefore, in order to verify the error correction capability of a QSC $\mathcal{C}$, first, we need to evaluate the minimum distance d based on the stabilizer operators $S_i \in \mathcal{S}$. Let the normalizer $\mathcal{N}(\mathcal{S}) \in \mathcal{P}_n$ is the set of operators $P_i \in \mathcal{P}_n$ such that $PS_iP^\dagger = S_j \in \mathcal{S}$ for all $S_i \in \mathcal{S}$ and i is not necessarily equal to j. It is clear that all the stabilizer operators $S_i \in \mathcal{S}$ are automatically in $\mathcal{N}(\mathcal{S})$. Now, we are interested in the set of operators in the normalizer

$\mathcal{N}(\mathcal{S})$ that does not belong to stabilizer operators $\mathcal{S}$, which is denoted by $\mathcal{N}(\mathcal{S}) - \mathcal{S}$. The minimum distance of a QSC $\mathcal{C}$ is equal to d if and only if $\mathcal{N}(\mathcal{S}) - \mathcal{S}$ contains no elements with weight less than d, where the weight of a Pauli operator $P_i \in \mathcal{P}_n$ is the number of non-identity Pauli operators. In other words, the minimum distance of a QSC $\mathcal{C}$ can be defined by the minimum weight of the operators P_i, which commutes with all stabilizer operators $S_i \in \mathcal{S}$, but not an element of $\mathcal{S}$.

In the case of rectangular lattice structure given in Fig. 5.9, the good example for such operator P_i is the chains connecting the two boundaries of the lattice. To elaborate a little further, let us take a Pauli operator P represented by the shortened version $P = \mathbf{X}_2\mathbf{X}_7\mathbf{X}_{12}$ connecting the boundaries of the lattice given in Fig. 5.9. It can be easily checked that this specific Pauli operator P commutes with all the stabilizer generators $G_i \in \mathcal{S}$, but it cannot be represented as the product of any stabilizer generators $G_i \in \mathcal{S}$. Since P_i represents the lowest weight Pauli operator P_i commuting with all the stabilizer operators $S_i \in \mathcal{S}$, but not an element of $\mathcal{S}$, the weight of P_i determines the minimum distance of the QSC defined by the rectangular lattice of Fig. 5.9. Therefore, we conclude that based on the stabilizer generators given in Table 5.6, the minimum distance of the QSC defined by rectangular lattice of Fig 5.9 is $d = 3$. Furthermore, the dimension of the lattices defining the stabilizer operators $G_i \in \mathcal{S}$ can be used to calculate the minimum distance d, the number of logical qubits and physical qubits, as well as the quantum coding rate r_Q.

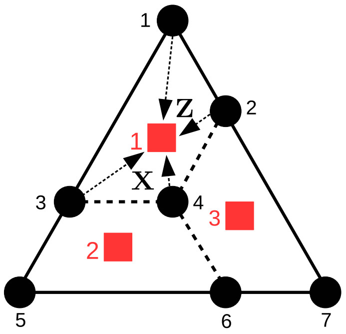


Figure 5.10: Example of a qubit arrangement for colour code, which is a type of QTECCs whose stabilizer operators are defined by a triangular lattice structure. The black circles-based qubits on the vertices of the lattice represent the physical qubits, while the faces or the plaquettes of the lattice denoted by red squares define stabilizer operators of the colour code. The resultant code has a minimum distance of $d = 3$ and hence becomes capable of correcting a single qubit error. This specific configuration bears a resemblance to the $\mathcal{C}[7, 1, 3]$ Steane's 7 qubit code.

Again, similar to the classical TECCs, the construction of QTECCs is indeed not limited to the square lattice structure. Let us now elaborate on another construction inspired by the construction proposed in [103] using the triangular lattice based on the classic example of Fig. 5.4. In the proposal of [103], this specific code construction is often referred to as the (triangular) colour code, since the underlying triangular lattice is composed by the tri-coloured hexagonal tiles. However, constructing the stabilizer operators of colour codes slightly differs from that of the surface codes. The colour codes use the lattice plaquettes to define both the $\mathbf{Z}$ and $\mathbf{X}$ stabilizer operators. Consequently, the resultant colour codes belong to the family of dual-containing CSS codes, which is in contrast to the surface codes that belong to the class of non-dual-containing CSS codes. For colour codes, defining both the **Z** and **X** stabilizer operators using the same plaquette always guarantees to satisfy the symplectic criterion of Eq. (7.8). However, for surface codes, we cannot always satisfy the symplectic criterion by using the same procedure. Therefore, the dual of the lattice is used for defining half of the stabilizer operators of the surface codes to satisfy the symplectic criterion.[2]

Let us consider Fig. 5.10 for constructing the stabilizer operators of distance-3 colour codes, which are only capable of correcting a single qubit error. The plaquette denoted by red square at index 3 is used to define both the **Z** and **X** stabilizer operators. Thus, the resultant **X** stabilizer operator is $A_3 = \mathbf{X}_2\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7$ and the resultant of **Z** stabilizer operator is $B_3 = \mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_6\mathbf{Z}_7$. The stabilizer operators for the colour code having the minimum distance 3 in Fig. 5.10 are listed in Table 5.7. We can observe that the colour code of Fig. 5.4 exhibits a strong resemblance to Steane's 7-qubit code.

To draw on the parallelism between classical TECCs and QTECCs, let us consider the stabilizer operators of the colour code having a minimum distance of $d = 3$, as seen in Table 5.7. Since the distance-3 colour code belongs to the family of quantum CSS codes, the PCM **H** obtained by using Eq. (3.16) and (3.19) is encapsulted as follows:

$$\mathbf{H} = \left(\begin{array}{ccccccc|ccccccc}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1
\end{array}\right). \tag{5.26}$$

A CSS stabilizer code $\mathcal{C}[n,k,d]$ having $(n-k)$ stabilizer operators can be portrayed as a classical code having a PCM **H** containing $(n-k) \times 2n$ elements. Therefore, the coding rate of the classical dual of a quantum CSS code can be expressed as follows [79]:

$$\begin{aligned}
r_C &= \frac{2n-(n-k)}{2n}, \\
&= \frac{n+k}{2n}, \\
&= \frac{1}{2}\left(1+\frac{k}{n}\right), \\
&= \frac{1}{2}\left(1+r_Q\right),
\end{aligned} \tag{5.27}$$

where r_C is the coding rate of the classical dual of the stabilizer code $C[n,k,d]$ exhibiting a quantum coding rate of r_Q. The relationship between the classical and quantum coding

---

[2] The dual of a lattice or a graph G is the graph that has a vertex for each plaquette of the graph.

rate in Eq. (5.27) can be rewritten as

$$r_Q = 2r_C - 1. \tag{5.28}$$

For instance, let us consider the distance-3 colour codes $\mathcal{C}[n,k,d] = \mathcal{C}[7,1,3]$, as exemplified in Fig. 5.10, and its classsical dual $\mathcal{C}(n,k,d) = \mathcal{C}(7,4,3)$, as seen in Fig. 5.4. Explicitly, we have the classical coding rate of $r_C = 4/7$ for the $\mathcal{C}(7,4,3)$ code. By substituting $r_C = 4/7$ into Eq. (5.28), we obtain the quantum coding rate for its quantum counterpart as $r_Q = 1/7$, which is the quantum coding rate of distance-3 colour code $\mathcal{C}[7,1,3]$. The same goes for the classical square codes and their quantum counterpart, namely for the surface codes. Let us consider the distance-5 classical square code, which is labeled by S2 in Fig. 5.7 and its quantum pair, which is labeled by S2 in Fig. 5.11. We can readily determine the quantum coding rate of the surface code S2 $\mathcal{C}[41,1,5]$, which is $r_Q = 1/41$. Therefore, by substituting $r_Q = 1/41$ into Eq. (5.27), we arrive at the coding rate of its classical dual given by $r_C = 21/41$, which is indeed the coding rate of the classical square code S2 $\mathcal{C}(41,21,5)$.

Table 5.7: The stabilizer operators (S_i) of the colour code seen in Fig. 5.10. The code has a minimum distance of 3 ($d = 3$), which means that it is only capable of correcting a single qubit error.

S_i	A_p	S_i	B_p
S_1	$\mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4$	S_4	$\mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4$
S_2	$\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6$	S_5	$\mathbf{Z}_3\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6$
S_3	$\mathbf{X}_2\mathbf{X}_4\mathbf{X}_6\mathbf{X}_7$	S_6	$\mathbf{Z}_2\mathbf{Z}_4\mathbf{Z}_6\mathbf{Z}_7$

Table 5.8: The code parameters for various QTECCs based on the minimum distance d of the code.

Codes type	**Dimension**	**Number of physical qubits**	**Number of stabilizers**	**Number of logical qubits**
Colour	d^*	$\frac{1}{4}\left(3d^2+1\right)$	$\frac{1}{4}\left(3d^2-3\right)$	1
Rotated-surface	$d \times d$	d^2	d^2-1	1
Surface	$d \times d$	$2d^2-2d+1$	$2d^2-2d$	1
Toric	$d \times d$	$2d^2$	$2d^2-2$	2

* for triangular colour codes the dimension is defined by the side length of the equilateral triangle

Similar to their classical counterparts, the code parameters of QTECCs, such as the number of logical qubits k, the number of physical qubits n, the minimum distance of the code d, as well as the quantum coding rate r_Q, depend on the size of the lattices. Following the same line of investigation as for the classical TECCs, we derive the complete formulation for the number of logical qubits k and the number of physical qubits n as a function of the minimum distance of the codes, which is given in Table 5.8. We plot the minimum distance (d) versus quantum coding rate (r_Q) of QTECCs in Fig. 5.11 for colour codes [103], for

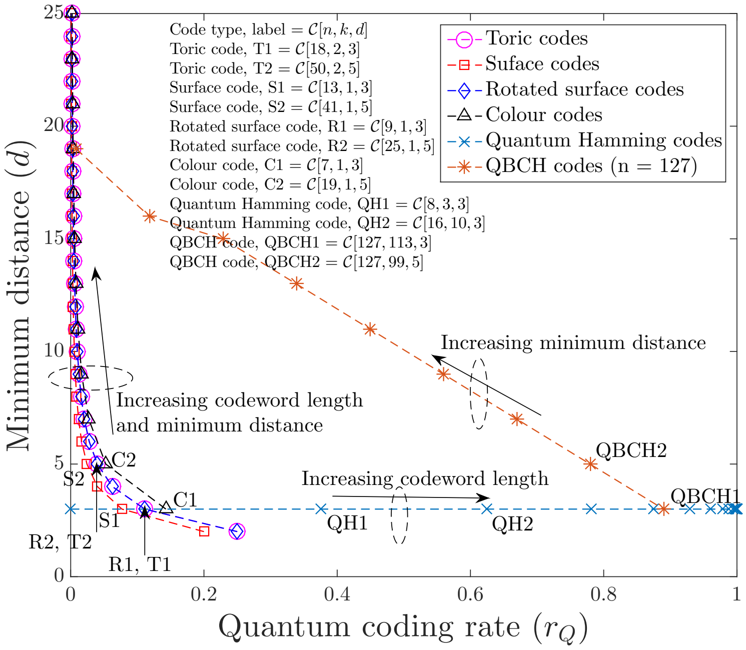


Figure 5.11: The minimum distance (d) versus the quantum coding rate (r_Q) of QTECCs based on the parameter given in Table 5.8. For QTECCs, the quantum coding rate tends to zero as we increase the minimum distance. We also include the QBCH codes having the physical qubits of $n = 127$ and quantum Hamming codes for the sake of comparing the QTECCs with the non-topological QSCs.

Table 5.9: Code parameters of quantum Hamming codes having a single error correction capability, which is used in Fig. 5.11 and 5.12. The quantum coding rate r_Q and normalized minimum distance δ are calculated using Eq. (5.1) and (5.17), respectively.

n	k	d	n	k	d
8	3	3	256	246	3
16	10	3	512	501	3
32	25	3	1024	1012	3
64	56	3	2048	2035	3
128	119	3	...	...	...

rotated surface codes [102], for surface codes [101] and for toric codes [98]. We also include the non-topological QSCs, namely the QBCH codes [63] having $n = 127$ physical qubits and the quantum Hamming codes, which constitute the quantum analogue of Hamming bound-achieving code constructions [59]. Similarly to the classical domain, the behaviour of both the QBCH codes and the quantum Hamming codes is as expected, exhibiting the behaviour inherited from their classical analogues. However, it is interesting to observe that the quantum coding rate of QTECCs tends to zero for long codewords. Nevertheless, this phenomenon is expected, if we consider the classical to quantum isomorphism in the context of the coding rate given in Eq. (5.27) and (5.28). For the classical TECCs, the coding rate r_C approaches the value of $r_C = 1/2$ for long codewords. Hence, by substituting $r_C = 1/2$ into Eq. (5.28), we arrive at $r_Q = 0$, which is the phenomenon we observe in Fig. 5.11.

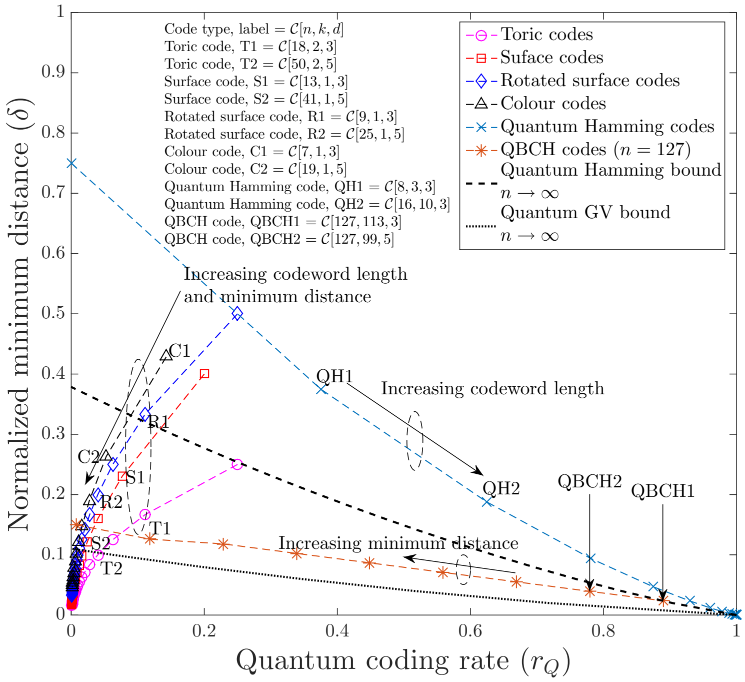


Figure 5.12: The normalized minimum distance (δ) versus the quantum coding rate (r_Q) of QTECCs based on the parameter given in Table 5.8. For QTECCs, the normalized minimum distance and quantum coding rate tend to zero as we increase the minimum distance. We also include the QBCH codes having the physical qubits of $n = 127$, quantum Hamming codes, quantum Hamming bound and also quantum GV bound for CSS codes for the sake of comparing the QTECCs with the non-topological QSCs.

Next, we plot the normalized minimum distance (δ) versus the quantum coding rate (r_Q) in Fig. 5.12. Once again, for the sake of comparison, we also include the quantum Hamming bound [60] and the quantum GV bound derived for CSS codes [88] in addition to the QBCH codes and the quantum Hamming codes. The quantum Hamming bound is defined by [60]

$$\frac{k}{n} \leq 1 - \left(\frac{d}{2n}\right) \log_2 3 - H\left(\frac{d}{2n}\right), \tag{5.29}$$

while the quantum GV bound for CSS codes is given by [88]

$$\frac{k}{n} \geq 1 - 2H\left(\frac{d}{n}\right). \tag{5.30}$$

Both the quantum Hamming bound and the quantum GV bound of Fig. 5.12 serve the same purpose as the classical Hamming bound and the GV bound seen in Fig. 5.8. Explicitly, they portray the upper bound and the lower bound of normalized minimum distance versus quantum coding rate trade-off. Once again, the puzzling behaviour of classical TECCs resurfaces for the QTECCs, as observed in Fig. 5.12. Since all the QBCH codes, quantum Hamming codes and QTECCs inherit the properties of their classical counterparts, their behaviour is reminiscent of that of their classical counterparts. As for the QTECCs, the definitive interpretation of this unusual behaviour is left for future exploration in our

Table 5.10: Code parameters of QBCH codes having codeword length of $n = 127$, which is used in Fig. 5.11 and 5.12. The quantum coding rate r_Q and normalized minimum distance δ are calculated using Eq. (5.1) and (5.17), respectively.

n	k	d	n	k	d
127	1	19	127	71	9
127	15	16	127	85	7
127	29	15	127	99	5
127	43	13	127	113	3
127	57	11			

research. Nonetheless, for a relatively long codeword, the QTECCs are reminiscent of QLDPC codes. Observe from Fig. 5.12 that both the normalized minimum distance and the quantum coding rate of QTECCs tend to zero upon increasing the minimum distance by increasing the codeword length. Therefore, the QTECCs are deemed to be more favourable for short to medium codeword lengths.

5.4 Performance of Quantum Topological Error Correction Codes

In this treatise, we consider the performance of QTECCs under the popular quantum depolarizing channel. Explicitly, the quantum depolarizing channel is characterized by the quantum depolarizing probability p inflicting an error pattern constituted by the Pauli operators $P \in \mathcal{P}_n$ upon the state of physical qubits, where each qubit may independently experience a bit-flip error ($\mathbf{X}$), a phase-flip error ($\mathbf{Z}$), or both bit-flip and phase-flip error ($\mathbf{Y}$) with an equal probability of $p/3$. In order to get a more precise insight into the performance trends of QTECCs, we have to distinguish how the different error patterns affect the state representing the physical qubits. Explicitly, the n-tuple Pauli error pattern may be classified as follows, which will be exemplified in Fig. 5.13 and 5.14 after their definitions:

(a) **Harmful detected error pattern**. This specific type of error pattern has a similarity to the conventional bit error in the classical domain. The error pattern of $\mathcal{P}$ anti-commutes with the stabilizer operators $S_i \in \mathcal{S}$ hence triggers non-trivial syndrome values.

(b) **Harmful undetected error pattern**. The error pattern commutes with all of the stabilizer operators, except that it does not belong to the stabilizer group $\mathcal{S}$. In the classical domain, this is similar to the error pattern that returns the all-zero syndrome. The error pattern is harmful, since it does not trigger a non-trivial syndrome value, yet it corrupts the legitimate state of the physical qubits.

(c) **Harmless undetected error pattern**. This particular error pattern does not have any classical analogue. The error pattern is harmless because it belongs to the stabilizer group $\mathcal{S}$. This is also referred to as a degenerate error pattern. Consequently, the error pattern does not alter the legitimate state of the physical qubits. By considering the degeneracy, the actual performances of QTECCs are potentially improved.

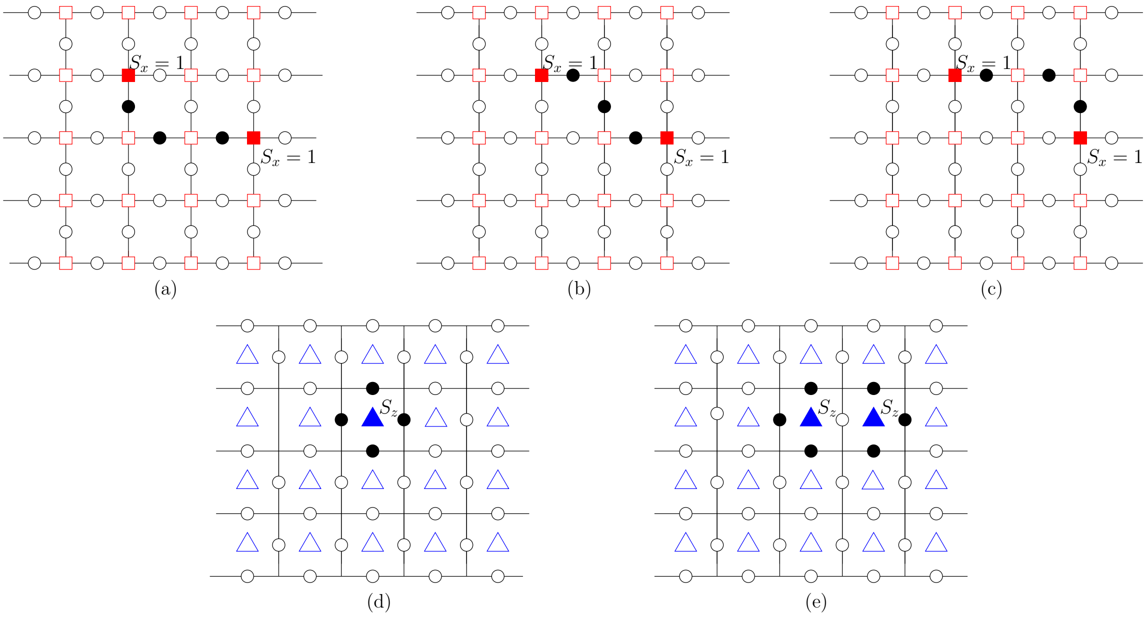
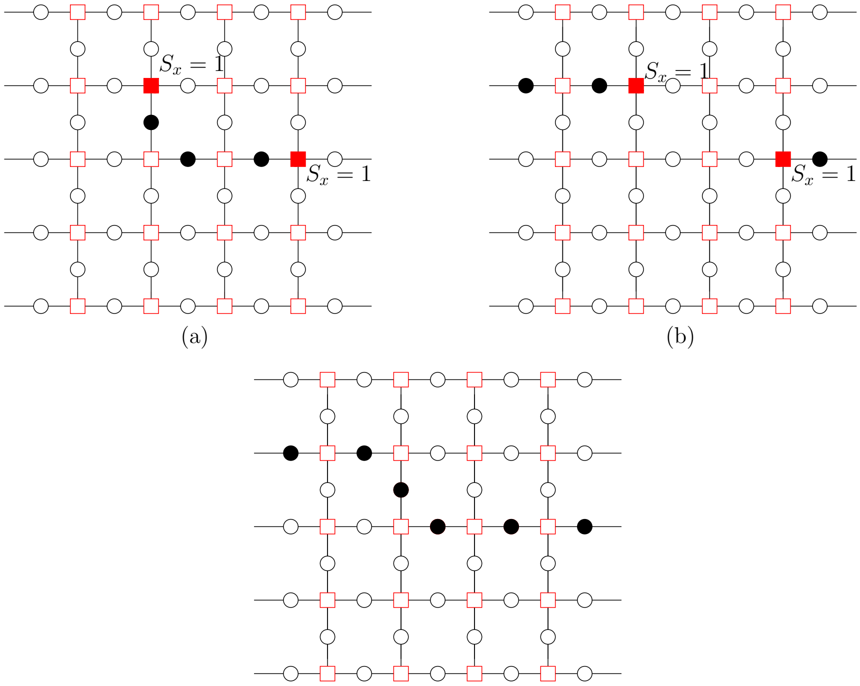


Figure 5.13: Illustration of how the error recovery operator $\mathcal{R}$ creates the degenerate error patterns and how the degeneracy nature of QECCs may improve the performance of QTECCs. All of the error patterns given in (a), (b) and (c) represent error patterns generating an identical syndrome value. Without loss of generality, let us assume that based on the generated syndrome value, the decoder always decides to perform error recovery operator $\mathcal{R}$ of (a) on the corrupted state of physical qubits. If the actual error pattern is (a), the corrupted state of physical qubits will be fully recovered. By contrast, figure (d) shows the resultant error pattern if the actual error pattern is (b), but it is corrected using the error pattern given in (a). Moreover, figure (e) represents the resultant error pattern if the actual error pattern is (c) and it is corrected using the error recovery pattern of (a). As a result, the error pattern (d) represents a stabilizer operator of a plaquette, while the error pattern (e) resembles the product of two adjacent stabilizer operators. Both error patterns of (d) and (e) constitute the *harmless undetectable error patterns*, since they belong to the stabilizer group $\mathcal{S}$. Therefore, the state of physical qubits is not altered after the recovery operator $\mathcal{R}$ of (a) is applied to all error patterns of (a), (b) and (c). In classical setup, both error patterns (d) and (e) are considered as error events. However, in the quantum domain, both error patterns (d) and (e) are considered as error-free cases. This specific error-type has no similarity in the classical domain and hence potentially improves the performance of QTECCs.

To illustrate both the harmless and harmful undetected error patterns, we refer to Fig. 5.13 and 5.14. First, we commence with the harmless undetected error pattern, which is illustrated in Fig. 5.13. In this example, we consider a surface code having a minimum distance of 5, which implies that it is only capable of correcting two-qubit errors. Following the stabilizer formulation of QTECCs discussed in Section 5.3, the physical qubits are arranged along the edges of the square lattice, while the **X** stabilizer operators are located in the vertices. Therefore, the **X** stabilizer operators on the vertices are used for indicating the **Z** errors, which will trigger eigenvalues of -1 if they anticommute with the **X** stabilizer operators. Let us assume that the quantum depolarizing channel inflicts three **Z** errors



(a)

(b)

(c)

Figure 5.14: Illustration of the harmful undetectable error pattern in the quantum domain. The actual error pattern inflicts the state of physical qubits is given in (b), while the decoder always decides to perform a recovery operator given in (a). Instead of recovering the legitimate state of the physical qubits, the specified error recovery procedure generates a chain of error that commutes with all of the stabilizer operators, as shown in (c). In the quantum domain, it constitutes the *harmful undetectable error patterns*. In the classical domain, it resembles the error pattern that generates all-zero syndrome values.

on the physical qubits, which are denoted by the filled black circles in Fig 5.13, while the hollow black circles represent the error-free physical qubits. All of the error patterns given in Fig 5.13 (a), (b) and (c) trigger the eigenvalues of -1 for the stabilizer operators denoted by filled red squares, while the rest of the stabilizer operators are represented by hollow red squares, which return eigenvalues of $+1$. Since the decoder relies on hard-decision ML decoding, all of the error patterns given in Fig. 5.13 (a), (b) and (c) have the same probability of occurrence. Let us assume that the decoder always decides to apply the error recovery pattern of Fig. 5.13 (a) for the specified values of stabilizer measurement. When the actual error pattern is the one given in Fig. 5.13 (a), the states of the physical qubits are fully recovered. By contrast, if the actual error pattern is the one seen in Fig. 5.13 (b), but it is corrected using the error recovery operator of Fig. 5.13 (a), we arrive at the accumulated error pattern shown in Fig. 5.13 (d). Lastly, when the actual error pattern is the one given by Fig. 5.13 (c), but we attempt to correct it using the error recovery of Fig. 5.13 (a), we obtain the error pattern seen Fig. 5.13 (e). However, if we observe closely the error pattern illustrated in Fig. 5.13 (d), it is reminiscent of a plaquette $\mathbf{Z}$ stabilizer operator denoted by the filled blue triangle. Therefore, based on the definition of stabilizer operators, the error pattern given in Fig. 5.13 (d) does not alter the legitimate state of physical qubits. Similarly, the error pattern of Fig. 5.13 (e) resembles the product of two adjacent plaquette stabilizer operators. Since the product between a pair of stabilizer operators return another valid stabilizer operator, the error pattern given in Fig. 5.13 (e) belongs to the stabilizer group $\mathcal{S}$. Once again, by definition, the error pattern given in Fig. 5.13 (e) does not corrupt the legitimate state of physical qubits. This is an example of *harmless undetectable error patterns.*

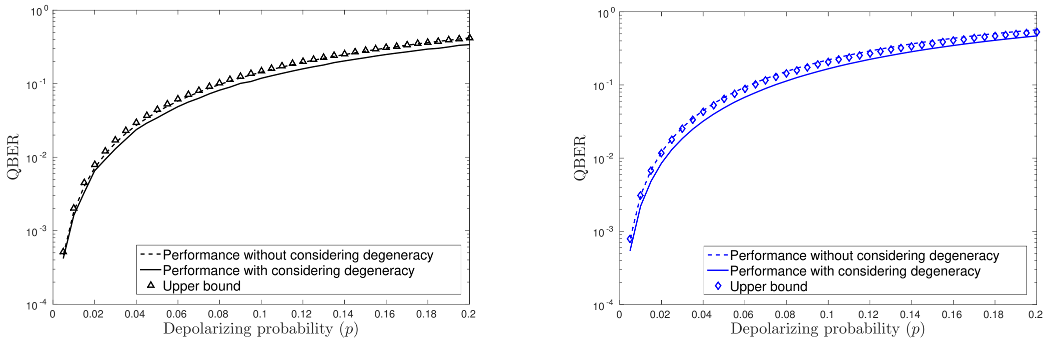
To elaborate a little further, a harmless undetected error can be directly generated by the quantum decoherence, where the Pauli operator $P \in \mathcal{P}_n$ imposed by the quantum depolarizing channel is identical to the stabilizer operator S_i. Another possibility is that it is generated by the associated error recovery procedure when trying to recover an ambiguous error pattern, where there are more than one possible error patterns associated with a specific syndrome value, as illustrated in Fig. 5.13. The degeneracy property, which is associated with the harmless undetectable error patterns, does not have a classical analogue, because the resultant error patterns illustrated in Fig. 5.13 (d) and (e) will always be considered as an error in the classical setup. Ultimately, considering the degeneracy potentially improves the performance of QECCs.

Let us consider a range of different scenario for illustrating the presence of harmful undetected error patterns, which is portrayed in Fig. 5.14. Similar to the previous example of Fig. 5.13, three $\mathbf{Z}$ errors are imposed on the state of logical qubits by the quantum depolarizing channel. The error patterns given in Fig. 5.14 (a) and (b) trigger the eigenvalues of -1 for the stabilizer operators denoted by filled red squares in Fig. 5.14, while the rest of the stabilizer operators represented by hollow red squares return eigenvalues of $+1$. Given the associated syndrome value, the decoder always decides to apply the error recovery operator of Fig. 5.14 (a). In the specific scenario, where the actual error pattern is the one given by Fig. 5.14 (b), the resultant error pattern is given in Fig. 5.14 (c). We can observe that the resultant error pattern of Fig. 5.14 (c) commutes with all of the stabilizer operators in Fig. 5.14. However, this specific error pattern does not belong to the stabilizer operator $\mathcal{S}$, since we cannot represent a chain of errors by the product of stabilizer operators. Consequently, this undetectable error pattern inevitably corrupts the legitimate state representing the physical qubits. This is an example of the *harmful undetectable error patterns.* This error pattern is similar to that of its counterpart in the classical domain, where the error pattern returns the all-zero syndrome.

Therefore, based on these conditions, by modifying the probabilty of correct decoding in the classical domain [167], we can readily formulate the worst-case upper bound QBER performance of QTECCs as

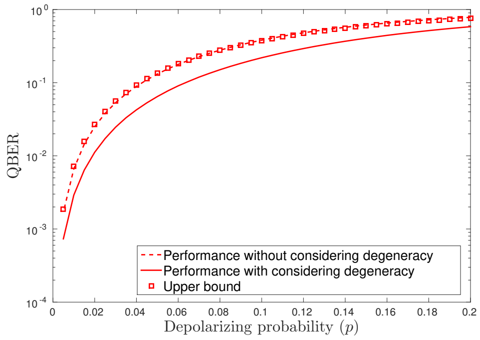
$$\text{QBER}_{\text{upper}}(n, d, p) = 1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i} - \sum_{i=1, \forall S_i \in \mathcal{S}}^{|\mathcal{S}|} p^{w(S_i)} (1-p)^{n-w(S_i)}, \quad (5.31)$$

where $w(S_i)$ is the weight of the stabilizer operator S_i, which is defined by the number of non-identity Pauli operators within the stabilizer operators. The second term of Eq. (5.31) represents all the correctable error patterns of QTECCs, while the last term of Eq. (5.31) represents the degenerate error patterns that belong to the stabilizer operators. For example, let us revisit the construction of the surface codes of Fig. 5.9. There are 12 stabilizer generators for a distance-3 surface code, as seen in Table 5.6. Hence, we can potentially generate 2^{12} unique stabilizer operators, since the product of the stabilizer operators returns another valid stabilizer operator. However, in order to further simplify the expression given in Eq. (5.31), we only consider the error patterns resembling the specified stabilizer operators given in Table 5.6, since they exhibit a lower weight of non-identity Pauli matrices and hence have a higher probability of occurance. Therefore, for surface codes, the last term of Eq. (5.31) can be approximated as $(2d^2 - 2d)p^4(1-p)^{n-4}$. The term $(2d^2 - 2d)$ represents the number of stabilizer operators, which is given in Table 5.8, and we assume that all the weight of the stabilizer operators $w(S_i)$ are equal to 4.



(a) Colour codes.

(b) Rotated-surface codes.



(c) Surface codes.

Figure 5.15: QBER performance of the distance-3 QTECCs over the quantum depolarizing channel, which is capable of correcting a single qubit error. The code parameters are given in Table 5.11. For this scenario, the decoder using hard-input ML decoding approach for predicting the error pattern.

5.4.1 QBER Versus Depolarizing Probability

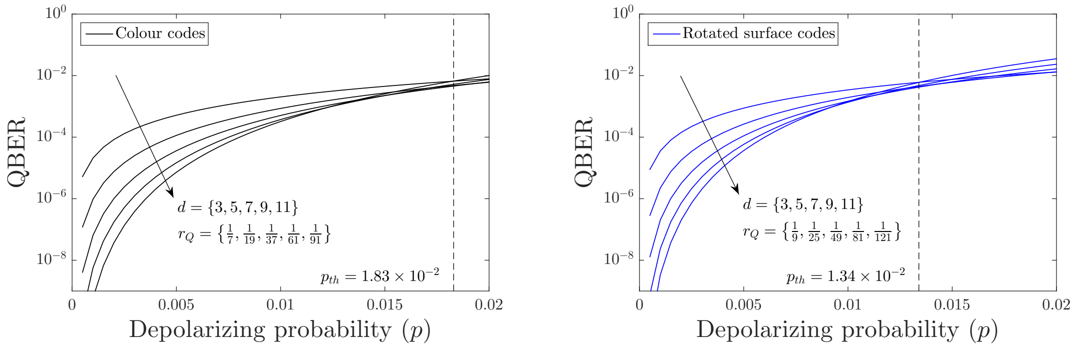
In order to characterize the performance of QTECCs by simulations, we exploit the fact that the QTECCs belong to the family of CSS codes, which handle the bit-flips (**X**) and phase-flips (**Z**) separately. Hence, we invoke two independent binary symmetric channels (BSC), one for the **X** channel and one for the **Z** channel, where each channel is characterized by the flip probability of $2p/3$, where p is the associated depolarizing probability of the quantum depolarizing channel [71, 75]. The decoder utilizes hard-decision ML decoding relying on a simple LUT decoder, as exemplified in Section 3.3. However, this classical-

Table 5.11: Code parameters for distance-3 colour code, rotated-surface code and surface code.

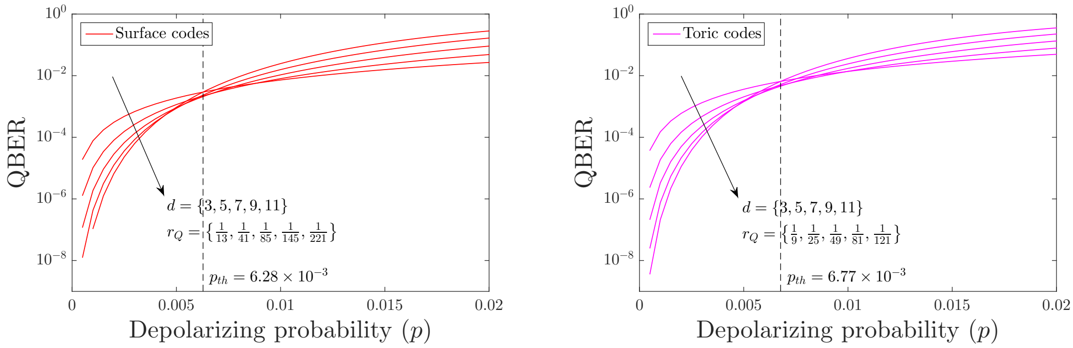
Code type	n	k	d	r_Q
Colour code	7	1	3	1/7
Rotated-surface code	9	1	3	1/9
Surface code	13	1	3	1/13

domain simulation only represents the performance of QTECCs without considering the degenerate error patterns. To elaborate a little further, we transmitted all-zero information bits. Therefore, we always consider the non-all-zero bits at the decoder output as an error. In order to additionally consider several cases of degenerate error patterns, which is exemplified in Fig. 5.13, we performed another evaluation step. We evaluate the non-all-zero corrected received words and check for the degenerate error patterns. If it satisfies to the degenerate error pattern criterion that we have above, we conclude that this is an error-free case. However, we are not capable of providing a complete list of all possible degenerate error patterns and in this treatise, we only consider the error pattern resembling the stabilizer generators of S_i, which is exemplified in Table 5.6 and 5.7 for surface codes and triangular codes, respectively. The QBER performance of distance-3 QTECCs versus the quantum depolarizing probability is portrayed in Fig. 5.15, where the code parameters are given in Table 5.11. We also include the upper bound of the QTECCs performance of Eq. (5.31) in Fig. 5.15. It can be observed that the upper bounds match with the QTECCs performance without considering the degenerate error patterns.

As we mentioned earlier, there are two sources of the degenerate error pattern at the output of the decoder. Firstly, the degenerate error pattern that imposed directly by the quantum channel, where the error exhibits an identical pattern to the stabilizer operator S_i. Secondly, the degenerate error pattern generated by the recovery operator $\mathcal{R}$, when it tries to recover the legitimate physical qubits, as illustrated in Fig. 5.13. The second case is more dominant than the first one. The reason can be explained as follows. Let us assume the **Z** stabilizer operators of distance-3 surface code given in Table 5.6. There are six **Z** stabilizer operators correspondent to the $2^6 = 64$ possible syndrome vector, including the error-free scenario. Remember that the distance-3 surface code can only correct flawlessly a single error qubit within a block of 13 physical qubits, where each of the single-qubit error pattern associated with only one syndrome vector. In other words, amongst all of 64 possible syndrome vectors, there are only 13 syndrome vectors used to uniquely distinguish the correctable error patterns, while the rest of the syndrome vectors are associated with the error pattern ambiguity, as exemplified in Fig. 5.13 and 5.14. Due to this reason, the QTECCs are considered as highly degenerate QSCs. Hence, the upper bound of the QBER performance matches the simulation-based performance recorded without considering the degeneracy, since it considers the first case of degeneracy, where we only consider a portion of all valid stabilizer operators $S_i \in \mathcal{S}$ in Eq. (5.31). As expected, by accommodating both of the degeneracy cases, the QBER performance of QTECCs are improved, as portrayed in Fig. 5.15.



(a) Colour codes. (b) Rotated-surface codes.



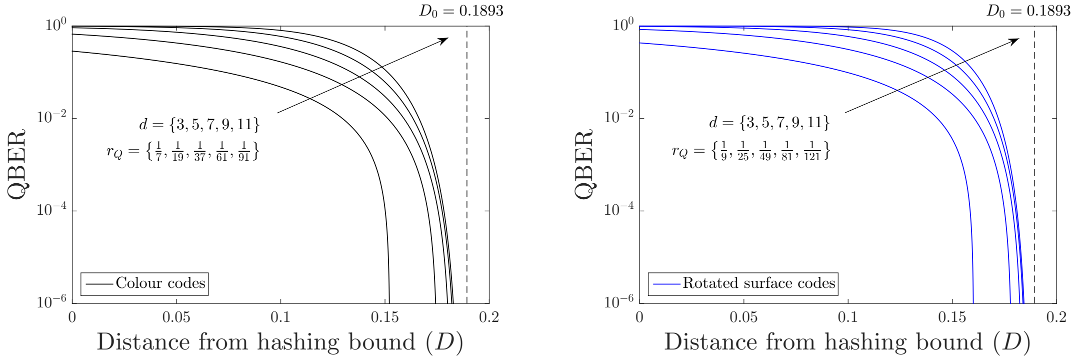
(c) Surface codes. (d) Toric codes.

Figure 5.16: Upper bound QBER performance of QTECCs for the minimum distance of $d = \{3, 5, 7, 9, 11\}$ based on Eq. (5.31) and code parameters given in Table 5.8. The crossover amongst the QBER curves represents the threshold probability (p_{th}), which are portrayed in dashed line.

5.4.2 QBER Versus Distance from Hashing Bound

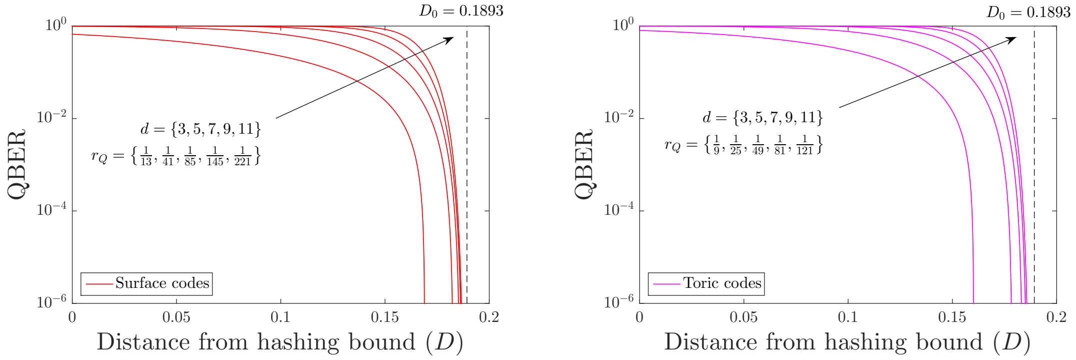
Increasing the minimum distance of a given QSC construction, which directly improves its per-codeword error correction capability (t), is achieved by increasing the number of physical qubits (n) or by decreasing the quantum coding rate. Specifically for QTECCs, increasing the minimum distance means increasing the number of physical qubits (n) and decreasing the quantum coding rate (r_Q) simultaneously. Naturally, the goal of increasing the minimum distance of the QSC is to achieve a better QBER performance. However, the improvement of QBER the performance can only be observed below a certain value of depolarizing probability (p), which may be referred to as the threshold probability (p_{th}). Using the upper bound QBER performance of Eq. (5.31), we plot the QBER curves for colour, rotated-surface, surface and toric codes in Fig. 5.16. For each of the QTECC constructions, we portray the upper bound QBER performance for the minimum distances of $d = \{3, 5, 7, 9, 11\}$. The threshold probability of each code is denoted by the crossover QBER curves, which we portray in dashed line. The threshold probability of colour codes, rotated-surface, surface and toric codes are 1.83×10^{-2}, 1.34×10^{-2}, 6.28×10^{-3} and 6.77×10^{-3}, respectively.

However, presenting the performance of QTECCs over quantum depolarizing channel by portraying the QBER curves versus the depolarizing probability (p) does not take the



(a) Colour codes.

(b) Rotated-surface codes.



(c) Surface codes.

(d) Toric codes.

Figure 5.17: Upper bound performance of QTECCs in term of the QBER versus the distance D from the hashing bound. The dashed lines portray the ultimate distance to the quantum hashing bound of $D_0 = 0.1893$.

quantum coding rate (r_Q) into consideration. As we mentioned earlier, we can simply decrease the quantum coding rate further and further to increase the error correction capability of the QTECCs. Nonetheless, for the sake of depicting a fair comparison upon reducing the quantum coding rate, we have to scrutinize how much performance improvement we obtain upon decreasing the quantum coding rate. Therefore, to demonstrate how much performance improvement we attain compared to how much we decrease the quantum coding rate, we normalize the QBER performance by incorporating the quantum hashing bound. More explicitly, the quantum hashing bound can be expressed as follows [168]:

$$C_Q(p) = 1 - H(p) - p.\log_2(3), \tag{5.32}$$

where $H(p)$ is the binary entropy of p. More specifically, the quantum hashing bound of Eq. (5.32) dictates that a random quantum code $\mathcal{C}$ having a sufficiently long codeword and a quantum coding rate $r_Q \leq C_Q(p)$ may yield an infinitesimally low QBER for a given depolarizing probability p. Alternatively, we can refer to $C_Q(p)$ as the hashing limit for the quantum coding rate r_Q associated with a given depolarizing probability p. In terms of its classical dual pair, the value of C_Q is similar to the capacity limit. Similarly, for a given coding rate r_Q, we can find a value of p^* satisfying $r_Q = C_Q(p^*)$, where p^* denotes the maximum value of depolarizing probability p so that a quantum code $\mathcal{C}$ having quantum coding rate of r_Q can operate at an infinitesimally low QBER. The value of p^* may be referred to as the hashing limit for depolarizing probability of p associated with a given quantum coding rate r_Q. In the classical domain, the value of p^* is similar to the noise limit. Therefore, in general, the aim is that of finding a QSC that is capable of performing as close as possible to the quantum hashing bound. For example, let us consider the distance-3 and distance-5 rotated-surface codes having quantum coding rate of $r_Q = 1/9$ and $r_Q = 1/25$, respectively. By substituting $C_Q = 1/9$ and $C_Q = 1/25$ into the Eq. (5.32), we obtain the noise limit of $p^* = 0.160$ and $p^* = 0.179$, respectively. It can be concluded that the noise limit is higher for the quantum code exhibiting a lower quantum coding rate. To incorporate the quantum hashing bound into the QBER performances of QTECC, we define the distance from hashing bound as follows:

$$D \triangleq p(r_Q) - p. \tag{5.33}$$

In other words, by changing the horizontal axis from the depolarizing probability p to the distance D from hashing bound, we shift all the QBER curves according to their hashing bounds, so that all the hashing bounds are at the reference point of $D = 0$.

Several pertinent questions arise from the quantum hashing bound formulation. Firstly, is there a noise limit, where no QSC constructions are capable of achieving a satisfactorily low QBER? Indeed, the answer is yes. By substituting the $C_Q = 0$ into Eq. (5.32), which is the lowest possible value of achievable quantum coding rate, we arrive at the ultimate hashing bound of $p(0) \approx 0.1893$. Secondly, what is the farthest possible distance from the quantum hashing bound for any QSC construction? To answer this question, we have to consider the worst-case scenario, where a QSC exhibiting a near-zero quantum coding rate ($r_Q \approx 0$) achieves an infinitesimally low QBER at near-zero quantum depolarizing probability ($p \approx 0$). By substituting the value of $r_Q = 0$ and $p = 0$ into Eq. (5.33), we define the ultimate distance of hashing bound D_0 as

$$\begin{aligned} D_0 &= p(0) - p \\ &= 0.1893 - 0 \\ &= 0.1893. \end{aligned} \tag{5.34}$$

Therefore, the desirable performance of any QSCs quantified in terms of the QBER versus distance from the quantum hashing bound is represented by the curves exhibiting a reasonably low QBER as close as possible to the reference point of $D = 0$. Naturally, this implies having a low QBER as far as possible from the ultimate distance from the hashing bound of $D_0 = 0.1893$. In simpler terms, any QSCs can only operate at a reasonably low QBER within the hashing bound range of $0 \leq D \leq D_0$. Furthermore, we should consider the quantum coding rate reduction of r_Q as beneficial only if the associated QBER performance curve moves closer to the reference point of $D = 0$. Otherwise, it is more advisable to find a better code construction exhibiting an identical quantum coding rate, to increase the number of physical qubits, while maintaining the quantum coding rate, or to invoke more powerful decoding scheme, for example by utilizing a soft-decision-aided decoder. The QBER performance of QTECCs versus their distances from the quantum hashing bound are portrayed in Fig. 5.17. It can be observed that even though increasing the minimum distance of the QTECCs yields a performance improvement in terms of their QBER versus depolarizing probability p shown in Fig. 5.17 in terms of their distance from the hashing bound D, at low QBER, the curves are crowded in the vicinity of the ultimate hashing bound distance of D_0. Moreover, the results show an agreement with the quantum coding rate versus minimum distance evolution of QTECCs seen in Fig. 5.12. The improvement of the minimum distance, which is directly linked to the error correction capability, is not fast enough upon reducing the quantum coding rate is not fast enough to compensate the increasing number of physical qubits. Therefore, we believe that QTECCs are most suitable for short to moderate codeword lengths.

5.4.3 Fidelity

From an implementational perspective, a quantum gate or quantum channel is often characterized by the so-called fidelity, which represents the closeness of a pure quantum state of $|\overline{\psi}\rangle$ compared to the mixed states having the quantum density operator of ρ. More explicitly, since the quantum channel imposes the quantum decoherence on our legitimate quantum state representing the physical qubits $|\overline{\psi}\rangle$, there is a probability that decoder does not successfully recover the legitimate state. Therefore, the ensemble of all the possible predicted legitimate state of physical qubits $|\widehat{\psi}\rangle$ can be represented using the state of $|\psi_i\rangle$ having a probability of p_i. The fidelity can be formulated as follows [87,169,170]:

$$F = \langle\overline{\psi}|\rho|\overline{\psi}\rangle. \tag{5.35}$$

while ρ, which portrays the statistical characteristics of a the mixed states, is defined by

$$\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|, \tag{5.36}$$

where the $|\psi_i\rangle$ represents all of the possible state in the ensemble and p_i is the probability of having state $|\psi_i\rangle$ in the ensemble, which is subject to unity constraint of $\sum_{i=1}^{N} p_i = 1$.

In order to demonstrate the benefit of QTECCs in the context of quantum depolarizing channel, we compare the so-called uncoded fidelity F_{uncoded} and final fidelity F_{coded}. The uncoded fidelity is the fidelity of the pure quantum state of $|\psi\rangle$ over the quantum depolarizing channel $\mathcal{P}$ unprotected by any QSCs scheme. Therefore, the uncoded fidelity F_{uncoded} can be expressed as follows:

$$F_{\text{uncoded}} = 1 - p. \tag{5.37}$$

The coded fidelity is that of the pure state of the desired output $|\psi'\rangle$ protected by the a QSC scheme after the recovery procedure $\mathcal{R}$ and inverse encoder $\mathcal{V}^\dagger$ of Fig. 6.4. Therefore, the coded fidelity F_{coded} of the quantum system can be readily described as

$$F_{\text{coded}} = 1 - \text{QBER}. \tag{5.38}$$

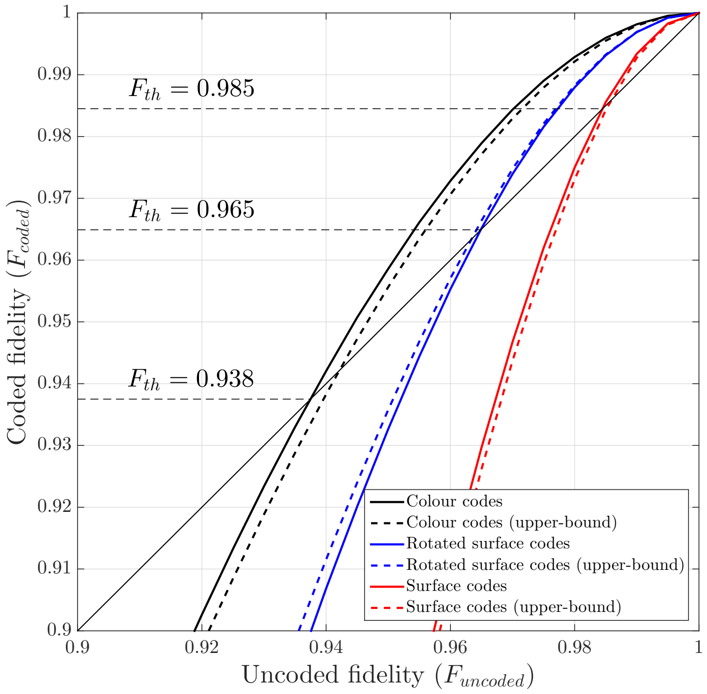
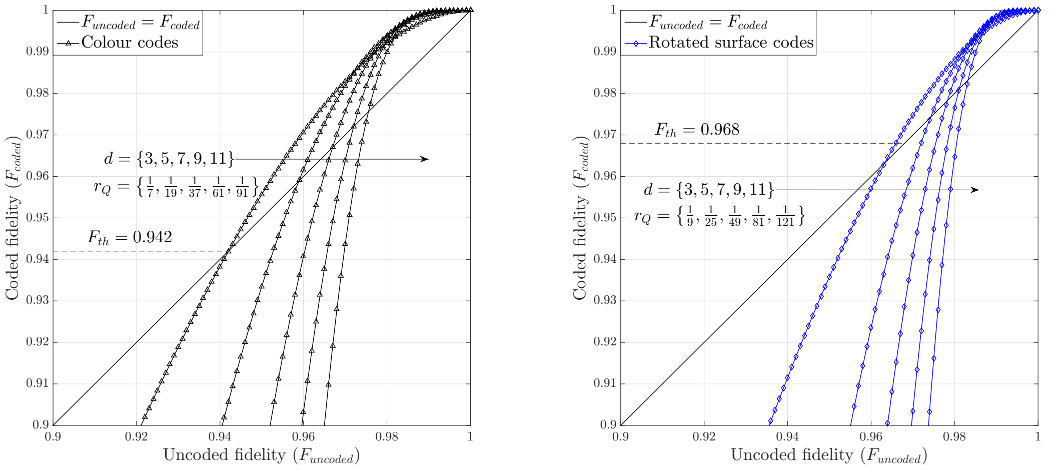


Figure 5.18: The performance of QTECCs having a minimum distance of 3 in terms of fidelity of Eq. (5.35). The colour code reaches the fidelity threshold earlier than the rotated-surface and surface code, since the colour code has the lowest number of physical qubits compared to the rotated-surface code and the surface code. The code parameters are given in Table 5.11

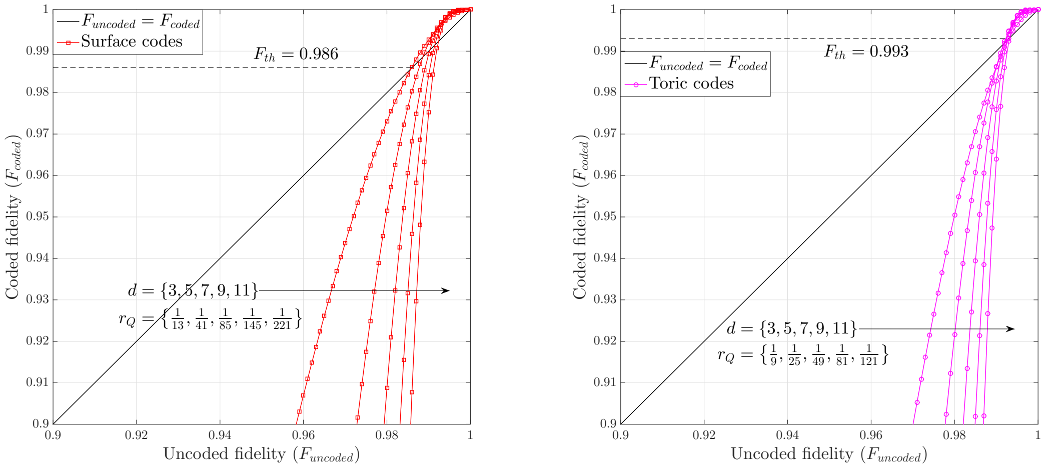
The fidelity performances for the distance-3 QTECCs are depicted in Fig. 5.18. The black solid line represents the condition of $F_{\text{uncoded}} = F_{\text{coded}}$. The crossover point between the line of $F_{\text{uncoded}} = F_{\text{coded}}$ and fidelity performance curve of QTECCs is the break-even point, which we may referred to as the *threshold fidelity* F_{th}. The break-even point denotes the minimal uncoded fidelity required to ensure that we do acquire a fidelity improvement upon the applicaton of the QSC scheme, which is invoked for protecting the state of the physical qubits. The upper bound of threshold fidelity F_{th} for the different types of QTECCs is depicted in Fig. 5.19. It can be observed that different code families having various minimum distances d result in different threshold fidelity F_{th}. For the QSCs utilizing hard-decision syndrome decoding, we derive the upper bound approximation formula for F_{th}. First, from Eq. (5.31) and Eq. (5.38), we arrive at

$$\begin{aligned} F_{\text{coded}} &= 1 - \text{QBER}_{\text{upper}} \\ &= 1 - \left(1 - \sum_{i=0}^{t=\lfloor\frac{d-1}{2}\rfloor} \binom{n}{i} p^i (1-p)^{n-i}\right) \\ &= 1 - \sum_{\lfloor\frac{d-1}{2}\rfloor+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}. \end{aligned} \tag{5.39}$$

For a low depolarizing probability p, the expression given in Eq. (5.39) can be approximated



(a) Colour codes. (b) Rotated-surface codes.



(c) Surface codes. (d) Toric codes.

Figure 5.19: Upper bound fidelity performance of QTECCs.

in order to determine the upper bound of the output fidelity as follows:

$$F_{\text{coded}} \approx 1 - \binom{n}{\lfloor \frac{d-1}{2} \rfloor + 1} p^{\lfloor \frac{d-1}{2} \rfloor + 1}. \tag{5.40}$$

Since the threshold fidelity satisfies the relationship of $F_{\text{th}} = F_{\text{uncoded}} = F_{\text{coded}}$, we can substitute $F_{\text{coded}} = F_{\text{th}}$ and $p = 1 - F_{\text{th}}$ into Eq. (5.40). Finally, the upper bound for the threshold probability can be encapsulated as

$$F_{\text{th}}(n, d) = 1 - \binom{n}{\lfloor \frac{d-1}{2} \rfloor + 1}^{-1/\lfloor \frac{d-1}{2} \rfloor}. \tag{5.41}$$

For example, the threshold for a distance-3 colour code having a quantum coding rate $r_Q = 1/7$ based on Fig. 5.19(a) is $F_{\text{th}} = 0.942$, while using the upper bound approximation of the fidelity threshold in Eq. (5.41) we have $F_{\text{th}} = 0.952$. For the distance-3 of rotated-surface code, surface code and toric code, the threshold fidelity values based on Fig. 5.19(b), 5.19(c) and 5.19(d) are $F_{\text{th}} = 0.968$, $F_{\text{th}} = 0.986$ and $F_{\text{th}} = 0.993$, respectively. By using the approximation of Eq. (5.41), the upper bound fidelity thresholds are given by $F_{\text{th}} = 0.972$, $F_{\text{th}} = 0.987$ and $F_{\text{th}} = 0.994$, respectively for the distance-3 rotated-surface code, surface code and toric code. Here, we used the family of QTECCs as our representative examples, while the threshold fidelity of Eq. (5.41) is generically applicable for any QSCs using hard-decision syndrome decoding. Ultimately, the implementation of QTECCs are capable of reducing the effect of quantum decoherence, which is demonstrated by the QBER reduction and also improving the reliability of quantum channel, which is demonstrated by the fidelity improvement.

5.5 Summary and Conclusions

We portrayed the evolution of the topological error correction codes designed in the classical domain to their quantum-domain dual pairs. We showed that by arranging the bits of the codeword on a lattice structure in the classical domain provides a beneficial inherent error correction capability. Furthermore, for a long codeword, the classical topological error correction codes (TECCs) correspond to the family of LDPC codes exhibiting attractive properties, such as unbounded minimum distance as a function of the codeword length, structured construction and a coding rate of $r = 1/2$. By contrast, the quantum topological error correction codes (QTECCs) are more suitable for applications requiring short to moderate codeword lengths, since the quantum coding rate of QTECCs tends to zero for a long codeword. We characterized the performance of QTECCs in the face of the quantum depolarizing channel in terms of the QBER attained. First, we showed that QTECCs are highly degenerate quantum codes, therefore the classical simulation is only capable of portraying the performance of QTECCs without considering the degeneracy property. Secondly, we demonstrated that increasing the minimum distance of the QTECCs improves QBER performance. Additionally, we normalized the performance by considering the coding rate, which was achieved by introducing the *distance from the hashing bound*. Explicitly, we have shown that the growth of minimum distance of QTECCs upon increasing the codeword length is not fast enough to compensate for the increased codeword length. Consequently, the QBER performance of QTECCs gradually tends to the *ultimate distance from the hashing bound*. Finally, we determined the fidelity threshold for QSCs based on hard-decision syndrome decoding, which represents the minimum fidelity value required for a quantum system to glean benefits from QSCs. Ultimately, the employment of QSCs will improve the reliability of quantum computers.

Chapter 6

Protecting Quantum Gates Using Quantum Topological Error Correction Codes

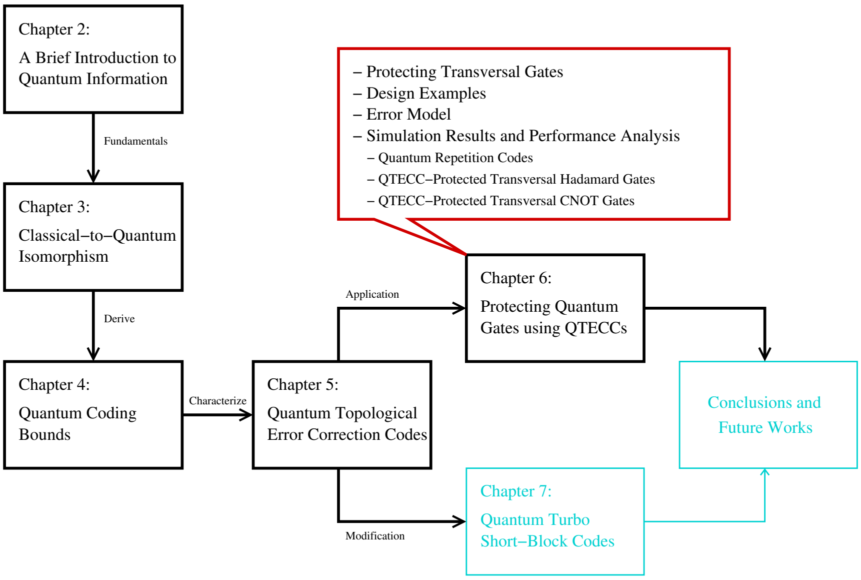


Figure 6.1: The outline of this thesis with the highlight of Chapter 6.

6.1 Introduction

So far, we have described the classical-to-quantum isomorphism for deriving and characterizing QSCs. In the classical domain, the error correction codes are invoked for dealing with the imperfections of the communication channel, either in a form of imperfections imposed by the transmission medium or by information storage. However, in the quantum domain, the quantum decoherence is imposed by the entanglement between the quantum information and environment, or by the coherence time of qubits, or by the imperfection of quantum gates. In the classical domain, we often assume that the information is contaminated by the transmission medium or by the storage medium. The imperfections of the encoding and decoding operations tend to have a negligible effect, hence they are usually ignored. However, in the quantum domain, the impact of imperfect quantum gates cannot be neglected. Consequently, the QSC can also be designed specifically for handling the imperfections caused by the quantum gates. Although the general principle is similar to that of protecting quantum information through the noisy quantum channel, several modifications are needed and additional constraints have to be considered.

In this chapter, we present the general framework of protecting quantum gates using QSCs. The ultimate goal of invoking QSCs is to answer the cardinal question: "is it possible to build reliable quantum computers using unreliable quantum circuits?" The concept of reliable computation using unreliable components can be traced back to Von Neumann's work in 1956 [171]. However, the work of Von Neumann is not directly applicable in the context of quantum computers, since he dealt with classical computation heavily relying on irreversible logic gates, while quantum computers are composed of reversible quantum gates. Realizing that in order to invoke QSCs we have to introduce additional unreliable quantum gates into the system, the field of fault-tolerant quantum computers was introduced [54,89, 91,95,172]. The quest for finding the answer was partly settled, when the threshold theorem was proposed [119]. The main result suggested that it is indeed possible to create a reliable quantum computer from unreliable quantum gates, given that the error probability of the quantum gates is below a certain probability threshold value and a reasonable redundant overhead is tolerable.

Now, it is pertinent to mention that throughout this thesis, we consider gate-based quantum computation [131, 173], noting that there are many other models for quantum computation, such as measurement-based quantum computation [174], quantum cellular automata [175], topological quantum computation [176], and adiabatic quantum computation [177]. Therefore, in this chapter, we refer the readers to the method presented in [148, 149, 178] for creating an efficient quantum encoder $\mathcal{V}$ for QSCs. To elaborate a little further, given the so-called stabilizer operators $S_i \in \mathcal{S}$, we can transform the stabilizer operators $S_i \in \mathcal{S}$ into their classical binary PCM using the so-called Pauli-to-binary isomorphism [1, 141]. The resultant binary PCM $\mathbf{H}$ derived from the stabilizer formalism $S_i \in \mathcal{S}$ is utilized for constructing the quantum encoder $\mathcal{V}$ of the associated QECC $\mathcal{C}$. Since we deal with the family of gate-based quantum computers, naturally, the quantum encoder $\mathcal{V}$ is also composed of quantum gates.

The method specified in [148, 149, 178] is applicable to both CSS [57, 88, 94] and non-CSS codes [62, 96]. However, colour codes [103], which belong to the QTECCs family, can also be classified further as the member of a more specific category of quantum CSS codes, namely, the family of dual-containing CSS codes. For dual-containing CSS codes, a specific technique can be invoked for creating the associated quantum encoder $\mathcal{V}$. This method of generating the quantum encoder $\mathcal{V}$ of dual-containing CSS codes has been detailed in [71, 134]. It is important to note that upon using the method detailed in [71, 134, 148, 149, 178], the number of quantum gates required for constructing a quantum encoder $\mathcal{V}$ for a QSC $\mathcal{C}$

is linearly proportional to the number of physical qubits [148, 178].

However, the need for invoking a of quantum encoder $\mathcal{V}$ can be eliminated by simply preparing all the auxiliary qubits in the state of $|+\rangle$ and then performing stabilizer measurements, as suggested in [179, 180]. By initializing all the $(n-k)$ auxiliary qubits in the $|+\rangle$ states, we create the superposition of all possible combination of all $(n-k)$-bit sequences. Therefore, to generate a legitimate encoded state of the physical qubits, we only require stabilizer measurements for projecting the space created by the above-mentioned initialization into a specific code space based on the classical bits obtained from the stabilizer measurements.

The rest of this chapter is organized as follows. We provide the formulation of our framework in Section 6.2. This is followed by the design examples of QSC-protected Hadamard gates and CNOT gates in Section 6.3, where we invoke a simple quantum repetition code as our QSC. To evaluate the performance of our proposed framework, in Section 6.4, we present the decoherence model utilized in our simulations. Then in Section 6.5, we quantify the performance of QTECC-protected transversal Hadamard gates and CNOT gates both in terms of their QBER and fidelity along with the derivation of the QBER upper bound. The lower bound of the depolarization fidelity threshold is also determined. Finally, we conclude in Section 6.6.

6.2 Protecting Transversal Gates

In this section, we present the design of QSC-protected quantum gates along with the pivotal theory in quantum information processing required for formulating the proposed framework.

6.2.1 Quantum Clifford Gates

The quantum gates manipulating the state of the qubits are represented using the unitary transformation U, which satisfies

$$U^{\dagger}U = \mathbf{I}. \tag{6.1}$$

Since the quantum gates themselves also potentially impose the deleterious effect of quantum decoherence, which is represented by the Pauli group $\mathcal{P}_n$, the evolution of quantum decoherence through the quantum gates can be described using the conjugation of the unitary transformation.

Let us assume that a unitary transformation of M is applied to a quantum state of $N|\psi\rangle$, where N is also a unitary transformation that has been applied previously. Therefore, the final quantum state is given by $MN|\psi\rangle$. Since M is a unitary transformation, thus we have

$M^\dagger M = \mathbf{I}$. The quantum state of $MN|\psi\rangle$ can be transformed as follows:

$$\begin{aligned} MN|\psi\rangle &= MNM^\dagger M|\psi\rangle \\ &= VM|\psi\rangle. \end{aligned} \tag{6.2}$$

Therefore, we have

$$V = MNM^\dagger, \tag{6.3}$$

where V is the conjugate of N under the unitary transformation M. Consequently, Eq. (6.3) implies that the unitary transformation $MNM^\dagger$ after the operator M acts similarly to the unitary transformation N before the operator M. For instance, a Hadamard gate is defined by a unitary matrix as follows:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{6.4}$$

The transformation carried out by the Hadamard gates map the quantum state in computational basis into the Hadamard basis, as described below:

$$\begin{aligned} \mathbf{H}|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \equiv |+\rangle, \\ \mathbf{H}|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv |-\rangle \end{aligned} \tag{6.5}$$

and vice versa. Based on the conjugation of Eq. (6.3), we arrive at the following transformations:

$$\begin{aligned} \mathbf{HXH}^\dagger &= \mathbf{Z}, \\ \mathbf{HZH}^\dagger &= \mathbf{X}, \\ \mathbf{HYH}^\dagger &= -\mathbf{Y}. \end{aligned} \tag{6.6}$$

One way to interpret the transformation given in Eq. (6.6) is that a bit-flip ($\mathbf{X}$) error before the Hadamard gate is equivalent to a phase-flip ($\mathbf{Z}$) error after the Hadamard gate. Similarly, a phase-flip ($\mathbf{Z}$) error before the Hadamard gate can be treated as an $\mathbf{X}$ error after the Hadamard gate. Another example is the phase gate ($\mathbf{S}$), which is defined by the unitary transformation of

$$\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{6.7}$$

Based on Eq. (6.3) and on the unitary matrix of $\mathbf{S}$ in Eq. (6.7), we arrive at the following transformations:

$$\begin{aligned}\mathbf{SXS}^\dagger &= \mathbf{Y}\\ \mathbf{SZS}^\dagger &= \mathbf{Z}\\ \mathbf{SYS}^\dagger &= -\mathbf{X}\end{aligned} \tag{6.8}$$

Moreover, the relationship given in Eq. (6.3) can also be adopted to the model of the conjugation over two-qubit quantum gates. An example of two-qubit quantum gate is CNOT, whose unitary transformation is defined by the following unitary matrix:

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{6.9}$$

A CNOT gate is a two-qubit quantum gate, where the first qubit is called control qubit and the second qubit is referred to as target qubit. The value of target qubit is flipped if and only if the value of control qubit is equal to one. Based on Eq. (6.3), the two-qubit conjugation over the CNOT gate can be readily formulated as follows:

$$\begin{aligned}(\mathbf{CNOT})(\mathbf{X}\otimes\mathbf{I})(\mathbf{CNOT})^\dagger &= \mathbf{X}\otimes\mathbf{X},\\ (\mathbf{CNOT})(\mathbf{I}\otimes\mathbf{X})(\mathbf{CNOT})^\dagger &= \mathbf{I}\otimes\mathbf{X},\\ (\mathbf{CNOT})(\mathbf{Z}\otimes\mathbf{I})(\mathbf{CNOT})^\dagger &= \mathbf{Z}\otimes\mathbf{I},\\ (\mathbf{CNOT})(\mathbf{I}\otimes\mathbf{Z})(\mathbf{CNOT})^\dagger &= \mathbf{Z}\otimes\mathbf{Z}.\end{aligned} \tag{6.10}$$

We can also interpret the result as an error transformation or an error propagation process, illustrated in Fig. 6.2. It can be observed that a bit-flip or **X**-type error imposed on the control qubit before the CNOT gate will propagate to the target qubit after the CNOT gate. Meanwhile, a **Z**-type error inflicted upon the target qubit before the CNOT gate will impose another **Z**-type error on the control qubit after the CNOT gate.

In this chapter, we limit our discussions to quantum gates belonging to the Clifford group, since the stabilizer formalism of QTECCs will be preserved under conjugation [53, 132]. The theory of protecting quantum circuits using QSCs has been widely investigated [54, 89, 90, 91, 95, 172, 181] and in this chapter, we provide a comparative study of the quantum circuits protected by QSCs, specifically by the family of QTECCs. The most reasonable way of embedding QSCs into quantum gates is by the transversal implementation of quantum gates. The physical interpretation of the transversal implementation of QTECCs, specifically that of CNOT gates, is illustrated in Fig. 6.3. In the physical implementation, we can imagine having a pair of lattice structures arranged on a wafer, where each of the physical qubit layers is encoded using a QTECC scheme. The first qubit from the upper layer acts as the control qubit, while the first qubit from the lower layer serves

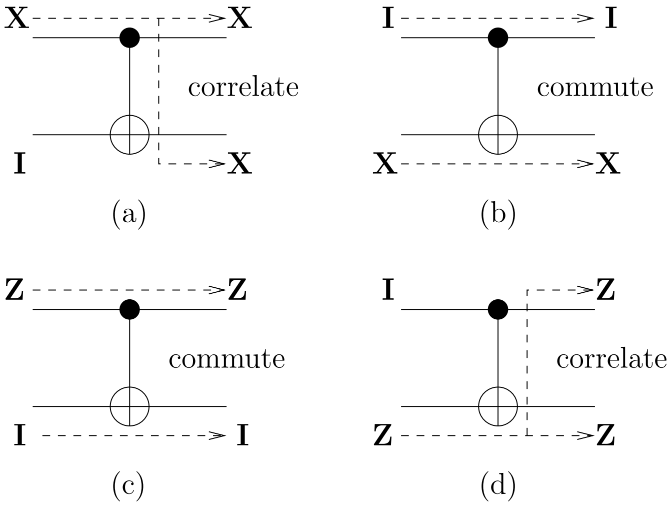


Figure 6.2: The evolution of two-qubit unitary transformation over the CNOT quantum gate, which is the circuit level interpretation of Eq. (6.10). For example, an **X**-type error imposed on the control qubit will propagate to the target qubit after the CNOT gate, as we can observe in (a). By contrast, a **Z**-type error inflicting the target qubit will propagate to the control qubit after the CNOT gate, which is shown in (d).

as the target qubit. It is followed by the second, the third, and all the remaining physical qubits from the upper as well as the lower layer.

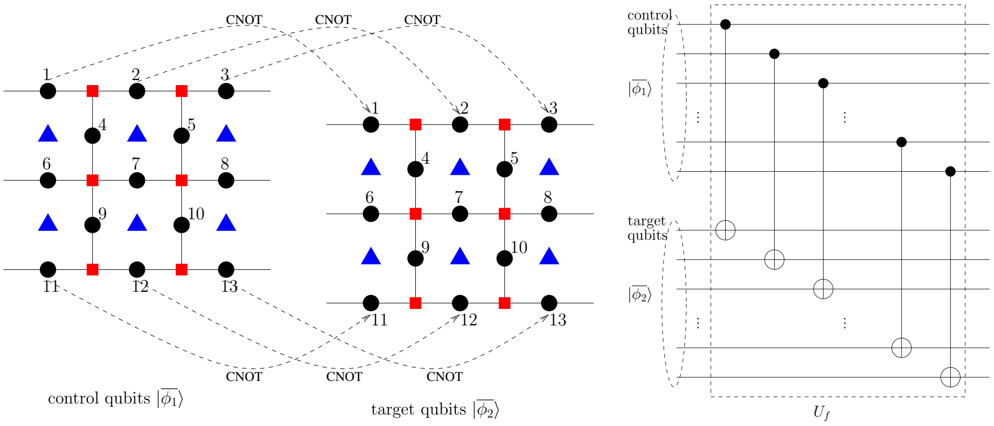
6.2.2 Design Formulation

The employment of QSCs for protecting the quantum circuits indeed increases the reliability of quantum computing, as shown in [134]. However, in order to avoid a perpetual encoding and decoding process throughout the quantum circuit before the number of errors exceeds the error correction capability of the QSC, we present a more efficient framework, where we encode the logical qubits at the input of the quantum circuit and decode them afterwards at the output of the computational step. However, the unitary transformation U_f applied to the state of physical qubits alters the legitimate state of physical qubits. Therefore, the initial stabilizer operators $S_i \in \mathcal{S}$ designed for stabilizing the legitimate state of physical qubits are no longer valid after the application of the unitary transformation U_f. Fortunately, we are able to conceive an *effective stabilizer formalism* and *effective inverse encoder* for successfully circumventing the problem[1].

To elaborate a little further, let us observe the basic model for QSC portrayed of Fig. 6.4 and the basic scheme of protecting quantum gates using QSC, as depicted in Fig. 6.5. We would like to highlight the main differences between the conventional QSC scheme of Fig. 6.4 and the QSC scheme conceived for protecting the quantum gates shown in Fig. 6.5. Firstly, in Fig. 6.4, the stabilizer operators $S_i \in \mathcal{S}$ are designed for stabilizing the state of physical qubits $|\overline{\psi}\rangle$, while the effective stabilizer operators $\widehat{S}_i \in \widehat{\mathcal{S}}$ in Fig. 6.5 are constructed for stabilizing the state of physical qubits after the unitary transformation $U_f|\overline{\psi}\rangle = |\overline{\psi_2}\rangle$.

---

[1] The term *effective* means that the stabilizer formalism and the inverse encoder at the output of computational step takes into account both the initial stabilizer formalism and quantum encoder when we encode the logical qubits at the input and the unitary transformation applied upon the input physical qubits.



(a) Physical implementation. (b) Gate-level implementation.

Figure 6.3: The physical and gate-level implementation of the transversal CNOT gates. In the physical implementation, we can imagine two layers of physical qubits, where on each layer the physical qubits are arranged over a lattice structure portrayed in Fig. 5.9. The CNOT interactions are performed accordingly on each of the pairs of physical qubits. The CNOT interactions between the physical qubits number #4 to #10 are removed from the figure for the sake of avoiding obfuscation. In the gate-level implementation, the physical layout portrayed in (a) can be translated into a chain of CNOT gates illustrated in (b).

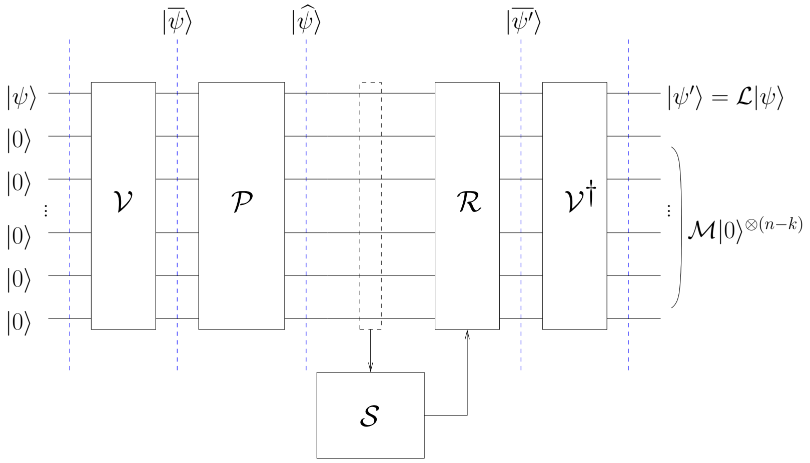


Figure 6.4: The basic model of QSCs implementation over the quantum depolarizing channel. The standard scheme for protecting the encoded state of physical qubits $|\overline{\psi}\rangle$. In this scheme, the purpose of applying a QSC is to recover the state of logical qubit $|\psi\rangle$ by stabilizing the state $|\overline{\psi}\rangle$ using the stabilizer operators $S_i \in \mathcal{S}$ in the presence of depolarizing channel $\mathcal{P}$.

Consequently, the recovery procedures of $R_i \in \mathcal{R}$ based on stabilizer operators $\mathcal{S}$ is also modified according to the effective stabilizer operators $\widehat{\mathcal{S}}$ into the effective recovery operators $\widehat{R}_i \in \widehat{\mathcal{R}}$. Secondly, the inverse encoder $\mathcal{V}^\dagger$ of Fig. 6.4 is designed to recover the original state of the logical qubit $|\psi\rangle$, while in Fig. 6.5, the block $\widehat{\mathcal{V}}^\dagger$ is invoked for restoring the state of the logical qubits $|\overline{\psi_0}\rangle$, which has been transformed by the unitary transformation U_f into $U_f|\overline{\psi_0}\rangle$.

Now, we proceed to specifically elaborate further on the scheme proposed for protecting quantum gates using QSCs, as shown in Fig. 6.4. Let us commence with the logical qubits in the state of $|\psi\rangle$ representing the input of the quantum circuit. In order to encode the

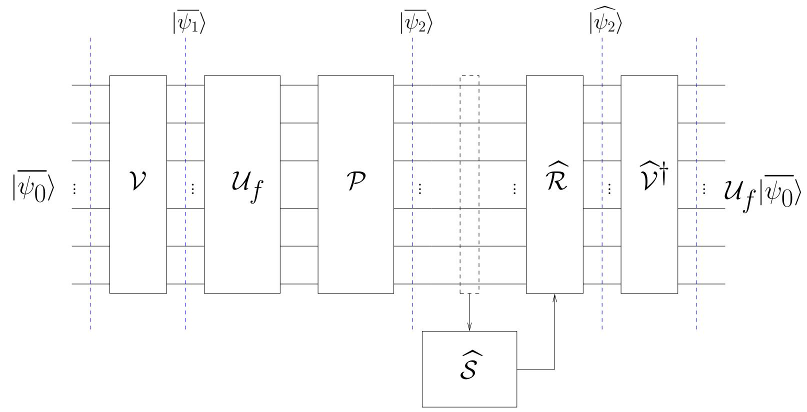


Figure 6.5: The basic model for QSC-protected quantum gates where the unitary transformation $\mathcal{U}_f$ introduces quantum depolarizing channel. It portrays the modified scheme for protecting the encoded state of physical qubits $|\overline{\psi_2}\rangle$, which is the encoded state after unitary transformation $\mathcal{U}_f$. In this scheme, instead of stabilizing the state of $|\overline{\psi_1}\rangle$, the stabilizer operators have to stabilize the state of $|\overline{\psi_2}\rangle$. Since the stabilizer operator $S_i \in \mathcal{S}$ is only valid for the encoded state of $|\overline{\psi_1}\rangle$, we have to reformulate the stabilizer operators S_i for stabilizing the encoded state $|\overline{\psi_2}\rangle$, which we refer to as the *effective stabilizer operators* $\widehat{S}_1 \in \widehat{\mathcal{S}}$.

logical qubits, we require $(n-k)$ auxiliary qubits (ancillas) all in the state of $|0\rangle$. We assume that the fresh ancillas are always available provided by a quantum memory. Hence, the state of the logical qubits and of the ancillas can be expressed as

$$|\overline{\psi_0}\rangle = |\psi\rangle \otimes |0\rangle^{\otimes(n-k)}. \tag{6.11}$$

The quantum encoder $\mathcal{V}$ of Fig. 6.5 maps the input state of $|\overline{\psi_0}\rangle$ into the state of encoded logical qubits or physical qubits $|\overline{\psi_1}\rangle$ as follows:

$$|\overline{\psi_1}\rangle = \mathcal{V}|\overline{\psi_0}\rangle. \tag{6.12}$$

The unitary operation U_f of Fig 6.5, which is the unitary transformation that we wish to protect, maps the physical qubits in the state of $|\overline{\psi_1}\rangle$ onto $|\overline{\psi_2}\rangle$ as follows:

$$|\overline{\psi_2}\rangle = U_f|\overline{\psi_1}\rangle = U_f\mathcal{V}|\overline{\psi_0}\rangle. \tag{6.13}$$

It is important to note that the unitary transformation of U_f may impose quantum errors $\mathcal{P}$ on the encoded state $|\overline{\psi_2}\rangle$, as it will be shown later in Section 6.4.

Due to the unitary tranformation U_f after the quantum encoder $\mathcal{V}$, the stabilizer operators of $S_i \in \mathcal{S}$ are not applicable for the encoded state of $|\overline{\psi_2}\rangle$, because the stabilizer formalism $\mathcal{S}$ was designed for stabilizing the encoded state of $|\overline{\psi_1}\rangle$. Since the aim of this scheme is to protect the state of $|\overline{\psi_2}\rangle$ instead of $|\overline{\psi_1}\rangle$, a different stabilizer formalism, which we refer to as the effective stabilizer operators $\widehat{S}_i \in \widehat{\mathcal{S}}$, should be designed for stabilizing the state of $|\overline{\psi_2}\rangle$ by taking into account the unitary transformation U_f. Given the formulation in Eq. (6.3), we formulate the effective stabilizer operator $\widehat{S}$ as follows:

$$\begin{aligned} |\overline{\psi_2}\rangle &= U_f|\overline{\psi_1}\rangle \\ &= U_f S|\overline{\psi_1}\rangle \\ &= U_f S U_f^\dagger U_f|\overline{\psi_1}\rangle \\ &= \widehat{S} U_f|\overline{\psi_1}\rangle \\ &= \widehat{S}|\overline{\psi_2}\rangle, \end{aligned} \tag{6.14}$$

where $\widehat{S}$ is the effective stabilizer for $|\overline{\psi_2}\rangle$, which is defined by

$$\widehat{S} = U_f S U_f^\dagger, \tag{6.15}$$

for stabilizing the state of $|\overline{\psi_2}\rangle$ in Fig. 6.5.

Given a unitary function U_f and a set of stabilizer operators $S_i \in \mathcal{S}$, there are three possible outcomes due to the effective stabilizer formalism of Eq. (6.15). First, the set of stabilizer operators does not change ($\widehat{\mathcal{S}} = \mathcal{S}$). In other words, the overall stabilizer operators are preserved. This specific result can be obtained specifically given that the unitary transformation U_f is constituted by some types of transversal quantum Clifford gates, for instance, transversal Hadamard gates or CNOT gates, and $S_i \in \mathcal{S}$ belongs to dual-containing CSS-type QSCs. Second, the stabilizer operators changes ($\widehat{\mathcal{S}} \neq \mathcal{S}$). One of the possible reasons that we can obtain the second result is that we apply the stabilizer codes for non-transversal quantum Clifford gates. Since the set of stabilizer operators are changed, there is a possibility that the resultant stabilizer operators $\widehat{S}_i \in \widehat{\mathcal{S}}$ is associated with a QSC exhibiting a higher error correction capability. This idea is reminiscent of the idea of code deformation presented in [182, 183, 184, 185]. Defining the U_f for the non-transversal configurations of the quantum Clifford gates to obtain a higher error correction capability is a full research question on its own. We will leave this question as one of our future research directions. Third, the resultant $\widehat{S}_i$ is no longer a set of n-tuple Pauli operators. It means that the unitary transformation U_f is containing non-Clifford quantum gates. More specifically, if the unitary transformation U_f is not a quantum Clifford gate, for example, Tofolli gate [131], the QSCs cannot be used directly for protecting the quantum gates as presented in this chapter. To tackle this problem, a method for protecting the non-Clifford quantum gates namely, magic state distillation, was proposed [118]. In this chapter, we focus on the first possible outcome, since we are dealing with the transversal quantum Clifford gates. Nevertheless, the two remaining implications of effective stabilizer formalism are also interesting research directions.

Next, after performing the stabilizer measurements of $\widehat{S}_i \in \widehat{\mathcal{S}}$, the error recovery procedure $\widehat{\mathcal{R}}$ of Fig. 6.5 acts according to the effective stabilizer measurements and we obtain the predicted legitimate physical qubits state of $|\widehat{\psi_2}\rangle$. The final task of our system given in Fig. 6.5 is to perform a unitary transformation in order to transform the final state of $|\widehat{\psi_2}\rangle$ into the state of $U_f|\overline{\psi_0}\rangle$. Similar to the stabilizer formalism $\mathcal{S}$ in Fig. 6.4, the inverse encoder $\mathcal{V}$ was also designed for recovering the state of $|\overline{\psi}_1\rangle$, which is based on the stabilizer formalism $\mathcal{S}$. Therefore, we require the *effective inverse encoder* $\widehat{\mathcal{V}}^\dagger$, which is designed based on the effective stabilizer operators $\widehat{\mathcal{S}}$, as seen in Fig. 6.5, to recover the state of $U_f|\overline{\psi_0}\rangle$. The formulation used for describing the effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ is given by

$$\begin{aligned} U_f|\overline{\psi_0}\rangle &= U_f\,(U_f\mathcal{V})^\dagger\,(U_f\mathcal{V})\,|\overline{\psi_0}\rangle \\ &= U_f\,(U_f\mathcal{V})^\dagger\,|\overline{\psi_2}\rangle \\ &= U_f\mathcal{V}^\dagger U_f^\dagger|\overline{\psi_2}\rangle \\ &= \widehat{\mathcal{V}}^\dagger|\overline{\psi_2}\rangle, \end{aligned} \tag{6.16}$$

where $\widehat{\mathcal{V}}^\dagger$ is the effective inverse encoder for $|\overline{\psi_2}\rangle$, which is defined as:

$$\widehat{\mathcal{V}}^\dagger = U_f\mathcal{V}^\dagger U_f^\dagger. \tag{6.17}$$

Finally, as seen in Eq. (6.16), the effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ succesfully transforms the state $|\overline{\psi_2}\rangle$ into the state of $U_f|\overline{\psi_0}\rangle$.

6.3 Design Examples

One of the strategies we may rely on for creating high-reliability quantum gates is that of invoking the unitary transformation U_f, which is a sequence of quantum gates arranged in a transversal fashion. For example, let us consider a quantum gate protected by 1/3-rate quantum repetition code as shown in Fig. 6.6. More explicitly, based on the model depicted in Fig. 6.5, we describe the transversal implementation of both the Hadamard and of the CNOT gates protected by the 1/3-rate quantum repetition code.

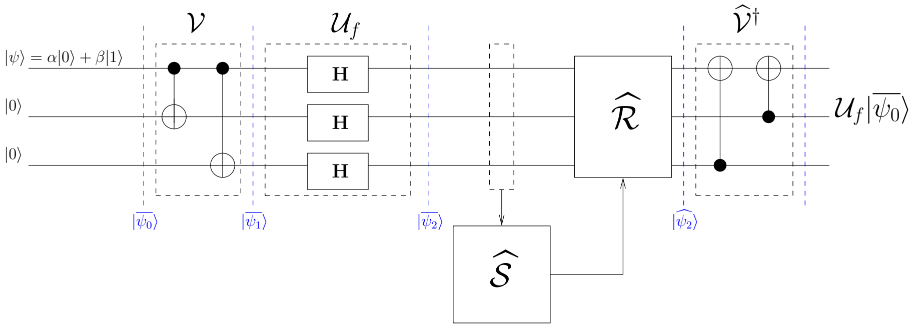


Figure 6.6: Example of transversal implementation of Hadamard gates protected by a 1/3-rate quantum repetition code with quantum encoder $\mathcal{V}$.

6.3.1 Transversal Hadamard Gates

First, we would like to elaborate on the transversal implementation of Hadamard gates protected by a 1/3-rate quantum repetition code. Let us refer to Fig. 6.6. The procedure begins with encoding the state of a single logical qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and two auxiliarry qubits in the state of $|0\rangle$ into the state of physical qubits of $|\overline{\psi_1}\rangle$ with the aid of quantum

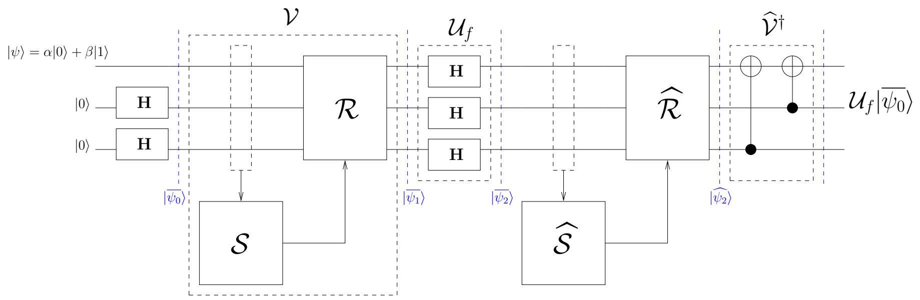


Figure 6.7: Example of transversal implementation of Hadamard gates protected by a 1/3-rate quantum repetition code with repeated stabilizer measurements.

encoder $\mathcal{V}$ as follows:

$$\begin{aligned}|\overline{\psi_1}\rangle &= \mathcal{V}\left(|\psi\rangle \otimes |0\rangle^{\otimes 2}\right)\\ &= \mathcal{V}\left((\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle^{\otimes 2}\right)\\ &= \alpha|000\rangle + \beta|111\rangle\\ &\equiv \alpha|0\rangle_L + \beta|1\rangle_L,\end{aligned} \tag{6.18}$$

where $|0\rangle_L = |000\rangle$, $|1\rangle_L = |111\rangle$, and the quantum encoder $\mathcal{V}$ for this mapping is portrayed by the part marked by $\mathcal{V}$ in Fig. 6.6. The encoded state of the physical qubits given in Eq. (6.18) is stabilized by the stabilizer operators generated by S_i:

$$\begin{aligned}S_1 &= \mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3,\\ S_2 &= \mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3,\end{aligned} \tag{6.19}$$

which can be invoked for correcting a single bit-flip ($\mathbf{X}$) error. The Hadamard gates, which carry out the unitary transformation we wish to protect, are arranged transversally, where the Hadamard gate is applied to each of the encoded logical qubits as seen in Fig. 6.6. Hence, the unitary transformation U_f can be expressed as

$$U_f = \mathbf{H}^{\otimes n}, \tag{6.20}$$

where the superscript $\otimes n$ of $\mathbf{H}$ represents the n-fold tensor product. The unitary transform U_f transforms the quantum state $|\overline{\psi_1}\rangle$ into quantum state $|\overline{\psi_2}\rangle$ as follows:

$$|\overline{\psi_2}\rangle = \alpha| + ++\rangle + \beta| - --\rangle. \tag{6.21}$$

Based on Eq. (6.15), the stabilizer operators of Eq. (6.19) and the unitary transformation U_f of Eq. (6.20), we obtain the effective stabilizer generators $\widehat{S}_i$ for stabilizing the quantum state $|\overline{\psi_2}\rangle$ in Fig. 6.6 as follows:

$$\begin{aligned}\widehat{S}_1 &= \left(\mathbf{H}^{\otimes 3}\right)(\mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3)\left(\mathbf{H}^{\otimes 3}\right)^\dagger\\ &= (\mathbf{HZH}^\dagger)_1 \otimes (\mathbf{HIH}^\dagger)_2 \otimes (\mathbf{HZH}^\dagger)_3\\ &= \mathbf{X}_1 \otimes \mathbf{I}_2 \otimes \mathbf{X}_3,\end{aligned} \tag{6.22}$$

$$\begin{aligned}\widehat{S}_2 &= \left(\mathbf{H}^{\otimes 3}\right)\left(\mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3\right)\left(\mathbf{H}^{\otimes 3}\right)^{\dagger} \\ &= (\mathbf{HZH}^{\dagger})_1 \otimes (\mathbf{HZH}^{\dagger})_2 \otimes (\mathbf{HIH}^{\dagger})_3 \\ &= \mathbf{X}_1 \otimes \mathbf{X}_2 \otimes \mathbf{I}_3, \end{aligned} \tag{6.23}$$

which are capable of correcting a single phase-flip ($\mathbf{Z}$) error. Finally, to transform the physical qubits in the state of $|\overline{\psi_2}\rangle$ to the state of $U_f|\overline{\psi_0}\rangle$, we design the effective inverse encoder of $\widehat{\mathcal{V}}^{\dagger}$ based on Eq. (6.17) and we obtain the quantum circuit portrayed in Fig. 6.6. Therefore, the final state of $U_f|\overline{\psi_0}\rangle$ can be described as follows:

$$\begin{aligned} U_f|\overline{\psi_0}\rangle &= \mathbf{H}^{\otimes n}(|\psi\rangle \otimes |0\rangle^{\otimes(n-k)}) \\ &= \mathbf{H}^{\otimes k}|\psi\rangle \otimes (\mathbf{H}^{\otimes(n-k)} \otimes |0\rangle^{\otimes(n-k)}) \\ &= \mathbf{H}^{\otimes k}|\psi\rangle \otimes |+\rangle^{\otimes(n-k)}. \end{aligned} \tag{6.24}$$

The last term of $|+\rangle^{\otimes(n-k)}$ can be discarded during measurement, since it is no longer entangled. In this example, we arrive at $|++\rangle$. Finally, from the design example specified in Fig. 6.6, we acquire the desired output in the state of $\mathbf{H}^{\otimes k}|\psi\rangle = \mathbf{H}|\psi\rangle = \alpha|+\rangle + \beta|-\rangle$, given that we have $k = 1$ and $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

In this chapter, another approach for utilizing QSC for protecting the transversal quantum Clifford gates without quantum encoder $\mathcal{V}$ is considered. In order to relax the assumption of having a perfect quantum encoder $\mathcal{V}$, all of $(n-k)$ auxiliarry qubits required for creating the encoded state of the physical qubits are all initialized in the $|+\rangle$ state and followed by stabilizer measurements. The implementation of the quantum circuit of tranversal Hadamard gates protected by a 1/3-rate quantum repetition code is portrayed in Fig. 6.7. Let us denote the encoded state of physical qubits $\alpha|000\rangle + \beta|111\rangle$ of Eq. (6.18) as $|\overline{\psi_1}\rangle$ and the encoded state of physical qubits $\alpha|+++\rangle + \beta|---\rangle$ of Eq. (6.21) as $|\overline{\psi_2}\rangle$. The quantum state $|\overline{\psi_0}\rangle$ of Fig. 6.7 can be expressed as

$$|\overline{\psi_0}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |+\rangle \otimes |+\rangle. \tag{6.25}$$

Given that $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, we can expand and rewrite the quantum state $|\overline{\psi_0}\rangle$ of Eq. (6.25) in terms of $|\overline{\psi_1}\rangle = \alpha|000\rangle + \beta|111\rangle$ as follows:

$$|\overline{\psi_0}\rangle = |\overline{\psi_1}\rangle + \mathbf{X}_2|\overline{\psi_1}\rangle + \mathbf{X}_3|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_3|\overline{\psi_1}\rangle, \tag{6.26}$$

where the notation of $\mathbf{X}_i$ indicates that Pauli matrix $\mathbf{X}$ is applied on i-th qubit. The current quantum state of $|\overline{\psi_0}\rangle$ is in a form of superposition of $|\overline{\psi_1}\rangle$ states. More specifically, the action of stabilizer measurements ($S_i \in \mathcal{S}$) will collapse the quantum state $|\overline{\psi_0}\rangle$ into one of the following possibilities: $|\overline{\psi_1}\rangle$, $\mathbf{X}_2|\overline{\psi_1}\rangle$, $\mathbf{X}_3|\overline{\psi_1}\rangle$, and $\mathbf{X}_2\mathbf{X}_3|\overline{\psi_2}\rangle$ with equal probabilities. The resultant of the collapsed quantum state $|\overline{\psi_1}\rangle$ can be determined by the ± 1 values from the stabilizer measurements. Hence, the error recovery $\mathcal{R}$ can restore the resultant collapsed quantum state back into the legitimate quantum state $|\overline{\psi_1}\rangle$, which is similar to the scheme with quantum encoder $\mathcal{V}$. Next, the action of unitary operator U_f, which is represented by transversal Hadamard gates of Eq. (6.20), transforms the quantum state

$|\overline{\psi_1}\rangle$ into the quantum state $|\overline{\psi_2}\rangle$ as follows:

$$\begin{aligned}|\overline{\psi_2}\rangle &= U_f|\overline{\psi_1}\rangle \\ &= \alpha|+++\rangle + \beta|---\rangle. \end{aligned} \tag{6.27}$$

From this point onwards, the recovery operators $\widehat{\mathcal{R}}$ as well as the effective quantum inverse encoder $\widehat{\mathcal{V}}^\dagger$ of both schemes, with and without quantum encoder $\mathcal{V}$, are identical. Therefore, the error correction performance between the two schemes are also expected to be identical.

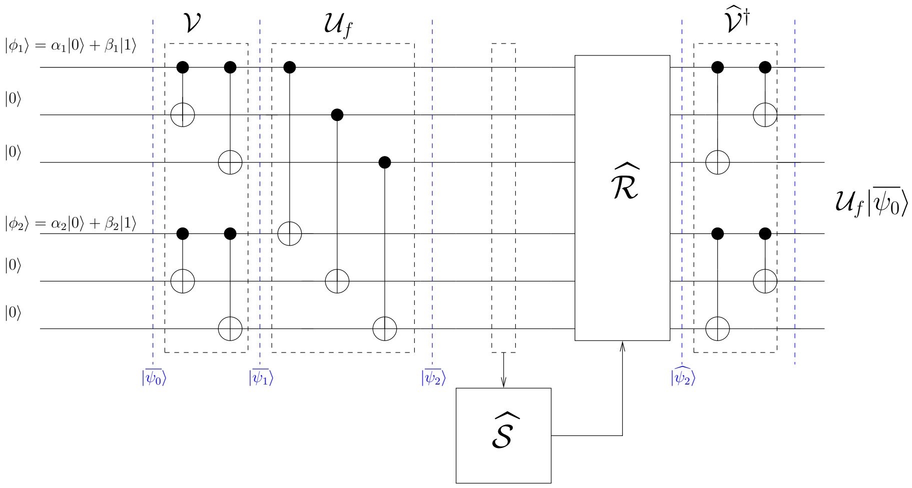


Figure 6.8: Example of transversal implementation of CNOT gates protected by a 1/3-rate quantum repetition code with quantum encoder $\mathcal{V}$.

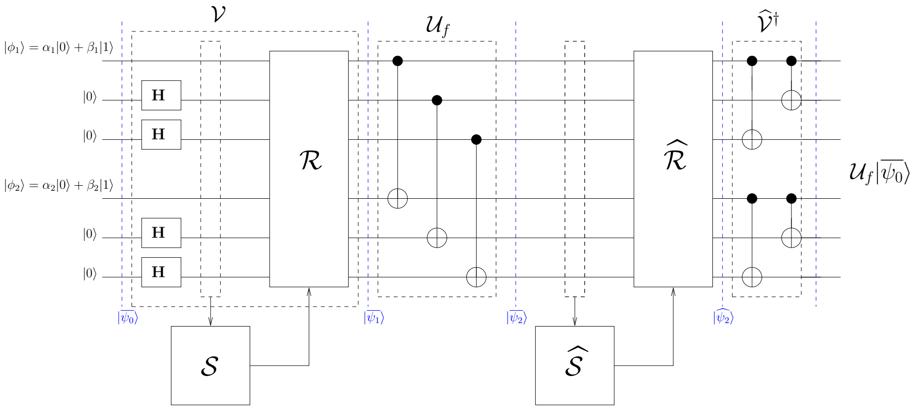


Figure 6.9: Example of transversal implementation of CNOT gates protected by a 1/3-rate quantum repetition code with repeated stabilizer measurements.

6.3.2 Transversal CNOT Gates

For our next example, we aim for conceiving the transversal implementation of CNOT gates protected by the 1/3-rate quantum repetition code. The model is depicted in Fig. 6.8 and 6.9. For the scheme portrayed in Fig. 6.8, the initial state is defined by $|\psi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ and our desired output is $\mathbf{CNOT}(|\phi_1\rangle \otimes |\phi_2\rangle)$, where $|\phi_1\rangle$ acts as the control qubit and $|\phi_2\rangle$ serves as the target qubit. The quantum encoder $\mathcal{V}$ of Fig. 6.9 encodes each of the logical qubits in the state of $|\phi_1\rangle$ and $|\phi_2\rangle$ independently, yielding the physical qubits in the state of $|\overline{\psi_1}\rangle = |\overline{\phi_1}\rangle \otimes |\overline{\phi_2}\rangle$, where $|\overline{\phi_1}\rangle$ and $|\overline{\phi_2}\rangle$ are the encoded logical qubits of $|\phi_1\rangle$ and $|\phi_2\rangle$, respectively. Therefore, the stabilizer operators S_i provided for the physical qubits in the state of $|\overline{\psi_1}\rangle$ in Fig. 6.8 are generated by the following stabilizer generators:

$$\begin{aligned}
S_1 &= \mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6,\\
S_2 &= \mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6,\\
S_3 &= \mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{I}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{I}_5 \otimes \mathbf{Z}_6,\\
S_4 &= \mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{I}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{Z}_5 \otimes \mathbf{I}_6.
\end{aligned} \tag{6.28}$$

In this example, the quantum gate that we try to protect is the CNOT gate. Therefore, the unitary transformation U_f of Fig. 6.8 and 6.9 represents the unitary matrix of the transversal CNOT gates. Now, let us denote the unitary matrix of the n transversal CNOT gates as $\overline{\mathbf{CNOT}}^n$. Therefore, the unitary transformation U_f of Fig. 6.8 and 6.9, can be expressed as a 64×64-element matrix by expanding the following transformation:

$$\begin{aligned}
U_f &= \overline{\mathbf{CNOT}}^3\\
&= |000\rangle\langle 000| \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} + |001\rangle\langle 001| \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X}\\
&+ |010\rangle\langle 010| \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} + |011\rangle\langle 011| \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{X}\\
&+ |100\rangle\langle 100| \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{I} + |101\rangle\langle 101| \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X}\\
&+ |110\rangle\langle 110| \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{I} + |111\rangle\langle 111| \otimes \mathbf{X} \otimes \mathbf{X} \otimes \mathbf{X}.
\end{aligned} \tag{6.29}$$

Based on the stabilizer generators S_i in Eq. (6.28) and the unitary transformation U_f of Eq. (6.29), we can obtain the effective stabilizer operators $\widehat{S}_i$ by applying Eq. (6.15), which formulated for protecting the state of $|\overline{\psi_2}\rangle$ in Fig. 6.8. Explicitly, the effective stabilizer operators $\widehat{S}_i$ is generated by the following stabilizer generators:

$$\begin{aligned}
\widehat{S}_1 &= \mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6,\\
\widehat{S}_2 &= \mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6,\\
\widehat{S}_3 &= \mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{I}_5 \otimes \mathbf{Z}_6,\\
\widehat{S}_4 &= \mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{Z}_5 \otimes \mathbf{I}_6.
\end{aligned} \tag{6.30}$$

Based on the commutativity property of stabilizer operators, where the multiplication among stabilizer operators will produce another valid stabilizer operator, we may rewrite the list of stabilizer generators given in Eq. (6.30). Hence, by multiplying $\widehat{S}_1$ and $\widehat{S}_3$ also by multiplying $\widehat{S}_2$ and $\widehat{S}_4$, we obtain the following effective stabilizer operators $\widehat{S}_i$ generated by the following stabilizer generators:

$$\begin{aligned}
\widehat{S}_1 &= \mathbf{Z}_1 \otimes \mathbf{I}_2 \otimes \mathbf{Z}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6, \\
\widehat{S}_2 &= \mathbf{Z}_1 \otimes \mathbf{Z}_2 \otimes \mathbf{I}_3 \otimes \mathbf{I}_4 \otimes \mathbf{I}_5 \otimes \mathbf{I}_6, \\
\widehat{S}_3 &= \mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{I}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{I}_5 \otimes \mathbf{Z}_6, \\
\widehat{S}_4 &= \mathbf{I}_1 \otimes \mathbf{I}_2 \otimes \mathbf{I}_3 \otimes \mathbf{Z}_4 \otimes \mathbf{Z}_5 \otimes \mathbf{I}_6.
\end{aligned} \tag{6.31}$$

As we can observe, the resultant effective stabilizer operators $\widehat{S}_i \in \widehat{\mathcal{S}}$ of Eq. (6.31) are identical with the stabilizer operators $S_i \in \mathcal{S}$ of Eq. (6.28). Consequently, it demonstrates the convenience of exploiting the transversal implementation of CNOT gates. Since the effective stabilizer operators $\widehat{S}_i$ of Eq. (6.31) are identical to the stabilizer operators S_i of Eq. (6.28), the quantum circuit of the effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ of Fig. 6.8 is also identical to the inverse encoder $\mathcal{V}^\dagger$ designed for transforming the state $|\overline{\psi_1}\rangle$ to the state $|\overline{\psi_0}\rangle$. Finally, the desired state for the output physical qubits based on the transversal configuration given in Fig. 6.8 can be formulated as

$$\begin{aligned}
U_f|\overline{\psi_0}\rangle &= \overline{\mathbf{CNOT}}^n(|\phi_1\rangle \otimes |0\rangle^{\otimes(n-k)}, (|\phi_2\rangle \otimes |0\rangle^{\otimes(n-k)})) \\
&= \overline{\mathbf{CNOT}}^k(|\phi_1\rangle, |\phi_2\rangle) \otimes |00\rangle^{\otimes(n-k)},
\end{aligned} \tag{6.32}$$

where the last term represents the auxiliary qubits in the state of $|00\rangle^{\otimes(n-k)}$ that can be discarded after measurement, since they are no longer entangled with the logical qubits in the state of $\overline{\mathbf{CNOT}}^k(|\phi_1\rangle, |\phi_2\rangle)$. Given that we have $k = 1$ and $n = 3$ for our example in Fig. 6.8, we succesfully protect the unitary transformation of $\mathbf{CNOT}(|\phi_1\rangle, |\phi_2\rangle)$ at the end of our scheme. Therefore, we have outlined the general framework of QSC-protected transversal quantum gates.

Additionally, we also present the scheme of protecting transversal CNOT gates without quantum encoder $\mathcal{V}$ in Fig. 6.9. Instead of using quantum encoder $\mathcal{V}$ portraying in Fig. 6.8, we can also utilize the scheme of Fig. 6.9, where the quantum encoder $\mathcal{V}$ is replaced with stabilizer masurement to create the code space. More specifically, the quantum state of the physical qubits $|\overline{\psi_1}\rangle$ of Fig. 6.8 is given by

$$\begin{aligned}
|\overline{\psi_1}\rangle &= (\alpha_1|000\rangle + \beta_1\rangle|111\rangle) \otimes (\alpha_2|000\rangle + \beta_2\rangle|111\rangle) \\
&= \alpha_1\alpha_2|000\rangle|000\rangle + \alpha_1\beta_2|000\rangle|111\rangle + \alpha_2\beta_1|111\rangle|000\rangle + \beta_1\beta_2|111\rangle|111\rangle.
\end{aligned} \tag{6.33}$$

In Fig. 6.9, the physical qubits are prepared in the quantum state of $|\overline{\psi_0}\rangle$ as follows:

$$|\overline{\psi_0}\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes |+\rangle \otimes |+\rangle \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \otimes |+\rangle \otimes |+\rangle. \tag{6.34}$$

Given that $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, we can expand and rewrite the quantum state $|\overline{\psi_0}\rangle$ of Eq. (6.34) in terms of $|\overline{\psi_1}\rangle$ of Eq. (6.33) as follows:

$$\begin{aligned}|\overline{\psi_0}\rangle &= |\overline{\psi_1}\rangle + \mathbf{X}_2|\overline{\psi_1}\rangle + \mathbf{X}_3|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_3|\overline{\psi_1}\rangle \\ &+ \mathbf{X}_5|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_5|\overline{\psi_1}\rangle + \mathbf{X}_3\mathbf{X}_5|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_3\mathbf{X}_5|\overline{\psi_1}\rangle \\ &+ \mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_3\mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_3\mathbf{X}_6|\overline{\psi_1}\rangle \\ &+ \mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_3\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle + \mathbf{X}_2\mathbf{X}_3\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle, \end{aligned} \tag{6.35}$$

where the notation of $\mathbf{X}_i$ indicates that Pauli matrix $\mathbf{X}$ is applied on i-th qubit. Notice that the stabilizer operators of Eq. (6.28) are associated with 16 possible classical syndrome vectors, where each of the syndrome vectors is associated with one of the superimposed states given in Eq. (6.35). When the stabilizer measurements are performed, the superposition state of Eq. (6.35) will collapse to one of the following 16 possibilities: $|\overline{\psi_1}\rangle$, $\mathbf{X}_2|\overline{\psi_1}\rangle$, $\mathbf{X}_3|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_3|\overline{\psi_1}\rangle$, $\mathbf{X}_5|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_5|\overline{\psi_1}\rangle$, $\mathbf{X}_3\mathbf{X}_5|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_3\mathbf{X}_5|\overline{\psi_1}\rangle$, $\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_3\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_3\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_3\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle$, $\mathbf{X}_2\mathbf{X}_3\mathbf{X}_5\mathbf{X}_6|\overline{\psi_1}\rangle$, where the collapsed quantum state can be inferred from the classical syndrome vector obtained from stabilizer measurements. Therefore, we can apply the recovery operator $\mathcal{R}$ to obtain the encoded state of physical qubits of $|\overline{\psi_1}\rangle$ from Eq. (6.33). After the recovery operator is carried out, the unitary transformation U_f is applied, which transforms the quantum state of $|\overline{\psi}_1\rangle$ into quantum state $|\overline{\psi}_1\rangle$ as follows:

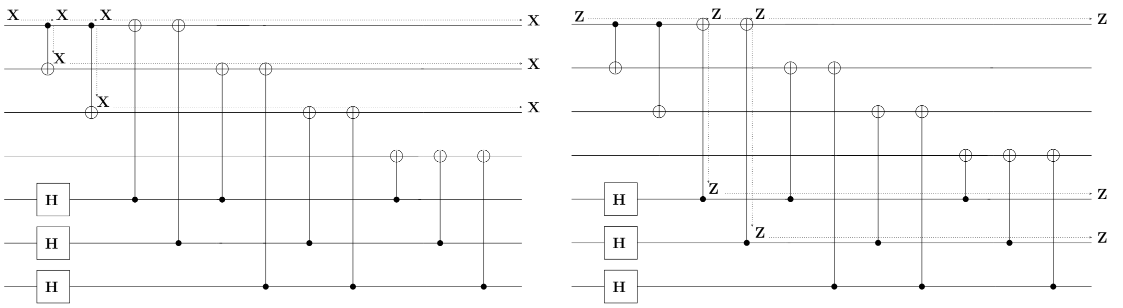
$$|\overline{\psi_2}\rangle = U_f|\overline{\psi}_1\rangle. \tag{6.36}$$

Similar to the case of transversal Hadamard gates, from this point onwards, all the effective stabilizer measurements, error recovery operators, and inverse encoder of Fig. 6.9 are identical with the ones of Fig. 6.8. Hence, we expect the performance of the scheme illustrated in Fig. 6.8 to be identical with the one in Fig. 6.9.

6.4 Error Model

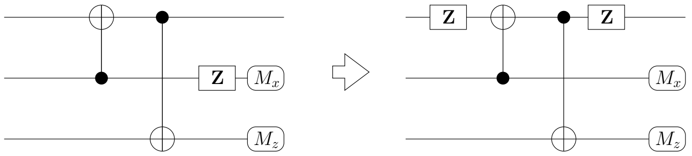
In order to show the benefit of utilizing the framework exemplified in Section 6.3, we have to opt for a realistic quantum decoherence model of the system to produce the most realistic performance results. However, several assumptions have to be made to justify the proposed error model. Based on [186, 187, 188, 189], we stipulate the assumption that quantum decoherence may be imposed by single-qubit quantum gates, two-qubit quantum gates, as well as by the deleterious effects of the stabilizer measurements. In order to consider the decoherence inflicted by multiple components within our framework, we offer the following two propositions:

Proposition 1. An error-infested quantum encoder $\mathcal{V}$ and a unitary transformation U_f can be modeled as a perfect quantum encoder $\mathcal{V}$ and a perfect unitary transformation U_f followed by the quantum channel $P \in \mathcal{P}_n$. To elaborate a little further, the encoder of QSCs can be fully constructed from the quantum gates belonging to the Clifford group. Consequently, we can use the formulation of Eq. (6.3), which is illustrated in Fig. 6.2, to model the error propagation throughout the quantum encoder. More explicitly, let us

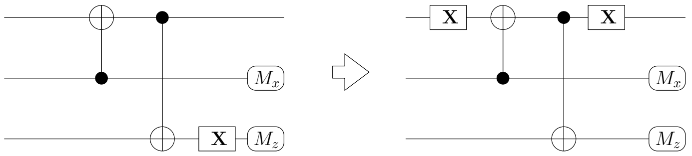


(a) $\mathbb{X}$-type error propagation. (b) $\mathbb{Z}$-type error propagation.

Figure 6.10: The quantum encoder for Steane's 7-qubit code can be implemented purely consisting of quantum gates from the Clifford group. Therefore, a faulty quantum encoder of any QSC can be assumed to be modelled as a perfect quantum encoder followed by the quantum depolarizing channel. A single bit-flip (**X**) error at the input can be transformed into three bit-flip errors at the output of quantum encoder $\mathcal{V}$. Similarly, a phase-flip (**Z**) inflicted at the input of quantum encoder **V** may propagate resulting in three phase-flip error at the output.



(a) **X** error on **Z** stabilizer measurements

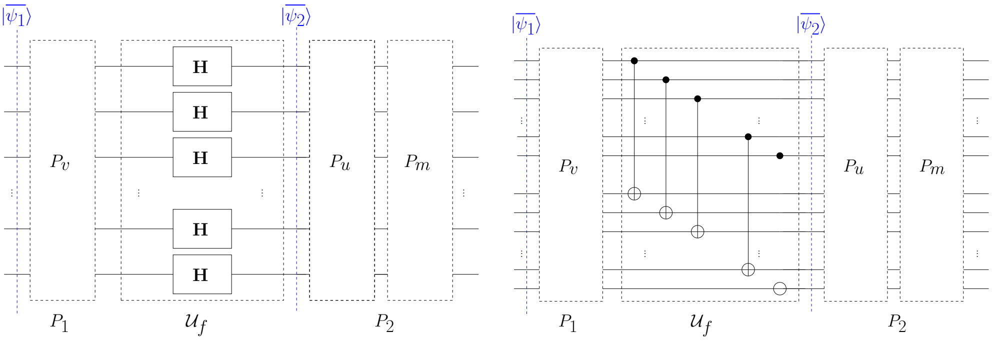


(b) **Z** error on **X** stabilizer measurements

Figure 6.11: Error on stabilizer measurements.

provide an example using the quantum encoder of Steane's 7-qubit code, which is equivalent to the quantum encoder of the distance-3 colour code, as portrayed in Fig. 6.10. We can observe from Fig. 6.10(a) that a single bit-flip (**X**) error at the input of the quantum encoder is transformed into three separated bit-flip (**X**) errors, which are accumulated at the output of the encoder $\mathcal{V}$. Similarly in Fig. 6.10(b), a phase-flip (**Z**) at the input of the quantum encoder propagating across the quantum encoder is transformed into three different phase-flip errors at three different locations at the output of the quantum encoder $\mathcal{V}$. Hence, in general, the severity of error propagation within the quantum encoder $\mathcal{V}$ is determined by the number of two-qubit quantum Clifford gates composing it.

Proposition 2. An error-infested stabilizer measurement of the QSC protecting the transversal quantum gates of Fig. 6.5 can be substituted by perfect stabilizer measurement and the quantum channel $P \in \mathcal{P}$ after the transversal configuration of quantum gates, which is illustrated in Fig. 6.11. This is also one of the natural consequences of the conjugation given in Eq. (6.3). Since the **X** stabilizer operators anti-commute with the **Z** Pauli operator, only **Z**-type errors are considered for **X** stabilizer measurements. Equivalently, since the **Z** stabilizer operators anti-commute with the **X** Pauli operator,



(a) Transversal Hadamard gates. (b) Transversal CNOT gates.

Figure 6.12: The potential quantum decoherence model imposed in QSC-protected transversal Hadamard and CNOT gates. There are several potential sources of quantum decoherences including the quantum encoder, quantum gates, and stabilizer measurement, denoted by P_v, P_u and P_m, respectively.

only **X**-type errors affect the result of **Z** stabilizer measurements.

6.4.1 Source of Decoherence

By considering the potential sources of quantum-decoherence based on our proposed framework and also the nature of error propagation, we conclude that diverse sources of decoherence can be efficiently modelled as the accumulated quantum decoherence before and after the transversal quantum gates U_f, as explicitly shown in Fig. 6.12. To elaborate a little further, the quantum decoherence before the transversal quantum gates is constituted by $P_1 \in \mathcal{P}_n$ that corrupts the physical qubits in the state of $|\overline{\psi_1}\rangle$ by **X**, **Z** and **Y**-type errors independently with depolarizing probability of $p_{\mathbf{X}} = p_{\mathbf{Y}} = p_{\mathbf{Z}} = p_1/3$. Similarly, the quantum decoherence after the transversal gates is denoted by $P_2 \in \mathcal{P}_n$), which is described by the depolarizing probability of p_2, corrupting the physical qubits in the state of $|\overline{\psi_2}\rangle$.

It is important to note that each of the error operators P_1 and P_2 may encapsulate several sources of quantum decoherence. For example, observe from Fig. 6.12(a) and 6.12(b) that the error operator P_1 represents the decoherence from the quantum encoder $\mathcal{V}$ of Fig. 6.5, which is denoted by P_v. The error operator of $P_v \in \mathcal{P}_n$ is characterized by the depolarizing probability of p_v. The error operator of $P_2 \in \mathcal{P}_n$ encapsulates both the quantum decoherence imposed by the quantum gates P_u as well as the quantum decoherence imposed by the stabilizer measurement P_m. If the error operator P_u is specified by the depolarizing probability of p_u and the error operator P_m is specified by the depolarizing probability of p_m, the error operator P_2 can be determined by $P_m \cdot P_u = P_2 \in \mathcal{P}_n$.

Let us now consider various error models available in the literature. Most of the error models used for evaluating the performance of QSCs for protecting quantum gates consist of three parameters namely, the the error probability imposed by a single qubit gates denoted by p_a, the error probability imposed by two-qubit quantum gates denoted by p_b, and the error probability imposed by the stabilizer measurements denoted by p_m. The *standard error model* [187] assumes that $p_a = p_b = p_m = p$. By contrast, the *balanced error model* [187] assumes that the error rate imposed by the single-qubit quantum gate is $p_a = 4p/5$, that by the two-qubit quantum gate is $p_b = p$, and that by the stabilizer measurements is given by $p_m = 8p/15$. From the experimental point of view, let us consider the *ion trap error model* [187], where the parameters is defined by $p_1 = p/1000$, $p_2 = p$, and $p_m = p/100$. In this chapter, one of our main goals is to fully simulate the overall scheme using the quantum-to-classical isomorphism. Therefore, we simulate the quantum decoherence on each of the physical qubits as an individual and independent binary symmetric channel (BSC) as suggested in [71, 79]. Consequently, for the classical simulation based on independent BSCs, we have the parameters of $p_a = p_m = p$ and $p_b \approx 2p$. A more detailed description of the error model used for this work is provided in the following subsection.

The various error models arise from various technology platforms available for developing quantum computers. In this chapter, however, we focus on how we can investigate the performance of transversal quantum Clifford gates protected by two-dimensional QTECCs using classical simulation. Intuitively, what we want is to have the value of depolarizing probability to be as low as possible. However, state-of-the-art quantum gates have relatively low fidelity values ranging between 90.00% − 99.90% across various technology platforms, such as spin electronics, photonics, superconducting, trapped-ion, and silicon [39, 40, 41, 42, 44, 46, 47, 48, 116]. Fortunately, based on the threshold theorem [119], it is possible to construct a reliable quantum computer from unreliable quantum gates, given that the error probability of the quantum gates is below a certain probability threshold value and a reasonable size of overhead is allowed. Therefore, most of the studies on the QECCs are focusing on finding the specific value of gate error probabilities p_a, p_b, and p_m so that the QECCs can be implemented to significantly improve the reliability of the quantum computers.

6.4.2 Faulty Quantum Gates

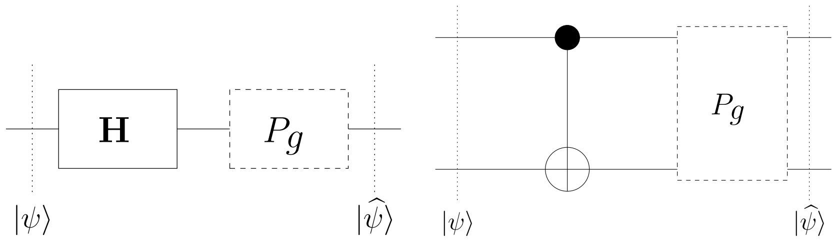
In this chapter, we rely on the model illustrated in Fig. 6.13, where each qubit experiences an independent quantum depolarizing channel characterized by its depolarizing probability. The metric used for evaluating the performance of our system is the qubit error rate (QBER) and the fidelity (F). First, the QBER is defined as the ratio between the number of erroneous qubits to the total number of qubits. For a single-qubit quantum gate, which is exemplified by Hadamard gate **H**, the QBER value can be represented as

$$\text{QBER}_{\text{Had}} = p, \tag{6.37}$$

where p is the depolarizing probability value of the single qubit quantum decoherence caused by the imperfection of the quantum gate.

Secondly, the reliability of a quantum gate can also be quantified using its *fidelity*. Explicitly, the fidelity may be used to reflect the closeness of an ensemble of quantum states in the mixed-state to the desired pure state, which is formulated as follows [87, 169, 170]:

$$F = \langle\overline{\psi}|\rho|\overline{\psi}\rangle, \tag{6.38}$$



(a) Faulty Hadamard gate. (b) Faulty CNOT gate.

Figure 6.13: The model of faulty quantum gates. The Pauli channel $Pg \in \mathcal{P}$ is inflicted after the quantum gates.

where $|\overline{\psi}\rangle$ is the desired pure state and ρ is the density matrix encapsulating the statistical characteristics of the mixed-states. The density matrix ρ is defined by

$$\rho = \sum_{i=1}^{N} p_i |\psi_i\rangle\langle\psi_i|, \tag{6.39}$$

where $|\psi_i\rangle$ represents all the possible quantum states in the ensemble and p_i is the probability of obtaining the quantum state $|\psi_i\rangle$, which is consequently constrained by the unity requirement of $\sum_{i=1}^{N} p_i = 1$. For a quantum Clifford gate, the relationship between fidelity and the QBER is as simple as

$$F = 1 - \text{QBER}, \tag{6.40}$$

where QBER is the qubit error ratio of the unprotected gate. Consequently, we obtain the analytical expression of the uncoded fidelity (F_{uncoded}) for a Hadamard gate as a function of the depolarizing probability p as follows:

$$F_{\text{uncoded}} = 1 - p. \tag{6.41}$$

Similar to the Hadamard gate, the fidelity of the CNOT gate can be defined using Eq. (6.40). Since a CNOT gate is a two-qubit quantum gate, the fidelity can be explicitly formulated as the probability of having the Pauli operator **I** on both the control qubit and the target qubit, which can be formulated as

$$\begin{aligned} F_{\text{uncoded}} &= (1-p)(1-p) \\ &= 1 - 2p + p^2. \end{aligned} \tag{6.42}$$

Therefore, the QBER of a CNOT gate can be rewritten as follows:

$$\text{QBER}_{\text{CNOT}} = 2p - p^2 \approx 2p, \tag{6.43}$$

for $p \ll 1$. Therefore, given that p_a is the error rate or the QBER of a single qubit quantum gate and p_b is the error rate or the QBER of a two-qubit quantum gate, we obtain the relationship between p_a and p_b obtained for classical simulation utilizing BSC as follows:

$$p_b \approx 2p_a. \tag{6.44}$$

Additionally, the relationship between the error rate of a single-qubit quantum gate p_a and the error rate of a stabilizer measurement p_m can be simply formulated as

$$p_m = p_a. \tag{6.45}$$

6.4.3 Effective Depolarizing Channel

As we have described in Subsection 6.4.1, in the QSC-protected quantum transversal gates, there are multiple sources of decoherence. For example, in Fig. 6.12, the decoherence effects imposed by the transversal quantum gates and stabilizer measurements can be modelled by multiple subsequent quantum depolarizing channels. To simplify the analytical calculations and their approximation, we introduce the notion of *effective depolarizing channel.*

For example, let us assume that the first depolarizing channel is constituted by the error operator $P_1 \in \mathcal{P}_n$, which is characterized by the depolarizing probability $p_1 = p$, while the second depolarizing channel is constituted by the error operator $P_2 \in \mathcal{P}_n$, which is characterized by the depolarizing probability $p_2 = p$. Then, the probability of obtaining the Pauli matrix $\mathbf{I}$ at the output of two consecutive Pauli channels can be expressed as follows:

$$\begin{aligned} p_{\mathbf{I},f} &= p_{\mathbf{I},1}p_{\mathbf{I},2} + p_{\mathbf{X},1}p_{\mathbf{X},2} + p_{\mathbf{Y},1}p_{\mathbf{Y},2} + p_{\mathbf{Z},1}p_{\mathbf{Z},2} \\ &= (1-p)(1-p) + \left(\frac{p}{3}\right)\left(\frac{p}{3}\right) + \left(\frac{p}{3}\right)\left(\frac{p}{3}\right) + \left(\frac{p}{3}\right)\left(\frac{p}{3}\right) \\ &= 1 - 2p + \frac{4}{3}p^2. \end{aligned} \tag{6.46}$$

Consequently, we obtain the following probability of experiencing the Pauli error $\mathbf{X}$, $\mathbf{Y}$, and $\mathbf{Z}$:

$$p_{\mathbf{X},f} = p_{\mathbf{Y},f} = p_{\mathbf{Z},f} = \frac{2}{3}p - \frac{4}{9}p^2. \tag{6.47}$$

In other words, the effective depolarizing probability can be expressed as

$$p_f = 2p - \frac{4}{3}p^2 \approx 2p. \tag{6.48}$$

In can be concluded that a pair of depolarizing channels each characterized by the depolarizing probability p can be effectively viewed as a single quantum depolarizing channel associated with the aggregated depolarizing probability of $p_f = 2p$. Furthermore, the effective depolarizing probability p_f for c consecutives depolarizing channels, where each of the channels is characterized by an identical depolarizing probability p, can be approximated as

$$p_f \approx cp, \tag{6.49}$$

for $p \ll 1$.The expression given in Eq. (6.49) is our basis for deriving the analytical upper bound expressions in Section 6.5.

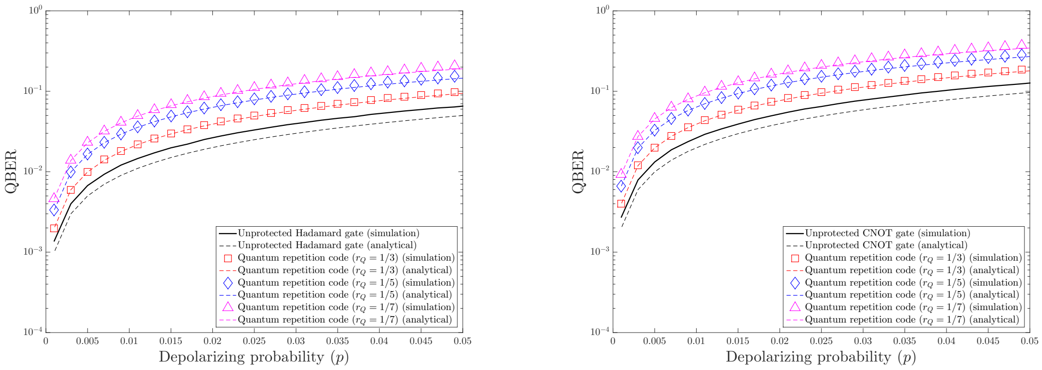
We need to emphasize once again that this is one of the desirable properties of QTECCs compared to the rest of QSCs family that the number of stabilizer measurements applied to each physical qubit remains constant upon increasing the number of physical qubits n due to the convenient construction of the underlying lattice structure. As we can observe that the effective depolarizing probability p_f is governed by the value of c and mostly is contributed from the number of stabilizer measurements experienced by each of the physical qubits. In the case of the QTECCs, the value of c remains constant as we increase the minimum distance of the code d and the number of the physical qubits n. For instance, for colour codes, the number of stabilizer measurement is defined by the number of adjacent plaquettes for a given vertice. More specifically, each of physical qubits in colour codes experience at most six stabilizer measurements, which is independent of the minimum distance of the code d and the number of physical qubits n. A similar case is applied to surface codes. The number of stabilizer measurements experienced by each of the physical qubits is defined by the number of vertices and plaquettes given an edge of a lattice. Each of the physical qubits in surface codes experiences at most only four stabilizer measurements, which is also independent of the minimum distance of the code d and number of physical qubits n.

6.5 Simulation Results and Performance Analysis

To evaluate the performance of the system considered, we exploited the classical-to-quantum Pauli isomorphism [1,79]. To elaborate further, we generated two independent binary symmetric channels, where one of the channels modelled the bit-flip channel, while the other emulated the phase-flip channel. Since it is impossible to mimic identically the actual quantum depolarizing channel using two independent binary symmetric channels (BSCs), for approximating the quantum depolarizing channel having an equal probability of $\mathbf{X}$, $\mathbf{Z}$, and $\mathbf{Y}$-type of errors ($p_{\mathbf{X}} = p_{\mathbf{Z}} = p_{\mathbf{Y}} = p/3$), it is widely accepted that the flip probability of each BSCs in the classical simulation is adjusted to $p_{\mathbf{X}} = p_{\mathbf{Z}} = 2p/3$ [71], [75]. The maximum-likelihood hard-decision decoding technique was invoked, which was translated into a look-up table (LUT) based decoder. For the full exposure of how we conceived the LUT decoder, we refer the reader to [1]. We take the value of frame error rate (FER) from the classical simulation to portray the QBER since we concern with unitary transformation on the arbitrary and unknown quantum state.

6.5.1 Simple Examples

In this section, we present the simplest scenario of transversal Hadamard gates and CNOT gates protected by quantum repetition codes. Let us revisit Fig. 6.6 and 6.7 and observe the associated QBER performance. Based on the error model described in Section 6.4, the quantum depolarizing channel $P_g \in \mathcal{P}_n$ associated with the depolarizing probability p



(a) Hadamard gates.

(b) CNOT gates.

Figure 6.14: QBER performance of the transversal Hadamard and CNOT gates protected by 1/3, 1/5, and 1/7-rate quantum repetition codes. We applied the depolarizing channel after the transversal configuration of the quantum gates, where the depolarizing channel is characterized by depolarizing probability p.

corrupted the quantum state of the physical qubits $|\overline{\psi_2}\rangle$. For the simplest scenario here, we assumed that the quantum encoder $\mathcal{V}$ and the syndrome measurement were also error-free.

For the transversal Hadamard gates protected by a 1/3-rate quantum repetition code, which is illustrated in Fig. 6.6 and 6.7, the simulation results are portrayed in Fig. 6.14(a). We also have included the performance results for transversal Hadamard gates protected by 1/5-rate and 1/7-rate quantum repetition codes. Naturally, the quantum repetition codes can only protect the transversal Hadamard gates from one type of error, either the phase-flip or the bit-flip errors. In other words, they are not capable of protecting the quantum gates from a more realistic quantum depolarizing channel. Furthermore, reducing the quantum coding rate - for quantum repetition codes this only allows increasing the error correction capability for either bit-flip or phase-flip errors - imposes increased quantum decoherence on our system, which is shown explicitly by the increase of QBER in Fig. 6.14(a). To elaborate further, upon increasing the number of qubits, we only increase the error correction capability for either phase-flip or bit-flip errors. Consequently, the deleterious effect of other types of errors imposed by the quantum depolarizing channel is accumulated and left uncorrected.

We have also invoked our QSC-protected scheme for transversal two-qubit Clifford quantum gates, as exemplified by the CNOT gate. We portray the performance of an unprotected CNOT gate along with that of its QSC-protected counterpart utilizing a 1/3-rate quantum repetition code, as illustrated in Fig. 6.8 and 6.9, in Fig. 6.14(b). Furthermore, we also have included the QBER performance curves of 1/5-rate and 1/7-rate quantum repetition codes. As expected, similar to transversal Hadamard gates, instead of being improved, the QBER performance of transversal CNOT gates is degraded upon reducing the quantum coding rate. Again, invoking QSCs for protecting quantum gates remains futile if we only consider protecting one type of errors. In conclusion, we have to employ QSCs, which are capable of correcting the bit-flip, phase-flip as well as the simultaneous bit-flip and phase-flip errors.

6.5.2 QTECC-Protected Transversal Hadamard Gates

In this section, we utilized the QTECCs as opposed to the above-mentioned quantum repetition codes, since the QTECCs are capable of mitigating both bit-flip and phase-flip errors. More specifically, we considered colour codes [103], rotated-surface codes [102], and surface codes [101], exhibiting a minimum distance of $d = 3$ in our model of Fig. 6.5. For this scenario, we used the assumption that the encoded physical qubits can be created fault-tolerantly, hence the quantum encoder $\mathcal{V}$ was assumed to be error-free, or we can utilize the scheme without the quantum encoder $\mathcal{V}$ as we have described earlier in Section 6.3. The quantum depolarizing channel was inflicted by the quantum unitary operation U_f and also by the stabilizer measurements. The error operator $P_u \in \mathcal{P}_n$ imposed by the unitary operation U_f was characterized by the depolarizing probability $p_u = p$. However, for the stabilizer measurements, as we have mentioned in Chapter 5, each of the physical qubits will have a constant number of measurement for each $\mathbf{X}$ and $\mathbf{Z}$ stabilizer operators. More explicitly, for surface codes and rotated-surface codes, each of the physical qubits will have at most two interactions for each $\mathbf{X}$ and $\mathbf{Z}$ stabilizer measurements, while for colour codes each of the physical qubits will have at most three interactions for each $\mathbf{X}$ and $\mathbf{Z}$ stabilizer measurements.

To elaborate a little further, due to the stabilizer measurements, we encountered four additional consecutive depolarizing channels after the error operator P_u imposed by the unitary operation U_f for surface and rotated-surface codes. Therefore, we had five consecutives depolarizing channels, where each of the error operators $P_i \in \mathcal{P}_n$ for $i = \{1, 2, 3, 4, 5\}$ was characterized by the depolarizing probability $p_i = p$. Similarly, for colour codes we inflicted six additional consecutive depolarizing channels after the error operator P_u imposed by the unitary operation U_f, hence we imposed seven consecutive depolarizing channels after unitary operation U_f, where each of the error operators $P_i \in \mathcal{P}_n$ for $i = \{1, 2, 3, 4, 5, 6, 7\}$ was also characterized by depolarizing probability $p_i = p$.

Formally, the effective error operator P_f after c consecutive error operators P_i can be expressed as

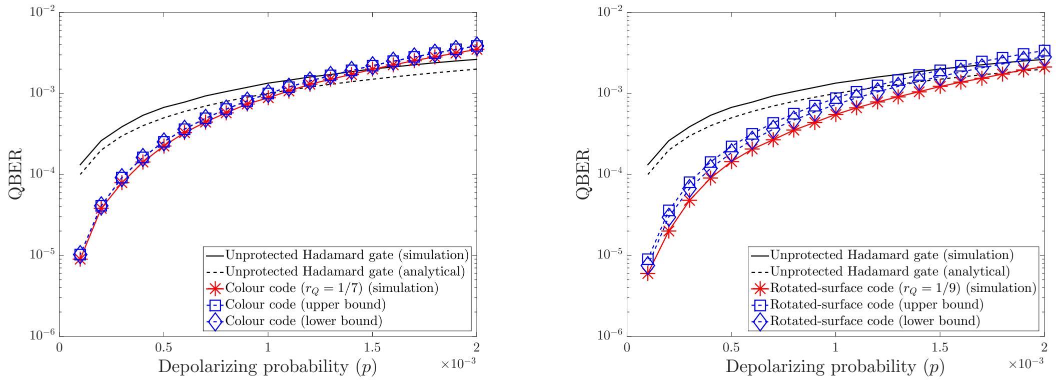
$$P_f = \prod_{i=1}^{c} P_i \text{ for } P_i \in \mathcal{P}_n. \tag{6.50}$$

For c consecutive depolarizing channels, the j-th qubit from n physical qubits will experience independently the effective error operators P_f, which is defined as

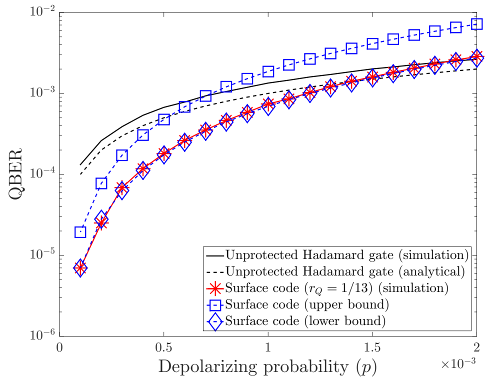
$$P_{f,j} = \prod_{i=1}^{c} P_i, \text{ for } \forall P_i \in \mathcal{P}_1^*. \tag{6.51}$$

Since there are c consecutive depolarizing channels, the probability of obtaining identity matrix $\mathbf{I}$ is equal to the sum of all probabilities from all the possible combinations of $P_{f,j}$ resulting in Pauli matrix $\mathbf{I}$, where we assume that $p_{\mathbf{I}} = (1 - p)$ and $p_{\mathbf{X}} = p_{\mathbf{Y}} = p_{\mathbf{Z}} = p/3$. Therefore, the effective probability of obtaining Pauli matrix $\mathbf{I}$ for five consecutive depolarizing channels can be expressed as shown in Eq. (6.74).

To elaborate a little further, we can infer from Eq. (6.74) that there are 30 possible



(a) Colour codes. (b) Rotated-surface codes.



(c) Surface codes.

Figure 6.15: QBER performance for transversal Hadamard gates protected by distance-3 QTECCs over quantum depolarizing channel. The quantum decoherence is inflicted after the transversal configuration of Hadamard gates, where the error operators of $\prod_{i=1}^{c} P_i \in \mathcal{P}_n$ are defined by $p_i = p$. The number of consecutive error operators is $c = 7$ for colour codes and $c = 5$ for rotated-surface and surface codes.

$$\begin{aligned} p_{\mathbf{I},f} &= (1-p)^5 + 30(1-p)^3\left(\frac{p}{3}\right)^2 + 60(1-p)^2\left(\frac{p}{3}\right)^3 + 105(1-p)\left(\frac{p}{3}\right)^4 + 60\left(\frac{p}{3}\right)^5 \\ &= 1 - 5p + \frac{40}{3}p^2 - \frac{160}{9}p^3 + \frac{320}{27}p^4 - \frac{256}{81}p^5. \qquad (6.74) \end{aligned}$$

$$\begin{aligned} p_f &= 1 - p_f^{\mathbf{I}} \\ &= 5p - \frac{40}{3}p^2 + \frac{160}{9}p^3 - \frac{320}{27}p^4 + \frac{256}{81}p^5. \qquad (6.75) \end{aligned}$$

combinations from $\prod_{i=1}^{5} P_i$ which give us $P_{f,j} = \mathbf{I}$ consisting of two non-identity Pauli operators $P_i \in \mathcal{P}_1^*$, 60 combinations consisting of three non-identity Pauli operators, 105 combinations consisting of four non-identity Pauli operators, and finally, 60 combinations consisting of five non-identity Pauli operators. Therefore, the effective depolarizing probability p_f for $c = 5$ can be formulated as shown in Eq. (6.75). However, in case of $p \ll 1$, the effective depolarizing probability can be approximated as

$$p_f \approx 5p, \qquad (6.76)$$

as we have suggested earlier in Eq. (6.49).

$$
\begin{aligned}
p_{\mathbf{I},f} &= (1-p)^7 + 63(1-p)^5\left(\frac{p}{3}\right)^2 + 210(1-p)^4\left(\frac{p}{3}\right)^3 + 735(1-p)^3\left(\frac{p}{3}\right)^4 + 1260(1-p)^2\left(\frac{p}{3}\right)^5 \\
&\quad + 966(1-p)\left(\frac{p}{3}\right)^6 + 756\left(\frac{p}{3}\right)^7 \\
&= 1 - 7p + 28p^2 - \frac{560}{9}p^3 + \frac{2270}{27}p^4 - \frac{1792}{27}p^5 + \frac{5488}{243}p^6 - \frac{3711}{729}p^7. \qquad (6.77) \\
p_f &= 1 - p_f^{\mathbf{I}} \\
&= 7p - 28p^2 + \frac{560}{9}p^3 - \frac{2270}{27}p^4 + \frac{1792}{27}p^5 - \frac{5488}{243}p^6 + \frac{3711}{729}p^7. \qquad (6.78)
\end{aligned}
$$

Similarly, for $c = 7$, the sum of the probabilties from all of the possible combinations $P_{f,j}$ resulting in the Pauli matrix $\mathbf{I}$ can be expressed as shown in Eq. (6.77). Therefore, the effective depolarizing probability p_f for $c = 7$ can be expressed as portrayed in Eq. (6.78). Again, for $p \ll 1$, the value of p_f in Eq. (6.78) can be approximated as

$$p_f \approx 7p, \qquad (6.79)$$

as we have suggested in Eq. (6.49).

Table 6.1: The code parameters for various QTECCs based on the minimum distance d of the code [2].

Codes type	**Dimension**	**Physical qubits (n)**	**Stabilizers ($\lvert\mathcal{S}\rvert$)**	**Logical qubits (k)**
Colour [103]	d^*	$\frac{1}{4}\left(3d^2+1\right)$	$\frac{1}{4}\left(3d^2-3\right)$	1
Rotated-surface [102]	$d \times d$	d^2	d^2-1	1
Surface [101]	$d \times d$	$2d^2-2d+1$	$2d^2-2d$	1
Toric [98]	$d \times d$	$2d^2$	$2d^2-2$	2

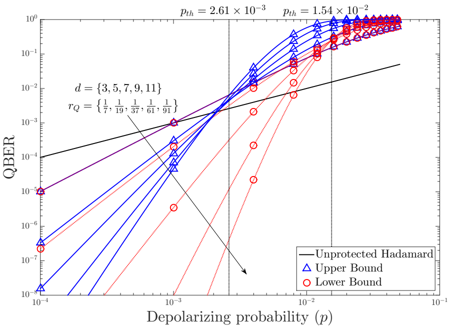
* for triangular colour codes the dimension is defined by the side length of the equilateral triangle

We have simulated the system using the quantum-to-classical Pauli isomorphism for simulating the QSCs. The simulation results are portrayed in Fig. 6.15. The performance of the proposed scheme is quantified using the QBER values, which is portrayed by the vertical axis, given various depolarizing probability values p, which is portrayed by the horizontal axis. For a minimum distance of $d = 3$, the quantum coding rate r_Q of colour codes, of rotated-surface codes, and of surface codes are given by 1/7, 1/9, and 1/13, respectively, based on the code parameters given in Table 6.1. We can observe the QBER performance improvement upon applying the scheme given in Fig. 6.5 compared to the unprotected quantum gates, especially for depolarizing probability values of $p < 2 \times 10^{-3}$.

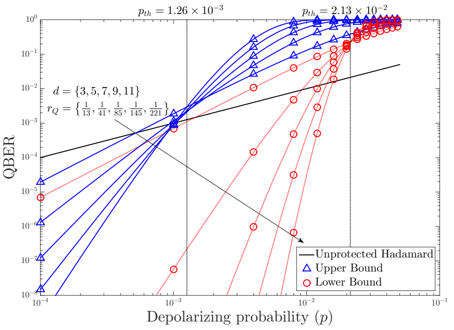
In general, the analytical QBER performance of QSC-protected single-qubit quantum gates can be calculated as follows:

$$\mathrm{QBER}^{(1)}_{\mathrm{approx}}(n,d,p) = 1 - \sum_{i=0}^{n} A_i \binom{n}{i} p^i (1-p)^{n-i}, \qquad (6.80)$$

where A_i is a real number coefficient portraying the success probability of correcting the



(a) Colour codes. (b) Rotated-surface codes.



(c) Surface codes. (d) Toric codes.

Figure 6.16: The upper and lower bound QBER analytical performance curves of the transversal implementation of Hadamard gates protected by various QTECCs.

error patterns having weight i. For a large number of n, finding the value of A_i for each of i becomes an intractable problem. One example of works of finding these A_i values specifically for colour codes can be seen in [190], where the authors successfully characterized the A_i values for colour codes up to minimum distance of $d = 7$. However, for non-degenerate QSCs, the analytical QBER performance can be approximated using the following upper bound as described in [1, 2] denoted by $\text{QBER}^{(1)}_{\text{upper}}$ as follows:

$$\text{QBER}^{(1)}_{\text{upper}}(n, d, p) = 1 - \sum_{i=0}^{t=\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} p^i (1-p)^{n-i} = \sum_{i=t+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}, \qquad (6.81)$$

where for QSCs-protected transversal single-qubit gate $p = p_f$, which in our case is the effective depolarizing probability defined by Eq. (6.75) for rotated-surface and surface codes and by Eq. (6.78) for colour codes.

To elaborate a little further, the upper bound of Eq. (6.81) provides the worst-case scenario performance assuming that any syndrome associated with the error pattern beyond the error correction capability of the quantum code is ignored, considering that attempting to correct the error will potentially introduce additional error. However, this decoding method is not utilizing the full benefit of the remaining syndromes. For instance, for a distance-3 surface code, we have $n = 13$ and $k = 1$, and hence we have $|\mathcal{G}| = n - k = 12$. Since the surface codes belong to the CSS-type quantum codes, the syndrome operator $G_i \in \mathcal{G}$ is invoked to correct the bit-flip and phase-flip error separately. Consequently, for a distance-3 surface code, we have six stabilizer operators dedicated for correcting bit-flip errors ($|\mathcal{G}_z| = 6$) and six stabilizer operators dedicated for correcting phase-flip errors ($|\mathcal{G}_x| = 6$). Since each of the syndrome measurement values is associated with an element of syndrome vector $\mathbf{s}$, we have a total of 64 possible syndrome vectors $\mathbf{s}$. We know that a distance-3 surface code is capable of correcting a single qubit error from both bit-flip and phase flip error. Consequently, from the total of 64 possible syndrome vectors $\mathbf{s}$, only 14 syndrome vectors are actually associated with recoverable error patterns. More explicitly, one syndrome vector is the all-zero syndrome vector associated with the error-free quantum state of the physical qubits and 13 syndrome vectors associated with a single bit-flip or phase-flip error patterns. The remaining 50 syndromes are capable of detecting error patterns exhibiting error weight beyond the error correction capability of the distance-3 surface code, although the decoder cannot make a definitive error recovery decision from these remaining syndromes, since each of them may be associated with multiple error patterns with the identical error weight. In the upper bound formulation of Eq. (6.81), these remaining 50 syndrome vectors are ignored, considering that making a wrong decision, for instance by making a random decision for the error recovery operator, will further degrade the received quantum state of the physical qubits.

In order to provide a confidence interval for the QBER performance of QSCs protected single-qubit quantum gates, we introduce the lower bound performances for the CSS-types quantum codes based on the classical sphere-packing bound [191, 192], or also known as quantum GV bound [1,88]. Formally, the lower bound of the QBER analytical performance can be defined as follows [191, 192]:

$$\text{QBER}^{(1)}_{\text{lower}}(n, d, p) = 1 - \sum_{i=0}^{t'+1} A_i p^i (1-p)^{n-i}, \tag{6.82}$$

where for QSCs-protected tranversal single-qubit gates $p = pf$ and A_i is a whole number coefficient subjected to

$$\sum_{i=0}^{t'+1} A_i \leq 2^{(n-k)/2}, \text{ where } A_i = \binom{n}{i}. \tag{6.83}$$

Consequently, the final coefficient of $A_{t'+1}$ can be determined by

$$A_{t'+1} = 2^{(n-k)/2} - \sum_{i=0}^{t'} A_i. \tag{6.84}$$

If the final coeffient of $A_{t'+1} = 0$, the code construction is referred to as perfect CSS-type QSCs. Otherwhise, the code is referred to as quasi-perfect CSS-type QSCs.

For instance, based on Eq. (6.81), the upper bound QBER performance of a distance-3 surface code can be approximated as

$$\text{QBER}^{(1)}_{\text{upper}}(13, 3, p_f) = 1 - (1-p_f)^{13} - 13 p_f (1-p_f)^{12}. \tag{6.85}$$

As a comparison, based on Eq. (6.82), the lower bound QBER performance of a distance-3 surface code can be approximated as

$$\mathrm{QBER}^{(1)}_{\mathrm{lower}}(13, 3, p_f) = 1 - (1 - p_f)^{13} - 13p(1 - p_f)^{12} - 50p_f^2(1 - p_f)^{11} \tag{6.86}$$

Let us revisit the analytical upper bound QBER performance of Eq. (6.81) and the lower bound of Eq. (6.82), as well as the simulation results for the transversal Hadamard gates protected by selected distance-3 QTECCs, are depicted in Fig. 6.15. We observe that the analytical QBER upper bound of Eq. (6.81) is a very good approximation for the QBER performance of distance-3 colour code based on the simulation results in Fig. 6.15(a). It is because the construction of distance-3 colour code is identical with the 7-qubit Steane's code, which is a non-degenerate QSC. In general, Eq. (6.81) is a good approximation for non-degenerate QSCs. By contrast, a slightly different phenomenon can be observed in Fig. 6.15(b) and 6.15(c), where the simulation results are closer with the analytical lower bound QBER performance owing to their highly degenerate property.

Next, in Fig. 6.16, we portray the analytical upper bound and the lower bound QBER performance of transversal Hadamard gates protected by QTECCs for various minimum distance values. More specifically, we calculate the upper bound QBER performance of colour codes, rotated-surface codes, surface codes, and toric codes having the minimum distances of $d = \{3, 5, 7, 9, 11\}$ using Eq. (6.81) and their lower bound QBER performances using Eq. (6.82). The code parameters of the QTECCs used for calculating the upper bound and lower bound QBER performance are summarized in Table 6.1. One of the unique properties of QTECCs is that upon increasing the minimum distance of the code d, we simultaneously increase the number of the physical qubits length n and decrease the quantum coding rate r_Q [2]. The quantum coding rate r_Q portrayed in Fig. 6.16 is calculated using $r_Q = k/n$, where the number of logical qubits k and the number of physical qubits n are also given in Table 6.1.

Increasing the error correction capability of QTECCs means that we simultaneously increase the number of auxiliary qubits and reduce the quantum coding rate r_Q. On the other hand, at high error rates, a lower quantum coding rate QECCs often carry out flawed corrections, hence actually degrading the QBER more at high depolarizing probability values. The superior error correction capability of the lower rate quantum codes start to impose below a specific depolarizing probability p, which we refer to as the *depolarizing probability threshold* (p_{th}). More specifically, p_{th} represents the point below which increasing the error correction capability of a quantum code is considered to be beneficial. Additionally, the value of p_{th} also can be used to infer the asymptotic performance of the QTECCs exhibiting a large number of physical qubits, where the quantum coding rate r_Q approaches zero. In Fig. 6.16, the p_{th} is denoted by a dashed line at the cross-over point of the QBER performance curves. First, we obtain the upper bound of p_{th} for colour codes, rotated-surface codes, surface codes, and toric codes as follows: 2.61×10^{-3}, 2.71×10^{-3}, 1.26×10^{-3}, and 1.36×10^{-3}, respectively. These specific p_{th} values are obtained by taking into account the erroneous stabilizer measurements. Specifically, each of the physical qubits of rotated-surface and surface codes experiences only at most two **X** and two **Z** stabilizer measurements, while for colour codes, each of the physical qubits experience at most only three **X** and three **Z** stabilizer measurements. These numbers of the stabilizer measurements experienced by each of the physical qubits are independent of the total number of the physical qubits. In a case where we want to consider that we have perfect stabilizer measurements, indeed we can achieve a higher p_{th} values. We can simply use Eq. (6.75) and (6.78) to obtain the p_{th} values associated with error-free stabilizer measurements. More specifically, we obtain the p_{th} values as follows: 1.83×10^{-2}, 1.36×10^{-2}, 6.30×10^{-3}, and 6.80×10^{-3}, respectively, for colour, rotated-surface, surface, and toric codes.

Secondly, in Fig. 6.16, we can also observe the lower bound of the p_{th} values as follows: 1.54×10^{-2}, 2.04×10^{-2}, 2.13×10^{-2}, and 2.17×10^{-2}, respectively, for colour, rotated-surface, surface, and toric codes, which are associated with errorneous stabilizer measurements. Similarly, in a case where we assume that we have the error-free stabilizer measurements, the obtained p_{th} values are: 10.78%, 10.20%, 10.65%, and 10.85%, respectively, for colour, rotated-surface, surface, and toric codes. We observe that all of the p_{th} lower bound values are in the proximity of $p_{th} \approx 11\%$, which is very relevant with the quantum Hashing limit for dual-containing CSS-type QSCs, which is formulated as:

$$C_Q = 1 - 2H(p), \tag{6.87}$$

where $H(p)$ is the binary entropy of p defined by $H(p) = -p \log_2 p - (1-p)\log_2(1-p)$. Since the quantum coding rate of two-dimensional of QTECCs vanishes to zero to ($r_Q \to 0$) for a very large n ($n \to \infty$), we can calculate that for the asymptotical limit, the QBER performance of QTECCs approaches the ultimate hashing limit for dual-containing CSS-type QSCs, given by $p^* = 11\%$, as we have $r_Q = 0$. It is important to note that the quantum GV bound is a strong lower bound for non-degenerate QSCs. We also need to mention that the value $p^* = 11\%$ is also obtained in different way in [190], where the value is atrributed to Nishimori line.

Finally, we present the performance of the transversal single-qubit quantum gates protected by QSCs in terms of the fidelity (F_{th}) of each of the single-qubit quantum gate. Based on Eq. (6.38), we define the coded fidelity as follows:

$$F_{\text{coded}} = 1 - \text{QBER}_{\text{protected}}. \tag{6.88}$$

Since for asymptotical limit the QBER performance approaches the p_{th} value, we can also determine the fidelity threshold (F_{th}), which is defined as the minimum fidelity required for each of the quantum gates in order to benefit from employing the transversal quantum gates protected by the QSCs. Explicitly, the value of F_{th} for a single-qubit quantum gate can be simply determined as follows:

$$F_{\text{th}} = 1 - p_{th}. \tag{6.89}$$

Based on all the results presented in Fig. 6.16, we can obtain the upper bound of the F_{th} for single-qubit quantum Clifford gates as follows: 99.74%, 99.73%, 99.87%, and 99.86%, respectively, for colour codes, rotated-surface codes, surface codes, and toric codes. Similarly, we also obtain the lower bound of the F_{th} for single-qubit quantum Clifford gates as follows: 98.48%, 97.96%, 97.87%, and 97.83%, respectively, for colour codes, rotated-surface codes, surface codes, and toric codes. These F_{th} values mark the minimum requirement for the physical implementation of the single-qubit quantum gates if the implementation of QECCs within the quantum computers is considered. We have demonstrated that any quantum gates exhibiting lower F_{th} values will not provide any benefit of reliability improvement offered by the QECCs. Finally, all the results presented in this subsection are summarized in Table 6.2.

6.5.3 QTECC-Protected Transversal CNOT Gates

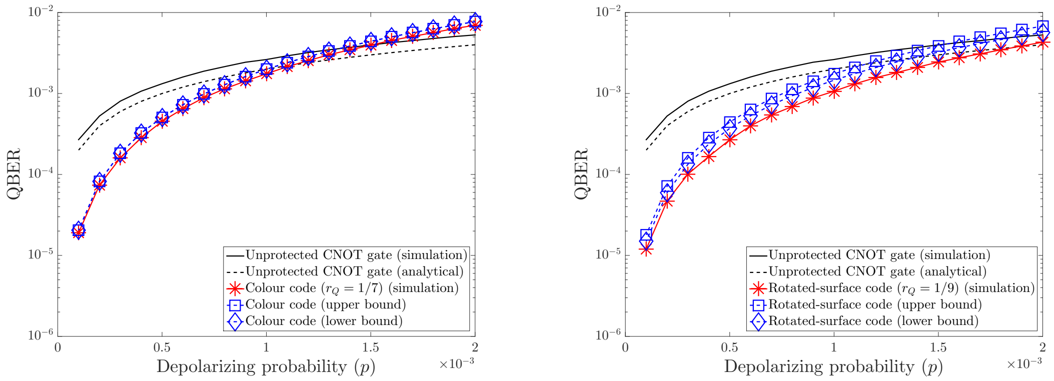
Following similar investigations to those in Subsection 6.5.2, we also employed the family of QTECCs for protecting the transversal CNOT gates. For the transversal configuration of CNOT gates, we have two sets of QSCs, one QSC is invoked for protecting the physical control qubits and another one is for the physical target qubits. We assumed the QSCs used for both target and control qubits are identical. Due to the stabilizer preservation of QSCs after the transversal CNOT gates, as demonstrated in Section 6.3, each of the QSCs handles the errors inherent in the target qubits and in the control qubits independently. The scheme considered as success if both QSCs for control and target qubits perform a flawless error correction procedure simultaneously. Therefore, the upper bound QBER performance of the QSC-protected two-qubit quantum gates, which is denoted as $\text{QBER}^{(2)}_{\text{upper}}$, can be determined by modifying Eq. (6.81) as follows:

$$\begin{aligned}\text{QBER}^{(2)}_{\text{upper}}(n,d,p) &= 1-\left(1-\text{QBER}^{(1)}_{\text{upper}}(n,d,p)\right)^2 \\ &= 1-\left(\sum_{i=0}^{t=\lfloor\frac{d-1}{2}\rfloor}\binom{n}{i}p^i(1-p)^{n-i}\right)^2 . \qquad (6.90)\end{aligned}$$

In this case, we assume that $p = p_f$ considering the errorneous stabilizer measurements, which is given by Eq. (6.75) for rotated-surface codes, surface codes, and toric codes, and by Eq. (6.78).

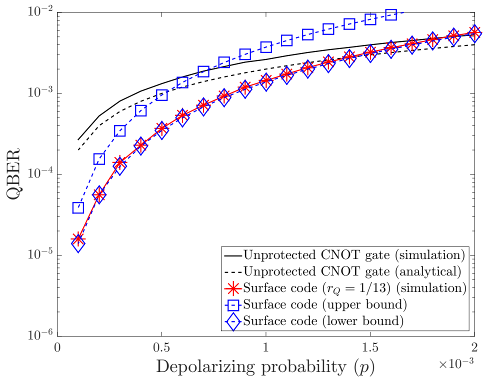
Similar to the case of transversal Hadamard gates, we also incorporate the formula of Eq. (6.82) for determining the lower bound of the QBER performance of the transversal CNOT gates protected by QSCs as follows:

$$\begin{aligned}\text{QBER}^{(2)}_{\text{upper}}(n,d,p) &= 1-\left(1-\text{QBER}^{(1)}_{\text{lower}}(n,d,p)\right)^2 \\ &= 1-\left(1-\sum_{i=0}^{t'+1}A_i p^i(1-p)^{n-i}\right)^2 \qquad (6.91)\end{aligned}$$



(a) Colour codes.

(b) Rotated-surface codes.



(c) Surface codes.

Figure 6.17: QBER performance for transversal CNOT gates protected by distance-3 QTECCs over quantum depolarizing channel. The quantum decoherence is inflicted after the transversal configuration of CNOT gates, where the error operators of $\prod_{i=1}^{c} P_i \in \mathcal{P}_n$ are defined by $p_i = p$. The number of consecutive error operators is $c = 7$ for colour codes and $c = 5$ for rotated-surface and surface codes.

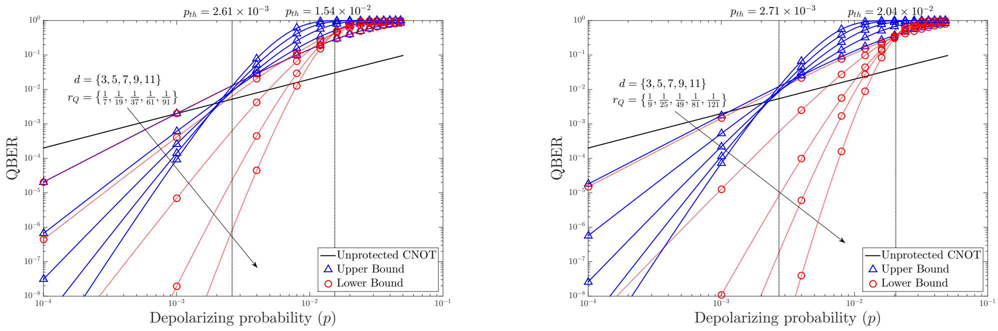
given that A_i is a whole number coefficient subjected to

$$\sum_{i=0}^{t'+1} A_i \leq 2^{(n-k)/2}, \text{ where } A_i = \binom{n}{i}. \tag{6.92}$$

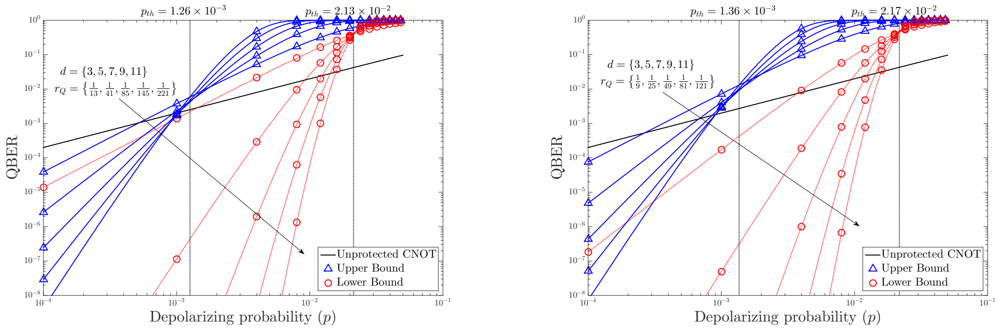
Consequently, the final coefficient $A_{t'+1}$ can be determined by

$$A_{t'+1} = 2^{(n-k)/2} - \sum_{i=0}^{t'} A_i. \tag{6.93}$$

To verify the analytical expression of Eq. (6.90), we have simulated the performance of QTECC-protected transversal CNOT gates protected by distance-3 colour code, rotated-surface code, and surface code, exploiting the classical-to-quantum Pauli isomorphism. The results are depicted in Fig. 6.17. As expected, a similar trend to the QBER performance to the transversal Hadamard gates protected by QTECCs is displayed. An improvement in terms of QBER can be observed for depolarizing probabilities $p < 2 \times 10^{-3}$. Therefore, we conclude that our design in Fig. 6.5 indeed improves the reliability of both Hadamard



(a) Colour codes. (b) Rotated-surface codes.



(c) Surface codes. (d) Toric codes.

Figure 6.18: The upper and lower bound QBER analytical performance curves of the transversal implementation of CNOT gates protected by various QTECCs.

gates as well as of CNOT gates.

Furthermore, we have plotted the upper and lower bound QBER analytical performance given in Eq. (6.90) for the transversal implementation of CNOT gates employing various types of QTECCs for different minimum distances d based on the code parameters of Table 6.1. The corresponding QBER performance curves are portrayed in Fig. 6.18. We can also infer p_{th} values, which define the depolarizing probability value where we can start observing QBER improvements upon decreasing the quantum coding rate. Again, they also mark the QBER performance of the QSCs at the asymptotical limit. The p_{th} is represented by dashed lines, where we have 2.61×10^{-3}, 2.71×10^{-3}, 1.26×10^{-3}, and 1.36×10^{-3}, respectively, for colour codes, rotated-surface codes, surface codes, and toric codes. Similarly, we have also plotted the lower bound QBER analytical performance of the transversal CNOT gates protected by various QTECCs in Fig. 6.18 based on Eq. (6.91). In this case, we have the p_{th} values of 1.54×10^{-2}, 2.04×10^{-2}, 2.13×10^{-2}, and 2.17×10^{-2}, respectively, for colour, rotated-surface, surface, and toric codes.

Since the improvement in QBER domain can be clearly observed, it is logical that the corresponding fidelity improvement can also be achieved. The essential question is what level of the fidelity the quantum gates have to be provided for ensuring that the QSC-protected quantum gates improve the overall fidelity of the system. Firstly, we have defined the output fidelity of the CNOT gates in Eq. (6.42), which is given below:

$$F_{\text{coded}} = 1 - \text{QBER}_{\text{protected}}. \tag{6.94}$$

For asymptotical limit, based on Eq. (6.42), we can determine the threshold fidelity (F_{th}) as follows:

$$\begin{aligned} F_{\text{th}} &= 1 - 2p_{\text{th}} + p_{\text{th}}^2 \\ &\approx 1 - 2p_{\text{th}}, \end{aligned} \tag{6.95}$$

for $p_{\text{th}} \ll 1$. First, based on the upper bound QBER analytical performance curves portrayed in Fig. 6.18, we can obtain the upper bound F_{th} values required by each of the CNOT gates in order to gain the benefit of employing QSCs for protecting the transversal CNOT gates. By using Eq. (6.95), we have the upper bound of the F_{th} values of 99.48%, 99.46%, 99.74%, and 99.72%, respectively, for colour codes, rotated-surface codes, surface codes, and toric codes. Additionally, the lower bound of the F_{th} can also be obtained using Eq. (6.95), where we have: 99.48%, 99.46%, 99.74%, and 99.72%,, respectively, for colour codes, rotated-surface codes, surface codes, and toric codes. All of the results presented in this subsection are summarized in Table 6.2. Finally, we have shown that our framework proposed for protecting transversal quantum Clifford gates will provide a reliability improvement for both single-qubit and two-qubit gates, provided that the fidelity threshold required for each of the quantum gates is satisfied.

6.6 Conclusions and Research

6.6.1 Conclusions

We have presented a general framework for protecting quantum Clifford gates using QSCs along with the notion of effective stabilizer formalism. In this chapter, we have also provided examples of how to utilize the advocated framework for protecting quantum Clifford gates. More specifically, in order to protect quantum Clifford gates, we arrange the gates in a transversal configuration to exploit the benefit of stabilizer operators preservation. Furthermore, since we considered imperfect quantum gates and also imperfect stabilizer measurements in our scheme, we chose the QTECCs to perform error correction procedure on the erroneous physical qubits. The additional benefit of employing QTECCs is that the number of stabilizer measurements experienced by each of the physical qubits remains constant as we increase the number of physical qubits. Hence, the spreading and propagation of decoherence due to the interaction between qubits during stabilizer measurements can be effectively circumvented. We have shown that by combining the transversal implementation of quantum Clifford gates and the QTECCs, we can indeed improve the reliability of quantum Clifford gates provided that they satisfy a minimum depolarization fidelity threshold F_{th}. In order to determine the approximate value of F_{th}, first, we provide the upper bound and the lower bound for QBER analytical performance for a single-qubit and two-qubit transversal gates protected by QSCs. Based on the upper bound of the QBER performance, we obtain the F_{th} values for single-qubit quantum gates as follows: 99.74%, 99.73%, 99.87%, and 99.86%, respectively, protected using colour, rotated-surface, surface, and toric codes. These F_{th} values were obtained at asymptotical limit, meaning that the number of physical qubits are extremely large ($n \to \infty$) and the quantum coding rates are approaching zero ($r_Q \to 0$). We need to highlight that the upper bound QBER analytical performance portrays the worst-case scenario, where the error correction performance is purely defined by the minimum distance of the QSCs and not considering the advantage of exploiting the degeneracy property inherited by QSCs. As a comparison, based on the upper bound of the QBER performance, we obtain the F_{th} values for single-qubit quantum gates as follows: 98.46%, 97.96%, 97.87%, and 97.83%, respectively, protected by colour, rotated-surface, surface, and toric codes. By contrast, the lower bound QBER analytical performance portrays the optimistic scenario, where we assume that the degeneracy property inherited by QTECCs can be exploited to approach the sphere-packing bound for non-degenerate QSCs.

By following the same line of investigation, we have also obtained the minimum depolarization fidelity threshold F_{th} values for two-qubit quantum gates, which is exemplified by CNOT gates in this chapter. The upper bound of the F_{th} values are given by, 99.48%, 99.46%, 99.74%, and 99.72%, respectively, protected by colour, rotated-surface, surface, and toric codes. Similarly, the lower bound of the F_{th} values are 96.92%, 95.92%, 95.74%, and 95.66%,, respectively, protected using colour, rotated-surface, surface, and toric codes. Ultimately, we believe that all the F_{th} values presented in this chapter mark the minimum requirement need to be satisfied by the physical implementation of quantum gates if we want to achieve the benefit of reliability improvement offered by QECCs for quantum computation.

Table 6.2: The summary of results of QTECC-protected transversal quantum Clifford gates.

Results	Colour codes	Rotated-surface codes	Surface codes	Toric codes
Upper bound p_{th} (error-free measurement)	1.83%	1.36%	0.63%	0.68%
Lower bound p_{th} (error-free measurement)	10.78%	10.20%	10.65%	10.85%
Upper bound p_{th} (with errorneous measurement)	0.26%	0.27%	0.13%	0.14%
Lower bound p_{th} (with errorneous measurement)	1.54%	2.04%	2.13%	2.17%
Upper bound F_{th} for Hadamard gates	99.74%	99.73%	99.87%	99.86%
Lower bound F_{th} for Hadamard gates	98.46%	97.96%	97.87%	97.83%
Upper bound F_{th} for CNOT gates	99.48%	99.46%	99.74%	99.72%
Lower bound F_{th} for CNOT gates	96.92%	95.92%	95.74%	95.66%

6.6.2 Future Research

Our main goal with this chapter is to propose the general framework for protecting quantum gates utilizing QSCs. In these preliminary results, we assume that each of the physical qubits experiences an individual and uncorrelated quantum depolarizing channel. Each of the quantum depolarizing channels is heavily characterized by the number of quantum gates interacting with the associated physical qubit. However, it is important to note that the existence two-qubit quantum gates, such as CNOT gate, potentially introduces error propagations between the physical qubits and hence, creates some level of correlation amongst the quantum depolarizing channels of each of the physical qubits. Therefore, our next step is to include this correlation into our error model to get more realistic insight on error correction performance of the proposed scheme.

We have exemplified the application of the framework for protecting transversal Hadamard and CNOT gates, which is equivalent to a single-step operation of Hadamard gates and CNOT gates. The natural extension of this work is to try to implement the framework for much more complex circuits. Additionally, we have mentioned in this chapter that we only exploited the effective stabilizer formalism for transversal quantum Clifford gates. Therefore, combining the scheme for the Clifford and non-Clifford gates indeed will create the universal set of quantum gates for quantum computation. Ultimately, the final goal is to try to build a universal framework of protecting large-scale quantum computers using QECCs.

Chapter 7

Near-Hashing-Bound Quantum Turbo Short-Block Codes

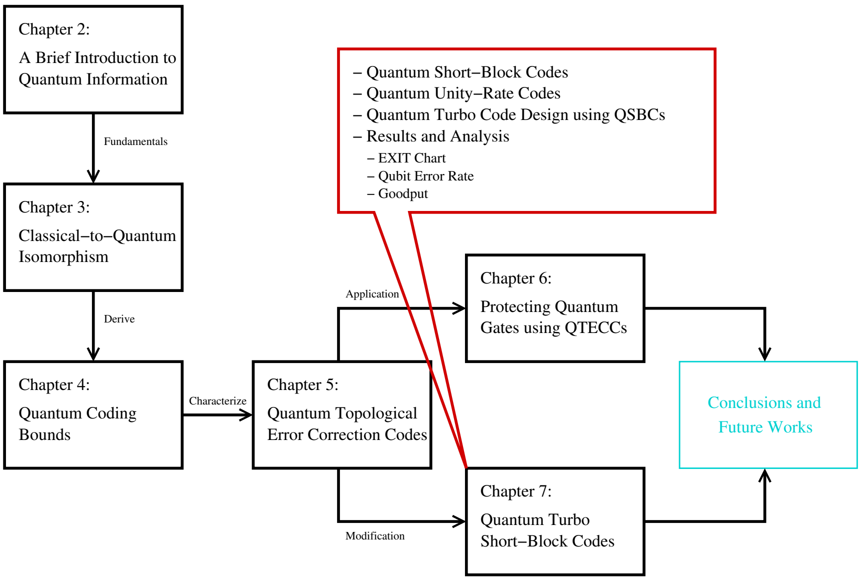


Figure 7.1: The outline of this thesis with the highlight of Chapter 7.

7.1 Introduction

We have established that QSCs [56, 57, 61, 62, 88, 94, 96] are capable of estimating both the number and the position of quantum bit (qubit) errors without collapsing the quantum state of physical qubits into their classical state. Hence, they can be viewed as syndrome-based QECCs. In Chapter 5 and Chapter 6, we have shown that the family of QTECCs suffer from a lower quantum coding rate (r_Q) than their classical counterparts, since they have to tackle not only the bit-flip ($\mathbf{X}$) errors but also the phase-flip ($\mathbf{Z}$) errors [1]. In this chapter, in order to circumvent the issue of having low quantum coding rates, we present a QTC scheme having high quantum coding rates by concatenating quantum error detection codes (QEDCs) inspired by QTECCs with quantum unity rate codes (QURCs).

This work is motivated by [193], where it has been demonstrated that concatenating a quantum linear block code with a unity-rate quantum convolutional code (QCC), which is also referred to as a quantum unity-rate code (QURC), facilitates soft-decision-aided iterative decoding. Hence, a dramatic performance improvement may be attained without reducing the quantum coding rate. However, the solution in [193] suffered from a relatively high error floor, despite relying on a low overall quantum coding rate of $r_Q = 1/8$, when using a block code having a minimum distance of $d = 3$ as the outer code. Additionally, to eliminate the error floor, this specific code construction required a doping mechanism for triggering the convergence of iterative decoding, since the QURC utilized a catastrophic encoder structure. Later in [130], it was shown that by carefully selecting the inner and the outer codes using an EXIT-chart-aided code search, a half-rate quantum turbo code (QTC) can be conceived, which is capable of performing relatively close to the quantum hashing bound. Explicitly, this excellent error correction performance was achieved by a half-rate quantum irregular convolutional codes (QIrCCs) used as the outer codes combined with a QURC as the inner code. This specific code is referred to as the QIrCC-QURC scheme.

As an important result in the classical domain, it was shown that an outer code exhibiting a minimum distance of $d = 2$ is capable of guaranteeing the convergence of iterative decoding to a vanishingly low bit error ratio (BER) [194,195], as exemplified by the family of single parity-check codes (SPCs) or short-block codes (SBCs) [196,197]. Furthermore, by exploiting the classical-to-quantum isomorphism [1,2], we can indeed conceive the quantum-domain version of the classical SBCs, which we referred to as quantum short-block codes (QSBCs). As an additional benefit, the QSBCs can also be viewed as quantum topological error correction codes (QTECCs). More specifically, the QTECC construction exhibits an inherent error detection and error correction capability, when the physical qubits are appropriately arranged on a lattice structure. However, most of the conventional techniques of constructing the QTECCs suffer from a low quantum coding rate as well as from the lack of flexibility, when choosing the number of logical qubits and also the quantum coding rate [2]. By contrast, when a similar approach relying on utilizing a lattice structure is invoked for constructing quantum error detection codes (QEDCs) instead of quantum error correction codes (QECCs), we found that the resultant topological QEDCs are flexible and exhibit high quantum coding rates.

The rest of this chapter is organized as follows. In Section 7.2, we present the general formulation of QSBCs in terms of their code construction, encoder, and stabilizer measurement. This is followed by Section 7.3, where we propose serially concatenated QTCs by utilizing QSBCs as the outer codes and a QURC as the inner code, which we refer to as the QSBC-QURC scheme. We analyze the convergence behaviour of our iterative-decoding-aided QSBC-QURC scheme using EXIT charts and evaluate both its QBER and its goodput in Section 7.4. Finally, we conclude the chapter and present some promising directions for future research in Section 7.5.

7.2 Quantum Short-Block Codes

In this section, we introduce the quantum version of classical SBCs by describing their general construction, the structure of the quantum encoder, as well as the quantum circuit required for the stabilizer measurements. This section will also characterize both the flexibility and scalability of the QSBC encoders and the associated stabilizer measurements, as the natural evolution from their PCM structure. Furthermore, we present a short tutorial on conducting the classical simulation for QSBCs. In order to avoid ambiguity, throughout the rest of this chapter the notation $\mathcal{C}(n,k,d)$ is used to denote the classical error correction code having codeword length of n bits, information word k bits, and a minimum distance of d, while the notation $\mathcal{C}[n,k,d]$ is used for the quantum stabilizer code.

7.2.1 Codes Construction

The classical SBCs are systematic linear binary block codes $\mathcal{C}\left(n,k,d\right)$, whose generator matrix $\mathbf{G}$ is defined by:

$$\mathbf{G} = \left[\mathbf{I}_k|\mathbf{P}_{k,(n-k)}\right] = \left[\mathbf{I}_k|\mathbf{J}_{k,1}\right], \tag{7.1}$$

where $\mathbf{I}_k$ is a k-dimension identity matrix, $\mathbf{P}_{k,(n-k)}$ is a $(k\times(n-k))$-element binary matrix and $\mathbf{J}_{m,n}$ is a matrix with all-one $(m\times n)$-element. Hence, the PCM $\mathbf{H}$ of a systematic linear block code is encapsulated in

$$\mathbf{H} = \left[\mathbf{I}_{n-k}|\mathbf{P}^T\right]. \tag{7.2}$$

Therefore, the PCM $\mathbf{H}$ of the classical SBCs is given by

$$\mathbf{H} = \mathbf{J}_{1,n}, \tag{7.3}$$

which is an all-one $(1\times n)-$element matrix. Finally, the resultant coding rate is given by

$$r = \frac{k}{n} = \frac{k}{k+1} = \frac{n-1}{n}. \tag{7.4}$$

The minimum distance of the SBCs conceived is $d=2$, hence this guarantees the convergence of iterative decoding to a vanishingly low BER, when they constitute the outer code [194, 195].

By exploiting the classical-to-quantum isomorphism [1], this specific type of classical SBCs can be readily transformed into their quantum counterparts. To elaborate a little further, given a pair of classical codes $\mathcal{C}_1(n,k_1,d_1)$ and $\mathcal{C}_2(n,k_2,d_2)$ having PCMs $\mathbf{H}_1$ and $\mathbf{H}_2$, respectively, a QSC $\mathcal{C}[\tilde{n},\tilde{k},\tilde{d}]$ having a binary PCM $\mathbf{H}$ can be constructed from $\mathbf{H}_x = \mathbf{H}_1$ and $\mathbf{H}_z = \mathbf{H}_2$ so that $\mathbf{H}_x$ will be used for mitigating the bit-flip errors and $\mathbf{H}_z$ will be used for mitigating the phase-flip errors, where we have $\tilde{n}=n$, $\tilde{k}=k_1+k_2-n$, and $\tilde{d}=\min(d_1,d_2)$. In general, there are two ways of constructing the binary PCM $\mathbf{H}$ of a QSC $\mathcal{C}$ given a pair of PCMs $\mathbf{H}_x$ and $\mathbf{H}_z$. Firstly, we may construct a CSS type quantum code, whose binary PCM **H** is as follows [88]:

$$\mathbf{H} = \left[\begin{array}{c|c} \mathbf{H}_z & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_x \end{array}\right]. \tag{7.5}$$

Secondly, we may also construct a non-CSS type quantum code, whose binary PCM **H** is given by [96]

$$\mathbf{H} = \left[\begin{array}{c|c} \mathbf{H}_z & \mathbf{H}_x \end{array}\right]. \tag{7.6}$$

In order to conceive a valid PCM **H** for a QSC $\mathcal{C}$, a pair of PCMs $\mathbf{H}_x$ and $\mathbf{H}_z$ has to satisfy the symplectic criterion, which is defined as [96]

$$\mathbf{H}_z.\mathbf{H}_x^T + \mathbf{H}_x^T.\mathbf{H}_z = 0. \tag{7.7}$$

Therefore, the symplectic criterion formulated for a CSS type quantum code can be reduced to

$$\mathbf{H}_z.\mathbf{H}_x^T = 0. \tag{7.8}$$

A specific case of CSS type quantum codes, where we have $\mathbf{H}_x = \mathbf{H}_z$, is referred to as a dual-containing CSS quantum code. Therefore, the dual-containing CSS quantum codes can be instantly derived from the classical SBCs having the following PCMs:

$$\mathbf{H}_z^T = \mathbf{H}_x^T = \mathbf{J}_{1,n}, \tag{7.9}$$

where n is an even number. This automatically satisfies the symplectic criterion of Eq. (7.8). Ultimately, the resultant PCM of QSBCs is given by:

$$\mathbf{H} = \left[\begin{array}{c|c} \mathbf{J}_{1,n} & \mathbf{0} \\ \mathbf{0} & \mathbf{J}_{1,n} \end{array}\right]. \tag{7.10}$$

Hence, for dual-containing CSS quantum codes, the relationship between the classical coding rate r_C and the quantum coding rate r_Q can be described as follows [2, 79, 141]

$$r_Q = 2r_C - 1. \tag{7.11}$$

Since the quantum coding rate r_Q has to be positive ($r_Q > 0$), the original classical code must exhibit a classical coding rate of $r_C > 1/2$.

For QSCs, the PCM **H** is associated with stabilizer operators $S_i \in \mathcal{S}$. For example, let us consider a classical SBC $\mathcal{C}(4, 3, 2)$ having a PCM of

$$\mathbf{H}_x = \mathbf{H}_z = [1\ 1\ 1\ 1], \tag{7.12}$$

exhibiting a classical coding rate of $r_C = 3/4$, which is associated with a QSBC of

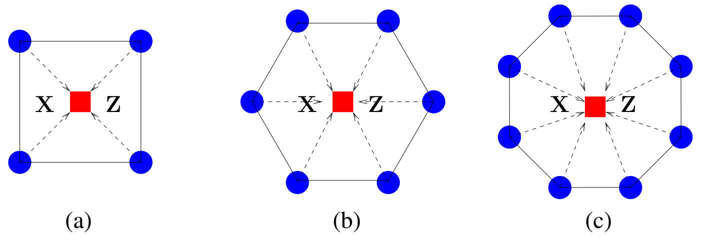


Figure 7.2: QSBCs can be arranged to match the qubit layout on a lattice structure. The blue circles represent the physical qubits, while the red circles denote the stabilizer operators. Each red square is utilized for measuring both **X** and **Z** operator. Hence, the resultant quantum codes belong to the family of dual-containing CSS codes. The quantum coding rate r_Q for construction (a) is 1/2, for (b) is 2/3, and for (c) is 3/4. All of the QSBCs exhibit a minimum distance of $d = 2$.

$\mathcal{C}[n,k,d] = \mathcal{C}[4,2,2]$ having a quantum coding rate of $r_Q = 1/2$. The stabilizer operators of $\mathcal{C}[4,2,2]$ are given by

$$\begin{aligned} S_1 &= \mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4, \\ S_2 &= \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4, \end{aligned} \tag{7.13}$$

where **X** and **Z** are the Pauli matrices. By exploiting the classical-to-quantum isomorphism, we arrive at the PCM **H** of the $\mathcal{C}[4,2,2]$ dual-containing CSS quantum code formulated as

$$\mathbf{H}_{[4,2,2]} = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right]. \tag{7.14}$$

Similarly, we can readily extend the construction to a higher quantum coding rate, as exemplified by $\mathcal{C}[n,k,d] = \mathcal{C}[6,4,2]$, which is derived from a classical SBC of $\mathcal{C}(6,5,2)$. Hence, the stabilizer operators for $\mathcal{C}[6,4,2]$ are defined by

$$\begin{aligned} S_1 &= \mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6, \\ S_2 &= \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6. \end{aligned} \tag{7.15}$$

For this construction, the resultant quantum coding rate is $r_Q = 2/3$. The same analogy can be used for constructing $\mathcal{C}[n,k,d] = \mathcal{C}[8,6,2]$ derived from a classical SBC $\mathcal{C}(8,7,2)$. Therefore, the stabiizer operators are as follows:

$$\begin{aligned} S_1 &= \mathbf{Z}_1\mathbf{Z}_2\mathbf{Z}_3\mathbf{Z}_4\mathbf{Z}_5\mathbf{Z}_6\mathbf{Z}_7\mathbf{Z}_8, \\ S_2 &= \mathbf{X}_1\mathbf{X}_2\mathbf{X}_3\mathbf{X}_4\mathbf{X}_5\mathbf{X}_6\mathbf{X}_7\mathbf{X}_8. \end{aligned} \tag{7.16}$$

The resultant QSBC exhibits a quantum coding rate of $r_Q = 3/4$. The discussion on how the stabilizer operators S_i can be invoked for detecting quantum errors will be discussed in subsection 7.2.3.

Furthermore, the QSBCs can also be classified as a family of QTECCs, as shown in Fig. 7.2. Assuming that we can arrange the physical qubits on the vertices of a lattice structure, it inherently provides a localized stabilizer measurement property. Since the resultant QSC constructions are only capable of error detection, which is a consequence of having a minimum distance of $d = 2$, the stabilizer measurements can only indicate the presence or the absence of quantum errors, but not the specific numbers or the position of the errors. However, we will show later that this error detection capability can be transformed into error correction capability by concatenating QSBCs with a carefully selected inner code.

7.2.2 Quantum Encoder

In quantum domain, a k-logical qubit information word in the state of $|\psi\rangle$ can be transformed into a n-physical qubit codeword in the state of $|\overline{\psi}\rangle$, where $n > k$, with the aid of $(n-k)$ auxiliary qubits initialized in the state of $|0\rangle$. This specific transformation, which is carried out by a unitary transformation $\mathcal{V}$ referred to as a quantum encoder, can be formally described as follows[1]:

$$\mathcal{V}\left(|\psi\rangle^{k} \otimes |0\rangle^{\otimes(n-k)}\right) = |\overline{\psi}\rangle^{n}. \tag{7.17}$$

This process is reminiscent of the encoding process of classical error correction codes. To elaborate, in the classical domain, we can transform a k-bit information word into an n-bit codeword with the aid of the generator matrix $\mathbf{G}$, where the additional $(n-k)$ bits are referred to as the redundant bits.

Based on the description of QSBCs in Subsection 7.2.1, they can be classified as a member of the dual-containing CSS code family. For this specific class of quantum codes, the design of the quantum encoder $\mathcal{V}$ can be readily derived from its classical PCMs [71,134]. More specifically, the PCM of the classical code $\mathcal{C}(n,k,d)$ may be utilized to obtain the quantum encoder $\mathcal{V}$ of a QSC $\mathcal{C}[\tilde{n},\tilde{k},\tilde{d}]$, where $\tilde{n} = n$, $\tilde{k} = 2k - n$, and $\tilde{d} = d$.

Let us now embark on creating the quantum encoder $\mathcal{V}$ of dual-containing CSS codes derived from the classical codes $\mathcal{C}(n,k,d)$. The PCM of the classical code $\mathcal{C}(n,k,d)$ can be represented by a full-rank matrix $\mathbf{H}$ having $n \times (n-k)$ elements. Naturally, every PCM $\mathbf{H}$ of linear block codes can be transformed into the corresponding systematic form of

$$\widetilde{\mathbf{H}} = [\mathbf{I}_{n-k} | \mathbf{A}_{n-k,k}] \tag{7.18}$$

by using row operations and column permutations, where $\mathbf{I}_{n-k}$ is a $(n-k)$-dimension identity matrix, and the matrix $\mathbf{A}$ has $(n-k) \times k$ elements. For the next step, we may further reduce the matrix $\mathbf{A}$ into another systematic form of

$$\widetilde{\mathbf{A}} = [\mathbf{I}_{n-k} | \mathbf{B}_{n-k,2k-n}], \tag{7.19}$$

where $\mathbf{I}_{n-k}$ is another $(n-k)$-dimension identity matrix and the matrix $\mathbf{B}$ has $(n-k) \times (2k-n)$ elements.

---

[1] The superscript of n in notation $|\psi\rangle^{n}$ denotes the number of physical qubits, which is n, given a quantum state $|\psi\rangle$. This notation will be used throughout this chapter.

Ultimately, the quantum encoder $\mathcal{V}$ of a dual-containing CSS code can be described as a two-stage encoder. The first stage of the quantum encoder is used for initializing a set of codewords $\mathcal{C}$, which must not have a difference exactly corresponding to a specific legitimate codeword of $\mathcal{C}^{\perp}$, where $\mathcal{C}^{\perp}$ is the dual code of $\mathcal{C}$. Therefore, it can be utilized for generating the unique cosets of $\mathcal{C}$ relative to $\mathcal{C}^{\perp}$. Next, the second stage of quantum encoder $\mathcal{V}$ is invoked for generating the code space of $\mathcal{C}^{\perp}$ according to the PCM $\widetilde{\mathbf{H}}$. Hence, the resultant states after the first and the second stage are constituted by the superposition of all the codewords of $\mathcal{C}^{\perp}$ generated by the second stage added to the codewords of $\mathcal{C}$ generated in the first stage. The more general method of constructing the quantum encoder $\mathcal{V}$ for all types of QSCs, including the non-dual-containing CSS codes and non-CSS codes, can be found in [148, 149].

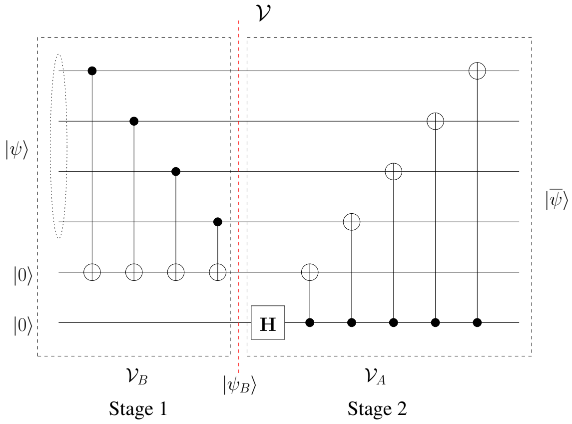


Figure 7.3: The quantum encoder $\mathcal{V}$ can be described as a two-stage encoder. For the QSBCs, the CNOT connections of the first stage $\mathcal{V}_B$ are defined by matrix $\mathbf{B}$ of Eq. (7.22), while those of the second stage $\mathcal{V}_A$ are defined by matrix $\mathbf{A}$ of Eq. (7.21).

For gleaning a clearer idea about the two-stage quantum encoder $\mathcal{V}$, let us consider the QSBC $\mathcal{C}\,[6,4,2]$ and construct its quantum encoder $\mathcal{V}$ based on the classical PCM $\mathbf{H}$ derived from a classical code $\mathcal{C}(6,5,2)$ as follows:

$$\mathbf{H} = [1\ 1\ 1\ 1\ 1\ 1]. \tag{7.20}$$

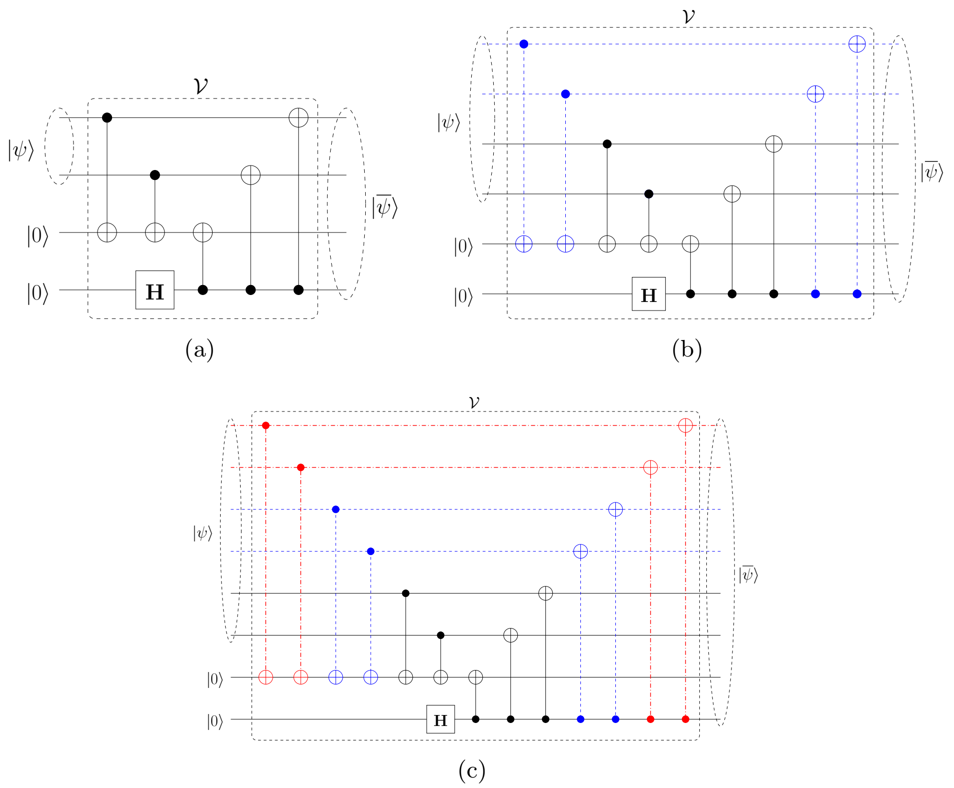
Fortunately, the PCM $\mathbf{H}$ has already a systematic structure, hence we have $\mathbf{H} = \widetilde{\mathbf{H}}$. From the PCM $\mathbf{H}$ in Eq. (7.20), matrix $\mathbf{A}$ is readily given by

$$\mathbf{A} = [1\ 1\ 1\ 1\ 1]. \tag{7.21}$$

Consequently, given that $\mathbf{A} = \widetilde{\mathbf{A}}$, we obtain the matrix $\mathbf{B}$ as follows:

$$\mathbf{B} = [1\ 1\ 1\ 1]. \tag{7.22}$$

Based on Eq. (7.21) and (7.22), the first stage and the second stage of the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[6,4,2]$ is denoted by $\mathcal{V}_B$ and $\mathcal{V}_A$, respectively, in Fig. 7.3. To elaborate a little further, the CNOT connections between the logical qubits in the state of $|\psi\rangle$ and the first auxiliary qubits are defined by the matrix $\mathbf{B}$. More specifically, given



(a) (b) (c)

Figure 7.4: The quantum encoder $\mathcal{V}$ of QSBSc for various quantum coding rates: (a) $\mathcal{C}[4,2,2]$, $r_Q = 1/2$, (b) $\mathcal{C}[6,4,2]$, $r_Q = 2/3$, (c) $\mathcal{C}[8,6,2]$, $r_Q = 3/4$.

the element $b_{i,j}$ of matrix $\mathbf{B}$, if the value of $b_{i,j} = 1$, it means that the j-th logical qubit controls the CNOT connection of the i-th auxiliary target qubit. As an example, based on the matrix $\mathbf{B}$ in Eq. (7.22), we can see that at the first stage $\mathcal{V}_B$ of the quantum encoder $\mathcal{V}$ the first auxiliary qubit is controlled by all four logical qubits in the state of $|\psi\rangle$, since the matrix $\mathbf{B}$ contains all 1 elements.

Consequently, the first stage $\mathcal{V}_B$ of the quantum encoder $\mathcal{V}$ transforms the first m auxiliary qubits, which are initialized to the state of $|0\rangle$, according to the logical qubits $|\psi\rangle$. Explicitly, given that $|\psi\rangle = |\mathbf{c}\rangle$, where c is a k-bit binary string, the first stage $\mathcal{V}_B$ of the quantum encoder $\mathcal{V}$ transforms the auxiliary qubits into the state of $|\mathbf{Bc}\rangle$. Therefore, the state of physical qubits at the output of the first stage $\mathcal{V}_B$, namely $|\psi_B\rangle$, created by the action of the first stage $\mathcal{V}_B$ of quantum encoder $\mathcal{V}$ of Fig. 7.3 can be expressed as follows:

$$|\psi_B\rangle = \mathcal{V}_B\left(|\mathbf{c}\rangle^k|\mathbf{0}\rangle^{\otimes m}|\mathbf{0}\rangle^{\otimes m}\right) = |\mathbf{c}\rangle^k|\mathbf{Bc}\rangle^m|\mathbf{0}\rangle^{\otimes m}, \tag{7.23}$$

where $m = n - k$. Hence, as we have mentioned earlier that the first stage $\mathcal{V}_B$ of quantum encoder $\mathcal{V}$ creates a set of codewords $\mathcal{C}$, which must not have a difference exactly corresponding to a specific legitimate codeword in $\mathcal{C}^\perp$. For example, based on the PCM $\mathbf{H}$ of a classical code $\mathcal{C}(6,5,2)$ given in Eq. (7.20), we can construct the code space of the dual code $\mathcal{C}^\perp$ as follows:

$$\mathcal{C}^\perp = \{000000, 111111\}. \tag{7.24}$$

For a given k-bit binary string of $\mathbf{c}$, the binary string of $[\mathbf{c}, \mathbf{Bc}, \mathbf{0}]$ is indeed a codeword in

$\mathcal{C}$. Let us denote the set of all the n-bit binary string of $[\mathbf{c}, \mathbf{Bc}, \mathbf{0}]$ as $\mathcal{B}$, which basically creates a subspace of $\mathcal{C}$, i.e. $\mathcal{B} \subseteq \mathcal{C}$. More explicitly, the code space of $\mathcal{B}$ based on matrix $\mathbf{B}$ of Eq. (7.22) is given as follows:

$$\begin{aligned}\mathcal{B} = \{&000000, 000110, 001010, 001100, 010010, 010100, 011000, 011110,\\ &100010, 100100, 101000, 101110, 110000, 110110, 111010, 111100\}.\end{aligned} \tag{7.25}$$

It is clear that none of the codeword in $\mathcal{B}$ differs by one element in $\mathcal{C}^{\perp}$, i.e. adding any codeword from the non-zero codeword in $\mathcal{C}^{\perp}$ to the one of the codeword in $\mathcal{B}$ does not yield another codeword in $\mathcal{B}$, since the last m bits of $\mathcal{B}$ contains all 0 element, while the non-zero codeword of $\mathcal{C}^{\perp}$ has 1s in the last m bits. Hence, each k-bit binary string of $\mathbf{c}$ creates a unique coset in $\mathcal{C}$ relative to the $\mathcal{C}^{\perp}$.

The second stage $\mathcal{V}_A$ of the quantum encoder $\mathcal{V}$ is started by initializing the remaining $m = n - k$ auxiliary qubits in the state of $|+\rangle$ states by using m Hadamard gates, which can be expressed mathematically as follows:

$$\mathbf{H}^{\otimes m}|\mathbf{0}\rangle^{\otimes m} = |+\rangle^{\otimes m} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes m} = \frac{1}{2^{m/2}} \sum_{i}^{2^m-1} |\mathbf{i}\rangle. \tag{7.26}$$

Explicitly, Eq. (7.26) basically represents a sum of an equal superposition of all possible states over all 2^m binary strings of length m. Next, we combine the initialized equal superposition of Eq. (7.26) with the output of the first stage $|\psi_B\rangle$. Let us assume that string $\mathbf{t}$ denotes the string of $[\mathbf{c}, \mathbf{Bc}]$. The effect of this operation is to add rows of PCM $\widetilde{\mathbf{H}} = [\mathbf{I}_{n-k}|\mathbf{A}_{n-k,k}]$ to the binary string $\mathbf{t}$. Hence, for a given k-bit binary input string of $\mathbf{c}$, the final state of the physical qubits after the first and the second stage of the quantum encoder $\mathcal{V}$ can be expressed as

$$|\overline{\psi}\rangle = \frac{1}{2^{m/2}} \sum_{\mathbf{r} \in \mathcal{C}^{\perp}(\mathbf{H})} |\mathbf{r} + \mathbf{t}\rangle^n. \tag{7.27}$$

Finally, if the state of the k logical qubits is expressed in the form of the superposition the binary strings $\mathbf{c}_i$ as follows:

$$|\psi\rangle^k = \sum_{i}^{2^k-1} p_i |\mathbf{c}_i\rangle^k, \tag{7.28}$$

then the output state of the physical qubits $|\overline{\psi}\rangle$ can be formulated as

$$|\overline{\psi}\rangle^n = \sum_{\mathbf{y} \in \mathcal{C}(\mathbf{H})} p_{\mathbf{y}} \sum_{\mathbf{r} \in \mathcal{C}^{\perp}(\mathbf{H})} |\mathbf{r} + \mathbf{y}\rangle^n. \tag{7.29}$$

Readers who might be interested in different examples of creating encoders for various dual-containing CSS codes exemplified by Steane's code $\mathcal{C}[7, 1, 3]$ of [94] and by the quantum Bose-Chaudhuri-Hocquenghem (QBCH) code $\mathcal{C}[15, 7, 3]$ of [63], please refer to [134].

The resultant quantum encoders $\mathcal{V}$ conceived for the QSBCs $\mathcal{C}[4, 2, 2]$, $\mathcal{C}[6, 4, 2]$, and $\mathcal{C}[8, 6, 2]$ can be seen in Fig. 7.4, where they demonstrate that the QSBC encoders $\mathcal{V}$ exhibit the natural design for flexibility. Figure 7.4(a) depicts the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[4,2,2]$. By incorporating additional gates and connections denoted by the dashed blue lines in Fig. 7.4(b) into the quantum encoder of Fig. 7.4(a), we obtain the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[6,4,2]$. Similarly, by adding more gates and connections denoted by a dashed-dotted red lines to the quantum encoder of Fig. 7.4(b), we can readily create the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[8,6,2]$ of Fig. 7.4(c). In other words, we can construct the quantum encoder $\mathcal{V}$ of QSBCs for a high quantum coding rate, which will simultaneously contain the quantum encoder $\mathcal{V}$ of the lower quantum coding rate. Therefore, it is no longer necessary to build more than one quantum encoder $\mathcal{V}$ for various quantum coding rates of QSBCs because the quantum encoder $\mathcal{V}$ of QSBCs exhibits a self-contained structure. This is reminiscent of the classical rate-compatible punctured codes proposed in [198].

7.2.3 Stabilizer Measurement for QSBCs

The QSCs are capable of predicting both the number and the position of errors without actually observing the states of the physical qubits. In order to achieve this, a syndrome-decoding-like method was introduced [61]. Instead of observing the information within the physical qubits, which would collapse the superposition state to a classical state, a set of auxiliary qubits are prepared for observing the syndrome of the physical qubits using the so-called stabilizer operators. A stabilizer operator S_i belonging to the stabilizer group $\mathcal{S} \in \mathcal{P}_n$ is an n-tuple Pauli operator, which stabilizes the state of the encoded physical qubits $|\overline{\psi}\rangle$ may be formulated as follows:

$$S_i|\overline{\psi}\rangle = |\overline{\psi}\rangle. \tag{7.30}$$

An error operator $P \in \mathcal{P}_n$ inflicted by the quantum channel on the encoded state of physical qubits transforms the legitimate state $|\overline{\psi}\rangle$ into the contaminated received state $|\widetilde{\psi}\rangle$, which can be expressed as follows:

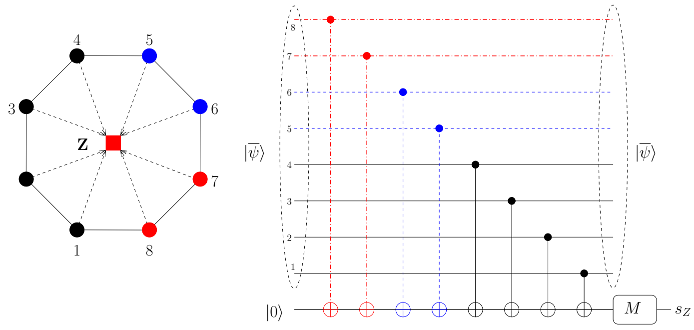
$$|\widetilde{\psi}\rangle = P|\overline{\psi}\rangle. \tag{7.31}$$

The syndrome values can be obtained by performing eigenvalue-based measurement of the received state $|\widehat{\psi}\rangle$ assisted by the auxiliary qubits, which can be defined as follows:

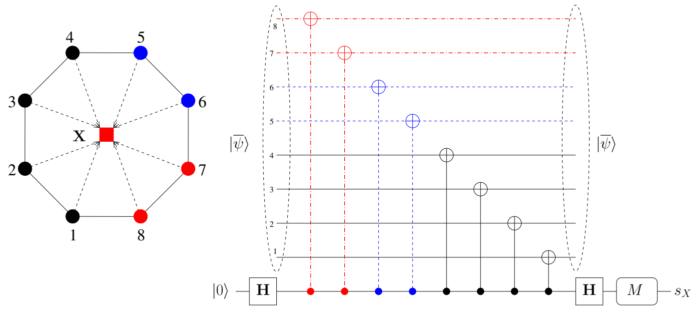
$$S_i|\widetilde{\psi}\rangle = \begin{cases} |\widetilde{\psi}\rangle & , \quad S_iP = PS_i \\ -|\widetilde{\psi}\rangle & , \quad S_iP = -PS_i. \end{cases} \tag{7.32}$$

The ±1 eigenvalues attained from the stabilizer measurement act similarly to the $\{0,1\}$ values of the classical syndrome measurements. Hence, they also can be used for inferring both the number and the position of errors without actually observing the state of the physical qubits.

As we briefly discussed, the eigenvalue measurements require an extra auxiliary qubit



(a) **Z**-stabilizer measurement.



(b) **X**-stabilizer measurement.

Figure 7.5: Stabilizer measurements of QSBCs, which are capable of supporting various quantum coding rates.

for each stabilizer measurement. As for QSBCs, the stabilizer measurement can be implemented using the circuits seen in Fig. 7.5. More specifically, Fig. 7.5(a) depicts the **Z**-stabilizer measurement, while Fig. 7.5(b) portrays the **X**-stabilizer measurement. It can be observed that for both **X** and **Z** stabilizer measurements, the circuit constructed for realizing the stabilizer measurements of a QSBC having a higher quantum coding rate inherently contains the stabilizer measurements required for a QSBC having a lower quantum coding rate. To elaborate a little further, in Fig. 7.5, the circuit implementation of the stabilizer measurements of a 1/2-rate QSBC is highlighted using black solid lines. In case we want to employ another QSBC having a higher quantum coding rate, for example, a 2/3-rate QSBC, we can simply incorporate the stabilizer measurement from the 1/2-rate scheme and add further gates, which are highlighted using blue dashed lines in Fig. 7.5 without changing the stabilizer measurement circuit. A similar approach is applicable when we want to employ a 3/4-rate QSBC. We incorporate the stabilizer measurements of the 2/3-rate QSBC and then add more gates, which are highlighted using red dashed lines. Ultimately, we have shown that the nature of the PCMs from the QSBCs leads to a very convenient design for their quantum encoders and for their stabilizer measurements, which are capable of supporting multiple quantum coding rates of $r_Q = \frac{k}{k+1}$ using a single quantum circuit implementation.

7.2.4 Classical Simulation for QSBCs

The quantum encoder $\mathcal{V}$ of a QSBC and its inverse encoder $\mathcal{V}^\dagger$ are composed of quantum Clifford gates. This implies that they can be conveniently simulated using classical computers [132]. An n-tuple Pauli operator $P \in \mathcal{P}_n$ can be represented by a $2n$-element binary vector, where each of the n-element binary vectors constitutes a Pauli $\mathbf{Z}$ and a Pauli $\mathbf{X}$ component. The mapping of the Pauli matrix to the associated binary vector can be formulated as follows:

$$\begin{aligned}
\mathbf{I} &\rightarrow \left[\begin{array}{c|c} 0 & 0 \end{array}\right], \\
\mathbf{X} &\rightarrow \left[\begin{array}{c|c} 0 & 1 \end{array}\right], \\
\mathbf{Y} &\rightarrow \left[\begin{array}{c|c} 1 & 1 \end{array}\right], \\
\mathbf{Z} &\rightarrow \left[\begin{array}{c|c} 1 & 0 \end{array}\right].
\end{aligned} \tag{7.33}$$

The evolution of the Pauli operator $P \in \mathcal{P}_n$ over quantum Clifford gates can be described using the conjugation operation. Explicitly, the conjugation of a unitary operator $\mathbf{N}$ under the unitary transformation $\mathbf{M}$ is the unitary transformation $\mathbf{V}$, which is defined as [132]

$$\mathbf{V} = \mathbf{M} \cdot \mathbf{N} \cdot \mathbf{M}^{\dagger}. \tag{7.34}$$

For instance, based on Eq. (7.34), the conjugation of the Pauli matrix $\mathbf{Z}$ and $\mathbf{X}$ over Hadamard ($\mathbf{H}$) gate is given by

$$\begin{aligned}
\mathbf{H} \cdot \mathbf{Z} \cdot \mathbf{H}^{\dagger} &= \mathbf{X}, \\
\mathbf{H} \cdot \mathbf{X} \cdot \mathbf{H}^{\dagger} &= \mathbf{Z}.
\end{aligned} \tag{7.35}$$

Additionally, we can also describe the conjugation of a Pauli matrix $\mathbf{Z}$ and $\mathbf{X}$ over a two-qubit quantum gate, as exemplified by a CNOT gate, as follows:

$$\begin{aligned}
(\mathbf{CNOT}) \cdot (\mathbf{Z} \otimes \mathbf{I}) \cdot (\mathbf{CNOT})^{\dagger} &= \mathbf{Z} \otimes \mathbf{I}, \\
(\mathbf{CNOT}) \cdot (\mathbf{I} \otimes \mathbf{Z}) \cdot (\mathbf{CNOT})^{\dagger} &= \mathbf{Z} \otimes \mathbf{Z}, \\
(\mathbf{CNOT}) \cdot (\mathbf{X} \otimes \mathbf{I}) \cdot (\mathbf{CNOT})^{\dagger} &= \mathbf{X} \otimes \mathbf{X}, \\
(\mathbf{CNOT}) \cdot (\mathbf{I} \otimes \mathbf{X}) \cdot (\mathbf{CNOT})^{\dagger} &= \mathbf{I} \otimes \mathbf{X},
\end{aligned} \tag{7.36}$$

where the first Pauli matrix is applied to the control qubit, while the second Pauli matrix is applied to the target qubit.

Therefore, using the conjugation definition of Eq. (7.34), we can keep track of the evolution of any n-tuple Pauli operator $P \in \mathcal{P}_n$ owing to unitary operations carried out by quantum Clifford gates, such as the QSBC encoders $\mathcal{V}$ and also its inverse encoder $\mathcal{V}^{\dagger}$ illustrated in Fig. 7.4. Since the quantum encoders $\mathcal{V}$ of QSBCs are only composed of Hadamard and CNOT gates, we can create a $(2n \times 2n)$-element binary matrix V for classically simulating the evolution of the Pauli operator $P \in \mathcal{P}_n$ over the quantum encoder $\mathcal{V}$. As an example, let us consider the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[4, 2, 2]$ seen in Fig. 7.6.

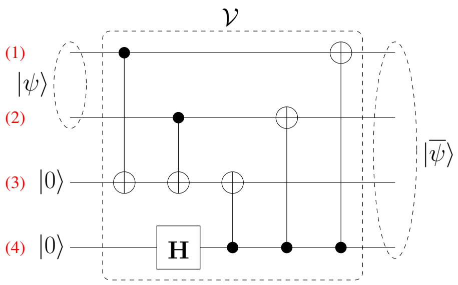


Figure 7.6: The quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[4,2,2]$.

We commence by initializing $V^{(0)} = \mathbf{I}_{2n}$, where $\mathbf{I}_{2n}$ is a $2n$-dimensional identity matrix formulated as follows:

$$V^{(0)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]. \tag{7.37}$$

The i-th and the $(n+i)$-th column of matrix $V^{(0)}$ are associated with the evolution of the Pauli matrices $\mathbf{Z}$ and $\mathbf{X}$, respectively, on the i-th qubit.

The first unitary operation in the QSBC encoder $\mathcal{V}$ of Fig. 7.6 is the unitary operation $\text{CNOT}(1,3)$, where the notation $\text{CNOT}(i,j)$ means that the i-th qubit controls the j-th qubit. Now, based on Eq. (7.36), the CNOT unitary transformation propagates the Pauli $\mathbf{X}$ matrix from the control qubit to the target qubit and by contrast, propagates the Pauli $\mathbf{Z}$ matrix from the target qubit to the control qubit. Therefore, in the matrix V, the unitary transformation $\text{CNOT}(i,j)$ can be carried out by replacing the i-th column with the modulo-2 addition between the i-th column and the j-th column then replacing the $(n+j)$-th column with the modulo-2 addition between the $(n+i)$-th column and the $(n+j)$-th column. In the case of $V^{(0)}$, the unitary transformation $\text{CNOT}(1,3)$ can simply be viewed as copying the 1 value from the 3-rd column to the 1-st column then copying the value 1 from 5-th column to the 7-th column. Hence, the unitary transformation $\text{CNOT}(1,3)$ transforms the matrix $V^{(0)}$ into the matrix $V^{(1)}$ as follows:

$$V^{(1)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \color{red}\mathbf{1} & 0 & \color{red}\mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \color{red}\mathbf{1} & 0 & \color{red}\mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]. \tag{7.38}$$

We indicate the matrix elements involved in the associated transformation using bold red fonts. The unitary transformation $\text{CNOT}(1,3)$ is followed by the second unitary transformation taking place in the QSBC encoder $\mathcal{V}$ of Fig. 7.6, namely the CNOT$(2,3)$. Following the same method as that used for obtaining the matrix $V^{(1)}$, the action of CNOT$(2,3)$ applied to the matrix $V^{(1)}$ yields the matrix $V^{(2)}$ as follows:

$$V^{(2)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]. \tag{7.39}$$

The third unitary transformation taking place within the QSBC encoder $\mathcal{V}$ of Fig. 7.6 is the Hadamard transformation $\mathbf{H}(4)$. Based on Eq. (7.35), the Hadamard transformation modifies the Pauli matrix $\mathbf{Z}$ into $\mathbf{X}$ and vice versa. Therefore, in a matrix V, a Hadamard transformation of $\mathbf{H}(i)$ can be interpreted as swapping the value of the i-th column and the $(n+i)$-th column. In case of the matrix $V^{(2)}$, the action of the unitary transformation $\mathbf{H}(4)$ swaps the value of 4-th column and the 8-th column, hence resulting in the matrix $V^{(3)}$ as follows:

$$V^{(3)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]. \tag{7.40}$$

These operations are then followed by the unitary transformation CNOT$(4,3)$, which yields the matrix $V^{(4)}$ as follows:

$$V^{(4)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]. \tag{7.41}$$

The action of CNOT$(4,2)$ upon the matrix $V^{(4)}$ gives us the matrix $V^{(5)}$ as follows:

$$V^{(5)} = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]. \tag{7.42}$$

Finally, applying the CNOT$(4,1)$ transforms the matrix $V^{(5)}$ into the final matrix V as follows:

$$V = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}\right]. \tag{7.43}$$

The resultant matrix V is the classical analogue of the quantum encoder $\mathcal{V}$ of the QSBC $\mathcal{C}[4,2,2]$ seen in Fig. 7.6. In order to obtain the matrix V^{-1} of the quantum inverse encoder $\mathcal{V}^{\dagger}$, the same method is invoked. The only difference is that we apply the transformation for each step by reading the quantum circuit from right to the left.

In order to show that the matrix V can be used for classical simulation, let us consider a Pauli operator $P \in \mathcal{P}_4$ as follows:

$$P = \mathbf{Z} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{Y}. \tag{7.44}$$

By using the Pauli-to-binary mapping of Eq. (7.33), the Pauli operator P given in Eq. (7.44) can be transformed into its classical analogue as follows:

$$P = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right]. \tag{7.45}$$

The resultant Pauli operator $\widehat{P}$ due to the QSBC encoder V can be obtained by modulo-2 multiplication $(*)$ of the vector P and the matrix V, which gives us

$$\begin{aligned} \widehat{P} &= P * V \\ &= \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]. \end{aligned} \tag{7.46}$$

From the resultant vector $\widehat{P}$ of Eq. (7.46) and also from the Pauli-to-binary mapping of Eq. (7.33), we can map back the binary vector $\widehat{P}$ into its corresponding Pauli operator, which gives us $\widehat{P} \in \mathcal{P}_4$ as follows:

$$\widehat{P} = \mathbf{Y} \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X}. \tag{7.47}$$

In order to simplify the expression of matrix V, often the seed transformation $\mathcal{U}$ representation is used. The U_i element of the seed transformation $\mathcal{U} = \{U_1, U_2, \ldots, U_{2n}\}$ is the decimal representation of the i-th row of the binary matrix V. Therefore, based on the matrix V of Eq. (7.43), the associated seed transformation $\mathcal{U}$ is given by

$$\mathcal{U} = \{144, 80, 240, 15, 10, 6, 2, 16\}_{10}. \tag{7.48}$$

Finally, the seed transformations $\mathcal{U}$ for all the QSBC encoders of Fig. 7.4 are provided in Table 7.1.

7.3 Quantum Turbo Code Design Using QSBCs

QSBCs on their own are only capable of detecting the presence of errors in the state of physical qubits, but not correcting them. This limited capability is due to the minimum distance of $d = 2$ inherited from the classical SBCs. In this chapter, we invoke the QTC scheme utilized in [76,79] as the foundation of developing QSBC-based QTCs. The QSBCs are invoked as the outer codes, while a non-catastrophic and non-recursive QURC is used as the inner code, which we will refer to as the QSBC-QURC scheme for the rest of this chapter.

The QTC scheme was first introduced by Poulin *et. al* in [76]. The proposed QTC utilized two QCCs, which were concatenated serially. Each of the QCC components exhibits a 1/3 quantum coding rate and hence, the final quantum coding rate r_Q is 1/9. To the best of our knowledge, the QTCs operating closest to the quantum hashing bound rely on the construction presented in [79,199] in the open literature. The near-hashing-bound performance was attained by utilizing QIrCCs both as the outer and the inner codes. Furthermore, the weighting factors of the QIrCC component codes were optimized by invoking EXIT-chart-based heuristic search [199,200]. Readers who are interested to delve deeper into QTCs and near-hashing-bound constructions, please refer to [79].

7.3.1 Encoding Process

In this section, we will describe the proposed QSBC-QURC scheme, whose general schematic can be seen in Fig. 7.7. The outer encoder $\mathcal{V}_1$ in Fig. 7.7 is a QSBC encoder, which is already shown in Fig. 7.4(a) for an instance of half-rate QSBC. It maps k_1 logical qubits into n_1 physical qubits with the aid of $(n_1 - k_1)$ auxiliary qubits according to the following transformation:

$$\mathcal{V}_1 \left(|\psi\rangle^{k_1} \otimes |0\rangle^{\otimes(n_1-k_1)} \right) = |\overline{\psi_1}\rangle^{n_1}. \tag{7.49}$$

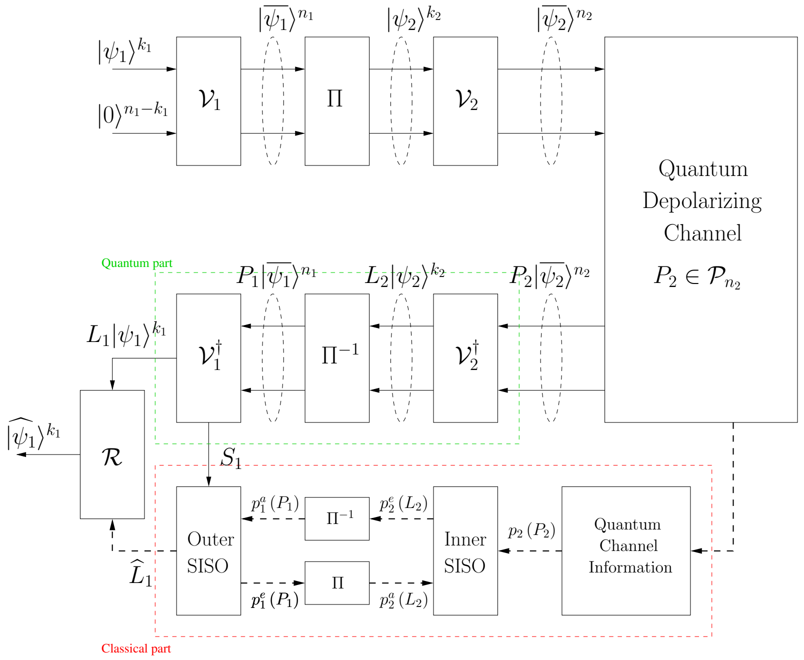


Figure 7.7: The general schematic of serial QTCs utilizing QURC as the inner code. The decoding process, in general, can be separated into two parallel processes, namely the quantum processing part and the classical processing part. The quantum part is represented by the green dashed lines, while the classical part is represented by red the dashed lines.

The output of $\mathcal{V}_1$ is fed to the interleaver Π, which can be represented mathematically as a permutation matrix and can be realized physically as a series of quantum SWAP gates. The interleaving process can be formally written as

$$\Pi\left(|\overline{\psi_1}\rangle^{n_1}\right) = |\psi_2\rangle^{k_2}, \tag{7.50}$$

where we have $k_2 = n_1$, since the interleaver does not alter the number of physical qubits, only rearranges the position of the qubits indices in the quantum state. Hence, the Hamming weight of the state of physical qubits is not changed after this process. Next, the output of the interleaver Π is fed into the inner encoder $\mathcal{V}_2$, which carries out the following transformation:

$$\mathcal{V}_2\left(|\psi\rangle^{k_2} \otimes |0\rangle^{\otimes(n_2-k_2)}\right) = |\overline{\psi_2}\rangle^{n_2}. \tag{7.51}$$

The encoder $\mathcal{V}_2$ maps the state of k_2 logical qubits into the state of n_2 physical qubits with the aid of $(n_2 - k_2)$ auxiliary qubits. Since, we are employing the QURCs as the inner codes, the transformation in Eq. (7.51) can be further simplified as

$$\mathcal{V}_2\left(|\psi\rangle^{k_2}\right) = |\overline{\psi_2}\rangle^{n_2}. \tag{7.52}$$

The main difference between the interleaver and the QURC is that the state of physical qubits after the QURC may experience Hamming weight alterations.

7.3.2 Quantum Depolarizing Channel

After the encoding process, the encoded state of physical qubits may experience quantum decoherence. In this study, we use the quantum depolarizing channel [131]. This depolarizing channel models the imperfection of quantum gates, as well as the coherence taking place in the quantum memory, and even the actual quantum transmission channel through free space or optical fiber channels. The quantum decoherence is represented by the n-tuple Pauli operator $P_2 \in \mathcal{P}_n$ and its action imposed upon the encoded state of physical qubits $|\overline{\psi_2}\rangle^{n_2}$ can be expressed as

$$|\widetilde{\psi}\rangle = P_2\left(|\overline{\psi_2}\rangle^{n_2}\right). \tag{7.53}$$

The error operator P_2 is characterized by the depolarizing probability p. To elaborate a little further, the error operator $P \in \mathcal{P}_n$ is an n-tuple Pauli operator, where each qubit may independently experience a bit-flip ($\mathbf{X}$) error, a phase-flip ($\mathbf{Z}$) error as well as a simultaneous bit-flip and phase flip ($\mathbf{Y}$) error. The probability of each qubit experiencing an $\mathbf{X}$, $\mathbf{Z}$, and $\mathbf{Y}$ error is denoted by $p_{\mathbf{X}}$, $p_{\mathbf{Z}}$, and $p_{\mathbf{Y}}$, respectively. Under the assumption that $p_{\mathbf{X}} + p_{\mathbf{Y}} + p_{\mathbf{Z}} = p$ and $p_{\mathbf{X}} = p_{\mathbf{Y}} = p_{\mathbf{Z}} = p/3$, this quantum channel is referred to as *symmetric quantum depolarizing channel* [131]. Needless to say, it is always possible to create a model where we have the assumption that $p_{\mathbf{X}} \neq p_{\mathbf{Y}} \neq p_{\mathbf{Z}}$, which can be deeemed to be more realistic [117]. However, choosing the value such as $p_{\mathbf{X}} = p_{\mathbf{Y}} = p_{\mathbf{Z}}$ will provide us with the worst-case scenario, because we have to provide the same level of protection for different types of errors without favoring only one specific type of error, which can result in quantum coding rate or QBER improvements. A more detailed discourse on QSC design for asymmetric quantum depolarizing channels, enthusiastic readers might like to refer to [117, 147, 201, 202].

7.3.3 Decoding Process

Generally speaking, the decoding process of any QSC relies on the conjunction of two parts, namely the quantum information processing part and the classical information processing part. In Fig. 7.7, the quantum processing part is marked by the components bounded by the green dashed lines, while the classical processing part is represented by the components bounded by the red dashed lines. First, let us describe the quantum processing part. The corrupted state of physical qubits $|\widetilde{\psi_2}\rangle^{n_2}$ is fed to the inverse encoder $\mathcal{V}_2^\dagger$ of Fig. 7.7, which represents the conjugate transpose of encoder $\mathcal{V}_2$. Physically, they can be implemented identically with the only difference is that the input and output of the inverse encoder $\mathcal{V}^\dagger$ is in the reverse position compared to the encoder $\mathcal{V}$. Since the quantum encoder $\mathcal{V}$ and its inverse encoder $\mathcal{V}^\dagger$ are composed by the quantum Clifford gates and the error operator P is an n-tuple Pauli operator $P \in \mathcal{P}_n$, the act of inverse encoders $\mathcal{V}_2^\dagger$ will decompose the error operator P_2 into two error components as follows:

$$\mathcal{V}_2^\dagger\left(P_2\left(|\overline{\psi_2}\rangle^{n_2}\right)\right) = L_2|\overline{\psi_2}\rangle^{k_2} \otimes S_2|0\rangle^{n_2-k_2}, \tag{7.54}$$

where L_2 is the error operator on k_2 logical qubits and S_2 is the error operator on $(n_2 - k_2)$ auxiliary qubits. The auxiliary qubits are then measured in the relevant computational basis, where the value S_2 can be treated as a syndrome in classical error correction codes, which is forwarded to the classical processing part. However, since the inverse encoder of $\mathcal{V}_2^\dagger$ is an inverse encoder of a QURC, Eq. (7.54) can be further simplified to

$$\mathcal{V}_2^\dagger \left(P_2 \left(|\psi_2\rangle^{n_2}\right)\right) = L_2|\psi_2\rangle^{k_2}, \tag{7.55}$$

since we have $k_2 = n_2$. Next, the output of the inverse encoder $\mathcal{V}_2^\dagger$ is passed trough the deinterleaver Π^{-1}. This transformation can be formally expressed as

$$\Pi^{-1}\left(L_2|\overline{\psi_2}\rangle^{k_2}\right) = P_1|\overline{\psi_1}\rangle^{n_1}. \tag{7.56}$$

The output of the deinterleaver is then processed as the input of $\mathcal{V}_1^\dagger$, which is subjected to an identical transformation as $\mathcal{V}_2^\dagger$. This can be expressed as follows:

$$\mathcal{V}_1^\dagger \left(P_1 \left(|\overline{\psi_1}\rangle^{n_1}\right)\right) = L_1|\psi_1\rangle^{k_1} \otimes S_1|0\rangle^{n_1-k_1}. \tag{7.57}$$

In this QSBC-QURC scheme, the inverse encoder of $\mathcal{V}_1^\dagger$ is constituted by the quantum inverse encoder $\mathcal{V}^\dagger$ of the QSBC, which is implemented by flipping the input and ouput of the quantum encoder $\mathcal{V}$ seen in Fig. 7.4(a) for an instance of half-rate QSBC.

Finally, based on the information obtained from the classical information processing part, the error recovery operator $\mathcal{R}$ is applied to the output of the inverse encoder $\mathcal{V}_1^\dagger$ in order to obtain the predicted logical qubit state as follows:

$$\mathcal{R}\left(L_1|\psi_1\rangle^{k_1}\right) = |\widehat{\psi_1}\rangle^{k_1}. \tag{7.58}$$

If $\mathcal{R} = L_1$, we obtain $|\widehat{\psi_1}\rangle^{k_1} = |\psi_1\rangle^{k_1}$, which completes our decoding process.

Let us now take a step back to elaborate a little further on the classical processing part of the decoding process. The classical decoder part for a QTC is very similar to that of classical turbo codes. It consists of two soft-input soft-output (SISO) decoders, an interleaver, and a deinterleaver.

As seen in Fig. 7.7, the classical processing is started by obtaining the quantum depolarizing probability p of the quantum channel associated with the error operator P_2. In this work, we assume that we have perfect knowledge of the quantum depolarizing probability p. The depolarizing probability value p and the *a priori* information $p_2^a(L_2)$ obtained from the outer SISO decoder are used by the inner SISO decoder for calculating the extrinsic information $p_2^e(L_2)$. For the first iteration, the depolarizing probability p is the only input value used by the inner SISO decoder. Hence, the value of $p_2^a(L_2)$ is initialized to be equiprobable. Next, the extrinsic information $p_2^e(L_2)$ is interleaved in order to obtain the *a priori* information $p_1^a(P_1)$ for the outer SISO decoder. By combining the *a priori* information $p_1^a(P_1)$ and the syndrome value S_1, the outer SISO decoder calculates the extrinsic information $p_1^e(P_1)$. The extrinsic value is then deinterleaved to yield $p_2^a(L_2)$ which is fed into the inner SISO decoder. This process is performed iteratively until one of the following conditions is satisfied: the converged mutual information is attained or the maximum affordable number of iterations is reached. On the final iteration, the outer SISO decoder will produce $\widehat{L}_1$, which is the most likely error pattern, given the value of p and S_1 provided by the quantum processing part. The value of $\widehat{L}_1$ is obtained for performing error recovery, as detailed in Eq. (7.58). A more rigorous treatment on the classical processing part of QTCs can be found in [78, 79]

7.4 Results and Analysis

In this section, firstly, we analyze the performance of the QSBC-QURC conceived using EXIT charts [200,203,204]. In the classical domain, EXIT charts constitute a powerful tool, which is often used for guiding the design of near-capacity iterative error correction and for predicting their performance. An initial encouraging effort conducted in [199] invoked EXIT charts for predicting the performance of iterative QTCs demonstrating that EXIT charts can be indeed extended to the quantum domain. Secondly, we proceed by characterizing the performance of the QSBC-QURC scheme in terms of its quantum bit error ratio (QBER), which we obtained from our Monte Carlo simulations. Thirdly, we translate the QBER performance to the distance from the quantum hashing bound, which directly corresponds to the efficiency of quantum channel utilization, which is also related to the goodput. Finally, we use the goodput metric for determining the depolarizing probability at which switching to different quantum coding rate becomes beneficial for conceiving a multi-rate QSBC-QURC scheme.

7.4.1 EXIT Chart

In the classical domain, the encoders exhibiting recursive and non-catastrophic properties are highly desirable for conceiving near-capacity turbo codes. Unfortunately, in the quantum domain, the QCCs cannot be simultaneously recursive and non-catastrophic [205]. The recursive structure of QCCs is required for ensuring the convergence of iterative decoding to a vanishingly low QBER. Additionally, the QCCs exhibiting catastrophic structure require a doping mechanism or entanglement-assisted solution to substantially benefit from iterative decoding, since catastrophic QCCs provide zero *a priori* information [78, 206]. These two solutions are beyond the scope of our discussions in this paper. Fortunately, a non-recursive and non-catastrophic QCCs can still be designed for striking an attractive compromise, since they can achieve beneficial iteration gains even if the inner decoder EXIT curve terminates at the $(1, y)$ point for $y < 1$, provided that it only intersects with the outer decoder EXIT curves near $x = 1$ [130]. Based on these conditions, an exhaustive EXIT-chart-based heuristic search has been conducted to find a "good" QURC. The resultant seed transformation for such a QURC is given by

$$\mathcal{U} = \{21, 56, 5, 46, 44, 38\}_{10}. \tag{7.59}$$

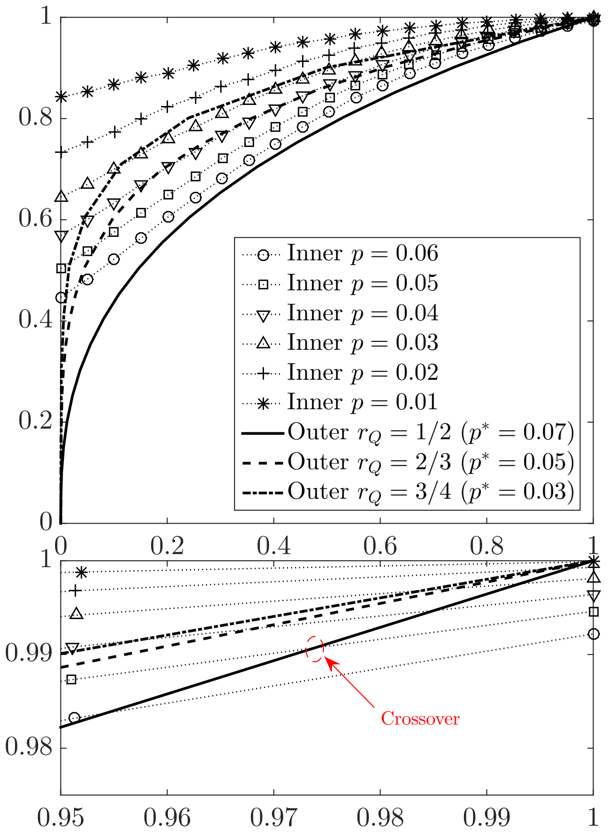


Figure 7.8: Outer decoder EXIT curves for the QSBCs used as the outer codes and the inner decoder EXIT curves for the QURC as the inner code. We can take a closer look at the vicinity of the $(1, 1)$ point and observe that despite having been carefully selected, the inner decoder EXIT curve does not reach the $(1, 1)$ point due to the nature of the non-recursive structure.

In this chapter, our QSBC-QURC scheme utilized a specific QURC whose seed transformation is given in Eq. (7.59) and the QSBCs of $\mathcal{C}[4, 2, 2]$, $\mathcal{C}[6, 4, 2]$ and $\mathcal{C}[8, 6, 2]$ were used as the outer codes. The seed transformations of the QSBCs are given in Table 7.1. As a benchmark, we use the QIrCC-QURC scheme presented in [130], where the QIrCCs are optimized using EXIT-chart-aided method specified in [79, 199]. The seed transformation of the QIrCC component codes is given in Table 7.2. As we have described briefly in Subsection 7.2.4, the seed transformation is the decimal representation used for describing the quantum gate connections amongst the physical qubits within the quantum encoder $\mathcal{V}$. Also, it can be used for simulating the QSCs classically.

The QURC we chose, which is defined by the seed transformation in Eq. (7.59), has a non-recursive and non-catastrophic structure. Therefore, the inner decoder EXIT curve will terminate at the $(1, y)$ point, where $y < 1$. In Fig. 7.8, we have plotted the inner decoder EXIT curves for QURCs in the face of various depolarizing probabilities of $p = \{0.06, 0.05, 0.04, 0.03, 0.02, 0.01\}$. At a glance, the inner decoder EXIT curves of the QURC are seen to be capable of reaching the $(1, 1)$ point. However, a closer inspection in the vicinity of the $(1, 1)$ point reveals that indeed the inner decoder EXIT curves terminate at

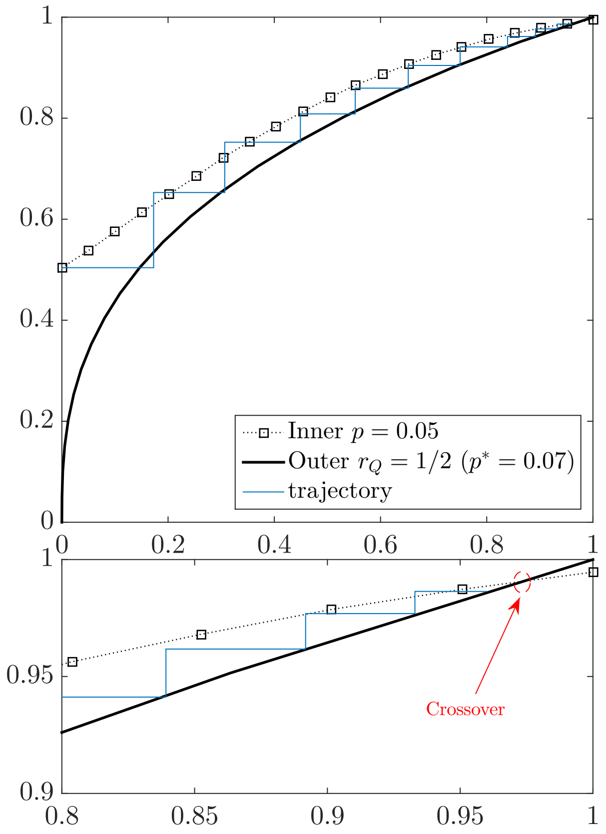


Figure 7.9: The Monte Carlo simulation-based decoding trajectory of mutual information exchange between the classical inner and outer SISO decoders. It can be observed that the decoding trajectory is stuck at the vicinity of $(1, 1)$-point after approximately 10 decoding iterations.

the $(1, y)$ point, where $y < 1$. Hence, in order to attain an infinitesimally low QBER, the condition that the intersection of the inner and outer decoder EXIT curves has to be in the proximity of the $(1, 1)$ point is no longer trivial. Therefore, in Fig. 7.8, we have also plotted the outer decoder EXIT curves for QSBCs having the quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$. We can observe that the intersections of the inner and outer decoder EXIT curves for various quantum coding rates r_Q are in the proximity of the $(1, 1)$ point, as desired. Furthermore, a marginally open EXIT tunnel emerges between the inner decoder EXIT curve for $p = 0.05$ and the outer decoder EXIT curve for a $1/2$-rate QSBC. This indicates that convergence of the iterative decoding is attained at $p \leq 0.05$, which exhibits itself as waterfall region in the QBER curves. Additionally, in Fig. 7.9, we have plotted the stair-case-shaped Monte Carlo simulation-based decoding trajectory of mutual information exchange between the inner and outer SISO decoders. As expected, the decoding trajectory got stuck after approximately 10 iterations between the inner and outer SISO decoder in the vicinity of the $(1, 1)$ point. Given that the iterative decoding of the QSBC-QURC scheme technically does not achieve a full convergence, we expected an error-floor to be present in the QBER curves, which we will discuss in the next subsection.

7.4.2 Quantum Bit Error Rate

Let us now evaluate the error correction performance of the conceived QSBC-QURC schemes based on their QBER and the distance to the quantum hashing bound. The QBER curves of the half-rate QSBC-QURC scheme having $n = \{500, 1000, 2000\}$ physical qubits after 16 decoding iterations using Monte Carlo simulations is portrayed in Fig. 7.10. For the sake of benchmarking, we also simulated the QIrCC-QURC scheme from [130] and we added the QBER curves to Fig. 7.10. Beneficial performance improvements can be observed for both the QSBC-QURC and the QIrCC-QURC arrangements upon increasing the number of physical qubits.

Let us now compare the QBER performance of the QSBC-QURC and the QIrCC-QURC schemes, where the latter is the most powerful half-rate QTC scheme at the time of writing exhibiting the best QBER performance. It can be observed from Fig. 7.10 that for $n = 2000$ physical qubits, the proposed QSBC-QURC scheme offer a substantial performance improvement in the depolarizing probability region of $0.035 < p < 0.055$. However, as we reduce the depolarizing probability of the quantum channel to the region of $p < 0.035$, the QIrCC-QURC scheme outperforms the QSBC-QURC, where the latter has a relatively high error floor. There are two possible explanations for this specific phenomenon exhibited by our design. Firstly, based on our EXIT chart analysis, we already expected the emergence of an error floor since the stair-case-shaped decoding trajectory of the QSBC-QURC scheme got stuck before reaching the $(1, 1)$-point of perfect convergence. However, based on this argument, the QIrCC-QURC should also have an error floor. Indeed, in reality, the QIrCC-QURC scheme is also expected to have an error floor, but at a very low QBER, which is unobservable in Fig. 7.10. This brings us to the second reason, which also explains why the QSBC-QURC scheme has a significantly higher error floor than the QIrCC-QURC scheme. The answer is related to the characteristics of the outer codes. Explicitly, as for the QIrCC-QURC scheme, the outer code is constituted by a set of QCCs exhibiting strong error correction performance despite failing to converge fully. The seed transformation of the QCCs that assembles the QIrCC is given in Table 7.2 [130]. For more detailed descriptions on QIrCCs, we refer the motivated reader to [79]. By contrast, the outer codes for our QSBC-QURC schemes are constituted by QSBCs having a minimum distance of $d = 2$. Compared to QIrCCs, QSBCs are the weaker codes. Consequently, it results in residual qubit errors even in the region of low depolarizing probability p. Our QBER performance comparison between the QIrCC-QURC and QSBC-QURC schemes is summarized in Table 7.3. Once again, we want to highlight that the QSBC-QURC outperforms the QIrCC-QURC scheme for the scenarios of $\text{QBER} < \text{QBER}_{\text{uncoded}}$ and $\text{QBER} < 10^{-3}$. However, due to the relatively high error floor of the QSBC-QURC scheme, for a scenario where $\text{QBER} < 10^{-4}$ is required, the QIrCC-QURC scheme succeeds in meeting this requirement at a higher depolarizing probability p.

However, the main problem with using QIrCCs as the outer codes is that for each quantum coding rate r_Q, it requires another exhaustive search for finding the best code and the resultant codes may not share the same quantum encoder structure. By contrast, the QSBCs having various quantum coding rates r_Q share the same quantum encoder structure,

Table 7.1: The seed transformation $\mathcal{U}$ associated with QSBCs having various quantum coding rates r_Q.

Quantum coding rate (r_Q)	Seed transformation $\mathcal{U}$
1/2	$\{144, 80, 240, 15, 10, 6, 2, 16\}_{10}$
2/3	$\{2112, 1088, 576, 320, 4032, 63, 34, 18, 10, 6, 2, 64\}_{10}$
3/4	$\{33024, 16640, 8448, 4352, 2304, 1280, 65280, 255, 130, 66, 34, 18, 10, 6, 2, 256\}_{10}$

Table 7.2: The seed transformation $\mathcal{U}$ associated with QCCs exhibiting various quantum coding rates r_Q for constructing the QIrCC of [130]. All of the QCCs exhibiting a memory of $m = 3$.

Quantum coding rate (r_Q)	Seed transformation $\mathcal{U}$
1/4	$\{9600, 691, 11713, 4863, 1013, 6907, 1125, 828, 10372, 6337, 5590, 11024, 12339, 3439\}_{10}$
1/3	$\{3968, 1463, 2596, 3451, 1134, 3474, 657, 686, 3113, 1866, 2608, 2570\}_{10}$
1/2	$\{848, 1000, 930, 278, 611, 263, 744, 260, 356, 880\}_{10}$
2/3	$\{529, 807, 253, 1950, 3979, 2794, 956, 1892, 3359, 2127, 3812, 1580\}_{10}$
3/4	$\{62, 6173, 4409, 12688, 7654, 10804, 1763, 15590, 6304, 3120, 2349, 1470, 9063, 4020\}_{10}$

Table 7.3: Performance comparison of half-rate QIrCC-QURC to half-rate QSBC-QURC for $k = \{500, 1000, 2000\}$ logical qubits. The performance is described using the maximum tolerable depolarizing probability p given various requirements, below which the code improves the QBER. For any half-rate QSC, the quantum hashing bound is $p^* = 0.074$.

Requirement	$k = 500$		$k = 1000$		$k = 2000$	
	p QIrCC	p QSBC	p QIrCC	p QSBC	p QIrCC	p QSBC
QBER < uncoded QBER	0.037	**0.050**	0.039	**0.055**	0.043	**0.058**
QBER $= 10^{-3}$	0.028	**0.032**	0.033	**0.039**	0.037	**0.045**
QBER $= 10^{-4}$	**0.024**	0.019	**0.029**	0.028	**0.035**	0.030

as illustrated in Fig. 7.4. Therefore, in terms of flexibility and adaptivity, the QIrCCs-QURC schemes may not be favourable. Since the QSBC-QURC schemes can be configured for various r_Q values using the same quantum encoder, we have to further investigate the performance of the QSBC-QURC scheme exhibiting various r_Q values. In Fig. 7.11, we have plotted the QBER performance of the QSBC-QURC scheme having quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$. Naturally, we can go beyond $r_Q = 3/4$, however, our QTC simulations are limited by the computational power of our classical computers. Figure 7.11 shows that we can reduce the error floor by increasing the number of physical qubits. It also shows that the QSBC-QURC scheme exhibiting a higher quantum coding rate can only cope with a lower quantum depolarizing probability p. However, by increasing the quantum coding rate r_Q, the effective throughput of the quantum depolarizing channel can be improved, since it requires a lower number of auxiliary qubits, which will be discussed further in the next subsection. The performance results of QSBC-QURC schemes exhibiting various quantum coding rates are summarized in Table 7.4.

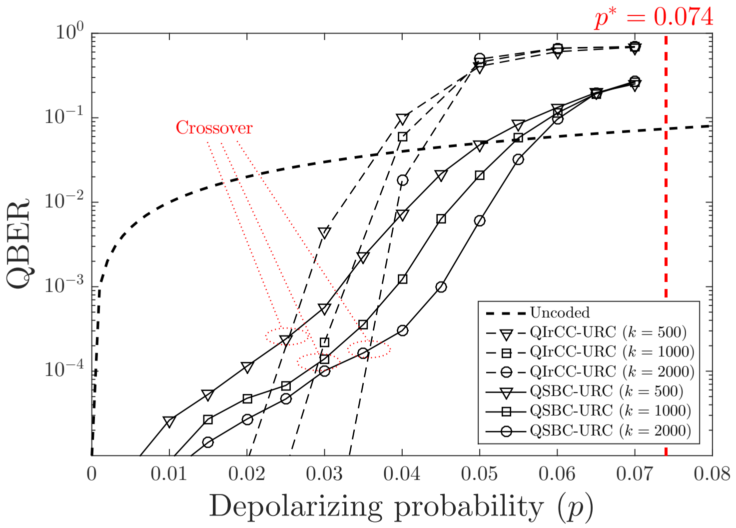


Figure 7.10: QBER versus quantum depolarizing probability curves for the half-rate QSBC-QURC and the half-rate QIrCC-QURC scheme exhibiting various numbers of logical qubits after 16 decoding iterations. For a half-rate QSC, the quantum hashing bound is $p^* = 0.074$.

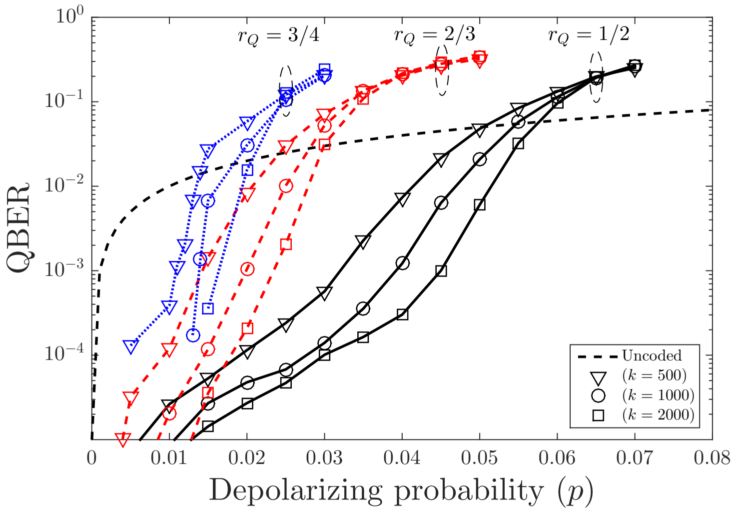


Figure 7.11: QBER versus quantum depolarizing probability curves for QSBC-QURC schemes exhibiting quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$ having $k = \{500, 1000, 2000\}$ logical qubits after 16 decoding iterations.

7.4.3 Goodput

When the quality of the quantum channel starts degrading, a QSC having a certain quantum coding rate r_Q, which was previously capable of correcting all the quantum errors flawlessly, may no longer succeed in error-free decoding. In a condition where a QSC operates in the face of the quantum channel having the depolarizing probability beyond its error correction capability, the QSC may in fact inflict more quantum errors by correcting them in the wrong positions. Hence, the quantum coding rate of a QSC should be adjusted according to the quality of the quantum channel. The most intuitive way of improving the error correction capability of a QSC is to reduce its quantum coding rate, which means imposing more redundancy. Similarly, when the quality of the quantum channel starts

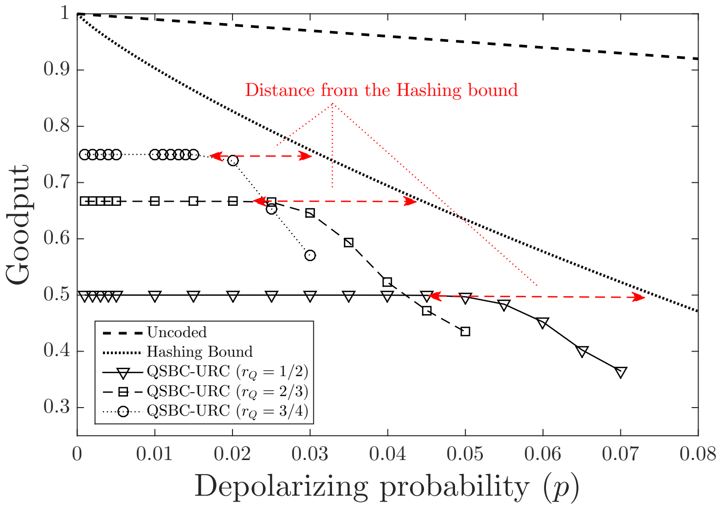


Figure 7.12: Goodput curves versus depolarizing probability for QSBC-URC exhibiting various quantum coding rates having logical qubits $k = 2000$ after 16 decoding iterations. The red dashed lines represent the distance to the quantum hashing bound for each quantum coding rate.

Table 7.4: Performance comparison of QSBC-QURC schemes having $k = \{500, 1000, 2000\}$ logical qubits and quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$. The performance is described using the maximum tolerable depolarizing probability p given various requirements, below which the code improves the QBER performance. The quantum hashing bound for QSCs having $r_Q = \{1/2, 2/3, 3/4\}$ is given by $p^* = \{0.074, 0.044, 0.031\}$.

Requirement	QBER < uncoded QBER			QBER $= 10^{-3}$		
	$r_Q = 1/2$	$r_Q = 2/3$	$r_Q = 3/4$	$r_Q = 1/2$	$r_Q = 2/3$	$r_Q = 3/4$
$k = 500$	0.051	0.024	0.014	0.032	0.014	0.011
$k = 1000$	0.055	0.028	0.018	0.039	0.020	0.014
$k = 2000$	**0.058**	**0.030**	**0.021**	**0.045**	**0.023**	**0.016**

improving, one can increase the quantum coding rate accordingly to reduce the overhead imposed by the QSC and hence, improve the effective throughput.

To elaborate a little further, for a random QSC $\mathcal{C}$ exhibiting quantum coding rate of r_Q having a sufficiently high number of physical qubits, there exists a limit p^* below which it can operate perfectly yielding an infinitesimally low QBER. Hence, the goal of designing a QSC is to ensure that it can operate as close as possible to the limit of p^*. Similarly, for a given depolarizing probability p, we can find a random QSC $\mathcal{C}$ exhibiting a quantum coding rate of $r_Q \leq C_Q(p)$ and having a sufficiently high number of physical qubits that is capable of yielding an infinitesimally low QBER. This specific limit is referred to as the quantum hashing bound, which is defined as follows [71, 78, 168]:

$$\mathcal{C}_Q = 1 - H(p) - p \cdot \log_2(3), \tag{7.60}$$

where $H(p)$ is the binary entropy of p defined by $H(p) = -p \log_2 p - (1-p) \log_2(1-p)$. Given a value of p, then C_Q is the quantum hashing bound for p. Conversely, given a value of r_Q, the value of $p^* = p(r_Q)$ represents the quantum hashing bound for r_Q. For instance, a QSC having a quantum coding rate of $r_Q = 1/2$, the quantum hashing bound is given by $p^* = 0.074$. In Fig. 7.10, the quantum hashing bound is represented by red dashed line. It can be observed that for QBER $= 10^{-3}$, the QSBC-QURC scheme operates close to the quantum hashing bound. Quantitatively, the distance from the quantum hashing bound can be formally defined as

$$D \triangleq p^* - p, \tag{7.61}$$

where p is the achievable depolarizing probability, below which the QSC yields an infinitesimally low QBER. For example, in this chapter, we set the QBER $= 10^{-3}$. Therefore, based on the results in Table 7.3, the half-rate QIrCC-QURC scheme having $n = 2000$ physical qubits operates at $D = 0.074 - 0.037 = 0.0037$ from the quantum hashing bound, while the half-rate QSBC-QURC scheme also having $n = 2000$ physical qubits operates at $D = 0.074 - 0.045 = 0.029$ from the quantum hashing bound, provided that we have QBER $= 10^{-3}$. The distance from the quantum hashing bound constitutes a fair metric of comparing the efficiency of QSCs exhibiting various quantum coding rates. Hence, it has a direct relationship with the goodput, which represents the effective number of logical qubits after the decoding step. The achievable goodput taking quantum coding rate r_Q into account for normalization can be formally defined as

$$\text{Goodput} = r_Q \cdot (1 - \text{QBER}). \tag{7.62}$$

By applying Eq. (7.62), we can transform the QBER perfomance seen in Fig. 7.11 into the goodput performance of Fig. 7.12. We have also plotted the quantum hashing bound formula of Eq. (7.60) to show the visual representation of the relationship between the quantum hashing bound and the goodput performance. In Fig. 7.12, the distance from the quantum hashing bound is shown by the red dashed lines for various quantum coding rates r_Q at QBER $= 10^{-3}$. Quantitatively, given that $r_Q = \{1/2, 2/3, 3/4\}$, the resultant quantum hashing bound is given by $p^* = \{0.074, 0.044, 0.031\}$, while the distance from the quantum hashing bound is given by $D = \{0.029, 0.021, 0.015\}$.

7.4.4 Reconfigurable Scheme

Given a range of various requirements and quantum coding rates, the maximum tolerable depolarizing probability value, below which the QSBC-QURC schemes improve the QBER performance is portrayed in Table 7.4. As we have described earlier, for a certain requirement, there is a quantum coding scheme $\mathcal{C}$ that will satisfy it with the highest quantum coding rate. Again, for instance, given that the depolarizing probability of the quantum channel is $p = 0.01$ and the QBER requirement of QBER $< 10^{-3}$ is sufficient for the quantum computation or communication considered, we do not necessarily invoke a half-rate QSBC-QURC scheme for this purpose, since a 3/4-rate QSBC-QURC scheme is already capable of satisfying the aforementioned conditions. By utilizing a 3/4-rate QSBC-QURC scheme, we can have 50% less auxiliary qubits. For QSBC-QURC scheme, a multi-rate scheme can be readily constructed since a single QSBC-QURC encoder is capable of providing multiple quantum coding rates, as described in Section 7.2.

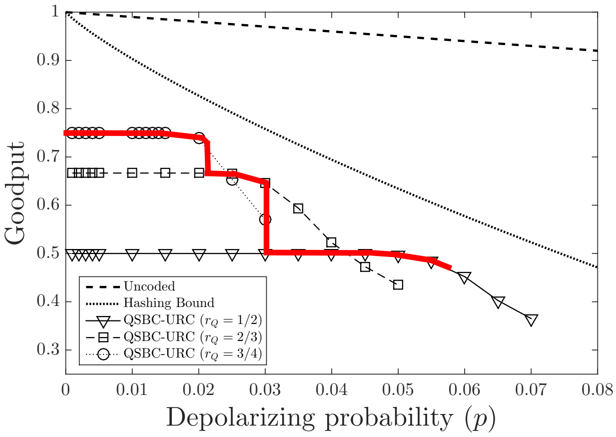
Consequently, based on the goodput results of Fig. 7.12, we can determine the quantum coding rate switching point for our QSBC-QURC scheme in order to adjust the quantum coding rate based on the depolarizing probability experienced. For instance, the switching depolarizing probability for the requirement of QBER $<$ QBER$_{\text{uncoded}}$ is given by $p = \{0.058, 0.030, 0.021\}$ for the three QSBC-QURC schemes considered, which can be seen in Table 7.4. The effective goodput after applying the switching probability is represented by the bold red line in Fig. 7.13(a). We can also infer from Fig. 7.13(a) that for a depolarizing probability of $0.030 \leq p \leq 0.058$ we can utilize the QSBC-QURC having $r_Q = 1/2$ in order to maintain the requirement of QBER $<$ QBER$_{\text{uncoded}}$, while the QSBC-QURC having $r_Q = 2/3$ is invoked for $0.021 \leq p \leq 0.030$, and finally a QSBC-QURC having $r_Q = 3/4$ is invoked for $p < 0.021$.

Similarly, the effective goodput attained upon applying the switching regime specified in Table 7.4 for maintaining QBER $< 10^{-3}$ is portrayed in Fig. 7.13(b). Based on Table 7.4 and Fig. 7.13(b), the QSBC-QURC schemes may be configured for operating at $r_Q = 1/2$ for $0.023 \leq p \leq 0.045$, operating at $r_Q = 2/3$ for $0.016 \leq p \leq 0.023$, operating at $r_Q = 2/3$ for $10^{-3} \leq p \leq 0.016$ and finally, the system may switch to the uncoded mode when the quantum channel reaches the condition of $p < 10^{-3}$.

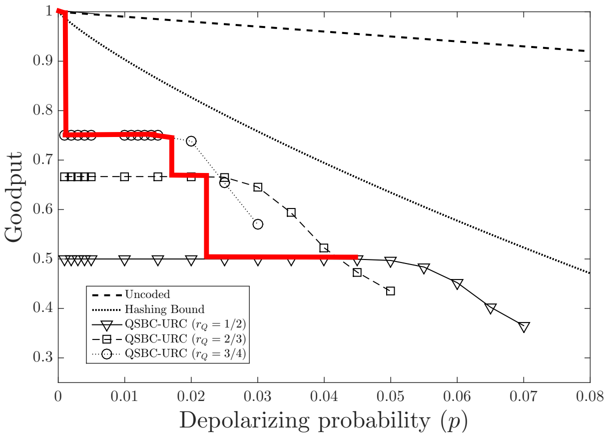
7.5 Conclusions and Future Research

We have conceived a QTC scheme exhibiting multiple quantum coding rates using a single quantum encoder. This construction was created by exploiting the inherent property of our QSBC encoders. We have amalgamated the QSBCs and QURC schemes to transform the error detection capability of QSBCs into an error correction capability without sacrificing the quantum coding rate. We predicted and analyzed the performance of our QSBC-QURC schemes both by EXIT chart analysis and by Monte Carlo simulations. Despite its low complexity, the QSBC-QURC schemes are capable of operating relatively close to the quantum hashing bound at QBER $= 10^{-3}$. Furthermore, we have compared our half-rate QSBC-QURC with the best performing half-rate QTC scheme, namely the QIrCC-QURC of [130]. The QSBC-QURC outperforms the QIrCC-QURC in terms of operating closer to the quantum hashing bound at QBER $= 10^{-3}$, but observe in Fig. 7.10 that the QIrCC-QURC has the edge over the QSBC-QURC for low values of p due to the relatively high error floor of QSBC-QURC, which was indeed expected from its EXIT chart analysis.

We have also extended our discussions to the option of creating a multi-rate scheme for our QSBC-QURC. By using the distance from quantum hashing bound and the goodput, we quantified the normalized performance of our QSBC-QURC scheme by taking into account its quantum coding rate. Furthermore, we have also determined the quantum coding rate switching point based on the depolarizing probability for two specific requirements, QBER $<$ QBER$_{\text{uncoded}}$ and QBER $< 10^{-3}$. Finally, we quantified the goodput achieved by adapting to the quantum depolarizing probability.



(a)



(b)

Figure 7.13: Goodput versus depolarizing probability curves for QSBC-QURC schemes exhibiting various quantum coding rates having $k = 2000$ logical qubits after 16 decoding iterations. The bold red line represents the achievable goodput using our multi-rate scheme given the minimum requirement: (a) QBER $\leq$ QBER$_{\text{uncoded}}$, (b) QBER $= 10^{-3}$.

As an initial study and first instantiation of QTCs exhibiting multiple quantum coding rates in a single quantum encoder, we present several potential research direction as an extension of this result. Firstly, it is indeed possible to have a higher quantum coding rate than $r_Q = 3/4$ as we have demonstrated in this chapter. However, the simulations will become more time consuming, since the simulation time of each block of the quantum encoder is roughly doubled each time we add one more qubit into the block. Our powerful parallel computer is only capable of simulating the QSBC-QURC exhibiting quantum coding rates up to $r_Q = 3/4$. Ultimately, the QSBCs can be combined to create a QSBC-QURC exhibiting an arbitrary quantum coding rate, similar to the QIrCCs. An EXIT-chart-based heuristic search can also be certainly conducted to yield the best combination of the sub-component QSBCs. Consequently, this would result in a very smooth goodput performance curve.

However, one of the requirements for the multi-rate scheme for QSCs to work flawlessly is having perfect channel estimation for predicting the depolarizing probability. Our simulation results are based on the assumption that we have perfect knowledge of the depolarizing probability at the decoder. However, it is worth mentioning that it has been demonstrated in classical settings that classical parallel turbo codes are generally rather insensitive to inaccurate signal-to-noise ratio (SNR) estimation [207, 208, 209]. However, for QTCs, the effect of inaccurate depolarizing probability knowledge on the QBER performance is still unknown. Some investigations towards the inaccuracy problem have been conducted for QLDPC codes in [210, 211]. These results give an early indication that there is no significant QBER performance difference variation between having a perfect and imperfect quantum channel knowledge [212]. Hence, the next step is to find the most appropriate depolarizing probability estimator for QSBCs. A plausible option is using some known pilot qubits or pre-shared entanglement for estimating the depolarizing probability. However, we have to rely on the idealistic assumption that the quantum depolarizing channel is a static channel implying that the value of depolarizing probability of the quantum channel does not vary much over time [213, 214, 215]. An alternative approach is invoking syndrome-based depolarizing probability estimation, which can be derived from the classical realm [212, 216, 217, 218]. The syndrome-based estimator may be deemed to be more efficient because it eliminates the need for pilot qubits or pre-shared entanglement and also the necessity of measuring the quantum information. However, a syndrome-based channel estimator would require a high number of physical qubits work accurately whereas currently, we are working on a QSC scheme having a relatively short block ($k < 2000$). Needless to say, a joint study of the effect of the inaccuracy depolarizing probability on the QBER performance of our QSBC-QURC scheme and the design of online depolarizing probability estimation is a promising subject.

Chapter 8

Summary and Future Research

Throughout this thesis, we have presented the fundamental background on quantum information theory, the challenges in designing QSCs, along with the conflicting parameters involved in QSCs design. By exploiting the classical-to-quantum isomorphism, we can characterize the effects of code parameters on the QBER performance of the QSCs derived from their classical counterparts, including the family QTECCs. Next, we provided the general framework of increasing the reliability of imperfect quantum gates by invoking QSCs and utilized QTECCs as our prime examples. Finally, we introduced the concept of quantum turbo-short block codes as one of the possible solutions for creating multiple-rate near-hashing-bound QSCs. In this concluding chapter, we commence by summarizing our conclusions in Section 8.1, while a range of promising future research directions will be discussed in Section 8.2.

8.1 Summary

The employment of QECCs for mitigating the deleterious effects of quantum decoherence is one of the promising techniques of realizing large-scale high-reliability quantum computers. The proposal of QSCs, which can be viewed as syndrome-based QECCs, has opened up the opportunity of transforming any powerful classical error correction codes into the quantum domain. In the field of classical error correction codes, the main goal is to protect the transmission of classical information over classical channels. However, in the quantum domain, the quantum transmission channel is not the only source of quantum decoherence that may erode the integrity of quantum information. The imperfect quantum gates also may impose additional deleterious effects on quantum information. Against this background, this thesis aimed for

(a) Exploiting the classical-to-quantum isomorphism to characterize the performance of QSCs;

(b) Finding the appropriate mechanism of utilizing QSCs not only for protecting the transmission of fragile quantum information over quantum channels but also for improving the reliability of imperfect quantum gates.

In light of these goals, the results of this thesis can be summarized as follows:

(a) **Chapter 1**. In Section 1.1, we presented the motivation of quantum computation as well as quantum communication and argued that using QECCs is vital for realizing reliable quantum computers. In Section 1.2, we proceeded with a historical perspective on the important milestones in the field of QSCs and QTECCs. The outline of the thesis was presented in Section 1.3 and finally, the contributions of the thesis were listed in Section 1.4.

(b) **Chapter 2**. In this chapter, we provided a rudimentary introduction to quantum information processing. In Section 2.2, we introduced the elementary unit of quantum information, namely quantum bit (qubit). This was followed by Section 2.3, where we described the basics of quantum information processing widely used for manipulating the quantum state of the qubits, which covers the unitary transformations and quantum measurements. In Section 2.4, we elaborated the different quantum channel models used throughout this thesis, while in Section 2.5, we presented one of the challenges imposed on designing QSCs, namely the no-cloning theorem. Finally, in Section 2.6, we portrayed the quantum entanglement as one of the distinct properties inherited by quantum information, which does not have a classical counterpart.

(c) **Chapter 3**. In this chapter, we presented the classical-to-quantum isomorphism and used it for constructing QSCs by highlighting their similarity with classical linear block codes. The general concept of syndrome-based decoding conceived for classical linear block codes was introduced in Section 3.2. By exploiting the classical-to-quantum Pauli mapping in Section 3.3, we demonstrated that any QSC can be treated as a classical linear block code having two separate PCMs. Furthermore in Section 3.4, we described three pioneering contributions on QSCs, namely, the 9-qubit Shor's code, the 7-qubit Steane's code, and the 5-qubit Laflamme's code. The code parameters and the description of the aforementioned codes are given in Table 8.1. In Fig. 3.9, we have demonstrated that the three codes performed similarly in the face of quantum depolarizing channels despite their different code parameters and exhibiting different types of QSCs.

Table 8.1: Code parameters for Shor's, Steane's, and Laflamme's code. All the QSCs presented here are capable of correcting a single-qubit error.

Codes	n	k	d	r_Q	Type
Shor's code	9	1	3	1/9	non-dual-containing CSS
Steane's code	7	1	3	1/7	dual-containing CSS
Laflamme's code	5	1	3	1/5	non-CSS

(d) **Chapter 4**. In this chapter, we discussed the natural trade-off between the conflicting parameters of QSC design, which described with the aid of quantum coding bound formulations. By exploiting the classical to quantum isomorphism in Section 4.2, we have derived the quantum coding bounds from their classical counterparts. More explicitly, we derived the quantum-domain version of Singleton, Hamming, and Gilbert-Varshamov bounds. Next, we conducted a comprehensive survey of quantum coding bounds along with the proposal of a simple closed-form approximation for determining the realistically achievable minimum distance given, a specific the codeword length and quantum coding rate as a promising toolkit for designing the QSCs. Our proposed formula is applicable for both the idealized asymptotical case as detailed in Section 4.3, as well as for practical finite-length codeword length as described in Section 4.4. Finally in Section 4.5, we derived the quantum coding bounds for arbitrarily-entangled QSCs to unify the bounds for entanglement-assisted and the unassisted QSCs.

More explicitly, we constructed Table 8.2 portraying the realistically achievable minimum distance for finite-length QSCs exhibiting various quantum coding rates and numbers of physical qubits based on the approximation formula provided in Section 4.4. Furthermore, provided that we have obtained the realistically achievable minimum distance value, we can directly approximate the QBER performance using the formula in Eq. (4.30). It is pertinent to mention that for a QSC having a very large number of physical qubits ($n \to \infty$), the minimum distance of the QSC is linearly proportional to the number of physical qubits as defined by the constant factor δ. For instance, the δ value obtained is equal to 0.100 for a half-rate QSC at the asymptotical limit, as shown in Table 8.2. Furthermore, we constructed Table 8.3, where we describe the value of normalized minimum distance δ for various EA-QSCs having entanglement ratios of $\theta = \{0.1, 0.25, 0.50, 0.75, 1\}$. Additionally, when θ is equal to 0, we arrive at the relevant approximation for the unassisted QSCs. By contrast, when $\theta = 1$ and $r_Q = 0$, we achieve the ultimate limit of QSCs, where we have $\delta = 0.750$.

Table 8.2: The realistically achievable minimun distance d for QSCs exhibiting various quantum coding rates and various numbers of physical qubits. Additionally, when the number of physical qubits is sufficiently large ($n \to \infty$), the scaling of the minimum distance d is linear with constant factor δ. The values portrayed here were obtained using the approximation presented in Section 4.5 and have been illustrated in Fig. 4.9.

r_Q	$d(n = 32)$	$n = 64$	$n = 128$	$n = 256$	$n = 512$	$n = 1024$	$n \to \infty$
3/4	4	5	9	15	26	47	$\delta = 0.048$
2/3	5	7	11	19	35	67	$\delta = 0.065$
1/2	6	10	17	29	54	99	$\delta = 0.100$
1/3	8	13	22	40	75	139	$\delta = 0.137$
1/4	8	14	25	46	87	163	$\delta = 0.157$
$1/n \approx 0$	10	18	34	66	130	258	$\delta = 0.219$

(e) **Chapter 5**. In this chapter, we extended our parametric study of the minimum distance versus quantum coding rate to QTECCs. In Section 5.2, we commenced by presenting the explicit construction of classical TECCs based on the underlying

Table 8.3: The normalized minimum distance δ for EA-QSCs having a sufficiently large number of physical qubits ($n \to \infty$) for various entanglement ratios θ. The values portrayed here were calculated using the approximation described in Section 4.4 and have been illustrated in Fig. 4.5

r_Q	$\delta(\theta = 0.10)$	$\theta = 0.25$	$\theta = 0.50$	$\theta = 0.75$	$\theta = 1$
3/4	0.053	0.061	0.073	0.087	0.100
2/3	0.072	0.082	0.100	0.118	0.137
1/2	0.111	0.128	0.157	0.187	0.219
1/3	0.153	0.177	0.219	0.265	0.316
1/4	0.175	0.203	0.253	0.310	0.375
$1/n \approx 0$	0.246	0.290	0.374	0.484	**0.750**

lattice structure. We found that the resultant TECCs constitute a class of LDPC codes for long codewords. The properties of the classical TECC-based LDPC codes are summarized in Table 8.4. We can observe that the resultant LDPC codes inherit some beneficial properties, such as low row-weight (ρ) and low column-weight (γ). However, the TECC-based LDPC codes have a moderate advantage, since the growth of the minimum distance is proportional to the square-root of the codeword length. Additionally, we can find numerous short cycles in the Tanner graph representation of the TECC-based LDPC codes.

Table 8.4: The code parameters of TECC-based LDPC codes obtained from Section 5.2.

Parameter	Square	Triangular	Rotated-Square
r	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
d	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$
δ	$\frac{d}{2d^2-2d+1}$	$\frac{4d}{3d^2+1}$	$\frac{1}{d}$
$\rho_{\max}$	4	6	4
$\gamma_{\max}$	2	3	2
Girth	6	4	8

Next in Section 5.3, we extended the code construction of the classical domain to create the associated quantum dual pairs, namely the QTECCs. In contrast to the classical TECCs, the QTECCs suffer from a low quantum coding rate, because in order to create the stabilizer formalism of the QTECCs, we need a pair of classical PCM of the TECCs. Consequently, the quantum coding rate of QTECCs tends to zero, when the number of physical qubits is high. Therefore, we believe that the QTECCs are preferable for short to moderate codeword lenghts. We summarized the properties of QTECCs as QLDPC codes in Table 8.5. Once again, the properties of the QTECCs are practically identical to those of the classical TECCs, except for having low quantum coding rates. In addition, based on the QBER formula of Eq. (5.31), we found the values of the quantum depolarizing probability threshold

Table 8.5: The code parameters of QTECC viewed as QLDPC codes obtained from Section 5.3.

Parameter	Square	Triangular	Rotated-Square
r	≈ 0	≈ 0	≈ 0
d	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$	$\mathcal{O}(\sqrt{n})$
δ	$\frac{d}{2d^2-2d+1}$	$\frac{4d}{3d^2+1}$	$\frac{1}{d}$
ρ_{max}	4	6	4
γ_{max}	2	3	2
Girth	6	4	8

Table 8.6: The upper-bound and the lower bound of the depolarizing probability threshold (p_{th}) values for different QTECCs. The upper-bound values are obtained using Eq. (5.31) in Section 5.4, while the lower-bound values are obtained using Eq. (6.82) in Setion 6.5.2.

Codes	Upper-bound p_{th}	Lower-bound p_{th}
Colour codes	1.83%	10.78%
Rotated-surface codes	1.36%	10.20%
Surface codes	0.63%	10.63%
Toric codes	0.68%	10.85%

(p_{th}) for four different QTECCs, namely the colour, rotated-surface, surface, and toric codes. These p_{th} values ultimately characterize the QBER performance of the QTECCs on asymptotical limit, namely when $n \to \infty$ and $r_Q \approx 0$. However, this QBER formula, unfortunately, does not capture the benefit of the degeneracy property, which is inherent in the QTECCs construction. Nonetheless, the p_{th} values obtained from Eq. (5.31) can be used for estimating the upper-bound, which is the worst-case scenario of the attainable QTECCs performance. The p_{th} value of each type of the QTECC is presented in Table 8.6.

(f) **Chapter 6**. The benefits of QSCs are more far-reaching than simply protecting quantum information from the effects of quantum decoherence imposed by the quantum channel. They are also eminently suitable for improving the reliability of imperfect quantum gates. In this chapter, we presented the general framework of protecting quantum gates by utilizing QSCs. In Section 6.2, we commenced by demonstrating how to transform the formulation of QSCs conceived for correcting quantum bits into the QSCs formulation suitable for improving the reliability of imperfect quantum gates. More specifically, we introduced the notion of effective stabilizer formalism and effective inverse encoder in the context of accommodating imperfect unitary transformations. More specifically, we represented the unitary transformations by the transversal configuration of quantum Clifford gates. In Section 6.3, we provided an elaborate example of the scheme advocated by using 1/3-rate quantum repetition codes for protecting transversal Hadamard gates and transversal CNOT gates. Moving one step further, by exploiting the attractive properties of QTECCs such as the limited number of interactions amongst the qubits and the localized stabilizer measurements, we invoked QTECCs as our prime examples for this scheme in Section 6.5.

Table 8.7: The upper-bound and the lower bound of the depolarizing fidelity threshold (F_{th}) values for Hadamard gates protected by different types of QTECCs. These values are obtained from Section 6.5.2 using Eq. (6.81) and (6.82) for the upper-bound and the lower-bound, respectively.

Codes	Upper-bound F_{th}	Lower-bound F_{th}
Colour codes	99.74%	98.46%
Rotated-surface codes	99.73%	97.96%
Surface codes	97.87%	97.87%
Toric codes	99.86%	97.83%

Table 8.8: The upper-bound and the lower bound of the depolarizing fidelity threshold (F_{th}) values for CNOT gates protected by different types of QTECCs. These values are obtained from Section 6.5.3 using Eq. (6.90) and (6.91) for the upper-bound and the lower-bound, respectively.

Codes	Upper-bound F_{th}	Lower-bound F_{th}
Colour codes	99.48%	96.92%
Rotated-surface codes	99.46%	95.92%
Surface codes	99.74%	95.74%
Toric codes	99.72%	95.66%

The main results of this chapter can be summarized as follows. Firstly, in order to gain a better insight into the true QBER performance of QTECCs, we derived an analytical lower-bound formula for a given number of logical and physical qubits in Eq. (6.82). This lower bound QBER performance of Eq. (6.82) is obtained by using the sphere-packing bound for CSS-type QSCs. When n is very large, this lower bound is equivalent to the quantum hashing limit for CSS-type QSCs. This formula can be used as the lower bound of the QBER performance since, at the time of writing, there are no QSCs that can perform beyond the hashing limit, not even when the degeneracy property can be successfully exploited. Based on Eq. (6.82), we also obtained the lower-bound of the depolarizing probability threshold (p_{th}) values for various QTECCs, which we have summarized in Table 8.6.

Secondly, by assuming that we can provide a perfectly encoded quantum state and that the effects of quantum decoherence imposed on the qubits are uncorrelated, we obtained the minimum fidelity threshold values required by the physical implementation of quantum gates. In other words, we can significantly improve the performance of imperfect quantum Clifford gates, provided that a set of quantum gates exhibiting fidelity values better than F_{th} are available. Otherwise, instead of beneficially improving the reliability of the quantum gates, the QSCs will actually further aggravate the error effects imposed by the imperfection of the quantum gates. The summary of the fidelity threshold F_{th} values obtained for Hadamard and CNOT gates protected by various QTECCs is depicted in Table 8.7 and 8.8, respectively.

(g) **Chapter 7**. We have repeatedly emphasized that QSCs suffer from a low quantum coding rate since they have to recover the qubits in the face of both bit-flip and phase-flip errors. In this chapter, we conceived a low-complexity concatenated QTC design exhibiting a high quantum coding rate. This high quantum coding rate was achieved by combining the quantum-domain version of SBCs as the outer codes and QURCs as the inner codes. In Section 7.2, we commenced by providing the explicit description of QSBCs in terms of the PCM formulations, quantum encoders, stabilizer measurements, as well as their classical simulation. In Section 7.3, we detailed our novel QTC design, which utilizing QSBCs as the outer codes and QURCs as the inner codes referred to as QSBC-QURC scheme. Then in Section 7.4, we presented the simulation results of the proposed QTCs in the face of the quantum depolarizing channels.

Table 8.9: The minimum depolarizing probability (p) values required for QIrCC-QURC and QSBC-QURC for achieving various QBER targets as seen in Fig. 7.10. The number of logical qubits is $k = 2000$.

Target	p QIrCC-QURC	p QSBC-QURC
QBER < $\text{QBER}_{\text{uncoded}}$	0.043	**0.058**
QBER < 10^{-3}	0.037	**0.045**
QBER < 10^{-4}	**0.035**	0.030

Table 8.10: The minimum depolarizing probability (p) values required QSBC-QURC having quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$ for achieving various QBER targets as seen in Fig. 7.11. The number of logical qubits is $k = 2000$.

Target	$r_Q = 1/2$	$r_Q = 2/3$	$r_Q = 3/4$
QBER < $\text{QBER}_{\text{uncoded}}$	0.058	0.030	0.021
QBER < 10^{-3}	0.045	0.023	0.016

Despite its design simplicity, the proposed QTC yields a near-hashing-bound error correction performance. For instance, compared to the best half-rate QTC known in the literature, namely the QIrCC-QURC scheme of [130], which operates at the distance of $D = 0.037$ from the quantum hashing bound, our novel QSBC-QURC scheme can operate at the distance of $D = 0.029$ at the depolarizing probability value of $p = 10^{-3}$. Table 8.9 portrays the partial results we have presented in Chapter 7. We can observe in Fig. 7.10 that our QSBC-QURC scheme has an advantage over QIrCC-QURC of [130] in the range of QBER $> 10^{-4}$. However, as we reduced the target depolarizing probability values, an error floor started to emerge for our QSBC-QURC and the above trend was reversed. Also, it is worth mentioning that this is the first instantiation of QTCs that are capable of adjusting the quantum encoders according to the quantum coding rate required for mitigating the Pauli errors, given the different depolarizing probabilities of the quantum channel. A single reconfigurable quantum encoder of the proposed QSBC-QURC scheme is capable of accommodating a range of quantum coding rates, specifically $r_Q = \frac{k}{k+1}$. The depolarizing probability values at which quantum coding rate switching is recommended for different QBER targets are summarized in Table 8.10.

8.2 Future Research

In this section, we will briefly discuss a range of potential future research directions.

(a) **Conceiving QSCs for protecting a complex quantum circuit.** In this thesis, we have provided the general formalism of protecting quantum gates, which is denoted by unitary transformation U_f, and we exemplified the employment of our protocol by utilizing transversal Hadamard gates and CNOT gates as the unitary transformation U_f. Choosing transversal Hadamard and CNOT gates has the advantages of preserving the stabilizer group $\mathcal{S}$ and simplified construction of effective inverse encoder $\widehat{\mathcal{V}}^\dagger$. As we observe from Fig. 8.1, the effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ is identical to the initial inverse encoder $\widehat{\mathcal{V}}^\dagger$, if we consider protecting the transversal CNOT gates. However, as we try to involve more quantum gates, for instance, by simply concatenating transversal Hadamard gates with the transversal CNOT gates, the advantage of having a preserved effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ no longer exists, as illustrated in Fig. 8.2. Therefore, finding a way of transforming the complex effective inverse encoder into a simpler circuit can be an interesting research direction. Another technique that can be considered is the stabilizer measurement-based quantum encoder and the employment of repeated stabilizer measurements for the inverse encoder, as presented in [180, 188].

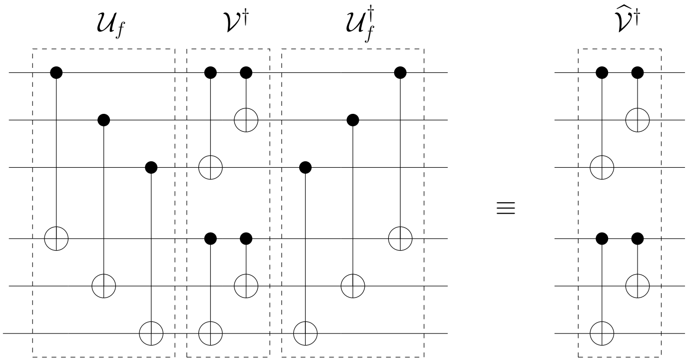


Figure 8.1: Given that the unitary transformation U_f is represented by the transversal CNOT gates, the quantum circuit for inverse encoder $\mathcal{V}^\dagger$ and effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ can be realized identically.

(b) **The irregular version of quantum turbo short-block codes** In Chapter 7, we have utilized QSBCs as the outer codes for our novel QTC scheme. However in Fig. 7.10, we still observe a relatively high error-floor. A possible technique of eliminating this error-floor is that of optimizing the code parameters using EXIT-chart-aided heuristic search [163, 219, 220]. In Fig. 8.3, we have presented a single

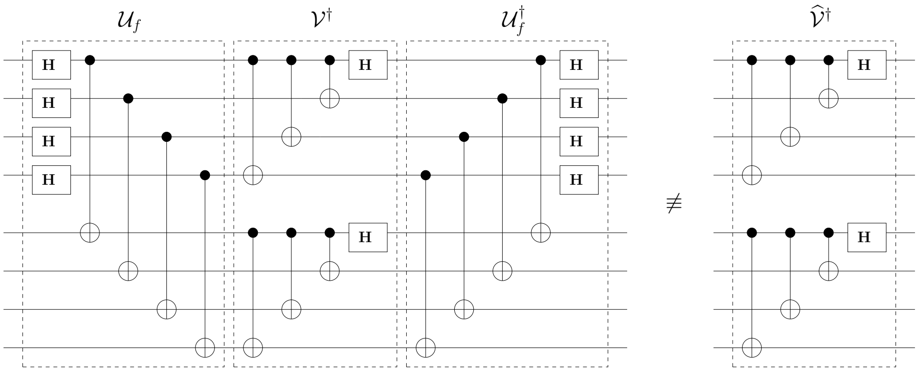


Figure 8.2: For a more comple quantum circuit, the effective inverse encoder $\widehat{\mathcal{V}}^\dagger$ is not always identical with the inverse encoder $\mathcal{V}^\dagger$. In fact, if we follow explicitly the formulation of effective inverse encoder in Eq. (6.17), the resultant effective inverse encoder can be deeemed to be more complex. Finding a way to simplify the circuit is an interesting research avenue to pursue.

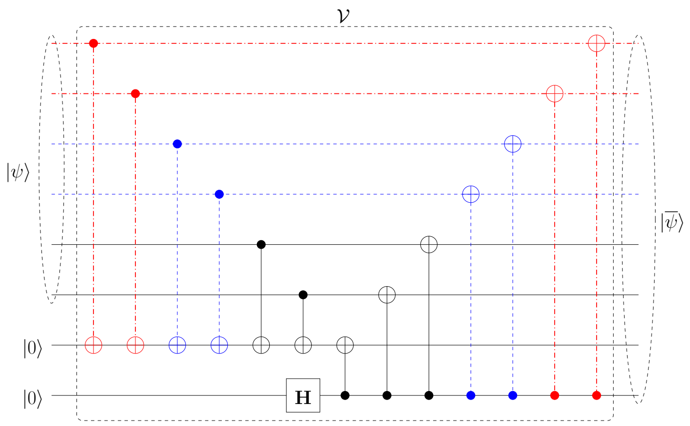


Figure 8.3: Multiple-rate QSBCs encoder. This specific encoder accomodates QSBCs having quantum coding rate of $r_Q = \{1/2, 2/3, 3/4\}$. The half-rate QSBC in this encoder is identical with half-rate QSBC in Fig. 8.4. The seed transformation for each of quantum coding rate is described in Table 8.11.

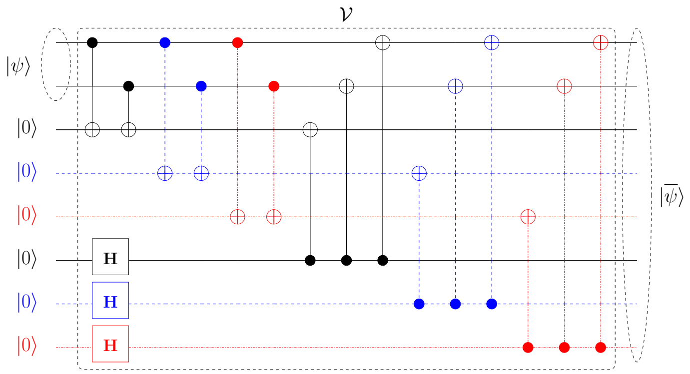


Figure 8.4: Multiple-rate QSBCs encoder. This specific encoder accomodates QSBCs having quantum coding rate of $r_Q = \{1/2, 1/3, 1/4\}$. The half-rate QSBC in this encoder is identical with half-rate QSBC in Fig. 8.3. The seed transformation for each of quantum coding rate is described in Table 8.11.

quantum encoder $\mathcal{V}$ that is capable of accommodating multiple quantum coding rates. Specifically, this quantum encoder $\mathcal{V}$ can be used as a quantum encoder for QSBCs

Table 8.11: The seed transformation $\mathcal{U}$ associated with various QSBCs quantum coding rates r_Q.

r_Q	Seed transformation $\mathcal{U}$
1/4	$\{34560, 18176, 58368, 53760, 51456, 228, 210, 201, 184, 120, 32, 16, 8, 1024, 512, 256\}_{10}$
1/3	$\{2240, 1216, 3712, 3392, 58, 53, 44, 28, 8, 4, 128, 64\}_{10}$
1/2	$\{144, 80, 240, 15, 10, 6, 2, 16\}_{10}$
2/3	$\{2112, 1088, 576, 320, 4032, 63, 34, 18, 10, 6, 2, 64\}_{10}$
3/4	$\{33024, 16640, 8448, 4352, 2304, 1280, 65280, 255, 130, 66, 34, 18, 10, 6, 2, 256\}_{10}$

having quantum coding rates of $r_Q = \{1/2, 2/3, 3/4\}$, which are relatively high quantum coding rates. Interestingly, we can also create a version of $\mathcal{V}$, which is capable of providing multiple encoders for QSBCs in the lower quantum coding rate region, as illustrated in Fig. 8.4. This specific quantum encoder is capable of supporting quantum coding rates of $r_Q = \{1/2, 1/3, 1.4\}$. Observe that the half-rate QSBCs of Fig. 8.3 and 8.4 are identical. An EXIT-chart-based search can be invoked for finding the optimized QTC, provided that the component codes are multiple-rate QSBCs. Based on Fig. 8.3 and 8.4, the seed transformations of the component codes can be seen in Table 8.11. Additionally, we can invoke QSBCs as the inner code of a QTC to have a QTC structure purely constructed from QSBCs. However, the main drawback with QSBCs used as the inner codes is that they exhibit a non-recursive and non-catastrophic structure. Consequently, the inner EXIT curve will not reach the $(1, 1)$ point. This means that we potentially have to exploit entanglement-assisted QSBCs as the inner code to achieve full-convergence for iterative decoding.

Bibliography

[1] D. Chandra, Z. Babar, H. V. Nguyen, D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum coding bounds and a closed-form approximation of the minimum distance versus quantum coding rate," *IEEE Access*, vol. 5, pp. 11 557–11 581, 2017.

[2] ——, "Quantum topological error correction codes: The classical-to-quantum isomorphism perspective," *IEEE Access*, vol. 6, pp. 13 729–13 757, 2018.

[3] ——, "Quantum topological error correction codes are capable of improving the performance of Clifford gates," *IEEE Access*, 2019.

[4] D. Chandra, Z. Babar, S. X. Ng, and L. Hanzo, "Near-hashing-bound multiple-rate quantum turbo short-block codes," *IEEE Access*, vol. 7, pp. 52 712–52 730, 2019.

[5] E. Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik," *Naturwissenschaften*, vol. 23, no. 49, pp. 823–828, 1935.

[6] J. D. Trimmer, "The present situation in quantum mechanics: A translation of Schrödinger's "Cat Paradox" paper," *Proceedings of the American Philosophical Society*, vol. 124, no. 5, pp. 323–338, 1980.

[7] "Moore's Law - The Number of transistors on integrated circuit chips (1971-2018)," https://ourworldindata.org/technological-progress, accessed: 2019-08-21.

[8] G. E. Moore, "Cramming more components onto integrated circuits," *Electronics Magazine*, pp. 114–117, 1965.

[9] M. M. Waldrop, "The chips are down for Moore's law," *Nature News*, vol. 530, pp. 144–147, 2016.

[10] L. Hanzo, H. Haas, S. Imre, D. O'Brien, M. Rupp, and L. Gyongyosi, "Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless," *Proceedings of the IEEE (Special Centennial Issue)*, vol. 100, pp. 1853–1888, 2012.

[11] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, 1982.

[12] D. E. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 400, no. 1818, pp. 97–117, 1985.

[13] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of 35th Annual Symposium on Foundations of Computer Science (FOCS)*, 1994, pp. 124–134.

[14] ——, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[15] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[16] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *arXiv preprint quant-ph/9605034*, 1996.

[17] C. Durr and P. Høyer, "A quantum algorithm for finding the minimum," *arXiv preprint quant-ph/9607014*, 1996.

[18] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Physical Review Letters*, vol. 79, no. 2, 1997.

[19] C. Zalka, "Grovers quantum searching algorithm is optimal," *Physical Review A*, vol. 60, no. 4, 1999.

[20] G. Brassard, F. Dupuis, S. Gambs, and A. Tapp, "An optimal quantum algorithm to approximate the mean and its application for approximating the median of a set of points over an arbitrary distance," *arXiv preprint arXiv:1106.4267*, 2011.

[21] P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum search algorithms, quantum wireless, and a low-complexity maximum likelihood iterative quantum multi-user detector design," *IEEE Access*, vol. 1, pp. 94–122, 2013.

[22] ——, "Fixed-complexity quantum-assisted multi-user detection for CDMA and SDMA," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 990–1000, 2014.

[23] P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Low-complexity soft-output quantum-assisted multiuser detection for direct-sequence spreading and slow subcarrier-hopping aided SDMA-OFDM systems," *IEEE Access*, vol. 2, pp. 451–472, 2014.

[24] D. Alanis, P. Botsinis, S. X. Ng, and L. Hanzo, "Quantum-assisted routing optimization for self-organizing networks," *IEEE Access*, vol. 2, pp. 614–632, 2014.

[25] P. Botsinis, D. Alanis, Z. Babar, S. X. Ng, and L. Hanzo, "Noncoherent quantum multiple symbol differential detection for wireless systems," *IEEE Access*, vol. 3, pp. 569–598, 2015.

[26] ——, “Iterative quantum-assisted multi-user detection for multi-carrier interleave division multiple access systems,” *IEEE Transactions on Communications*, vol. 63, no. 10, pp. 3713–3727, 2015.

[27] D. Alanis, P. Botsinis, Z. Babar, S. X. Ng, and L. Hanzo, “Non-dominated quantum iterative routing optimization for wireless multihop networks,” *IEEE Access*, vol. 3, pp. 1704–1728, 2015.

[28] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, “Quantum search algorithms for wireless communications,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2018.

[29] C. H. Bennett, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings on IEEE International Conference on Computer System and Signal Processing*, 1984, pp. 175–179.

[30] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, 1991.

[31] C. H. Bennett and S. J. Wiesner, “Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states,” *Physical Review Letters*, vol. 69, no. 20, 1992.

[32] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, 1993.

[33] F.-G. Deng, G. L. Long, and X.-S. Liu, “Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block,” *Physical Review A*, vol. 68, no. 4, 2003.

[34] F.-G. Deng and G. L. Long, “Secure direct communication with a quantum one-time pad,” *Physical Review A*, vol. 69, no. 5, 2004.

[35] N. L. Piparo and M. Razavi, “Long-distance trust-free quantum key distribution,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 123–130, 2014.

[36] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, “Memory-assisted measurement-device-independent quantum key distribution,” *New Journal of Physics*, vol. 16, no. 4, 2014.

[37] M. Razavi, “Multiple-access quantum key distribution networks,” *IEEE Transactions on communications*, vol. 60, no. 10, pp. 3071–3079, 2012.

[38] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, “When entanglement meets classical communications: Quantum teleportation for the quantum internet,” *arXiv preprint arXiv:1907.06197*, 2019.

[39] G. De Lange, Z. Wang, D. Riste, V. Dobrovitski, and R. Hanson, “Universal dynamical decoupling of a single solid-state spin from a spin bath,” *Science*, vol. 330, no. 6000, pp. 60–63, 2010.

[40] T. Van der Sar, Z. Wang, M. Blok, H. Bernien, T. Taminiau, D. Toyli, D. A. Lidar, D. Awschalom, R. Hanson, and V. Dobrovitski, “Decoherence-protected quantum gates for a hybrid solid-state spin register,” *Nature*, vol. 484, no. 7392, pp. 82–86, 2012.

[41] J. L. O’Brien, G. Pryde, A. Gilchrist, D. James, N. Langford, T. Ralph, and A. White, “Quantum process tomography of a controlled-NOT gate,” *Physical Review Letters*, vol. 93, no. 8, 2004.

[42] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, and J. L. O’Brien, “Silica-on-silicon waveguide quantum circuits,” *Science*, vol. 320, no. 5876, pp. 646–649, 2008.

[43] A. Politi, J. C. Matthews, and J. L. O’brien, “Shors quantum factoring algorithm on a photonic chip,” *Science*, vol. 325, no. 5945, pp. 1221–1221, 2009.

[44] L. DiCarlo, J. M. Chow, J. M. Gambetta, L. Bishop, B. Johnson, D. Schuster, J. Majer, A. Blais, L. Frunzio, S. Girvin *et al.*, “Demonstration of two-qubit algorithms with a superconducting quantum processor,” *Nature*, vol. 460, no. 7252, p. 240, 2009.

[45] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O’Brien, “Experimental realization of Shor’s quantum factoring algorithm using qubit recycling,” *Nature Photonics*, vol. 6, no. 11, pp. 773–776, 2012.

[46] J. M. Chow, J. M. Gambetta, A. Córcoles, S. T. Merkel, J. A. Smolin, C. Rigetti, S. Poletto, G. A. Keefe, M. B. Rothwell, J. Rozen *et al.*, “Universal quantum gate set approaching fault-tolerant thresholds with superconducting qubits,” *Physical Review Letters*, vol. 109, no. 6, 2012.

[47] M. Veldhorst, J. Hwang, C. Yang, A. Leenstra, B. De Ronde, J. Dehollain, J. Muhonen, F. Hudson, K. M. Itoh, A. Morello *et al.*, “An addressable quantum dot qubit with fault-tolerant control-fidelity,” *Nature Nanotechnology*, vol. 9, no. 12, pp. 981–985, 2014.

[48] M. Veldhorst, C. Yang, J. Hwang, W. Huang, J. Dehollain, J. Muhonen, S. Simmons, A. Laucht, F. Hudson, K. M. Itoh *et al.*, “A two-qubit logic gate in silicon,” *Nature*, vol. 526, no. 7573, pp. 410–414, 2015.

[49] S. Weidt, J. Randall, S. Webster, K. Lake, A. Webb, I. Cohen, T. Navickas, B. Lekitsch, A. Retzker, and W. K. Hensinger, “Trapped-ion quantum logic with global radiation fields,” *Physical review letters*, vol. 117, no. 22, 2016.

[50] B. Lekitsch, S. Weidt, A. G. Fowler, K. Mølmer, S. J. Devitt, C. Wunderlich, and W. K. Hensinger, “Blueprint for a microwave trapped ion quantum computer,” *Science Advances*, vol. 3, no. 2, 2017.

[51] D. P. DiVincenzo, “The physical implementation of quantum computation,” *Fortschritte der Physik*, vol. 48, no. 9-11, pp. 771–783, 2000.

[52] P. A. Dirac, “A new notation for quantum mechanics,” *Proceedings of the Cambridge Philosophical Society*, vol. 35, pp. 416–418, 1939.

[53] S. Aaronson and D. Gottesman, “Improved simulation of stabilizer circuits,” *Physical Review A*, vol. 70, no. 5, 2004.

[54] J. Preskill, “Reliable quantum computers,” *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 385–410, 1998.

[55] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[56] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, vol. 52, no. 4, 1995.

[57] A. M. Steane, “Error correcting codes in quantum theory,” *Physical Review Letters*, vol. 77, no. 5, 1996.

[58] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, “Perfect quantum error correcting code,” *Physical Review Letters*, vol. 77, no. 1, 1996.

[59] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound,” *Physical Review A*, vol. 54, no. 3, 1996.

[60] A. K. Ekert and C. Macchiavello, “Quantum error correction for communication,” *Physical Review Letters*, vol. 77, no. 12, 1996.

[61] D. Gottesman, “Stabilizer codes and quantum error correction,” Ph.D. dissertation, California Institute of Technology, 1997.

[62] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction via codes over GF(4),” *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[63] M. Grassl and T. Beth, “Quantum BCH codes,” in *Proceedings of International Symposium Theoretical Electrical Engineering*, 1999, pp. 207–212.

[64] M. Grassl, W. Geiselmann, and T. Beth, “Quantum Reed-Solomon codes,” in *Applied Algebra, Algebraic Algorithms and Error-correcting Codes.* Springer Berlin Heidelberg, 1999, pp. 231–244.

[65] A. M. Steane, “Quantum Reed-Muller codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1701–1703, 1999.

[66] G. Bowen, “Entanglement required in achieving entanglement-assisted channel capacities,” *Physical Review A*, vol. 66, no. 5, 2002.

[67] T. A. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, 2006.

[68] H. Ollivier and J.-P. Tillich, "Description of a quantum convolutional code," *Physical Review Letters*, vol. 91, no. 17, 2003.

[69] M. M. Wilde and T. A. Brun, "Entanglement-assisted quantum convolutional coding," *Physical Review A*, vol. 81, no. 4, 2010.

[70] M. S. Postol, "A proposed quantum low density parity check code," *arXiv preprint quant-ph/0108131*, 2001.

[71] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.

[72] T. Camara, H. Ollivier, and J.-P. Tillich, "Constructions and performance of classes of quantum LDPC codes," *arXiv preprint quant-ph/0502086*, 2005.

[73] ——, "A class of quantum LDPC codes: Construction and performances under iterative decoding," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 811–815.

[74] M.-H. Hsieh, T. A. Brun, and I. Devetak, "Entanglement-assisted quantum quasicyclic low-density parity-check codes," *Physical Review A*, vol. 79, no. 3, 2009.

[75] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Fifteen years of quantum LDPC coding and improved decoding strategies," *Access, IEEE*, vol. 3, pp. 2492–2519, 2015.

[76] D. Poulin, J.-P. Tillich, and H. Ollivier, "Quantum serial turbo codes," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2776–2798, 2009.

[77] M. M. Wilde and M.-H. Hsieh, "Entanglement boosts quantum turbo codes," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2011, pp. 445–449.

[78] M. M. Wilde, M.-H. Hsieh, and Z. Babar, "Entanglement-assisted quantum turbo codes," *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1203–1222, 2014.

[79] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "The road from classical to quantum codes: A hashing bound approaching design procedure," *IEEE Access*, vol. 3, pp. 146–176, 2015.

[80] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Physical Review Letters*, vol. 109, no. 5, 2012.

[81] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2012, pp. 334–338.

[82] M. Grassl, T. Beth, and T. Pellizzari, “Codes for the quantum erasure channel,” *Physical Review A*, vol. 56, no. 1, 1997.

[83] H. F. Chau, “Quantum convolutional error-correcting codes,” *Physical Review A*, vol. 58, no. 2, 1998.

[84] D. A. Lidar and K. B. Whaley, “Decoherence-free subspaces and subsystems,” in *Irreversible Quantum Dynamics.* Springer, 2003, pp. 83–120.

[85] A. Shabani and D. A. Lidar, “Theory of initialization-free decoherence-free subspaces and subsystems,” *Physical Review A*, vol. 72, no. 4, 2005.

[86] D. A. Lidar and T. A. Brun, *Quantum Error Correction.* Cambridge University Press, 2013.

[87] E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” *Physical Review A*, vol. 55, no. 2, 1997.

[88] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Physical Review A*, vol. 54, no. 2, 1996.

[89] D. Gottesman, “Theory of fault-tolerant quantum computation,” *Physical Review A*, vol. 57, no. 1, 1998.

[90] E. Knill, R. Laflamme, and W. H. Zurek, “Resilient quantum computation,” *Science*, vol. 279, no. 5349, pp. 342–345, 1998.

[91] ——, “Resilient quantum computation: Error models and thresholds,” *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 454, no. 1969, pp. 365–384, 1998.

[92] D. Gottesman, “Fault-tolerant quantum computation with constant overhead,” *Quantum Information & Computation*, vol. 14, no. 15-16, pp. 1338–1372, 2014.

[93] J. Akhtman, R. Maunder, N. Bonello, and L. Hanzo, “Closed-form approximation of maximum free distance for binary block codes,” in *Proceedings of IEEE 70th Vehicular Technology Conference Fall (VTC-Fall)*, 2009, pp. 1–3.

[94] A. M. Steane, “Multiple-particle interference and quantum error correction,” *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[95] P. W. Shor, “Fault-tolerant quantum computation,” in *Proceedings of 37th Annual Symposium on Foundations of Computer Science (FOCS)*, 1996, pp. 56–65.

[96] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, “Quantum error correction and orthogonal geometry,” *Physical Review Letters*, vol. 78, no. 3, 1997.

[97] “IBM Quantum Experience,” https://www.research.ibm.com/ibm-q, accessed: 2017-10-01.

[98] A. Y. Kitaev, “Quantum computations: Algorithms and error correction,” *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997.

[99] ——, “Fault-tolerant quantum computation by anyons,” *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003.

[100] M. H. Freedman, D. A. Meyer, and F. Luo, “Z2-systolic freedom and quantum codes,” *Mathematics of Quantum Computation*, pp. 287–320, 2002.

[101] S. Bravyi and A. Y. Kitaev, “Quantum codes on a lattice with boundary,” *arXiv preprint quant-ph/9811052*, 1998.

[102] C. Horsman, A. G. Fowler, S. J. Devitt, and R. Van Meter, “Surface code quantum computing by lattice surgery,” *New Journal of Physics*, vol. 14, no. 12, 2012.

[103] H. Bombin and M. A. Martin-Delgado, “Topological quantum distillation,” *Physical Review Letters*, vol. 97, no. 18, 2006.

[104] J. Haah, “Local stabilizer codes in three dimensions without string logical operators,” *Physical Review A*, vol. 83, no. 4, 2011.

[105] G. Zémor, “On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction,” in *Coding and Cryptology.* Springer, 2009, pp. 259–273.

[106] A. Couvreur, N. Delfosse, and G. Zemor, “A construction of quantum LDPC codes from Cayley graphs,” *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 6087–6098, 2013.

[107] N. Delfosse, “Tradeoffs for reliable quantum information storage in surface codes and color codes,” in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 917–921.

[108] J.-P. Tillich and G. Zémor, “Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength,” in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2009, pp. 799–803.

[109] A. A. Kovalev and L. P. Pryadko, “Improved quantum hypergraph-product LDPC codes,” in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2012, pp. 348–352.

[110] J.-P. Tillich and G. Zémor, “Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength,” *IEEE Transactions on Information Theory*, vol. 60, no. 2, pp. 1193–1202, 2014.

[111] S. Bravyi and M. B. Hastings, “Homological product codes,” in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, 2014, pp. 273–282.

[112] S. Bravyi and J. Haah, “Quantum self-correction in the 3D cubic code model,” *Physical Review Letters*, vol. 111, no. 20, 2013.

[113] L. Guth and A. Lubotzky, “Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds,” *Journal of Mathematical Physics*, vol. 55, no. 8, 2014.

[114] H. Bombín, “Dimensional jump in quantum error correction,” *New Journal of Physics*, vol. 18, no. 4, 2016.

[115] W. Zeng and L. P. Pryadko, “Higher-dimensional quantum hypergraph-product codes with finite rates,” *Physical Review Letters*, vol. 122, no. 23, 2019.

[116] C. Ballance, T. Harty, N. Linke, M. Sepiol, and D. Lucas, “High-fidelity quantum logic gates using trapped-ion hyperfine qubits,” *Physical review letters*, vol. 117, no. 6, 2016.

[117] H. V. Nguyen, Z. Babar, D. Alanis, P. Botsinis, D. Chandra, S. X. Ng, and L. Hanzo, “EXIT-chart aided quantum code design improves the normalised throughput of realistic quantum devices,” *IEEE Access*, vol. 4, pp. 10 194–10 209, 2016.

[118] S. Bravyi and A. Y. Kitaev, “Universal quantum computation with ideal Clifford gates and noisy ancillas,” *Physical Review A*, vol. 71, no. 2, 2005.

[119] D. Aharonov and M. Ben-Or, “Fault-tolerant quantum computation with constant error rate,” *SIAM Journal on Computing*, vol. 38, no. 4, pp. 1207–1282, 2008.

[120] H. Bombín, “Single-shot fault-tolerant quantum error correction,” *Physical Review X*, vol. 5, no. 3, 2015.

[121] O. Fawzi, A. Grospellier, and A. Leverrier, “Constant overhead quantum fault-tolerance with quantum expander codes,” in *Proceedings of 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, 2018, pp. 743–754.

[122] E. Campbell, “A theory of single-shot error correction for adversarial noise,” *Quantum Science and Technology*, vol. 4, no. 2, 2019.

[123] T. Jochym-O’Connor, “Fault-tolerant gates via homological product codes,” *Quantum*, vol. 3, 2019.

[124] S. Bravyi and B. Terhal, “A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes,” *New Journal of Physics*, vol. 11, no. 4, 2009.

[125] S. Bravyi, D. Poulin, and B. Terhal, “Tradeoffs for reliable quantum information storage in 2D systems,” *Physical Review Letters*, vol. 104, no. 5, 2010.

[126] Y. Fujiwara, “Ability of stabilizer quantum error correction to protect itself from its own imperfection,” *Physical Review A*, vol. 90, no. 6, 2014.

[127] A. Ashikhmin, C.-Y. Lai, and T. A. Brun, “Robust quantum error syndrome extraction by classical coding,” in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2014, pp. 546–550.

[128] ——, "Correction of data and syndrome errors by stabilizer codes," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 2274–2278.

[129] W. Zeng, A. Ashikhmin, M. Woolls, and L. P. Pryadko, "Quantum convolutional data-syndrome codes," *arXiv preprint arXiv:1902.07395*, 2019.

[130] Z. Babar, H. V. Nguyen, P. Botsinis, D. Alanis, D. Chandra, S. X. Ng, and L. Hanzo, "Serially concatenated unity-rate codes improve quantum codes without coding-rate reduction," *IEEE Communications Letters*, vol. 20, no. 10, pp. 1916–1919, 2016.

[131] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[132] D. Gottesman, "The Heisenberg representation of quantum computers," *arXiv preprint quant-ph/9807006*, 1998.

[133] T. Toffoli, "Reversible computing," in *International Colloquium on Automata, Languages, and Programming.* Springer, 1980, pp. 632–644.

[134] P. Botsinis, Z. Babar, D. Alanis, D. Chandra, H. V. Nguyen, S. X. Ng, and L. Hanzo, "Quantum error correction protects quantum search algorithms against decoherence," *Scientific Reports*, vol. 6, 2016.

[135] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, 1995.

[136] U. Fano, "Description of states in quantum mechanics by density matrix and operator techniques," *Reviews of Modern Physics*, vol. 29, no. 1, 1957.

[137] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, "Quantum tomography," *Advances in Imaging and Electron Physics*, vol. 128, pp. 206–309, 2003.

[138] J. Roffe, "Quantum error correction: An introductory guide," *arXiv preprint arXiv:1907.11157*, 2019.

[139] A. Ashikhmin, "Remarks on bounds for quantum codes," *arXiv preprint quant-ph/9705037*, 1997.

[140] P. K. Sarvepalli and A. Klappenecker, "Degenerate quantum codes and the quantum Hamming bound," *Physical Review A*, vol. 81, no. 3, 2010.

[141] Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 970–1010, 2018.

[142] F. Schmidt-Kaler, S. Gulde, M. Riebe, T. Deuschle, A. Kreuter, G. Lancaster, C. Becher, J. Eschner, H. Häffner, and R. Blatt, "The coherence of qubits based on single Ca+ ions," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 36, no. 3, p. 623, 2003.

[143] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," *Nature*, vol. 414, no. 6866, pp. 883–887, 2001.

[144] A. Tyryshkin, J. Morton, S. Benjamin, A. Ardavan, G. Briggs, J. Ager, and S. Lyon, "Coherence of spin qubits in silicon," *Journal of Physics: Condensed Matter*, vol. 18, no. 21, p. S783, 2006.

[145] J. Petta, A. C. Johnson, J. Taylor, E. Laird, A. Yacoby, M. D. Lukin, C. Marcus, M. Hanson, and A. Gossard, "Coherent manipulation of coupled electron spins in semiconductor quantum dots," *Science*, vol. 309, no. 5744, pp. 2180–2184, 2005.

[146] P. Bertet, I. Chiorescu, G. Burkard, K. Semba, C. Harmans, D. P. DiVincenzo, and J. Mooij, "Dephasing of a superconducting qubit induced by photon noise," *Physical Review Letters*, vol. 95, no. 25, 2005.

[147] L. Ioffe and M. Mézard, "Asymmetric quantum error-correcting codes," *Physical Review A*, vol. 75, no. 3, 2007.

[148] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Physical Review A*, vol. 56, no. 1, 1997.

[149] I. Djordjevic, *Quantum Information Processing and Quantum Error Correction: An Engineering Approach.* Academic press, 2012.

[150] R. C. Singleton, "Maximum distance Q-nary codes," *IEEE Transactions on Information Theory*, vol. 10, no. 2, pp. 116–118, 1964.

[151] R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, 1950.

[152] E. N. Gilbert, "A comparison of signalling alphabets," *Bell System Technical Journal*, vol. 31, no. 3, pp. 504–522, 1952.

[153] R. J. McEliece, E. R. Rodemich, H. Rumsey Jr, and L. R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Transactions on Information Theory*, vol. 23, no. 2, pp. 157–166, 1977.

[154] M. Plotkin, "Binary codes with specified minimum distance," *IRE Transactions on Information Theory*, vol. 6, no. 4, pp. 445–450, 1960.

[155] E. M. Rains, "Quantum shadow enumerators," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2361–2366, 1999.

[156] A. Ashikhmin and S. Litsyu, "Upper bounds on the size of quantum codes," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1206–1215, 1999.

[157] C.-Y. Lai and C.-C. Lu, "A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 7163–7179, 2011.

[158] Y. Xie, J. Yuan *et al.*, "Design of quantum stabilizer codes from quadratic residues sets," *arXiv preprint arXiv:1407.8249*, 2014.

[159] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," Online available at http://www.codetables.de, 2007, accessed on 2016-05-14.

[160] C.-Y. Lai, "Linear programming bounds for entanglement-assisted quantum error-correcting codes by split weight enumerators," *arXiv preprint arXiv:1602.00413*, 2016.

[161] L. Guo and R. Li, "Linear Plotkin bound for entanglement-assisted quantum codes," *Physical Review A*, vol. 87, no. 3, 2013.

[162] C.-Y. Lai, T. A. Brun, and M. M. Wilde, "Dualities and identities for entanglement-assisted quantum codes," *Quantum Information P rocessing*, vol. 13, no. 4, pp. 957–990, 2014.

[163] L. Hanzo, T. Liew, B. Yeap, R. Tee, and S. X. Ng, *Turbo coding, turbo equalisation and space-time coding: EXIT-chart-aided near-capacity designs for wireless channels.* IEEE Press-John Wiley, 2011.

[164] H. Bombin and M. A. Martin-Delgado, "Homological error correction: Classical and quantum codes," *Journal of Mathematical Physics*, vol. 48, no. 5, 2007.

[165] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.

[166] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, "Factor graphs and the sum-product algorithm," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 498–519, 2001.

[167] R. Steele and L. Hanzo, *Mobile Radio Communications: Second and Third Generation Cellular and WATM Systems.* IEEE Press-John Wiley, 1999.

[168] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, 1996.

[169] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[170] B. Schumacher, "Quantum coding," *Physical Review A*, vol. 51, no. 4, 1995.

[171] J. Von Neumann, "Probabilistic logics and the synthesis of reliable organisms from unreliable components," *Automata Studies*, vol. 34, pp. 43–98, 1956.

[172] A. M. Steane, "Space, time, parallelism and noise requirements for reliable quantum computing," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 443–457, 1998.

[173] D. E. Deutsch, "Quantum computational networks," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 425, no. 1868, pp. 73–90, 1989.

[174] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," *Physical Review A*, vol. 68, no. 2, 2003.

[175] G. Grössing and A. Zeilinger, "Quantum cellular automata," *Complex Systems*, vol. 2, no. 2, pp. 197–208, 1988.

[176] M. H. Freedman, A. Y. Kitaev, M. Larsen, and Z. Wang, "Topological quantum computation," *Bulletin of the American Mathematical Society*, vol. 40, no. 1, pp. 31–38, 2003.

[177] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," *arXiv preprint quant-ph/0001106*, 2000.

[178] M. Grassl, "Variations on encoding circuits for stabilizer quantum codes," in *Proceedings of International Conference on Coding and Cryptology.* Springer, 2011, pp. 142–158.

[179] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, 2013.

[180] J. Łodyga, P. Mazurek, A. Grudka, and M. Horodecki, "Simple scheme for encoding and decoding a qubit in unknown state for various topological codes," *Scientific Reports*, vol. 5, 2015.

[181] A. M. Steane, "Overhead and noise threshold of fault-tolerant quantum error correction," *Physical Review A*, vol. 68, no. 4, 2003.

[182] H. Bombin and M. A. Martin-Delgado, "Quantum measurements and gates by code deformation," *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 9, 2009.

[183] H. Bombin, "Clifford gates by code deformation," *New Journal of Physics*, vol. 13, no. 4, 2011.

[184] J. T. Anderson, G. Duclos-Cianci, and D. Poulin, "Fault-tolerant conversion between the Steane and Reed-Muller quantum codes," *Physical review letters*, vol. 113, no. 8, 2014.

[185] C. Vuillot, L. Lao, B. Criger, C. G. Almudever, K. Bertels, and B. Terhal, "Code deformation and lattice surgery are gauge fixing," *New Journal of Physics*, vol. 21, no. 3, 2019.

[186] A. G. Fowler, A. M. Stephens, and P. Groszkowski, "High-threshold universal quantum computation on the surface code," *Physical Review A*, vol. 80, no. 5, 2009.

[187] D. S. Wang, A. G. Fowler, and L. C. Hollenberg, "Surface code quantum computing with error rates over 1%," *Physical Review A*, vol. 83, no. 2, 2011.

[188] A. G. Fowler, M. Mariantoni, J. M. Martinis, and A. N. Cleland, "Surface codes: Towards practical large-scale quantum computation," *Physical Review A*, vol. 86, no. 3, 2012.

[189] T. A. Brun, Y.-C. Zheng, K.-C. Hsu, J. Job, and C.-Y. Lai, "Teleportation-based fault-tolerant quantum computation in multi-qubit large block codes," *arXiv preprint arXiv:1504.03913*, 2015.

[190] A. J. Landahl, J. T. Anderson, and P. R. Rice, "Fault-tolerant quantum computing with color codes," *arXiv preprint arXiv:1108.5738*, 2011.

[191] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes.* Elsevier, 1977.

[192] J. I. Hall, *Notes on coding theory.* FreeTechBooks, 2003.

[193] M. Abbara and J.-P. Tillich, "Quantum turbo codes with unbounded minimum distance and excellent error-reducing performance," in *Proceedings of IEEE Information Theory Workshop (ITW)*, 2011, pp. 252–256.

[194] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "Serial concatenation of interleaved codes: Performance analysis, design, and iterative decoding," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 909–926, 1998.

[195] I. Land, "Reliability information in channel decoding," Ph.D. dissertation, Christian-Albrechts-University of Kiel, 2005.

[196] L. Hanzo and Nasruminallah, "Short block codes for guaranteed convergence in soft-bit assisted iterative joint source and channel decoding," *Electronics Letters*, vol. 44, no. 22, pp. 1315–1316, 2008.

[197] ——, "EXIT-chart optimized short block codes for iterative joint source and channel decoding in H. 264 video telephony," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4306–4315, 2009.

[198] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Transactions on Communications*, vol. 36, no. 4, pp. 389–400, 1988.

[199] Z. Babar, S. X. Ng, and L. Hanzo, "EXIT-chart-aided near-capacity quantum turbo code design," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 3, pp. 866–875, 2015.

[200] M. El-Hajjar and L. Hanzo, "EXIT charts for system design and analysis," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 127–153, 2014.

[201] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: constructions, bounds and performance," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 465, no. 2105, pp. 1645–1672, 2009.

[202] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: Characterization and constructions," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2938–2945, 2010.

[203] S. Ten Brink, “Convergence behavior of iteratively decoded parallel concatenated codes,” *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 1727–1737, 2001.

[204] J. Kliewer, S. X. Ng, and L. Hanzo, “Efficient computation of EXIT functions for non-binary iterative decoding,” *IEEE Transactions on Communications*, vol. 54, no. 12, pp. 2133–2136, 2006.

[205] M. Houshmand and M. M. Wilde, “Recursive quantum convolutional encoders are catastrophic: A simple proof,” *IEEE Transactions on Information Theory*, vol. 59, no. 10, pp. 6724–6731, 2013.

[206] A. Banerjee, F. Vatta, B. Scanavino, and D. J. Costello, “Nonsystematic turbo codes,” *IEEE Transactions on Communications*, vol. 53, no. 11, pp. 1841–1849, 2005.

[207] T. A. Summers and S. G. Wilson, “SNR mismatch and on-line estimation in turbo decoding,” *IEEE Transactions on Communications*, vol. 46, pp. 421–423, 1998.

[208] A. Worm, P. Hoeher, and N. Wehn, “Turbo-decoding without SNR estimation,” *IEEE Communications Letters*, vol. 4, no. 6, pp. 193–195, 2000.

[209] M. A. Khalighi, “Effect of mismatched SNR on the performance of log-MAP turbo detector,” *IEEE Transactions on Vehicular Technology*, vol. 52, no. 5, pp. 1386–1397, 2003.

[210] Y. Xie, J. Li, R. Malaney, and J. Yuan, “Channel identification and its impact on quantum LDPC code performance,” in *Proceedings of the Australian Communications Theory Workshop (AusCTW)*, 2012, pp. 140–144.

[211] ——, “Improved quantum LDPC decoding strategies for the misidentified quantum depolarization channel,” in *Proceedings of the 24th European Signal Processing Conference (EUSIPCO)*, 2016, pp. 493–497.

[212] Y. Fujiwara, “Instantaneous quantum channel estimation during quantum information processing,” *arXiv preprint arXiv:1405.6267*, 2014.

[213] T. C. Bschorr, D. G. Fischer, and M. Freyberger, “Channel estimation with noisy entanglement,” *Physics Letters A*, vol. 292, no. 1, pp. 15–22, 2001.

[214] D. Collins and J. Stephens, “Depolarizing-channel parameter estimation using noisy initial states,” *Physical Review A*, vol. 92, no. 3, 2015.

[215] E. Dumitrescu and T. S. Humble, “Direct characterization of quantum dynamics with noisy ancilla,” *Physical Review A*, vol. 92, no. 5, 2015.

[216] V. Toto-Zarasoa, A. Roumy, and C. Guillemot, “Maximum likelihood BSC parameter estimation for the Slepian-Wolf problem,” *IEEE Communications Letters*, vol. 15, no. 2, pp. 232–234, 2011.

[217] G. Lechner and C. Pacher, “Estimating channel parameters from the syndrome of a linear code,” *IEEE Communications Letters*, vol. 17, no. 11, pp. 2148–2151, 2013.

[218] J. Combes, C. Ferrie, C. Cesare, M. Tiersch, G. Milburn, H. J. Briegel, and C. M. Caves, “In-situ characterization of quantum devices with error correction,” *arXiv preprint arXiv:1405.5656*, 2014.

[219] M. Tüchler, “EXIT charts of irregular codes,” in *Proceedings of the Conference on Information Sciences and Systems*, 2002, pp. 748–753.

[220] ——, “Design of serially concatenated systems depending on the block length,” *IEEE Transactions on Communications*, vol. 52, no. 2, pp. 209–218, 2004.

Subject Index

Author Index